Tenable Agent 11.1.x User Guide

Last Updated: January 21, 2026

Table of Contents

Welcome to Tenable Agent 11.1.x

Tip: The *Tenable Agent User Guide* is available in English and Japanese.

About Tenable Agents

Tenable Agents are lightweight, low-footprint, user space programs that you install locally on hosts to supplement network-based scanning or to provide visibility into gaps that network scanning misses. Tenable Agents collect vulnerability, compliance, and system data, and report that information back to a manager for analysis. With Tenable Agents, you extend scan flexibility and coverage. You can scan hosts and endpoints that intermittently connect to the internet without using credentials. You can also run large-scale concurrent agent scans with little network impact.

Tenable Agents help you address the challenges of network-based scanning, specifically for the assets where it's impossible or nearly impossible to collect information about your organization's security posture consistently. Network scanning typically occurs at selected intervals or during designated windows and requires systems to be accessible when a scan executes. If laptops or other transient devices are not accessible when a scan executes, they are excluded from the scan, leaving you unaware of vulnerabilities on those devices.

Once installed on servers, portable devices, or other assets found in today’s complex IT environments, Tenable Agents identify vulnerabilities, policy violations, misconfigurations, and malware on the hosts where they are installed and report results back to the managing product. You can manage Tenable Agents with Tenable Nessus Manager or Tenable Vulnerability Management.

For more information, see the Tenable Agents Product Page.

Agent Deployment Workflow

The following document outlines the recommended workflow for deploying Tenable Agents.

Before you begin:

- If you are using Tenable Nessus Manager to manage Tenable Agents, you must deploy and configure Tenable Nessus Manager before you deploy Tenable Agents. For more information, see Install Tenable Nessus in the *Tenable Nessus User Guide*.

- If you are using Tenable Vulnerability Management to manage your Tenable Agents, you do not need to execute a preliminary deployment.

To deploy Tenable Agents:

1. On each host, install Tenable Agents.

   As part of this step, you link the agent to the manager and verify that link. The link must be successful before you continue to the next step.

2. (Optional) On the manager, create an agent group.

3. (Optional) Modify the default agent settings.

4. (Optional) Configure a freeze window.

5. (Optional) Create agent profiles. For more information, see:

   - Agent Profiles (Tenable Nessus Manager)
   - Agent Profiles (Tenable Vulnerability Management)

6. Create a scan targeting the agent group. For more information, see:

   - Create a Scan (Tenable Nessus Manager)
   - Create a Scan (Tenable Vulnerability Management)

   As part of this step, you configure the type of scan you want the agents to perform and the scan window during which agents communicate with the manager.

   The next time an agent in the specified agent group checks in during the scan window, it will download the scan policy from Tenable Nessus Manager or Tenable Vulnerability Management, run the scan, and upload the scan results back to the manager.

Benefits and Limitations

Agent scans and network scans each have their own benefits and limitations when discovering assets and analyzing vulnerabilities on your network.

In a nutshell, network scans originate from a Tenable Nessus scanner that reaches out to the hosts targeted for scanning, while agent scans run on hosts regardless of network location or connectivity and then report the results back to the manager (for example, Tenable Nessus Manager or Tenable Vulnerability Management) when network connectivity resumes.

If network scanning is adequate for your environment and requirements, you may not need to use agents. However, for most organizations, Tenable recommends a combination of agents and network scanning to ensure full visibility into the entire network.

As you design the optimal scanning strategy for your organization's technology infrastructure, it is important to understand the differences between each scanning technology available to you. The following sections describe the benefits and limitations of each scanning method:

Non-credentialed Network Scans

A non-credentialed network scan, also known as an unauthenticated scan, is a common method for assessing the security of systems without system privileges. Non-credentialed scans enumerate a host's exposed ports, protocols, and services and identifies vulnerabilities and misconfigurations that could allow an attacker to compromise your network

Benefits

- Ideal for large-scale assessments in traditional enterprise environments.
- Discovers vulnerabilities that an outside attacker can use to compromise your network (provides a malicious adversary's point of view).
- Runs network-based plugins that an agent is restricted from performing.
- Can perform targeted operations like the brute forcing of credentials.

Limitations

- Can be disruptive; that is, can sometimes have a negative effect on the network, device, or application you are testing.
- Misses client-side vulnerabilities such as detailed patch information.
- Can miss transient devices that are not always connected to the network.

Credentialed Network Scans

A credentialed network scan, also known as an authenticated scan, provides a deeper insight than a non-credentialed scan. The scan uses credentials to log into systems and applications and can provide a definitive list of required patches and misconfigurations.

Because a credentialed scan looks directly at the installed software, including at the version numbers, it can assess items such as:

- Identifying vulnerabilities in the software.
- Evaluating password policies.
- Enumerating USB devices.
- Checking anti-virus software configurations.

It performs all these tasks with minimal to no impact on the device.

Benefits

- Consumes far fewer resources than non-credentialed scanning because the scan executes on hosts themselves rather than across the network.
- Non-disruptive; that is, does not have a negative effect on the network, device, or application you are testing.
- Provides more accurate results—a complete enumeration of software and patches installed on the host.
- Uncovers client-side software vulnerabilities.

Limitations

- Requires credentials management for each scanned host.
  - Large organizations can potentially struggle with creating service accounts with the proper rights and access needed to safely conduct a credentialed scan.
  - Password rotation requirements can add to management complexity.

  > **Note:**Tenable integrates with leading password vaults and password managers to alleviate this limitation for credentialed network scanning.

- Misses transient devices that are not always connected to the network.

Agent Scans

Tenable Agent scans use lightweight, low-footprint programs that you install locally on hosts. Tenable Agents collect vulnerability, compliance, and system data, and report that information back to Tenable Nessus Manager or Tenable Vulnerability Management for analysis. Tenable Agents are designed to have minimal impact on the system and the network, giving you the benefit of direct access to all hosts without disrupting your end users.

Benefits

- Provides extended scan coverage and continuous security:
  - Can deploy where it’s not practical or possible to run network-based scans.
  - Can assess off-network assets and endpoints that intermittently connect to the internet (such as laptops). Tenable Agents can scan the devices regardless of network location and report results back to the manager.
- Eliminates the need for credential management:
  - Doesn't require host credentials to run, so you don't need to update scan configuration credentials manually when credentials change, or share credentials among administrators, scanning teams, or organizations.
  - Can deploy where remote credentialed access is undesirable, such as Domain Controllers, DMZs, or Certificate Authority (CA) networks.
- Efficient:
  - Can reduce your overall network scanning overhead.
  - Relies on local host resources, where performance overhead is minimal.
  - Reduces network bandwidth need, which is important for remote facilities connected by slow networks.
  - Removes the challenge of scanning systems over segmented or complex networks.
  - Minimizes maintenance, because Tenable Agents can update automatically without a reboot or end-user interaction.
  - Large-scale concurrent agent scans can run with little network impact.

- Easy deployment and installation:
  - You can install and operate Tenable Agents on all major operating systems.
  - You can install Tenable Agents anywhere, including transient endpoints like laptops.
  - You can deploy Tenable Agents using software management systems such as Microsoft’s System Center Configuration Manager (SCCM).

Limitations

Agents are not designed to perform network checks, so certain plugins items cannot be checked or obtained if you deploy only agent scans. Combining network scans with agent-based scanning eliminates this gap.

- Agents miss things that can only be performed through remote connectivity, such as logging into a DB server, trying default credentials (brute force), or traffic-related enumeration.
- In situations where the agent is not allowed sufficient time for plugin updates to finish before a scan (for example, if the agent host is turned off), the agent can run scans with a dated plugin set. This is because a scheduled scan can take priority over plugin updates if it has started before the plugin update completes.

Agent Use Cases

The following sections describe various use cases for Tenable Agents.

Mobile, Distributed Workforce

Tenable recommends deploying agents for a mobile workforce, because agents eliminate the need for your employees to VPN into your organization's headquarters to have their devices scanned. In this scenario, active scanning over WAN or VPN connections incurs risks of low link speed, high encryption overhead, and possible problems with link stability. Agents can reduce scan times from hours to minutes.

To support a mobile workforce, Tenable recommends that you:

- Deploy the manager in the DMZ and assign it a publicly facing IP address that the agents can use to communicate. All communication between agent and manager occurs via TLS encrypted communication.

- Configure appropriate scan windows for agent scans. The scan window is the period of time where agents conduct their scans and report their results back to the manager. The agent discards any scan requests or results submitted after the scan window is discarded, and marks the system as not scanned.

  This approach helps ensure accurate security data while also reducing the need for duplicative and irrelevant scanning. For example, an employee returning from a two-week vacation will not have to endure 14 queued scans (one for each day their system was offline).

High Latency Networks

In Tenable Nessus network scanning, a best practice is to put the scanner close to the assets targeted for scanning and never scan across a WAN. This strategy has proven difficult for deployment scenarios where the targeted assets do not have the luxury of a local Tenable Nessus server. These scenarios include ships underway, mobile military operations, and areas with high latency and low bandwidth. These networks typically rely on satellite connections for connectivity. The network burden that a port, protocol, and service scan produces when running a full active scan can easily take down a satellite connection.

Tenable Agents help solve this problem by significantly minimizing network traffic related to scanning.

There are three types of data transmitted when using Tenable Agents:

- Command and control data — Transmitted from the manager to Tenable Agents, this data represents the who, what, when, where and how needed to complete the task of local scanning. This data is the smallest set of data that traverses the network.

- Results data — Result data varies in size due to the scan configuration. Historically, compliance scans are larger than vulnerability scans. This data transmits back to the manager for aggregation. Update data is the largest data type transmitted using Tenable Agents.

- Updates — When you install a Tenable Agent and link it to a Tenable Nessus Manager, the agent downloads a full set of plugins. Once that first full download completes, the agent only downloads incremental plugin updates. This approach drastically reduces the ongoing network traffic by only pulling content deltas across the network. Also, you can handle code updates by patch management systems like System Center Configuration Manager (SCCM) or Yellowdog Updater Modified (YUM), or via the manager itself.

Hardened Systems

Active network scanning using scanners such as Tenable Nessus Professional has long been the preferred method for scanning systems in the enterprise environment. Active scanning is done remotely and requires access to key services that are typically disabled as part of system hardening (for example, Remote Registry access). The hardening of systems can actually limit the data collected by active scanning. Compounding this problem is that enumeration of key services requires credential scanning. To access key datasets, elevated privileges are required (that is, root, local admin, or domain admin). Many security professionals are hesitant to use these elevated privileges across the network. On high-value targets such as domain controllers, this caution is further elevated.

Tenable Agents do not require elevated privileges or extra accounts because they operate at the system level. The use of agents allows a low-risk approach to scanning hardened systems without requiring that you reduce security. You can effectively eliminate the need for credentials while scanning at the system level.

Deployment Considerations

All organizations face their own unique challenges for deploying technology, and as such, these deployment considerations are not a step-by-step guide for deploying Tenable Agents. Consult the Tenable technical support team to address specific product issues. You can also contact the Tenable Professional Services team for product integration requirements, complex deployment scenarios, and product training.

The following sections contain deployment guidance:

- General Considerations
- Large-scale Deployment Considerations (more than 10,000 hosts)

File and Process Allow List

Tenable recommends allowing the following Tenable Agent folders and processes in first-party and third-party endpoint security products such as anti-virus applications and host-based intrusion and prevention systems.

For information about allowlisting Tenable Nessus processes, see File and Process Allowlist in the *Tenable Nessus User Guide*.

Note: In addition to the folders and processes listed below, Tenable recommends allowlisting certain Tenable sites on your firewall. For more information, see the Which Tenable sites should I allow? KB article.

Windows
Folders
Tip: If your Windows installation uses a non-standard drive or folder structure, you can use the `%PROGRAMFILES%` and `%PROGRAMDATA%` environment variables.
C:\Program Files\Tenable\Nessus Agent*
C:\Program Files (x86)\Tenable\Nessus Agent*
Processes
C:\Program Files\Tenable\Nessus Agent\nasl.exe
C:\Program Files\Tenable\Nessus Agent\nessuscli.exe
C:\Program Files\Tenable\Nessus Agent\nessusd.exe
C:\Program Files\Tenable\Nessus Agent\nessus-service.exe
C:\Program Files\Tenable\Nessus Agent\nessus-agent-module.exe
C:\Program Files (x86)\Tenable\Nessus Agent\nasl.exe
C:\Program Files (x86)\Tenable\Nessus Agent\nessuscli.exe
C:\Program Files (x86)\Tenable\Nessus Agent\nessusd.exe
C:\Program Files (x86)\Tenable\Nessus Agent\nessus-service.exe
C:\Program Files (x86)\Tenable\Nessus Agent\nessus-agent-module.exe
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\libcrypto-3*.dll
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\libssl-3*.dll
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\nasl.exe

C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\nessuscli.exe
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\nessusd.exe
C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\pre-install-check\nessus-agent-module.exe
C:\ProgramData\Tenable\Nessus Agent\nessus\agent.db
%SystemRoot%\tenable_ovaldi_2ef350e0435440418f7d33232f74f260.exe
%SystemRoot%\tenable_mw_scan_*.exe
%SystemRoot%\temp\nessus_*.bat
%SystemRoot%\tenable_ovaldi_2ef350e0435440418f7d33232f74f260.exe
%SystemRoot%\Tenable\Nessus Agent\tenable_mw_scan_*.exe
%SystemRoot%\Tenable\Nessus Agent\temp\nessus_*.bat
Linux
Folders
/opt/nessus_agent/sbin/*
/opt/nessus_agent/bin/*
/opt/nessus_agent/lib/nessus/*
Files
/opt/nessus_agent/bin/nasl
/opt/nessus_agent/sbin/nessusd
/opt/nessus_agent/sbin/nessuscli
/opt/nessus_agent/sbin/nessus-service
/opt/nessus_agent/sbin/nessus-agent-module
/opt/nessus_agent/var/nessus/tmp/pre-install-check/libssl.so.3

/opt/nessus_agent/var/nessus/tmp/pre-install-check/libcrypto.so.3
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nasl
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessuscli
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessusd
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessus-agent-module
/opt/nessus_agent/var/nessus/tmp/pre-install-check/openssl
/opt/nessus_agent/var/nessus/agent.db
Processes
/opt/nessus_agent/bin/nasl
/opt/nessus_agent/bin/openssl
/opt/nessus_agent/sbin/nessusd
/opt/nessus_agent/sbin/nessuscli
/opt/nessus_agent/sbin/nessus-service
/opt/nessus_agent/sbin/nessus-agent-module
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nasl
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessuscli
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessusd
/opt/nessus_agent/var/nessus/tmp/pre-install-check/nessus-agent-module
/opt/nessus_agent/var/nessus/tmp/pre-install-check/openssl
macOS
Folders
/Library/NessusAgent/run/sbin/*
/Library/NessusAgent/run/bin/*

Files
/Library/NessusAgent/run/bin/nasl
/Library/NessusAgent/run/sbin/nessusd
/Library/NessusAgent/run/sbin/nessuscli
/Library/NessusAgent/run/sbin/nessus-service
/Library/NessusAgent/run/sbin/nessus-agent-module
/Library/NessusAgent/run/sbin/nessusmgt
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nasl
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessuscli
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessusd
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessus-agent-module
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/openssl
/Library/NessusAgent/run/var/nessus/agent.db
Processes
/Library/NessusAgent/run/bin/nasl
/Library/NessusAgent/run/bin/openssl
/Library/NessusAgent/run/sbin/nessusd
/Library/NessusAgent/run/sbin/nessuscli
/Library/NessusAgent/run/sbin/nessus-service
/Library/NessusAgent/run/sbin/nessus-agent-module
/Library/NessusAgent/run/sbin/nessusmgt
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nasl
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessuscli

/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessusd
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/nessus-agent-module
/Library/NessusAgent/run/var/nessus/tmp/pre-install-check/openssl

General Considerations

The following are some common questions that you should answer before deploying Tenable Agents:

> **Note:** In addition to these deployment considerations, Tenable recommends reviewing the Tenable Agent General Best Practices.

- What operating system do you plan to deploy the Tenable Agent on?
  - Linux (Debian/RHEL/Fedora/Ubuntu)
  - Windows (Win 10, Win Server 2012/2016 R2)
  - OS X (10.8+)
- How many Tenable Agents do you plan to deploy?
  - Fewer than 1,000
  - More than 1,000 and fewer than 5,000
  - More than 5,000 and fewer than 10,000
  - More than 10,000

  > **Note:** In deployment scenarios with more than 10,000 agents you should consider optimizing performance with agent group sizing and scan staggering as discussed in Large-Scale Deployments.
- What are the typical hardware specifications of the hosts where you want to install Tenable Agents? For example, consider disk space, disk type and speed, CPU, cores, and RAM.
- Are there any countermeasures that exist on the host that would prevent the egress communications from the Tenable Agent to the Tenable Nessus Manager (DST: TCP/8834 [default, customizable])?

- Are there any countermeasures that exist on the host that would prevent the agent process from executing?

  > **Note:** See File and Process Allow List for a list of files and processes to allow per operating system.

- How do you plan to deploy Tenable Agents across the enterprise? For example, do you want to use an enterprise deployment technology such as Active Directory, SMS, Microsoft SCCM, and/or Red Hat Satellite?
- Do you want to deploy Tenable Agents to virtual or non-persistent systems? If so, consider adding the agent to your base device template. Tenable recommends that you review your organization's process for commissioning and decommissioning virtual/non-persistent hosts to ensure successful activation or deactivation of the Tenable Agents.
- How do you plan to track the ratio of potentially deployable agent assets to actual assets with deployed agents?
- How do you plan to track the health and status of the agent on the host? For example, you might want to monitor for condition *x* (where *x* is the status of the service or the registration status of the agent); if that condition is present, you might then trigger an action or notification.
- What naming schema would best fit the infrastructure where deployed agents exist? It is important to plan how you would like to organize the breakdown of hosts running agents.
- Do you plan to supplement agent-based scanning with network scans? How do you plan to maintain vulnerability information across agent and network scans? How do you plan to manage multiple repositories?

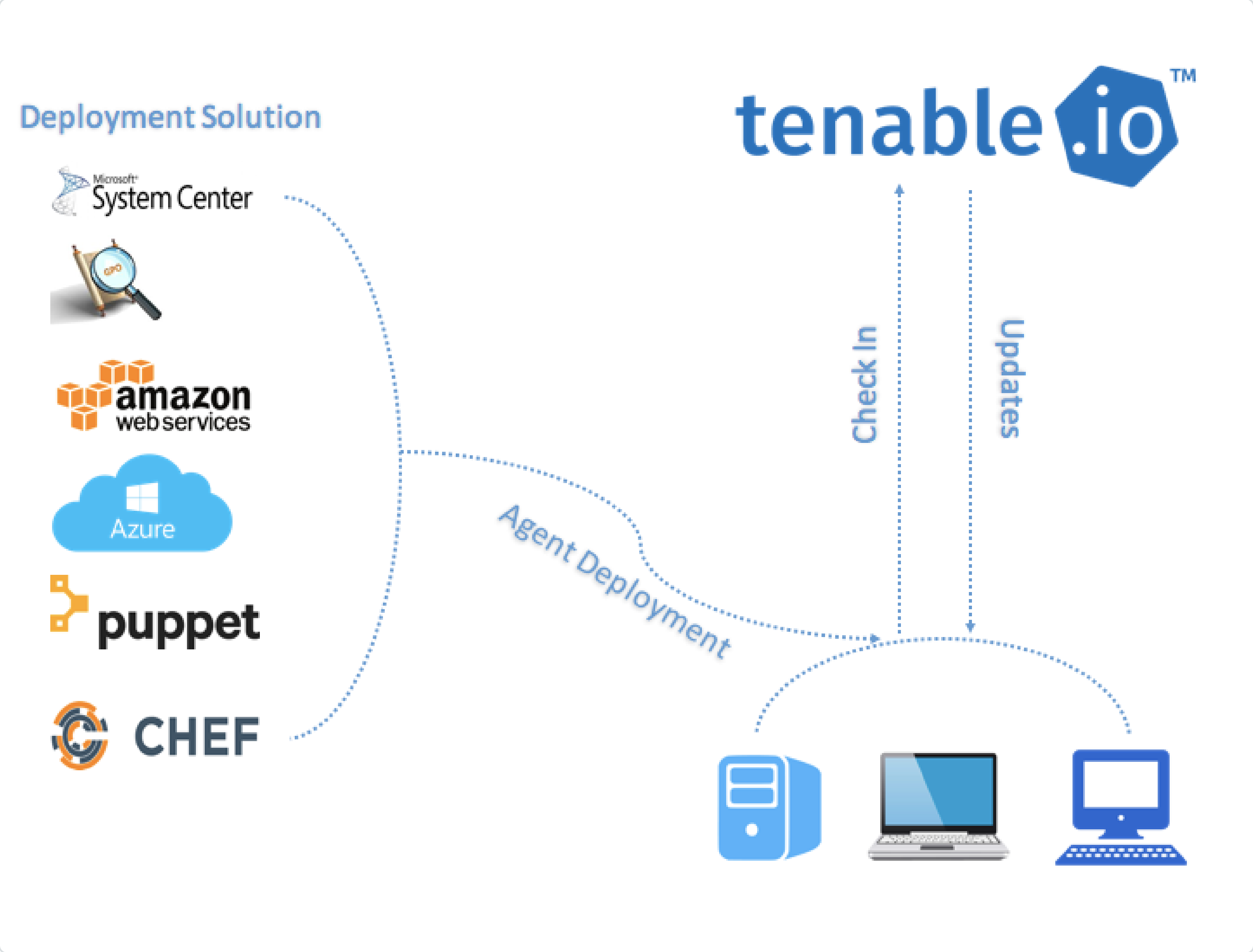
Large-scale Deployment Considerations

If you want to deploy agents across a large-scale environment, your deployment strategy must ensure that all agents are continuously active and stay connected to Tenable Vulnerability Management or Tenable Nessus Manager.

> **Note:** In addition to these deployment considerations, Tenable recommends reviewing the Tenable Agent General Best Practices.

Deployment Strategy

When deploying many agents, consider using software to push agents through the network. For example:



Tenable recommends that you deploy batches of agents over a 24-hour period when deploying a large number of agents. This is especially helpful if you have a limited network bandwidth and need to limit the amount of data your network is downloading at one time.

After you install an agent, it receives its first plugin update once it receives instructions to run an assessment. The agent sets a timer to attempt the next update 24 hours from the initial plugin update time (and update the plugin update date on subsequent successful plugin downloads). Deploying your agents in batches also prevents too many agents from checking for product updates at one time and consuming too much bandwidth.

An agent links to Tenable Nessus Manager or Tenable Vulnerability Management after a random delay ranging from zero to five minutes. This delay occurs when the agent initially links, and also when the agent restarts either manually or through a system reboot. Enforcing a delay reduces network traffic when deploying or restarting large amounts of agents, and reduces the load on Tenable Nessus Manager or Tenable Vulnerability Management.

Clustering

With Tenable Nessus Manager clustering, you can deploy and manage large numbers of agents from a single Tenable Nessus Manager instance. For Tenable Security Center users with over 10,000 agents and up to 200,000 agents, you can manage your agent scans from a single Tenable Nessus Manager cluster, rather than needing to link multiple instances of Tenable Nessus Manager to Tenable Security Center.

A Tenable Nessus Manager instance with clustering enabled acts as a *parent node* to *child nodes*, each of which manage a smaller number of agents. Once a Tenable Nessus Manager instance becomes a parent node, it no longer manages agents directly. Instead, it acts as a single point of access where you can manage scan policies and schedules for all the agents across the child nodes. With clustering, you can scale your deployment size more easily than if you had to manage several different Tenable Nessus Manager instances separately.

Example scenario: Deploying 100,000 agents

You are a Tenable Security Center user who wants to deploy 100,000 agents, managed by Tenable Nessus Manager.

Without clustering, you deploy 10 Tenable Nessus Manager instances, each supporting 10,000 agents. You must manually manage each Tenable Nessus Manager instance separately, such as setting agent scan policies and schedules, and updating your software versions. You must separately link each Tenable Nessus Manager instance to Tenable Security Center.

With clustering, you use one Tenable Nessus Manager instance to manage 100,000 agents. You enable clustering on Tenable Nessus Manager, which turns it into a parent node, a management point for child nodes. You link 10 child nodes, each of which manages around 10,000 agents. You can either link new agents or migrate existing agents to the cluster. The child nodes receive agent scan policy, schedule, and plugin and software updates from the parent node. You link only the Tenable Nessus Manager parent node to Tenable Security Center.

Note: All Tenable Nessus nodes in a cluster must be on the same version (for example, using the clustering example above, the Tenable Nessus Manager parent node and 10 children nodes need be on the same Tenable Nessus version). Otherwise, the cluster deployment is unsupported.

For more information, see Clustering in the *Tenable Nessus User Guide*.

Agent Groups

Tenable recommends that you size agent groups appropriately, particularly if you are managing scans in Tenable Nessus Manager or Tenable Vulnerability Management and then importing the scan data into Tenable Security Center. You can size agent groups when you manage agents in Tenable Nessus Manager or Tenable Vulnerability Management.

The more agents that you scan and include in a single agent group, the more data that the manager must process in a single batch. The size of the agent group determines the size of the `.nessus` file that must be imported into Tenable Security Center. The `.nessus` file size affects hard drive space and bandwidth.

Group Sizing

Product	Agents Assigned per Group
Tenable Vulnerability Management	Unlimited agents per group if not sending to Tenable Security Center 20,000 agents per group if sending to Tenable Security Center
Tenable Nessus Manager	Unlimited agents per group if not sending to Tenable Security Center 20,000 agents per group if sending to Tenable Security Center
Tenable Nessus Manager Clusters	Unlimited since scans are automatically broken up as appropriate by separate child nodes.

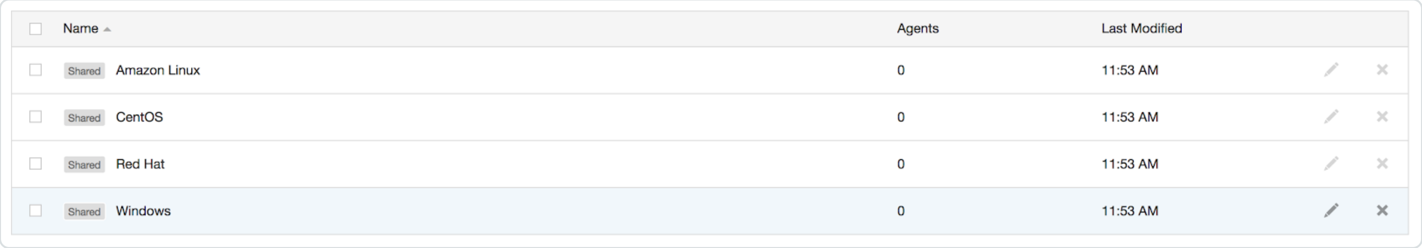
Caution: If you scan multiple groups of agents in a single scan, the total number of agents per scan might not match the total number of agents per group. For example, if you have three groups of 7,500 agents in Tenable Vulnerability Management, all in one scan, then data for 22,500 agents would be imported into Tenable Security Center at one time and may overwhelm it.

Group Types

Before you deploy agents to your environment, create groups based on your scanning strategy.

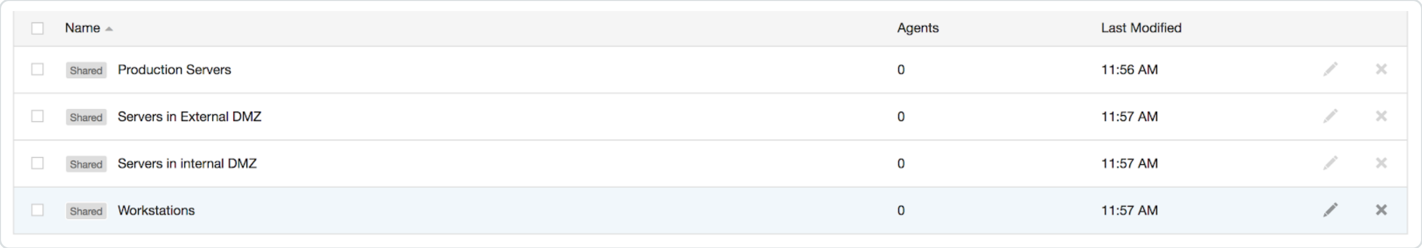
The following are example group types:

Operating System



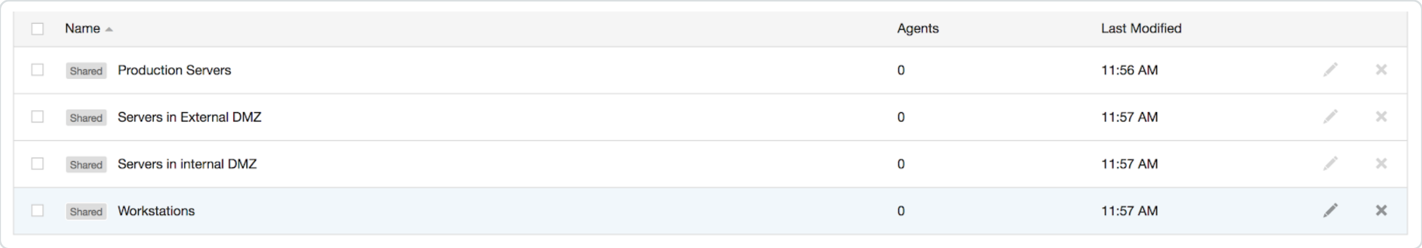
□	Name ▲	Agents	Last Modified		
□	Shared Amazon Linux	0	11:53 AM	✎	✕
□	Shared CentOS	0	11:53 AM	✎	✕
□	Shared Red Hat	0	11:53 AM	✎	✕
□	Shared Windows	0	11:53 AM	✎	✕

Asset Type or Location



□	Name ▲	Agents	Last Modified		
□	Shared Production Servers	0	11:56 AM	✎	✕
□	Shared Servers in External DMZ	0	11:57 AM	✎	✕
□	Shared Servers in internal DMZ	0	11:57 AM	✎	✕
□	Shared Workstations	0	11:57 AM	✎	✕

You can also add agents to more than one group if you have multiple scanning strategies.



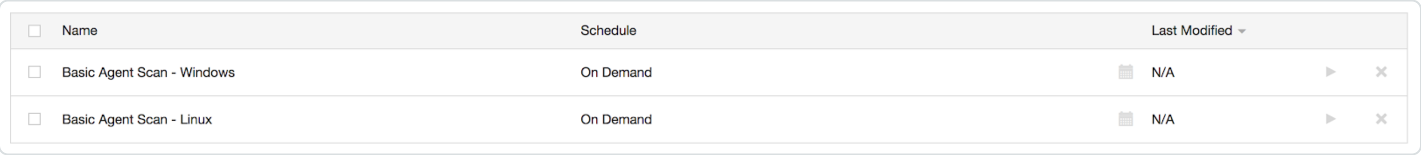
□	Name ▲	Agents	Last Modified		
□	Shared Production Servers	0	11:56 AM	✎	✕
□	Shared Servers in External DMZ	0	11:57 AM	✎	✕
□	Shared Servers in internal DMZ	0	11:57 AM	✎	✕
□	Shared Workstations	0	11:57 AM	✎	✕

Scan Profile Strategy

Once you deploy agents to all necessary assets, you can create scan profiles and tie them to existing agent groups. The following section describes a few scan strategies.

Operating System Scan Strategy

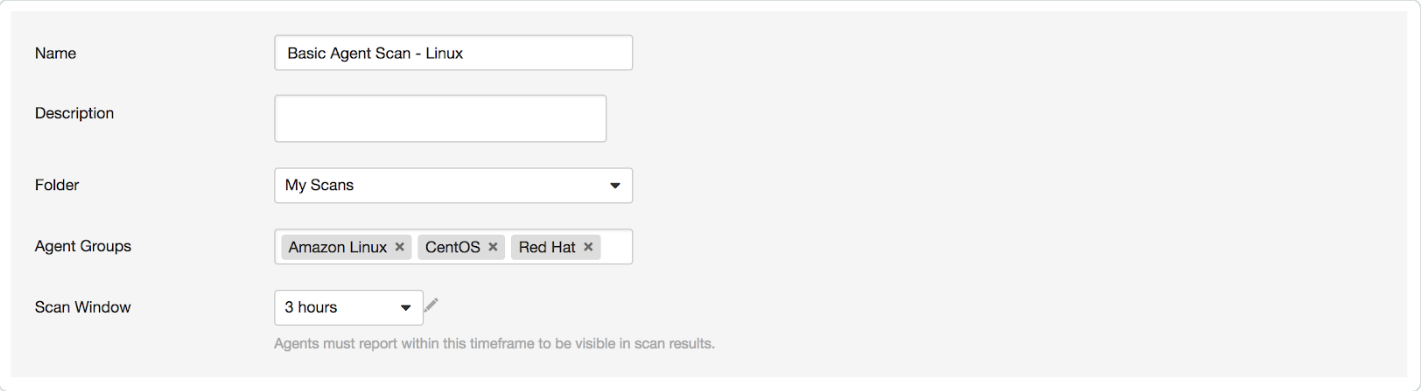
The following strategy is useful if your scanning strategy is based off of the operating system of an asset.



□	Name	Schedule		Last Modified		
□	Basic Agent Scan - Windows	On Demand	📅	N/A	▶	✕
□	Basic Agent Scan - Linux	On Demand	📅	N/A	▶	✕

Basic Agent Scan - Linux

In this example, a scan is created based on the **Basic Agent Scan** template, and is assigned the group *Amazon Linux*, *CentOS*, and *Red Hat*. This scan only scans these assets.



Name: Basic Agent Scan - Linux

Description:

Folder: My Scans

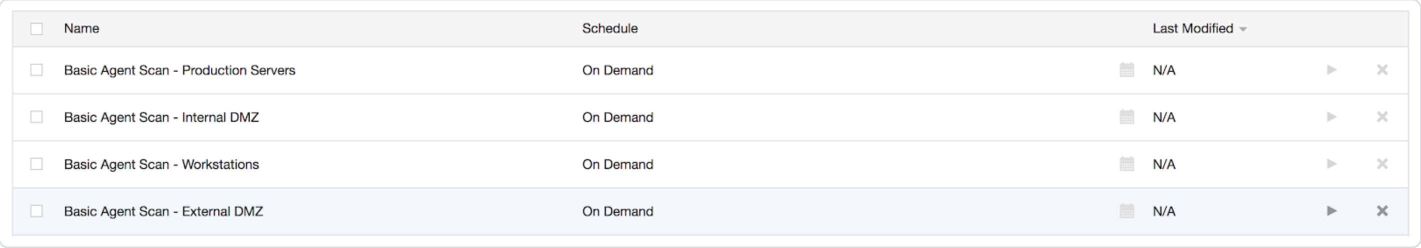
Agent Groups: Amazon Linux ✕ CentOS ✕ Red Hat ✕

Scan Window: 3 hours

Agents must report within this timeframe to be visible in scan results.

Asset Type or Location Scan Strategy

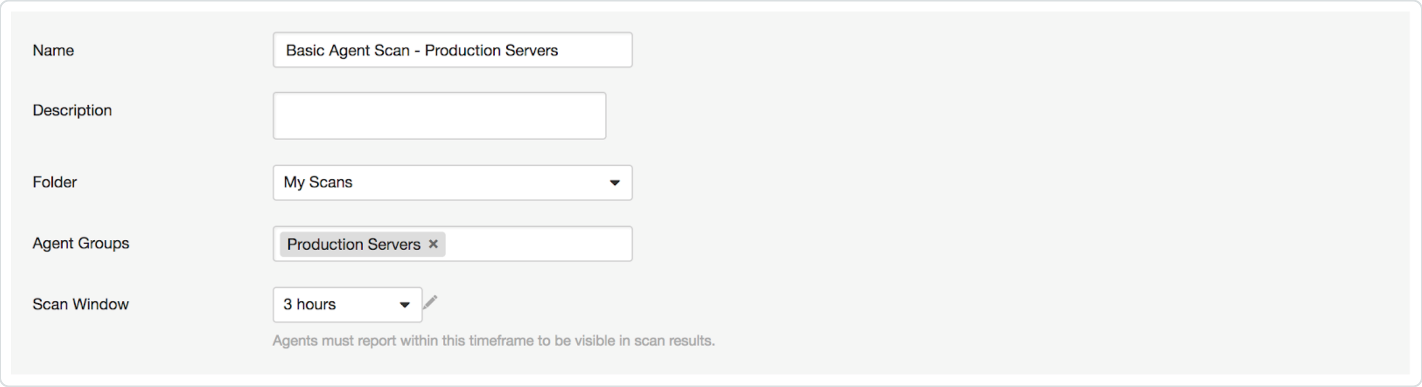
The following strategy is useful if your scanning strategy is based off of the asset type or location of an asset.



□	Name	Schedule		Last Modified		
□	Basic Agent Scan - Production Servers	On Demand	📅	N/A	▶	✕
□	Basic Agent Scan - Internal DMZ	On Demand	📅	N/A	▶	✕
□	Basic Agent Scan - Workstations	On Demand	📅	N/A	▶	✕
□	Basic Agent Scan - External DMZ	On Demand	📅	N/A	▶	✕

Basic Agent Scan - Production Servers

In this example, a scan is created a scan based on the **Basic Agent Scan** template, and is assigned the group *Production Servers.* This scan only scans production server assets.

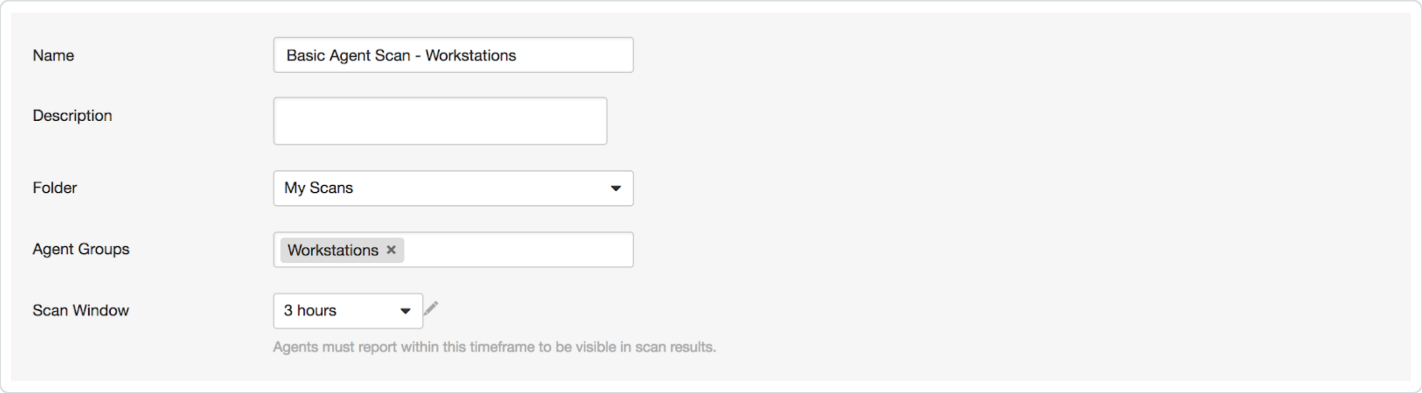


Name	Basic Agent Scan - Production Servers
Description	
Folder	My Scans
Agent Groups	Production Servers ×
Scan Window	3 hours

Agents must report within this timeframe to be visible in scan results.

Basic Agent Scan - Workstations

In this example, a scan is created based on the **Basic Agent Scan** template, and is assigned the group *Workstations*. This scan only scans workstation assets.



Name	Basic Agent Scan - Workstations
Description	
Folder	My Scans
Agent Groups	Workstations ×
Scan Window	3 hours

Agents must report within this timeframe to be visible in scan results.

Note: You may want to configure workstation scans with longer scan windows, as most organizations cannot guarantee when these systems are online (as opposed to servers which are typically on 24/7).

Scan Staggering

While scans with the Tenable Agents are more efficient in many ways than network scans, scan staggering is something to consider on certain types of systems.

For example, if you install Tenable Agents on virtual machines, you may want to distribute agents among several groups and have their associated scan windows start at slightly different times.

Staggering scans limits the one-time load on the virtual host server, because agents run their assessments as soon as possible at the start of the scan window. Oversubscribed or resource-limited virtual environments may experience performance issues if agent assessments start on all systems at the same time.

Best Practices for Tenable Agents

The following sections contain best practice guidance:

General Best Practices

Note: For agent deployment best practices and considerations, see Deployment Considerations.

- With network scans, never scan through or try to bypass devices such as firewalls, switches, etc., that are designed to obfuscate or impede scans (for example, network address translation).
- Either put Tenable Nessus scanners in every segment, closest to the host, *or* run agents locally on the system, which does not require explicitly making an overage of firewall rules. Both solutions require minimal firewall rules to provide connectivity when implemented correctly.
- For full visibility into your network, Tenable recommends that you combine agent-based and network scanning to identify risk across your entire network. This approach is especially important for organizations in the United States Federal Government as there are specific laws and acts that mandate you evaluate the entire spectrum of your risk.
- For shared resource environments, such as VDI or ESXi, Tenable recommends setting agents' Plugin Compilation Performance to `medium` or `low` to ensure that agents have a minimal impact on CPU usage when compiling plugins.

Data Aggregation in a Hybrid Environment

This section briefly identifies areas to consider when aggregating Tenable Agent data from Tenable Nessus Manager into Tenable Security Center repositories. It is important to note that communications to the Tenable Nessus Manager for data retrieval initiate from Tenable Security Center. Once Tenable Agent data is imported, all normal Tenable Security Center operations such as vulnerability analysis, compliance, and workflow automation apply.

- Carefully consider agent group size to reduce the volume of data being imported into Tenable Security Center at a given time. Tenable recommends limiting the number of agents per scan in Tenable Nessus Manager or Tenable Vulnerability Management to 1,000 agents. Importing large amounts of data to Tenable Security Center while parallel operations are occurring impacts Tenable Security Center performance.

- Properly plan the number of Tenable Nessus scanners and Tenable Nessus Managers connected to Tenable Security Center, seeking guidance from Tenable technical support staff if needed.
- Properly plan the number of concurrent scans to include agent scans (agent data retrieval process), concurrent users, number of dashboards configured, and frequency/type of reports operating on a Tenable Security Center, seeking guidance from Tenable technical support staff if needed.

System Requirements

This section includes information related to the requirements necessary to install Tenable Agents.

- Hardware
- Software
- Dataflow
- Licensing
- Agent CPU Resource Control
- Performance Metrics
  - Tenable Agent Performance
    - Software Footprint
    - Agent Lifecycle & Bandwidth
  - Tenable Nessus Manager Performance

Hardware Requirements

Tenable Agents

Tenable Agents is a lightweight, user space program and only use minimal system resources.

Generally, an agent uses 50 MB to 60 MB of RAM (all pageable). However, agents use additional memory when scanning (all pageable; the amount of memory depends on the scan configuration) and when updating plugins (all pageable). Agents use almost no CPU while idle, but they are designed to use up to 100% of CPU when available during jobs.

For more information on Tenable Agent resource usage, see Tenable Agent Performance.

The following table outlines the minimum recommended hardware for operating a Tenable Agent. You can install Tenable Agents on a virtual machine that meets the same requirements specified.

Hardware	Minimum Requirement
Processor	1 dual-core CPU
Processor Speed	> 1 GHz
RAM	> 1 GB
Disk Space	> 3 GB, not including space used by the host operating system The agent may require more space during certain processes, such as applying a plugin update. The selected scan frequency, volume of findings, and log rotation options impact agent disk utilization. If disk space is a chief concern in your deployment scenario, Tenable recommends allocating up to 4 GB (not including space used by the host operating system).
Disk Speed	15-50 IOPS

Note: You can control the priority of the Tenable Agent relative to the priority of other tasks running on the system. For more information see Agent CPU Resource Control.

Tenable Nessus Manager

Scenario	Minimum Recommended Hardware
Tenable Nessus Manager with 0-	**CPU** — 4 2GHz cores **Memory** — 16 GB RAM **Disk space**

Scenario	Minimum Recommended Hardware
10,000 agents	• Environments with triggered agent scanning — 5 MB ***x*** the number of agents ***x*** (the number of times those agents are triggered over seven days if initiating scans through Tenable Nessus Manager **or** the number of times those agents are triggered over two days if initiating scans through Tenable Security Center) **+** 6,644 MB For example: • If a standalone Tenable Nessus Manager is scanning daily with 1,100 agents, the disk space requirement is 5 MB x 1,100 x 7 + 6,644 MB = **45,114 MB** (**44.09 GB**). • If Tenable Nessus Manager, managed by Tenable Security Center, is scanning daily with 1,100 agents, the disk space requirement is 5 MB x 1,100 x 2 + 6,644 MB = **17,664 MB** (**17.23 GB**). • Environments without triggered agent scanning — 5 GB per 5,000 agents per concurrent scan + 6 GB **Note:** Scan results and plugin updates require more disk space over time.
Tenable Nessus Manager with 10,001-20,000 agents	**CPU** — 8 2GHz cores **Memory** — 32 GB RAM **Disk space** • Environments with triggered agent scanning — 5 MB ***x*** the number of agents ***x*** (the number of times those agents are triggered over seven days if initiating scans through Tenable Nessus Manager **or** the number of times those agents are triggered over two days if initiating scans through Tenable Security Center) **+** 6,644 MB For example: • If a standalone Tenable Nessus Manager is scanning daily with 15,000 agents, the disk space requirement is 5 MB x 15,000 x 7 + 6,644 MB = **531,644 MB** (**519.18 GB**).

Scenario	Minimum Recommended Hardware
	• If Tenable Nessus Manager, managed by Tenable Security Center, is scanning daily with 15,000 agents, the disk space requirement is 5 MB x 15,000 x 2 + 6,644 MB = **156,644 MB** (**152.97 GB**). • Environments without triggered agent scanning — 5 GB per 5,000 agents per concurrent scan + 6 GB **Notes:** • Scan results and plugin updates require more disk space over time. • Engage with your Tenable representative for large deployments.

Software Requirements

Tenable Agent supports the following Linux, macOS, and Windows operating systems:

> **Notes:**
>
> - Tenable Agent does not require an external runtime environment, such as Java.
> - Microsoft Visual C++ Redistributable 14.22 is included as part of a bundled license package with Tenable Agent.
> - Tenable Agent requires Windows host systems to be running the latest version of Universal Microsoft C Runtime Library (UCRT) and PowerShell 5.0 or newer. Some older versions of Microsoft Windows require a minimum update to work with Tenable Agent.
> - Tenable Agent only supports the 4 KB base page size on Linux AArch64 architecture.
> - Tenable does not currently support AWS Fargate integration.

Tenable Agent 11.1

Operating System	Supported Versions	Supported Architecture
Linux	AlmaLinux 8.10 and 9.5	x86_64 AArch64

	Amazon Linux 2023, Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9 and 10	x86_64
	Debian 11, 12, and 13	x86_64
	Kali Linux 2017, 2018, 2019, and 2020	x86_64
	Fedora 42 and 43	x86_64
	Miracle Linux 9	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64 AArch64
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.6, 8.8, 8.10, 9.0, 9.2, 9.4, 9.6 and later, and 10	x86_64 AArch64
	Rocky Linux 8.10, 9.5, and 10	x86_64 AArch64
	SUSE 12 SP5, SUSE Enterprise 15 SP3 and later	x86_64
	TencentOS	x86_64
	Ubuntu 16.04, 18.04, 20.04, 22.04, and 24.04	x86_64
	Ubuntu 18.04, 20.04, 22.04, and 24.04	AArch64
macOS	macOS 14, 15, and 26	x86_64 Apple Silicon
Windows	Windows 10 and 11	x86_64 ARM64
	Windows Server 2012, 2012 R2, 2016, 2019, 2022, and 2025	x86_64

Tenable Agent 11.0

Operating System	Supported Versions	Supported Architecture
Linux	AlmaLinux 8.10 and 9.5	x86_64 AArch64
	Amazon Linux 2023, Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9 and 10	x86_64
	Debian 11 and 12	x86_64
	Kali Linux 2017, 2018, 2019, and 2020	x86_64
	Fedora 41 and 42	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64 AArch64
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4, 8.6, 8.8, 8.10, 9.0, 9.2, 9.4 and later, and 10	x86_64 AArch64
	Rocky Linux 8.10 and 9.5	x86_64 AArch64
	SUSE 12 SP5, SUSE Enterprise 15 SP3 and later	x86_64
	TencentOS	x86_64
	Ubuntu 16.04, 18.04, 20.04, 22.04, and 24.04	x86_64
	Ubuntu 18.04, 20.04, 22.04, and 24.04	AArch64
macOS	macOS 13, 14, 15, and 26	x86_64 Apple Silicon

Windows	Windows 10	x86
	Windows 10 and 11	x86_64
	Windows Server 2012, 2012 R2, 2016, 2019, 2022, and 2025	x86_64

Tenable Agent 10.9

Operating System	Supported Versions	Supported Architecture
Linux	AlmaLinux 8.10 and 9.5	x86_64 AArch64
	Amazon Linux 2023, Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11 and 12	x86_64
	Kali Linux 2017, 2018, 2019, and 2020	x86_64
	Fedora 41 and 42	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64 AArch64
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4, 8.6, 8.8, 8.10, 9.0, 9.2, and 9.4 and later	x86_64 AArch64
	Rocky Linux 8.10 and 9.5	x86_64 AArch64
	SUSE 12 SP5, SUSE Enterprise 15 SP3 and later	x86_64
	TencentOS	x86_64

	Ubuntu 16.04, 18.04, 20.04, 22.04, and 24.04	x86_64
	Ubuntu 18.04, 20.04, 22.04, and 24.04	AArch64
macOS	macOS 13, 14, and 15	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10 and 11	x86_64
	Windows Server 2012, 2012 R2, 2016, 2019, 2022, and 2025	x86_64

Tenable Agent 10.8

Operating System	Supported Versions	Supported Architecture
Linux	AlmaLinux 8.10 and 9.5	x86_64 AArch64
	Amazon Linux 2023, Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11 and 12	x86_64
	Kali Linux 2017, 2018, 2019, and 2020	x86_64
	Fedora 40	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64 AArch64
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4, 8.6, 8.8, 8.10, 9.0, 9.2, and 9.4 and later	x86_64 AArch64

	Rocky Linux 8.10 and 9.5	x86_64 AArch64
	SUSE 12 SP5, SUSE Enterprise 15 SP2 and later	x86_64
	TencentOS	x86_64
	Ubuntu 16.04, 18.04, 20.04, 22.04, and 24.04	x86_64
	Ubuntu 18.04, 20.04, 22.04, and 24.04	AArch64
macOS	macOS 13, 14, and 15	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10 and 11	x86_64
	Windows Server 2012, 2012 R2, 2016, 2019, 2022, and 2025	x86_64

Tenable Agent 10.7

Operating System	Supported Versions	Supported Architecture
Linux	AlmaLinux 8.10 and 9.5	x86_64 AArch64
	Amazon Linux 2023, Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64
	Debian 11 and 12	x86_64
	Kali Linux 2017, 2018, 2019, and 2020	x86_64
	Fedora 38 and 39	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64

		AArch64
	Red Hat EL 7.9	x86_64
	Red Hat EL 8.4, 8.6, 8.8, 8.10, 9.0, 9.2, and 9.4 and later	x86_64 AArch64
	Rocky Linux 8.10 and 9.5	x86_64 AArch64
	SUSE 12 SP5, SUSE Enterprise 15 SP2 and later	x86_64
	TencentOS	x86_64
	Ubuntu 16.04, 18.04, 20.04, 22.04, and 24.04	x86_64
	Ubuntu 18.04, 20.04, 22.04, and 24.04	AArch64
macOS	macOS 12, 13, 14, and 15	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10 and 11	x86_64
	Windows Server 2012, 2012 R2, 2016, 2019, and 2022	x86_64

Tenable Agent 10.6

Operating System	Supported Versions	Supported Architecture
Linux	AlmaLinux 8.10 and 9.5	x86_64 AArch64
	Amazon Linux 2023, Amazon Linux 2	x86_64 AArch64
	CentOS Stream 9	x86_64

	Debian 11 and 12	x86_64
	Kali Linux 2017, 2018, 2019, and 2020	x86_64
	Fedora 38 and 39	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 6, 7, 8, and 9	x86_64 AArch64
	Red Hat EL 6.x and 7.9	x86_64
	Red Hat EL 8.4, 8.6, 8.8, 8.10, 9.0, 9.2, and 9.4 and later	x86_64 AArch64
	Rocky Linux 8.10 and 9.5	x86_64 AArch64
	SUSE 12 SP5, SUSE Enterprise 15 SP2 and later	x86_64
	TencentOS	x86_64
	Ubuntu 14.04, 16.04, 18.04, 20.04, and 22.04	x86_64
	Ubuntu 18.04, 20.04, and 22.04	AArch64
macOS	macOS 12, 13, and 14	x86_64 Apple Silicon
Windows	Windows 10	x86
	Windows 10 and 11	x86_64
	Windows Server 2012, 2012 R2, 2016, 2019, and 2022	x86_64

Customize SELinux Enforcing Mode Policies

Security-Enhanced Linux (SELinux) enforcing mode policies require customization to interact with Tenable Agents.

Tenable Support does not assist with customizing SELinux policies, but Tenable recommends monitoring your SELinux logs to identify errors and solutions for your policy configuration.

Before you begin:

- Install the SELinux `sealert` tool in a test environment that resembles your production environment.

To monitor your SELinux logs to identify errors and solutions:

1. Run the `sealert` tool, where `/var/log/audit/audit.log` is the location of your SELinux audit log:

   ```
   sealert -a /var/log/audit/audit.log
   ```

   The tool runs and generates a summary of error alerts and solutions. For example:

   ```
   SELinux is preventing /usr/sbin/sshd from write access on the sock_file /dev/log
   SELinux is preventing /usr/libexec/postfix/pickup from using the rlimitinh access
   on a process.
   ```

2. Execute the recommended solution for each error alert.

3. Restart Tenable Agent.

4. Run the `sealert` tool again to confirm you resolved the error alerts.

Port Requirements

Tenable Agent port requirements include Tenable Agent-specific requirements and manager-specific requirements. Depending on your deployment setup, see the Tenable Nessus Manager and Tenable Nessus Cluster Nodes and Tenable Security Center port requirements.

Tenable Agent

Your Tenable Agents require access to specific ports for outbound traffic.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 443	Communicating with Tenable Vulnerability Management.
TCP 8834	Communicating with Tenable Nessus Manager. **Note:** The default Tenable Nessus Manager port is TCP 8834. However, this port is configurable and may be different for your organization.
UDP 53	External DNS support for the host that Tenable Agent is installed on. Several plugins use DNS resolution in their operation.

> **Note:** Operating system installation commands, such as `dnf install`, may require other connections besides Tenable Vulnerability Management or Tenable Nessus Manager. Consult your operating system administrator for more information.

Tenable Nessus Manager and Tenable Nessus Cluster Nodes

Your Tenable Nessus instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 8834	Accessing the Tenable Nessus interface. Communicating with Tenable Security Center. Interacting with the API.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 25	Sending SMTP email notifications.
TCP 443	Communicating with Tenable Vulnerability Management (sensor.cloud.tenable.com or sensor.cloud.tenablecloud.cn).

Port	Traffic
	Communicating with the `plugins.nessus.org` server for plugin updates.
UDP 53	Performing DNS resolution.

Tenable Security Center

Your Tenable Security Center instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 22	Performing remote repository synchronization with another Tenable Security Center.
TCP 443	Accessing the Tenable Security Center interface. Communicating with Tenable Security Center Director instances. Communicating with OT Security instances. Performing the initial key push for remote repository synchronization with another Tenable Security Center. Interacting with the API.
TCP 8837	Communicating with Sensor Proxy.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 22	Synchronizing repositories from other Tenable Security Center instances.
TCP 25	Sending SMTP email notifications.

Port	Traffic
TCP 389	Communicating with customer-managed LDAP servers.
TCP 443	Communicating with Tenable One for synchronization. Communicating with the `plugins.nessus.org` server for plugin updates.
TCP 465	Sending SMTP email notifications.
TCP 587	Sending SMTP email notifications.
TCP 636	Communicating with customer-managed LDAP servers.
TCP 8834	Communicating with Tenable Nessus.
TCP 8835	Communicating with Tenable Network Monitor.
UDP 53	Performing DNS resolution.

Note: If your Tenable Security Center instance is not configured as an offline instance, you must also allow outbound traffic to the Tenable websites listed in the Which Tenable sites should I allow? article in the Knowledge Base.

SSL inspection on traffic to and from the Tenable update sites is not supported. While access to the update sites can be established, it may not be able to complete updates due to SSL inspection of the traffic.

Tenable Security Center Services

The following are reserved ports for Tenable Security Center services.

Port	Traffic
TCP 8840	Tenable Security Center asset service.

Agent Content Distribution Network (CDN)

Dependent on rule logic in place, you may need to adjust your firewall or proxy rules in order to utilize the Agent Content Distribution Network (CDN).

FQDN Updates

The CDN leverages `sensor.cloud.tenable.com` for downloading plugins and binary updates, uploading scan results, and linking and communicating with Tenable Vulnerability Management. If you have a firewall or proxy rule configured for `sensor.cloud.tenable.com` then you should not encounter issues. However, if there are stricter rules in place then you need to update your rule set.

IP Allowlisting

The IP addresses associated with `sensor.cloud.tenable.com` are dynamic and dependent on the locale of the agent and its connectivity to the internet. If you currently have IP-based rules configured for proxies and firewalls you must update the rules based on IP ranges utilized by Amazon CloudFront. Amazon's documentation Locations and IP Address Ranges of CloudFront Edge Servers has a list of the IP ranges available for download.

> **Note:** If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.

Licensing Requirements

Tenable Agents are licensed through the product that manages them: Tenable Nessus Manager or Tenable Vulnerability Management.

Tenable Nessus Manager

Tenable Nessus is available to operate either as a subscription or managed by Tenable Security Center. Tenable Nessus requires a plugin feed activation code to operate in subscription mode. This code identifies which version of Tenable Nessus that Tenable licensed you to install and use, and if applicable, how many IP addresses you can scan, how many remote scanners you can link to Tenable Nessus, and how many Tenable Agents you can link to Tenable Nessus Manager. Tenable Nessus Manager licenses are specific to your deployment size, especially for large deployments or deployments with multiple Tenable Nessus Manager instances. Discuss your requirements with your Tenable Customer Success Manager.

You must obtain the activation code before starting the installation process and setting up Tenable Nessus.

Your activation code:

- is a **one-time** code, unless your license or subscription changes, at which point Tenable issues you a new activation code.
- must be used with the Tenable Nessus installation within 24 hours.
- cannot be shared between scanners.
- is not case-sensitive.
- is required to manage Tenable Nessus offline.

> **Note:** For more information about managing Tenable Nessus offline, refer to the *Tenable Nessus User Guide*.

> **Note:** See the Obtain an Activation Code page to obtain an activation code.

For managed Tenable Nessus scanners, the activation code and plugin updates are managed from Tenable Security Center. You must start Tenable Nessus before it communicates with Tenable Security Center, which it normally does not do without a valid activation code and plugins. To have Tenable Nessus ignore this requirement and start (so that it can get the information from Tenable Security Center), when you register your scanner, select **Managed by Security Center**.

Agent CPU Resource Control

You can control the priority of the Tenable Agent relative to the priority of other tasks running on the system by using the `process_priority` preference. Due to the relative nature of this preference, the amount of system resources consumed by the Tenable Agent depends not only on the value of the `process_priority` preference, but also on the overall load on the system. This may reflect on system monitors as if the agent is consuming resources over the higher priority processes. For resource control commands see Tenable Agent CLI Commands .

> **Note:** There may be a slight delay between setting a value for `process_priority` and seeing the change reflected in Linux nice values, macOS nice values, or Windows Priority Class.

To see the effect of the `process_priority` preference, see the following table.

Preference Value	Windows Priority Class	macOS Nice Value	Linux Nice Value

normal	normal	0	0
low	low	10	10
high	high	-10	-5

Note: Setting your `process_priority` preference value to low could cause longer running scans. You may need to increase your scan-window timeframe to account for this value.

Agent CPU Resource Control Advanced Settings

You can configure the following agent settings in the command line interface using the `nessuscli` utility.

Use the command `# nessuscli fix --set` *`setting=value`*. For more information, see [Tenable Agent CLI Commands]().

For more information, and a complete list of CLI-configurable settings, see [Advanced Settings]().

Tip: If you have many agents (10,000+), you may want to configure the `agent_merge_audit_trail`, `agent_merge_kb`, `agent_merge_journal_mode`, and `agent_merge_synchronous_setting` settings. Modifying these settings can dramatically lower the amount of time it takes to merge agent scan results. Review the descriptions in the following table for suggested configurations.

Name	Setting	Description	Default	Valid Values
Plugin Compilation Performance	plugin_load_ performance_ mode	Sets plugin compilation performance, which affects CPU usage. Low performance slows down plugin compilation, but reduces the agent's CPU consumption. Setting the performance to medium or high means	Tenable Agent 10.8.3 and later — `medium` Tenable Agent 10.8.2 and earlier — `high`	`low`, `medium`, or `high`

		that plugin compilation completes more quickly, but the agent consumes more CPU. Target ranges for each setting value are: • `low` — Uses exactly one thread. Deliberately consumes less time than available, approximating 50% usage of one core. • `medium` — Uses up to half as many threads as cores available, up to a maximum of four cores on a system with eight or more cores. Always uses at least one thread. • `high` — Uses as many threads as cores available, up to a maximum of eight threads. **Note:** Tenable		

		recommends setting Plugin Compilation Performance to `medium` or `low` for shared resource environments, such as VDI or ESXi.		
Scan Performance	scan_performance_mode	Sets scan performance, which affects CPU usage. Low performance slows down scans, but reduces the agent's CPU consumption. Setting the performance to medium or high means that scans complete more quickly, but the agent consumes more CPU. Target ranges for each setting value are: • `low` — Targets a usage of approximately half of one CPU core during scanning. • `medium` — Uses up to half of each available core, up to eight cores, during scanning.	`high`	`low`, `medium`, or `high`

		- `high` — Uses up to eight total cores during scanning.		

Tenable Agent Performance

Tenable transparently provides performance metrics based on internal performance testing. Performance varies by environment and you may or may not see similar results.

The following sections describe various performance metrics for Tenable Agents:

Lifecycle and Bandwidth

> **Note:** Performance varies by environment and you may or may not see similar results.

Process or File	Windows	macOS	Linux
Agent Core Software Initial Install	~70 MB	~38 MB	~15-25 MB
Agent Core Software Updates	~32 MB	~38 MB	~20-30 MB
Initial Plugin Download	301 MB	220 MB	242 MB
Differential Plugin Updates **Note:** Plugin update sizes vary depending on the difference between the new plugins available and the last date the agent updated its plugins.	0.1-301 MB	0.1-220 MB	0.1-242 MB
Report Size **Note:** Report size can vary greatly depending on the scan. Compliance audit scans can be especially large.	1-100+ MB	1-100+ MB	1-100+ MB

Software Footprint

> **Note:** Performance varies by environment and you may or may not see similar results.

Agents Running Standard Agent Scans

Agent Footprint on Disk	Total Agent Software Footprint on Disk	Average RAM Usage While Not Scanning	Average RAM Usage While Scanning	Average RAM Usage During Plugin Compilation	Average Network Bandwidth Usage
~85 MB	~875 MB including plugin updates **Note:** Under certain conditions, disk usage can spike up to 3 GB or more.	~50 MB RAM **Note:** In Linux environments, the `Hugepagesize` value plays a significant role in the usage shown by the `systemctl status nessusagent` command. The shown usage not only includes the agent processes' RAM consumption but also any cached data that would be stored on disk if the system experiences memory	~85 MB RAM	~150 MB RAM	~8 MB/day

Agent Footprint on Disk	Total Agent Software Footprint on Disk	Average RAM Usage While Not Scanning	Average RAM Usage While Scanning	Average RAM Usage During Plugin Compilation	Average Network Bandwidth Usage
		pressure. For example, x86-64-based Linux systems typically exhibit a total usage ranging from 200 MB to 600 MB with the default `Hugepagesize` value of 2048 kB. ARM64-based Linux systems with a larger `Hugepagesize` value show correspondingly high memory usage (for example, the usage shows as multiple gigabytes with a default `Hugepagesize` of 512 M).			

Agents Running Inventory Scans

Agent Footprint on Disk	Total Agent Software Footprint on Disk	Average RAM Usage While Not Scanning	Average RAM Usage While Scanning	Average RAM Usage During Plugin Compilation	Average Network Bandwidth Usage
~85 MB	~150 MB including plugin updates **Note:** Under certain conditions, disk usage can spike up to 200 MB.	~50 MB RAM **Note:** In Linux environments, the `Hugepagesize` value plays a significant role in the usage shown by the `systemctl status nessusagent` command. The shown usage not only includes the agent processes' RAM consumption but also any cached data that would be stored on disk if the system experiences memory pressure. For example, x86-64-based	~80 MB RAM	~105 MB RAM	~8 MB/day

Agent Footprint on Disk	Total Agent Software Footprint on Disk	Average RAM Usage While Not Scanning	Average RAM Usage While Scanning	Average RAM Usage During Plugin Compilation	Average Network Bandwidth Usage
		Linux systems typically exhibit a total usage ranging from 200 MB to 600 MB with the default `Hugepagesize` value of 2048 kB. ARM64-based Linux systems with a larger `Hugepagesize` value show correspondingly high memory usage (for example, the usage shows as multiple gigabytes with a default `Hugepagesize` of 512 M).			

For more information about inventory scanning, see Tenable-Provided Agent Templates in the *Tenable Vulnerability Management User Guide*.

Host System Utilization

> **Note:** Performance varies by environment and you may or may not see similar results.

Generally, a Tenable Agent uses 50 MB to 60 MB of RAM (all pageable). A Tenable Agent uses almost no CPU while idle, but is designed to use up to 100% of the CPU when available during jobs.

To measure network utilization when uploading results, Tenable monitored agent uploads intoTenable Vulnerability Management over a seven-day period. Of over 36,000 uploads observed:

- The average size was 1.6 MB.
- The largest size was 37 MB.
- 90% of uploads were 2.2 MB or less.
- 99% of uploads were 5 MB or less.
- Tenable Agent processes consume between 45 MB and 60 MB of RAM when dormant, depending on the operating system.

  > **Note:** In Linux environments, the `Hugepagesize` value plays a significant role in the usage shown by the `systemctl status nessusagent` command. The shown usage not only includes the agent processes' RAM consumption but also any cached data that would be stored on disk if the system experiences memory pressure.
  >
  > For example, x86-64-based Linux systems typically exhibit a total usage ranging from 200 MB to 600 MB with the default `Hugepagesize` value of 2048 kB. ARM64-based Linux systems with a larger `Hugepagesize` value show correspondingly high memory usage (for example, the usage shows as multiple gigabytes with a default `Hugepagesize` of 512 M).

- The Watchdog service consumes 3 MB.
- Plugins consume approximately 300 MB of disk space (varies based on operating system). However, under certain conditions, disk or memory usage can spike up to 1 GB or more.
- Scan results from Tenable Agents to Tenable Nessus Manager and Tenable Vulnerability Management range between 2-3 MB.
- Check-in frequency starts at 30 seconds and is adjusted by Tenable Nessus Manager orTenable Vulnerability Management based on the management system load (number of agents).

Tenable Nessus Manager Performance

Tenable tested Tenable Nessus Manager performance in two scenarios. **Scenario 1** is when Tenable Agents are connected to Tenable Nessus Manager and polling for jobs. **Scenario 2** is when Tenable Agents are actively scanning and uploading scan results.

Testing Environments

Tenable used the following testing environments for the two scenarios.

Scenario 1

- OS: Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-75-generic x86_64)
- RAM: 16 GB
- CPU: Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz
- Cores: 2

Scenario 2

- OS: Windows 10 v. 1703 (OS Build: 15063.447)
- RAM: 16 GB
- CPU: Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.59GHz
- Cores: 2

Scenario 1: When Tenable Agents are Connected to Tenable Nessus Manager and Polling for Jobs

Number of Agents	Number of Agents Sending Job Requests at a Time (2%)	MAX CPU Usage	Average CPU Usage	Average Agents Page Load Time
1,000	20	33%	5%	0.60 seconds
2,000	40	34%	5%	1.05 seconds
5,000	100	43%	6%	1.7 seconds
7,500	150	92%	7%	3.22 seconds
10,000	200	100%	7%	3.26 seconds

Number of Agents	Number of Agents Sending Job Requests at a Time (5%)	MAX CPU Usage	Average CPU Usage	Average Agents Page Load Time
1,000	50	38%	7%	0.88 seconds
2,000	100	39%	7%	1.14 seconds
5,000	250	54%	6%	1.73 seconds

Scenario 2: When Tenable Agents are Actively Scanning and Uploading Scan Results

Number of Agents	MAX CPU Usage	Average CPU Usage	Average Agents Page Load Time	Scan Report Size
1,000	65%	52%	1.16 seconds	363 MB
2,000	82%	53%	1.45 seconds	726 MB
3,000	82%	46%	1.67 seconds	1079 MB
4,000	86%	40%	1.70 seconds	1452 MB
5,000	99%	47%	1.73 seconds	1780 MB

Manage Agents

Install Tenable Agent

This section describes how to install a Tenable Agent on the following operating systems:

- Windows
- macOS
- Linux

Once installed, an agent links to Tenable Nessus Manager or Tenable Vulnerability Management after a random delay ranging from zero to five minutes. Enforcing a delay reduces network traffic when deploying or restarting large amounts of agents, and reduces the load on Tenable Nessus Manager or Tenable Vulnerability Management. Agents download plugins from the manager upon the first scan starting; this process can take several minutes and must take place before an agent can return scan results.

Install a Tenable Agent on Linux

Use the following procedure to install Tenable Agent on a Linux system. After the installation, you link the agent to its manager Tenable Vulnerability Management or Tenable Nessus Manager) so that it can begin sending scan data once the installation is complete.

Before you begin:

- Retrieve the Tenable Agent linking key. For more information, see the *Tenable Nessus User Guide* or the *Tenable Vulnerability Management User Guide*, depending on what manager you use.
- If you previously had the Tenable Agent installed on your system, see the knowledge base article on how to avoid linking errors.

> **Caution:** If you install a Tenable Agent on a system where an existing Tenable Agent, Tenable Nessus Manager, or Tenable Nessus scanner is running `nessusd`, the installation process kills all other `nessusd` processes. You may lose scan data as a result.

Download the Tenable Agent

On the Tenable Agent Download Page, download the package specific to your operating system.

Once you download the agent package, install the agent.

Install the Agent

> **Note:** The following procedure requires root privileges.

Using the command line interface, install the Tenable Agent.

Example Linux Install Commands

Debian / Ubuntu

```
# dpkg -i NessusAgent-<OS and version number>.deb
```

Red Hat 8 and later, Oracle Linux 8 and later, and Fedora 34 and later

```
# dnf install NessusAgent-<OS and version number>.rpm
```

Red Hat 7 and earlier / Oracle Linux 7 and earlier

```
# rpm -ivh NessusAgent-<OS and version number>.rpm
```

SUSE

```
# sudo zypper install NessusAgent-<OS and version number>.rpm
```

> **Tip:** You can install a full plugins set before linking to reduce the bandwidth impact during a mass installation. You can accomplish this by using the `nessuscli agent update` command with the `--file` parameter, which specifies the location the plugins set. You must do this before starting the Tenable Agent. For example:
>
> ```
> /opt/nessus_agent/sbin/nessuscli agent update --file=./plugins_set.tgz
> ```
>
> The plugins set must be less than five days old. A stale plugin set older than five days forces a full plugin download to occur. You can download a recent plugins set from the Tenable Agent download page.

> **Note:** After installing a Tenable Agent, you must manually start the service using the **`/sbin/service nessusagent start`** command. Tenable also recommends running **`systemctl enable nessusagent`** to ensure that the Tenable Agent service starts anytime the host is rebooted.

Link the Agent Using the Command Line

At the command prompt, use the `nessuscli agent link` command. For example:

```
/opt/nessus_agent/sbin/nessuscli agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=MyOSXAgent --groups="All" --host=yourcompany.com --port=8834
```

> **Note:** You must copy and paste the entire link command on the same line. Otherwise, you receive an error.

The supported arguments for this command are:

Argument	Required?	Value
--key	yes	(Required) Use the values obtained from the manager. To retrieve the linking key from the manager, see the *Tenable Nessus User Guide* or the *Tenable Vulnerability Management User Guide*, depending on which manager you use.
--host	yes	
--port	yes	
--name	no	Specify a name for your agent. If you do not specify a name for your agent, the name defaults to the name of the computer where you are installing the agent.
--groups	no	Specify existing agent group or groups where you want to add the agent. If you do not specify an agent group during the install process, you can add your linked agent to an agent group later in Tenable Nessus Manager or Tenable Vulnerability Management. **Note:** The agent group name is case-sensitive and must match exactly. You must encase the agent group name in quotation marks (for example, `--groups="My Group"`).

Argument	Required?	Value
--offline-install	no	You can install the Tenable Agent on a system even if it is offline. Add the command line option `offline-install="yes"` to the command line input. The Tenable Agent periodically attempts to link itself to either Tenable Vulnerability Management or Tenable Nessus Manager. If the agent cannot connect to the controller then it retries every hour, and if the agent can connect to the controller but the link fails then it retries every 24 hours.
--cloud	no	Specify the `--cloud` argument to link to Tenable Vulnerability Management. The `--cloud` argument is a shortcut to specifying `--host=sensor.cloud.tenable.com --port=443`. **Caution:** The `--cloud` argument is not supported in FedRAMP environments. You must specify `--host=fedcloud.tenable.com --port=443`. **Note:** If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com. **Note:** For more information about linking agents to Tenable Vulnerability Management, see Link a Sensor in the *Tenable Vulnerability Management User Guide*.
--network	no	For Tenable Vulnerability Management-linked agents, add the agent to a custom network. If you do not specify a network, the agent belongs to the default network. **Note:** You must encase the network name in quotation marks (for example, `--network="My Network"`).

Argument	Required?	Value
--profile-uuid	no	The UUID of the agent profile that you want to assign the agent to (for example, `12345678-9abc-4ef0-9234-56789abcdef0`). For more information, see Agent Profiles in the *Tenable Vulnerability Management User Guide*.

Once you install and link the agent, Tenable recommends that you verify that the agent is successfully linked to the manager by viewing the agent in the manager user interface.

> **Tip:** If you attempt to clone an agent and link it to Tenable Nessus Manager or Tenable Vulnerability Management, a 409 error may appear. This error appears because another machine was linked with the same UUID value in the **`/etc/machine_id`** or **`/etc/tenable_tag`** file. To resolve this issue, replace the value in the **`/etc/tenable_tag`** file with a valid UUIDv4 value. If the **`/etc/machine_id`** file does not exist, you can delete **`/etc/tenable_tag`** to generate a new value.

Verify the Linked Agent

Once you install and link the agent, use the following steps to view the new agent in the manager user interface:

- To verify a linked agent 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 **Settings**.

     The **Settings** page appears.

  3. Click the **Sensors** tile.

     The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

  4. In the left navigation menu, click **Nessus Agents**.

     The **Nessus Agents** page appears and the **Linked Agents** tab is active.

  5. Locate the new agent in the linked agents table.

- To verify a linked agent in Tenable Nessus Manager:

1. In the top navigation bar, click **Sensors**.

   The **Linked Agents** page appears.

2. Locate the new agent in the linked agents table.

Install a Tenable Agent on Windows

Use the following procedure to install Tenable Agent on a Windows system. During the installation process, you link the agent to its manager Tenable Vulnerability Management or Tenable Nessus Manager) so that it can begin sending scan data once the installation is complete.

Before you begin:

- Retrieve the Tenable Agent linking key. For more information, see the *Tenable Nessus User Guide* or the *Tenable Vulnerability Management User Guide*, depending on what manager you use.
- If you previously had the Tenable Agent installed on your system, see the knowledge base article on how to avoid linking errors.

> **Note:** You may be required to restart your computer to complete installation.

> **Caution:** If you install a Tenable Agent on a system where an existing Tenable Agent, Tenable Nessus Manager, or Tenable Nessus scanner is running `nessusd`, the installation process kills all other `nessusd` processes. You may lose scan data as a result.

Download Tenable Agent

On the Tenable Agent Download Page, download the package specific to your operating system.

Once you download the agent package, you can install and link the agent using the command line, or you can install and link the agent with the GUI installation wizard.

Install and Link via the Command Line

> **Note:** You must have administrator-level privileges to deploy and link via the command line.

> **Note:** This procedure describes deploying Tenable Agents via the command line. You can also deploy Tenable Agents with a standard Windows service such as Active Directory (AD), Systems Management

Server (SMS), or other software delivery system for MSI packages. For more information on deploying via these methods, see the appropriate vendor's documentation.

You can install and link Tenable Agents via the command line with a number of linking parameters. For example:

```
msiexec /i NessusAgent-<version number>-x64.msi NESSUS_GROUPS="Agent Group Name"
NESSUS_SERVER="192.168.0.1:8834" NESSUS_
KEY=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00 /qn
```

The following are available linking parameters:

Parameter	Description
`ADDLOCAL=ALL`	Install the Tenable Agent system tray application, as described in step 8 of Install a Tenable Agent on Windows in the *Tenable Agent User Guide*.
`NESSUS_CA_PATH`	Specify a custom CA certificate to use to validate the manager's server certificate.
`NESSUS_GROUPS`	Specify existing agent group or groups where you want to add the agent. If you do not specify an agent group during the install process, you can add your linked agent to an agent group later in Tenable Nessus Manager or Tenable Vulnerability Management. **Note:** The agent group name is case-sensitive and must match exactly. You must encase the agent group name in quotation marks (for example, `--groups="My Group"`). **Note:** Quotation marks (") are necessary when listing multiple groups, or one group with spaces in its name. For example: • GroupName

	• "Group Name" • "Group, Another Group"
NESSUS_NAME	Specify the name for your agent. If you do not specify a name for your agent, the name defaults to the name of the computer where you are installing the agent.
NESSUS_OFFLINE_INSTALL	You can install the Tenable Agent on a system even if it is offline. Add the command line option `NESSUS_OFFLINE_INSTALL="yes"` to the command line input. The Tenable Agent will periodically attempt to link itself to either Tenable Vulnerability Management or Tenable Nessus Manager. If the agent cannot connect to the controller then it retries every hour, and if the agent can connect to the controller but the link fails then it retries every 24 hours.
NESSUS_PLUGINS_ FILEPATH="C:\path\to\plugins_ set.tgz"	Install a full plugins set before linking to reduce the bandwidth impact during a mass installation. Add the command line option `NESSUS_PLUGINS_ FILEPATH="C:\path\to\plugins_set.tgz"` where *plugins_set.tgz* is a recent plugins set tarball less than five days old. A stale plugins set older than five days will force a full plugins download to occur. You can download a recent plugins set from the Tenable downloads page.
NESSUS_PROCESS_PRIORITY	Determine the priority of the agent relative to the priority of other tasks running on the system. For valid values and more information on how the setting works, see Agent CPU Resource Control in the *Tenable Agent Deployment and User Guide*.
NESSUS_PROXY_AGENT	Specify the user agent name, if your proxy requires

	a preset user agent.
`NESSUS_PROXY_PASSWORD`	Specify the password of the user account that you specified as the username.
`NESSUS_PROXY_SERVER`	Specify the hostname or IP address of your proxy server.
`NESSUS_PROXY_USERNAME`	Specify the name of a user account that has permissions to access and use the proxy server.
`NESSUS_SERVER`	Specify the hostname or IP address of your server. • To link to Tenable Vulnerability Management, enter **sensor.cloud.tenable.com:443**. • To link to Tenable Nessus Manager, enter the IP/hostname of the manager with the appended port **8834**; for example, **192.168.2.1:8834**.
`NESSUS_SERVICE_AUTOSTART=false`	Prevents the Tenable Agent from starting up after installation. This parameter can be useful for streamlined deployment options (for example, deploying using a JSON file). **Note:** On Windows, the agent service `StartType` is set to **Automatic**. Therefore, when you reboot a Windows system, the agent service always starts.

Once you install and link the agent, Tenable recommends that you verify that the agent is successfully linked to the manager by viewing the agent in the manager user interface.

Install and Link with the Installation Wizard

> **Note:** You may have to restart your computer to complete installation on Windows.

1. Navigate to the folder where you downloaded the Tenable Agent installer.
2. Next, double-click the file name to start the installation process. The **Welcome to the InstallShield Wizard for Nessus Agent** window appears.
3. In the **Welcome to the InstallShield Wizard for Nessus Agent** window, click **Next** to continue.
4. In the **License Agreement** window, read the terms of the Tenable, Inc. Nessus software license and subscription agreement.
5. Click **I accept the terms of the license agreement**.
6. Click **Next**.
7. In the **Destination Folder** window, click **Next** to accept the default installation folder.

   -or-

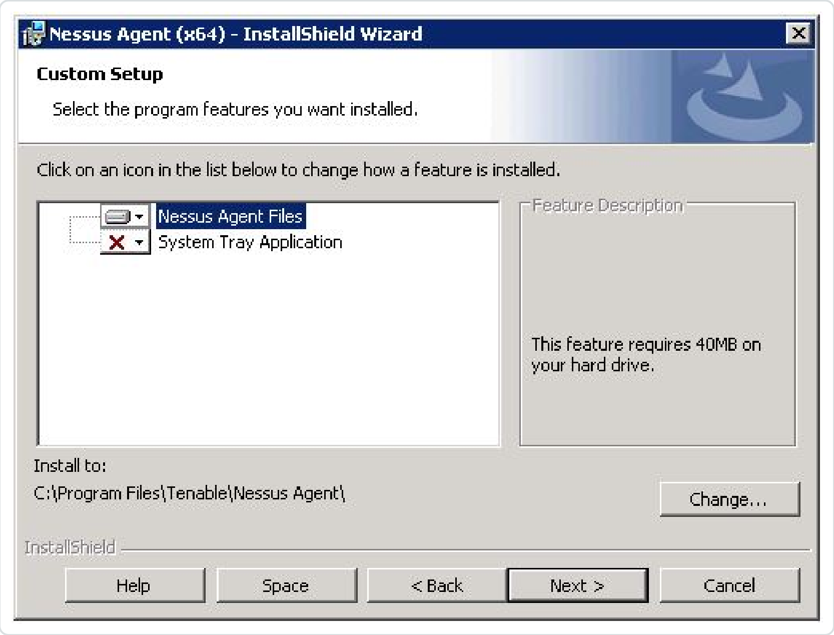
   Click **Change** to browse and select a different folder where you want to install Tenable Agents, then click **Next**.
8. In the **Setup Type** window, do one of the following:
   - To install the agent with the System Tray Application, which allows you to view the agent status on your machine, select **Custom**, click **Next**, and complete the steps in the following drop-down menu:

     System Tray Application configuration

Field	Value
Key	(Required) Use the linking key you obtained from the manager. To retrieve the linking key from the manager, see the *Tenable Nessus User Guide* or the *Tenable Vulnerability Management User Guide*, depending on which manager you use.
Server	(Required) Enter the manager's host server: • To link to Tenable Vulnerability Management, enter **sensor.cloud.tenable.com:443**.

	Note: If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com. **Note:** For more information about linking agents to Tenable Vulnerability Management, see Link a Sensor in the *Tenable Vulnerability Management User Guide*. • To link to Tenable Nessus Manager, enter the IP/hostname of the manager with the appended port **8834**; for example, **192.168.2.1:8834**.
Groups	Specify the existing agent group or groups where you want to add the agent. If you do not specify an agent group during the installation process, you can later add your linked agent to an agent group.

a. The **Custom Setup** page appears. By default, the system tray application is excluded from the installation package.



Nessus Agent (x64) - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

Nessus Agent Files

System Tray Application

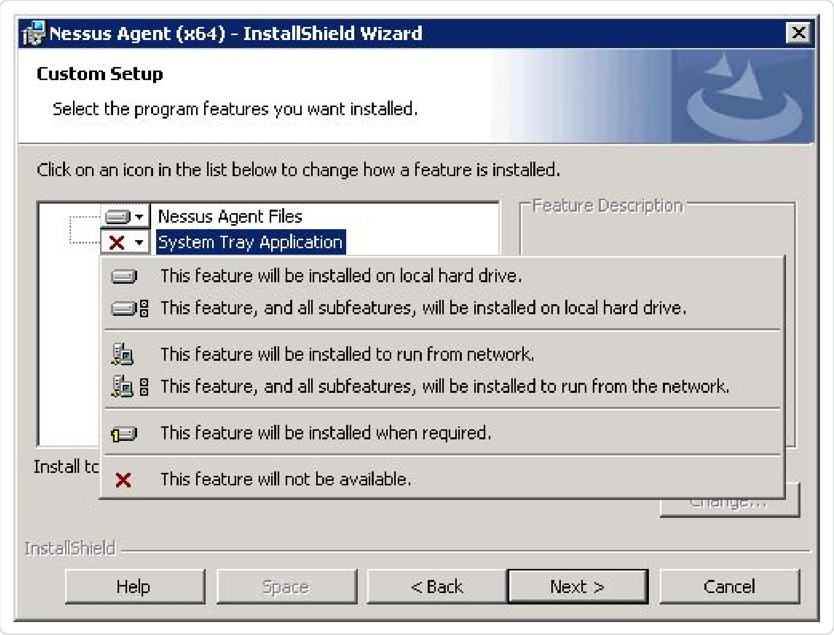
Feature Description

This feature requires 40MB on your hard drive.

Install to:

C:\Program Files\Tenable\Nessus Agent\

b. Click the **System Tray Application** drop-down box.



Nessus Agent (x64) - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

Nessus Agent Files

System Tray Application

Feature Description

This feature will be installed on local hard drive.

This feature, and all subfeatures, will be installed on local hard drive.

This feature will be installed to run from network.

This feature, and all subfeatures, will be installed to run from the network.

This feature will be installed when required.

This feature will not be available.

c. Click **This feature will be installed on local hard drive.**

d. Click **Next**.

- To install the agent without the System Tray Application, select **Typical** and click **Next**.

9. In the **Configuration Options** window, type the **Agent Key** values:

Field	Value
Key	(Required) Use the linking key you obtained from the manager. To retrieve the linking key from the manager, see the *Tenable Nessus User Guide* or the *Tenable Vulnerability Management User Guide*, depending on which manager you use.
Server	(Required) Enter the manager's host server: • To link to Tenable Vulnerability Management, enter **sensor.cloud.tenable.com:443**. **Note:** If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com. **Note:** For more information about linking agents to Tenable Vulnerability Management, see Link a Sensor in the *Tenable Vulnerability Management User Guide*. • To link to Tenable Nessus Manager, enter the IP/hostname of the manager with the appended port **8834**; for example, **192.168.2.1:8834**.
Groups	Specify the existing agent group or groups where you want to add the agent. If you do not specify an agent group during the installation process, you can later add your linked agent to an agent group.

10. Click **Next**.

11. In the **Ready to Install the Program** window, click **Install**.

12. If presented with a **User Account Control** message, click **Yes** to allow the Tenable Agent to install.

13. In the **InstallShield Wizard Complete** window, click **Finish**.

Once you install and link the agent, Tenable recommends that you verify that the agent is successfully linked to the manager by viewing the agent in the manager user interface.

Note: The agent name defaults to the name of the computer where you are installing the agent.

Tip: If you attempt to clone an agent and link it to Tenable Nessus Manager or Tenable Vulnerability Management, a 409 error may appear. This error appears because another machine was linked with the same UUID value in the **`HKLM/Software/Tenable/TAG`** file. To resolve this issue, replace the value in the **`HKLM/Software/Tenable/TAG`** file with a valid UUIDv4 value.

Verify the Linked Agent

Once you install and link the agent, use the following steps to view the new agent in the manager user interface:

- To verify a linked agent 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 **Settings**.

     The **Settings** page appears.

  3. Click the **Sensors** tile.

     The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

  4. In the left navigation menu, click **Nessus Agents**.

     The **Nessus Agents** page appears and the **Linked Agents** tab is active.

  5. Locate the new agent in the linked agents table.

- To verify a linked agent in Tenable Nessus Manager:

  1. In the top navigation bar, click **Sensors**.

     The **Linked Agents** page appears.

  2. Locate the new agent in the linked agents table.

Install a Tenable Agent on macOS

Use the following procedure to install Tenable Agent on a macOS system. After the installation, you link the agent to its manager Tenable Vulnerability Management or Tenable Nessus Manager) so that it can begin sending scan data once the installation is complete.

Before you begin:

- Retrieve the Tenable Agent linking key. For more information, see the *Tenable Nessus User Guide* or the *Tenable Vulnerability Management User Guide*, depending on what manager you use.
- If you previously had the Tenable Agent installed on your system, see the knowledge base article on how to avoid linking errors.

> **Note:** Agents may need Full Disk Access when using some audits for full directory access. Therefore, Tenable recommends granting Full Disk Access to agents installed on macOS.

> **Caution:** If you install a Tenable Agent on a system where an existing Tenable Agent, Tenable Nessus Manager, or Tenable Nessus scanner is running `nessusd`, the installation process kills all other `nessusd` processes. You may lose scan data as a result.

Download Tenable Agent

On the Tenable Agent Download Page, download the package specific to your operating system.

Once you download the agent package, install the agent.

Install the Agent

> **Note:** You need root privileges to perform the following steps.

To install the Tenable Agent, you can use either the GUI installation wizard or the command line.

GUI Installation:

1. Double-click the Tenable Agent `.dmg` (macOS disk image) file.
2. Double-click `Install Nessus Agent.pkg`.
3. Complete the **Nessus Agent Install Wizard**.

Command line Installation:

1. Extract `Install Nessus Agent.pkg` and `.NessusAgent.pkg` from `NessusAgent-<version number>.dmg`.

   > **Note:** The `.NessusAgent.pkg` file is normally invisible in the macOS Finder.

2. Open Terminal.

3. From the command line, enter the following command:

   ```
   # sudo installer -pkg /<path-to>/Install Nessus Agent.pkg -target /
   ```

Once the agent installation completes, link the agent to the manager.

> **Tip:** You can install a full plugin set before linking to reduce the bandwidth impact during a mass installation. You can accomplish this by using the `nessuscli agent update` command with the `--file` parameter, which specifies the location the plugins set. You must do this before starting the Tenable Agent. For example:
>
> ```
> /opt/nessus_agent/sbin/nessuscli agent update --file=./plugins_set.tgz
> ```
>
> The plugins set must be less than five days old. A stale plugin set older than five days forces a full plugins download to occur. You can download a recent plugin set from the Tenable Agent download page.

Link Agent Using the Command Line

To link an agent on macOS:

1. Open Terminal.

2. From the command line, use the `nessuscli agent link` command.

   For example:

   ```
   # sudo /Library/NessusAgent/run/sbin/nessuscli agent link
   --key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
   --name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
   ```

> **Note:** You must copy and paste the entire link command on the same line. Otherwise, you receive an error.

The supported arguments for this command are:

Argument	Required?	Value
--key	yes	(Required) Use the values obtained from the manager. To retrieve the linking key from the manager, see the *Tenable Nessus User Guide* or the *Tenable Vulnerability Management User Guide*, depending on which manager you use.
--host	yes	
--port	yes	
--name	no	Specify a name for your agent. If you do not specify a name for your agent, the name defaults to the name of the computer where you are installing the agent.
--groups	no	Specify an existing agent group or groups where you want to add the agent. If you do not specify an agent group during the installation process, you can add your linked agent to an agent group later in Tenable Nessus Manager or Tenable Vulnerability Management. **Note:** The agent group name is case-sensitive and must match exactly. You must encase the agent group name in quotation marks (for example, `--groups="My Group"`).
--offline-install	no	You can install the Tenable Agent on a system even if it is offline. Add the command line option `NESSUS_OFFLINE_INSTALL="yes"` to the command line input. The Tenable Agent periodically attempts to link itself to either Tenable Vulnerability Management or Tenable Nessus Manager. If the agent cannot connect to the controller then it

		retries every hour, and if the agent can connect to the controller but the link fails then it retries every 24 hours.
--cloud	no	Specify the `--cloud` argument to link to Tenable Vulnerability Management. The `--cloud` argument is a shortcut to specifying `--host=cloud.tenable.com --port=443`. **Caution:** The `--cloud` argument is not supported in FedRAMP environments. You must specify `--host=fedcloud.tenable.com --port=443`. **Note:** If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com. **Note:** For more information about linking agents to Tenable Vulnerability Management, see Link a Sensor in the *Tenable Vulnerability Management User Guide*.
--network	no	For Tenable Vulnerability Management-linked agents, add the agent to a custom network. If you do not specify a network, the agent belongs to the default network.
--profile-uuid	no	The UUID of the agent profile that you want to assign the agent to (for example, `12345678-9abc-4ef0-9234-56789abcdef0`). For more information, see Agent Profiles in the *Tenable Vulnerability Management User Guide*.

Once you install and link the agent, Tenable recommends that you verify that the agent is successfully linked to the manager by viewing the agent in the manager user interface.

Tip: If you attempt to clone an agent and link it to Tenable Nessus Manager or Tenable Vulnerability Management, a 409 error may appear. This error appears because another machine was linked with the same UUID value in the `/private/etc/tenable_tag` file. To resolve this issue, replace the value in the `/private/etc/tenable_tag` file with a valid UUIDv4 value.

Verify the Linked Agent

Once you install and link the agent, use the following steps to view the new agent in the manager user interface:

- To verify a linked agent 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 **Settings**.

     The **Settings** page appears.
  3. Click the **Sensors** tile.

     The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.
  4. In the left navigation menu, click **Nessus Agents**.

     The **Nessus Agents** page appears and the **Linked Agents** tab is active.
  5. Locate the new agent in the linked agents table.
- To verify a linked agent in Tenable Nessus Manager:
  1. In the top navigation bar, click **Sensors**.

     The **Linked Agents** page appears.
  2. Locate the new agent in the linked agents table.

Start or Stop a Tenable Agent

You can temporarily stop an agent from gathering data and restart the agent to resume gathering data. Stopping and starting an agent can be helpful for troubleshooting. Tenable also recommends stopping the agent whenever you perform a manual update.

The following sections describe best practices for starting and stopping a Tenable Agent on a host.

Windows

1. Navigate to **Services**.
2. In the **Name** column, click **Tenable Nessus Agent**.
3. Do one of the following:
   - To stop the agent service, right-click **Tenable Nessus Agent**, and then click **Stop**.
   - To restart the agent service, right-click **Tenable Nessus Agent**, and then click **Start**.

Alternatively, you can start or stop an agent from the command line using the following commands:

Start or Stop	Windows Command Line Operation
Start	`C:\Windows\system32>net start "Tenable Nessus Agent"`
Stop	`C:\Windows\system32>net stop "Tenable Nessus Agent"`

Linux

Use the following commands to start or stop an agent on a Linux system:

Start or Stop	Linux Command Line Operation
Start	`# systemctl start nessusagent`
Stop	`# systemctl stop nessusagent`

macOS

1. Navigate to **System Settings**.
2. Click the ◎ button.
3. Click the 🔒 button.

4. Type your username and password.

5. Do one of the following:

   - To stop the agent service, click the **Stop Nessus Agent** button.
   - To start the agent service, click the **Start Nessus Agent** button.

Alternatively, you can start or stop an agent from the command line using the following commands:

Start or Stop	macOS Command Line Operation
Start	`# sudo launchctl start com.tenablesecurity.nessusagent`
Stop	`# sudo launchctl stop com.tenablesecurity.nessusagent`

Update a Tenable Agent

After you install an agent, it automatically retrieves updates from its manager (either Tenable Vulnerability Management or Tenable Nessus Manager).

In either manager's user interface, you can set an agent update plan to determine the version that the agents automatically update to. For more information, following the procedures described in the Tenable Vulnerability Management and Tenable Nessus Manager user guides.

Manual Updates

In certain cases, such as air-gapped or internet-restricted networks, you may want to download agent updates manually. You can install updates directly to individual agents, or you can install a bulk `tar.gz` update file in the Tenable Nessus Manager directory. In the latter case, Tenable Nessus Manager uses the `tar.gz` update file to distribute updates to each linked agent.

> **Note:** By default, Tenable Vulnerability Management-linked agents update to the generally available (GA) version one week after the version is GA. Therefore, if you manually update a Tenable Vulnerability Management-linked agents to the latest version prior to that date, you should either disable automatic updates or set your update plan to opt in to Early Access releases. This ensures that the agent does not automatically downgrade to the previous version (GA).

To install updates to Tenable Agent manually:

> **Note:** If you need to perform the following steps on an offline machine, complete steps 1-3 on a machine with internet access. Then, copy the downloaded file to the offline machine after step 3 and perform step 4 on the offline machine.

1. Navigate to the Tenable Agent Downloads page.

2. Click the agent update file that you want to download, depending on your operating system.

   The **License Agreement** window appears.

3. Click **I Agree**.

   The update file downloads to your machine.

4. Do one of the following, depending on your operating system:

   > **Note:** You need administrator-level privileges to complete the following steps.

   - **Windows**

     Do one of the following:

     - Double-click the `.msi` file you downloaded and follow the on-screen instructions.

     - In the command line interface, enter the following command, using the location and file name of the package you downloaded:

       ```
       > msiexec /i  <path-to>\NessusAgent-<version>.msi /qn
       ```

   - **Linux**

     In the command line interface, use the install or upgrade command specific to your Linux environment to install the downloaded file.

   - **macOS**

     a. Mount the `.dmg` file you downloaded:

     ```
     # sudo hdiutil attach <path-to>/NessusAgent-<version>.dmg
     ```

     b. Install the package:

```
# sudo installer -package /Volumes/Nessus\ Install/Install\ <path-to>/NessusAgent-<version>.dmg -target /
```

Your operating system installs the Tenable Agent updates.

In some instances, instead of installing updates to agents directly, you may want to install agent updates to your Tenable Nessus Manager, which then distributes the updates to any linked agents.

As new versions of Tenable Agent are released, Tenable Nessus Manager becomes aware of them through feed updates, and then passes those updates to the linked agents. A Tenable Nessus Manager registered in offline or air-gapped mode does not become aware of the new agent versions automatically; you need to install the latest Tenable Agent updates file manually to update the agent versions using the following steps:

To install agent updates to Tenable Nessus Manager manually:

> **Note:** If you need to perform the following steps on an offline machine, complete steps one and two on a machine with internet access. Then, copy the downloaded file to the offline machine during step three.

1. Navigate to the Tenable Agent Downloads page.
2. Download the `nessus-agent-updates-<version>.tar.gz` file. This file contains the update files for all operating systems and platforms that you can install Tenable Agent on.

   Since the package will be transferred from one system to another, always pull the MD5 checksum to verify file integrity after transit.
3. Copy the `tar.gz` file to your Tenable Nessus Manager directory. You can paste the file into any accessible child folder within the Tenable Nessus Manager directory.
4. Depending on your operating system, run one of the following commands to prepare the update files for the agents:

   > **Note:** You need administrator-level privileges to run the following commands:

- **Windows**

  ```
  > C:\Program Files\Tenable\Nessus\nessuscli.exe update <\path\to\nessus-agents-update-<version>.tar.gz>
  ```

- **Linux**

  ```
  # /opt/nessus/sbin/nessuscli update </path/to/nessus-agent-updates-<version>.tar.gz>
  ```

- **macOS**

  ```
  # /Library/Nessus/run/sbin/nessuscli update </path/to/nessus-agent-updates-<version>.tar.gz>
  ```

The update packages are pushed into the `/remote` directory, which acts as the local agent store.

5. Verify that Tenable Nessus Manager is set to update linked agents automatically by clicking **Sensors** > **Agent Updates** in the Tenable Nessus Manager user interface. Clear the **Enable Agent Updates** option if it is enabled.

   As the linked agents routinely check in with Tenable Nessus Manager, the new versions applicable to their operating system is provided to them automatically the next time they check in with the manager.

In-place Operating System Updates

Tenable Agent does not support upgrading the operating system on the host where Tenable Agent is installed. To prevent data loss, reinstall and relink the agent to the upgraded operating system.

Downgrade Tenable Agent

Tenable Agents support the ability to downgrade Tenable Nessus to a previous version of Tenable Nessus.

The following examples describe two scenarios: one scenario where you manually downgrade the agent software, and one scenario where the agent automatically downgrades because of your agent update plan setting.

Example 1: Manually Downgrade Agent

Scenario:

You are currently running an Early Access release, 10.0.0, and now want to downgrade to the previous version, 8.3.0.

Solution:

1. Turn off automatic software updates by doing any of the following:
    - On Tenable Nessus Manager, disable the advanced setting **Automatically Download Agent Updates**, or `agent_updates_from_feed`.
    - On Tenable Vulnerability Management, enable the agent setting **Exclude all agents from software updates**.
    - On the agent, enable the advanced setting `disable_core_updates`.
2. Uninstall the agent.
3. Manually download and install the package of the previous version; in this example, Tenable Agent 8.3.0.

Example 2: Agent Automatically Downgrades to Align with your Update Plan

Scenario:

Your agent update plan determines what version Tenable Agent updates to, if you have automatic updates enabled. In this scenario, your update plan is set to `ga`, meaning the agent automatically updates to the latest generally available (GA) release. You are currently on a GA version of Tenable Agent; for example, 10.0.0.

However, you change your update plan setting to `stable`, meaning the agent delays updates and stays on an older release.

Result:

According to your new agent update plan setting, your agent version should be an older release than the latest GA version (which you are currently on). Therefore, to align your agent version with this setting, the next time agent checks for an update, the agent automatically updates to be on an older version. Tenable Agent automatically downgrades to 8.3.0, one release before the latest GA version.

Back Up Tenable Agent

Using Tenable Agent CLI Commands , you can back up your Tenable Agent to restore it later on any system, even if it is a different operating system. When you back up Tenable Agent, your settings are preserved. Tenable Agent does not back up scan results.

> **Note:** If you perform a cross-platform backup and restore between Linux and Windows systems, after you restore Tenable Agent, you must reconfigure any Tenable Agent configurations that use schedules (for example, scan schedules). Schedules do not transfer correctly across these platforms because the operating systems use different timezone names.

To back up Tenable Agent:

1. Access Tenable Agent from a command terminal.
2. Create the Tenable Agent backup file:

   ```
   > nessuscli backup --create <backup_filename>
   ```

   Tenable Agent creates the backup file in the following directory:

   - Linux: `/opt/nessus_agent/var/nessus`
   - Windows: `C:\ProgramData\Tenable\Nessus Agent\nessus\`
   - Mac: `/Library/NessusAgent/run/var/nessus/`

What to do next:

- Restore Tenable Agent

Restore Tenable Agent

Using Tenable Agent CLI Commands , you can use a previous backup of Tenable Agent to restore later on any system, even if it is a different operating system. When you back up Tenable Agent, you preserve your settings. Tenable Agent does not restore scan results.

> **Note:** If you perform a cross-platform backup and restore between Linux and Windows systems, after you restore Tenable Agent, you must reconfigure any Tenable Agent configurations that use schedules (for example, scan schedules). Schedules do not transfer correctly across these platforms because the operating systems use different timezone names.

Before you begin:

- Back Up Tenable Agent

To restore Tenable Agent:

1. Access Tenable Agent from a command terminal.

2. Stop your Tenable Agent service.

   For example:

   ```
   # systemctl stop nessusagent
   ```

   Tenable Agent terminates all processes.

3. Restore Tenable Agent from the backup file you previously saved:

   ```
   > nessuscli backup --restore path/to/<backup_filename>
   ```

   Tenable Agent restores your backup.

4. Stop and start your Tenable Agent service.

   For example:

   ```
   # systemctl stop nessusagent
   # systemctl start nessusagent
   ```

   Tenable Agent begins initializing and uses settings from the backup.

Unlink a Tenable Agent

When you manually unlink an agent, the agent disappears from the manager's linked agent listing, but the system retains related data for the period of time specified in agent settings. When you manually unlink an agent, the agent does *not* automatically relink to either Tenable Nessus Manager or Tenable Vulnerability Management. Unlinking an agent does not stop the agent service itself; the agent continues running on its host.

You can unlink an agent from the `nessuscli` tool by running the `# nessuscli agent unlink` command.

You can also unlink an agent from the manager. For more information, see the following documentation:

- To unlink an agent in Tenable Nessus Manager, see Unlink an Agent in the *Tenable Nessus User Guide*.
- To unlink an agent in Tenable Vulnerability Management, see Unlink an Agent in the *Tenable Vulnerability Management User Guide*.

Tip: *Unlinking* an agent refers to the act of removing the connection between the agent and the manager, whether that be Tenable Nessus Manager or Tenable Vulnerability Management. If you want to remove or uninstall an agent from your machine, see Remove Tenable Agent.

Remove Tenable Agent

This section includes information for uninstalling a Tenable Agent from hosts.

Note: For instructions on how to remove an agent from a manager while leaving the agent installed on the host, see Unlink a Tenable Agent.

Uninstall a Tenable Agent on Windows

You can uninstall an agent from Windows via the Windows user interface or the Windows CLI.

Before you begin:

- Unlink the agent from the manager.

To uninstall Tenable Agent from the Windows user interface:

1. Navigate to the portion of Windows where you can **Add or Remove Programs** or **Uninstall or change a program**.

2. In the list of installed programs, select the **Tenable Agent** product.

3. Click **Uninstall**.

   A dialog box appears, prompting you to confirm your selection to remove Tenable Agent.

4. Click **Yes**.

   Windows deletes all Nessus related files and folders.

To uninstall Tenable Agent from the Windows CLI:

1. Open PowerShell with administrator privileges.

2. Run the following command:

   ```
   msiexec.exe /x <path to Tenable Agent package>
   ```

   > **Note:** For information about optional `msiexec /x` parameters, see msiexec in the Microsoft documentation.

What to do next:

- If you plan on reinstalling the Tenable Agent on the system, see the knowledge base article on how to avoid linking errors.

Uninstall a Tenable Agent on Linux

You can uninstall an agent on Linux from the command line.

Before you begin:

- Unlink the agent from the manager.

To uninstall Tenable Agent on Linux:

1. Type the remove command specific to your Linux-style operating system.

   Example Tenable Agent Remove Commands

Debian/Kali and Ubuntu

```
# dpkg -r NessusAgent
```

Red Hat 6 and 7, Oracle Linux 6 and 7

```
# yum remove NessusAgent
```

Red Hat 8 and later, Oracle Linux 8 and later, Fedora

```
# dnf remove NessusAgent
```

SUSE

```
# sudo zypper remove NessusAgent
```

> **Note:** To completely remove Tenable Agent from the system, you must manually delete the agent filesystem after running the remove command.

What to do next:

- If you plan on reinstalling the Tenable Agent on the system, see the knowledge base article on how to avoid linking errors.

Uninstall a Tenable Agent on macOS

You can uninstall an agent on macOS by deleting the related agent directories and disabling the agent service.

Before you begin:

- Unlink the agent from the manager.

To uninstall Tenable Agent on macOS:

1. Remove the Tenable Agent directories. From a command prompt, type the following commands:

- `$ sudo rm -rf /Library/NessusAgent`
- `$ sudo rm /Library/LaunchDaemons/com.tenablesecurity.nessusagent.plist`
- `$ sudo rm -r "/Library/PreferencePanes/Nessus Agent Preferences.prefPane"`

> **Note:** To completely remove Tenable Agent from the system, you must manually delete the agent filesystem after running the remove command.

2. Disable the Tenable Agent service:

   a. From a command prompt, type the following command:

   ```
   $ sudo launchctl remove com.tenablesecurity.nessusagent
   ```

   b. If prompted, provide the administrator password.

What to do next:

- If you plan on reinstalling the Tenable Agent on the system, see the knowledge base article on how to avoid linking errors.

Agent Status

Tenable Agents can be in one of the following statuses:

Status	Description
Online	The host that contains the Tenable Agent is currently connected and in communication with Tenable Nessus Manager or Tenable Vulnerability Management.
Offline	The host that contains the Tenable Agent is currently powered down or not connected to a network.
Initializing	The Tenable Agent is in the process of checking in with Tenable Nessus Manager or Tenable Vulnerability Management.
Unlinked	(Tenable Nessus Manager only) The agent is in an unlinked state. Agents with this status are only present if **Track unlinked agents** is enabled.

Status	Description
	Note: Agents that are automatically unlinked via the **Unlink inactive agents after X days** setting can automatically relink to Tenable Nessus Manager if they come back online. You must manually relink agents that were manually unlinked.

Scans

You can create and configure Tenable Agents scans in Tenable Nessus Manager and Tenable Vulnerability Management.

For information about configuring agent scans, agent groups, agent templates, and agent settings, see the *Tenable Nessus User Guide* or the *Tenable Vulnerability Management User Guide*, depending on which manager your organization uses.

Settings

You can configure Tenable Agent settings in two ways: remotely from your agent manager (Tenable Vulnerability Management or Tenable Nessus Manager) or locally on the agent's command line interface.

Settings Configured on the Manager

You can configure most agent settings, such as freeze windows, logging, and proxy settings, from the manager interface.

- Configure general settings for linked Tenable Agents.
    - Tenable Vulnerability Management — Agent Settings
    - Tenable Nessus Manager — Modify Agent Settings
- Create, modify, and delete freeze windows for Tenable Agents.
    - Tenable Vulnerability Management — Freeze Windows
    - Tenable Nessus Manager — Freeze Windows
- (Tenable Nessus Manager-only) Modify agent log settings.
    - Tenable Nessus Manager — Manage Logs

Settings Configured on the Agent

You can configure advanced settings and proxy settings directly on the agent using the command line interface.

Advanced Settings

You can manually configure agents by setting advanced settings from the agent command line interface. You can modify some system-wide agent settings from Tenable Nessus Manager Advanced Settings or the **Linked Agents** tab in Tenable Vulnerability Management (see Agent Settings in the *Tenable Vulnerability Management User Guide* for more information). Tenable Agent validates your input values to ensure only valid configurations are allowed.

Tenable Agent Advanced Settings

You can configure the following agent settings in the command line interface using the `nessuscli` utility.

Use the command `# nessuscli fix --set` *`setting`*`=`*`value`*. For more information, see [Tenable Agent CLI Commands](#).

> **Tip:** Customers with many agents (10,000+) may want to configure the `agent_merge_audit_trail`, `agent_merge_kb`, `agent_merge_journal_mode`, and `agent_merge_synchronous_setting` settings. Modifying these settings can dramatically lower the amount of time it takes to merge agent scan results. Review the descriptions in the following table for suggested configurations.

Setting	Description	Default	Valid Values
agent_update_channel	(Tenable Vulnerability Management-linked agents only) Sets the agent update plan to determine what version the agent automatically updates to. **Note:** For agents linked to Tenable Vulnerability Management, you need to run the `agent_update_channel` command from the agent `nessuscli` utility. For agents linked to Tenable Nessus Manager, you need to run the `agent_update_channel` command from the Early	ga	• ga — Automatically updates to the latest Agent version when it is made generally available (GA). **Note:** This date is usually *one week after* the version is made generally available. For versions that address critical security issues, Tenable may make the version available immediately. • ea — Automatically updates to the latest Agent version as soon as it is released for Early

Setting	Description	Default	Valid Values
	Tenable Nessus Manager`nessuscli` utility.		Access (EA), typically a few weeks before general availability. - `stable` — Does not automatically update to the latest Tenable Agent version. Remains on an earlier version of Tenable Agent set by Tenable, usually one release older than the current generally available version, but no earlier than 7.7.0. When Tenable Agent releases a new version, your agent updates software versions, but stays on a version prior to the latest release.
strict_certificate_validation	When enabled, always validate SSL server certificates, even during initial remote link (requires manager to use a trusted root CA).	no	`yes` or `no`

Setting	Description	Default	Valid Values
update_hostname	When enabled, when someone modifies the endpoint hostname, the new hostname is updated in the agent's manager. This feature is disabled by default to prevent custom agent names from being overridden.	no	yes or no
connection_status_check_time	(Tenable Vulnerability Management-linked agents only) Determines how often the agent checks its connection status when offline in seconds.	900	Integers >299
days_to_keep_unused_plugins	(Tenable Vulnerability Management-linked agents only) Determines the duration of time (in days) after which an agent deletes an unused plugin set. For example, if you set this setting to **14** and the agent has not used one of its plugin set for scanning in	14	Integers >7

Setting	Description	Default	Valid Values
	over 14 days, the agent deletes that plugin set.		
detect_duplicates	Regardless of this setting, the agent automatically checks if it is a duplicate agent by comparing its current list of MAC addresses to the MAC addresses the agent had at link time. For agents linked to Tenable Vulnerability Management or Tenable Nessus Manager 8.11.1 and later, the manager performs the same check to identify duplicate agents. When disabled, the agent automatically logs duplicates in `backend.log`, but no action is taken. When enabled, if either the agent or the manager detects a duplicate agent, the agent automatically	no	`yes` or `no`

Setting	Description	Default	Valid Values
	unlinks and regenerates its identifying information (for example, the UUID) so that it can be linked again. This event is logged in `backend.log`. You must manually relink the agent.		
disable_core_updates	When set to `yes`, the agent does not request automatic core updates. You can still upgrade software versions manually. The agent can still receive plugin updates.	`no`	`yes` or `no`
logfile_max_files	Determines the maximum number of `nessusd.messages` files that Tenable Agent keeps on the disk. If the number of `nessusd.messages` log files exceeds the specified value, Tenable Agent deletes the oldest log files.	Tenable Nessus — 100 Tenable Agent — 2	Integers 1-1000

Setting	Description	Default	Valid Values
logfile_max_size	Determines the maximum size of the `nessusd.messages` file in MB. If the file size exceeds the maximum size, Tenable Agent creates a new messages log file.	Tenable Nessus —512 Tenable Agent — 10	Integers 1-2048
logfile_rotation_time	Determines how often Tenable Agent messages log files are rotated in days.	1	Integers 1-365
logfile_rot	Determines whether Tenable Agent rotates messages log files based on maximum rotation size or rotation time.	`size`	• `size` — Tenable Agent rotates log files based on size, as specified in `logfile_max_size`. • `time` — Tenable Agent rotates log files based on time, as specified in `logfile_rotation_time`.
long_term_upload_interval_seconds	(Tenable Vulnerability Management-linked agents only) Determines the number of seconds the agent waits	180	Integers >59

Setting	Description	Default	Valid Values
	between attempting to upload smart scan results.		
report.max_ports	The maximum number of allowable ports. If there are more ports in the scan results than this value, Tenable Nessus discards the port scan results. This limit helps guard against fake targets that may have thousands of reported ports, but can also result in the deletion of valid results from the scan results database, so you may want to increase the default if this is a problem.	1024	Integers
portscanner.max_ports	The maximum number of ports that the Tenable Nessus port-scanning plugins can mark as open. This includes the port scanners proper and any plugin that calls NASL function `scanner_add_port`	1024	Integers 0-65535

Setting	Description	Default	Valid Values
	`()`.		
maximum_scans_per_day	Determines the maximum number of scans an agent can run per day.	10	Integers 1-48
min_metadata_update_interval	(Tenable Vulnerability Management-linked agents only) Determines the minimum number of minutes between the agent's attempts to push metadata to Tenable Vulnerability Management. **Note:** The agent only attempts to push metadata to Tenable Vulnerability Management if the metadata changes.	10	Integers >4
dumpfile_max_files	Sets the maximum number of the `nessusd.dump` files kept on disk. If the number exceeds the specified value, the setting deletes the oldest dump file.	100	Integers 1-1000
dumpfile_max_size	Sets the maximum	512	Integers 1-2048

Setting	Description	Default	Valid Values
	size of the `nessusd.dump` files in MB. If file size exceeds the maximum size, the setting creates a new dump file.		
offline_agent_scan_trigger_ execution_threshold_days	(Tenable Vulnerability Management-linked agents only) Determines the number of days of being offline after which rule-based scans no longer launch.	14	Integers >0
plugin_load_performance_mode	Sets plugin compilation performance, which affects CPU usage. Low performance slows down plugin compilation, but reduces the agent's CPU consumption. Setting the performance to medium or high means that plugin compilation completes more quickly, but the agent	Tenable Agent 10.8.3 and later — `medium` Tenable Agent 10.8.2 and earlier — `high`	`low`, `medium`, or `high`

Setting	Description	Default	Valid Values
	consumes more CPU. • `low`: Uses exactly one thread. Deliberately consumes less time than available, approximating 50% usage of one core. • `medium`: Uses up to half as many threads as cores available, up to a maximum of four cores on a system with eight or more cores. Always uses at least one thread. • `high`: Uses as many threads as cores available, up to a maximum of eight threads. For more information, see Agent CPU		

Setting	Description	Default	Valid Values
	Resource Control. **Note:** Tenable recommends setting Plugin Compilation Performance to `medium` or `low` for shared resource environments, such as VDI or ESXi.		
scan_performance_mode	Sets scan performance, which affects CPU usage. Low performance slows down scans, but reduces the agent's CPU consumption. Setting the performance to medium or high means that scans complete more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control.	`high`	`low`, `medium`, or `high`
skip_asset_observation_on_update	Determines whether the agent only updates the asset metadata when linking to Tenable Vulnerability	`no`	`yes` or `no`

Setting	Description	Default	Valid Values
	Management. When you set this setting to no, the agent updates Tenable Vulnerability Management with new asset metadata based on the Advanced Settings.		
ssl_cipher_list	Sets the cipher list to use for Agent outbound connections.	`compatible`	- `legacy` — A list of ciphers that can integrate with older APIs. - `compatible` — A list of secure ciphers. May not include all the latest ciphers. - `modern` — A list of the latest and most secure ciphers. - `custom` — A custom OpenSSL cipher list. For more information on valid cipher list formats, see the OpenSSL documentation. **Tip**: For a list of Tenable-supported ciphers, see System Requirements in the *Tenable Vulnerability*

Setting	Description	Default	Valid Values
			Management User Guide.
ssl_mode	Minimum supported version of TLS.	`tls_1_2`	- `ssl_3_0` — SSL v3+ - `tls_1_2` — TLS v1.2+

Tenable Agent Secure Settings

You can configure the following secure settings in the command line interface, using the `nessuscli` utility.

Use the command `# nessuscli fix --secure --set` *`setting=value`*. For more information, see Tenable Agent CLI Commands .

Caution: Tenable does not recommend changing undocumented `--secure` settings as it may result in an unsupported configuration.

Setting	Description	Valid Values
`auto_proxy`	(Windows-only) If enabled, the agent uses Web Proxy Auto Discovery (WPAD) to obtain a Proxy Auto Config (PAC) file for proxy settings. This setting overrides all other proxy configuration preferences. If disabled, the agent defaults to the remaining proxy settings.	`true` or `false`
`ignore_proxy`	If enabled, the agent attempts a direct connection to the manager instead of using the set proxy, until it fails 10 times. If disabled, the agent attempts to connect using the set proxy, until it fails three times. This setting changes automatically, as described in Proxy Connection Fallback. You can also set this setting manually; however, if at any point the agent meets one of the conditions described in Proxy Connection Fallback, the agent	`yes` or `no`

Setting	Description	Valid Values
	automatically changes the setting.	
`ms_proxy`	When enabled, the agent uses a proxy to connect to its manager.	`true` or `false`
`proxy`	The hostname or IP address of your proxy server.	String
`proxy_port`	The port number of the proxy server.	String
`proxy_auth`	(Optional) If you want to use authentication to connect to the proxy, specify the authentication scheme.	`basic`, `digest`, `ntlm`, or `auto`
`proxy_username`	If using authentication to connect to the proxy, the name of a user account that has permissions to access and use the proxy server.	String. If there are spaces, use quotes (").
`proxy_password`	If authenticating with the proxy, password associated with the username.	String

Tenable Nessus Manager Advanced Settings

You can configure the following system-wide agent settings in Tenable Nessus Manager, under the **Settings** > **Advanced Settings** > **Agents & Scanners** section. For more information, see Advanced Settings in the *Tenable Nessus User Guide*.

Setting	Description	Default	Valid Values	Restart Required?
agent_auto_delete	Controls whether agents are automatically deleted after they	no	`yes` or `no`	no

Setting	Description	Default	Valid Values	Restart Required?
	have been inactive for the duration of time set for `agent_auto_delete_threshold`.			
agent_auto_delete_threshold	The number of days after which inactive agents are automatically deleted if `agent_auto_delete` is set to `yes`.	60	Integers 1-365	no
agent_auto_unlink	Controls whether agents are automatically unlinked after they have been inactive for the duration of time set for `agent_auto_unlink_threshold`.	`no`	`yes` or `no`	no
agent_auto_unlink_threshold	The number of days after which inactive agents are automatically unlinked if `agent_auto_unlink` is set to `yes`.	30	Integers 30-90	no

Setting	Description	Default	Valid Values	Restart Required?
	Note: This value must be less than the `agent_auto_delete_threshold`.			
agents_progress_viewable	When a scan gathers information from agents, Tenable Nessus Manager does not show detailed agents information if the number of agents exceeds this setting. Instead, a message indicates that results are being gathered and will be viewable when the scan is complete.	100	Integers. If set to 0, this defaults to 100.	no
agent_updates_from_feed	When enabled, new Tenable Agent software updates are automatically downloaded.	`yes`	`yes` or `no`	yes
cloud.manage.download_	The maximum	10	Integers	no

Setting	Description	Default	Valid Values	Restart Required?
max	concurrent agent update downloads.			
agent_merge_audit_trail	Controls whether or not agent scan result audit trail data is included in the main agent database. Excluding audit trail data can significantly improve agent result processing performance. If this setting is set to false, the **Audit Trail Verbosity** setting in an individual scan or policy defaults to `No audit trail`. Available in Nessus 8.3 and later.	`false`	`true` or `false`	no
agent_merge_kb	Includes the agent scan result KB data in the main agent	`false`	`true` or `false`	no

Setting	Description	Default	Valid Values	Restart Required?
	database. Excluding KB data can significantly improve agent result processing performance. If this setting is set to false, the **Include the KB** setting in an individual scan or policy defaults to `Exclude KB`. Available in Nessus 8.3 and later.			

agent_merge_journal_mode	Sets the journaling mode to use when processing agent results. Depending on the environment, this can somewhat improve processing performance, but also introduces a small risk of a	`DELETE`	`MEMORY`
			`TRUNCATE`
			`DELETE`
				no

Setting	Description	Default	Valid Values	Restart Required?
	corrupted scan result in the event of a crash. For more details, refer to the sqlite3 documentation. Available in Nessus 8.3 and later.			
agent_merge_synchronous_setting	Sets the filesystem sync mode to use when processing agent results. Turning this off will significantly improve processing performance, but also introduces a small risk of a corrupted scan result in the event of a crash. For more details, refer to the sqlite3 documentation. Available in Nessus 8.3 and	FULL	OFF NORMAL FULL	no

Setting	Description	Default	Valid Values	Restart Required?
	later.			
track_unique_agents	When enabled, Tenable Nessus Manager checks if MAC addresses of agents trying to link match MAC addresses of currently linked agents with the same hostname, platform, and distro. Tenable Nessus Manager deletes duplicates that it finds.	no	yes or no	no

Proxy Settings

Configure Proxy Settings

You can configure a Tenable Agent to connect to its manager (Tenable Nessus Manager or Tenable Vulnerability Management) via a proxy in one of the following ways:

- During initial installation and linking.

  For more information, see the linking command proxy settings in Tenable Agent CLI Commands .

- After you have installed and linked.

After initial linking, you can configure a proxy or change existing proxy settings via the command line. For more information, see Tenable Agent Secure Settings.

Proxy Connection Fallback

If an agent is using a proxy to connect to its manager, there is a built-in proxy fallback in case of a connection failure.

The automatic fallback process happens as follows:

1. If the agent is unable to access its manager through the proxy, and fails three times in a row, the agent tries connecting directly to the manager.

2. If the agent successfully connects directly to the manager, the agent automatically sets the secure setting `ignore_proxy` to `yes`. When you enable this setting, the agent will connect directly to the manager on future attempts, instead of using the proxy.

3. However, if the agent fails to connect directly to the manager 10 times in a row, the agent retries connecting via the proxy again. If the agent successfully connects via the proxy, the agent automatically sets `ignore_proxy` to `no`, meaning the agent will connect using the proxy on future attempts.

4. The process repeats as needed, depending on whether the agent fails to connect to the proxy or directly to the manager.

At any point, you can manually change the secure setting `ignore_proxy` to `yes` or `no` to interrupt the automatic fallback process. This forces the agent to attempt to connect either directly or via the proxy, depending on what you set. However, if at any point the agent meets one of the conditions listed above (for example, fails to connect via proxy three times in a row), the automatic fallback process resumes.

Configure Agent Profiles to Avoid Asset Duplication in Tenable Vulnerability Management

In Tenable Vulnerability Management configurations that scan hosts with both Tenable Nessus scanners and Tenable Agents, there are instances where a scanner scans and records an asset that already has an agent installed on it. This causes the asset to be identified as two (or more, in some cases) separate assets in Tenable Vulnerability Management.

For Tenable Agents versions 10.6.0 and later, you can configure an **Open Agent Port** (also known as the **Advanced Asset Identification** setting) in Tenable Vulnerability Management agent profiles to avoid this case of asset duplication.

Enabling and configuring an agent profile's **Open Agent Port** allows the agents of that profile to run an agent identification service on their installed hosts. The service opens a configurable port on the host and allows Tenable scanners to identify that the installed agent has already inventoried the host as an asset. Unauthenticated remote network scans identify the agent's Tenable UUID via the open agent port.

This identification ensures that the host is recorded as a single asset in Tenable Vulnerability Management, regardless of whether they are the target of a scanner's network scan or are generating agent scans.

For information on how to configure the **Open Agent Port** for an agent profile, see Agent Profiles in the *Tenable Vulnerability Management User Guide*.

Considerations

Consider the following when configuring the **Open Agent Port**:

- Only agents version 10.6.0 and later can use the **Open Agent Port** setting. The setting does not apply to any agent on an earlier version.
- Configuring the **Open Agent Port** permits your network scanners to probe each target system on the port you select.

- The agent identification service is only started if the agent profile specifies a valid **Open Agent Port**.

- The agent identification service attempts to open and listen on the TCP port specified in the agent profile's **Open Agent Port**. If you have any local firewall or host protection products installed on the host, you need to configure them to allow the agent identification service to open this port for incoming connections. Tenable recommends allowlisting Tenable Agent files and processes to ensure that the **Open Agent Port** feature works without interruption.

- On macOS and Linux, the agent identification service creates a low-privilege service account to execute under. On Windows, the agent identification service runs as a low integrity process.

- The **Open Agent Port** assigned to an agent reopens whenever the agent upgrades or restarts or whenever the host reboots.

- If the agent identification service detects a record that belongs to two Tenable networks, the merged asset is added to the network of the scanner that last found the asset.

- On macOS and Linux hosts, the agent identification service requires a system user to run under. When you initially configure **Open Agent Port**, the agent automatically creates a system user called **_tenabletag** on macOS hosts, or **tenabletag** on Linux hosts. The tenabletag user is a locked system user and cannot be used for logging in.

  When you uninstall Tenable Agent from a macOS or Linux host, the tenabletag user is not deleted to preserve the UID mapping. To remove the user, refer to your operating system's user deletion documentation.

- On all operating systems, the asset UUID service requires the operating system to have a basic level of IPv6 support, though IPv6 itself does not have to be enabled on any network interfaces. On Linux, this may cause problems in older Linux distributions following configuration guides that used to recommend disabling the Linux IPv6 driver via kernel boot parameters. On such a system, you can disable IPv6 via `sysctl` parameters in /etc/sysctl.conf, instead of disabling them on the kernel boot command line. This allows the asset UUID service to function without allowing IPv6 to be enabled on such a system.

  ```
  net.ipv6.conf.all.disable_ipv6 = 1
  net.ipv6.conf.default.disable_ipv6 = 1
  ```

This is only required if you are trying to explicitly disable IPv6 on your hosts while using the asset UUID service. The current CIS benchmarks for various Linux distributions no longer recommend disabling IPv6, but older editions of the CIS benchmarks offer the above settings as a less-instrusive way to disable IPv6.

Logging and Troubleshooting

You can view log information about the **Open Agent Port** in agent bug report bundles and in the following directories:

Operating System	Log Location
Windows	C:\ProgramData\Tenable\NessusAgent\nessus\mod\com.tenable.agent_identifier_service\data\com.tenable.agent_identifier_service.log
macOS	/Library/NessusAgent/run/var/nessus/mod/com.tenable.agent_identifier_service/data/com.tenable.agent_identifier_service.log
Linux	/opt/nessus_agent/var/nessus/mod/com.tenable.agent_identifier_service/data/com.tenable.agent_identifier_service.log

To verify that the agent identification service is working, view plugin 191492 - Tenable Agent Identification. The plugin generates an Info-level finding when the agent identification service triggers and provides the Tenable UUID of the detected agent.

Configure Tenable Agent for NIAP Compliance

If your organization requires that Tenable Agent meets National Information Assurance Partnership (NIAP) standards, you can configure Tenable Agent so that relevant settings are compliant with NIAP standards.

Before you begin:

- If Tenable Agent is linked to Tenable Nessus Manager, verify that the CA certificate of Tenable Nessus Manager is in custom_CA.inc or known_CA.inc.
- Confirm you have enabled the full disk encryption capabilities provided by the operating system on the host where Tenable Agent is installed.

To configure Tenable Agent for NIAP compliance:

1. Access the agent from the command line interface.

2. Enable NIAP mode using the command line interface:

   - In the command line, enter the following command:

     ```
     nessuscli fix --set niap_mode=enforcing
     ```

     Linux example:

     ```
     /opt/nessus_agent/sbin/nessuscli fix --set niap_mode=enforcing
     ```

   Tenable Agent does the following:

   > **Note:** When Tenable Agent is in NIAP mode, Tenable Agent overrides the following settings as long as Tenable Agent remains in NIAP mode. If you disable NIAP mode, Tenable Agent reverts to what you had set before.

   - Overrides the SSL mode (`ssl_mode`) with TLS 1.2 (`niap`).
   - Overrides the SSL cipher list (`ssl_cipher_list`) setting with NIAP-compliant ciphers (`niap`), which sets the following ciphers:
     - ECDHE-RSA-AES128-SHA256
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-AES256-GCM-SHA384
   - Uses strict certificate validation:
     - Disallows certificate chains if any intermediate certificate lacks the CA extension.
     - Authenticates a server certificate, using the signing CA certificate.
     - Authenticates a client certificate when using client certificate authentication for login.

    - Checks the revocation status of a CA certificate using the Online Certificate Status Protocol (OCSP). If the certificate is revoked, then the certificate is marked as invalid. If there is no response, then the certificate is not marked as invalid, and its use is permitted if it is otherwise valid.
    - Ensures that the certificate has a valid, trusted CA that is in known_CA.inc. CA Certificates for Tenable Vulnerability Management and plugins.nessus.org are already in known_CA.inc in the plugins directory.
    - If linked to Tenable Nessus Manager, verifies that the CA certificate of Tenable Nessus Manager is found in custom_CA.inc or known_CA.inc.

- Enforces the current validated FIPS module for agent communication and database encryption. The FIPS module does not affect scanning encryption.

  > **Note:** You can enforce the FIPS module from the agent nessuscli utility without enforcing NIAP mode. For more information, see Tenable Agent CLI Commands .

Create Windows or Linux Golden Image with Tenable Agent Installed

You can install a Tenable Agent on a Windows or Linux golden image. However, there are files and registry settings that you must set per host.

> **Note:** By removing and changing files, the agent generates new files once the agent reboots. If the host is imaged with these files and you attempt to link several imaged agents, you receive a 409 UUID error.

The following steps require administrative or root privileges. You only need to perform the following steps if the agent you want to use in the image is already linked to Tenable Vulnerability Management or Tenable Nessus Manager.

To create a golden image with Tenable Agent installed:

1. Stop the agent service.
2. Run the `prepare-image` command (using Linux syntax as an example):

   ```
   ./nessuscli prepare-image
   ```

   Running this command performs the following pre-imaging cleanup tasks:

- Unlinks the agent, if linked.
- Deletes any host tag on the agent. For example, the registry key on Windows or `tenable_tag` on Unix.
- Deletes any UUID file on the agent (for example, `/opt/nessus/var/nessus/uuid` or an equivalent on macOS and Windows).
- Deletes plugin dbs.
- Deletes the global db.
- Deletes `master.key`.
- Deletes the backups directory.

> **Note:** Do not restart the agent service on the host until you have created the image. Restarting the agent service regenerates the UUIDs, tags, and files that the `prepare-image` command has purged.

3. Once the command finishes running, create the golden image based on your organization's standards.

> **Caution:** Ensure that your golden image is properly configured before linking agents to instances of the golden image. Using an improperly configured golden image can cause multiple agents to share the same UUID, which may result in duplicate asset issues.

4. Link the agent back to Tenable Vulnerability Management or Tenable Nessus Manager on individual instances of the golden image via the config.json method or by running the `nessuscli agent link` command.

More resources:

- Mass Deployment Support

Customer Case Studies

The customer case studies describe Tenable Agent deployments in real customer environments. The case studies highlight key configuration and deployment considerations.

- ACME's environment consisted of 70,000 assets. ACME utilized the Tenable Vulnerability Management platform to manage agent scanning operations, and a single Tenable Security Center instance to manage 40 scanners and to provide unified analytics of both network and Tenable Agent assessment results.

  For more information, see ACME.

- Initech is a global organization consisting of 30+ sub-organizations, 40,000 users, 60,000 devices, and 150,000+ active IP addresses. Initech used a hybrid Tenable Vulnerability Management and Tenable Nessus Manager solution for managing Tenable Agents. Tenable Vulnerability Management was used for user workstation Tenable Agent scan operations, and Tenable Nessus Manager was used for servers and other permanent on-premise infrastructure. Initech then imported all Tenable Agent scan data into Tenable Security Center for unified reporting and analytics.

  For more information, see Initech.

- Sprocket utilized Tenable Vulnerability Management for Tenable Agent management and local scan and audit information, remote network scan functionality, and integration with their third-party applications via the Tenable Vulnerability Management API.

  For more information, see Sprocket.

ACME Customer Case Study

A customer, ACME, was using a single Tenable Security Center instance that managed 40 scanners to perform network vulnerability assessments of approximately 1,200 stores on a monthly basis.

ACME wished to update their existing operational model to leverage Tenable Agents to collect assessment results from approximately 70,000 assets. ACME implemented a hybrid approach using the Tenable Vulnerability Management platform to manage agent scanning operations and import agent scan results into Tenable Security Center for unified analytics and reporting of both network and agent assessment results.

The intent of this case study is to highlight key configuration considerations that were implemented when ACME moved forward with deploying Tenable Agents.

Objectives

The primary goal defined by ACME to measure the success of the Tenable Agent project was their ability to leverage agents across their store infrastructure to collect in-depth asset data, while reducing the current network latency experienced by remote network scans.

Scanning coverage:

- To implement local host scanning using agents on assets across stores to provide more detailed vulnerability assessment results than the current unauthenticated network active scan to stores from headquarter datacenters.
- To use agent scans to reduce the impact to ACME's network and allow for more frequent scans.

Solution

A Tenable Vulnerability Management and Tenable Security Center hybrid deployment was used in their enterprise environment. Tenable Vulnerability Management was required for agent scan operations, and the existing Tenable Security Center infrastructure was used for advanced analytics and reporting. By leveraging Tenable Vulnerability Management for agent scan operations, ACME could automatically scale for large numbers of agents and assets, without the need for on-prem software and hardware.

ACME leveraged their existing Tenable Security Center infrastructure to achieve their vulnerability management program goals by importing agent scan data from Tenable Vulnerability Management into Tenable Security Center for unified reporting and analytics. This solution split the environment into two tiers, Reporting (Tenable Security Center) and Operational (Tenable Vulnerability Management), so that ACME could optimize reporting experiences for its end users, while not impacting the data acquisition capabilities of the platform.

Tenable Agent Operational Tier (Tenable Vulnerability Management)

The primary purpose for the Operational Tier (Tenable Vulnerability Management) was to perform agent management and agent scan operations.

Functions performed

The following processes and uses take place in the Operational Tier (Tenable Vulnerability Management).

- Deployed agents are linked to Tenable Vulnerability Management.
- Agents are organized in agent groups. Agents can be assigned to agent groups during the installation process.
- Agent scans are established to obtain assessment results from agents via agent groups.
- Agents automatically have plugin and version updates applied by Tenable Vulnerability Management.
- Customers can “opt out” of having agent version updates automatically applied.

Considerations

- Agents were deployed using ACME's internal software distribution processes (in this case, SCCM).
- Agent groups included no more than 20,000 agents per group (10,000 is recommended). Limiting the number of agents in each agent group ensures that Tenable Security Center can import scan results successfully. This limitation only applies when Tenable Security Center is part of the deployment.
- Agent scans were restricted to a single agent group each.
- Agent group membership was established by functional zones (by location, role, etc.) for organizational purposes.
- ACME monitored for agent deployment issues (failed installations, linking failures, etc.) out of band (logging client, scripts, etc.).
- Agents only performed local vulnerability assessments and did not perform network-based assessment (for example, SSL or CGI network-based assessments).
- Network and firewalls were configured to allow agents to communicate with https://cloud.tenable.com.

Tier design

Design assumptions included:

- ACME leverages internal processes and tooling to deploy the Tenable Agent software.
- ACME establishes 50-70 agent groups.
- ACME configures 50-70 agent scans.

Reporting Tier (Tenable Security Center)

The primary purpose of the reporting tier was to allow for centralized analytics and reporting of data collected from the Tenable Agent operational tier (Tenable Vulnerability Management). Dashboards, analytics, reports, and Assurance Report Cards are leveraged on this tier.

Functions performed

The following processes and uses take place in the Reporting Tier (Tenable Security Center).

- Tenable Vulnerability Management was added to Tenable Security Center as an "agent capable" scanner.
- Agent scans in Tenable Security Center were configured to retrieve agent scan results from Tenable Vulnerability Management.
- Analytics, dashboards, reports, and Assurance Report Cards in Tenable Security Center were leveraged for all assessment types (Agent and Network Scanning).

Considerations

- Tenable recommended that ACME configure Tenable Security Center to retrieve agent scan results from Tenable Vulnerability Management the same day Tenable Vulnerability Management collects assessment results from agents. This configuration ensures that Tenable Security Center captures proper detection dates.
- Tenable Security Center required additional data repositories to support the agent results. Tenable recommended that ACME establish two new repositories in Tenable Security Center for agent results, because repositories can only handle upwards of 50,000 assets each.
- Tenable Security Center 5.7 introduced an agent-specific repository that leverages the agent UUID to better track uniqueness when results are imported into Tenable Security Center.
- ACME needed to perform a full analysis on their current Tenable Security Center hardware configuration to determine if additional CPU/RAM/HDD was required for the additional data resulting from importing agent scan results.

Tier design

Design assumptions included:

- ACME will establish two (2) repositories to store agent scan results.
- ACME will establish 50-70 agent scans to retrieve agent scan results from Tenable Vulnerability Management.
- ACME will balance each agent scan retrieval evenly across the two (2) new repositories.
- ACME will evaluate current infrastructure to determine if additional CPU/RAM/HDD is required.

Initech Customer Case Study

A customer, Initech, was using a tiered Tenable Security Center deployment across a large federated environment consisting of 30+ sub-organizations, 40,000 users, 60,000 devices, and 150,000+ active IPs. They performed weekly network vulnerability assessments with over 75 scanners at sites located around the United States.

Initech had a reporting requirement to perform more frequent assessments of their systems and to be able to remotely gather data from user laptops when they were off-site. Initech deployed over 50,000 Tenable Agents to accomplish this task, using a hybrid model with both Tenable Nessus Manager and Tenable Vulnerability Management, feeding data back into Tenable Security Center for analytics and reporting.

The intent of this case study is to highlight key configuration considerations that were implemented when Initech moved forward with deploying Tenable Agents.

Objectives

The primary goals defined by Initech to measure the success of the Tenable Agent project were to gather data more frequently, assess remote systems, and reduce the burden posed by managing credentials across a large disparate enterprise.

Solution

A Tenable Nessus Manager and Tenable Vulnerability Management hybrid deployment was used for agents in their enterprise environment. Tenable Vulnerability Management was required for user workstation Tenable Agent scan operations, and Tenable Nessus Manager was used for servers and other permanent on-premise infrastructure.

- Initech used the scaling ability, uptime guarantee, and cloud flexibility of Tenable Vulnerability Management to meet the dynamic requirements of a constantly changing workstation environment.
- Initech used Tenable Nessus Manager, an on-premise solution, to provide more user control over the scan data for more sensitive systems, such as server infrastructure.

Initech leveraged their existing Tenable Security Center infrastructure to achieve their vulnerability management program goals by importing agent scan data from Tenable Nessus Manager and Tenable Vulnerability Management into Tenable Security Center for unified reporting and analytics.

Agent Deployment (Tenable Nessus Manager and Tenable Vulnerability Management)

The primary purpose for Tenable Nessus Manager was to perform agent management and agent scan operations for on-premise infrastructure (10,000 systems), while Tenable Vulnerability Management was used for agent management and scan operations of user workstations (40,000 systems).

Functions performed

- Deployed agents are linked to Tenable Nessus Manager or Tenable Vulnerability Management depending on system type.
- Agents are organized in agent groups. Agents can be assigned to agent groups during the installation process.
- Agent scans are established to obtain assessment results from agents via agent groups.
- Agents automatically have plugin and version updates applied by Tenable Nessus Manager or Tenable Vulnerability Management.

Considerations

- Agents were deployed using Initech's internal software distribution processes (in this case, a large variety of platforms including Altiris, SCCM, Tivoli, Casper, and others).
- Agent groups included no more than 2,000 agents per group (1,000 is recommended). Limiting the number of agents in each agent group ensures that Tenable Security Center is able to

successfully import scan results. This limitation only applies when Tenable Security Center is part of the deployment.

- Agent scans were restricted to a single agent group each.
- Agent scan policies were more thorough and verbose than the network scans due to the increased efficiency of agent scan distribution.
- On-Premise/Server agent scan windows were restricted to custom time frames selected by each sub-org to meet individual organizational requirements.
- User workstation scan windows were set to ~24 hours and repeated daily to ensure full coverage regardless of when a system was turned on.
- Agent group membership was established by organization and in some cases, operational tier or other functional requirements.
- Initech monitored for agent deployment issues (failed installations, linking failures, etc.) out of band (logging client, scripts, etc.).
- Agents only performed local vulnerability assessments and did not perform network-based assessment (for example, SSL or CGI network based assessments).
- Network and firewalls were configured to allow infrastructure agents to communicate with the on-premise Tenable Nessus Manager via a custom port, and user workstations to communicate with https://cloud.tenable.com.

Tier design

Design assumptions included:

- Initech will leverage internal processes and tooling to deploy the agent software.
- Initech will establish 30-50 agent groups in both Tenable Nessus Manager and Tenable Vulnerability Management.
- Initech will configure 30-50 agent scans in both Tenable Nessus Manager and Tenable Vulnerability Management.
- Initech will configure and provision a Tenable Nessus Manager that can handle 10,000 agents connecting to it.

Reporting and Network Scanning (Tenable Security Center)

The primary purpose of the reporting tier was to allow for centralized analytics and reporting of data collected from the Tenable Agents and existing network scans. Dashboards, analytics, reports, and Assurance Report Cards are leveraged on this tier.

Functions performed

The following processes and uses take place in Tenable Security Center.

- Tenable Nessus Manager and Tenable Vulnerability Management were added to Tenable Security Center as an "agent capable" scanners.
- Agent scans in Tenable Security Center were configured to retrieve agent scan results from Tenable Nessus Manager and Tenable Vulnerability Management.
- Agent data was placed in new repositories according to existing data models.
- Analytics, dashboards, reports, and Assurance Report Cards in Tenable Security Center were leveraged for all assessment types (Agent and Network Scanning).

Considerations

- Tenable Security Center required additional data repositories to support the agent results. Tenable recommended that Initech establish multiple new repositories in Tenable Security Center for agent results, because combining agent and network assessment results in the same repository can cause reporting challenges.
- Initech needed to perform a full analysis on their current Tenable Security Center hardware configuration to determine if additional CPU/RAM/HD was required for the additional data resulting from importing agent scan results.
- Initech needed to evaluate their existing network scan structures/policies to ensure limited data overlap once agent assessments were implemented and data imported into Tenable Security Center.

Tier design

Design assumptions included:

- Initech will establish multiple repositories to store agent scan results.
- Initech will establish 60-100 agent jobs to retrieve agent scan results from Tenable Vulnerability Management and Tenable Nessus Manager.

- Initech will evaluate current infrastructure to determine if additional CPU/RAM/HDD is required.
- Initech will evaluate existing scan structures/policies to limit data overlap.

Sprocket Customer Case Study

Sprocket Inc. is a global company with offices and employees in almost all countries. Sprocket's large and distributed workforce presented several challenges when selecting and designing a security solution. Sprocket required a solution that provided the following:

- Immediate and consistent local scans across all 330,000 assets including servers in company data centers, cloud servers (Azure and AWS), and transient devices like employee laptops.
- Minimized network load since their data centers were at capacity.
- Improved credential management due to their global distributed workforce and siloed organizations.
- The ability to integrate with third-party applications that are used to manage and monitor information across their IT landscape.
- A solution that could scale as their OT Security, Tenable Web App Scanning, and container environments increased.

Solution

Sprocket leveraged Tenable Vulnerability Management to manage all aspects of their environment. The solution used Tenable Agents for all Windows, Linux, and macOS devices for local scan and audit information, and Tenable Nessus scanners located in private cloud instances in each organizational theater for remote network scanning. Tenable Vulnerability Management also provided the needed API to utilize their third-party and customized applications.

Sprocket deployed Tenable Agents using customized scripts for each operating system based on the asset function. The Tenable Agents were assigned to one of 130 groups based on the operating system and asset owner.

FAQ

Are agents or network-based scans easier to run?

The ease or difficulty of each scanning method depends on your environment and your organizational needs.

Consider the following questions:

- Is it possible to install a Tenable Nessus scanner and possibly a Tenable Network Monitor in every network segment?
- Would it be easier to install fewer Tenable Nessus Managers (for example, one or three) and allow the agents to report back in over and through hops and firewalls, etc.?
- Are all your systems online, connected, and reporting back full results during your scan windows?
- Are all systems, when sleeping, configured correctly and respond appropriately to wake-on-lan?
- Do you spend time trying to keep track or obtain the current credentials for many systems?
- Does your network include laptops that work remotely that you cannot credential scan through VPN or when not connected to the organization network directly?

What plugins work with agents / credentialed scans?

> **Note:** The Tenable Research team is constantly adding and updating plugins. For a comprehensive list of plugins, see https://www.tenable.com/plugins.

Most plugins work with Tenable Agents. The exceptions include:

- Plugins that work based on remotely disclosed information or that detect activity performed through remote connectivity, such as logging into a DB server, trying default credentials (brute force), or traffic-related enumeration.
- Plugins related to network checks.

There are also cases where there is overlap in the intent of the check. For example, if you use OS fingerprinting without credentials in a network-based scan and query the system for the exact version of its OS in a credentialed scan, this overlap heightens the credential findings over the network, since the network version tends to be a best guess.

What data does an agent send to Tenable Vulnerability Management / Tenable Nessus Manager?

Agents send the following data to Tenable Vulnerability Management/Tenable Nessus Manager:

- Version information (agent version, host architecture)
- Versions of installed Tenable plugins
- OS information (for example, `Microsoft Windows Server 2019 Enterprise Service Pack 1`)
- Tenable asset IDs (for example, `/etc/tenable_tag` on Unix, `HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\TAG` on Windows)
- Network interface information (network interface names, MAC addresses, IPv4 and IPv6 addresses, hostnames and DNS information if available)
- Hostname if `update_hostname` is set to `yes` (see Advanced Settings for more information)
- AWS EC2 instance metadata, if available:
  - `privatelp`
  - `accountId`
  - `imageId`
  - `region`
  - `instanceType`
  - `availabilityZone`
  - `architecture`
  - `instanceId`
  - `local-hostname`
  - `public-hostname`
  - `public-ipv4`
  - `mac`

- `iam/security-credentials/`
- `public-keys/0/openssh-key`
- `security-groups`

Manage Logs

The following topic describes Tenable Agent log files. Agent log files are located in the following directories:

Operating System	Log Location
Windows	`C:\ProgramData\Tenable\Nessus Agent\nessus\logs`
Linux	`/opt/nessus_agent/var/nessus/logs`
macOS	`/Library/NessusAgent/run/var/nessus/logs`

nessusd.dump

`nessusd.dump` is the agent dump log file used for debugging output.

To configure `nessusd.dump`:

1. Open the agent command line interface.
2. Use the command `# nessuscli fix --set` *`setting=value`* to configure the following settings:

Name	Setting	Description	Default	Valid Values
Nessus Dump File Max Files	dumpfile_max_files	Sets the maximum number of the `nessusd.dump` files kept on disk. If the number exceeds the specified value, the setting deletes the	100	Integers 1-1000

		oldest dump file.		
Nessus Dump File Max Size	dumpfile_ max_size	Sets the maximum size of the `nessusd.dump` files in MB. If the file size exceeds the maximum size, the setting creates a new dump file.	512	Integers 1-2048

For more information, see Advanced Settings.

nessusd.messages

`nessusd.messages` is the agent message log.

To configure `nessusd.messages`:

1. Open the agent command line interface.
2. Use the command `# nessuscli fix --set setting=value` to configure the following settings:

Name	Setting	Description	Default	Valid Values
Log File Maximum Files	logfile_ max_files	Determines the maximum number of `nessusd.messages` files that Tenable Agent keeps on the disk. If the number of `nessusd.messages` log files exceeds the specified value, Tenable Agent deletes the oldest log files.	2	Integers 1-1000

Log File Maximum Size	logfile_max_size	Determines the maximum size of the `nessusd.messages` file in MB. If the file size exceeds the maximum size, Tenable Agent creates a new message log file.	10	Integers 1-2048

For more information, see Advanced Settings.

backend.log

`backend.log` is the agent backend log.

You can configure log locations and rotation strategies for `backend.log` by editing the `log.json` file. You can also configure custom logs by creating a new `reporters[x].reporter` section and creating a custom file name.

To configure `backend.log`:

1. Using a text editor, open the `log.json` file, located in the corresponding directory:

   - **Windows** — `C:\ProgramData\Tenable\Nessus Agent\nessus\log.json`
   - **Linux** — `/opt/nessus_agent/var/nessus/log.json`
   - **macOS** — `/Library/NessusAgent/run/var/nessus/log.json`

2. For `backend.log`, edit or create a `reporters[x].reporter` section, and add or modify the following parameters:

Parameter	Default value	Can be modified?	Description
`tags`	`log, info, warn, error, trace`	yes	Determines what log information the log includes. - `response` —

			Web server activity logs - `info` — Informational logs for a specific task - `warn` — Warning logs for a specific task - `error` — Error logs for a specific task - `debug` — Debugging output - `verbose` — debugging output with more information than debug - `trace` — Logs used to trace output
`type`	`file`	not recommended	Determines the type of the log file.
`rotation_ strategy`	`size`	yes	Determines whether the log archives files based on maximum

			rotation size or rotation time. Valid values: • `size` — Rotate the log based on size, as specified in `max_size`. • `daily` — Rotate the log based on time, as specified in `rotation_time`.
`rotation_time`	86400 (1 day)	yes	Rotation time in seconds. Only used if `rotation_strategy` is `daily`.
`max_size`	10485760 (10 MB)	yes	Rotation size in bytes. Only used if `rotation_strategy` is `size`.
`max_files`	2	yes	Maximum number of files allowed in the file rotation. The maximum number includes the main file, so 10 `max_files` is 1

			main file and 9 backups. If you decrease this number, Tenable Nessus deletes the old logs.
`file`	Depends on the operating system and log file	yes	The location and name of the log file. If you change the name of a default Tenable Agent log file, some advanced settings may not be able to modify the log settings.
`context`	`true`	not recommended	Enables more context information for logs.
`format`	`system`	not recommended	Determines the format of the output. • `combined` — Presents output in a format used for web server logs. • `system` — Presents output in the default operating system log format.

3. Save the `log.json` file.

4. Restart the agent service.

   The agent updates the log settings.

nessuscli.log

`nessuscli.log` contains a record of CLI events.

Mass Deployment Support

You can automatically configure and deploy agents using environment variables or a configuration JSON file. This allows you to streamline a mass deployment.

When you first launch the agent after installation, the agent first checks for the presence of environment variables, then checks for the `config.json` file. When the agent launches for the first time, the agent uses that information to link to a manager and set preferences.

> **Note:** If you have information in both environment variables and `config.json`, the agent uses both sources of information. If there is conflicting information (for example, environment variables and `config.json` contain a different linking key), the agent uses the information from the environment variables.

For more information, see:

- Environment Variables
- Deploy Tenable Agent Using JSON

Environment Variables

If you want to configure based on environment variables, you can set the following environment variables in the shell environment that is running in.

When you first launch after installation, first checks for the presence of environment variables, then checks for the `config.json` file.

Linking Configuration

Use the following environment variables for linking configuration:

- `NCONF_LINK_HOST` - The hostname or IP address of the manager you want to link to. To link to Tenable Vulnerability Management, use cloud.tenable.com.
- `NCONF_LINK_PORT` - Port of the manager you want to link to.
- `NCONF_LINK_NAME` - Name of the to use when linking.
- `NCONF_LINK_KEY` - Linking key of the manager you want to link to.
- `NCONF_LINK_CERT` - (Optional) CA certificate to use to validate the connection to the manager.
- `NCONF_LINK_RETRY` - (Optional) Number of times should retry linking.
- `NCONF_LINK_GROUPS` - (Optional) One or more existing agent groups where you want to add the agent. If you do not specify an agent group during the install process, you can add your linked agent to an agent group later in Tenable Nessus Manager or Tenable Vulnerability Management. List multiple groups in a comma-separated list. If any group names have spaces, use quotes around the whole list. For example: `"Atlanta,Global Headquarters"`

Deploy Tenable Agent Using JSON

When you first launch the agent after installation, the agent first checks for the presence of environment variables, then checks for the `config.json` file. When the agent launches for the first time, the agent uses that information to link to a manager and set preferences.

To deploy Tenable Agent with the config.json file:

1. Configure the `config.json` file.

   > **Note:**`config.json` must be in ASCII format. Some tools, such as PowerShell, create test files in other formats by default.

   > **Note:** All sections are optional; if you do not include a section, it is not configured when you first launch Tenable Agent. You can manually configure the settings later.

   The `link` section sets preferences to link the agent to a manager.

   > **Tip:** Specifying the `link` preferences in `config.json` and leaving the `retry` preference blank achieves the same result as using the `--install-offline` linking argument in the `nessuscli`. Doing

so installs Tenable Agent on the specified host, even if it is offline. The agent then indefinitely tries to link to the host, given that you did not specify a `retry` value.

Setting	Description
`name`	(Optional) A name for the scanner. A name for your agent. If you do not specify a name for your agent, the name defaults to the name of the computer where you are installing the agent.
`host`	The hostname or IP address of the manager you want to link to. To link to Tenable Vulnerability Management, use cloud.tenable.com.
`port`	The port for the manager you want to link to. For Tenable Nessus Manager: 8834 or your custom port. For Tenable Vulnerability Management: 443
`key`	The linking key that you retrieved from the manager.
`network`	(Optional, Tenable Vulnerability Management-linked agents only) The custom network you want to link to. If you do not specify a network, the agent belongs to the default network.
`ms_cert`	(Optional) A custom CA certificate to use to validate the manager's server certificate.
`groups`	(Optional) One or more existing scanner groups where you want to add

Setting	Description
	the scanner. List multiple groups in a comma-separated list. If any group names have spaces, use quotes around the whole list. For example: `"Atlanta,Global Headquarters"` One or more existing agent groups where you want to add the agent. If you do not specify an agent group during the install process, you can add your linked agent to an agent group later in Tenable Nessus Manager or Tenable Vulnerability Management. List multiple groups in a comma-separated list. If any group names have spaces, use quotes around the whole list. For example: `"Atlanta,Global Headquarters"` **Note:** The agent group name is case-sensitive and must match exactly. You must encase the agent group name in quotation marks (for example, `--groups="My Group"`).
`retry`	(Optional) The number of times the agent attempts to link to the manager if it fails the first attempt. If you do not include the `retry` preference, the agent attempts to link indefinitely. **Note:** If you set `retry` to 1, the agent tries to link to the manager 30 seconds after the initial failure. Every proceeding retry occurs twice as long after the prior retry. For example, if you set `retry` to 5, the agent attempts to link 30 seconds after the first failure, 60 seconds after the second failure, 120 seconds after the third failure, 240 seconds after the fourth failure, and 480 seconds after the fifth failure.

Setting	Description
`proxy`	(Optional) If you are using a proxy server, include the following: • `proxy`: The hostname or IP address of your proxy server. • `proxy_port:`The port number of the proxy server. • `auto_proxy` (Windows only): If enabled, the agent uses Web Proxy Auto Discovery (WPAD) to obtain a Proxy Auto Config (PAC) file for proxy settings. This setting overrides all other proxy configuration preferences. If disabled, the agent defaults to the remaining proxy settings. **Note:** If you include `auto_proxy` in your configuration file, you must also provide the `proxy` and `proxy_port` parameters. • `proxy_username`: The name of a user account that has permissions to access and use the proxy server. • `proxy_password`: The password of the user account that you specified as the username. • `user_agent`: The user agent name, if your proxy requires a preset user agent. • `proxy_auth`: The authentication method to use for the proxy.
`profile_uuid`	(Optional) The UUID of the agent profile that you want to assign the agent to (for example, `12345678-9abc-4ef0-9234-56789abcdef0`). For more information, see Agent Profiles in

Setting	Description
	the *Tenable Vulnerability Management User Guide*.

The `preferences` section configures any advanced settings. For more information, see Advanced Settings.

The following is an example of the `config.json` file format:

```
{
        "link": {
                "name": "sensor name",
                "host": "hostname or IP address",
                "port": 443,
                "key": "abcdefghijklmnopqrstuvwxyz",
                "ms_cert": "CA certificate for linking",
                "retry": 1,
                "proxy": {
                        "proxy": "proxyhostname",
                        "proxy_port": 443,
                        "proxy_username": "proxyusername",
                        "proxy_password": "proxypassword",
                        "user_agent": "proxyagent",
                        "proxy_auth": "NONE"
                }
        },
        "preferences": {
                "global.max_hosts": "500"
        }
}
```

The following is an example of `config.json` when using `auto_proxy`:

```
{
        "link": {
                "name": "sensor name",
                "host": "hostname or IP address",
                "port": 443,
                "key": "abcdefghijklmnopqrstuvwxyz",
                "ms_cert": "CA certificate for linking",
                "retry": 1,
                "proxy": {
                        "proxy": "proxyhostname",
                        "proxy_port": 443,
                        "auto_proxy": "true"
                }
        }
}
```

2. Download the Tenable Agent installation package for your operating system.

3. (Windows only) Before you install the package, you must modify the package so that the agent does not start automatically after installation. This is because the agent must read the `config.json` file when you start the agent service for the first time.

   To modify the package, run the following command:

   ```
   msiexec /i <agent  package>.msi NESSUS_SERVICE_AUTOSTART=false /qn
   ```

4. Install Tenable Agent. For more information, see Install a Tenable Agent on Windows , Install a Tenable Agent on macOS, or Install a Tenable Agent on Linux.

5. (macOS only) Unlike Windows, there is no way to turn off autostart before installing Tenable Agent. Therefore, you need to reset the Tenable Agent to a fresh state before adding `config.json` and starting the agent service.

   To return Tenable Agent to a fresh state on macOS, validate `config.json`, and place `config.json` in the correct directory, run the following command:

   ```
   /Library/NessusAgent/run/sbin/nessuscli prepare-image --json=<path to json file>
   ```

   > **Note:** Tenable Agent autostart is disabled by default in Linux packages. Therefore, if you are using Linux, you can ignore steps 3 and 5.

6. Place config.json in the Tenable Agent directory if it is not already there:

Operating System	config.json Directory
Windows	`C:\ProgramData\Tenable\Nessus Agent\nessus\config.json`
Linux	`/opt/nessus_agent/var/nessus/config.json`
macOS	`/Library/NessusAgent/run/var/nessus/config.json`

7. Start the agent service.

8. Depending on your operating system, run the following command to verify the `config.json` preferences:

Operating System	Command
Windows	`"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" fix --secure --list`
Linux	`/opt/nessus_agent/sbin/nessuscli fix --secure --list`
macOS	`/Library/NessusAgent/run/sbin/nessuscli fix --secure --list`

Once you verify that the preferences were successfully applied, the linking process is complete.

Tenable Agent Cheatsheet

Benefits

- Provides extended scan coverage and continuous security:
  - Can deploy where it's not practical or possible to run network-based scans.
  - Can assess off-network assets and endpoints that intermittently connect to the internet (such as laptops). Tenable Agents can scan the devices regardless of network location and report results back to the manager.

- Eliminates the need for credential management:
    - Does not require host credentials to run, so you don't need to update credentials manually in scan configurations when credentials change, or share credentials among administrators, scanning teams, or organizations.
    - Can deploy where remote credentialed access is undesirable, such as Domain Controllers, DMZs, or Certificate Authority (CA) networks.
- Efficient:
    - Can reduce your overall network scanning overhead.
    - Relies on local host resources, where performance overhead is minimal.
    - Reduces network bandwidth need, which is important for remote facilities connected by slow networks.
    - Removes the challenge of scanning systems over segmented or complex networks.
    - Minimizes maintenance, because Tenable Agents can update automatically without a reboot or end-user interaction.
    - Large-scale concurrent agent scans can run with little network impact.
- Easy deployment and installation:
    - You can install and operate Tenable Agents on all major operating systems.
    - You can install Tenable Agents anywhere, including transient endpoints like laptops.
    - You can deploy Tenable Agents using software management systems such as Microsoft’s System Center Configuration Manager (SCCM).

Limitations

- Network checks — Agents are not designed to perform network checks, so certain plugin items cannot be checked or obtained if you deploy only agent scans. Combining network scans with agent-based scanning eliminates this gap.
- Remote connectivity — Agents miss things that can only specifically be performed through remote connectivity, such as logging into a DB server, trying default credentials (brute force), traffic-related enumeration, etc.

System Requirements for Tenable Agents

For dataflow and licensing requirements, refer to Port Requirements and Licensing Requirements. To view the Tenable Agent software requirements, see Tenable Agent Software Requirements.

Hardware Requirements

Tenable Agents are lightweight and only use minimal system resources. Generally, a Tenable Agent uses 50 to 60 MB of RAM (all pageable). A Tenable Agent uses almost no CPU while idle, but is designed to use up to 100% of the CPU when available during jobs.

For more information on Tenable Agent resource usage, refer to Software Footprint.

The following table outlines the minimum recommended hardware for operating a Tenable Agent. Tenable Agents can be installed on a virtual machine that meets the same requirements specified.

Hardware	Minimum Requirement
Processor	1 dual-core CPU
Processor Speed	> 1 GHz
RAM	> 1 GB
Disk Space	> 3 GB, not including space used by the host operating system The agent may require more space during certain processes, such as applying a plugin update. The selected scan frequency, volume of findings, and log rotation options impact agent disk utilization. If disk space is a chief concern in your deployment scenario, Tenable recommends allocating up to 4 GB (not including space used by the host operating system).
Disk Speed	15-50 IOPS

Install and Link Tenable Agents

The following installation instructions are for the command line. To install using the user interface, see Install a Tenable Agent on Windows or Install a Tenable Agent on macOS.

Linux

1. Install the package:

   - Red Hat and Oracle Linux

     ```
     # dnf install NessusAgent-<version number>-es8.x86_64.rpm
     ```

   - Fedora

     ```
     # dnf install NessusAgent-<version number>-fc34.x86_64.rpm
     ```

   - Ubuntu

     ```
     # dpkg -i NessusAgent-<version number>-ubuntu1110_i386.deb
     ```

   - Debian

     ```
     # dpkg -i NessusAgent-<version number>-debian6_amd64.deb
     ```

   > **Note:** After installing an agent, you must start the service manually by running the **`/sbin/service nessusagent start`** command.

2. Link the agent to Tenable Nessus Manager or Tenable Vulnerability Management:

   At the command prompt, use the `nessuscli agent link` command. For example:

   ```
   /opt/nessus_agent/sbin/nessuscli agent link
   --key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
   --name=MyOSXAgent --groups="All" --host=yourcompany.com --port=8834
   ```

   > **Note:** You must copy and paste the entire link command on the same line. Otherwise, you receive an error.

Windows

You can deploy and link Tenable Agents via the command line. For example:

```
msiexec /i NessusAgent-<version number>-x64.msi NESSUS_GROUPS="Agent Group Name"
NESSUS_SERVER="192.168.0.1:8834" NESSUS_
KEY=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00 /qn
```

macOS

1. Install the package:

   a. Extract `Install Nessus Agent.pkg` and `.NessusAgent.pkg` from `NessusAgent-<version number>.dmg`.

   > **Note:** The `.NessusAgent.pkg` file is normally invisible in the macOS Finder.

   b. Open Terminal.

   c. At the command prompt, enter the following command:

   ```
   # sudo installer -pkg /<path-to>/Install Nessus Agent.pkg -target /
   ```

2. Link the agent to Tenable Nessus Manager or Tenable Vulnerability Management:

   a. Open Terminal.

   b. At the command prompt, use the `nessuscli agent link` command.

   For example:

   ```
   # sudo /Library/NessusAgent/run/sbin/nessuscli agent link
   --key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
   --name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
   ```

Tenable Agent CLI Commands

Use the Agent `nessuscli` utility to perform some Tenable Agent functions through a command line interface.

> **Note:** You must run all Agent `nessuscli` commands as a user with administrative privileges.

Nessuscli Syntax

Operating System	Command
Windows	`C:\Program Files\Tenable\Nessus Agent\nessuscli.exe`

Operating System	Command
	`<cmd> <arg1> <arg2>`
macOS	`# sudo /Library/NessusAgent/run/sbin/nessuscli <cmd> <arg1> <arg2>`
Linux	`# /opt/nessus_agent/sbin/nessuscli <cmd> <arg1> <arg2>`

Nessuscli Commands

Command	Description
Informational Commands	
`# nessuscli help`	Shows a list of `nessuscli` commands.
`# nessuscli -v`	Shows your current version of Tenable Agent.
`# nessuscli fix --get` *`<agent setting>`*	Shows the current value of an agent setting.
Bug Reporting Commands	
`# nessuscli bug-report-generator`	Generates an archive of system diagnostics. If you run this command without arguments, the utility prompts you for values. **Optional arguments:** • `--quiet` — Run the bug report generator without prompting user for feedback. • `--scrub` — The bug report generator sanitizes the last two octets of the IPv4 address. • `--full` — The bug report generator collects extra data.

Command	Description
Image Preparation Commands	
`# nessuscli prepare-image`	Performs pre-imaging cleanup, including the following: • Unlinks the agent, if linked. • Deletes any host tag on the agent. For example, the registry key on Windows or `tenable_tag` on Unix. • Deletes any UUID file on the agent. For example, `/opt/nessus/var/nessus/uuid` (or equivalent on MacOS/Windows). • Deletes `plugin dbs`. • Deletes `global db`. • Deletes `master.key`. • Deletes the backups directory. **Optional arguments:** • `--json=<file>` — Validates an auto-configuration `.json` file and places it in the appropriate directory.
Local Agent Commands Used to link, unlink, and display agent status	
`# nessuscli agent link --key=<key> --host=<host> --port=<port>`	Using the Tenable Agent Linking Key, this command links the agent to the Tenable Nessus Manager or Tenable Vulnerability Management. **Required arguments:**

Command	Description
	• `--key` — The linking key that you retrieved from the manager. • `--host` — To link to Tenable Nessus Manager: The static IP address or hostname you set during the Tenable Nessus Manager installation. To link to Tenable Vulnerability Management: `sensor.cloud.tenable.com` (for Tenable Agents 8.0.x and earlier, `cloud.tenable.com`) **Note:** Starting with Tenable Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using `sensor.cloud.tenable.com`. If agents are unable to connect to `sensor.cloud.tenable.com`, they use `cloud.tenable.com` instead. Agents with earlier versions continue to use the `cloud.tenable.com` domain. • `--port` — To link to Tenable Nessus Manager, use 8834 or your custom port. To link to Tenable Vulnerability Management, use 443. **Tenable Vulnerability Management arguments:** • `--cloud`— To link to Tenable Vulnerability Management, pass the argument `--cloud`. The `--cloud` argument is a shortcut to

Command	Description
	specifying --host=sensor.cloud.tenable.com --port=443. If you use --cloud, you do not need to set --host and --port. **Caution:** The --cloud argument is not supported in FedRAMP environments. You must specify --host=fedcloud.tenable.com --port=443. **Note:** If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com. **Optional arguments:** • --auto-proxy — (Windows-only) When set, the agent uses Web Proxy Auto Discovery (WPAD) to obtain a Proxy Auto Config (PAC) file for proxy settings. This setting overrides all other proxy configuration preferences. • --name — A name for your agent. If you do not specify a name for your agent, the name defaults to the name of the computer where you are installing the agent. • --groups — One or more existing agent

Command	Description
	groups where you want to add the agent. If you do not specify an agent group during the install process, you can add your linked agent to an agent group later in Tenable Nessus Manager or Tenable Vulnerability Management. List multiple groups in a comma-separated list. If any group names have spaces, use quotes around the whole list. For example: `"Atlanta,Global Headquarters"` **Note:** The agent group name is case-sensitive and must match exactly. You must encase the agent group name in quotation marks (for example, `--groups="My Group"`). - `--ca-path` — A custom CA certificate to use to validate the manager's server certificate. - `--offline-install` — When enabled, installs Tenable Agent on the system, even if it is offline. Tenable Agent periodically attempts to link itself to its manager. If the agent cannot connect to the controller, it retries every hour. If the agent can connect to the controller but the link fails, it retries every 24 hours. **Tip:** Specifying the `link` preferences in `config.json` and leaving the `retry` preference blank achieves the same

Command	Description
	result as using the `--install-offline` linking argument. • `--network` — For Tenable Vulnerability Management-linked agents, adds the agent to a custom network. If you do not specify a network, the agent belongs to the default network. • `--profile-uuid` — The UUID of the agent profile that you want to assign the agent to (for example, `12345678-9abc-4ef0-9234-56789abcdef0`). For more information, see Agent Profiles in the *Tenable Vulnerability Management User Guide*. • `--proxy-host` — The hostname or IP address of your proxy server. • `--proxy-port` — The port number of the proxy server. • `--proxy-password` — The password of the user account that you specified as the username. • `--proxy-username` — The name of a user account that has permissions to access and use the proxy server. • `--proxy-agent` — The user agent name, if your proxy requires a preset user agent.
`# nessuscli agent relink --host=<new_host> --`	Relinks the linked agent from Tenable Vulnerability Management to Tenable Sensor

Command	Description
`port=<new_port>`	Proxy, or vice versa. **Note:** This command is not supported for agents connected to Tenable Nessus Manager.
`# nessuscli agent unlink`	Unlinks the agent from Tenable Nessus Manager or Tenable Vulnerability Management. **Optional arguments:** • `--force` — Forces the agent to unlink from Tenable Nessus Manager or Tenable Vulnerability Management, even if the agent cannot communicate with the manager. Tenable recommends using this flag for unlinking an agent that is unable to communicate with Tenable Nessus Manager or Tenable Vulnerability Management. If you use the `--force` flag, you may also have to unlink the agent in Tenable Nessus Manager or Tenable Vulnerability Management.
`# nessuscli scan-triggers --list`	Lists details about the agent's rule-based scans: • Scan name • Status (for example, **uploaded**) • Time of last activity (shown next to the status) • Scan description • Time of last policy modification

Command	Description
	- Time of last run - Scan triggers - Scan configuration template - Command to launch the scan (`nessuscli scan-triggers --start --UUID=<scan-uuid>`)
`# nessuscli scan-triggers --start --UUID=<scan-uuid>`	(Tenable Vulnerability Management-linked agents only) Manually executes a rule-based scan based on UUID.
`# nessuscli agent status`	Displays the status of the agent, rule-based scanning information, jobs pending, and whether the agent is linked to the server. The command output provides some of the following information: - Running — Indicates whether the agent is currently active on the host. - Linked to — Indicates which manager the agent is linked to. - Link status — Indicates the agent's current link status with the manager. - Proxy — Indicates the proxy the agent is connected through, if any. - Plugin set — Indicates the agent's current plugin set. - Scanning — Indicates whether the agent is currently scanning the host. This

Command	Description
	value also shows the number of scan jobs pending and the number of scan triggers configured for the agent (this value is labeled **smart scan configs** in the output). • Scans run today — Indicates the number of scans the agent has run today. • Last scanned — Indicates the last date and time at which the agent ran a scan. • Last connect — Indicates the last date and time at which the agent connected to its manager. • Last connection attempt — Indicates the last date and time at which the agent attempted to connect with its manager. **Optional arguments:** • `--local` — (Default behavior) Provides the status, current jobs count, and jobs pending. This option prevents the agent from contacting its management software to fetch the status. Instead, it shows the last known information from its most recent sync. • `--remote` — Fetches the job count from the manager and displays the status. **Note:** Tenable does not recommend running frequent status checks with the `--remote` option (for example, when using automation).

Command	Description
	• `--offline` — Provides the most recently cached agent status when it cannot connect to Tenable Nessus Manager or Tenable Vulnerability Management. • `--show-token` — Displays the agent's token that is used to identify and authenticate with its manager. • `--show-uuid` — Displays the agent's Tenable UUID.
`# nessuscli plugins --info`	Lists details about the agent's `full` and `inventory` plugin sets: • `Installed version` • `Last downloaded` • `Last needed` • `Expires in` — The plugin set's expiration time and date (that is, when the plugin set is no longer needed). • `Plugins` — The total number of plugins in the plugin set. • `Uncompressed source size` Lists details and statistics about the agent's plugins, such as: • `Last plugin update time` • `Last plugin update check time` • `Total compressed plugins source size`

Command	Description
	• `Total compiled plugins size` • `Total plugins attributes data` • `Total plugin size on disk`
`# nessuscli plugins --reset`	Deletes all plugins and plugin-related data off the disk. The agent is able to download plugins immediately after the deletion completes. **Note:** This command only triggers if the agent has plugin data on its disk.
`# nessuscli profile --show`	Retrieves information about the Tenable Vulnerability Management agent profile that the agent is assigned to, if applicable.
`# nessuscli install-relay --linking-key=`*`<Tenable Identity Exposure relay linking key>`*	Installs a Tenable Identity Exposure Secure Relay on the agent. To retrieve the Tenable Identity Exposure relay linking key, see Secure Relay in the *Tenable Identity Exposure Administrator Guide*. `install-relay` supports the following optional parameters: • `proxy_address` — The proxy IP or DNS to use if you require a proxy to reach Tenable domains. If you enter a `proxy_address`, you need to enter a `proxy_port`. • `proxy_port` — The proxy port to use if you require a proxy to reach Tenable domains. If you enter a `proxy_port`,

Command	Description
	you need to enter a `proxy_address`. • `proxy_basic_login` — The proxy login username. If you enter a `proxy_basic_login`, you need to enter a `proxy-basic-password`. • `proxy-basic-password` — The proxy login password. If you enter a `proxy-basic-password`, you need to enter a `proxy_basic_login`. If you do not want to specify a proxy, do not enter any proxy parameters. To specify an unauthorized proxy, enter a `proxy_address` and a `proxy_port`. To specify an authorized proxy, enter a `proxy_address`, a `proxy_port`, a `proxy_basic_login`, and a `proxy-basic-password`.
Update Commands	
`# nessuscli agent update --file=<plugins_set.tgz>`	Manually installs a plugin set.
Fix Commands	
`# nessuscli fix --list`	Shows a list of agent settings and their values.
`nessuscli fix --set <setting>=<value>`	Set an agent setting to the specified value. For a list of agent settings, see Advanced Settings.
`# nessuscli fix --set update_hostname="<value>"`	Updates agent hostnames automatically in Tenable Vulnerability Management or Tenable Nessus Manager.

Command	Description
	You can set the `update_hostname` parameter to `yes` or `no`. By default, this preference is disabled. **Note:** Restart the agent service for the change to take effect in Tenable Nessus Manager.
`# nessuscli fix --set agent_update_channel=<value>`	(Tenable Vulnerability Management-linked agents only) Sets the agent update plan to determine what version the agent automatically updates to. Values: • **`ga`** — Automatically updates to the latest Agent version when it is made generally available (GA). **Note:** This date is usually *one week after* the version is made generally available. For versions that address critical security issues, Tenable may make the version available immediately. • **`ea`** — Automatically updates to the latest Agent version as soon as it is released for Early Access (EA), typically a few weeks before general availability. • **`stable`** — Does not automatically update to the latest Tenable Agent version. Remains on an earlier version of Tenable Agent set by Tenable, usually one release older than the current generally available version, but no earlier than 7.7.0. When Tenable Agent

Command	Description
	releases a new version, your agent updates software versions, but stays on a version prior to the latest release. **Note:** For agents linked to Tenable Vulnerability Management, you need to run the `agent_update_channel` command from the agent `nessuscli` utility. For agents linked to Tenable Nessus Manager, you need to run the `agent_update_channel` command from the Tenable Nessus Manager`nessuscli` utility.
`# nessuscli fix --set maximum_scans_per_day=<value>`	(Tenable Vulnerability Management-linked agents only) Sets the maximum number of scans an agent can run per day. The minimum amount is **1**, the maximum amount is **48**, and the default amount is **10**.
`# nessuscli fix --set max_retries="`*`<value>`*`"`	Sets the maximum number of times an agent should retry in the event of a failure when executing the `agent link`, `agent status`, or `agent unlink` commands. The commands retry, the specified number of times, consecutively, sleeping increasing increments of time set by `retry_sleep_milliseconds` between attempts. The default value for `max_retries` is 0. The minimum value is 0, and the maximum value is 10. For example, if you set `max_retries` to 4 and set `retry_sleep_milliseconds` to the default of 1500, then the agent will sleep for 1.5 seconds after the first try, 3 seconds after

Command	Description
	the second try, and 4.5 seconds after the third try. **Note:** This setting does not affect offline updates or the agent's normal 24 hour check-in after it is linked.
`# nessuscli fix --set retry_sleep_milliseconds="<value>"`	Sets the number of milliseconds that an agent sleeps for between retries in event of a failure when executing the `agent link`, `agent status`, or `agent unlink` commands. The default is 1500 milliseconds (1.5 seconds).
`# nessuscli fix --set niap_mode=enforcing`	Enforces NIAP mode for Tenable Agent. For more information about NIAP mode, see Configure Tenable Agent for NIAP Compliance.
`# nessuscli fix --set niap_mode=non-enforcing`	Disables NIAP mode for Tenable Agent. For more information about NIAP mode, see Configure Tenable Agent for NIAP Compliance.
`# nessuscli fix --set fips_mode=enforcing`	Enforces the current validated FIPS module for Tenable Agent communication and database encryption. The FIPS module does not affect scanning encryption. **Note:** Tenable Agent also enforces the FIPS module when you enforce NIAP mode. For more information, see Configure Tenable Agent for NIAP Compliance.
`# nessuscli fix --set fips_mode=non-enforcing`	Disables the FIPS module for Tenable Agent communication and database encryption.

Command	Description
	Note: Tenable Agent also disables the FIPS module when you disable NIAP mode. For more information, see Configure Tenable Agent for NIAP Compliance.
Fix Secure Settings	
`nessuscli fix`	You can use `--list`, `--set`, `--get`, and `--delete` to modify or view advanced agent settings. Using the `--secure` option acts on the encrypted preferences, which contain information about registration. **Caution:** Tenable does not recommend changing undocumented `--secure` settings as it may result in an unsupported configuration. For a list of agent settings, see Advanced Settings.
`nessuscli fix [--secure] --list`	
`nessuscli fix [--secure] --set <setting=value>`	
`nessuscli fix [--secure] --get <setting>`	
`nessuscli fix [--secure] --delete <setting>`	
`# nessuscli fix --secure --get agent_linking_key`	(Tenable Nessus Manager versions 10.4.0 and later only) Retrieve your unique agent linking key. **Note**: You can only use this linking key to link an agent. You cannot use it to link a scanner or a child node.
Resource Control Commands	

`# nessuscli fix --set process_priority="<value>"`
`# nessuscli fix --get process_priority`
	Commands
	Set, get, or delete the `process_priority` setting.
	You can control the priority of the Tenable Agent relative to the priority of other tasks

Command	Description
`# nessuscli fix --delete process_priority`	running on the system by using the `process_priority` preference. For valid values and more information on how the setting works, see Agent CPU Resource Control.

Tenable Nessus Service

If necessary, whenever possible, Nessus services should be started and stopped using Nessus service controls in the operating system's interface.

However, there are many **`nessus-service`** functions that can be performed through a command line interface.

Unless otherwise specified, the **`nessusd`** command can be used interchangeably with **`nessus-service`** server commands.

The **`# killall nessusd`** command is used to stop all Nessus services and in-process scans.

Note: All commands must be run by a user with administrative privileges.

Nessus-Service Syntax

Operating System	Command
Linux	# /opt/nessus_agent/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]
macOS	# /Library/NessusAgent/run/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]

Suppress Command Output Examples

You can suppress command output by using the **`-q`** option.

Linux

```
# /opt/nessus_agent/sbin/nessus-service -q -D
```

Nessusd Commands

Option	Description
-c <config-file>	When starting the nessusd server, this option is used to specify the server-side nessusd configuration file to use. It allows for the use of an alternate configuration file instead of the standard db.
-S <ip [,ip2,...]>	When starting the nessusd server, force the source IP of the connections established by Nessus during scanning to <ip>. This option is only useful if you have a multihomed machine with multiple public IP addresses that you would like to use instead of the default one. For this setup to work, the host running nessusd must have multiple NICs with these IP addresses set.
-D	When starting the nessusd server, this option forces the server to run in the background (daemon mode).
-v	Display the version number and exit.
-l	Display a list of those third-party software licenses.
-h	Show a summary of the commands and exit.
--ipv4-only	Only listen on IPv4 socket.
--ipv6-only	Only listen on IPv6 socket.
-q	Operate in "quiet" mode, suppressing all messages to stdout.
-R	Force a re-processing of the plugins.
-t	Check the time stamp of each plugin when starting up to only compile newly updated plugins.
-K	Set a master password for the scanner. If a master password is set, Nessus encrypts all policies and credentials contained in the policy. When a password is set, the Nessus UI prompts you for

Option	Description
	the password. If your master password is set and then lost, it cannot be recovered by your administrator nor Tenable Support.

Notes

If you are running nessusd on a gateway and if you do not want people on the outside to connect to your nessusd, set your `listen_address` advanced setting.

To set this setting:

```
nessuscli fix --set listen_address=<IP address>
```

This setting tells the server to only listen to connections on the address *`<address>`* that is an IP address, not a machine name.

Plugin Updates

Before any plugin updates occur, Tenable Agent performs an initial plugin download from its linked manager (Tenable Vulnerability Management or Tenable Nessus Manager).

- **Tenable Nessus Manager** — The agent performs the initial plugin download upon successfully linking to Tenable Nessus Manager.
- **Tenable Vulnerability Management** — The agent performs the initial plugin download when the agent receives its first scan job or when you assign the agent a triggered scan.

After the initial plugin download, Tenable Agent keeps its plugin set current by checking its linked manager (Tenable Vulnerability Management or Tenable Nessus Manager) for updates. The agent checks for plugin updates no less than every 24 hours since the previous update.

Differential vs. Full Updates

When the agent successfully checks in with the manager, it performs either a differential or a full update depending on the linked manager and the age of the current plugin set.

Linked Manager	Differential Update	Full Update
Tenable Vulnerability Management	The agent performs a differential update when any of the agent plugin sets are 15 days or less behind the Tenable Vulnerability Management plugin sets.	The agent performs a full plugin update at scan time for any required plugin set if the agent does not have any plugins for that plugin set. For this reason, when you perform an agent vulnerability or inventory collection scan for the first time, expect the scan to use more bandwidth than the subsequent vulnerability or inventory scans. The agent also performs a full plugin update when any of the agent plugin sets are more than 15 days behind the Tenable Vulnerability Management plugin sets. The agent deletes unused plugin sets after a configurable amount of time (for more information, see the `days_to_keep_unused_plugins` advanced setting). After the amount of time passes, the agent deletes the unused plugin sets.
Tenable Nessus Manager	The agent performs a differential plugin update when the agent plugin set is 5 days or less behind the Tenable Nessus Manager plugin set.	The agent performs a full plugin update when the agent plugin set is more than 5 days behind the Tenable Nessus Manager plugin set.

Connectivity and Retry Logic

If the agent attempts to update but cannot connect to the plugin feed (due to network issues or feed availability), it employs an exponential retry strategy:

1. The agent attempts to update.
2. If the connection fails, the agent retries repeatedly over a 24-hour period, increasing the wait time between attempts (for example, 30 seconds, 60 seconds, 90 seconds).
3. If the agent cannot connect after 24 hours of retry attempts, it reverts to checking once every 24 hours.

Safe Mode

Safe mode is a feature that allows Tenable Agent to stay connected to Tenable Vulnerability Management or Tenable Nessus Manager for monitoring and remediation while agents are experiencing plugin compilation, scanning, host memory, and environmental issues.

When agents are in safe mode, they maintain communication with Tenable Vulnerability Management or Tenable Nessus Manager but are blocked from compiling plugins and scanning. This allows your organization to safely and remotely monitor, troubleshoot, and recover your agents. Safe mode is particularly useful for large-scale agent deployments in that you no longer need to manually manage individual agents when they encounter issues.

Safe Mode Activation

An agent automatically enters safe mode when it detects one of the following errors:

- The agent crashes during a scan.
- The agent crashes or hangs during plugin compilation or in response to plugin set changes.
- The agent becomes unusable due to failed plugin updates.
- The agent becomes unusable due to a bug.
- The agent is repeatedly terminated due to host memory issues.
- The agent is repeatedly terminated by antivirus or endpoint security software.

The agent then informs its manager that it has activated safe mode, and you are notified in Tenable Vulnerability Management or Tenable Nessus Manager via the agent user interface. The agent maintains connection with the manager to be monitored and accept plugin commands from a user, but it is otherwise blocked from scheduled plugin tasks and scanning.

Remediate and Recover Agents in Safe Mode

To remediate and recover agents that are in safe mode, you can report agents that are in safe mode on connect.tenable.com for Tenable Support assistance, or you can use the **Linked Agents** menu to self-remediate.

Note: Tenable strongly recommends submitting a support ticket when one or more agents go into safe mode. Do this *before* attempting one of the following remediation actions and make sure to include a debug file for one of the agents that has entered safe mode. Doing so allows Tenable Support to identify the root cause of the issue and plan any fixes. Without a debug file, the root cause of the issue will remain unknown and unable to be addressed.

Caution: If you choose to self-remediate without assistance from Tenable, Tenable highly recommends trying remediation methods on small subset of your agents before attempting them on large groups or all of your agents.

For more information about responding to agents in safe mode, see the **Agent Safe Mode** topics in the *Tenable Vulnerability Management* and *Tenable Nessus User Guides*.