Tenable Nessus 10.11.x User Guide

Last Updated: November 20, 2025

Table of Contents

Welcome to Tenable Nessus 10.11.x

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

Tenable Nessus Solutions

Tenable Nessus Essentials

Tenable Nessus Essentials provides a starting point for hobby practitioners to scan their home networks and learn vulnerability assessment. This free tier features high-speed asset discovery and vulnerability scanning for up to give IP addresses with a 30-day delayed plugin feed.

For students, educators, and individuals seeking more advanced capabilities, Tenable Nessus Essentials Plus increases the target limit to 20 IP addresses, provides real-time plugin feed updates, and enables PDF reporting and concurrent scans.

Tenable Nessus Professional

Tenable Nessus Professional, the industry's most widely deployed vulnerability assessment solution helps you reduce your organization's attack surface and ensure compliance. Tenable Nessus features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery, and more.

Tenable Nessus supports more technologies than competitive solutions, scanning operating systems, network devices, hypervisors, databases, web servers, and critical infrastructure for vulnerabilities, threats, and compliance violations.

With the world's largest continuously updated library of vulnerability and configuration checks, and the support of Tenable, Inc.'s expert vulnerability research team, Tenable Nessus sets the standard for vulnerability scanning speed and accuracy.

Tenable Nessus Professional Product Page

Tenable Nessus Expert

Tenable Nessus Expert combines the industry's most widely deployed vulnerability assessment solution with new features and functionality that are specifically engineered to address the

extended modern attack surface. With Nessus Expert you can not only reduce your organization's IP-based attack surface and ensure compliance, but also identify vulnerabilities and policy violations in Infrastructure as Code (IaC) and identify previously unknown internet-facing assets.

Tenable Nessus Expert supports more technologies than competitive solutions, scanning operating systems, network devices, IaC repositories, hypervisors, databases, web servers, and critical infrastructure for vulnerabilities, threats, and compliance violations.

With the world's largest continuously updated library of vulnerability and configuration checks, and the support of Tenable's expert vulnerability research team, Tenable Nessus Expert sets the standard for vulnerability scanning speed, accuracy, and is the only tool designed to address today's modern attack surface.

Nessus Expert Product Page

Tenable Nessus Manager

> **Note:** Tenable Nessus Manager is no longer sold as of February 1, 2018. For existing standalone Tenable Nessus Manager customers, Tenable continues to provide service through the duration of your contract. Tenable continues to support and provision Tenable Nessus Manager for the purpose of managing agents.

Nessus Manager combines the powerful detection, scanning, and auditing features of Nessus, the world's most widely deployed vulnerability scanner, with extensive management and collaboration functions to reduce your attack surface.

Nessus Manager enables the sharing of resources including Nessus scanners, scan schedules, policies, and scan results among multiple users or groups. Users can engage and share resources and responsibilities with their co-workers; system owners, internal auditors, risk and compliance personnel, IT administrators, network admins, and security analysts. These collaborative features reduce the time and cost of security scanning and compliance auditing by streamlining scanning, malware and misconfiguration discovery, and remediation.

Nessus Manager protects physical, virtual, mobile, and cloud environments. Nessus Manager is available for on-premises deployment or from the cloud, as Tenable Vulnerability Management. Nessus Manager supports the widest range of systems, devices and assets, and with both agent-less and Tenable Agent deployment options, easily extends to mobile, transient, and other hard-to-reach environments.

Tenable Agent

For Tenable Agent documentation, see the Tenable Agent User Guide.

Tenable Agents, available with Tenable Vulnerability Management and Nessus Manager, increase scan flexibility by making it easy to scan assets without needing ongoing host credentials or assets that are offline, and enable large-scale concurrent scanning with little network impact.

Tenable Agents are lightweight, low-footprint 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 without using credentials, and offline assets and endpoints that intermittently connect to the internet. 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 consistently collect information about your organization's security posture. Network scanning typically occurs at selected intervals or during designated windows and requires systems to be accessible when a scan is executed. If laptops or other transient devices are not accessible when a scan is executed, they are excluded from the scan, leaving you blind to vulnerabilities on those devices. Tenable Agents help reduce your organization’s attack surface by scanning assets that are off the network or powered-down during scheduled assessments or by scanning other difficult-to-scan assets.

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 you install them and report results back to the managing product. You can manage Tenable Agents with Tenable Nessus Manager or Tenable Vulnerability Management.

Tenable Agent Product Page

Tenable Vulnerability Management

Tenable Vulnerability Management is a subscription-based license and is available at the Tenable Store.

Tenable Vulnerability Management enables security and audit teams to share multiple Tenable Nessus scanners, scan schedules, scan policies and most importantly scan results among an unlimited set of users or groups.

By making different resources available for sharing among users and groups, Tenable Vulnerability Management allows for endless possibilities for creating highly customized work flows for your vulnerability management program, regardless of locations, complexity, or any of the numerous regulatory or compliance drivers that demand keeping your business secure.

In addition, Tenable Vulnerability Management can control multiple Tenable Nessus scanners, schedule scans, push policies and view scan findings—all from the cloud, enabling the deployment of Nessus scanners throughout your network to multiple physical locations, or even public or private clouds.

The Tenable Vulnerability Management subscription includes:

- Unlimited scanning of your perimeter systems
- Web application audits
- Ability to prepare for security assessments against current PCI standards
- Up to two quarterly report submissions for PCI ASV validation through Tenable, Inc.
- 24/7 access to the Tenable Community site for Tenable Nessus knowledge base and support ticket creation

Tenable Vulnerability Management Product Page

Tenable Vulnerability Management User Manual

System Requirements

You can run Tenable Nessus in the following environments.

Environment	More Information

Tenable Core	Virtual	VMware	Requirements in the *Tenable Core User Guide*
		Microsoft Hyper-V	
	Cloud	Microsoft Azure	
	Hardware		
Other platforms	Virtual	VMware	Hardware Requirements and Software Requirements
	Hardware		Hardware Requirements and Software Requirements

For information about license requirements, see Licensing Requirements.

Hardware Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for Tenable Nessus deployments include raw network speed, the size of the network, and the configuration of Tenable Nessus.

The following recommendations are guidelines for the minimum hardware allocations. Certain types of scans are more resource intensive. If you run complex scans, especially those with credentials, you may require more disk space, memory, and processing power.

Tip: For information on maximizing your scan performance and scan configuration tips, see the Tenable Nessus Scan Tuning Guide.

Note: For Linux environments, the disk space requirements apply to the `/opt` folder.

Note: In addition to the minimum recommended disk spaces listed in the following sections, consider how much additional disk space your organization needs to store Tenable Nessus log files. By default, `nessusd.dump` and `nessusd.messages` can store up to 50 GB of log files each, but you can configure this size to be larger or smaller depending on your organization's needs. For more information, see the `dumpfile_max_files`, `dumpfile_max_size`, `logfile_max_files`, and `logfile_max_size` settings in the *Tenable Nessus User Guide* Advanced Logging Settings.

Tenable Nessus Scanners and Tenable Nessus Professional

The following table lists the hardware requirements for Tenable Nessus scanners and Tenable Nessus Professional.

Scenario	Minimum Recommended Hardware
Scanning up to 50,000 hosts per scan	**CPU** — 4 2GHz cores **Memory** — 4 GB RAM (8 GB RAM recommended) **Disk space** — 30 GB, not including space used by the host operating system **Note:** Your usage (for example, scan results, plugin updates, and logs) increases the amount of disk space needed over time.
Scanning more than 50,000 hosts per scan	**CPU** — 8 2GHz cores **Memory** — 8 GB RAM (16 GB RAM recommended) **Disk space** — 30 GB, not including space used by the host operating system **Note:** Your usage (for example, scan results, plugin updates, and logs) increases the amount of disk space needed over time.

Tenable Nessus Manager

The following table lists the hardware requirements for Tenable Nessus Manager.

Note: To view the hardware requirements for Nessus Manager clustering, see Clustering System Requirements.

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) **+** 500 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 + 500 MB = **39,000 MB** (**39 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 + 500 MB = **11,500 MB** (**11.5 GB**). • Environments without triggered agent scanning — 5 GB per 5,000 agents per concurrent scan **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) **+** 500 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 + 500 MB = **525,500 MB** (**525.5 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 + 500 MB = **150,500 MB** (**150.5 GB**). • Environments without triggered agent scanning — 5 GB per 5,000 agents per concurrent scan **Notes:** • Scan results and plugin updates require more disk space over time. • Engage with your Tenable representative for large deployments.

Tenable Nessus with Web Application Scanning Enabled

The following table lists the hardware requirements for Tenable Nessus Expert with web application scanning enabled and Tenable Nessus scanners with web application scanning enabled in Tenable Security Center:

Hardware	Minimum Requirement
Processor	> 8 2GHz cores
RAM	> 8 GB Tenable recommends using 16 GB RAM for the best results. **Note:** In addition to > 8 GB of system RAM, you must ensure that Docker is configured to deploy with a memory limit of 8 GB or more. For more information, see the Docker documentation.
Disk Space	> 40 GB, not including space used by the host operating system Your overall usage (scan results, plugin updates, logging) increase the amount of disk space needed over time.

Storage Requirements

Tenable recommends a minimum of 5,000 MB of temporary space for the Tenable Nessus scanner to run properly.

Tenable recommends installing Tenable Nessus scanners and Tenable Nessus Manager on direct-attached storage (DAS) devices for non-virtualized hosts. For virtualized hosts, Tenable recommends installing Tenable Nessus Manager on storage area networks (SANs) with a storage latency of 10 milliseconds or less.

Tenable does not support installing Tenable Nessus Manager on network-attached storage (NAS), including network filesystems such as NFS.

> **Note:** Tenable Nessus is a CPU-intensive application. If you deploy Tenable Nessus in a virtualized infrastructure, take care to avoid running Tenable Nessus in a manner in which it may attempt to draw on oversubscribed resources, especially CPU. Refer to your vendor-specific virtualized infrastructure documentation for guidance on optimizing virtual infrastructure resource allocation.

NIC Requirements

Tenable recommends you configure the following, at minimum, to ensure network interface controller (NIC) compatibility with Tenable Nessus:

- Disable NIC teaming or assign a single NIC to Tenable Nessus.
- Disable IPv6 tunneling on the NIC.
- Disable packet capture applications that share a NIC with Tenable Nessus.
- Avoid deploying Tenable Nessus in a Docker container that shares a NIC with another Docker container.

For assistance confirming if other aspects of your NIC configuration are compatible with Tenable Nessus, contact Tenable Support.

Virtual Machines

Tenable Nessus can be installed on a virtual machine that meets the same requirements. If your virtual machine is using Network Address Translation (NAT) to reach the network, many of the Tenable Nessus vulnerability checks, host enumeration, and operating system identification are negatively affected.

> **Note:** Only *one* virtualized Tenable Nessus scanner can be run on any physical host. Tenable Nessus relies on low-level network operations and requires full access to the host's network interface controller (NIC). In a virtualization environment (for example, Hyper-V, Docker), this can cause incorrect scanner behavior, or

ost instability, if more than one virtualized Tenable Nessus scanner attempts to share a single physical NIC.

Note: Tenable Nessus is a CPU-intensive application. If you deploy Tenable Nessus in a virtualized infrastructure, take care to avoid running Tenable Nessus in a manner in which it may attempt to draw on oversubscribed resources, especially CPU. Refer to your vendor-specific virtualized infrastructure documentation for guidance on optimizing virtual infrastructure resource allocation.

Software Requirements

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

Tenable Nessus 10.11

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 2020	x86_64
	Fedora 41 and 42	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64 AArch64
	Raspberry Pi OS	ARMHF
	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	x86
	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
	Windows Server 2012, 2012 R2, 2016, 2019, 2022, and 2025	x86_64

Tenable Nessus 10.10

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 2020	x86_64

	Fedora 41 and 42	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64 AArch64
	Raspberry Pi OS	ARMHF
	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	x86
	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 Nessus 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 2020	x86_64
	Fedora 41 and 42	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64 AArch64
	Raspberry Pi OS	ARMHF
	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	x86
	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 Nessus 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 2020	x86_64
	Fedora 38 and 39	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64 AArch64
	Raspberry Pi OS	ARMHF
	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	x86
	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, 15, and 26	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 Nessus 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 2020	x86_64
	Fedora 38 and 39	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64 AArch64

	Raspberry Pi OS	ARMHF
	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 14.04, 16.04	x86
	Ubuntu 14.04, 16.04, 18.04, 20.04, and 22.04	x86_64
	Ubuntu 18.04	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

Tenable Nessus 10.5

Operating System	Supported Versions	Supported Architecture
Linux	AlmaLinux 9.5	x86_64 AArch64
	Amazon Linux 2	x86_64 AArch64

	CentOS Stream 9	x86_64
	Debian 11	x86_64
	Kali Linux 2020	x86_64
	Fedora 34 and 35	x86_64
	Oracle Linux (including Unbreakable Enterprise Kernel) 7, 8, and 9	x86_64 AArch64
	Raspberry Pi OS	ARMHF
	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 SP1 and later	x86_64
	TencentOS	x86_64
	Ubuntu 14.04, 16.04	x86
	Ubuntu 14.04, 16.04, 18.04, and 20.04	x86_64
	Ubuntu 18.04	AArch64
macOS	macOS 11, 12, and 13	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

Tip: For information about Tenable Core + Nessus, see System Requirements in the Tenable Core User Guide.

Note: Microsoft Visual C++ Redistributable 14.22 is included as part of a bundled license package with Tenable Nessus.

Supported Browsers

Tenable Nessus supports the following browsers:

- Google Chrome (76+)
- Apple Safari (10+)
- Mozilla Firefox (50+)
- Microsoft Edge (102+)

PDF Reports

The Tenable Nessus PDF report generation feature requires the latest version of Oracle Java or OpenJDK.

If your organization requires PDF reports, you must install Oracle Java or OpenJDK before installing Tenable Nessus. If you install Oracle Java or OpenJDK after installing Tenable Nessus, you need to reinstall Tenable Nessus for the PDF report feature to function properly.

SELinux Requirements

Tenable Nessus supports disabled, permissive, and enforcing mode Security-Enhanced Linux (SELinux) policy configurations.

- Disabled and permissive mode policies typically do not require customization to interact with Tenable Nessus.
- Enforcing mode policies require customization to interact with Tenable Nessus. For more information, see Customize SELinux Enforcing Mode Policies.

Note: Tenable recommends testing your SELinux configurations before deploying on a live network.

Customize SELinux Enforcing Mode Policies

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

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

Licensing Requirements

This topic explains how to license Tenable Nessus and lists its features.

Licensing Tenable Nessus

You can manage Tenable Nessus in Tenable Security Center or run it as a a standalone subscription product. To purchase a subscription, go to the Tenable website or work with a Tenable partner.

Tenable Nessus has two versions:

- **Tenable Nessus Professional** — A single subscription price.
- **Tenable Nessus Expert** — A subscription price plus any additional web application scanning or external attack surface scanning (EASM) domains beyond five per quarter.

Plugin Feed Activation Code

Wherever you manage Tenable Nessus, you need a *plugin feed activation code*, which identifies which version you are licensed for—and, if applicable, how many IP addresses you can scan, how many remote scanners you can link, and how many Tenable Agents you can link to Tenable Nessus Manager. Where you enter this code depends on how you manage Tenable Nessus.

- **Tenable Nessus Subscription** — Manage your activation code in Tenable Nessus, as described in Manage Activation Code.

  > **Tip**: To set up Tenable Nessus offline, see Manage Tenable Nessus Offline.

- **Tenable Nessus in Tenable Security Center** — Manage your activation code (and plugin updates) in Tenable Security Center. When you register Tenable Nessus, start it before Tenable Security Center and select **Managed by SecurityCenter**. For more information, see Apply a New License in the *Tenable Security Center User Guide*.

Manage Tenable Nessus with Tenable Vulnerability Management

If you are using Tenable Vulnerability Management to manage your Tenable Nessus scanners, the plugin and software updates are managed from Tenable Vulnerability Management. For more information, see Tenable Nessus Plugin and Software Updates in the *Tenable Nessus User Guide*.

Tenable Vulnerability Management includes the ability to link unlimited Tenable Nessus scanners as a default component.

For more information about Tenable Vulnerability Management licensing, see Tenable Vulnerability Management Licensing in the *Tenable Licensing Guide*.

Manage Tenable Nessus with Tenable Security Center

If you are using Tenable Security Center to manage your Tenable Nessus scanners, the activation code and plugin updates are managed from Tenable Security Center. For more information, see Tenable Nessus Plugin and Software Updates in the *Tenable Nessus User Guide*.

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 SecurityCenter**.

For more information about Tenable Security Center licensing, see Tenable Security Center Licensing in the *Tenable Licensing Guide*.

Tenable Nessus Versions

Tenable Nessus Professional and Tenable Nessus Expert have the following features.

Feature	Tenable Nessus Professional	Tenable Nessus Expert
Nessus Live Results	Yes	Yes
Vulnerability scanning	Yes	Yes
Compliance scanning	Yes	Yes
Dynamic Application Security Testing (DAST) web application scanning	No	Five web applications per quarter (purchase more as needed)
External attack surface scanning	No	Five domains per quarter (purchase more as needed)
Scan Infrastructure as Code	No	Yes

Port Requirements

Tenable Nessus port requirements include Tenable Nessus Manager, Tenable Nessus Professional, Tenable Nessus Expert, Tenable Nessus Essentials, Tenable Nessus scanners, and Tenable Nessus cluster node-specific requirements and Tenable Agent-specific requirements.

Tenable Nessus

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

Tenable Nessus Agents

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.

Port	Traffic
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.

Deployment Considerations

When deploying Tenable Nessus, knowledge of routing, filters, and firewall policies is often helpful. Deploying behind a NAT device is not desirable unless it is scanning the internal network. Anytime a vulnerability scan flows through a NAT device or application proxy of some sort, the check can distort and a false positive or negative can result.

In addition, if the system running Tenable Nessus has personal or desktop firewalls in place, these tools can drastically limit the effectiveness of a remote vulnerability scan. Host-based firewalls can interfere with network vulnerability scanning. Depending on your firewall's configuration, it may prevent, distort, or hide the probes of a Tenable Nessus scan.

Certain network devices that perform stateful inspection, such as firewalls, load balancers, and Intrusion Detection/Prevention Systems, may react negatively when Tenable Nessus conducts a scan through them. Tenable Nessus has several tuning options that can help reduce the impact of scanning through such devices, but the best method to avoid the problems inherent in scanning through such network devices is to perform a credentialed scan.

If you configure Tenable Nessus Manager for agent management, Tenable does not recommend using Tenable Nessus Manager as a local scanner. For example, do not configure Tenable Security Center scan zones to include Tenable Nessus Manager and avoid running network-based scans directly from Tenable Nessus Manager. These configurations can negatively impact agent scan performance.

This section contains the following deployment considerations:

- Port Requirements
- Host-Based Firewalls
- IPv6 Support

- Network Address Translation (NAT) Limitation
- Antivirus Software
- Security Warnings

Host-Based Firewalls

Port 8834

The Nessus user interface uses port **8834**. If not already open, open port **8834** by consulting your firewall vendor's documentation for configuration instructions.

Allow Connections

If you configured the Nessus server on a host with 3rd-party firewall such as ZoneAlarm or Windows firewall, you must configure it to allow connections from the IP addresses of the clients using Nessus.

Nessus and FirewallD

You can configure Tenable Nessus to work with FirewallD. When you install Tenable Nessus using `firewalld`, you can configure `firewalld` with the Nessus service and Nessus port.

To open the ports required for Nessus, use the following commands:

```
>> firewall-cmd --permanent --add-service=nessus
>> firewall-cmd --reload
```

IPv6 Support

Nessus supports scanning of IPv6 based resources. Many operating systems and devices ship with IPv6 support enabled by default. To perform scans against IPv6 resources, you must configure at least one IPv6 interface on the host where Nessus is installed, and Nessus must be on an IPv6 capable network (Nessus cannot scan IPv6 resources over IPv4, but it can enumerate IPv6 interfaces via credentialed scans over IPv4). Both full and compressed IPv6 notation are supported when initiating scans.

Nessus does not support scanning IPv6 Global Unicast IP address ranges unless you enter the IPs separately (in list format). Nessus does not support ranges expressed as hyphenated ranges or CIDR

addresses. Nessus supports Link-local ranges with the **link6** directive as the scan target or local link with **eth0**.

Network Address Translation (NAT) Limitation

If your virtual machine uses Network Address Translation (NAT) to reach the network, many of Nessus vulnerability checks, host enumeration, and operating system identification are negatively affected.

Antivirus Software

Due to the large number of TCP connections generated during a scan, some anti-virus software packages may classify Tenable Nessus as a worm or a form of malware. Antivirus software may increase your scan processing times.

- If your anti-virus software warns you, select **Allow** to let Tenable Nessus continue scanning.
- If your anti-virus package gives you the option to add processes to an exception list, add **`nessusd.exe`**, **`nessus-service.exe`**, and **`nessuscli.exe`**.

For more information about allowlisting Tenable Nessus folders, files, and processes in security products, see File and Process Allowlist.

Security Warnings

By default, Tenable Nessus is installed and managed using **HTTPS** and **SSL** uses port **8834**. The default installation of Tenable Nessus uses a self-signed SSL certificate.

During the web-based portion of the Tenable Nessus installation, the following message regarding SSL appears:

> *You are likely to get a security alert from your browser saying that the SSL certificate is invalid. You may either choose to accept the risk temporarily, or you can obtain a valid SSL certificate from a registrar.*

This information refers to a security-related message you encounter when accessing the Tenable Nessus user interface (https://[server IP]:8834).

Example Security Warning

- A connection privacy problem
- An untrusted site
- An unsecure connection

Because Tenable Nessus is providing a self-signed SSL certificate, this is normal behavior.

Bypassing SSL Warnings

Based on the browser you are using, use the following steps to proceed to the Tenable Nessus login page.

Browser	Instructions
Google Chrome and Microsoft Edge	Select **Advanced**, and then **Proceed to example.com (unsafe)**. **Note:** Some instances of Google Chrome and Microsoft Edge do not allow you to proceed. If this happens, Tenable recommends using a different browser, such as Safari or Mozilla Firefox.
Mozilla Firefox	Select **I Understand the Risks**, and then select **Add Exception**. Next select **Get Certificate**, and finally select **Confirm Security Exception**.

Get Started with Tenable Nessus

Prepare

1. Ensure that your setup meets the minimum system requirements:
    - Hardware Requirements
    - Software Requirements
2. Obtain your Activation Code for Tenable Nessus.

Install and Configure Tenable Nessus

1. Follow the installation steps depending on your Tenable Nessus software and operating system, as described in Install Tenable Nessus.
2. Perform the initial configuration steps.

Create and Configure Scans

1. Run a host discovery scan to identify assets on your network.
2. Create a scan.
3. Select a scan template that fits your needs.
    - Use a Tenable-provided scanner template.
    - (Tenable Nessus Manager only) Use a Tenable-provided Agent template.
    - Create and use a user-defined template by creating a policy.
4. Configure the scan:
    - Configure the scan settings available for your template.

      For information about scan targets, see Scan Targets.
    - (Optional) To configure live results, see Live Results.
    - (Optional) If you are running a credentialed scan, configure credentials.
    - (Optional) If you are running a compliance scan, select the compliance audits your scan includes.
    - (Optional) If you are using an advanced scan template, select what plugins your scan includes.
5. Launch the scan.

View and Analyze Scan Results

- View scan results.
- View and manage vulnerabilities.

- Manage scan folders.
- Create a scan report or export.

Refine Tenable Nessus Settings

- Adjust scan settings to address warning messages.
- Monitor scanner health.
- Configure Tenable Nessus advanced settings.

Navigate Tenable Nessus

The top navigation bar shows links to the two main pages: **Scans** and **Settings**. You can perform all Tenable Nessus primary tasks using these two pages. Click a page name to open the corresponding page.

Item	Description
	Toggles the **Notifications** box, which shows a list of notifications, successful or unsuccessful login attempts, errors, and system information generated by Tenable Nessus.
Username	Shows a drop-down box with the following options: **My Account**, **What's New**, **Documentation**, and **Sign Out**.

Install Tenable Nessus

To install Tenable Nessus, download Tenable Nessus from the Tenable Downloads site.

When you download Tenable Nessus, ensure the package selected is specific to your operating system and processor.

There is a single Tenable Nessus package per operating system and processor. Tenable Nessus Manager, Tenable Nessus Professional, and Tenable Nessus Expert do not have different packages; your activation code determines which Tenable Nessus product is installed.

Once you download Tenable Nessus, use one of the following procedures to install Tenable Nessus on your operating system:

- Linux
- Windows
- macOS
- Raspberry Pi
- Tenable Core+ Tenable Nessus
- Deploy Tenable Nessus as a Docker Image

Install Tenable Nessus on Linux

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

Note: Tenable Nessus does not support using symbolic links for `/opt/nessus/`.

Before you begin:

- `hostname` is now a dependency for Tenable Nessus rpm installations. Therefore, when installing any Tenable Nessus 10.8.x rpm package, you must also install a hostname package if one has not already been installed. You can do so by running the `install hostname` command that is specific to your Linux operating system. For example:

  ```
  zypper install -y hostname
  ```

  Some Linux CLI tools automatically include dependencies when you install the Tenable Nessus package (`yum install`, for example). In these cases, you do not have to separately install `hostname`.

To install Nessus on Linux:

1. Download the Tenable Nessus package file.
2. From the command line, run the Tenable Nessus installation command specific to your operating system.

   Example Tenable Nessus install commands:

   Debian/Kali and Ubuntu

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

   Red Hat

   ```
   # dnf install Nessus-<version number>-el8.x86_64.rpm
   ```

   SUSE

   ```
   # sudo zypper install Nessus-<version number>-suse12.x86_64.rpm
   ```
3. From the command line, restart the `nessusd` daemon.

   Example Tenable Nessus daemon start commands:

   CentOS, Debian/Kali, Fedora, Oracle Linux, Red Hat, SUSE, and Ubuntu

   ```
   # systemctl start nessusd
   ```
4. Open Tenable Nessus in your browser.
   - To access a remotely installed Tenable Nessus instance, go to https://<remote IP address>:8834 (for example, https://111.49.7.180:8834).
   - To access a locally installed Tenable Nessus instance, go to https://localhost:8834.
5. Perform the remaining Tenable Nessus installation steps in your browser.

Install Tenable Nessus on Windows

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

Note: Tenable Nessus does not support using symbolic links for `/opt/nessus/`.

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

Download Nessus Package File

Download Tenable Nessus from the Tenable Downloads site.

Start Tenable Nessus Installation

1. Navigate to the folder where you downloaded the Tenable Nessus installer.
2. Next, double-click the file name to start the installation process.

Complete the Windows InstallShield Wizard

1. First, the **Welcome to the InstallShield Wizard for Tenable, Inc. Nessus** screen appears. Select **Next** to continue.
2. On the **License Agreement** screen, read the terms of the Tenable Nessus software license and subscription agreement.
3. Select the **I accept the terms of the license agreement** option, and then click **Next**.
4. On the **Destination Folder** screen, select the **Next** button to accept the default installation folder. Otherwise, select the **Change** button to install Tenable Nessus to a different folder.
5. On the **Ready to Install the Program** screen, select the **Install** button.

The **Installing Tenable, Inc. Nessus** screen appears and a **Status** indication bar shows the installation progress. The process may take several minutes.

After the **InstallShield Wizard** completes, the **Welcome to Nessus** page loads in your default browser.

If the page does not load, do one of the following steps to open Tenable Nessus in your browser.

- To access a remotely installed Tenable Nessus instance, go to https://<remote IP address>:8834 (for example, https://111.49.7.180:8834).
- To access a locally installed Tenable Nessus instance, go to https://localhost:8834.

Perform the remaining Tenable Nessus installation steps in your web browser.

Install Tenable Nessus on macOS

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

Note: Tenable Nessus does not support using symbolic links for `/opt/nessus/`.

Download Tenable Nessus Package File

Download the Tenable Nessus package file.

To install Nessus with the GUI installation package:

Extract the Nessus Files

Double-click the `Nessus-<version number>.dmg` file.

Start Nessus Installation

Double-click **Install Nessus.pkg**.

Complete the Tenable, Inc. Nessus Server Install

When the installation begins, the **Install Tenable, Inc. Nessus Server** screen appears and provides an interactive navigation menu.

Introduction

The **Welcome to the Tenable, Inc. Nessus Server Installer** window provides general information about the Nessus installation.

1. Read the installer information.
2. To begin, select the **Continue** button.

License

1. On the **Software License Agreement** screen, read the terms of the **Tenable, Inc.** Nessus software license and subscription agreement.
2. **OPTIONAL**: To retain a copy of the license agreement, select **Print** or **Save**.
3. Next, select the **Continue** button.
4. To continue installing Nessus, select the **Agree** button, otherwise, select the **Disagree** button to quit and exit.

Installation Type

On the **Standard Install on <DriveName>** screen, choose one of the following options:

- Select the **Change Install Location** button.
- Select the **Install** button to continue using the default installation location.

Installation

When the **Preparing for installation** screen appears, you are prompted for a username and password.

1. Enter the **Name** and **Password** of an administrator account or the root user account.
2. On the **Ready to Install the Program** screen, select the **Install** button.

Next, the **Installing Tenable, Inc. Nessus** screen appears and shows a **Status** indication bar for the remaining installation progress. The process may take several minutes.

Summary

1. When the installation is complete, the **The installation was successful** screen appears. After the installation completes, select **Close**.
2. Open Tenable Nessus in your browser.
    - To access a remotely installed Nessus instance, go to https://<remote IP address>:8834 (for example, https://111.49.7.180:8834).
    - To access a locally installed Nessus instance, go to https://localhost:8834.
3. Perform the remaining Nessus installation steps in your browser.

To install Nessus from the command line:

1. Open Terminal.
2. Run the following commands in the listed order:
    a. `sudo hdiutil attach <Nessus .dmg package>`
    b. `sudo installer -package /Volumes/Nessus\ Install/Install\ Nessus.pkg -target /`
    c. `sudo hdiutil detach /Volumes/Nessus\ Install`
3. Open Tenable Nessus in your browser.
    - To access a remotely installed Nessus instance, go to https://<remote IP address>:8834 (for example, https://111.49.7.180:8834).
    - To access a locally installed Nessus instance, go to https://localhost:8834.
4. Perform the remaining Nessus installation steps in your browser.

Install Tenable Nessus on Raspberry Pi

Tenable Nessus 10.0.0 and later supports scanning on the Raspberry Pi 4 Model B with a minimum of 8GB memory.

1. Download the Tenable Nessus Raspberry Pi OS package file from the Tenable Downloads site.
2. From a command prompt or terminal window, run the Tenable Nessus installation command:

```
dpkg -i Nessus-<version>-raspberrypios_armhf.deb
```

3. From a command prompt or terminal window, start the `nessusd` daemon by running the following command:

```
/bin/systemctl start nessusd.service
```

4. Open Tenable Nessus in your browser.

- To access a remotely installed Tenable Nessus instance, go to https://<remote IP address>:8834 (for example, https://111.49.7.180:8834).
- To access a locally installed Tenable Nessus instance, go to https://localhost:8834.

5. Perform the remaining Tenable Nessus installation steps in your browser.

Deploy Tenable Nessus as a Docker Image

You can deploy a managed Tenable Nessus scanner or an instance of Tenable Nessus Professional as a Docker image to run on a container. Tenable provides two base Tenable Nessus images: Oracle Linux 8 (x86_64 and AArch64) and Ubuntu (x86_64 and AArch64). You can configure the Tenable Nessus instance with environment variables to configure the image with the settings you configure automatically. Using operators and variables, you can deploy the Tenable Nessus image as linked to Tenable Vulnerability Management or Tenable Security Center.

Tenable does not recommend deploying Tenable Nessus in a Docker container that shares a network interface controller (NIC) with another Docker container.

Note: Tenable Nessus does not support storage volumes. Therefore, if you deploy a new Tenable Nessus image, you will lose your data and need to reconfigure Tenable Nessus. However, while deploying the new image, you can configure any initial user and linking information with environment variables, as described in step two of the following procedure.

Before you begin:

- Download and install Docker for your operating system.
- Access the Tenable Nessus Docker image from https://hub.docker.com/r/tenable/nessus.

To deploy Tenable Nessus as a Docker image:

1. In your terminal, use the `docker pull` command to get the image.

```
$ docker pull tenable/nessus:<version-OS>
```

For the <*version-OS*> tag, you must specify the Tenable Nessus version and whether you are pulling Oracle Linux 8 or Ubuntu. You can use the `latest` tag in place of a specific Tenable Nessus version (for example, `latest-ubuntu`).

2. Use the `docker run` command to run your image.

    - Use the operators with the appropriate options for your deployment, as described in Operators.
    - To preconfigure Tenable Nessus, use the `-e` operator to set environment variables, as described in Environment Variables.

    > **Note:** Tenable recommends using environment variables to configure your instance of Tenable Nessus when you run the image. If you do not include environment variables such as an activation code, username, password, or linking key (if creating a managed Tenable Nessus scanner), you must configure those items later.

3. Open Tenable Nessus in your browser:

    - To access a remotely installed Tenable Nessus instance, go to **https://<remote IP address>:8834** (for example, https://111.49.7.180:8834).
    - To access a locally installed Tenable Nessus instance, go to **https:/</localhost>:8834**.

4. Perform the remaining Tenable installation steps in your browser. If you did not include environment variables, complete any remaining configuration steps in the command-line interface or Tenable Nessus configuration wizard.

To stop and remove Tenable Nessus as a Docker image:

- To stop and remove the container, see Remove Tenable Nessus as a Docker Container.

Operators

Operator	Description
`--name`	Sets the name of the container in Docker.
`-d`	Starts a container in detached mode.
`-p`	Publishes to the specified port in the format *host port*:*container port*. By default, the port is 8834:8834.

	If you have several Tenable Nessus containers running, use a different host port. The container port must be 8834 because Tenable Nessus listens on port 8834.
`-e`	Precedes an environment variable. For descriptions of environment variables you can set to configure settings in your Tenable Nessus instance, see Environment Variables.

Environment Variables

The required and optional environment variables differ based on your Tenable Nessus license and whether you are linking to Tenable Vulnerability Management. Click the following bullets to view the environment variables.

Deploying a Tenable Nessus image that is linked to Tenable Vulnerability Management

Variable	Required?	Description
`USERNAME`	Yes	Creates the administrator user.
`PASSWORD`	Yes	Creates the password for the user.
Linking Options		
`LINKING_KEY`	Yes	The linking key from the manager.
`NAME`	No	The name of the Tenable Nessus scanner that shows in the manager. By default, the name is the container ID.
`MANAGER_HOST`	No	The hostname or IP address of the manager. By default, the hostname is cloud.tenable.com.
`MANAGER_PORT`	No	The port of the manager. By default, the port is 443.
`GROUPS`	No	A single group or comma-separated list of groups that the scanner should be added to. Group names are case-sensitive.
Proxy Options		

PROXY	No	The hostname or IP address of the proxy server.
PROXY_PORT	No	The port number of the proxy server.
PROXY_USER	No	The name of a user account that has permissions to access and use the proxy server.
PROXY_PASS	No	The password of the user account that you specified as the proxy user.
Tenable Nessus Settings		
AUTO_UPDATE	No	Sets whether Tenable Nessus should automatically receive updates. Valid values are as follows: • `all` — (Default) Automatically update plugins and Tenable Nessus software. • `plugins` — Only update plugins. • `no` — Do not automatically update software or plugins.

Example: Managed Tenable Nessus scanner linked to Tenable Vulnerability Management

```
docker run --name "nessus-managed" -d -p 8834:8834  -e LINKING_KEY=<Tenable
Vulnerability Management linking key> -e USERNAME=admin -e PASSWORD=admin -e MANAGER_
HOST=cloud.tenable.com -e MANAGER_PORT=443 tenable/nessus:<version-OS>
```

Deploying a Tenable Nessus image that is linked to Tenable Security Center

Variable	Required?	Description
USERNAME	Yes	Creates the administrator user.
PASSWORD	Yes	Creates the password for the user.
Linking Options		

SC_MANAGED	Yes	If set to **yes**, starts the container in Tenable Security Center mode. You must include this operator to deploy the image as a Tenable Security Center-managed scanner.
NAME	No	The name of the Tenable Nessus scanner that shows in the manager. By default, the name is the container ID.
Proxy Options		
PROXY-HOST	No	The hostname or IP address of the proxy server.
PROXY-PORT	No	The port number of the proxy server.
PROXY-USERNAME	No	The name of a user account that has permissions to access and use the proxy server.
PROXY-PASSWORD	No	The password of the user account that you specified as the proxy user.
PROXY-AGENT	No	The user agent name, if your proxy requires a preset user agent.

Example: Managed Tenable Nessus scanner linked to Tenable Security Center

```
docker run --name "nessus-managed" -d -p 8834:8834 -e SC_MANAGED=yes -e USERNAME=admin
tenable/nessus:<version-OS>
```

Deploying a Tenable Nessus Professional image

Variable	Required?	Description
ACTIVATION_CODE	Yes	The activation code to register Tenable Nessus.
USERNAME	Yes	Creates the administrator user.
PASSWORD	Yes	Creates the password for the user.

Example: Tenable Nessus Professional

```
docker run --name "nessus-pro" -d -p 8834:8834  -e ACTIVATION_CODE=<activation code> -e
USERNAME=admin -e PASSWORD=admin tenable/nessus:<version-OS>
```

Deploying other Tenable Nessus images

Variable	Required?	Description
USERNAME	No	Creates the administrator user.
PASSWORD	No	Creates the password for the user.

Configure Tenable Nessus

When you access Tenable Nessus in a browser, a warning appears to regard a connection privacy problem, an untrusted site, an unsecure connection, or a related security certificate issue. This is normal behavior. Tenable Nessus provides a self-signed SSL certificate.

Refer to the Security Warnings section for steps necessary to bypass the SSL warnings.

Note: Depending on your environment, plugin configuration and initialization can take several minutes.

To configure Tenable Core + Tenable Nessus, see Deploy or Install Tenable Core in the *Tenable Core+ Tenable Nessus User Guide*.

Before you begin:

- Install Tenable Nessus.

To configure Tenable Nessus:

1. Follow the Install Tenable Nessus instructions to open to the **Welcome to Nessus** page in your browser.
2. On the **Welcome to Nessus** page, do the following:
    - (Optional) Select **Register Offline** if you cannot connect Tenable Nessus to the Internet for installation. Doing so sets Tenable Nessus in offline mode.
    - (Optional) Click **Settings** to configure the following Tenable Nessus settings manually.

- Proxy Server — Configure a proxy server.

  > **Note:** You must enter a proxy server if you want to link the Tenable Nessus scanner through a proxy server. You can also configure a proxy connection later on in the user interface. For more information, see Proxy Server and Remote Link.

- Plugin Feed — Enter a custom host for the Tenable Nessus plugin feed. Tenable Nessus does not interact with the plugin feed if it is in offline mode.

- Encryption Password — Enter a Tenable Nessus encryption a password. Tenable Nessus enforces the encryption password after you create your user in the user interface.

  If you set an encryption password, Nessus encrypts all policies, scans results, and scan configurations. You must enter the password when Tenable Nessus restarts.

  > **Caution:** If you lose your encryption password, it cannot be recovered by an administrator or Tenable Support.

> **Tip:** You can also configure these settings later on in the user interface.

Once you finish, click **Save** to save the settings and return to the **Welcome to Nessus** page.

3. Click **Continue**.

   A new **Welcome to Nessus** page appears.

4. Do one of the following:

   - If you are installing Tenable Nessus online, follow the configuration steps for your selected product:

     - Install Tenable Nessus Essentials, Professional, Expert, or Manager
     - Activate a Tenable Nessus Professional or Tenable Nessus Expert Trial
     - Link to Tenable Vulnerability Management
     - Link to Tenable Security Center

- Link to Tenable Nessus Manager
- Link a Node (Tenable Nessus Manager cluster)

- If you are installing Tenable Nessus offline, continue at step 1 of Install Tenable Nessus Offline.

Install Tenable Nessus Essentials, Professional, Expert, or Manager

This option installs a standalone version of Tenable Nessus Essentials, Nessus Professional, Tenable Nessus Expert, or Nessus Manager. During installation, you must enter your Nessus Activation Code; this Activation Code determines which product is installed.

For information on activating a Nessus trial, see Activate a Tenable Nessus Professional or Tenable Nessus Expert Trial.

To configure Tenable Nessus as Tenable Nessus Essentials, Tenable Nessus Professional, Tenable Nessus Expert, or Tenable Nessus Manager:

1. During the browser portion of the Nessus installation, on the Welcome to Nessus page, click **Continue**. Then, on the second **Welcome to Nessus** screen, do one of the following:
    - Select **Set up a Nessus purchase** to install one of the following Nessus versions:
        - **Nessus Essentials Plus** — The basic standard vulnerability assessment solution for students and educators.
        - **Nessus Professional** — The de-facto industry standard vulnerability assessment solution for security practitioners.
        - **Nessus Expert** — The industry-leading vulnerability assessment solution for the modern attack surface.
        - **Nessus Manager** — The enterprise solution for managing Tenable Agents at scale.
    - Select **Register for Nessus Essentials** to install Tenable Nessus Essentials — The free version of Nessus for educators, students, and hobbyists.

2. Click **Continue**.

    - If you selected **Set up a Nessus purchase**, the **Login** page appears. Do one of the following:

        - If you need an activation code:

            a. On the **Login** page, enter your email and password.

            b. Click **Continue**. The **Activate Product** page appears with your email address and Tenable customer ID.

            c. In the drop-down menu, select the product and activation code you want to activate.

            d. Click **Activate Product**. The **License Information** page appears.

            e. Click **Continue**. The **Create a user account** screen appears.

            f. Continue the process at step 5.

        - If you already have an activation code, click **Skip**.

    - If you selected **Register for Nessus Essentials**, the **Get an activation code** screen appears. Do one of the following:

        - If you need an activation code:

            a. On the **Get an activation code** screen, type your name and email address.

            b. Click **Email**.

            c. Check your email for your free activation code.

        - If you already have an activation code, click **Skip**.

    The **Register Nessus** page appears.

3. On the **Register Nessus** screen, type your **Activation Code**.

    The **Activation Code** is the code you obtained from your activation email or from the Tenable Downloads Page.

4. Click **Continue**.

The **Create a user account** screen appears.

5. Create a Tenable Nessus administrator user account that you use to log in to Tenable Nessus:

   a. In the **Username** box, enter a username.

   b. In the **Password** box, enter a password for the user account.

   > **Note:** Passwords cannot contain Unicode characters.

6. Click **Submit**.

   Tenable Nessus finishes the configuration process, which may take several minutes.

7. Using the administrator user account you created, **Sign In** to Tenable Nessus.

   > **Note:** When you sign in to Tenable Nessus for the first time, you receive the following message: *Plugins are compiling. Tenable Nessus functionality will be limited until compilation is complete.* You cannot create or launch scans, view or create policies or plugin rules, or use the upgrade assistant while Tenable Nessus compiles plugins.

Activate a Tenable Nessus Professional or Tenable Nessus Expert Trial

The following topic describes how to activate a seven-day trial of Tenable Nessus Professional or Tenable Nessus Expert.

> **Tip:** If you forgot to create a user account during activation, you can create an account with the `adduser` nessuscli command.

To activate your Tenable Nessus Professional or Tenable Nessus Expert trial:

1. On the **Welcome to Nessus** screen, select the Tenable Nessus trial you want to activate:

   - **Start a trial of Nessus Expert**
   - **Start a trial of Nessus Professional**

2. Click **Continue**.

   The **Get Started** page appears.

3. Do one of the following:

- **If you do not already have a Tenable community account and/or an activation code for your trial:**

  a. Enter the email address you want to connect to your Tenable community account.

  b. Click **Continue**. Tenable sends a verification email to the email address you entered.

     - If Tenable Nessus does not recognize the email address, the **Create Account** page appears.

       i. Enter your new account information.

     - If Tenable Nessus recognizes the email address, a page appears saying that Tenable Nessus found your account.

  c. Click **Start Trial**.

     The **Verify Email** page appears.

  d. Navigate to the chosen email address's inbox.

  e. Open the **Verify Your Email Address** message.

  f. Click the **Verify Your Email Address** link within the message.

  g. Return to the Tenable Nessus **Verify Email** page.

  h. Click **Verify**.

     The **Trial License Information** page appears, and shows your activation code and the ending date of your trial. Tenable recommends recording your activation code somewhere safe.

  i. Click **Continue**.

     The **Create a user account** screen appears.

  j. Create a Tenable Nessus administrator user account that you use to log in to Tenable Nessus:

a. In the **Username** box, enter a username.

b. In the **Password** box, enter a password for the user account.

> **Note:** Passwords cannot contain Unicode characters.

k. Click **Submit**.

Tenable Nessus finishes the configuration process and signs you into the user interface.

> **Note:** When you sign in to Tenable Nessus for the first time, you receive the following message: *Plugins are compiling. Tenable Nessus functionality will be limited until compilation is complete.* You cannot create or launch scans, view or create policies or plugin rules, or use the upgrade assistant while Tenable Nessus compiles plugins.

- **If you already have a Tenable community account and an activation code for your trial:**

a. Click **Skip**.

b. Follow the prompts to sign in to your account and submit your activation code.

Tenable Nessus finishes the configuration process and signs you into the user interface.

> **Note:** When you sign in to Tenable Nessus for the first time, you receive the following message: *Plugins are compiling. Tenable Nessus functionality will be limited until compilation is complete.* You cannot create or launch scans, view or create policies or plugin rules, or use the upgrade assistant while Tenable Nessus compiles plugins.

Link to Tenable Vulnerability Management

During initial installation, you can install Tenable Nessus as a remote scanner linked to Tenable Vulnerability Management. If you choose not to link the scanner during initial installation, you can link your Tenable Nessus scanner later. Once you link Tenable Nessus to Tenable Vulnerability Management, it remains linked until you unlink it.

> **Note:** If you use domain allowlists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allowlist. This ensures communication with sensor.cloud.tenable.com, which the scanner uses to communicate with Tenable Vulnerability Management.

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.

Before you begin:

- Configure Tenable Nessus as described in Configure Tenable Nessus.
- If the Tenable Nessus scanner is or was previously linked to Tenable Vulnerability Management, Tenable Security Center, or Tenable Nessus Manager, you need to unlink the scanner or run the `nessuscli fix --reset-all` command (for more information, see Fix Commands).
- View and copy the Tenable Nessus scanner linking key. You need the linking key for step 4 of the following process. You can find it in the following Tenable Vulnerability Management menu: **Settings** > **Sensors** > **Linked Scanners** > **Add Nessus Scanner**.

To link Tenable Nessus to Tenable Vulnerability Management from the Tenable Nessus user interface:

1. On the **Welcome to Nessus** screen, select **Link Nessus to another Tenable product**.
2. Click **Continue**.

   The **Managed Scanner** screen appears.
3. From the **Managed by** drop-down box, select **Tenable Vulnerability Management**.
4. In the **Linking Key** box, type the linking key of your Tenable Vulnerability Management instance.

   Note: You can find the Tenable Nessus scanner linking key in the **Add Nessus Scanner** menu of Tenable Vulnerability Management (**Settings** > **Sensors** > **Linked Scanners** > **Add Nessus Scanner**).
5. Click **Continue**.

   The **Create a user account** screen appears.

6. Create a Tenable Nessus administrator user account that you use to log in to Tenable Nessus:

    a. In the **Username** box, enter a username.

    b. In the **Password** box, enter a password for the user account.

    > **Note:** Passwords cannot contain Unicode characters.

7. Click **Submit**.

    Tenable Nessus finishes the configuration process, which may take several minutes.

8. Using the administrator user account you created, **Sign In** to Tenable Nessus.

To link Tenable Nessus to Tenable Vulnerability Management from the command-line interface (CLI):

If you registered or linked Tenable Nessus previously, you need to reset Tenable Nessus before linking to Tenable Vulnerability Management.

Run the following commands to reset Tenable Nessus and link to Tenable Vulnerability Management based on your operating system. To retrieve the linking key needed in the following commands, see Link a Sensor in the *Tenable Vulnerability Management User Guide*.

> **Note:** The `--reset-all` command used in the following steps removes any existing users, data, settings, and configurations. Tenable recommends exporting scan data and creating a backup before resetting. For more information, see Backing Up Tenable Nessus.

Linux

> **Note:** You must have root permissions or greater to run the link commands successfully.

1. Open the Linux CLI.
2. Run the following commands in the listed order:

```
# service nessusd stop
```

```
# cd /opt/nessus/sbin
```

```
# ./nessuscli fix --reset-all
```

3. Do one of the following:

   - If you are linking to a Tenable Vulnerability Management FedRAMP site, run the following link command:

     ```
     # /opt/nessus/sbin/nessuscli managed link --key=<key> --fedcloud
     ```

   - If you are not linking to a FedRAMP site, run the following link command:

     ```
     # ./nessuscli managed link --key=<LINKING KEY> --cloud
     ```

     Tip: There are many scanner options that you can configure by adding optional parameters to the `managed link` command (for example, scanner name, custom CA path, and proxy server information). For more information, see Managed Scanner Commands.

4. Run the following linking command:

   ```
   # service nessusd start
   ```

Windows

Note: You must have admin permissions to run the link commands successfully.

1. Open the Windows CLI.
2. Run the following commands in the listed order:

   ```
   net stop "tenable nessus"
   ```

   ```
   cd C:\Program Files\Tenable\Nessus
   ```

   ```
   nessuscli fix --reset-all
   ```

3. Do one of the following:

    - If you are linking to a Tenable Vulnerability Management FedRAMP site, run the following link command:

      ```
      C:\Program Files\Tenable\Nessus\nessuscli.exe managed link --key=<key> --fedcloud
      ```

    - If you are not linking to a FedRAMP site, run the following link command:

      ```
      nessuscli managed link --key=<LINKING KEY> --cloud
      ```

      Tip: There are many scanner options that you can configure by adding optional parameters to the `managed link` command (for example, scanner name, custom CA path, and proxy server information). For more information, see Managed Scanner Commands.

4. Run the following command:

   ```
   net start "tenable nessus"
   ```

macOS

Note: You must have admin permissions to run the link commands successfully.

1. Open Terminal.
2. Run the following commands in the listed order:

   ```
   # launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
   ```

   ```
   # /Library/Nessus/run/sbin/nessuscli fix --reset-all
   ```

3. Do one of the following:

- If you are linking to a Tenable Vulnerability Management FedRAMP site, run the following link command:

  ```
  # /Library/Nessus/run/sbin/nessuscli managed link --key=<key> --fedcloud
  ```

- If you are not linking to a FedRAMP site, run the following link command:

  ```
  # /Library/Nessus/run/sbin/nessuscli managed link --key=<LINKING KEY> --cloud
  ```

  Tip: There are many scanner options that you can configure by adding optional parameters to the `managed link` command (for example, scanner name, custom CA path, and proxy server information). For more information, see Managed Scanner Commands.

4. Run the following command:

   ```
   # launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
   ```

Link to Tenable Nessus Manager

Note: When deployed for Tenable Agent management in Tenable Security Center, Tenable Nessus Manager does not support linking Tenable Nessus scanners.

During initial installation, you can install Tenable Nessus as a remote scanner linked to Tenable Nessus Manager. If you choose not to link the scanner during initial installation, you can link your Tenable Nessus scanner later.

Note: Once you link Nessus to Tenable Nessus Manager, it remains linked until you unlink it.

Before you begin:

- Configure Tenable Nessus as described in Configure Tenable Nessus.
- If the Tenable Nessus scanner is or was previously linked to Tenable Vulnerability Management, Tenable Security Center, or Tenable Nessus Manager, you need to unlink the

scanner or run the `nessuscli fix --reset-all` command (for more information, see Fix Commands).

To link Nessus to Tenable Nessus Manager:

1. On the **Welcome to Nessus** screen, select **Link Nessus to another Tenable product**.
2. Click **Continue**.

   The **Managed Scanner** screen appears.
3. From the **Managed by** drop-down box, select **Nessus Manager (Scanner)**.
4. In the **Host** box, type Tenable Nessus Manager host.
5. In the **Port** box, type the Tenable Nessus Manager port.
6. In the **Linking Key** box, type the linking key from Tenable Nessus Manager.
7. Click **Continue**.

   The **Create a user account** screen appears.
8. Create a Tenable Nessus administrator user account, which you use to log in to Tenable Nessus:
   a. In the **Username** box, enter a username.
   b. In the **Password** box, enter a password for the user account.

   > **Note:** Passwords cannot contain Unicode characters.
9. Click **Submit**.

   Tenable Nessus finishes the configuration process, which may take several minutes.
10. Using the administrator user account you created, **Sign In** to Tenable Nessus.

Link to Tenable Security Center

During initial installation, you can install Tenable Nessus as a remote scanner linked to Tenable Security Center. If you choose not to link the scanner during initial installation, you can link your Tenable Nessus scanner later.

> **Note:** Once you link Tenable Nessus to Tenable Security Center, it remains linked until you unlink it.

Note: Tenable Security Center does not send plugins to linked Nessus Managers. Nessus Manager pulls plugins directly from Tenable's plugin sites. Therefore, to update plugin sets, Nessus Manager needs access to the internet and Tenable's plugin sites (for more information, see the Which Tenable sites should I allow? community article). If your Nessus Manager does not have internet access, you can manually update its version and plugins offline (for more information, see Manage Nessus Offline).

Before you begin:

- Configure Tenable Nessus as described in Configure Tenable Nessus.
- If the Tenable Nessus scanner is or was previously linked to Tenable Vulnerability Management, Tenable Security Center, or Tenable Nessus Manager, you need to unlink the scanner or run the `nessuscli fix --reset-all` command (for more information, see Fix Commands).

To link Nessus to Tenable Security Center:

1. On the **Welcome to Nessus**, select **Link Nessus to another Tenable product**.
2. Click **Continue**.

   The **Managed Scanner** screen appears.
3. From the **Managed by** drop-down box, select **Tenable.sc**.
4. Click **Continue**.

   The **Create a user account** screen appears.
5. Create a Tenable Nessus administrator user account, which you use to log in to Tenable Nessus:

   a. In the **Username** box, enter a username.

   b. In the **Password** box, enter a password for the user account.

   Note: Passwords cannot contain Unicode characters.
6. Click **Submit**.

   Tenable Nessus finishes the configuration process, which may take several minutes.
7. Using the administrator user account you created, **Sign In** to Tenable Nessus.

What to do next:

- Add the Tenable Nessus scanner to Tenable Security Center as described in Add a Nessus Scanner in the *Tenable Security Center User Guide*.

Manage Activation Code

> **Note:** Tenable Nessus allows you to generate an activation code during the installation process. For more information, see Install Tenable Nessus Essentials, Professional, Expert, or Manager.

The following topic provides Tenable Nessus licensing information.

Licensing Tenable Nessus

You can manage Tenable Nessus in Tenable Vulnerability Management or Tenable Security Center or run it as a standalone subscription product. To purchase a subscription and receive an activation code, go to the Tenable website or work with a Tenable partner.

Tenable Nessus Activation Code

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.

Your activation code:

- is a **one-time** code, unless your license or subscription changes, at which point Tenable issues you a new activation code. Alternatively, you can transfer an existing activation code to a different system. For more information, see Transfer 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, see Manage Tenable Nessus Offline.

Note: See the Obtain an activation code page for instructions on how to obtain and use an activation code.

Manage Tenable Nessus with Tenable Vulnerability Management

If you are using Tenable Vulnerability Management to manage your Tenable Nessus scanners, the plugin and software updates are managed from Tenable Vulnerability Management. For more information, see Tenable Nessus Plugin and Software Updates in the *Tenable Nessus User Guide*.

Tenable Vulnerability Management includes the ability to link unlimited Tenable Nessus scanners as a default component.

For more information about Tenable Vulnerability Management licensing, see Tenable Vulnerability Management Licensing in the *Tenable Licensing Guide*.

Manage Tenable Nessus with Tenable Security Center

If you are using Tenable Security Center to manage your Tenable Nessus scanners, the activation code and plugin updates are managed from Tenable Security Center. For more information, see Tenable Nessus Plugin and Software Updates in the *Tenable Nessus User Guide*.

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 SecurityCenter**.

For more information about Tenable Security Center licensing, see Tenable Security Center Licensing in the *Tenable Licensing Guide*.

To manage your activation code, use the following topics:

- View Activation Code
- Update Activation Code
- Transfer Activation Code

View Activation Code

View on Tenable Community

View your activation code on the Tenable Community site, as described in the Tenable Community Guide.

View in Tenable Nessus

1. Log in to Tenable Nessus.
2. In the top navigation bar, click **Settings**.

   The **About** page appears.
3. In the **Overview** tab, view your **Activation Code**.

Note: If you are using Tenable Nessus Scanner, the License Expiration and Activation Code values on the About page show as **N/A**.

View from Command Line

Use the `nessuscli fetch --code-in-use` command specific to your operating system.

Platform	Command
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --code-in-use`
macOS	`# /Library/Nessus/run/sbin/nessuscli fetch --code-in-use`
Linux	`# /opt/nessus/sbin/nessuscli fetch --code-in-use`

Update Activation Code

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

When you receive a new license with a corresponding activation code, you must register the new activation code in Tenable Nessus.

Note: If you are working with Tenable Nessus offline, see Manage Tenable Nessus Offline.

User Interface

1. In Tenable Nessus, in the top navigation bar, click **Settings**.
2. In the **Overview** tab, click the button next to the activation code.
3. Type the activation code and click **Activate**.

   The license is now active on this instance of Tenable Nessus.

Note: If you are using Tenable Nessus Scanner, the License Expiration and Activation Code values on the About page show as **N/A**.

Command Line Interface

1. On the system running Tenable Nessus, open a command prompt.
2. Run the `nessuscli fetch --register <Activation Code>` command specific to your operating system.

Platform	Command
Linux	`# /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx`
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register xxxx-xxxx-xxxx-xxxx`
macOS	`# /Library/Nessus/run/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx`

Tenable Nessus downloads and installs the Tenable Nessus engine and the latest Tenable Nessus plugins, and then restarts.

Note: To register Tenable Nessus without automatically downloading and installing the latest updates, use the command `nessuscli fetch --register-only`.

Transfer Activation Code

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

In Tenable Nessus Professional and Tenable Nessus Expert, you can use an activation code on multiple systems. This allows you to transfer a Tenable Nessus license from one system to another easily and without resetting your activation code each time.

When you transfer the activation code to a system, it becomes the active instance of Tenable Nessus for that license. Only the most recently activated system can receive plugin updates. All previous instances of Tenable Nessus with that activation code still function, but cannot receive plugin updates. On inactive instances, the following error message appears: **Access to the feed has been denied, likely due to an invalid or transferred license code.**

To transfer an activation code, use one of the following procedures on the system that you want to make the active instance of Tenable Nessus.

Nessus User Interface

Activate a new Tenable Nessus instance

1. Install Tenable Nessus as described in the appropriate procedure for your operating system.
2. Access the system in a browser.
3. In the **Create an account** window, type a username and password.
4. Click **Continue**.
5. In the **Register your scanner** window, in the **Scanner Type** drop-down box, select **Tenable Nessus Essentials, Professional, or Manager**.
6. In the **Activation Code** box, type your activation code.
7. Click **Continue**.

   Tenable Nessus finishes the installation process, which may take several minutes. Once installation is complete, the license is active on this instance of Tenable Nessus.

Update an existing Tenable Nessus instance

1. Access the system on which you want to activate Tenable Nessus.
2. In the top navigation bar, click **Settings**.
3. In the **Overview** tab, click the button next to the activation code.

4. Type the activation code and click **Activate**.

   The license is now active on this instance of Tenable Nessus.

Note: If you are using Tenable Nessus Scanner, the License Expiration and Activation Code values on the About page show as **N/A**.

Command Line Interface

Perform the following procedure as root, or use `sudo` as a non-root user.

1. On the system on which you want to activate Tenable Nessus, open a command prompt.
2. Run the `nessuscli fetch --register <Activation Code>` command specific to your operating system.

Platform	Command
Linux	`# /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx`
macOS	`# /Library/Nessus/run/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx`
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register xxxx-xxxx-xxxx-xxxx`

   Tenable Nessus downloads and installs the Nessus engine and the latest Nessus plugins, and then restarts.

Tenable Nessus Plugin and Software Updates

The following topic describes how Tenable Nessus receives plugin and software updates based on configuration and license type. Tenable Nessus plugins and software updates differently depending on how it is configured during the initial setup.

Note: Tenable Nessus Essentials receives plugin feed updates on a 30-day delay.

Tenable Nessus Configuration	Plugin Updates	Software Updates

Tenable Nessus standalone installation	By default, standalone Tenable Nessus is configured to receive plugins from plugins.nessus.org automatically on a daily interval. You can also trigger a manual update by navigating to the **Settings** > **About** page and clicking ↻ next to the **Last Updated** section. You can check the current installed plugin set in the same section.	By default, Tenable Nessus receives software updates from downloads.nessus.org automatically. If the following criteria is met, there is a banner at the top of the Tenable Nessus user interface when an update is available: • Automatic updates are not configured. • Automatic updates are configured but the version Tenable Nessus downloaded needs to do a service restart to complete. To configure automatic updates, see Update Tenable Nessus Software.
Tenable Nessus offline installation	For offline devices, you need to install plugins manually. For more information, see Update Plugins Offline.	For offline devices, you need to upgrade the Tenable Nessus software manually with the upgrade method dependent on the operating system that Tenable Nessus is installed on. For more information, see Update Tenable Nessus Manager Plugins on an Offline System.
Tenable Nessus managed by Tenable Security Center	Tenable Nessus receives plugins from Tenable Security Center. Tenable Security Center checks in with Tenable Nessus every 15 minutes to see if the Tenable Nessus plugin set matches the Tenable Security Center set. If it does not match, then Tenable	Tenable Nessus scanners managed by Tenable Security Center do not update their software automatically. The only exception to this is if Tenable Nessus is installed on Tenable Core and automatic updates are enabled.

	Security Center provides a new set of plugins.	
Tenable Nessus linked to Tenable Vulnerability Management	Devices linked to Tenable Vulnerability Management receive plugins from cloud.tenable.com.	Tenable Nessus linked to Tenable Vulnerability Management receives software updates from cloud.tenable.com automatically. Tenable Nessus checks in to Tenable Vulnerability Management once every 24 hours for core software updates by default.
Tenable Agents managed by Tenable Nessus Manager	Tenable Agents receive plugins from their Tenable Nessus Manager. Once deployed, agents download a full plugin set from their Tenable Nessus Manager instance. Once the agent downloads a full plugin set, it downloads differential plugin sets from its manager moving forward, unless the set becomes more than 5 days out of date.	Tenable Agents receive software updates from their Tenable Nessus Manager. Agents check in for core software updates every 24 hours, dependent on when the agent was deployed. If the agent is offline at its usual update time, such as if the agent host is off, it checks for software updates when it comes back online, and that becomes the agent's new update time.
Tenable Agents managed by Tenable Vulnerability Management	Tenable Agents receive plugins from Tenable Vulnerability Management. Agents remain without plugin sets until an agent needs plugin sets for scanning. When the agent needs to scan for the first time and the agent does not have plugin sets, the agent downloads the plugin set needed for the requested scan type (this	Tenable Agents receive software updates from Tenable Vulnerability Management. Agents check in for core software updates every 24 hours, dependent on when the agent was deployed. If the agent is offline at its usual update time, such as if the agent host is off, it checks for software updates when it comes back online, and that becomes the agent's new update time.

	can be the full vulnerability plugin set or the inventory plugin set). After the initial scan, the agent performs a differential plugin update when any of the agent plugin sets are 15 days or less behind the Tenable Vulnerability Management plugin sets. 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.	

Manage Tenable Nessus Offline

Required user role when using Tenable Nessus Manager: System Administrator

To manage Tenable Nessus offline, you need two computers: the Tenable Nessus server, which is not connected to the internet, and another computer that is connected to the internet. Use the

following procedures to manage your offline Tenable Nessus server:

- Install Tenable Nessus Offline
- Update License Offline
- Update Plugins Offline
- Update Tenable Nessus Manager Plugins on an Offline System
- Update the Audit Warehouse Manually

Install Tenable Nessus Offline

A Tenable Nessus **Offline** registration is suitable for computers that run Tenable Nessus, but are not connected to the internet. Tenable Nessus scanners that are registered **Offline** are set to *offline mode*, which automatically disables any features that require connection to the Tenable Nessus feed.

To ensure that Tenable Nessus has the most up-to-date plugins, use the following procedure to register Tenable Nessus servers not connected to the internet.

This process requires the use of two computers: the computer where you are installing Tenable Nessus, which is not connected to the internet, and another computer that is connected to the internet.

For the following instructions, we use computers **A** (offline Tenable Nessus server) and **B** (online computer) as examples.

> **Note:** Tenable Nessus Essentials does not support offline installation.

Install Tenable Nessus

1. During the browser portion of the Nessus installation, on the **Welcome to Nessus** page, select **Register Offline**.
2. Click **Continue**.
3. Select the Tenable Nessus type that you want to deploy: Tenable Nessus Expert, Tenable Nessus Professional, Tenable Nessus Manager, or Managed Scanner.

4. Click **Continue**.
5. (Managed Scanner only) If you select Managed Scanner, the **Managed Scanner** page appears.
    a. For **Managed by**, select the product you want to link Tenable Nessus to.
    b. For **Linking Key**, enter your linking key.
    c. Click **Continue**.
6. A unique **Challenge Code** appears. In the following example, the challenge code is: **aaaaaa11b2222cc33d44e5f6666a777b8cc99999**.

Generate the License

1. On a system with internet access (**B**), navigate to the Nessus Offline registration page.
2. In the top field, type the challenge code shown on the **Nessus Product Registration** screen.

   Example challenge code: aaaaaa11b2222cc33d44e5f6666a777b8cc99999
3. Next, where prompted, type your Tenable Nessus activation code.

   Example activation code: AB-CDE-1111-F222-3E4D-55E5-CD6F
4. Click the **Submit** button.

   The offline update page appears and includes the following elements:

   - **Custom URL** — The custom URL displayed downloads a compressed plugins file. This file is used by Nessus to obtain plugin information. This URL is specific to your Nessus license and must be saved and used each time plugins need to be updated.

     > **Tip:** If Tenable Nessus is in offline mode, you can view the **Custom URL** in the **Software Update** tab (**Settings** > **About**) after registration. If you register Tenable Nessus without activating offline mode, Tenable recommends copying and saving the **Custom URL** during registration.

   - **License** — The complete text-string starting with **-----BEGIN Tenable, Inc. LICENSE-----** and ends with **-----END Tenable, Inc. LICENSE-----** is your Nessus product license information. Tenable uses this text-string to confirm your product license and registration.

- **nessus.license** file — At the bottom of the web page, there is an embedded file that includes the license text-string.

Download and Copy Latest Plugins

1. While you are still using the computer with internet access (**B**), select the **Custom URL**.

   A compressed TAR file downloads.

2. Copy the compressed TAR file to the Nessus **offline** (**A**) system.

   Use the directory specific to your operating system:

Platform	Command
Windows	`C:\Program Files\Tenable\Nessus`
macOS	`# /Library/Nessus/run/sbin/`
Linux	`# /opt/nessus/sbin/`

Copy and Paste License Text

1. While still using the computer with internet access (**B**), copy the complete text string starting with **-----BEGIN Tenable, Inc. LICENSE-----** and ends with **-----END Tenable, Inc. LICENSE-----**.

2. On the computer where you are installing Nessus (**A**), on the **Nessus Product Registration** screen, paste the complete text string starting with **-----BEGIN Tenable, Inc. LICENSE-----** and ends with **-----END Tenable, Inc. LICENSE-----**.

3. Select **Continue**.

   Tenable Nessus finishes the installation process; this may take several minutes.

4. Using the system administrator account you created during setup, **Sign In** to Tenable Nessus.

Update License Offline

Required user role when using Tenable Nessus Manager: System Administrator

If you have an existing Tenable Nessus server that is offline, and you want to update Tenable Nessus with a new license, use the following procedure. You can use the procedure to update new and existing licenses.

To manage Tenable Nessus offline, you need two computers: the Tenable Nessus server, which is not connected to the internet, and another computer that is connected to the internet.

To update an offline Tenable Nessus server's license:

1. Generate a Tenable Nessus challenge code on the offline system running Tenable Nessus.

   Before performing offline update operations, you may need to generate a unique challenge code on the Tenable Nessus server.

   Whereas you use an activation code when performing Tenable Nessus operations while connected to the internet, you use a license when performing offline operations; the generated challenge code enables you to view and use your license for offline operations.

   Use one of the following procedures to generate the challenge code:

   - **Generate a challenge code in the Tenable Nessus user interface**

     a. On the offline system running Tenable Nessus, log in to Tenable Nessus.

     b. Click **Settings**.

     c. Click the pencil icon next to the activation code.

        The **Update Activation Code** window appears.

     d. In the **Registration** drop-down menu, select **Offline**.

     e. Click **Activate**.

        The challenge code appears in the window.

     f. Copy the alphanumeric challenge code to your machine.

        Example challenge code: aaaaaa11b2222cc33d44e5f6666a777b8cc99999

   - **Generate a challenge code from the command line interface**

a. On the offline system running Tenable Nessus, open a command prompt.

b. Use the `nessuscli fetch --challenge` command specific to your operating system.

Platform	Command
Windows	C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --challenge
macOS	# /Library/Nessus/run/sbin/nessuscli fetch --challenge
Linux	# /opt/nessus/sbin/nessuscli fetch --challenge

c. Copy the alphanumeric challenge code to your machine.

Example challenge code: aaaaaa11b2222cc33d44e5f6666a777b8cc99999

2. Copy your Tenable Nessus activation code on the offline system running Tenable Nessus.

To generate a Tenable Nessus license, you must enter your activation code. To view your activation code, use one of the following procedures:

- **View your activation code in the Nessus user interface**

1. Log in to Tenable Nessus.
2. In the top navigation bar, click **Settings**.

The **About** page appears.

3. In the **Overview** tab, view your **Activation Code**.

Copy the activation code to your machine.

- **View your activation code in the command line interface**

Use the `nessuscli fetch --code-in-use` command specific to your operating

system.

Platform	Command
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --code-in-use`
macOS	`# /Library/Nessus/run/sbin/nessuscli fetch --code-in-use`
Linux	`# /opt/nessus/sbin/nessuscli fetch --code-in-use`

Copy the activation code to your machine.

3. Generate the license in the Tenable Nessus user interface on a system *with* internet access.

   By default, when you install Tenable Nessus, your license is hidden and automatically registered. You cannot view this license.

   However, if your Tenable Nessus server is not connected to the internet (in other words, it is offline), you must generate a license. This license is unique to your Tenable Nessus product, and you cannot share it.

   Your license is a text-based file that contains a string of alphanumeric characters. The license is created and based on your unique challenge code.

   Generate the license in the Nessus user interface

   a. On a system *with* internet access, navigate to the Tenable Nessus offline registration page.

   b. Where prompted, type in your challenge code.

      Example challenge code: aaaaaa11b2222cc33d44e5f6666a777b8cc99999

   c. Next, where prompted, enter your Tenable Nessus activation code.

      Example activation code: AB-CDE-1111-F222-3E4D-55E5-CD6F

   d. Select **Submit**.

      At the bottom of the resulting web page, an embedded `nessus.license` file that includes the license text string appears.

4. Download and copy the license file (`nessus.license`) on a system *with* internet access.

   After you have generated your Tenable Nessus license, you now need to download and then copy the license to the offline system running Tenable Nessus.

   Download and copy the license file

   a. At the Tenable Nessus offline registration page, while still using the computer with internet access, select the on-screen `nessus.license` link.

      The link downloads the `nessus.license` file.

   b. Copy the `nessus.license` file to the system running Tenable Nessus.

      Use the directory specific to your operating system:

Platform	Directory
Windows	`C:\ProgramData\Tenable\Nessus\conf`
macOS	`# /Library/Nessus/run/etc/nessus`
Linux	`# /opt/nessus/etc/nessus/`

5. Register your license on the offline system running Tenable Nessus.

   Once you download and copy the `nessus.license` file to your offline Tenable Nessus server, use the `nessuscli fetch --register` command that corresponds to your operating system.

   Register your license offline

   a. On the offline system running Tenable Nessus, open the command line interface.

   b. Use the `nessuscli fetch --register-offline` command specific to your operating system.

Platform	Command
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register-offline`

	`"C:\ProgramData\Tenable\Nessus\conf\nessus.license"`
macOS	`# /Library/Nessus/run/sbin/nessuscli fetch --register-offline /Library/Nessus/run/etc/nessus/nessus.license`
Linux	`# /opt/nessus/sbin/nessuscli fetch --register-offline /opt/nessus/etc/nessus/nessus.license`

Update Plugins Offline

Required user role when using Tenable Nessus Manager: System Administrator

Use this procedure to update an existing offline Tenable Nessus server's plugins. The following steps assume that you have already completed steps to Install Tenable Nessus Offline.

Note: Tenable recommends that you only use this process to update offline Tenable Nessus instances. All online instances of Tenable Nessus receive automatic plugin updates. For information on how your Tenable Nessus instances receive plugin updates, see Plugins and the following Tenable knowledge base article.

To update plugins for an offline Tenable Nessus instance:

1. Using the computer with internet access, open the **Custom URL** that you saved during the initial Tenable Nessus license generation process.

   The Tenable Nessus plugins TAR file downloads to your machine.

2. Do one of the following:

   Install plugins TAR file via the Tenable Nessus user interface

   a. On the offline Tenable Nessus system, in the top navigation bar of the Tenable Nessus user interface, click **Settings**.

      The **About** page appears.

   b. Click the **Software Update** tab.

   c. In the upper-right corner, click the **Manual Software Update** button.

      The **Manual Software Update** dialog box appears.

d. In the **Manual Software Update** dialog box, select **Upload your own plugin archive**, and then select **Continue**.

e. Navigate to the compressed TAR file you downloaded, select it, then click **Open**.

Tenable Nessus updates with the uploaded plugins.

Install plugins TAR file via the command line interface

a. Copy the compressed TAR file to the *offline* Tenable Nessus system.

Use the directory specific to your operating system:

Platform	Command
Windows	`C:\Program Files\Tenable\Nessus`
macOS	`# /Library/Nessus/run/sbin/`
Linux	`# /opt/nessus/sbin/`

b. On the offline system, open a command prompt.

c. Use the `nessuscli update <tar.gz file name>` command specific to your operating system.

Platform	Command
Windows	`"C:\Program Files\Tenable\Nessus\nessuscli.exe" update <tar.gz file name>`
macOS	`# /Library/Nessus/run/sbin/nessuscli update <tar.gz file name>`
Linux	`# /opt/nessus/sbin/nessuscli update <tar.gz file name>`

Update Tenable Nessus Manager Plugins on an Offline System

Required user role when using Tenable Nessus Manager: System Administrator

Use the following procedure to update the plugins that a Tenable Nessus Manager parent node offers to its child nodes. For more information, see Clustering.

On Tenable Nessus Manager, you can update plugins on an offline system in two ways.

- **Option 1:** Use the **Manual Software Update** feature in the Tenable Nessus Manager user interface.
- **Option 2:** Use the command-line interface and the `nessuscli update` command.

Option 1: Manual Software Update via the User Interface

1. Download the file `nessus-updates-x.x.x.tar.gz`, where x.x.x is the version number, from https://www.tenable.com/downloads/nessus.
2. On the **offline** system running Tenable Nessus Manager (**A**), in the top navigation bar, select **Settings**.
3. From the left navigation menu, select **Software Update**.
4. Select **Manual Software Update**.
5. In the **Manual Software Update** dialog box, select **Upload your own plugin archive**, and then select **Continue**.
6. Navigate to the directory where you downloaded the compressed TAR file.
7. Select the compressed TAR file and then select **Open**.

   Tenable Nessus Manager updates with the uploaded plugins.

Option 2: Update via the Command Line

1. Download the file `nessus-updates-x.x.x.tar.gz`, where x.x.x is the version number, from https://www.tenable.com/downloads/nessus.
2. On the **offline** system running Tenable Nessus Manager (**A**), open a command prompt.
3. Use the `nessuscli update <tar.gz file name>` command specific to your operating system.

Platform	Command
Windows	`C:\Program Files\Tenable\Nessus\nessuscli.exe update <tar.gz file name>`

Platform	Command
macOS	`# /Library/Nessus/run/sbin/nessuscli update <tar.gz file name>`
Linux	`# /opt/nessus/sbin/nessuscli update <tar.gz file name>`

Update the Audit Warehouse Manually

Required user role when using Tenable Nessus Manager: System Administrator

The *audit warehouse*, which contains all currently published audits, updates automatically when you upgrade to a new version of Tenable Nessus. You can perform an offline update to update the audit warehouse without upgrading to a new version of Tenable Nessus.

Before you begin:

- Download the audit warehouse archive file from the Tenable audits page.

To update the audit warehouse manually using the Tenable Nessus user interface:

Note: You cannot use this procedure to update Tenable Vulnerability Management or Tenable Security Center-managed scanners.

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. Click the **Software Update** tab.

3. In the upper-right corner, click the **Manual Software Update** button.

   The **Manual Software Update** dialog box appears.

4. In the **Manual Software Update** dialog box, select **Upload your own plugin archive**, and then click **Continue**.

5. Navigate to the compressed TAR file you downloaded, select it, and then click **Open**.

   Tenable Nessus updates with the uploaded audit files.

To update the audit warehouse manually using the command-line interface:

1. On the system running Tenable Nessus, open a command prompt.
2. Use the `nessuscli update <tar.gz file name>` command specific to your operating system.

Platform	Command
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe update <tar.gz file name>`
macOS	`# /Library/Nessus/run/sbin/nessuscli update <tar.gz file name>`
Linux	`# /opt/nessus/sbin/nessuscli update <tar.gz file name>`

Tenable Nessus updates with the uploaded audit files.

Upgrade Nessus

Required user role when using Tenable Nessus Manager: System Administrator

This section includes information for updating and upgrading Nessus.

- Update Tenable Nessus Software
- Upgrade from Evaluation
- Upgrade Nessus on Linux
- Upgrade Nessus on Windows
- Upgrade Nessus on macOS

Upgrade from Evaluation

If you used an evaluation version of Nessus and are now upgrading to a full-licensed version of Tenable Nessus, type your full-version activation code on the **Settings** page, on the **About** tab.

Note: If you are using Tenable Nessus Scanner, the License Expiration and Activation Code values on the About page show as **N/A**.

To update the activation code:

1. Select the ✎ button next to the **Activation Code**.
2. In the **Registration** box, select your Nessus type.
3. In the **Activation Code** box, type your new activation code.
4. Click **Activate**.

   Nessus downloads and install the Nessus engine and the latest Nessus plugins, and then restarts.

For information about viewing, resetting, updating, and transferring activation codes, see Manage Activation Code.

Update Tenable Nessus Software

> **Note**: For information about upgrading an offline Tenable Nessus Manager parent node that manages Tenable Nessus scanners, see Update Tenable Nessus Manager Plugins on an Offline System.

As an administrator user, you can configure how Tenable Nessus updates software components and plugins. You can configure the Nessus update settings to update your Nessus version and plugins automatically, or you can manually update the Nessus version and plugins.

To configure Tenable Nessus software update settings:

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.
2. Click the **Software Update** tab.
3. (Tenable Nessus Professional, Tenable Nessus Expert, and Tenable Nessus Manager only) In the **Automatic Updates** section, select one of the following options:

   - **Update all components**: Tenable Nessus automatically updates its software and engine and downloads the latest plugin set.

     In Tenable Nessus Professional and managed Tenable Nessus scanners, Tenable Nessus updates the software version according to your **Nessus Update Plan** setting.
   - **Update plugins**: Tenable Nessus automatically downloads the latest plugin set.
   - **Disabled**: Tenable Nessus does not perform any automatic updates.

4. (Tenable Nessus Professional and Tenable Nessus Expert only) If you enabled automatic updates, in the **Update Frequency** section, do one of the following:

   - If you want to set a standard update interval, from the drop-down box, select **Daily**, **Weekly**, or **Monthly**.
   - If you want to set a custom update frequency in hours, click the ✎ button, then type the number of hours.

5. (Tenable Nessus Professional, Tenable Nessus Expert, and Tenable Vulnerability Management-managed Tenable Nessus scanners only) Set the **Nessus Update Plan** to determine what version Tenable Nessus automatically updates to:

   > **Note:** If you change your update plan and have automatic updates enabled, Tenable Nessus may immediately update to align with the version represented by your selected plan. Tenable Nessus may either upgrade or downgrade versions.

Option	Description
Update to the latest GA release (Default)	Automatically updates to the latest Tenable Nessus version when it is made generally available (GA). **Note:** This date is the same day the version is made generally available.
Opt in to Early Access releases	Automatically updates to the latest Tenable Nessus version as soon as it is released for Early Access (EA), typically a few weeks before general availability.
Delay updates, staying on an older release	Does not automatically update to the latest Tenable Nessus version. Remains on an earlier version of Tenable Nessus set by Tenable, usually one release older than the current generally available version, but no earlier than 8.10.0. When Tenable Nessus releases a new version, your Tenable Nessus instance updates software versions, but stays on a version prior to the latest release.

6. (Optional) Only if instructed to by Tenable Support, in the **Update Server** box, type the server from which you want Tenable Nessus to download plugins.
7. Click the **Save** button.

   Tenable Nessus downloads any available updates automatically according to your settings.

To download updates manually:

> **Note:** You cannot use this procedure to update Tenable Vulnerability Management or Tenable Security Center-managed scanners.

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

   The **About** page appears.
2. Click the **Software Update** tab.
3. In the upper-right corner, click **Manual Software Update**.

   A window appears.
4. In the window, select one of the following options:

   - **Update all components**: Tenable Nessus updates Nessus software and engine and downloads the latest plugin set.

     In Tenable Nessus Professional and Tenable Nessus Expert, Tenable Nessus updates the software version according to your **Nessus Update Plan** setting.

     > **Note:** If you change your update plan, Tenable Nessus may immediately update to align with the version represented by your selected plan. Nessus may either upgrade or downgrade versions.

   - **Update plugins**: Tenable Nessus downloads the latest plugin set.
   - **Upload your own plugin archive**: Tenable Nessus downloads plugins from a file that you upload.
5. Click the **Continue** button.
6. If you selected **Upload your own plugin archive**, browse for your file and select it.

   Tenable Nessus downloads any available updates.

Upgrade Nessus on Linux

Required user role when using Tenable Nessus Manager: System Administrator

Download Nessus

From the Tenable Downloads Page, download the latest, full-license version of Nessus.

Tip: If you are upgrading an offline instance of Tenable Nessus, download the package on an online system and transfer it to the offline instance using your organization's preferred method.

Use Commands to Upgrade Nessus

From a command prompt, run the Nessus upgrade command.

Note: Nessus automatically stops `nessusd` when you run the upgrade command.

Red Hat 6 and 7, CentOS 6 and 7, Oracle Linux 6 and 7

```
# yum upgrade Nessus-<version number and OS>.rpm
```

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

```
# dnf upgrade Nessus-<version number and OS>.rpm
```

SLES/SUSE

```
# zypper in Nessus-<version number and OS>.rpm
```

Debian/Kali and Ubuntu

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

Start the Nessus Daemon

From a command prompt, restart the `nessusd` daemon.

Red Hat, CentOS, Oracle Linux, Fedora, SUSE

```
# service nessusd start
```

Debian/Kali and Ubuntu

```
# /etc/init.d/nessusd start
```

This completes the process of upgrading Nessus on a Linux operating system.

Upgrade Nessus on Windows

Required user role when using Tenable Nessus Manager: System Administrator

Download Nessus

From the Tenable Downloads Page, download the latest, full-license version of Nessus. The download package is specific the Nessus build version, your platform, your platform version, and your CPU.

Tip: If you are upgrading an offline instance of Tenable Nessus, download the package on an online system and transfer it to the offline instance using your organization's preferred method.

Example Nessus Installer Files

```
Nessus-<version number>-Win32.msi
```

```
Nessus-<version number>-x64.msi
```

Start Nessus Installation

1. Navigate to the folder where you downloaded the Nessus installer.
2. Next, double-click the file name to start the installation process.

Complete the Windows InstallShield Wizard

1. At the **Welcome to the InstallShield Wizard for Tenable, Inc. Nessus** screen, select **Next**.
2. On the **License Agreement** screen, read the terms of the Tenable, Inc. Nessus software license and subscription agreement.

3. Select the **I accept the terms of the license agreement** option, and then select the **Next** button.
4. On the **Destination Folder** screen, select the **Next** button to accept the default installation folder. Otherwise, select the **Change** button to install Nessus to a different folder.
5. On the **Ready to Install the Program** screen, select the **Install** button.

   The **Installing Tenable, Inc. Nessus** screen appears and a **Status** indication bar shows the upgrade progress.
6. On the **Tenable Nessus InstallShield Wizard Completed** screen, select the **Finish** button.

   Nessus loads in your default browser, where you can log in.

Upgrade Nessus on macOS

Required user role when using Tenable Nessus Manager: System Administrator

The process of upgrading Nessus on macOS using the Nessus installation GUI is the same process as a new Mac Install.

Tip: If you are upgrading an offline instance of Tenable Nessus, download the package on an online system and transfer it to the offline instance using your organization's preferred method.

Downgrade Tenable Nessus Software

Required user role when using Tenable Nessus Manager: System Administrator

Tenable Nessus supports the ability to downgrade Tenable Nessus to a previous version of Tenable Nessus.

You can downgrade Tenable Nessus software manually, or, for you can configure the **Nessus Update Plan** to automatically downgrade to an older release.

Before you begin:

- Tenable recommends that you create a Tenable Nessus backup file.
- If Tenable Nessus has an encryption password, you cannot downgrade by changing the Tenable Nessus update plan. Remove the encryption password from Tenable Nessus before

you downgrade, then set the encryption password again after the downgrade is complete.

To remove the Tenable Nessus encryption password, see the How to remove the encryption password (formerly master password) through the command-line knowledge base article. To set the Tenable Nessus encryption password after downgrading, see Set an Encryption Password.

To downgrade Tenable Nessus manually on Linux or macOS:

Note: To manually downgrade Tenable Nessus on Windows, contact Tenable support.

1. Turn off automatic software updates by doing either of the following:
   - Change your Tenable Nessus software update plan as described in Update Tenable Nessus Software, set **Automatic Updates** to **Disabled**.
   - Modify the advanced setting **Automatically Update Nessus** (`auto_update_ui`), as described in Advanced Settings.
2. Use one of the following procedures depending on your operating system:

   Linux

   a. Download the Tenable Nessus version you want to install.

   b. Manually install the Tenable Nessus version. Force install the new Tenable Nessus `rpm` file over the current `rpm` file.

   macOS

   a. Download the Tenable Nessus version you want to install.

   b. Manually install the Tenable Nessus version. Replace the current Tenable Nessus `pkg` file with the new `pkg` file.

To configure Tenable Nessus to downgrade automatically (Tenable Nessus Professional, Tenable Nessus Expert, and Tenable Vulnerability Management-managed Tenable Nessus scanners only):

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. Click the **Software Update** tab.

3. Set the **Nessus Update Plan** to determine what version Tenable Nessus automatically updates to. To automatically downgrade, select **Delay updates, staying on an older release**.

   Note: If you change your update plan and have automatic updates enabled, Tenable Nessus may immediately update to align with the version represented by your selected plan. Tenable Nessus may either upgrade or downgrade versions.

Option	Description
Update to the latest GA release (Default)	Automatically updates to the latest Tenable Nessus version when it is made generally available (GA). **Note:** This date is the same day the version is made generally available.
Opt in to Early Access releases	Automatically updates to the latest Tenable Nessus version as soon as it is released for Early Access (EA), typically a few weeks before general availability.
Delay updates, staying on an older release	Does not automatically update to the latest Tenable Nessus version. Remains on an earlier version of Tenable Nessus set by Tenable, usually one release older than the current generally available version, but no earlier than 8.10.0. When Tenable Nessus releases a new version, your Tenable Nessus instance updates software versions, but stays on a version prior to the latest release.

4. Click the **Save** button.

   Tenable Nessus saves the update plan.

Back Up Tenable Nessus

Required user role when using Tenable Nessus Manager: System Administrator

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

Note: Nessus automatically creates a backup file every 24 hours, and you can configure how many daily backup files Nessus stores before discarding them. For more information, see the Backup Days To Keep logging setting.

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

To back up Tenable Nessus:

1. Access Tenable Nessus from a command terminal.
2. Create the Tenable Nessus backup file by running the following command:

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

   Tenable Nessus creates the backup file in the following directory:

   - Linux: `/opt/nessus/var/nessus`
   - Windows: `C:\ProgramData\Tenable\Nessus\nessus`
   - macOS: `/Library/Nessus/run/var/nessus`

   The backup file includes the following files:

   - /nessus/var/nessus/migrate.db
   - /nessus/var/nessus/tenable-plugins-a-20210201.pem
   - /nessus/var/nessus/log.json
   - /nessus/var/nessus/master.key
   - /nessus/var/nessus/tenable-plugins-b-20210201.pem
   - /nessus/var/nessus/tenable-plugins-20210201.pem

- /nessus/var/nessus/nessus_org.pem
- /nessus/var/nessus/users/admin/auth/hash
- /nessus/var/nessus/users/admin/auth/admin
- /nessus/var/nessus/users/admin/auth/rules
- /nessus/var/nessus/users/admin/policies.db
- /nessus/var/nessus/terrascan.db
- /nessus/var/nessus/uuid
- /nessus/var/nessus/backups/
- /nessus/etc/nessus/nessusd.conf.imported
- /nessus/etc/nessus/nessusd.rules
- /nessus/etc/nessus/nessusd.db
- /nessus/etc/nessus/nessus-fetch.db
- /nessus/com/nessus/CA/servercert.pem
- /nessus/com/nessus/CA/cacert.pem
- /nessus/var/nessus/CA/cakey.pem
- /nessus/var/nessus/CA/serverkey.pem
- /nessus/var/nessus/global.db

3. (Optional) Move the Tenable Nessus backup file to a backup location on your system.

What to do next:

- Restore Tenable Nessus

Restore Tenable Nessus

Required user role when using Tenable Nessus Manager: System Administrator

Using the Nessus CLI, you can use a previous backup of Tenable Nessus to restore later on any system, even if it is a different operating system. When you back up Tenable Nessus, your license information and settings are preserved. Tenable Nessus does not restore scan results.

You can restore a backup even if it was created on an earlier version of Tenable Nessus. For example, if you are on Tenable Nessus 10.5.1, you can restore a backup from Tenable Nessus 10.4.0.

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

Note: If you restore a Tenable Nessus Manager backup on a different device or MAC address, the license does not validate properly.

To fix this issue, Tenable recommends that you run the `nessuscli fix --reset` command, then run the `nessuscli fetch --register` command to register Tenable Nessus Manager on the new device or MAC address. Alternatively, you can reset the license via your license portal.

This issue only applies to Tenable Nessus Manager when clustering is not enabled; the license validates successfully when restoring Tenable Nessus Manager with clustering enabled.

Before you begin:

- Back Up Tenable Nessus

To restore Tenable Nessus:

1. Access Tenable Nessus from a command terminal.
2. Stop your Tenable Nessus service.

   Tenable Nessus terminates all processes.
3. Restore Tenable Nessus from the backup file you previously saved by running the following command:

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

   Tenable Nessus restores your backup.

4. Stop and start your Tenable Nessus service.

   Tenable Nessus begins initializing and uses the license information and settings from the backup.

Remove Tenable Nessus

Required user role when using Tenable Nessus Manager: System Administrator

This topic describes how to uninstall Tenable Nessus in different environments.

Uninstall Tenable Nessus on Linux

Use the following procedure to uninstall Tenable Nessus on Linux.

Before you begin:

1. (Optional) Export your scans and policies.
2. Stop Tenable Nessus.
3. Uninstall Tenable Nessus using the following steps:

To uninstall Tenable Nessus from Linux:

1. In Tenable Nessus, verify that any running scans have completed.
2. From a command prompt, stop the `nessusd` daemon.

   The following are examples of Tenable Nessus daemon stop commands:

   Debian/Kali and Ubuntu

   ```
   # /etc/init.d/nessusd stop
   ```

   Red Hat, CentOS, and Oracle Linux

   ```
   # /sbin/service nessusd stop
   ```

   SUSE

```
# /etc/rc.d/nessusd stop
```

3. Run the remove Tenable Nessus command specific to your Linux-style operating system.

   The following are examples of Tenable Nessus remove commands:

   Debian/Kali and Ubuntu

   ```
   # dpkg -r Nessus
   ```

   Red Hat 6 and 7, CentOS 6 and 7, Oracle Linux 6 and 7

   ```
   # yum remove Nessus
   ```

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

   ```
   # dnf remove Nessus
   ```

   SUSE

   ```
   # sudo zypper remove Nessus
   ```

4. Using the command specific to your Linux-style operating system, remove remaining files that were not part of the original installation.

   Examples: Nessus Remove Command

   Linux

   ```
   # rm -rf /opt/nessus
   ```

Uninstall Tenable Nessus on Windows

Use the following procedure to uninstall Tenable Nessus on Windows.

Before you begin:

1. (Optional) Export your scans and policies.
2. Stop Tenable Nessus.

3. Uninstall Tenable Nessus from the Windows user interface or the command line using the following steps:

To uninstall Tenable Nessus from the Windows user interface:

1. Navigate to the portion of Windows that allows you to **Add or Remove Programs** or **Uninstall or change a program**.
2. In the list of installed programs, select the **Tenable Nessus** product.
3. Click **Uninstall**.

   A dialog box appears, confirming your selection to remove Tenable Nessus.
4. Click **Yes**.

   Windows uninstalls Tenable Nessus.

To uninstall Tenable Nessus from the Windows CLI:

1. Open PowerShell with administrator privileges.
2. Run the following command:

```
msiexec.exe /x <path to Nessus installer package>
```

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

Uninstall Tenable Nessus on macOS

Use the following procedure to uninstall Tenable Nessus on macOS.

Before you begin:

1. (Optional) Export your scans and policies.
2. Stop Nessus.
3. Uninstall Tenable Nessus from the macOS user interface using the following steps:

To uninstall Tenable Nessus from the macOS user interface:

1. In **System Preferences**, select the **Nessus** button.
2. On the **Nessus.Preferences** screen, select the lock to make changes.
3. Next, enter your username and password.
4. Select the **Stop Nessus** button.

   The **Status** becomes red and shows as **Stopped**.
5. Finally, exit the **Nessus.Preferences** screen.
6. Remove the following Tenable Nessus directories, subdirectories, and files:
   - /Library/Nessus
   - /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
   - /Library/PreferencePanes/Nessus Preferences.prefPane
   - /Applications/Nessus
7. To prevent the macOS from trying to start the now non-existent service, type the following command from a command prompt to disable the Tenable Nessus service:

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

   If prompted, provide the administrator password.

Remove Tenable Nessus as a Docker Container

When you remove Tenable Nessus running as a Docker container, you lose the container data.

To remove Tenable Nessus as a docker container:

1. In your terminal, stop the container from running using the `docker stop` command.

   ```
   $ docker stop  <container name>
   ```

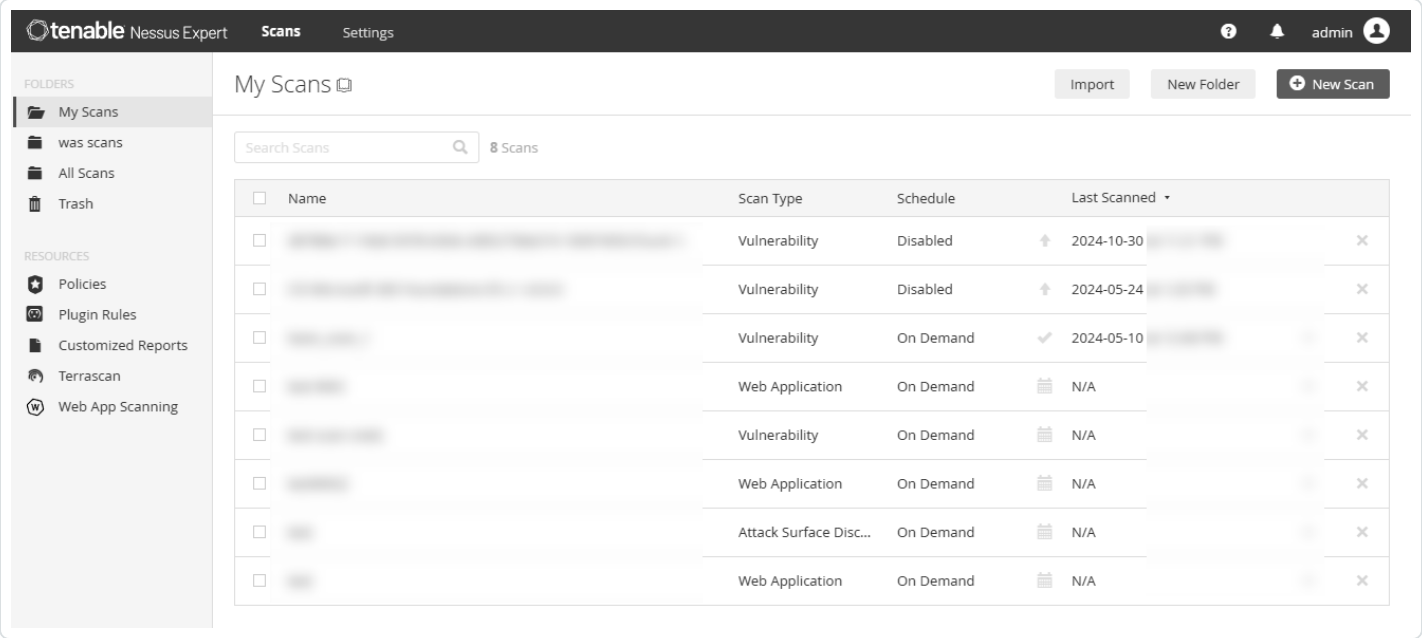
2. Remove your container using the `docker rm` command.

   ```
   $ docker rm  <container name>
   ```

Scans

Note: You cannot create and launch scans, create or view policies or plugin rules, or use the upgrade assistant while Tenable Nessus compiles plugins.

On the **Scans** page, you can create, view, and manage scans and resources. To access the **Scans** page, in the top navigation bar, click **Scans**. The left navigation bar shows the **Folders** and **Resources** sections.



The **Scans** page opens to the **My Scans** folder by default, but you can also view **All Scans** and any custom scan folders.

The page provides the following information for each listed scan:

Column	Description
Name	The scan name.
Scan Type	The scan type: • **Host Discovery** • **Vulnerability** • **Compliance**

	• (Tenable Nessus Expert only) **Web Application** • (Tenable Nessus Expert only) **Attack Surface Discovery** • (Tenable Nessus Manager only) **Agent** To learn more about each scan type, see Scan Templates.
Schedule	The schedule on which Tenable Nessus runs the scan: • **On Demand** — The scan can be launched directly from the scans listing by pressing ▶ in the scan's row. On demand scans can also run at repeating, scheduled intervals if they have a configured schedule. • (Tenable Nessus Manager agent scans only) **Triggered** — The scan can be launched via user-configured triggers. For more information, see Triggered Agent Scans (Tenable Nessus Manager). • **Disabled** — The scan is currently disabled and does not run.
Last Scanned	The date and time at which Tenable Nessus last ran the scan (for example, *January 5 at 8:18 PM* or *2024-12-23 at 6:00 PM*).

For more information on scans, see the following topics:

- Scan Templates
- Create and Manage Scans
- Scan Results
- Scan Folders
- Scan Policies
- Plugins
- Customized Reports
- Scanners
- Agents

Create and Manage Scans

This section contains the following tasks available on the Scans page.

- Create a Scan
- Import a Scan
- Create an Agent Scan
- Modify Scan Settings
- Configure an Audit Trail
- Delete a Scan

Scan Templates

You can use scan templates to create custom policies for your organization. Then, you can run scans based on Tenable's scan templates or your custom policies' settings. For more information, see Create a Policy.

When you first create a scan or policy, the **Scan Templates** section or **Policy Templates** section appears, respectively. Tenable Nessus provides separate templates for scanners and agents, depending on which sensor you want to use for scanning:

- Scanner Templates
- Web App Templates (Tenable Nessus Expert)
- Agent Templates (Tenable Nessus Manager only)

If you have custom policies, they appear in the **User Defined** tab.

When you configure a Tenable-provided scan template, you can modify only the settings included for the scan template type. When you create a user-defined scan template, you can modify a custom set of settings for your scan.

For descriptions of all the scanner and agent template settings, see Settings.

> **Note:** If a plugin requires authentication or settings to communicate with another system, the plugin is not available on agents. This includes, but is not limited to:

- Patch management
- Mobile device management
- Cloud infrastructure audit
- Database checks that require authentication

Scanner Templates

There are three scanner template categories in Tenable Nessus:

- Discovery — Tenable recommends using discovery scans to see what hosts are on your network, and associated information such as IP address, FQDN, operating systems, and open ports, if available. After you have a list of hosts, you can choose what hosts you want to target in a specific vulnerability scan.
- Vulnerabilities — Tenable recommends using vulnerability scan templates for most of your organization's standard, day-to-day scanning needs. Tenable also publishes vulnerability scan templates that allow you to scan your network for a specific vulnerability or group of vulnerabilities. Tenable frequently updates the Tenable Nessus scan template library with templates that detect the latest vulnerabilities of public interest, such as Log4Shell.
- Compliance — Tenable recommends using configuration scan templates to check whether host configurations are compliant with various industry standards. Compliance scans are sometimes referred to as *configuration scans*. For more information about the checks that compliance scans can perform, see Compliance and SCAP Settings.

  Note: Compliance templates are not available in Tenable Nessus Essentials or Essentials Plus. For information about upgrading to Tenable Nessus Professional, see Tenable Nessus Professional.

The following table describes the available scanner templates.

Tip: In the Tenable Nessus user interface, use the search box to find a template quickly.

Note: If you configure Tenable Nessus Manager for agent management, Tenable does not recommend using Tenable Nessus Manager as a local scanner. For example, do not configure Tenable Security Center scan zones to include Nessus Manager and avoid running network-based scans directly from Tenable Nessus Manager. These configurations can negatively impact agent scan performance. In most cases, use agent scan templates when working in Tenable Nessus Manager.

Template	Description
Discovery	
Attack Surface Discovery	(Tenable Nessus Expert only) Uses Tenable Attack Surface Management to scan a list of high-level domains and extract subdomains and DNS-related data. For more information, see Create an Attack Surface Discovery Scan.
Host Discovery	Performs a simple scan to discover live hosts and open ports. Launch this scan to see what hosts are on your network and associated information such as IP address, FQDN, operating systems, and open ports, if available. After you have a list of hosts, you can choose what hosts you want to target in a specific vulnerability scan. Tenable recommends that organizations who do not have a passive network monitor, such as Tenable Network Monitor, run this scan weekly to discover new assets on your network. **Note:** Assets identified by discovery scans do not count toward your license.
Ping-Only Discovery	A simple scan to discover live hosts with minimal network traffic.
Vulnerabilities	
Basic Network Scan	Performs a full system scan that is suitable for any host. Use this template to scan an asset or assets with all of Nessus's plugins enabled. For example, you can perform an internal vulnerability scan on your organization's systems.
Credential Validation	A lightweight scan template used to verify that host credential pairs for Windows and Unix successfully authenticate to scan targets. Use this scan template to quickly diagnose credential pair issues in your network.
Advanced Scan	The most configurable scan type. You can configure this scan template to match any policy. This template has the same default settings as the basic scan template, but it allows for additional configuration options. **Note:** Advanced scan templates allow you to scan more deeply using custom

	configuration, such as faster or slower checks, but misconfigurations can cause asset outages or network saturation. Use the advanced templates with caution. **Note:** Tenable automatically updates this template with any newly-released plugin families in which plugins rely on network traffic for detection.
Advanced Dynamic Scan	An advanced scan without any recommendations, where you can configure dynamic plugin filters instead of manually selecting plugin families or individual plugins. As Tenable releases new plugins, any plugins that match your filters are automatically added to the scan or policy. This allows you to tailor your scans for specific vulnerabilities while ensuring that the scan stays up to date as new plugins are released.
Malware Scan	Scans for malware on Windows and Unix systems. Tenable Nessus detects malware using a combined allow list and block list approach to monitor known good processes, alert on known bad processes, and identify coverage gaps between the two by flagging unknown processes for further inspection.
Nessus 10.8.0 / 10.8.1 Agent Reset	Scan to find, reset, and update Tenable Agents on versions 10.8.0 and 10.8.1. For more information, see the upgrade notes of the Tenable Agent 10.8.2 release notes.
Mobile Device Scan	(Tenable Nessus Manager only) Assesses mobile devices via Microsoft Exchange or an MDM. Use this template to scan what is installed on the targeted mobile devices and report on the installed applications or application versions' vulnerabilities. The Mobile Device Scan plugins allow you to obtain information from devices registered in a Mobile Device Manager (MDM) and from Active Directory servers that contain information from Microsoft Exchange Servers. • To query for information, the Tenable Nessus scanner must be able

	to reach the Mobile Device Management servers. Ensure no screening devices block traffic to these systems from the Nessus scanner. In addition, you must give Tenable Nessus administrative credentials (for example, domain administrator) to the Active Directory servers. • To scan for mobile devices, you must configure Tenable Nessus with authentication information for the management server and the mobile plugins. Since Tenable Nessus authenticates directly to the management servers, you do not need to configure a scan policy to scan specific hosts. • For ActiveSync scans that access data from Microsoft Exchange servers, Tenable Nessus retrieves information from phones that have been updated in the last 365 days.
Credentialed Patch Audit	Authenticates hosts and enumerates missing updates. Use this template with credentials to give Tenable Nessus direct access to the host, scan the target hosts, and enumerate missing patch updates.
Active Directory Starter Scan	Scans for misconfigurations in Active Directory. Use this template to check Active Directory for Kerberoasting, Weak Kerberos encryption, Kerberos pre-authentication validation, non-expiring account passwords, unconstrained delegation, null sessions, Kerberos KRBTGT, dangerous trust relationships, Primary Group ID integrity, and blank passwords.
Find AI	Scans for AI, LLM, and ML-related vulnerabilities.
Remote Monitoring and Management	Identifies assets within your environment that are used for remote monitoring and management. Remote monitoring and management assets are often targeted in cyber attacks to gain local access to systems via remote control. **Note:** This template disables port scanning by default, and you cannot enable port scanning settings for it. Plugins included in this template contain their own target port information.

	When you run a scan based on this template, Plugin 19506 (Nessus Scan Information) shows the following output warning: `WARNING: No port scanner was enabled during the scan. This may lead to incomplete results.` This warning is expected and does not indicate an error. You can safely ignore it.
Compliance	
Audit Cloud Infrastructure	Audits the configuration of third-party cloud services. You can use this template to scan the configuration of Amazon Web Service (AWS), Google Cloud Platform, Microsoft Azure, Rackspace, Salesforce.com, and Zoom, given that you provide credentials for the service you want to audit.
Internal PCI Network Scan	Performs an internal PCI DSS (11.2.1) vulnerability scan. This template creates scans that you can use to satisfy internal (PCI DSS 11.2.1) scanning requirements for ongoing vulnerability management programs that satisfy PCI compliance requirements. You can use these scans for ongoing vulnerability management and to perform rescans until passing or clean results are achieved. You can provide credentials to enumerate missing patches and client-side vulnerabilities. **Note:** While the PCI DSS requires you to provide evidence of passing or "clean" scans on at least a quarterly basis, you must also perform scans after any significant changes to your network (PCI DSS 11.2.3).
MDM Config Audit	Audits the configuration of mobile device managers. The MDM Config Audit template reports on a variety of MDM vulnerabilities, such as password requirements, remote wipe settings, and the use of insecure features, such as tethering and Bluetooth.
Offline Config Audit	Audits the configuration of network devices. Offline configuration audits allow Tenable Nessus to scan hosts without

	the need to scan over the network or use credentials. Organizational policies may not allow you to scan devices or know credentials for devices on the network for security reasons. Offline configuration audits use host configuration files from hosts to scan instead. Through scanning these files, you can ensure that devices' settings comply with audits without the need to scan the host directly. Tenable recommends using offline configuration audits to scan devices that do not support secure remote access and devices that scanners cannot access.
PCI Quarterly External Scan	Performs quarterly external scans as required by PCI. You can use this template to simulate an external scan (PCI DSS 11.2.2) to meet PCI DSS quarterly scanning requirements. However, you cannot submit the scan results from this template to Tenable for PCI Validation. Only Tenable Vulnerability Management customers can submit their PCI scan results to Tenable for PCI ASV validation.
Policy Compliance Auditing	Audits system configurations against a known baseline. **Note:** The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements. The compliance checks can audit against custom security policies, such as password complexity, system settings, or registry values on Windows operating systems. For Windows systems, the compliance audits can test for a large percentage of anything that can be described in a Windows policy file. For Unix systems, the compliance audits test for running processes, user security policy, and content of files.
SCAP and OVAL Auditing	Audits systems using SCAP and OVAL definitions. **Note:** The **SCAP and OVAL Auditing** scan template is retained for backward compatibility. This template supports SCAP version 1.2 and earlier, which is

	not compatible with modern operating systems such as Windows 10 and Windows 11 that require SCAP version 1.3 or later. The National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) is a set of policies for managing vulnerabilities and policy compliance in government agencies. It relies on multiple open standards and policies, including OVAL, CVE, CVSS, CPE, and FDCC policies. • SCAP compliance auditing requires sending an executable to the remote host. • Systems running security software (for example, McAfee Host Intrusion Prevention), may block or quarantine the executable required for auditing. For those systems, you must make an exception for either the host or the executable sent. • When using the **SCAP and OVAL Auditing** template, you can perform Linux and Windows **SCAP CHECKS** to test compliance standards as specified in NIST's Special Publication 800-126.

Web App Templates (Tenable Nessus Expert only)

The following table describes the available Tenable Web App Scanning templates.

You have to download Tenable Web App Scanning in Tenable Nessus before you can use the Web App templates. For more information, see Web Application Scanning in Tenable Nessus.

Template	Description
Vulnerabilities	
API	A scan that checks an API for vulnerabilities. This scan analyzes RESTful APIs described via an OpenAPI (Swagger) specification file.
Web App Config Audit	A high-level scan that analyzes HTTP security headers and other externally facing configurations on a web application to determine if the application is compliant with common security industry standards.

	If you create a scan using this scan template, Tenable Nessus analyzes your web application only for plugins related to security industry standards compliance. For information about setting up and launching a **Web App Config Audit** scan against a web application, see the following video: Web App Config Audit Scanning in Nessus Expert 10.6.
Log4Shell	Detects the Log4Shell vulnerability (CVE-2021-44228) in Apache Log4j.
Web App Overview	A high-level preliminary scan that determines which URLs in a web application Tenable Nessus scans by default. This scan template does not analyze the web application for active vulnerabilities. Therefore, this scan template does not offer as many plugin family options as the **Scan** template. For information about setting up and launching a **Web App Overview** scan against a web application, see the following video: Web App Overview Scanning in Nessus Expert 10.6.
PCI	A scan that assesses web applications for compliance with Payment Card Industry Data Security Standards (PCI DSS) for PCI ASV.
Scan	A comprehensive scan that assesses web applications for a wide range of vulnerabilities. The **Scan** template provides plugin family options for all active web application plugins. If you create a scan using the **Scan** template, Tenable Nessus analyzes your web application for all plugins that the scanner checks for when you create a scan using the **Config Audit**, **Overview**, or **SSL TLS** templates, as well as additional plugins to detect specific vulnerabilities. A scan run with this scan template provides a more detailed assessment of a web application and take longer to complete that other Tenable Web App Scanning scans. For information about scanning a web application with the **Scan** template, see the following video: Web App Scan in Nessus Expert 10.6.

SSL TLS	A scan to determine if a web application uses SSL/TLS public-key encryption and, if so, how the encryption is configured. When you create a scan using the **SSL TLS** template, Tenable Nessus analyzes your web application only for plugins related to SSL/TLS implementation. The scanner does not crawl URLs or assess individual pages for vulnerabilities. For information about setting up and launching an **SSL TLS** scan against a web application, see the following video: Web App SSL and TLS Scanning in Nessus Expert 10.6.
Quick Scan	A high-level scan similar to the **Web App Config Audit** scan template that analyzes HTTP security headers and other externally facing configurations on a web application to determine if the application is compliant with common security industry standards. Does not include scheduling. If you create a scan using the **Quick Scan** scan template, Tenable Nessus analyzes your web application only for plugins related to security industry standards compliance.

Agent Templates (Tenable Nessus Manager only)

There are two agent template categories in Tenable Nessus Manager:

- Vulnerabilities — Tenable recommends using vulnerability scan templates for most of your organization's standard, day-to-day scanning needs.
- Compliance — Tenable recommends using configuration scan templates to check whether host configurations are compliant with various industry standards. Compliance scans are sometimes referred to as *configuration scans*. For more information about the checks that compliance scans can perform, see Compliance and SCAP Settings.

The following table describes the available agent templates.

Tip: In the Tenable Nessus user interface, use the search box to find a template quickly.

Template	Description
Vulnerabilities	

Basic Agent Scan	Performs a full system scan that is suitable for any host. Use this template to scan an asset or assets with all of Nessus's plugins enabled. For example, you can perform an internal vulnerability scan on your organization's systems.
Advanced Agent Scan	The most configurable scan type. You can configure this scan template to match any policy. This template has the same default settings as the basic scan template, but it allows for additional configuration options. **Note:** Advanced scan templates allow you to scan more deeply using custom configuration, such as faster or slower checks, but misconfigurations can cause asset outages or network saturation. Use the advanced templates with caution.
Malware Scan	Scans for malware on Windows and Unix systems. Tenable Agent detects malware using a combined allow list and block list approach to monitor known good processes, alert on known bad processes, and identify coverage gaps between the two by flagging unknown processes for further inspection.
Agent Log4Shell	Detects the Log4Shell vulnerability (CVE-2021-44228) in Apache Log4j via local checks.
Compliance	
Policy Compliance Auditing	Audits system configurations against a known baseline. **Note:** The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements. The compliance checks can audit against custom security policies, such as password complexity, system settings, or registry values on Windows operating systems. For Windows systems, the compliance audits can test for a large percentage of anything that can be described in a Windows policy file. For Unix systems, the compliance audits test for running processes, user security policy, and content of files.

SCAP and OVAL Auditing	Audits systems using SCAP and OVAL definitions. **Note:** The **SCAP and OVAL Auditing** scan template is retained for backward compatibility. This template supports SCAP version 1.2 and earlier, which is not compatible with modern operating systems such as Windows 10 and Windows 11 that require SCAP version 1.3 or later. The National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) is a set of policies for managing vulnerabilities and policy compliance in government agencies. It relies on multiple open standards and policies, including OVAL, CVE, CVSS, CPE, and FDCC policies. • SCAP compliance auditing requires sending an executable to the remote host. • Systems running security software (for example, McAfee Host Intrusion Prevention), may block or quarantine the executable required for auditing. For those systems, you must make an exception for either the host or the executable sent. • When using the **SCAP and OVAL Auditing** template, you can perform Linux and Windows **SCAP CHECKS** to test compliance standards as specified in NIST's Special Publication 800-126.

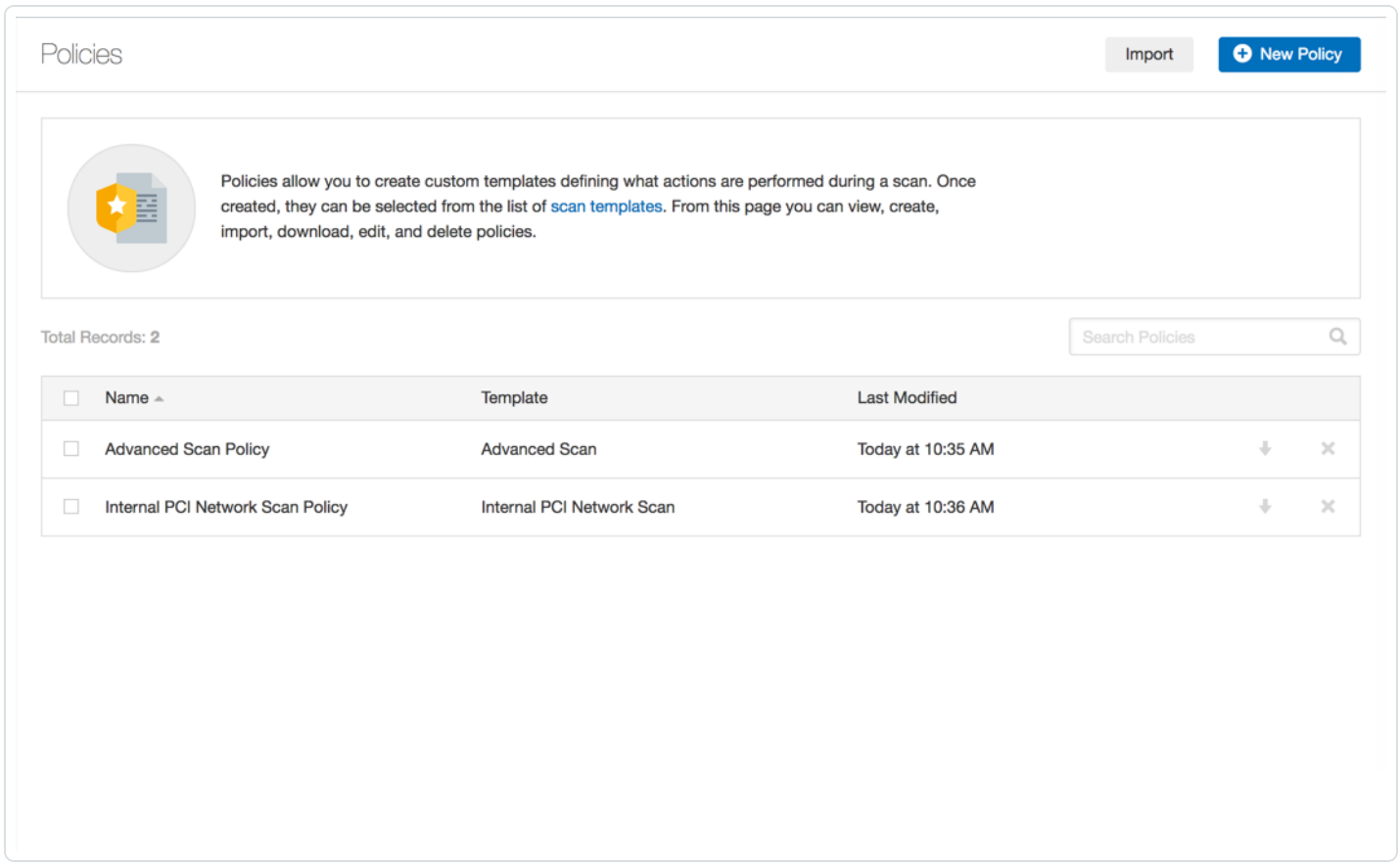
Scan Policies

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

A policy is a set of predefined configuration options related to performing a scan. After you create a policy, you can select it as a template when you create a scan.

Note: You cannot create and launch scans, create or view policies or plugin rules, or use the upgrade assistant while Tenable Nessus compiles plugins.

Tip: For information about default policy templates and settings, see Scan Templates.



Use the following procedures to manage your policies:

Create a policy

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.

   The **Policies** page appears.

3. In the upper right corner, click the **New Policy** button.

   The **Policy Templates** page appears.

4. Click the policy template that you want to use.

5. Configure the policy's settings.

6. Click the **Save** button.

Tenable Nessus saves the policy.

Modify a policy

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.

3. In the policies table, select the check box on the row corresponding to the policy that you want to configure.

   In the upper-right corner, the **More** button appears.

4. Click the **More** button.

5. Click **Configure**.

   The **Configuration** page for the policy appears.

6. Modify the settings.

7. Click the **Save** button.

   Tenable Nessus saves the settings.

Export a policy

You can export an existing scan policy in Tenable Nessus as a *.nessus* file and import it into a different Tenable Nessus installation. You can then view and modify the configuration settings for the imported policy.

To export a policy:

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.

   The **Policies** page appears.

3. In the row of the policy that you want to export, click ↓.

The policy downloads to your machine as a *.nessus* file. You can import the policy into a different Tenable Nessus installation, or you can save it for future use.

Import a policy

You can export a Tenable Nessus policy as a *.nessus* file and import it in a different Tenable Nessus installation. You can then view and modify the configuration settings for the imported policy. You cannot import a Nessus DB file as a policy.

To import a policy:

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.

   The **Policies** page appears.

3. In the upper-right corner, click **Import**.

   Your browser's file manager window appears.

4. Browse to and select the scan file that you want to import.

   > **Note:** The supported file type is an exported Nessus (`.nessus`) file.

   Tenable Nessus imports the file as a policy.

Delete a policy

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.

3. On the policies table, on the row corresponding to the policy that you want to delete, click the ✕ button.

   A dialog box appears, confirming your selection to delete the policy.

4. Click the **Delete** button.

Tenable Nessus deletes the policy.

Policy Characteristics

- Parameters that control technical aspects of the scan such as timeouts, number of hosts, type of port scanner, and more.
- Credentials for local scans (for example, Windows, SSH), authenticated Oracle database scans, HTTP, FTP, POP, IMAP, or Kerberos based authentication.
- Granular family or plugin-based scan specifications.
- Database compliance policy checks, report verbosity, service detection scan settings, Unix compliance checks, and more.
- Offline configuration audits for network devices, allowing safe checking of network devices without needing to scan the device directly.
- Windows malware scans which compare the MD5 checksums of files, both known good and malicious files.

Scan and Policy Settings

Scan settings enable you to refine parameters in scans to meet your specific network security needs. The scan settings you can configure vary depending on the Tenable-provided template on which a scan or policy is based.

You can configure these settings in individual scans or in policy from which you create individual scans.

Tenable Nessus organizes scan settings into the following categories:

- Basic Settings for Scans
- Basic Settings for Policies
- Discovery Settings
- Scope Scan Settings
- Assessment Settings

- Report Settings
- Advanced Settings

Settings in Policies

When configuring settings for policies, note the following:

- If you configure a setting in a policy, that setting applies to any scans you create based on that policy.
- You base a policy on a Tenable-provided template. Most of the settings are identical to the settings you can configure in an individual scan that uses the same Tenable-provided template.

  However, certain **Basic** settings are unique to creating a policy, and do not appear when configuring an individual scan. For more information, see Basic Settings for Policies.
- You can configure certain settings in a policy, but cannot modify those settings in an individual scan based on a policy. These settings include **Discovery**, **Assessment**, **Report**, **Advanced**, **Compliance**, **SCAP**, and **Plugins**. If you want to modify these settings for individual scans, create individual scans based on a Tenable-provided template instead.
- If you configure **Credentials** in a policy, other users can override these settings by adding scan-specific or managed credentials to scans based on the policy.

Basic Settings for Scans

> **Note:** This topic describes **Basic** settings you can set in scans. For **Basic** settings in policies, see Basic Settings for Policies.

The **Basic** scan settings are used to specify certain organizational and security-related aspects of the scan, including the name of the scan, its targets, whether the scan is scheduled, and who has access to the scan, among other settings.

Configuration items that are required by a particular scan are indicated in the Tenable Nessus interface.

The **Basic** settings include the follow sections:

The following tables list all available **Basic** settings by section.

General

Setting	Default Value	Description
Name	None	Specifies the name of the scan. This value is shown on the Tenable Nessus interface.
Description	None	(Optional) Specifies a description of the scan.
Folder	My Scans	Specifies the folder where the scan appears after being saved.
Dashboard	Disabled	(Tenable Nessus Manager only) (Optional) Determines whether the scan results page defaults to the interactive dashboard view.
Agent Groups	None	(Agent scans only) Specifies the agent group or groups you want the scan to target. Select an existing agent group from the drop-down box, or create a new agent group. For more information, see Create a New Agent Group.
Scan Type	Scan Window with a 1 hour interval	(Agent scans only) (Required) Specifies whether the agent scans occur based on a scan window or triggers: • **Scan Window**— Specifies the time frame during which agents must report in order to be included and visible in vulnerability reports. Use the drop-down box to select an interval of time, or click to type a custom scan window. Windows scans must be explicitly launched or scheduled to launch at a particular time interval. • **Triggered Scan** — Specifies the triggers that cause agents to report in. Use the drop-down boxes to select from the following trigger types: • **Interval** — The time interval (hours) between each scan (for example, every **12** hours).

Setting	Default Value	Description
		• **File Name** — The file name that triggers the agent scan. The scan triggers when the file name is detected in the trigger directory. You can set multiple triggers for a single scan, and the scan searches for the triggers in their listed order (in other words, if the first trigger does not trigger the scan, it searches for the second trigger). In addition to interval and file name-based triggered scans, you can use triggered scanning to launch scans directly from nessuscli. For more information, see Triggered Agent Scans.
Scanner	Auto-Select	(Tenable Nessus Manager only) Specifies the scanner that performs the scan. The scanners you can select for this parameter depend on the scanners and scanner groups configured for your Tenable Vulnerability Management instance, as well as your permissions for those scanners or groups.
Policy	None	This setting appears only when the scan owner edits an existing scan that is based on a policy. **Note:** After scan creation, you cannot change the Tenable-provided template on which a scan is based. In the drop-down box, select a policy on which to base the scan. You can select policies for which you have **Can View** or higher permissions. In most cases, you set the policy at scan creation, then keep the same policy each time you run the scan. However, you may want to change the policy when troubleshooting or debugging a scan. For example, changing the policy makes it

Setting	Default Value	Description
		easy to enable or disable different plugin families, change performance settings, or apply dedicated debugging policies with more verbose logging. When you change the policy for a scan, the scan history retains the results of scans run under the previously-assigned policy.
Target URL	None	(Web App templates only) Specifies the URL for the target you want to scan, as it appears on your Tenable Nessus Web Application Scanning license. Regular expressions and wildcards are not allowed. Targets must start with the `http://` or `https://` protocol identifier. **Note:** If the URL you type in the **Target** box has a different FQDN host from the URL that appears on your license, and your scan runs successfully, the new URL you type counts as an additional asset on your license. **Note:** If you create a user-defined scan template, the target setting is not saved to the template. Type a target each time you create a new scan.
Targets	None	Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets. Targets can be specified using a number of different formats. **Tip:** You can force Tenable Nessus to use a given host name for a server during a scan by using the `hostname[ip]` syntax (e.g., `www.example.com[192.168.1.1]`).
Upload Targets	None	Uploads a text file that specifies targets. The targets file must be formatted in the following manner:

Setting	Default Value	Description
		• ASCII file format • Only one target per line • No extra spaces at the end of a line • No extra lines following the last target **Note:** Unicode/UTF-8 encoding is not supported.
Show Dashboard	Off	Select this check box to show a scan dashboard as the scan's default landing page.

Schedule

By default, scans are not scheduled. When you first access the **Schedule** section, the **Enable Schedule** setting appears, set to **Off**. To modify the settings listed on the following table, click the **Off** button. The rest of the settings appear.

Setting	Default Value	Description
Frequency	Once	Specifies how often the scan is launched. • **Once**: Schedule the scan at a specific time. • **Daily**: Schedule the scan to occur every 1-20 days, at a specific time. • **Weekly**: Schedule the scan to occur every 1-20 weeks, by time and day or days of the week. • **Monthly**: Schedule the scan to occur every 1-20 months, by: • **Day of Month**: The scan repeats monthly on a specific day of the month at the selected time. For example, if you select a start date of October 3, the scan repeats on the 3rd of

Setting	Default Value	Description
		each subsequent month at the selected time. • **Week of Month**: The scan repeats monthly on a specific day of the week. For example, if you select a start date of the first Monday of the month, the scan runs on the first Monday of each subsequent month at the selected time. **Note:** If you schedule your scan to repeat monthly, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (for example, the 29th), Tenable Nessus cannot run the scan on those days. • **Yearly**: Schedule the scan to occur every year, by time and day, for up to 20 years.
Starts	Varies	Specifies the exact date and time when a scan launches. The starting date defaults to the date when you are creating the scan. The starting time is the nearest half-hour interval. For example, if you create your scan on 09/18/2023 at 9:17 AM, the default starting date and time is set to 09/18/2023 at 09:30 AM.
Timezone	America/New York	Specifies the timezone of the value set for **Starts**.
Repeat Every	Varies	Specifies the interval at which a scan is relaunched. The default value of this item varies based on the frequency you choose.
Repeat On	Varies	Specifies what day of the week a scan repeats. This item appears only if you specify *Weekly* for **Frequency**.

Setting	Default Value	Description
		The value for **Repeat On** defaults to the day of the week on which you create the scan.
Repeat By	Day of the Month	Specifies when a monthly scan is relaunched. This item appears only if you specify *Monthly* for **Frequency**.
Summary	N/A	Provides a summary of the schedule for your scan based on the values you have specified for the available settings.

Notifications

Setting	Default Value	Description
Email Recipient(s)	None	Specifies zero or more email addresses, separated by commas, that are alerted when a scan completes and the results are available.
Attach Report	Off	(Tenable Nessus Professional only) Specifies whether you want to attach a report to each email notification. This option toggles the **Report Type** and **Max Attachment Size** settings.
Report Type	Nessus	(Tenable Nessus Professional only) Specifies the report type (CSV, Nessus, or PDF) that you want to attach to the email.
Max Attachment Size	25	(Tenable Nessus Professional only) Specifies the maximum size, in megabytes (MB), of any report attachment. If the report exceeds the maximum size, then it is not attached to the email. Tenable Nessus does not support report attachments larger than 50 MB.
Result Filters	None	Defines the type of information to be emailed.

Permissions

Using settings in the **Permissions** section, you can assign various permissions to groups and individual users. When you assign a permission to a group, that permission applies to all users within the group. The following table describes the permissions that can be assigned.

Tip: Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

Permission	Description
No Access	Groups and users set to **No Access** cannot interact with the scan in any way. When you create a scan, by default no other users or groups have access to it.
Can View	Groups and users set to **Can View** can view the results of the scan.
Can Control	Groups and users set to **Can Control** can launch, pause, and stop a scan, as well as view its results.
Can Configure	Groups and users set to **Can Configure** can modify the configuration of the scan in addition to all other permissions.

Scan Targets

You can specify the targets of a scan using several different formats. The following table explains target types, examples, and a short explanation of what occurs when that Tenable Nessus scans that target type.

Target Description	Example	Explanation
A single IPv4 address	192.168.0.1	Tenable Nessus scans the single IPv4 address.
A single IPv6 address	2001:db8::2120:17ff:fe56:333b	Tenable Nessus scans the single IPv6 address.
A single link local IPv6 address with a scope	fe80:0:0:0:216:cbff:fe92:88d0%eth0	Tenable Nessus scans the single IPv6 address. Tenable Nessus does not

Target Description	Example	Explanation
identifier		support using the interface names instead of interface indexes for the scope identifier on Windows platforms.
A small list of IPv4 or IPv6 addresses	192.168.0.1, 192.169.1.1	Tenable Nessus scans the list of addresses. Separate each address with a comma or a new line; otherwise, Nessus cannot read the list.
An IPv4 range with a start and end address	192.168.0.1-192.168.0.255	Tenable Nessus scans all IPv4 addresses between the start address and end address, including both addresses.
An IPv4 address with one or more octets replaced with numeric ranges	192.168.0-1.3-5	The example expands to all combinations of the values given in the octet ranges: 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.168.1.3, 192.168.1.4 and 192.168.1.5.
An IPv4 subnet with CIDR notation	192.168.0.0/24	Tenable Nessus scans all addresses within the specified subnet. The address given is not the start address. Specifying any address within the subnet with the same CIDR scans the same set of hosts.
An IPv4 subnet with netmask	192.168.0.0/255.255.255.128	Tenable Nessus scans all addresses within the specified

Target Description	Example	Explanation
notation		subnet. The address is not a start address. Specifying any address within the subnet with the same netmask scans the same hosts.
A host resolvable to either an IPv4 or an IPv6 address	www.yourdomain.com	Tenable Nessus scans the single host. If the hostname resolves to multiple addresses the address to scan is the first IPv4 address or if it did not resolve to an IPv4 address, the first IPv6 address.
A host resolvable to an IPv4 address with CIDR notation	www.yourdomain.com/24	Tenable Nessus resolves the hostname to an IPv4 address and then treats it like any other IPv4 address with CIDR target.
A host resolvable to an IPv4 address with netmask notation	www.yourdomain.com/255.255.252.0	Tenable Nessus resolves the hostname to an IPv4 address and then treats it like any other IPv4 address with netmask notation.
The text 'link6' optionally followed by an IPv6 scope identifier	link6 or link6%16	Tenable Nessus sends out multicast ICMPv6 echo requests on the interface specified by the scope identifier to the ff02::1 address. Tenable Nessus scans all hosts that respond to the request. If you do not

Target Description	Example	Explanation
		provide a IPv6 scope identifier, Tenable Nessus sends out the requests on all interfaces. Tenable Nessus does not support using the interface names instead of interface indexes for the scope identifier on Windows platforms.
Some text with either a single IPv4 or IPv6 address within square brackets	"Test Host 1[10.0.1.1]" or "Test Host 2 [2001:db8::abcd]"	Tenable Nessus scans the IPv4 or IPv6 address within the brackets like a normal single target.

Tip: You can process hostname targets that look like either a link6 target (start with the text "link6") or like one of the two IPv6 range forms as a hostname by putting single quotes around the target.

Basic Settings for Policies

Note: This topic describes **Basic** settings you can set in policies. For **Basic** settings in individual scans, see Basic Settings for Scans.

You can use **Basic** settings to specify basic aspects of a policy, including who has access to the policy.

The **Basic** settings include the following sections:

General

The general settings for a policy.

Setting	Default Value	Description
Name	None	Specifies the name of the policy.
Description	None	(Optional) Specifies a description of the policy.

Permissions

You can share the policy with other users by setting permissions for users or groups. When you assign a permission to a group, that permission applies to all users within the group.

Permission	Description
No Access	(Default user only) Groups and users set to this permission cannot interact with the policy in any way.
Can Use	Groups and users with this permission can view the policy configuration and use the policy to create scans.
Can Edit	In addition to viewing the policy and using the policy to create scans, groups and users with this permission can modify any policy settings except user permissions. However, they cannot export or delete the policy.

Note: Only the policy owner can export or delete a policy.

Discovery Scan Settings

Note: If a scan is based on a policy, you cannot configure **Discovery** settings in the scan. You can only modify these settings in the related policy.

Note: Tenable Nessus indicates the settings that are required by a particular scan or policy.

The **Discovery** settings relate to discovery and port scanning, including port ranges and methods.

Certain Tenable-provided scanner templates include preconfigured discovery settings.

If you select the **Custom** preconfigured setting option, or if you are using a scanner template that does not include preconfigured discovery settings, you can manually configure **Discovery** settings in the following categories:

Note: The following tables include settings for the **Advanced Scan** template. Depending on the template you select, certain settings may not be available, and default values may vary.

Host Discovery

By default, Tenable Nessus enables some settings in the **Host Discovery** section. When you first access the **Host Discovery** section, the **Ping the remote host** item appears and is set to **On**.

The **Host Discovery** section includes the following groups of settings:

- General Settings
- Ping Methods
- Fragile Devices
- Wake-on-LAN

Setting	Default Value	Description
Ping the remote host	On	If set to `On`, the scanner pings remote hosts on multiple ports to determine if they are alive. Additional options **General Settings** and **Ping Methods** appear. If set to `Off`, the scanner does not ping remote hosts on multiple ports during the scan. **Note:** To scan VMware guest systems, **Ping the remote host** must be set to **Off**.
Scan unresponsive hosts	Disabled	Specifies whether the Nessus scanner scans hosts that do not respond to any ping methods. This option is only available for scans using the PCI Quarterly External Scan template.
General Settings		
Test the local Nessus host	Enabled	When enabled, includes the local Nessus host in the scan. This is used when the Nessus host falls within the target network range for the scan.

Use Fast Network Discovery	Disabled	When disabled, if a host responds to ping, Tenable Nessus attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. These checks can take some time, especially if the remote host is firewalled. When enabled, Tenable Nessus does not perform these checks.
Ping Methods		
ARP	Enabled	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.
TCP	Enabled	Ping a host using TCP.
Destination ports (TCP)	`built-in`	Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that are checked via TCP ping. Type one of the following: `built-in`, a single port, or a comma-separated list of ports. For more information about which ports `built-in` specifies, see the knowledge base article.
ICMP	Enabled	Ping a host using the Internet Control Message Protocol (ICMP).
Assume ICMP unreachable from the gateway means the host is down	Disabled	Assume ICMP unreachable from the gateway means the host is down. When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When this option is enabled, when the scanner receives an ICMP Unreachable message, it considers the targeted host dead. This approach helps speed up discovery on some networks. **Note:** Some firewalls and packet filters use this same

		behavior for hosts that are up, but connected to a port or protocol that is filtered. With this option enabled, this leads to the scan considering the host is down when it is indeed up.
Maximum number of retries	2	Specifies the number of attempts to retry pinging the remote host.
UDP	Disabled	Ping a host using the User Datagram Protocol (UDP). UDP is a stateless protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.
Fragile Devices		
Scan Network Printers	Disabled	When enabled, the scanner scans network printers.
Scan Novell Netware hosts	Disabled	When enabled, the scanner scans Novell NetWare hosts.
Scan Operational Technology devices	Disabled	When enabled, the scanner performs a full scan of Operational Technology (OT) devices such as programmable logic controllers (PLCs) and remote terminal units (RTUs) that monitor environmental factors and the activity and state of machinery. When disabled, the scanner uses ICS/SCADA Smart Scanning to cautiously identify OT devices and stops scanning them once they are discovered.
Wake-on-LAN		
List of MAC Addresses	None	The Wake-on-LAN (WOL) menu controls which hosts to send WOL magic packets to before performing a scan. Hosts that you want to start prior to scanning are provided by uploading a text file that lists one MAC

		address per line.
		For example:
		`33:24:4C:03:CC:C7`
		`FF:5C:2C:71:57:79`

Boot time wait (in minutes)	5	The amount of time to wait for hosts to start before performing the scan.

Port Scanning

The **Port Scanning** section includes settings that define how the port scanner behaves and which ports to scan.

The **Port Scanning** section includes the following groups of settings:

- Ports
- Local Port Enumerators
- Network Port Scanners

Setting	Default Value	Description
Ports		
Consider Unscanned Ports as Closed	Disabled	When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.
Port Scan Range	Default	Specifies the range of ports to be scanned. The supported ranges are: • `default` — Instructs the scanner to scan approximately 4,790 commonly used ports specified in the `nessus-services` file. You can also combine the `default` keyword with other ports and port ranges.

Setting	Default Value	Description
		Note: You can convert the `nessus-services` file to a custom list of ports by performing four consecutive regular expression (regex) replace-all operations in a text editor that supports such operations: • `.*\s+(\d+)\/(tcp|udp)(\r\n|\r|\n) to $1\/$2,` • `(\d+)\/(tcp|udp) to $2:$1` • `tcp to T` • `udp to U` You can find the `nessus-services` file in the following directories, depending on your operating system: • Linux — /opt/nessus/var/nessus/nessus-services • Windows — C:\ProgramData\Tenable\Nessus\nessus\nessus-services • macOS — /Library/Nessus/run/var/nessus/nessus-services • `all` — Instructs the scanner to scan all 65,536 ports, including port 0. You cannot combine the `all` keyword with other ranges. • A comma-separated list of ports (for example, **21,23,25,80,110**), port ranges (for example, **1-1024,9000-9200** or **1-65535** to scan all ports but 0 and **T:1-1024,U:300-500** or **1-1024,T:1024-65535,U:1025** to scan separate or overlapping TCP and UDP port ranges), or combinations thereof.

Setting	Default Value	Description
		If you disable the UDP, SYN, or TCP port scanner settings in the scan policy **Discovery** settings, those ports are not scanned despite what range of ports you specify. The UDP and TCP port scanner settings are disabled by default; the SYN port scanner setting is enabled by default.
Local Port Enumerators		
SSH (netstat)	Enabled	When enabled, the scanner uses netstat to check for open ports from the local machine. It relies on the netstat command being available via an SSH connection to the target. This scan is intended for Linux-based systems and requires authentication credentials. To use this setting, you must first configure SSH Credentials.
WMI (netstat)	Enabled	When enabled, the scanner uses netstat to determine open ports while performing a WMI-based scan. In addition, the scanner: • Ignores any custom range specified in the **Port Scan Range** setting. • Continues to treat unscanned ports as closed if the **Consider unscanned ports as closed** setting is enabled. If any port enumerator (netstat or SNMP) is successful, the port range becomes *all*. To use this setting, you must first configure Windows Credentials.
SNMP	Enabled	When enabled, if the appropriate credentials are provided by the user, the scanner can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.

Setting	Default Value	Description
Only run network port scanners if local port enumeration failed	Enabled	When this setting is enabled, the scanner relies on local port enumeration before relying on network port scans. If a local port enumerator runs, all network port scanners are disabled for the asset. When this setting is disabled, the scanner performs network port scans regardless of the local port enumeration status.
Verify open TCP ports found by local port enumerators	Disabled	When enabled, if a local port enumerator (for example, WMI or netstat) finds a port, the scanner also verifies that the port is open remotely. This approach helps determine if some form of access control is being used (for example, TCP wrappers or a firewall).
Network Port Scanners		
TCP	Disabled	Use the built-in Tenable Nessus TCP scanner to identify open TCP ports on the targets, using a full TCP three-way handshake. If you enable this option, you can also set the **Override Automatic Firewall Detection** option.
SYN	Enabled	Use the built-in Tenable Nessus SYN scanner to identify open TCP ports on the target hosts. SYN scans do not initiate a full TCP three-way handshake. The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines the port state based on a response or lack of response. If you enable this option, you can also set the **Override Automatic Firewall Detection** option.
Override automatic firewall detection	Disabled	This setting can be enabled if you enable either the **TCP** or **SYN** option. When enabled, this setting overrides automatic firewall detection. This setting has three options:

Setting	Default Value	Description
		• **Use aggressive detection** attempts to run plugins even if the port appears to be closed. It is recommended that this option not be used on a production network. • **Use soft detection** disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device. • **Disable detection** disables the firewall detection feature.
UDP	Disabled	This option engages the built-in Tenable Nessus UDP scanner to identify open UDP ports on the targets. Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP ports. Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enumeration options instead if possible.

Service Discovery

The **Service Discovery** section includes settings that attempt to map each open port with the service that is running on that port.

The **Service Discovery** section includes the following groups of settings:

- General Settings
- Search for SSL/TLS Services

Setting	Default Value	Description
General Settings		
Probe all ports	Enabled	When enabled, the scanner attempts to map each open port

Setting	Default Value	Description
to find services		with the service that is running on that port, as defined by the **Port scan range** option. **Caution:** In some rare cases, probing might disrupt some services and cause unforeseen side effects.
Search for SSL based services	On	Controls how the scanner tests SSL-based services. **Caution:** Testing for SSL capability on all ports may be disruptive for the tested host.
Search for SSL/TLS/DTLS Services (enabled)		
Search for SSL/TLS on	Known SSL/TLS ports	Specifies which ports on target hosts the scanner searches for SSL/TLS services. This setting has three options: • **None** **Note:** Setting this option to **None** enables the global_settings/disable_test_ssl_based_services KB item. • **Known SSL/TLS ports** • **All TCP ports**
Search for DTLS On	None	Specifies which ports on target hosts the scanner searches for DTLS services. This setting has the following options: • **None** • **Known DTLS ports** • **All UDP ports**
Identify	60	When enabled, the scanner identifies SSL and TLS certificates that are within the specified number of days of

Setting	Default Value	Description
certificates expiring within x days		expiring.
Enumerate all SSL ciphers	True	When enabled, the scanner ignores the list of ciphers advertised by SSL/TLS services and enumerates them by attempting to establish connections using all possible ciphers.
Enable CRL checking (connects to internet)	False	When enabled, the scanner checks that none of the identified certificates have been revoked.

Identity

The **Identity** section allows you to enable or disable the collection of Active Directory data.

Note: This section is only applicable in Tenable One Enterprise environments.

Setting	Default Value	Description
General Settings		
Collect Identity Data from Active Directory	Disabled	Enable this setting to allow Tenable Nessus to gather user, computer, and group objects from Active Directory. This setting requires that you specify an Active Directory user account for the scan. You also need to enable LDAPS on the Domain Controller that the scan is targeting.

Preconfigured Discovery Scan Settings

Certain Tenable-provided scanner templates include preconfigured discovery settings, described in the following table. The preconfigured discovery settings are determined by both the template and the **Scan Type** that you select.

Template	Scan Type	Preconfigured Settings
Discovery		
Host Discovery	**Host enumeration** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	OS Identification	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP
	Port scan (common ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings:

		◦ Scan common ports ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Port scan (all ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan all ports (1-65535) ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Custom	All defaults

Vulnerabilities		
Basic Network Scan	**Port scan (common ports)** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan common ports ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Port scan (all ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan all ports (1-65535) ◦ Use netstat if credentials are provided ◦ Use SYN scanner if

		necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Use fast network discovery	Use fast network discovery
Advanced Scan	–	All defaults
Advanced Dynamic Scan	–	All defaults
Malware Scan	**Host enumeration** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Host enumeration (include fragile hosts)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Ping hosts using: ◦ TCP

		◦ ARP ◦ ICMP (2 retries) • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Custom	All defaults
Mobile Device Scan	–	–
Web Application Tests	**Port scan (common ports)** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan common ports ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Port scan (all ports)	• General Settings: ◦ Always test the local Nessus host

		◦ Use fast network discovery • Port Scanner Settings: ◦ Scan all ports (1-65535) ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Custom	All defaults
Credentialed Patch Audit	**Port scan (common ports)** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan common ports ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP

		◦ ARP ◦ ICMP (2 retries)
	Port scan (all ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan all ports (1-65535) ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Custom	All defaults
Badlock Detection	**Normal** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan the default Nessus

		port range ◦ Detect SSL/TLS on ports where it is commonly used
	Quick	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan TCP ports 23, 25, 80, and 443 ◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports

	Custom	All defaults
Bash Shellshock Detection	**Normal** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Quick	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan TCP ports 23, 25, 80, and 443 ◦ Detect SSL/TLS on

		ports where it is commonly used • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Custom	All defaults
DROWN Detection	**Normal** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings:

		◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used
	Quick	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan TCP ports 23, 25, 80, and 443 ◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports

	Custom	All defaults
Intel AMT Security Bypass	**Normal** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used
	Quick	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan TCP ports 16992, 16993, 623, 80, and 443 ◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	• General Settings: ◦ Ping the remote host

		◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports
	Custom	All defaults
Shadow Brokers Scan	**Normal** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Thorough	• General Settings: ◦ Ping the remote host

		◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Custom	All defaults
Spectre and Meltdown	**Normal** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	• General Settings: ◦ Ping the remote host

		◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports
	Custom	All defaults
WannaCry Ransomware	**Normal** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used
	Quick	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery

		• Service Discovery Settings: ◦ Scan TCP ports 139 and 445 ◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports
	Custom	All defaults
Log4Shell	**Normal**	• General Settings: ◦ Ping the remote host ◦ Always test the local Tenable Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan the default Tenable Nessus port range

		◦ Detect SSL/TLS on ports where it is commonly used • Do not scan fragile devices.
	Quick	• General Settings: ◦ Ping the remote host ◦ Always test the local Tenable Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan TCP ports 80 and 443 ◦ Detect SSL/TLS on ports where it is commonly used • Do not scan fragile devices.
	Thorough (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Tenable Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports

		• Do not scan fragile devices.
	Custom	All defaults
Log4Shell Remote Checks	**Normal** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Tenable Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan the default Tenable Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used • Do not scan fragile devices.
	Quick	• General Settings: ◦ Ping the remote host ◦ Always test the local Tenable Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan TCP ports 80 and 443 ◦ Detect SSL/TLS on ports where it is

		commonly used • Do not scan fragile devices.
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Tenable Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports • Do not scan fragile devices.
	Custom	All defaults
Log4Shell Vulnerability Ecosystem	**Normal**	• General Settings: ◦ Ping the remote host ◦ Always test the local Tenable Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan the default Tenable Nessus port range ◦ Detect SSL/TLS on ports where it is

		commonly used • Do not scan fragile devices.
	Quick	• General Settings: ◦ Ping the remote host ◦ Always test the local Tenable Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan TCP ports 80 and 443 ◦ Detect SSL/TLS on ports where it is commonly used • Do not scan fragile devices.
	Thorough (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Tenable Nessus host ◦ Use fast network discovery • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports • Do not scan fragile devices.

	Custom	All defaults
Compliance		
Audit Cloud Infrastructure	–	–
Internal PCI Network Scan	**Port scan (common ports)** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan common ports ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Port scan (all ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan all ports (1-65535)

		◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Custom	All defaults
MDM Config Audit	–	–
Offline Config Audit	–	–
PCI Quarterly External Scan	–	**Scan unresponsive hosts** default
Policy Compliance Auditing	**Default** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Custom	All defaults
SCAP and OVAL Auditing	**Host enumeration** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network

		discovery • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Custom	All defaults

Scope Scan Settings

Configure **Scope** settings to specify the URLs and file types that you want to include in or exclude from your scan.

You can configure **Scope** settings when you create a scan or user-defined scan template and select the **Web App Overview** or **Scan** Web App templates. For more information, see Scan Templates and Web Application Scanning in Tenable Nessus.

> **Tip:** If you want to save your settings configurations and apply them to other scans, you can create and configure a policy.

The Scope settings include three sections:

- Crawl Scripts
- Scan Inclusion
- Scan Exclusion

Crawl Scripts

Specify the Selenium scripts you want to add to your scan to enable the scanner to analyze pages with complex access logic.

> **Note:** If you add more than one target to your scan, these settings are disabled.

Setting	Default Value	Description
Add File	n/a	Hyperlink that allows you to add one or more recorded Selenium script files to your scan. Your script must be added as a `.side` file.

Scan Inclusion

Specify the URLs to include when scanning the web application. The URLs must have the same domain as the target URL.

Setting	Default Value	Description
List of URLs	n/a	Specifies the URLs to include when scanning the web application. When listing multiple URLs, you must format them in a comma-separated list.
Specify how the scanner handles URLs found during the application crawl	Crawl all URLs detected	Specifies the limits you want the scanner to adhere to as it crawls URLs. Select one of the following: • **Crawl all URLs detected** — The scanner crawls all URLs and child paths it detects on the target URL's domain host. • **Limit crawling to specified URLs and child paths** — The scanner crawls only the target URL and child paths. • **Limit crawling to specified URLs** — The scanner crawls the target URL only. It does not crawl child paths for the target URL.

Scan Exclusion

Specify any URLs that you want to exclude from your scan.

Note: If you add more than one target to your scan, these settings are disabled.

Setting	Default Value	Description
Regex For Excluded URLs	logout	Specifies a regex pattern that the scanner can look for in URLs to exclude from the scan. When listing multiple regex patterns, you must format them in a comma-separated list. Regex values are case-sensitive. **Note**: The regex values should be values contained within the URL to be excluded. For example, in the URL `http://www.example.com/blog/today.htm`, valid regex values would be `blog` or `today` (not the full URL).
File Extensions to Exclude	js,css,png,jpeg,gif,pdf,csv,svn-base,svg,jpg,ico,woff,woff2,exe,msi,zip	Specifies the file types you want the scanner to exclude from the scan. When listing multiple URLs, you must format them in a comma-separated list. **Note**: Excluding certain file extensions may be useful as the scanner may not realize something is not a web page and attempt to scan it, as if it actually is a web page. This wastes time and slows down the scan. You can add additional file extensions if you know you use them, and are certain they do not need to be scanned. For example, Tenable includes different image extensions by default, such as .png and .jpeg.
Decompose Paths	Disabled	Specifies whether you want the scanner to break down each URL identified

Setting	Default Value	Description
		during the scan into additional URLs, based on directory path level. For example, if you specify *www.example.com/dir1/dir2/dir3* as your target and enable **Decompose Paths**, the scanner analyzes each of the following as separate URLs of the target: • www.example.com/dir1/dir2/dir3 • www.example.com/dir1/dir2 • www.example.com/dir1 When you enable this setting, the scanner attempts to audit the root of each sub-folder found in the path. This increases the web application detection surface, but also increases the scan time.
Exclude Binaries	Enabled	Specifies whether you want the scanner to audit URLs with responses in binary format. When you disable this setting, the scanner attempts to audit the URL for which the response is in the binary format and therefore cannot be read by the scanner, increasing the web application detection surface, but also leading to increased scan time.

Assessment Scan Settings

Note: If a scan is based on a policy, you cannot configure **Assessment** settings in the scan. You can only modify these settings in the related policy.

You can use **Assessment** settings to configure how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.

Certain Tenable-provided scanner templates include preconfigured assessment settings.

If you select the **Custom** preconfigured setting option, or if you are using a scanner template that does not include preconfigured assessment settings, you can manually configure **Assessment** settings in the following categories:

Note: The following tables include settings for the **Advanced Scan** template. Depending on the template you select, certain settings may not be available, and default values may vary.

General

The **General** section includes the following groups of settings:

- Accuracy
- Antivirus
- SMTP

Setting	Default Value	Description
Accuracy		
Override normal Accuracy	Disabled	In some cases, Tenable Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to **Show potential false alarms**, a flaw is reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of **Avoid potential false alarms** causes Tenable Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. As a middle ground between these two settings, disable this setting.

Perform thorough tests (may disrupt your network or impact scan speed)	Disabled	Causes various plugins to work harder. For example, when looking through SMB file shares, a plugin can analyze 3 directory levels deep instead of 1. This could cause much more network traffic and analysis sometimes. By being more thorough, the scan is more intrusive and is more likely to disrupt the network, while potentially providing better audit results.
Antivirus		
Antivirus definition grace period (in days)	0	Configure the delay of the Antivirus software check for a set number of days (0-7). The Antivirus Software Check menu allows you to direct Tenable Nessus to allow for a specific grace time in reporting when antivirus signatures are considered out of date. By default, Tenable Nessus considers signatures out of date if they are more than one day old. You can configure this setting to allow for up to 7 days before reporting them out of date.
SMTP		
Third party domain	Tenable Nessus attempts to send spam through each SMTP device to the address listed in this field. This third-party domain address must be outside the range of the site Tenable Nessus is scanning or the site performing the scan. Otherwise, the SMTP server might abort the test.	
From address	The test messages sent to the SMTP server or servers appear as if they originated from the address specified in this field.	
To address	Tenable Nessus attempts to send messages addressed to the mail recipient listed in this field. The postmaster address is the default value since it is a valid address on most mail servers.	

Brute Force

The **Brute Force** section includes the following groups of settings:

- General Settings
- Oracle Database
- Hydra

Setting	Default Value	Description
General Settings		
Only use credentials provided by the user	Enabled	In some cases, Tenable Nessus can test default accounts and known default passwords. This can lock out an account if too many consecutive invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Tenable Nessus from performing these tests.
Oracle Database		
Test default accounts (slow)	Disabled	Test for known default accounts in Oracle software.
Hydra **Note:** Hydra options only appear when Hydra is installed on the same computer as the scanner or agent executing the scan.		
Always enable Hydra (slow)	Disabled	Enables Hydra whenever Tenable Nessus performs the scan.

Logins file		A .txt file that contains usernames that Hydra uses during the scan.
		You must enter one username per line, and you must end the file with an empty line. For example:
		`<username1>`
		`<username2>`
		`<username3>`

Passwords file		A .txt file that contains passwords for user accounts that Hydra uses during the scan.
		
		You must enter one password per line, and you must end the file with an empty line. For example:
		
		`<password1>`
		`<password2>`
		`<password3>`

Number of parallel tasks	16	The number of simultaneous Hydra tests that you want to execute. By default, this value is 16.
Timeout (in seconds)	30	The number of seconds per login attempt.
Try empty passwords	Enabled	If enabled, Hydra tries usernames without using a password.
Try login as password	Enabled	If enabled, Hydra tries a username as the corresponding password.
Stop brute forcing after the first success	Disabled	If enabled, Hydra stops brute forcing user accounts after the first time an account is successfully accessed.
Add accounts found by other plugins to the login file	Enabled	If disabled, Tenable Nessus only uses the usernames specified in the logins file for the scan. Otherwise, Tenable Nessus discovers more usernames using other plugins and adds them to the logins file to use for the scan.
PostgreSQL database name		The database that you want Hydra to test.
SAP R/3 Client		The ID of the SAP R/3 client that you want Hydra to test.

ID (0 - 99)		
Windows accounts to test	Local accounts	You can set this to *Local accounts*, *Domain Accounts*, or *Either*.
Interpret passwords as NTLM hashes	Disabled	If enabled, Hydra interprets passwords as NTLM hashes.
Cisco login password		You use this password to log in to a Cisco system before brute forcing enable passwords. If you do not enter a password here, Hydra attempts to log in using credentials that were successfully brute forced earlier in the scan.
Web page to brute force		Enter a web page protected by HTTP basic or digest authentication. If you do not enter a web page here, Hydra attempts to brute force a page discovered by the Tenable Nessus web crawler that requires HTTP authentication.
HTTP proxy test website		If Hydra successfully brute forces an HTTP proxy, it attempts to access the website provided here via the brute-forced proxy.
LDAP DN		The LDAP Distinguish Name scope that Hydra authenticates against.

SCADA

Setting	Default Value	Description
Modbus/TCP Coil Access		Modbus uses a function code of 1 to read coils in a Modbus server. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message.
Start at	0	The register at which to start scanning.

Setting	Default Value	Description
Modbus/TCP Coil Access		Modbus uses a function code of 1 to read coils in a Modbus server. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message.
Register		
End at Register	16	The register at which to stop scanning.
ICCP/COTP TSAP Addressing Weakness		The ICCP/COTP TSAP Addressing menu determines a Connection-Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values.
Start COTP TSAP	8	Specifies the starting TSAP value to try.
Stop COTP TSAP	8	Specifies the ending TSAP value to try. Tenable Nessus tries all values between the **Start** and **Stop**.

Web Applications

By default, Tenable Nessus does not scan web applications. When you first access the **Web Application** section, the **Scan Web Applications** setting appears and is **Off**. To modify the Web Application settings listed on the following table, click the **Off** button. The rest of the settings appear.

The **Web Applications** section includes the following groups of settings:

- General Settings
- Web Crawler
- Application Test Settings

Setting	Default Value	Description
Use a custom User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	Specifies which type of browser Tenable Nessus impersonates while scanning.
Web Crawler		
Start crawling from	/	The URL of the first page that Tenable Nessus tests. If you want to test multiple pages, use a colon delimiter to separate them (for example, `/:/php4:/base`).
Excluded pages (regex)	/server_privileges\.php|logout	Specifies portions of the web site to exclude from being crawled. For example, to exclude the /manual directory and all Perl CGI, set this field to: (^/manual) **<>** (\.pl(\?.*)?$). Tenable Nessus supports POSIX regular expressions for string matching and handling and Perl-compatible regular expressions (PCRE).
Maximum pages to crawl	1000	The maximum number of pages to crawl.
Maximum depth to crawl	6	Limit the number of links Tenable Nessus follows for each start page.
Follow dynamic pages	Disabled	If you enable this setting, Tenable Nessus follows dynamic links and may exceed the parameters set above.
Application Test Settings		
Enable generic web application tests	Disabled	Enables the following Application Test Settings.

Setting	Default Value	Description
Abort web application tests if HTTP login fails	Disabled	If Tenable Nessus cannot log in to the target via HTTP, then do not run any web application tests.
Try all HTTP methods	Disabled	This option instructs Tenable Nessus to use POST requests for enhanced web form testing. By default, the web application tests only use GET requests, unless you enable this option. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required. When selected, Tenable Nessus tests each script or variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.
Attempt HTTP Parameter Pollution	Disabled	When performing web application tests, attempt to bypass filtering mechanisms by injecting content into a variable while also supplying the same variable with valid content. For example, a normal SQL injection test may look like /target.cgi?a='&b=2. With HTTP Parameter Pollution (HPP) enabled, the request may look like /target.cgi?a='&a=1&b=2.
Test embedded web servers	Disabled	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be

Setting	Default Value	Description
		prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.
Test more than one parameter at a time per form	Disabled	This setting manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, Tenable Nessus would attempt `/test.php?arg1=XSS&b=1&c=1`, where b and c allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This setting has four options: • **Test random pairs of parameters**: This form of testing randomly checks a combination of random pairs of parameters. This is the fastest way to test multiple parameters. • **Test all pairs of parameters (slow)**: This form of testing is slightly slower but more efficient than the one value test. While testing multiple parameters, it tests an attack string, variations for a single variable and then use the first value for all other

Setting	Default Value	Description
		variables. For example, Tenable Nessus would attempt `/test.php?a=XSS&b=1&c=1&d=1` and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Tenable Nessus would never test for `/test.php?a=XSS&b=3&c=3&d=3` when the first value of each variable is 1. • **Test random combinations of three or more parameters (slower)**: This form of testing randomly checks a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Increasing the amount of combinations by three or more increases the web application test time. • **Test all combinations of parameters (slowest)**: This method of testing checks all possible combinations of attack strings with valid input to variables. Where all pairs testing seeks to create a smaller data set as a tradeoff for speed, all combinations makes no compromise

Setting	Default Value	Description
		on time and uses a complete data set of tests. This testing method may take a long time to complete.
Do not stop after first flaw is found per web page	Stop after one flow is found per web server (fastest)	This setting determines when a new flaw is targeted. This applies at the script level. Finding an XSS flaw does not disable searching for SQL injection or header injection, but unless otherwise specified, there is at most one report for each type on a given port. Note that several flaws of the same type (for example, XSS or SQLi) may be reported if they were caught by the same attack. If this option is disabled, as soon as a flaw is found on a web page, the scan moves on to the next web page. If you enable this option, select one of the following options: • **Stop after one flaw is found per web server (fastest)** — (Default) As soon as a flaw is found on a web server by a script, Tenable Nessus stops and switches to another web server on a different port. • **Stop after one flaw is found per parameter (slow)** — As soon as one type of flaw is found in a parameter of a CGI (for example, XSS), Tenable Nessus switches to the next parameter of the same CGI, the next known CGI, or to the next port or

Setting	Default Value	Description
		server. • **Look for all flaws (slowest)** — Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.
URL for Remote File Inclusion	http://rfi.nessus.org/rfi.txt	During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to use for tests. By default, Tenable Nessus uses a safe file hosted by Tenable, Inc. for RFI testing. If the scanner cannot reach the internet, you can use an internally hosted file for more accurate RFI testing.
Maximum run time (min)	5	This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given website. Scanning the local network for web sites with small applications typically completes in under an hour, however web sites with large applications may require a higher value.

Windows

The Windows section contains the following groups of settings:

- General Settings
- User Enumeration Methods

Setting	Default Value	Description

General Settings		
Request information about the SMB Domain	Disabled	If enabled, the sensor queries domain users instead of local users. Enabling this setting allows plugins 10892 and 10398 to run and plugins 72684 and 10907 to query domain users.
User Enumeration Methods		
You can enable as many of the user enumeration methods as appropriate for user discovery.		
SAM Registry	Enabled	Tenable Nessus enumerates users via the Security Account Manager (SAM) registry.
ADSI Query	Enabled	Tenable Nessus enumerates users via Active Directory Service Interfaces (ADSI). To use ADSI, you must configure credentials under **Credentials** > **Miscellaneous** > **ADSI**.
WMI Query	Enabled	Tenable Nessus enumerates users via Windows Management Interface (WMI).
RID Brute Forcing	Disabled	Tenable Nessus enumerates users via relative identifier (RID) brute forcing. Enabling this setting enables the **Enumerate Domain Users** and **Enumerate Local User** settings.
Enumerate Domain Users (available with RID Brute Forcing enabled)		
Start UID	1000	The beginning of a range of IDs where Tenable Nessus attempts to enumerate domain users.
End UID	1200	The end of a range of IDs where Tenable Nessus attempts to enumerate domain users.
Enumerate Local User (available with RID Brute Forcing enabled)		
Start UID	1000	The beginning of a range of IDs where Tenable Nessus attempts to enumerate local users.
End UID	1200	The end of a range of IDs where Tenable Nessus attempts to enumerate local users.

Malware

The **Malware** section contains the following groups of settings:

- General Settings
- Hash and Allow List Files
- File System Scanning

Setting	Default Value	Description
Hash and Allowlist Files		
Custom Netstat IP Threat List	None	A text file that contains a list of known bad IP addresses that you want to detect. Each line in the file must begin with an IPv4 address. Optionally, you can add a description by adding a comma after the IP address, followed by the description. You can also use hash-delimited comments (e.g., #) in addition to comma-delimited comments. **Note:** Tenable does not detect private IP ranges in the text file.
Provide your own list of known bad MD5 hashes	None	You can upload any additional bad MD5 hashes via a text file that contains one MD5 hash per line. Optionally, you can include a description for a hash by adding a comma after the hash, followed by the description. If Tenable Nessus finds any matches while scanning a target, the description appears in the scan results. You can use standard hash-delimited comments (for example, #) in addition to the comma-separated comments.
Provide your own list of known good MD5 hashes	None	You can upload any additional good MD5 hashes via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash

		in the uploaded file. This is done by adding a comma after the hash, followed by the description. If Tenable Nessus finds any matches while scanning a target, and a description was provided for the hash, the description appears in the scan results. You can use standard hash-delimited comments (for example, #) in addition to the comma-separated comments.
Hosts file allowlist	None	Tenable Nessus checks system hosts files for signs of a compromise (for example, Plugin ID 23910 titled Compromised Windows System (hosts File Check). This option allows you to upload a file containing a list of IPs and hostnames that Tenable Nessus will ignore during the scan. Include one IP and one hostname (formatted identically to your hosts file on the target) per line in a regular text file.
Yara Rules		
Yara Rules	None	A `.yar` file containing the YARA rules to be applied in the scan. You can only upload one file per scan, so include all rules in a single file. For more information, see yara.readthedocs.io.
File System Scanning		
Scan file system	Off	Enabling this option allows you to scan system directories and files on host computers. **Caution:** Enabling this setting in scans targeting 10 or more hosts could result in performance degradation.
Windows Directories		
Scan %Systemroot%	Off	Enables file system scanning to scan %Systemroot%.
Scan %ProgramFiles%	Off	Enables file system scanning to scan %ProgramFiles%.

Scan %ProgramFiles (x86)%	Off	Enables file system scanning to scan %ProgramFiles (x86)%.
Scan %ProgramData%	Off	Enables file system scanning to scan %ProgramData%.
Scan User Profiles	Off	Enables file system scanning to scan user profiles.
Linux Directories		
Scan $PATH	Off	Enable file system scanning to scan for $PATH locations.
Scan /home	Off	Enable file system scanning to scan /home.
MacOS Directories		
Scan $PATH	Off	Enable file system scanning to scan $PATH locations.
Scan /Users	Off	Enable file system scanning to scan /Users.
Scan /Applications	Off	Enable file system scanning to scan /Applications.
Scan /Library	Off	Enable file system scanning to scan /Library.
Custom Directories		
Custom Filescan Directories	None	A custom file that lists directories to be scanned by malware file scanning. In the file, list each directory on a new line. Tenable Nessus does not accept root directories (such as `C:\` or `/`) or variables (such as `%Systemroot%`).

Databases

Setting	Default Value	Description
Oracle Database		
Use detected SIDs	Disabled	When enabled, if at least one host credential and one Oracle database credential are configured, the scanner

		authenticates to scan targets using the host credentials, and then attempts to detect Oracle System IDs (SIDs) locally. The scanner then attempts to authenticate using the specified Oracle database credentials and the detected SIDs. If the scanner cannot authenticate to scan targets using host credentials or does not detect any SIDs locally, the scanner authenticates to the Oracle database using the manually specified SIDs in the Oracle database credentials.

Web App Template Assessment Settings

The following table describes the scan settings that you can configure in Tenable Web App Scanning for Tenable Nessus. For more information, see Web Application Scanning in Tenable Nessus.

Setting	Default Value	Description
Detection Level	Most Detected Pages	Specify which pages you want the scanner to crawl. • **Most Detected Pages** - The scanner crawls only the most detected pages. • **Extended Dictionary** - The scanner tests more path variations for detecting hidden pages, increasing the overall scan duration.
Credentials Bruteforcing	Disabled	When enabled, the scan runs any plugins that perform brute forcing included in the **Plugins** settings. When disabled, the scan does not run brute forcing plugins, even if they are included in the **Plugins** settings.
Elements to Audit	All elements except Parameter Names	Specify the web application elements that you want Tenable Nessus to analyze for vulnerabilities. You can choose any combination of the following elements:

		• Links • Headers • Parameter Names • JSON Elements • User interface Forms • Cookies • Forms • Parameter Values • XML Elements • User interface Inputs
URL for Remote Inclusion	None	Specifies a file on a remote host that Tenable Nessus can use to test for a Remote File Inclusion (RFI) vulnerability. If the scanner cannot reach the internet, the scanner uses this internally hosted file for more accurate RFI testing. **Note**: If you do not specify a file, Tenable Nessus uses a safe, Tenable-hosted file for RFI testing.
JSON Containing Attribute Types and Values	None	

Preconfigured Assessment Scan Settings

Certain Tenable-provided scanner templates include preconfigured assessment settings, described in the following table. The preconfigured assessment settings are determined by both the template and the **Scan Type** that you select.

Template	Scan Type	Preconfigured Settings

Discovery		
Host Discovery	–	–
Vulnerabilities		
Basic Network Scan	**Default** (default)	• General Settings: ◦ Avoid false alarms ◦ Disable CGI scanning • Web Applications: ◦ Disable web application scanning
	Scan for known web vulnerabilities	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Generic web application tests disabled
	Scan for all web vulnerabilities (quick)	• General Settings: ◦ Avoid potential false alarms

		◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 5 minutes (max)
	Scan for all web vulnerabilities (complex)	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning ◦ Perform thorough tests • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 10 minutes

		(max) ◦ Try all HTTP methods ◦ Attempt HTTP Parameter Pollution
	Custom	All defaults
Advanced Scan	–	–
Advanced Dynamic Scan	–	–
Malware Scan	–	**Malware Settings** defaults
Mobile Device Scan	–	–
Web Application Tests	**Scan for known web vulnerabilities**	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Generic web application tests disabled
	Scan for all web vulnerabilities (quick)	• General Settings: ◦ Avoid potential false alarms

	(Default)	◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 5 minutes (max)
	Scan for all web vulnerabilities (complex)	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning ◦ Perform thorough tests • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications

		◦ Perform each generic web app test for 10 minutes (max) ◦ Try all HTTP methods ◦ Attempt HTTP Parameter Pollution
	Custom	All defaults
Credentialed Patch Audit	–	**Brute Force**, **Windows**, and **Malware** defaults
Badlock Detection	–	–
Bash Shellshock Detection		**Web Crawler** defaults
DROWN Detection	–	–
Intel AMT Security Bypass	–	–
Log4Shell	**Default**	• General Settings ◦ Avoid potential false alarms ◦ Disable CGI scanning • Web Applications ◦ Disable web application scanning
Log4Shell Remote Checks	**Default**	• General Settings ◦ Avoid potential false alarms ◦ Disable CGI scanning • Web Applications ◦ Disable web application

		scanning
Log4Shell Vulnerability Ecosystem	**Default**	• General Settings ◦ Avoid potential false alarms ◦ Disable CGI scanning • Web Applications ◦ Disable web application scanning
Shadow Brokers Scan	–	–
Spectre and Meltdown	–	–
WannaCry Ransomware	–	–
Compliance		
Audit Cloud Infrastructure	–	–
Internal PCI Network Scan	**Default**	• General Settings: ◦ Avoid false alarms ◦ Disable CGI scanning • Web Applications: ◦ Disable web application scanning
	Scan for known web vulnerabilities	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning

		• Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Generic web application tests disabled
	Scan for all web vulnerabilities (quick)	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 5 minutes (max)
	Scan for all web vulnerabilities (complex)	• General Settings: ◦ Avoid potential false alarms

		◦ Enable CGI scanning ◦ Perform thorough tests • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 10 minutes (max) ◦ Try all HTTP methods ◦ Attempt HTTP Parameter Pollution
	Custom	All defaults
MDM Config Audit	–	–
Offline Config Audit	–	–
PCI Quarterly External Scan	–	–
Policy Compliance Auditing	–	–
SCAP and OVAL Auditing	–	–

Report Scan Settings

The **Report** scan settings include the following groups of settings:

- Processing
- Output

Setting	Default Value	Description
Processing		
Override normal verbosity	Disabled	When disabled, provides the standard level of plugin activity in the report. The output does not include the informational plugins 56310, 64582, and 58651. When enabled, this setting has two options: • **I have limited disk space. Report as little information as possible** — Provides less information about plugin activity in the report to minimize impact on disk space. • **Report as much information as possible** — Provides more information about plugin activity in the report. When this option is selected, the output includes the informational plugins 56310, 64582, and 58651.
Show missing patches that have been superseded	Enabled	When enabled, includes superseded patch information in the scan report.
Hide results from plugins initiated as a dependency	Enabled	When enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disable this setting.
Output		
Allow users to edit scan	Enabled	When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other

Setting	Default Value	Description
results		types of audits, disable the setting to show that the scan was not tampered with.
Designate hosts by their DNS name	Disabled	Uses the host name rather than IP address for report output.
Display hosts that respond to ping	Disabled	Reports hosts that successfully respond to a ping.
Display unreachable hosts	Disabled	When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.
Display Unicode characters	Disabled	When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. **Note:** Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.

Advanced Scan Settings

Note: If a scan is based on a policy, you cannot configure **Advanced** settings in the scan. You can only modify these settings in the related policy.

The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

Certain Tenable-provided scanner templates include preconfigured advanced settings.

If you select the **Custom** preconfigured setting option, or if you are using a Nessus Scanner template that does not include preconfigured advanced settings, you can manually configure **Advanced** settings in the following categories:

- General Settings
- Performance
- Unix Find Command Exclusions
- Agent Performance (Agent scans only)
- Windows File Search Options
- Debug Settings
- Stagger Scan Start
- Compliance Output Options
- Vulnerability Options
- Web App Template Advanced Settings

Note: The following tables include settings for the **Advanced Scan** template. Depending on the template you select, certain settings may not be available, and default values may vary.

Setting	Default Value	Description
General Settings		
Enable Safe Checks	Enabled	When enabled, disables all plugins that may have an adverse effect on the remote host.
Stop scanning hosts that become unresponsive during the scan	Disabled	When enabled, Tenable Nessus stops scanning if it detects that the host has become unresponsive. This may occur if users turn off their PCs during a scan, a host has stopped responding after a denial of service plugin, or a security mechanism (for example, an IDS) has started to block traffic to a server. Normally, continuing scans on these machines sends unnecessary traffic across the network and delay the

Setting	Default Value	Description
		scan.
Scan IP addresses in a random order	Disabled	By default, Tenable Nessus scans a list of IP addresses in sequential order. When this option is enabled, Tenable Nessus scans the list of hosts in a random order within an IP address range. This approach is typically useful in helping to distribute the network traffic during large scans.
Automatically accept detected SSH disclaimer prompts	Disabled	When enabled, if a credentialed scan tries to connect via SSH to a host that presents a disclaimer prompt, the scanner provides the necessary text input to accept the disclaimer prompt and continue the scan. When disabled, credentialed scans on hosts that present a disclaimer prompt fail because the scanner cannot connect to the device and accept the disclaimer. The error appears in the plugin output.
Scan targets with multiple domain names in parallel	Disabled	When disabled, to avoid overwhelming a host, Tenable Nessus prevents against simultaneously scanning multiple targets that resolve to a single IP address. Instead, Tenable Nessus scanners serialize attempts to scan the IP address, whether it appears more than once in the same scan task or in multiple scan tasks on that scanner. Scans may take longer to complete. When enabled, a Tenable Nessus scanner can simultaneously scan multiple targets that resolve to a single IP address within a single scan task or across multiple scan tasks. Scans complete more quickly, but hosts could potentially become overwhelmed, causing timeouts and incomplete results.
Trusted CAs	none	Determines the certificate authorities (CAs) that Tenable Nessus allows for the scan. In the **Trusted CAs**

Setting	Default Value	Description
		box, enter the text of your CA or CAs. **Note:** Include the beginning text `-----BEGIN CERTIFICATE-----` and ending text `-----END CERTIFICATE-----`. **Tip:** You can save more than one certificate in a single text file, including the beginning and ending text for each one. You can also determine trusted CAs at the scanner level. For more information, see Trust a Custom CA.
Performance		
Slow down the scan when network congestion is detected	Disabled	When enabled, Tenable detects when it is sending too many packets and the network pipe is approaching capacity. If network congestion is detected, throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Tenable automatically attempts to use the available space within the network pipe again.
Network timeout (in seconds)	5	Specifies the time that Tenable waits for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may want to set this to a higher number of seconds.
Max simultaneous checks per host	5	Specifies the maximum number of checks a Tenable scanner will perform against a single host at one time.
Max simultaneous hosts per scan	30, or the Tenable Nessus scanner advanced setting **max_**	Specifies the maximum number of hosts that a scanner scans at the same time. If you set **Max simultaneous hosts per scan** to more than scanner's **max_hosts** setting, Nessus caps **Max simultaneous hosts per scan** at the **max_hosts** value.

Setting	Default Value	Description
	hosts value, whichever is smaller.	For example, if you set the **Max simultaneous hosts per scan** to 150 and scanner's **max_hosts** is set to 100, with more than 100 targets, Nessus scans 100 hosts simultaneously.
Max number of concurrent TCP sessions per host	none	Specifies the maximum number of established TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner sends, which is 10 times the number of TCP sessions. For example, if this option is set to 15, the SYN scanner sends 150 packets per second at most.
Max number of concurrent TCP sessions per scan	none	Specifies the maximum number of established TCP sessions the entire scan, regardless of the number of hosts being scanned. **Note:** The `MAX NUMBER OF CONCURRENT TCP SESSIONS PER SCAN` setting is not enforceable in a Discovery scan. The `global.max_simult_tcp_sessions` Nessus Engine setting (that you set on each scanner) is an absolute cap that applies across all running scans on a scanner. (For example, if you have four scanners and do not want them to generate more than 10000 simultaneous TCP sessions in total at any point in time, you can set that global setting to 2500 for each individual scanner.)
Max scan time per host	Disabled	Determines the maximum number of minutes that Tenable Nessus scans a single target. The range of valid values is integers 1-2,147,483,647. When the setting is disabled or null, there is no time limit on how long Tenable Nessus scans a single target. If Tenable Nessus reaches the maximum scan time, Tenable Nessus ends the scan or, if applicable, moves on to the next scan target. No scan results are

Setting	Default Value	Description
		produced for the target that timed out.
Unix Find Command Options		
Command Timeout	240	The maximum number of seconds the find command is allowed to run on Unix systems. Not all **Find** commands use this timeout. **Note:** For all **Find** command executions in the plugin to complete, and to prevent the plugin from timing out, its plugin timeout should be adjusted with `timeout_<plugin ID>` in the scanner's **Advanced Settings**,
Exclude Filepath	none	A plain text file containing a list of filepaths to exclude from all plugins that search using the `find` command on Unix systems. In the file, enter one filepath per line, formatted per patterns allowed by the Unix `find` command `-path` argument. For more information, see the `find` command man page.
Exclude Filesystem	none	A plain text file containing a list of filesystems to exclude from all plugins that search using the `find` command on Unix systems. In the file, enter one filesystem per line, using filesystem types supported by the Unix `find` command `-fstype` argument. For more information, see the `find` command man page.
Include Filepath	none	A plain text file containing a list of filepaths to include from all plugins that search using the `find` command on Unix systems. In the file, enter one filepath per line, formatted per patterns allowed by the Unix `find` command `-path` argument. For more information, see the `find`

Setting	Default Value	Description
		command man page. Including filepaths increases the locations that are searched by plugins, which extends the duration of the scan. Make your inclusions as specific as possible. **Tip:** Avoid having the same filepaths in **Include Filepath** and **Exclude Filepath**. This conflict may result in the filepath being excluded from the search, though results may vary by operating system.
Agent Performance Options		
Use Tenable supplied binaries for 'find' and 'unzip'	Disabled	When enabled, instead of running native operating system commands of `find` and `unzip`, plugins use binaries included within the plugin feed for agent-based scanning. This allows CPU consumption to be controlled for the Tenable Agent `find` command. Another benefit to enabling this setting is that if `find` or `unzip` are not found natively on the operating system, using the commands from the feed allows full plugin execution with these commands to continue. This setting works in tandem with the Scan Performance setting, which you can set locally on the agent. If you enable this setting and have adjusted the **Scan Performance** to a setting other than the default (**High**), the resulting scan findings may be different than previous scans with the same configuration. This is because the scan may experience timeouts in finding files due to the lower CPU resources. **Note:** Due to the need for thorough and complete results, audits do not leverage the `find` or `unzip` binaries from the Tenable feed.

Setting	Default Value	Description
		Note: With this setting enabled, CPU usage may spike up or close to 100% when the plugin requests a batch of results to process. The CPU then drops down to a lower level until the next batch is requested for processing.
Windows File Search Options		
Windows Exclude Filepath	none	A plain text file containing a list of filepaths to exclude from all plugins that search using Tenable's unmanaged software directory scans. In the file, enter one absolute or partial filepath per line, formatted as the literal strings you want to exclude. You can include absolute or relative directory names, examples such as `E:\`, `E:\Testdir\`, and `\Testdir\`. **Tip:** The default exclusion paths include `\Windows\WinSxS\` and `\Windows\servicing\` if you do not configure this setting. If you configure this setting, Tenable recommends adding those two paths to the file; those directories are very slow and do not contain unmanaged software.
Windows Include Filepath	none	A plain text file containing a list of filepaths to include from all plugins that search using Tenable's unmanaged software directory scans. In the file, enter one absolute or partial filepath per line, formatted as the literal strings you want to include. You can only include absolute directory names, examples such as `E:\`, `E:\Testdir\`, and `C:\`. **Note:** The **Windows Include Filepath** overrides the default included directory (for example, the C: drive on Windows). Therefore, if you want to include the default directory in addition to other directories, you must list the default directory in an additional filepath line.

Setting	Default Value	Description
		Caution: Avoid having the same filepaths in the **Windows Include Filepath** and **Windows Exclude Filepath** settings. This conflict results in the filepath being excluded from the search.
Debug Settings		
Log scan details	Disabled	Logs the start and finish time for each plugin used during a scan to nessusd.messages.
Enable plugin debugging	Disabled	Attaches available debug logs from plugins to the vulnerability output of this scan.
Audit Trail Verbosity	Default	Controls verbosity of the plugin audit trail. **All audit trail data** includes the reason why plugins were not included in the scan. **Default** uses the audit trail verbosity global setting set in Advanced Settings. For Tenable Nessus scans, the scan uses the advanced setting **Audit Trail Verbosity** (`audit_trail`). For agent scans, the scan uses the advanced setting **Include Audit Trail Data** (`agent_merge_audit_trail`).
Include the KB	Default	Controls whether to include the scan KB, which includes more debugging data, in the scan results. For Tenable Nessus scans, **Default** includes the KB. For agent scans, **Default** uses the global setting **Include KB Data** (`agent_merge_kb`) set in Advanced Settings.
Enumerate launched plugins	Disabled	Shows a list of plugins that Tenable Nessus launched during the scan. You can view the list in scan results under plugin 112154. **Note:** The setting does not function correctly if you disable plugin 112154.

Setting	Default Value	Description
Stagger scan start		
Maximum delay (minutes)	0	(Agents 8.2 and later) If set, each agent in the agent group delays starting the scan for a random number of minutes, up to the specified maximum. Staggered starts can reduce the impact of agents that use a shared resource, such as virtual machine CPU. If the maximum delay you set exceeds your scan window, Tenable shortens your maximum delay to ensure that agents begin scanning at least 30 minutes before the scan window closes.
Compliance Output Settings		
Maximum Compliance Output Length in KB	128,000 KB	Controls the maximum output length for each individual compliance check value that the target returns. If a compliance check value that is greater than this setting's value, Tenable Nessus truncates the result. **Note:** If you notice that your compliance scan processing is slow, Tenable recommends reducing this setting to increase the processing speed.
Maximum Compliance Check Timeout in Seconds	300 seconds	Controls the maximum timeout duration for compliance checks. This setting is used by checks with long run times, especially checks that run commands on remove targets for Windows and Unix audits. This timeout setting overrides all other timeout settings when it is available.
Vulnerability Options		
Scan for unpatched vulnerabilities (no	Disabled	Determines whether the scan searches for unpatched vulnerabilities. This includes CVEs marked as **Will Not Fix** by the related vendor.

Setting	Default Value	Description
patches or mitigations available)		Enabling this setting may increase your overall findings count; each platform and package combination results in an individual plugin. If additional CVEs are found to affect a platform and package combination, the CVEs are added to the existing plugin. **Note:** If you configure a scan to produce findings for unpatched vulnerabilities and then the setting is unchecked, Tenable Nessus remediates unpatched findings in the next scan. Additionally, if multiple scans target the same device and one has enabled findings for unpatched vulnerabilities and another does not, the findings results may vary per scan.
Custom Red Hat Repository Mapping	Disabled, requires you to upload a .json file	Upload a .json file that maps internal custom or mirrored repositories to their official Red Hat repository counterparts. For more information on how this works, see How Red Hat Local Vulnerability Checks Use Repositories To Determine Scope.

Web App Template Advanced Settings

The following sections describe the advanced settings that you can configure in Tenable Nessus Web App scan templates. For more information, see Web Application Scanning in Tenable Nessus.

The **Advanced Settings** options allow you to control the efficiency and performance of the scan.

- General
- HTTP Settings
- Limits
- Screen Settings
- Selenium Settings
- Performance Settings

General

You can configure **General** options in scans and user-defined scan templates based on the **Web App Overview** and **Scan** templates only.

Setting	Default	Description
Target Scan Max Time (HH:MM:SS)	08:00:00	Specifies the maximum duration the scanner runs a scan job runs before stopping, displayed in hours, minutes, and seconds. **Note:** The maximum duration you can set is 99:59:59 (hours: minutes: seconds).
Maximum Queue Time (HH:MM:SS)	08:00:00	Specifies the maximum duration the scan remains in the Queued state, displayed in hours, minutes, and seconds. **Note:** The maximum duration you can set is 48:00:00 (hours: minutes: seconds).
Enable Debug logging for this scan	disabled	Specifies whether the scanner attaches available debug logs from plugins to the vulnerability output of this scan.
Debug Flags	disabled	(Only visible when you enable the **Enable Debug logging for this scan** feature). Allows you to specify key and value pairs, provided by support, for debugging.

HTTP Settings

These settings specify the user-agent you want the scanner to identify and the HTTP response headers you want the scanner to include in requests to the web application.

Setting	Default	Description
Use a different User Agent to identify scanner	disabled	Specifies whether you want the scanner to use a user-agent header other than Chrome when sending an HTTP request.
User Agent	Chrome's	Specifies the name of the user-agent header you want the

	user-agent	scanner to use when sending an HTTP request. You can configure this option only after you select the **Use a different User Agent to identify scanner** check box. By default, Tenable Web App Scanning in Tenable Nessus uses the user-agent that Chrome uses for the operating system and platform that corresponds to your machine's operating system and platform. For more information about Chrome's user-agents, see the *Google Chrome documentation*. **Note:** Not all requests from scanner are guaranteed to have the user-agent sent.
Add Scan ID HTTP Header	disabled	Specifies whether the scanner adds an additional `X-Tenable-Was-Scan-Id` header (set with the scan ID) to all HTTP requests sent to the target, which allows you to identify scan jobs in web server logs and modify your scan configurations to secure your sites.
Custom Headers	none	Specifies the custom headers you want to inject into each HTTP request, in request and response format. You can add additional custom headers by clicking the ⊕ button and typing the values for each additional header. **Note:** If you enter a custom `User-Agent` header, that value overrides the value entered in the **User Agent** setting box.

Limits

You can configure **Limits** options in scans and user-defined scan templates based on the **Web App Overview** and **Scan** templates only.

Setting	Default	Description
Number of URLS to Crawl and Browse	10000	Specifies the maximum number of URLs the scanner attempts to crawl.

Path Directory Depth	10	Specifies the maximum number of sub-directories the scanner crawls. For example, if your target is `www.example.com`, and you want the scanner to crawl `www.example.com/users/myname`, type *2* in the text box.
Page DOM Element Depth	5	Specifies the maximum number of HTML nested element levels the scanner crawls.
Max Response Size	500000	Specifies the maximum load size of a page, in bytes, the scanner analyzes. If the scanner crawls a URL and the response exceeds the limit, the scanner does not analyze the page for vulnerabilities.
Request Direct Limit	1	Specifies the number of redirects the scanner follows before it stops trying to crawl the page.

Screen Settings

You can configure **Screen Settings** options in scans and user-defined scan templates based on the **Web App Overview** and **Scan** templates only.

Setting	Default	Description
Screen Width	1600	Specifies the screen width, in pixels, of the browser embedded in the scanner.
Screen Height	1200	Specifies the screen height, in pixels, of the browser embedded in the scanner.
Ignore Images	disabled	Specifies if the browser embedded in the scanner crawls or ignores images on your target web pages.

Selenium Settings

These settings specify how the scanner behaves when it attempts to authenticate to a web application using your recorded Selenium credentials.

Configure these options if you configured your scan to authenticate to the web application with Selenium credentials. For more information see Credentials.

You can configure **Selenium Settings** options in scans and user-defined scan templates based on the **Web App Overview** and **Scan** templates only.

Setting	Default	Description
Page Rendering Delay	30000	Specifies the time, in milliseconds, the scanner waits for the page to render.
Command Execution Delay	500	Specifies the time, in milliseconds, the scanner waits after processing a command before proceeding to the next command.
Script Completion Delay	5000	Specifies the time, in milliseconds, the scanner waits for all commands to render new content to finish processing.

Performance Settings

Setting	Default	Description
Max Number of Concurrent HTTP Connections	10	Specifies the maximum number of established HTTP sessions allowed for a single host.
Max Number of HTTP Requests Per Second	25	Specifies the maximum number of HTTP requests allowed for a single host for the duration of the scan.
Slow down the scan when network congestion is detected	disabled	Specifies whether the scanner throttles the scan in the event of network congestion.
Network Timeout (In Seconds)	5	Specifies the time, in seconds, the scanner waits for a response from a host before aborting the scan, unless otherwise specified in a plugin.

		If your internet connection is slow, Tenable recommends that you specify a longer wait time.
Browser Timeout (In Seconds)	30	Specifies the time, in seconds, the scanner waits for a response from a browser before aborting the scan, unless otherwise specified in a plugin. If your internet connection is slow, Tenable recommends that you specify a longer wait time.
Timeout Threshold	100	Specifies the number of consecutive timeouts allowed before the scanner aborts the scan.

Preconfigured Advanced Scan Settings

Certain Tenable-provided Nessus Scanner templates include preconfigured advanced settings, described in the following table. The preconfigured advanced settings are determined by both the template and the **Scan Type** that you select.

Template	Scan Type	Preconfigured Settings
Discovery		
Host Discovery	–	**Performance Options** defaults
Vulnerabilities		
Basic Network Scan	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max)

		◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected
	Custom	All defaults
Advanced Scan	–	All defaults
Advanced Dynamic Scan	–	All defaults
Malware Scan	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected

	Custom	All defaults
Mobile Device Scan	–	**Debug Settings** defaults
Web Application Tests	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected
	Custom	All defaults
Credentialed Patch Audit	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout

	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected
	Custom	All defaults
Badlock Detection	–	All defaults
Bash Shellshock Detection	–	All defaults
DROWN Detection	–	All defaults
Intel AMT Security Bypass	–	All defaults
Log4Shell	-	All defaults
Log4Shell Remote Checks	-	All defaults
Log4Shell Vulnerability Ecosystem	-	All defaults
Shadow Brokers Scan	–	All defaults
Spectre and Meltdown	–	All defaults
WannaCry Ransomware	–	All defaults
Compliance		
Audit Cloud Infrastructure	–	**Debug Settings** defaults
Internal PCI Network Scan	**Default** (default)	• Performance options:

		◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected
	Custom	All defaults
MDM Config Audit	–	–
Offline Config Audit	–	**Debug Settings** defaults
PCI Quarterly External Scan	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout
	Scan low	• Performance options:

	bandwidth links	◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected
	Custom	All defaults
Policy Compliance Auditing	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected

	Custom	All defaults
SCAP and OVAL Auditing	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected
	Custom	All defaults

Credentials

When you configure a scan or policy's **Credentials**, you can grant the Tenable Nessus scanner local access to scan the target system without requiring an agent. This can facilitate scanning of a large network to determine local exposures or compliance violations. As noted, some steps of policy creation may be optional. Once created, Tenable Nessus saves the policy with recommended settings.

Tenable Nessus has the ability to log into remote Linux hosts via Secure Shell (SSH); and with Windows hosts, Tenable Nessus uses various Microsoft authentication technologies. Tenable

Nessus also uses the Simple Network Management Protocol (SNMP) to make version and information queries to routers and switches. The scan credentials are stored in `global.db`.

Tip: For information about the encryption strength that Tenable Nessus uses for credentials, see Encryption Strength.

The scan or policy's **Credentials** page allows you to configure the Tenable Nessus scanner to use authentication credentials during scanning. Configuring credentials allows Tenable Nessus to perform a wider variety of checks that result in more accurate scan results.

There are several forms of authentication supported including but not limited to databases, SSH, Windows, network devices, patch management servers, and various plaintext authentication protocols.

In addition to operating system credentials, Tenable Nessus supports other forms of local authentication.

You can manage the following types of credentials in the **Credentials** section of the scan or policy:

- Cloud Services
- Database, which includes MongoDB, Oracle, MySQL, DB2, PostgreSQL, and SQL Server
- Host, which includes Windows logins, SSH, and SNMPv3
- Miscellaneous services, which include VMware, Red Hat Enterprise Virtualization (RHEV), IBM iSeries, Palo Alto Networks PAN-OS, and directory services (ADSI and X.509)
- Mobile Device Management
- Patch Management servers
- Plaintext Authentication mechanisms including FTP, HTTP, POP3, and other services
- Web Authentication Credentials (Web App scan templates only)

Credentialed scans can perform any operation that a local user can perform. The level of scanning depends on the privileges granted to the user account. The more privileges the scanner has via the login account (for example, root or administrator access), the more thorough the scan results.

Note: Tenable Nessus opens several concurrent authenticated connections. Ensure that the host being audited does not have a strict account lockout policy based on concurrent sessions.

If a scan contains multiple instances of one type of credential, Tenable Nessus tries the credentials on each scan target in the order you added the credentials to the scan.

Note: Tenable Nessus uses the first credential that allows successful login to perform credentialed checks on the target. After a credential allows a successful login, Tenable Nessus does not try any of the other credentials in the list, even if a different credential has greater privileges.

Note: If a Tenable Nessus scan contains multiple instances of one type of credential, Tenable Nessus attempts to log into a valid target using each credential in sequence, **in the same order in which they were added to the scan**. Tenable Nessus uses the first credential it is able to log in successfully with to perform credentialed checks on the target. Once Tenable Nessus is able to log in successfully with a credential set, it does not attempt to log in with any of the other credentials in the scan, regardless of their relative levels of access.

Cloud Services Credentials

Tenable Nessus supports Amazon Web Services (AWS), Microsoft Azure, Rackspace, and Salesforce.com.

AWS

Users can select Amazon Web Service (AWS) from the Credentials menu and enter credentials for compliance auditing an account in AWS.

Option	Description
AWS Access Key IDS	The AWS access key ID string.
AWS Secret Key	AWS secret key that provides the authentication for AWS Access Key ID.

AWS Global Credential Settings

Option	Default	Description
Regions to access	Rest of the World	For Tenable Nessus to audit an AWS account, you must define the regions you want to scan. Per Amazon policy, you need different credentials to audit account configuration for the

		China region than you need for the **Rest of the World**. Choosing the **Rest of the World** opens the following choices: • us-east-1 • us-east-2 • us-west-1 • us-west-2 • ca-central-1 • eu-west-1 • eu-west-2 • eu-central-1 • ap-northeast-1 • ap-northeast-2 • ap-southeast-1 • ap-southeast-2 • sa-east-1 • us-gov-west-1
HTTPS	Enabled	Use HTTPS to access AWS.
Verify SSL Certificate	Enabled	Verify the validity of the SSL digital certificate.

Microsoft Azure

There are multiple authentication methods for Microsoft Azure.

Authentication Method: Key

Option	Description	Required
Tenant ID	The Tenant ID or Directory ID for your Azure environment.	Yes
Application ID	The application ID (also known as client ID) for your registered application.	Yes
Client Secret	The secret key for your registered application.	Yes
Subscription IDs	List of subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.	No

Authentication Method: Password

Option	Description	Required
Username	The username required to log in to Microsoft Azure.	Yes
Password	The password associated with the username.	Yes
Client ID	The application ID (also known as client ID) for your registered application.	Yes
Subscription IDs	List of subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.	No

Authentication Method: Certificate

Option	Description	Required
Tenant ID	The Tenant ID or Directory ID for your Azure environment.	Yes
Application ID	The application ID (also known as client ID) for your registered application.	Yes
Private Key	A PEM formatted 2048-bit RSA private key and certificate.	Yes
Config File	Additional configuration parameters. Currently only applicable for SCuBA scans.	No
Subscription IDs	List of subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.	No

Rackspace

Option	Description
Username	Username required to log in.
Password or API Keys	Password or API keys associated with the username.
Authentication Method	Specify Password or API-Key from the drop-down box.
Global Settings	Location of Rackspace Cloud instance.

Salesforce.com

Users can select Salesforce.com from the Credentials menu. This allows Tenable Nessus to log in to Salesforce.com as the specified user to perform compliance audits.

Option	Description
Username	Username required to log in to Salesforce.com
Password	Password associated with the Salesforce.com username

Database Credentials

The following topic describes the available **Database** credentials.

Cassandra

Option	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **CyberArk** • **Lieberman**

Option	Description
	• **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Port	The port the database listens on. The default is port 9042.

Delinea Secret Server Auto-Discovery

Option	Description	Required
Delinea Host	The Delinea Secret Server host to pull the secrets from.	Yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	Yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	Yes
Delinea Login Name	The username to authenticate to the Delinea server.	Yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the provided Delinea Login Name.	Yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the API Key authentication method is selected.	Yes
Query Mode	Choose to query accounts using pre-set fields or by constructing a string of URL query parameters. By default, **Simple** is selected.	Yes
Folder ID	Query accounts with the given folder ID. This option is only available if query mode is set to **Simple**.	No
Search Text	Query accounts matching the given search text. This	No

Option	Description	Required
	option is only available if query mode is set to **Simple**.	
Search Field	The field to search using the given search text. If not specified, the query will search the `name` field. This option is only available if query mode is set to **Simple**.	No
Exact Match	Perform an exact match against the search text. By default, this is unselected. This option is only available if query mode is set to **Simple**.	No
Query String	Provide a string of URL query parameters. This option is only available if query mode is set to **Advanced**, and in that case it is required.	Yes
Use Private Key	Use key-based authentication for SSH connections instead of password authentication.	No
Use SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Verify the Delinea Secret Server SSL certificate.	No

DB2

The following table describes the additional options to configure for **IBM DB2** credentials.

Options	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **Import** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see

Options	Description
	Database Credentials Authentication Types.
Database Port	The TCP port that the IBM DB2 database instance listens on for communications from Tenable Nessus Manager. The default is port 50000.
Database Name	The name for your database (not the name of your instance).

MongoDB

Option	Description
Auth Type	The authentication method for providing the required credentials. **Note:** This option is only available for non-legacy versions of the MongoDB authentication method. • **Password** • **Client Certificate** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Username	(Required) The username for the database.
Password	(Required) The password for the supplied username.
Database	The name of the database to authenticate to. **Tip:** To authenticate via LDAP or saslauthd, type **$external**.
Port	(Required) The TCP port that the MongoDB database instance listens on for communications from Tenable Nessus.

MySQL

The following table describes the additional options to configure for **MySQL** credentials.

Options	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **Import** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Username	The username for a user on the database.
Password	The password associated with the username you provided.
Database Port	The TCP port that the MySQL database instance listens on for communications from Tenable Nessus. The default is port 3306.

Oracle

The following table describes the additional options to configure for **Oracle** credentials.

Options	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **Import** • **CyberArk** • **Lieberman** • **Hashicorp Vault**

Options	Description
	For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Database Port	The TCP port that the Oracle database instance listens on for communications from Tenable Nessus. The default is port 1521.
Auth Type	The type of account you want Tenable Nessus to use to access the database instance: • **Normal** • **System Operator** • **System Database Administrator** • **SYSDBA** • **SYSOPER** • **NORMAL**
Service Type	The Oracle parameter you want to use to specify the database instance: **SID** or **Service NameSERVICE_NAME**.
Service	The SID value or SERVICE_NAME value for your database instance. The **Service** value you enter must match your parameter selection for the **Service Type** option.

PostgreSQL

The following table describes the additional options to configure for **PostgreSQL** credentials.

Options	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **Client Certificate** • **CyberArk**

Options	Description
	• **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Database Port	The TCP port that the PostgreSQL database instance listens on for communications from Tenable Nessus. The default is port 5432.
Database Name	The name for your database instance.

SQL Server

The following table describes the additional options to configure for **SQL Server** credentials.

Options	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **Import** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Username	The username for a user on the database.
Password	The password associated with the username you provided.
Database Port	The TCP port that the SQL Server database instance listens on for communications from Tenable Nessus. The default is port 1433.
AuthType	The type of account you want Tenable Nessus to use to access the database

Options	Description
	instance: **SQL** or **Windows**.
Instance Name	The name for your database instance.

Sybase ASE

The following table describes the additional options to configure for **Sybase ASE** credentials.

Options	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Database Port	The TCP port that the Sybase ASE database instance listens on for communications from Tenable Nessus. The default is port 3638.
Auth Type	The type of authentication used by the Sybase ASE database: **RSA** or **Plain Text**.

Database Credentials Authentication Types

Depending on the authentication type you select for your database credentials, you must configure the options described in this topic.

Client Certificate

The **Client Certificate** authentication type is supported for **PostgreSQL** databases only.

Option	Description	Required
Username	The username for the database.	yes
Client Certificate	The file that contains the PEM certificate for the database.	yes
Client CA Certificate	The file that contains the PEM certificate for the database.	yes
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes
Client Certificate Private Key Passphrase	The passphrase for the private key, if required in your authentication implementation.	no
Database Port	The port on which Tenable Nessus communicates with the database.	yes
Database Name	The name of the database.	no

Password

Option	Database Types	Description	Required
Username	All	The username for a user on the database.	yes
Password	All	The password for the supplied username.	no
Database Port	All	The port on which Tenable Nessus communicates with the database.	yes
Database Name	DB2 PostgreSQL	The name of the database.	no
Auth type	Oracle SQL Server Sybase ASE	SQL Server values include: • Windows • SQL	yes

Option	Database Types	Description	Required
		Oracle values include: • SYSDBA • SYSOPER • NORMAL Sybase ASE values include: • RSA • Plain Text	
Instance name	SQL Server	The name for your database instance.	no
Service type	Oracle	Valid values include: • SID • SERVICE_NAME	yes
Service	Oracle	The SID value for your database instance or a SERVICE_NAME value. The **Service** value you enter must match your parameter selection for the **Service Type** option.	no

Import

Upload a `.csv` file with the credentials entered in the specified format. For descriptions of valid values to use for each item, see Database Credentials.

You must configure either CyberArk or HashiCorp credentials for a database credential in the same scan so that Tenable Nessus can retrieve the credentials.

Database Credential	CSV Format
DB2	`target, port, database_name, username, cred_manager, accountname_or_secretname`
MySQL	`target, port, database_name, username, cred_manager, accountname_or_secretname`
Oracle	`target, port, service_type, service_ID, username, auth_type, cred_manager, accountname_or_secretname`
SQL Server	`target, port, instance_name, username, auth_type, cred_manager, accountname_or_secretname`

Note: Include the required data in the specified order, with commas between each value, without spaces. For example, for Oracle with CyberArk: `192.0.2.255,1521,SID,`*`service_id`*`,`*`username`*`,SYSDBA,CyberArk,Database-Oracle-SYS`.

Note: The value for `cred_manager` must be either *CyberArk* or *HashiCorp*.

BeyondTrust

Option	Description	Required
Username	The username to log in to the host you want to scan.	yes
Domain	The domain of the username, which is recommended if using domain-linked accounts (managed accounts of a domain that are linked to a managed system).	no
BeyondTrust host	The BeyondTrust IP address or DNS address.	yes
BeyondTrust port	The port on which BeyondTrust listens.	yes
BeyondTrust API user	The API user provided by BeyondTrust.	yes
BeyondTrust API key	The API key provided by BeyondTrust.	yes

Checkout duration	The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the checkout duration to exceed the typical duration of your scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your scans. If BeyondTrust changes a password during a scan, the scan fails.	yes
Use SSL	When enabled, the integration uses SSL through IIS for secure communications. Configure SSL through IIS in BeyondTrust before enabling this option. **Caution:** If you do not enable this option the traffic that is sent is http and will not be accepted by the Beyond Trust server.	no
Verify SSL certificate	When enabled, the intergation validates the SSL certificate. Configure SSL through IIS in BeyondTrust before enabling this option.	no

CyberArk

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable Nessus can get credentials from CyberArk to use in a scan.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web Service. This can be the host, or the host with a custom URL added on in a single string.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk	yes

Option	Description	Required
	API connection.	
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Address**, **Identifier**, **Parameters**, or **Username**. **Note:** For more information about the **Parameters** option, refer to the **Parameters Options** table. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier.	yes
Username	(If **Get credential by** is set to **Username**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no

Option	Description	Required
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	no
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no

CyberArk (Legacy)

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable Nessus can get credentials from CyberArk to use in a scan.

Option	Database Types	Description	Required
Username	All	The target system's username.	yes
Central Credential Provider Host	All	The CyberArk Central Credential Provider IP/DNS address.	yes
Central Credential Provider Port	All	The port on which the CyberArk Central Credential Provider is listening.	yes
CyberArk AIM Service URL	All	The URL of the AIM service. By default, this field uses `/AIMWebservice/v1.1/AIM.asmx`.	no
Central Credential Provider Username	All	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.	no
Central Credential Provider	All	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field	no

Option	Database Types	Description	Required
Password		for authentication.	
CyberArk Safe	All	The safe on the CyberArk Central Credential Provider server that contained the authentication information you would like to retrieve.	no
CyberArk Client Certificate	All	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
CyberArk Client Certificate Private Key	All	The file that contains the PEM private key for the client certificate.	no
CyberArk Client Certificate Private Key Passphrase	All	The passphrase for the private key, if your authentication implementation requires it.	no
CyberArk AppId	All	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.	yes
CyberArk Folder	All	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.	no
CyberArk Account Details Name	All	The unique name of the credential you want to retrieve from CyberArk.	yes

Option	Database Types	Description	Required
PolicyId	All	The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.	no
Use SSL	All	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.	no
Verify SSL Certificate	All	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate, select this option. Refer to the custom_CA.inc documentation for how to use self-signed certificates.	no
Database Port	All	The port on which Tenable Nessus communicates with the database.	yes
Database Name	DB2 PostgreSQL	The name of the database.	no
Auth type	Oracle SQL Server Sybase ASE	SQL Server values include: • Windows • SQL Oracle values include: • **Normal** • **System Operator** • **System Database Administrator** • **SYSDBA** • **SYSOPER**	yes

Option	Database Types	Description	Required
		• **NORMAL** Sybase ASE values include: • RSA • Plain Text	
Instance Name	SQL Server	The name for your database instance.	no
Service type	Oracle	Valid values include: • SID • SERVICE_NAME	yes
Service	Oracle	The SID value for your database instance or a SERVICE_NAME value. The **Service** value you enter must match your parameter selection for the **Service Type** option.	no

Delinea

Option	Description	Required
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled Secret Name on the Delinea server.	yes
Delinea Host	The Delinea Secret Server IP address or DNS address.	yes
Delinea Port	The port on which Delinea Secret Server listens.	yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, credentials are selected.	yes

Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API key	The API key provided by Delinea Secret Server.	yes
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL certificate	If enabled, verifies the SSL Certificate on the Delinea server.	no

Delinea Auto Discovery

Option	Description	Required
Delinea Host	The Delinea Secret Server host to pull the secrets from.	Yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	Yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	Yes
Delinea Login Name	The username to authenticate to the Delinea server.	Yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the provided Delinea Login Name.	Yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the API Key authentication method is selected.	Yes
Query Mode	Choose to query accounts using pre-set fields or by constructing a string of URL query parameters. By default, **Simple** is selected.	Yes

Option	Description	Required
Folder ID	Query accounts with the given folder ID. This option is only available if query mode is set to **Simple**.	No
Search Text	Query accounts matching the given search text. This option is only available if query mode is set to **Simple**.	No
Search Field	The field to search using the given search text. If not specified, the query will search the `name` field. This option is only available if query mode is set to **Simple**.	No
Exact Match	Perform an exact match against the search text. By default, this is unselected. This option is only available if query mode is set to **Simple**.	No
Query String	Provide a string of URL query parameters. This option is only available if query mode is set to **Advanced**, and in that case it is required.	Yes
Use Private Key	Use key-based authentication for SSH connections instead of password authentication.	No
Use SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Verify the Delinea Secret Server SSL certificate.	No

HashiCorp Vault

HashiCorp Vault is a popular enterprise password vault that helps you manage privileged credentials. Tenable Nessus can get credentials from HashiCorp Vault to use in a scan.

Option	Description	Required
Hashicorp Vault host	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes

Hashicorp Vault port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate** and **Hashicorp Client Certificate Private Key** appear. Select the appropriate files for the client certificate and private key.	yes
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The path/subdirectory to the authentication endpoint. This is not the full URL. For example: `/v1/auth/approle/login`	yes
Namespace	The name of a specified team in a multi-team environment.	no
Vault Type	The Tenable Nessus version: KV1, KV2, AD, or LDAP. For additional information about Tenable Nessus versions, see the Tenable Nessus documentation.	yes
KV1 Engine URL	(KV1) The URL Tenable Nessus uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL Tenable Nessus uses to access the KV2 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL Tenable Nessus uses to access the	yes, if you

	active directory engine. Example: `/v1/path_to_secret`. No trailing `/`	select the AD **Vault Type**
LDAP Engine URL	(LDAP) The URL Tenable Nessus uses to access the LDAP engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the LDAP **Vault Type**
Username Source	(KV1 and KV2) A drop-down box to specify whether the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(KV1 and KV2) The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	(KV1 and KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	(KV1, KV2, and AD) The key secret you want to retrieve values for.	yes
Use SSL	If enabled, Tenable Nessus Manager uses SSL for secure communications. Configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no
Database Port	The port on which Tenable Nessus Manager communicates with the database.	yes
Auth Type	The authentication method for the database credentials. Oracle values include: • SYSDBA • SYSOPER	yes

	• NORMAL	
Service Type	(Oracle databases only) Valid values include: SID and SERVICE_NAME.	yes
Service	(Oracle database only) A specific field for the configuration for the database.	yes

Lieberman

Lieberman is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from Lieberman to use in a scan.

Option	Database Type	Description	Required
Username	All	The target system's username.	yes
Lieberman host	All	The Lieberman IP/DNS address. **Note:** If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Lieberman port	All	The port on which Lieberman listens.	yes
Lieberman API URL	All	The URL Tenable Nessus uses to access Lieberman.	no
Lieberman user	All	The Lieberman explicit user for authenticating to the Lieberman API.	yes
Lieberman password	All	The password for the Lieberman explicit user.	yes
Lieberman Authenticator	All	The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman. **Note:** If you use this option, append a	no

Option	Database Type	Description	Required
		domain to the **Lieberman user** option, i.e., *domain\user*.	
Lieberman Client Certificate	All	The file that contains the PEM certificate used to communicate with the Lieberman host. **Note:** If you use this option, you do not have to enter information in the **Lieberman user**, **Lieberman password**, and **Lieberman Authenticator** fields.	no
Lieberman Client Certificate Private Key	All	The file that contains the PEM private key for the client certificate.	no
Lieberman Client Certificate Private Key Passphrase	All	The passphrase for the private key, if required.	no
Use SSL	All	If Lieberman is configured to support SSL through IIS, check for secure communication.	no
Verify SSL Certificate	All	If Lieberman is configured to support SSL through IIS and you want to validate the certificate, check this option. Refer to Custom CA documentation for how to use self-signed certificates.	no
System Name	All	In the rare case your organization uses one default Lieberman entry for all managed systems, enter the default entry name.	no

Option	Database Type	Description	Required
Database Port	All	The port on which Tenable Nessus communicates with the database.	yes
Database Name	DB2 PostgreSQL	(PostgreSQL and DB2 databases only) The name of the database.	no
Auth type	Oracle SQL Server Sybase ASE	(SQL Server, Oracle. and Sybase ASE databases only) SQL Server values include: • Windows • SQL Oracle values include: • SYSDBA • SYSOPER • NORMAL Sybase ASE values include: • RSA • Plain Text	yes
Instance Name	SQL Server	The name for your database instance.	no
Service type	Oracle	Valid values include: • SID • SERVICE_NAME	no
Service	Oracle	The SID value for your database instance or a SERVICE_NAME value. The **Service** value you enter must match your parameter selection for the **Service Type** option.	yes

QiAnXin

QiAnXin is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from QiAnXin to use in a scan.

Option	Description	Required
QiAnXin Host	The IP address or URL for the QiAnXin host.	yes
QiAnXin Port	The port on which the QiAnXin API communicates. By default, Tenable uses 443.	yes
QiAnXin API Client ID	The Client ID for the embedded account application created in QiAnXin PAM	yes
QiAnXin API Secret ID	The Secret ID for the embedded account application created in QiAnXin PAM	yes
Username	The username to log in to the hosts you want to scan.	yes
Host IP	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on credential type (for example, for Windows credentials, the default is WINDOWS). Possible values: • **ACTIVE_DIRECTORY** — Windows Domain Account • **WINDOWS** — Windows Local Account • **LINUX** — Linux Account • **SQL_SERVER** — SQL Server Database • **ORACLE** — Oracle Database	no

Option	Description	Required
	• **MYSQL** — MySQL Database • **DB2** — DB2 Database • **HP_UNIX** — HP Unix • **SOLARIS** — Solaris • **OPENLDAP** — OpenLDAP • **POSTGRESQL** — PostgreSQL	
Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no

Senhasegura

Option	Description	Required
Senhasegura Host	The IP address or URL for the Senhasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Tenable uses 443.	yes
Senhasegura API Client ID	The Client ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Secret ID	The Secret ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes

Option	Description	Required
Senhasegura Credential ID or Identifier	The credential ID or identifier for the credential you are requesting to retrieve.	yes
Private Key File	The Private Key used to decrypt encrypted sensitive data from A2A. **Note:** You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, you must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Senhasegura.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
HTTPS	This is enabled by default.	yes
Verify SSL Certificate	This is disabled by default.	no

Host Credentials

Tenable Nessus supports the following forms of host authentication:

SNMPv3

Users can select SNMPv3 settings from the **Credentials** menu and enter credentials for scanning systems using an encrypted network management protocol.

Use these credentials to obtain local information from remote systems, including network devices, for patch auditing or compliance checks.

There is a field for entering the SNMPv3 username for the account that performs the checks on the target system, along with the SNMPv3 port, security level, authentication algorithm and password, and privacy algorithm and password.

If Nessus is unable to determine the community string or password, it may not perform a full audit of the service.

Note: You cannot configure SNMPv3 settings for the **Basic Network Scan** template.

Option	Description	Default
Username	(Required) The username for the SNMPv3 account that Tenable Nessus uses to perform checks on the target system.	-
Port	The TCP port that SNMPv3 listens on for communications from Tenable Nessus.	161
Security level	The security level for SNMP: • **No authentication and no privacy** • **Authentication without privacy** • **Authentication and privacy**	Authentication and privacy
Authentication algorithm	The algorithm the remove service supports: **SHA1**, **SHA224**, **SHA-256**, **SHA-384**, **SHA-512** or **MD5**.	SHA1
Authentication password	(Required) The password associated with the **Username**.	-
Privacy algorithm	The encryption algorithm to use for SNMP traffic: **AES**, **AES-192**, **AES-192C**, **AES-256**, **AES-256C**, or **DES**.	AES-192
Privacy password	(Required) A password used to protect encrypted SNMP communication.	-

SSH

Use SSH credentials for host-based checks on Unix systems and supported network devices. Tenable Nessus uses these credentials to obtain local information from remote Unix systems for patch auditing or compliance checks. Tenable Nessus uses Secure Shell (SSH) protocol version 2 based programs (e.g., OpenSSH, Solaris SSH, etc.) for host-based checks.

Tenable Nessus encrypts the data to protect it from being viewed by sniffer programs.

Tip: For information about supported key exchange (KEX) algorithms, see Credentialed Checks on Linux.

Note: Non-privileged users with local access on Linux systems can determine basic security issues, such as patch levels or entries in the `/etc/passwd` file. For more comprehensive information, such as system configuration data or file permissions across the entire system, an account with root privileges is required.

Note: You can add up to 1,000 SSH credentials in a single scan. For best performance, Tenable recommends adding no more than 10 SSH credentials per scan.

See the following settings for the different SSH authentication methods:

Global Credential Settings

There are four settings for SSH credentials that apply to all SSH Authentication methods.

Option	Default Value	Description
known_hosts file	none	If an SSH `known_hosts` file is available and provided as part of the **Global Credential Settings** of the scan policy in the **known_hosts file** field, Tenable Nessus attempts to log into hosts in this file. This can ensure that someone does not use the same username and password you are using to audit your known SSH servers to attempt a log into a system that may not be under your control.
Preferred port	22	You can set this option to direct Tenable Nessus to connect to SSH if it is running on a port other than 22.
Client version	OpenSSH_5.0	Specifies which type of SSH client Tenable Nessus impersonates while scanning.
Attempt least privilege	Cleared	Enables or disables dynamic privilege escalation. When enabled, Tenable Nessus attempts to run the scan with an account with lesser privileges, even if you enable the **Elevate privileges with**option. If a command fails, Tenable Nessus escalates privileges. Plugins 102095 and 102094 report which plugins ran with or without escalated privileges. **Note:** Enabling this option may increase scan run time by up to

Option	Default Value	Description
		30%.

Certificate

Option	Description
Username	Username of the account which is being used for authentication on the host system.
User Certificate	RSA or DSA certificate file of the user.
Private Key	RSA, DSA, ECDSA, or ED25519 OpenSSH private key of the user.
Private key passphrase	Passphrase of the private key.
Elevate privileges with	Allows for increasing privileges once authenticated.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

CyberArk (Tenable Nessus Manager only)

Tip: To view whether your Cyberark credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable Nessus Manager can get credentials from CyberArk to use in a scan.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web Service.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk API connection.	yes
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations.	no

Option	Description	Required
	For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target (for example, example.com). By default, Tenable Nessus uses 443.	yes
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Address**, **Identifier**, **Parameters**, or **Username**. **Note:** For more information about the **Parameters** option, refer to the **Parameters Options** table. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier.	yes
Username	(If **Get credential by** is set to **Username**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Address	The option should only be used if the Address value is unique to a single CyberArk account credential.	no
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is	no

Option	Description	Required
	configured to support SSL through IIS.	
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	no

CyberArk Auto-Discovery (Tenable Nessus Manager only)

Tip: To view whether your Cyberark credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

You can now take advantage of a significant improvement to Tenable's CyberArk Integration which gathers bulk account information for specific target groups without entering multiple targets.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the user's CyberArk Instance. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes

Option	Description	Required
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
AppID	The Application ID associated with the CyberArk API connection.	yes
Safe	Users may optionally specify a Safe to gather account information and request passwords.	no
AIM Web Service Authentication Type	There are two authentication methods established in the feature. **IIS Basic Authentication** and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	yes
CyberArk PVWA Web UI Login Name	Username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk PVWA Web UI Login Password	Password for the username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes

Option	Description	Required
CyberArk Platform Search String	String used in the PVWA REST API query parameters to gather bulk account information. For example, the user can enter `UnixSSH Admin TestSafe`, to gather all UnixSSH platform accounts containing a username `Admin` in a Safe called `TestSafe`. **Note:** This is a non-exact keyword search. A best practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	yes
Elevate Privileges with	Users can only select Nothing or sudo at this time.	no
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	yes
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	no

CyberArk (Legacy) (Tenable Nessus Manager only)

Tip: To view whether your Cyberark credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

The following is the legacy CyberArk authentication method.

Option	Description
Username	The target system's username.
CyberArk AIM Service URL	The URL of the AIM service. By default, this field uses `/AIMWebservice/v1.1/AIM.asmx`.
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.
Central Credential Provider Port	The port on which the CyberArk Central Credential Provider is listening.
Central Credential Provider Username	If you configured the CyberArk Central Credential Provider to use basic authentication, you can fill in this field for authentication.
Central Credential Provider Password	If you configured the CyberArk Central Credential Provider to use basic authentication, you can fill in this field for authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contained the authentication information you would like to retrieve.
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.
CyberArk Client	The file that contains the PEM private key for the client certificate.

Option	Description
Certificate Private Key	
CyberArk Client Certificate Private Key Passphrase	(Optional) The passphrase for the private key, if required.
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.
PolicyId	The PolicyID assigned to the credentials you would like to retrieve from the CyberArk Central Credential Provider.
Use SSL	If you configured the CyberArk Central Credential Provider to support SSL through IIS, select this for secure communication.
Verify SSL Certificate	Select this if you configured CyberArk Central Credential Provider to support SSL through IIS and you want to validate the certificate. Refer to the custom_CA.inc documentation for how to use self-signed certificates.
CyberArk Account Details Name	The unique name of the credential you want to retrieve from CyberArk.
CyberArk Address	The domain for the user account.
CyberArk Elevate Privileges With	The privilege escalation method you want to use to increase the user's privileges after initial authentication. Your selection determines the specific options you must configure.

DelineaSSH Authentication Method: Delinea

Tip: To view whether your Delinea credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the **API Key** authentication method is selected.	yes
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled **Secret Name** on the Delinea server.	yes
Delinea Host	The Delinea Secret Server host to pull the secrets from.	yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	yes
Use Private Key	If enabled, uses key-based authentication for SSH connections instead of password authentication.	no
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no

KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target.	yes
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL Certificate	If enabled, verifies the SSL Certificate on the Delinea server.	no
Elevate privileges with	The privilege escalation method you want to use to increase users' privileges after initial authentication. Multiple options for privilege escalation are supported, including su, su+sudo and sudo. Your selection determines the specific options you must configure.	no
Custom password prompt	Some devices are configured to prompt for a password with a non-standard string (for example, "secret-passcode"). This setting allows recognition of these prompts. Leave this blank for most standard password prompts.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential	no

	is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	

Delinea Secret Server Auto-Discovery

Tip: To view whether your Delinea credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
Delinea Host	The Delinea Secret Server host to pull the secrets from.	Yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	Yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	Yes
Delinea Login Name	The username to authenticate to the Delinea server.	Yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the provided Delinea Login Name.	Yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the API Key authentication method is selected.	Yes
Query Mode	Choose to query accounts using pre-set fields or by constructing a string of URL query parameters. By default, **Simple** is selected.	Yes
Folder ID	Query accounts with the given folder ID. This option is only available if query mode is set to **Simple**.	No

Option	Description	Required
Search Text	Query accounts matching the given search text. This option is only available if query mode is set to **Simple**.	No
Search Field	The field to search using the given search text. If not specified, the query will search the `name` field. This option is only available if query mode is set to **Simple**.	No
Exact Match	Perform an exact match against the search text. By default, this is unselected. This option is only available if query mode is set to **Simple**.	No
Query String	Provide a string of URL query parameters. This option is only available if query mode is set to **Advanced**, and in that case it is required.	Yes
Use Private Key	Use key-based authentication for SSH connections instead of password authentication.	No
Use SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Verify the Delinea Secret Server SSL certificate.	No
Delinea Elevate Privileges With	The privilege escalation method to use to increase users' privileges after initial authentication. Multiple options for privilege escalation are supported, including su, su+sudo and sudo. Selecting a privilege escalation method provides options to configure an escalation query, similar to “query mode” and its related options. These fields must only be completed if using a separate account for escalation than initial login (for example, “su”).	Yes

Kerberos

Kerberos, developed by MIT’s Project Athena, is a client/server application that uses a symmetric key encryption protocol. In symmetric encryption, the key used to encrypt the data is the same as

the key used to decrypt the data. Organizations deploy a KDC (Key Distribution Center) that contains all users and services that require Kerberos authentication. Users authenticate to Kerberos by requesting a TGT (Ticket Granting Ticket). Once you grant a user a TGT, the user can use it to request service tickets from the KDC to be able to utilize other Kerberos based services. Kerberos uses the CBC (Cipher Block Chain) DES encryption protocol to encrypt all communications.

Note: You must already have a Kerberos environment established to use this method of authentication.

The Tenable Nessus implementation of Linux-based Kerberos authentication for SSH supports the aes-cbc and aes-ctr encryption algorithms. An overview of how Tenable Nessus interacts with Kerberos is as follows:

- End user gives the IP of the KDC
- `nessusd` asks `sshd` if it supports Kerberos authentication
- `sshd` says yes
- `nessusd` requests a Kerberos TGT, along with login and password
- Kerberos sends a ticket back to `nessusd`
- `nessusd` gives the ticket to `sshd`
- `nessusd` is logged in

In both Windows and SSH credentials settings, you can specify credentials using Kerberos keys from a remote system. There are differences in the configurations for Windows and SSH.

Option	Description
Username	The target system's username.
Password	Password of the username specified.
Key Distribution Center (KDC)	This host supplies the session tickets for the user.
KDC Port	You can set this option to direct Tenable Nessus to connect to the KDC if it is running on a port other than 88.

Option	Description
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.
Realm	The Realm is the authentication domain, usually noted as the domain name of the target (for example, example.com).
Elevate privileges with	Allows for increasing privileges once authenticated.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

If Kerberos is used, you must configure sshd with Kerberos support to verify the ticket with the KDC. You must configure reverse DNS lookups properly for this to work. The Kerberos interaction method must be gssapi-with-mic.

Password

Option	Description
Username	The target system's username.
Password	Password of the username specified.
Elevate privileges with	Allows for increasing privileges once authenticated.

Option	Description
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Vulnerability Management receiving an unrecognized password prompt on the target host's interactive SSH shell.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

Public Key

Public Key Encryption, also referred to as asymmetric key encryption, provides a more secure authentication mechanism by the use of a public and private key pair. In asymmetric cryptography, Tenable Nessus uses the public key to encrypt data and Tenable Nessus uses the private key to decrypt it. The use of public and private keys is a more secure and flexible method for SSH authentication. Tenable Nessus supports both DSA and RSA key formats.

Like Public Key Encryption, Tenable Nessus supports RSA and DSA OpenSSH certificates. Tenable Nessus also requires the user certificate, which is signed by a Certificate Authority (CA), and the user's private key.

Note: Tenable Nessus supports the `openssh` SSH public key format (pre-7.8 OpenSSH). Tenable Nessus does not support the new `OPENSSH` format (OpenSSH versions 7.8+). To check which version you have, check your private key contents. `openssh` shows **-----BEGIN RSA PRIVATE KEY-----** or **-----BEGIN DSA PRIVATE KEY-----**, and the new, incompatible `OPENSSH` shows **-----BEGIN OPENSSH PRIVATE KEY-----**. You must convert non-`openssh` formats, including PuTTY and SSH Communications Security, to the `openssh` public key format.

The most effective credentialed scans are when the supplied credentials have root privileges. Since many sites do not permit a remote login as root, Tenable Nessus can invoke su, sudo, su+sudo, dzdo, .k5login, or pbrun with a separate password for an account that you set up to have su or sudo privileges. In addition, Tenable Nessus can escalate privileges on Cisco devices by selecting Cisco 'enable' or .k5login for Kerberos logins.

Note: Tenable Nessus supports the blowfish-cbc, aes-cbc, and aes-ctr cipher algorithms. Some commercial variants of SSH do not have support for the blowfish algorithm, possibly for export reasons. It is also possible to configure an SSH server to accept certain types of encryption only. Check your SSH server to ensure that it supports the correct algorithm.

Tenable Nessus encrypts all passwords stored in policies. However, Tenable recommends using SSH keys for authentication rather than SSH passwords. This helps ensure that someone does not use the same username and password you are using to audit your known SSH servers to attempt a log into a system that may not be under your control.

Note: For supported network devices, Tenable Nessus only supports the network device's username and password for SSH connections.

If you have to use an account other than root for privilege escalation, you can specify it under the Escalation account with the Escalation password.

Option	Description
Username	Username of the account which is being used for authentication on the host system.
Private Key	RSA, DSA, ECDSA, or ED25519 OpenSSH private key of the user.
Private key passphrase	Passphrase of the private key.
Elevate privileges with	Allows for increasing privileges once authenticated.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list.

Option	Description
	Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

QiAnXin (Tenable Nessus Manager only) SSH Authentication Method: QiAnXin

Tip: To view whether your QiAnXin credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
QiAnXin Host	The IP address or url for the QiAnXin host.	yes
QiAnXin Port	The port on which the QiAnXin API communicates. By default, Tenable uses 443.	yes
QiAnXin API Client ID	The Client ID for the embedded account application created in QiAnXin PAM.	yes
QiAnXin API Secret ID	The Secret ID for the embedded account application created in QiAnXin PAM.	yes
Username	The username to log in to the hosts you want to scan.	yes
Host IP	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on	no

Option	Description	Required
	credential type (for example, for Windows credentials, the default is WINDOWS). Possible values: • **ACTIVE_DIRECTORY** — Windows Domain Account • **WINDOWS** — Windows Local Account • **LINUX** — Linux Account • **SQL_SERVER** — SQL Server Database • **ORACLE** — Oracle Database • **MYSQL** — MySQL Database • **DB2** — DB2 Database • **HP_UNIX** — HP Unix • **SOLARIS** — Solaris • **OPENLDAP** — OpenLDAP • **POSTGRESQL** — PostgreSQL	
Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions
Escalate Privileges with	Use the drop-down menu to select the privilege elevation method, or select "Nothing" to skip privilege elevation. **Note:** Tenable supports multiple options for privilege escalation, including su, su+sudo and sudo. For example, if you select sudo, more fields for sudo user, Escalation Account Name, and Location of su and sudo (directory) are provided and	Required if you wish to escalate privileges.

Option	Description	Required
	can be completed to support authentication and privilege escalation through QiAnXin. The Escalation Account Name field is only required if the escalation password differs from the normal login password. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide or the Tenable Vulnerability Management User Guide.	
Escalation Account Username	If the escalation account has a different username or password from the least privileged user, enter the credential ID or identifier for the escalation account credential here.	no
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target.	yes

Option	Description	Required
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	no

Senhasegura (Tenable Nessus Manager only)

Tip: To view whether your Senhasegura credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
Senhasegura Host	The IP address or url for the Senhasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Tenable uses	yes

Option	Description	Required
	443.	
Senhasegura API Client ID	The Client ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Secret ID	The Secret ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura Credential ID or Identifier	The credential ID or identifier for the credential the you are requesting to retrieve.	yes
Use SSH Key for Target Authentication	The user can select this option to retrieve the SSH Key to authenticate to the target if the configuration is applicable in Senhasegura.	Required if authenticating to target with SSH Key.
Private Key File	The private key used to decrypt encrypted sensitive data from A2A. **Note:** You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, you must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Senhasegura.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
Escalate Privileges with	Use the drop-down menu to select the privilege elevation method, or select **Nothing** to skip privilege elevation. **Note:** Tenable supports multiple options for privilege escalation, including su, su+sudo and sudo. For example, if you select sudo, more fields for sudo user, Escalation Account	Required if you wish to escalate privileges.

Option	Description	Required
	Name, and Location of su and sudo (directory) are provided and can be completed to support authentication and privilege escalation through Senhasegura. The Escalation Account Name field is then required to complete your privilege escalation. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide, the Tenable Vulnerability Management User Guide, or the Tenable Security Center User Guide.	
Escalation account credential ID or identifier	If the escalation account has a different username or password from the least privileged user, enter the credential ID or identifier for the escalation account credential here.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the	no

Option	Description	Required
	scan to use the successful credential first, which allows the scan to access the target faster.	
HTTPS	This is enabled by default.	yes
Verify SSL Certificate	This is disabled by default.	no

Thycotic Secret Server (Tenable Nessus Manager only)

Option	Default Value
Username (required)	The username that is used to authenticate via ssh to the system.
Domain	Set the domain the username is part of if using Windows credentials.
Thycotic Secret Name (required)	This is the value to store the secret as on the Thycotic server. It is referred to as the "Secret Name" on the Thycotic server.
Thycotic Secret Server URL (required)	Use this option to set the transfer method, target, and target directory for the scanner. You can find this value in **Admin** > **Configuration** > **Application Settings** > **Secret Server URL** on the Thycotic server. For example consider the following address https://pw.mydomain.com/SecretServer/. We parse this to know that HTTPS defines it is a ssl connection, pw.mydomain.com is the target address, /SecretServer/ is the root directory.
Thycotic Login Name (required)	The username to authenticate to the Thycotic server.
Thycotic Password (required)	The password associated with the Thycotic Login Name.
Thycotic Organization	Use this value in cloud instances of Thycotic to define which organization your query should hit.

(required)	
Thycotic Domain (optional)	This is an optional value set if you set the domain value for the Thycotic server.
Private Key (optional)	Use key based authentication for SSH connections instead of password.
Verify SSL Certificate	Verify if the SSL Certificate on the server is signed by a trusted CA.
Thycotic elevate privileges with	The privilege escalation method you want to use to increase the user's privileges after initial authentication. Tenable Nessus supports multiple options for privilege escalation, including su, su+sudo and sudo. Your selection determines the specific options you must configure.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

BeyondTrust (Tenable Nessus only)

Tip: To view whether your BeyondTrust credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Default Value
Username	(Required) The username to log in to the hosts you want to scan.

BeyondTrust host	(Required) The BeyondTrust IP address or DNS address.
BeyondTrust port	(Required) The port BeyondTrust is listening on.
BeyondTrust API key	(Required) The API key provided by BeyondTrust.
Checkout duration	(Required) The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the Checkout duration to exceed the typical duration of your Tenable Nessus scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable Nessus scans. If BeyondTrust changes a password during a scan, the scan fails.
Use SSL	If enabled, Tenable Nessus uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.
Verify SSL certificate	If enabled, Tenable Nessus validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.
Use private key	If enabled, Tenable Nessus uses private key-based authentication for SSH connections instead of password authentication. If it fails, Tenable Nessus requests the password.
Use privilege escalation	If enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, it uses it for the scan.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that

	you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

Lieberman (Tenable Nessus Manager only)

Option	Description	Required
Username	The target system's username.	yes
Lieberman host	The Lieberman IP/DNS address. **Note:** If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Lieberman port	The port on which Lieberman listens.	yes
Lieberman API URL	The URL Tenable Nessus uses to access Lieberman.	no
Lieberman user	The Lieberman explicit user for authenticating to the Lieberman RED API.	yes
Lieberman password	The password for the Lieberman explicit user.	yes
Lieberman Authenticator	The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman. **Note:** If you use this option, append a domain to the **Lieberman user** option, i.e., *domain\user*.	no
Lieberman Client Certificate	The file that contains the PEM certificate used to communicate with the Lieberman host.	no

Option	Description	Required
	Note: If you use this option, you do not have to enter information in the **Lieberman user**, **Lieberman password**, and **Lieberman Authenticator** fields.	
Lieberman Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
Lieberman Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	no
Use SSL	If Lieberman is configured to support SSL through IIS, check for secure communication.	no
Verify SSL Certificate	If Lieberman is configured to support SSL through IIS and you want to validate the certificate, check this option. Refer to Custom CA documentation for how to use self-signed certificates.	no
System Name	In the rare case your organization uses one default Lieberman entry for all managed systems, enter the default entry name.	no
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Nessus receiving an unrecognized password prompt on the target host's interactive SSH shell.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing	no

Option	Description	Required
	a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	

Wallix Bastion (Tenable Nessus Manager only)

Tip: To view whether your Wallix Bastion credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
WALLIX Host	The IP address for the WALLIX Bastion host.	yes
WALLIX Port	The port on which the WALLIX Bastion API communicates. By default, Tenable uses 443.	yes
Authentication Type	**Basic** authentication (with WALLIX Bastion user interface username and Password requirements) or **API Key** authentication (with username and WALLIX Bastion-generated API key requirements).	no
WALLIX User	Your WALLIX Bastion user interface login username.	yes
WALLIX Password	Your WALLIX Bastion user interface login password. Used for **Basic** authentication to the API.	yes
WALLIX API Key	The API key generated in the WALLIX Bastion	yes

Option	Description	Required
	user interface. Used for **API Key** authentication to the API.	
Get Credential by Device Account Name	The account name associated with a **Device** you want to log in to the target systems with. **Note:** If your device has more than one account you must enter the specific device name for the account you want to retrieve credentials for. Failure to do this may result in credentials for the wrong account returned by the system.	Required only if you have a target and/or device with multiple accounts.
HTTPS	This is enabled by default. **Caution:** The integration fails if you disable **HTTPS**.	yes
Verify SSL Certificate	This is disabled by default and is not supported in WALLIX Bastion PAM integrations.	no
Elevate privileges with	This enables WALLIX Bastion Privileged Access Management (PAM). Use the drop-down menu to select the privilege elevation method. To bypass this function, leave this field set to **Nothing**. **Caution:** In your WALLIX Bastion account, the WALLIX Bastion super admin must have enabled "credential recovery" on your account for PAM to be enabled. Otherwise, your scan may not return any results. For more information, see your WALLIX Bastion documentation. **Note:** Multiple options for privilege escalation are supported, including *su*, *su+sudo* and *sudo*. For example, if you select **sudo**, more fields for **sudo user**, **Escalation Account Name**, and **Location of su and sudo** (directory) are provided and can be completed to support authentication and privilege	Required if you wish to escalate privileges.

Option	Description	Required
	escalation through WALLIX Bastion PAM. The **Escalation Account Name** field is then required to complete your privilege escalation. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Tenable Nessus User Guide.	
Database Port	The TCP port that the Oracle database instance listens on for communications from. The default is port 1521.	no
Auth Type	The type of account you want Tenable to use to access the database instance: • **SYSDBA** • **SYSOPER** • **NORMAL**	no
Service Type	The Oracle parameter you want to use to specify the database instance: **SID** or **SERVICE_NAME**.	no
Service	The SID value or SERVICE_NAME value for your database instance. The **Service** value you enter must match your parameter selection for the **Service Type** option.	yes
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works	no

Option	Description	Required
	against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	

HashiCorp Vault (Tenable Nessus Manager only)

Tip: To view whether your HashiCorp credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Windows and SSH Credentials		
Option	Description	Required
Hashicorp Vault host	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Hashicorp Vault port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate**(Required) and **Hashicorp Client Certificate Private Key** (Required) appear. Select the appropriate files for the client certificate and private key.	yes

Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The path/subdirectory to the authentication endpoint. This is not the full URL. For example: `/v1/auth/approle/login`	yes
Namespace	The name of a specified team in a multi-team environment.	no
Vault Type	The Tenable Nessus version: KV1, KV2, AD, or LDAP. For additional information about Tenable Nessus versions, see the Tenable Nessus documentation.	yes
KV1 Engine URL	(KV1) The URL Tenable Nessus uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL Tenable Nessus uses to access the KV2 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL Tenable Nessus uses to access the Active Directory engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the AD **Vault Type**
LDAP Engine URL	(LDAP) The URL Tenable Nessus uses to access the LDAP engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the LDAP **Vault Type**
Username Source	(KV1 and KV2) A drop-down box to specify if the	yes

	username is input manually or pulled from Hashicorp Vault.	
Username Key	(KV1 and KV2) The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	(KV1 and KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Domain Key (Windows)	(Required if Kerberos Target Authentication is enabled.) The key name that the domain is stored under in the secret.	yes
Secret Name	(KV1, KV2, and AD) The key secret you want to retrieve values for.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled.) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Domain (Windows)	(Required if Kerberos Target Authentication is enabled.) The domain to which Kerberos Target Authentication belongs, if applicable.	yes
Realm (SSH)	(Required if Kerberos Target Authentication is enabled.) The Realm is the authentication domain,	yes

	usually noted as the domain name of the target (for example, example.com).	
Use SSL	If enabled, Tenable Nessus Manager uses SSL for secure communications. Configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, Tenable Nessus Manager validates the SSL certificate. Configure SSL in Hashicorp Vault before enabling this option.	no
Enable for Tenable Nessus	Enables/disables IBM DataPower Gateway use with Tenable Nessus.	yes
Elevate privileges with (SSH)	Use a privilege escalation method such as su or sudo to use extra privileges when scanning. **Note:** Tenable supports multiple options for privilege escalation, including su, su+sudo and sudo. For example, if you select sudo, more fields for sudo user, Escalation account secret name, and Location of sudo (directory) are provided and can be completed to support authentication and privilege escalation through Tenable Nessus. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide and the Tenable Vulnerability Management User Guide.	Required if you wish to escalate privileges.
Escalation account secret name (SSH)	If the escalation account has a different username or password from the least privileged user, enter the credential ID or identifier for the escalation account credential here.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma	no

	or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	

Centrify (Tenable Nessus Manager only)

Option	Default Value
Centrify Host	(Required) The Centrify IP address or DNS address. **Note:** If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type *`IP address or hostname/subdirectory path`*.
Centrify Port	The port on which Centrify listens.
API User	(Required) The API user provided by Centrify
API Key	(Required) The API key provided by Centrify.
Tenant	The name of a specified team in a multi-team environment.
Authentication URL	The URL Tenable Nessus Manager uses to access Centrify.
Password Engine URL	The name of a specified team in a multi-team environment.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	The length of time, in minutes, that you want to keep credentials

Option	Default Value
	checked out in Centrify. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Nessus Manager scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Centrify so that password changes do not disrupt your Tenable Nessus Manager scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL	When enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

Arcon (Tenable Nessus Manager only)

Tip: To view whether your Arcon credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Default Value
Arcon host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon port	The port on which Arcon listens.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	The URL Tenable Nessus Manager uses to access Arcon.
Password Engine URL	The URL Tenable Nessus Manager uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Arcon Target Type	(Optional) The name of the target type. . Depending on the Arcon PAM version you are using and the system type the SSH credential has been created with, this is set to **linux** by default. Refer to the Arcon PAM Specifications document (provided by Arcon) for target type/system type mapping for the correct target type value.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Vulnerability Management scans. If Arcon changes a password during a scan, the scan fails.
Kerberos Target	If enabled, Kerberos authentication is used to log in to the specified

Option	Default Value
Authentication	Linux or Unix target.
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target.
Use SSL	When enabled, Tenable Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	When enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

Windows

The Windows credentials menu item has settings to provide Nessus with information such as SMB account name, password, and domain name. By default, you can specify a username, password, and domain with which to log in to Windows hosts. Also, Nessus supports several different types of authentication methods for Windows-based systems.

Regarding the authentication methods:

- The Lanman authentication method was prevalent on Windows NT and early Windows 2000 server deployments. It is retained for backward compatibility.
- The NTLM authentication method, introduced with Windows NT, provided improved security over Lanman authentication. The enhanced version, NTLMv2, is cryptographically more secure than NTLM and is the default authentication method chosen by Nessus when attempting to log into a Windows server. NTLMv2 can use SMB Signing.
- SMB signing is a cryptographic checksum applied to all SMB traffic to and from a Windows server. Many system administrators enable this feature on their servers to ensure that remote users are 100% authenticated and part of a domain. In addition, make sure you enforce a policy that mandates the use of strong passwords that cannot be easily broken via dictionary attacks from tools like John the Ripper and L0phtCrack. It is automatically used by Nessus if the remote Windows server requires it. There have been many different types of attacks against Windows security to illicit hashes from computers for re-use in attacking servers. SMB Signing adds a layer of security to prevent these man-in-the-middle attacks.
- The SPNEGO (Simple and Protected Negotiate) protocol provides Single Sign On (SSO) capability from a Windows client to various protected resources via the users' Windows login credentials. Nessus supports use of SPNEGO Scans and Policies: Scans 54 of 151 with either NTLMSSP with LMv2 authentication or Kerberos and RC4 encryption. SPNEGO authentication happens through NTLM or Kerberos authentication; nothing needs to be configured in the Nessus policy.
- If an extended security scheme (such as Kerberos or SPNEGO) is not supported or fails, Nessus attempts to log in via NTLMSSP/LMv2 authentication. If that fails, Nessus then attempts to log in using NTLM authentication.
- Nessus also supports the use of Kerberos authentication in a Windows domain. To configure this, the IP address of the Kerberos Domain Controller (actually, the IP address of the Windows Active Directory Server) must be provided.

Server Message Block (SMB) is a file-sharing protocol that allows computers to share information across the network. Providing this information to Nessus allows it to find local information from a remote Windows host. For example, using credentials enables Nessus to determine if important security patches have been applied. It is not necessary to modify other SMB parameters from default settings.

The SMB domain setting is optional and Nessus is able to log on with domain credentials without this setting. The username, password, and optional domain refer to an account that the target machine is aware of. For example, given a username of *joesmith* and a password of *my4x4mpl3*, a Windows server first looks for this username in the local system's list of users, and then determines if it is part of a domain.

Regardless of credentials used, Nessus always attempts to log into a Windows server with the following combinations:

- Administrator without a password
- A random username and password to test Guest accounts
- No username or password to test null sessions

The actual domain name is only required if an account name is different on the domain from that on the computer. It is entirely possible to have an Administrator account on a Windows server and within the domain. In this case, to log on to the local server, use the username of Administrator with the password of that account. To log on to the domain, use the Administrator username with the domain password and the name of the domain.

When multiple SMB accounts are configured, Nessus tries to log in with the supplied credentials sequentially. Once Nessus is able to authenticate with a set of credentials, it checks subsequent credentials supplied, but only use them if administrative privileges are granted when previous accounts provided user access.

Some versions of Windows allow you to create a new account and designate it as an administrator. These accounts are not always suitable for performing credentialed scans. Tenable recommends that the original administrative account, named Administrator be used for credentialed scanning to ensure full access is permitted. On some versions of Windows, this account may be hidden. The real administrator account can be unhidden by running a DOS prompt with administrative privileges and typing the following command:

```
C:\> net user administrator /active:yes
```

If an SMB account is created with limited administrator privileges, Nessus can easily and securely scan multiple domains. Tenable recommends that network administrators consider creating specific domain accounts to facilitate testing. Nessus includes various security checks for Windows 10, 11, Windows Server 2012, Server 2012 R2, Server 2016, Server 2019, and Server 2022 that are more accurate if you provide a domain account. Nessus attempts to try several checks if no account is provided.

Note: The Windows Remote Registry service allows remote computers with credentials to access the registry of the computer being audited. If the service is not running, reading keys and values from the registry is not possible, even with full credentials. This service must be started for a Nessus credentialed scan to fully audit a system using credentials.

For more information, see the Tenableblog post.

Credentialed scans on Windows systems require that you use a full administrator level account. Several bulletins and software updates by Microsoft have made reading the registry to determine software patch level unreliable without administrator privileges, but not all of them. Nessus plugins check that the provided credentials have full administrative access to ensure they execute properly. For example, full administrative access is required to perform direct reading of the file system. This allows Nessus to attach to a computer and perform direct file analysis to determine the true patch level of the systems being evaluated.

Authentication Methods

Global Credential Settings

Option	Default	Description
Never send credentials in the clear	Enabled	For security reasons, Windows credentials are not sent in the clear by default.
Do not use NTLMv1 authentication	Enabled	If this option is disabled, then it is theoretically possible to trick Nessus into attempting to log into a Windows server with domain credentials via the NTLM version 1

Option	Default	Description
		protocol. This provides the remote attacker with the ability to use a hash obtained from Nessus. This hash can be potentially cracked to reveal a username or password. It may also be used to log into other servers directly. Force Nessus to use NTLMv2 by enabling the Only use NTLMv2 setting at scan time. This prevents a hostile Windows server from using NTLM and receiving a hash. Because NTLMv1 is an insecure protocol this option is enabled by default.
Start the Remote Registry service during the scan	Disabled	This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running for Nessus to execute some Windows local check plugins.
Enable administrative shares during the scan	Disabled	This option allows Nessus to access the ADMIN$ and C$ administrative shares, which can be read with administrator privileges. **Caution:** The administrative shares have to be enabled for this setting to work properly. For most operating systems, ADMIN$ and C$ are enabled by default. However, Windows 10, Windows 11, and later Windows versions disable ADMIN$ by default. Therefore, you need to manually enable ADMIN$ in Windows environments in addition to using this setting for full access to the registry entries. For more information, see https://support.microsoft.com/kb/842715/en-us.
Start the Server service during the scan	Disabled	When enabled, the scanner temporarily enables the Windows Server service, which allows the computer to share files and other devices on a network. The service is disabled after the scan completes. By default, Windows systems have the Windows Server service enabled, which means you do not need to enable

Option	Default	Description
		this setting. However, if you disable the Windows Server service in your environment, and want to scan using SMB credentials, you must enable this setting so that the scanner can access files remotely.

CyberArk (Nessus Manager only)

Tip: To view whether your CyberArk credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Nessus Manager can get credentials from CyberArk to use in a scan.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web Service. This can be the host, or the host with a custom URL added on in a single string.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk API connection.	yes
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied

Option	Description	Required
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Domain	(Required if Kerberos Target Authentication is enabled) The domain to which Kerberos Target Authentication belongs, if applicable.	yes
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Address**, **Identifier**, **Parameters**, or **Username**. **Note:** For more information about the **Parameters** option, refer to the **Parameters Options** table. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier.	yes
Username	(If **Get credential by** is set to **Username**) The username of the CyberArk user to request a password from.	no

Option	Description	Required
Safe	The CyberArk safe the credential should be retrieved from.	no
Address	The option should only be used if the Address value is unique to a single CyberArk account credential.	no
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	no
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no

CyberArk Auto-Discovery (Nessus Manager only)

Tip: To view whether your CyberArk credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

You can now take advantage of a significant improvement to Tenable's CyberArk Integration which gathers bulk account information for specific target groups without entering multiple targets.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the user's CyberArk Instance. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes

Option	Description	Required
	Note: Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
AppID	The Application ID associated with the CyberArk API connection.	yes
Safe	Users may optionally specify a Safe to gather account information and request passwords.	no
AIM Web Service Authentication Type	There are two authentication methods established in the feature. **IIS Basic Authentication** and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	yes
CyberArk PVWA Web UI Login Name	Username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk PVWA Web UI Login Password	Password for the username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk Platform Search	String used in the PVWA REST API query parameters to gather bulk account information. For example, the user	yes

Option	Description	Required
String	can enter `UnixSSH Admin TestSafe`, to gather all Windows platform accounts containing a username `Admin` in a Safe called `TestSafe`. **Note:** This is a non-exact keyword search. A best practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	yes
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no

CyberArk (Legacy) (Nessus Manager only)

Tip: To view whether your CyberArk credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Nessus Manager can get credentials from CyberArk to use in a scan.

Option	Description
Username	The target system's username.
CyberArk AIM Service URL	The URL of the AIM service. By default, this setting uses `/AIMWebservice/v1.1/AIM.asmx`.
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.
Central	The port on which the CyberArk Central Credential Provider is listening.

Option	Description
Credential Provider Port	
Central Credential Provider Username	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this setting for authentication.
Central Credential Provider Password	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this setting for authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contained the authentication information you would like to retrieve.
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.
PolicyId	The PolicyID assigned to the credentials you would like to retrieve from the CyberArk Central Credential Provider.

Option	Description
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.
CyberArk Account Details Name	The unique name of the credential you want to retrieve from CyberArk.

Tip: To view whether your Delinea credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the **API Key** authentication method is selected.	yes
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled **Secret Name** on the Delinea server.	yes
Delinea Host	The Delinea Secret Server IP address for API requests.	yes
Delinea Port	The Delinea Secret Server Port for API requests. By	yes

	default, Tenable uses 443.	
Checkout Duration	The duration Tenable should check out the password from Delinea. Duration time is in hours and should be longer than the scan time.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Windows target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Domain	(Required if Kerberos Target Authentication is enabled) The Kerberos Domain is the authentication domain, usually noted as the domain name of the target.	yes
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL Certificate	If enabled. verifies the SSL Certificate on the Delinea server.	no

Delinea Secret Server Auto-Discovery

Tip: To view whether your Delinea credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
Delinea Host	The Delinea Secret Server host to pull the secrets from.	Yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	Yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	Yes
Delinea Login Name	The username to authenticate to the Delinea server.	Yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the provided Delinea Login Name.	Yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the API Key authentication method is selected.	Yes
Query Mode	Choose to query accounts using pre-set fields or by constructing a string of URL query parameters. By default, **Simple** is selected.	Yes
Folder ID	Query accounts with the given folder ID. This option is only available if query mode is set to **Simple**.	No
Search Text	Query accounts matching the given search text. This option is only available if query mode is set to **Simple**.	No
Search Field	The field to search using the given search text. If not specified, the query will search the `name` field. This option is only available if query mode is set to **Simple**.	No
Exact Match	Perform an exact match against the search text. By default, this is unselected. This option is only available if query mode is set to **Simple**.	No
Query String	Provide a string of URL query parameters. This option is	Yes

Option	Description	Required
	only available if query mode is set to **Advanced**, and in that case it is required.	
Use Private Key	Use key-based authentication for SSH connections instead of password authentication.	No
Use SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Verify the Delinea Secret Server SSL certificate.	No

Kerberos

Option	Default	Description
Password	none	Like with other credentials methods, this is the user password on the target system. This is a required setting.
Key Distribution Center (KDC)	none	This host supplies the session tickets for the user. This is a required setting.
KDC Port	88	You can configure this setting to direct Nessus to connect to the KDC if it is running on a port other than 88.
KDC Transport	TCP	If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.
Domain	none	The Windows domain that the KDC administers. This is a required setting.

LM Hash

Option	Description
Username	The target system's username.

Option	Description
Hash	The hash to use.
Domain	The Windows domain of the specified user's name.

NTLM Hash

Option	Description
Username	The target system's username.
Hash	The hash to use.
Domain	The Windows domain of the specified user's name.

QiAnXin

Tip: To view whether your QiAnXin credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
QiAnXin Host	The IP address or URL for the QiAnXin host.	yes
QiAnXin Port	The port on which the QiAnXin API communicates. By default, Tenable uses 443.	yes
QiAnXin API Client ID	The Client ID for the embedded account application created in QiAnXin PAM.	yes
QiAnXin API Secret ID	The Secret ID for the embedded account application created in QiAnXin PAM.	yes
Domain	The domain to which the username belongs.	no
Username	The username to log in to the hosts you want to scan.	yes
Host IP	Specify the host IP of the asset containing the	no

Option	Description	Required
	account to use. If not specified, the scan target IP is used.	
Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on credential type (for example, for Windows credentials, the default is WINDOWS). Possible values: • **ACTIVE_DIRECTORY** — Windows Domain Account • **WINDOWS** — Windows Local Account • **LINUX** — Linux Account • **SQL_SERVER** — SQL Server Database • **ORACLE** — Oracle Database • **MYSQL** — MySQL Database • **DB2** — DB2 Database • **HP_UNIX** — HP Unix • **SOLARIS** — Solaris • **OPENLDAP** — OpenLDAP • **POSTGRESQL** — PostgreSQL	no
Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions.
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Windows target.	no

Option	Description	Required
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Domain	(Required if Kerberos Target Authentication is enabled) The Kerberos Domain is the authentication domain, usually noted as the domain name of the target.	yes
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no

Senhasegura

Tip: To view whether your Senhasegura credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
Senhasegura Host	The IP address or URL for the Senhasegura host.	yes

Option	Description	Required
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Tenable uses 443.	yes
Senhasegura API Client ID	The Client ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Secret ID	The Secret ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Domain	The domain to which the username belongs.	no
Senhasegura Credential ID or Identifier	The credential ID or identifier for the credential the you are requesting to retrieve.	yes
Private Key File	The Private Key used to decrypt encrypted sensitive data from A2A. **Note:** You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, the user must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Senhasegura.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
HTTPS	This is enabled by default.	yes
Verify SSL Certificate	This is disabled by default.	no

Thycotic Secret Server (Tenable Nessus Manager only)

Option	Default Value
Username	(Required) The username for a user on the target system.
Domain	The domain of the username, if set on the Thycotic server.
Thycotic Secret Name	(Required) The Secret Name value on the Thycotic server.
Thycotic Secret Server URL	(Required) The value you want Tenable Nessus to use when setting the transfer method, target, and target directory for the scanner. Find the value on the Thycotic server, in **Admin > Configuration > Application Settings > Secret Server URL**. For example, if you type *https://pw.mydomain.com/SecretServer*, Tenable Nessus determines it is an SSL connection, that *pw.mydomain.com* is the target address, and that */SecretServer* is the root directory.
Thycotic Login Name	(Required) The username for a user on the Thycotic server.
Thycotic Password	(Required) The password associated with the **Thycotic Login Name** you provided.
Thycotic Organization	In cloud instances of Thycotic, the value that identifies which organization the Tenable Nessus query should target.
Thycotic Domain	The domain, if set for the Thycotic server.
Private Key	If enabled, Tenable Nessus uses key-based authentication for SSH connections instead of password authentication.
Verify SSL Certificate	If enabled, Tenable Nessus verifies the SSL Certificate on the Thycotic server. For more information about using self-signed certificates, see Custom SSL Server Certificates.

Windows LAPS

Option	Description	Required
LAPS Host Address	The IP address of the domain controller that hosts Active Directory and manages LAPS.	yes
LAPS Host Port	The port used to communicate with the LAPS host. The default port is 445.	no
Username	The username for an account with permissions to retrieve Windows LAPS credentials from Active Directory.	yes
Password	The password for the account specified in the Username field.	yes
LAPS Domain	The domain where the LAPS-managed devices reside.	yes
LAPS OU	The Distinguished Name (DN) of the Organizational Unit (OU) that contains the LAPS-managed target devices.	yes

BeyondTrust (Tenable Nessus Manager only)

Tip: To view whether your BeyondTrust credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Default Value
Username	(Required) The username to log in to the hosts you want to scan.
Domain	The domain of the username, if required by BeyondTrust.
BeyondTrust host	(Required) The BeyondTrust IP address or DNS address.
BeyondTrust port	(Required) The port BeyondTrust is listening on.

Option	Default Value
BeyondTrust API key	(Required) The API key provided by BeyondTrust.
Checkout duration	(Required) The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the Checkout duration to exceed the typical duration of your Nessus scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Nessus scans. If BeyondTrust changes a password during a scan, the scan fails.
Use SSL	If enabled, Nessus uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.
Verify SSL certificate	If enabled, Nessus validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.
Use private key	If enabled, Nessus uses private key-based authentication for SSH connections instead of password authentication. If it fails, the password is requested.
Use privilege escalation	If enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, it uses it for the scan.

Lieberman (Tenable Nessus Manager only)

Option	Description	Required
Username	The target system's username.	yes
Domain	The domain, if the username is part of a domain.	no
Lieberman host	The Lieberman IP/DNS address. **Note:** If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type *IP*	yes

Option	Description	Required
	address or hostname / subdirectory path.	
Lieberman port	The port on which Lieberman listens.	yes
Lieberman API URL	The URL Tenable Nessus uses to access Lieberman.	no
Lieberman user	The Lieberman explicit user for authenticating to the Lieberman RED API.	yes
Lieberman password	The password for the Lieberman explicit user.	yes
Lieberman Authenticator	The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman. **Note:** If you use this option, append a domain to the **Lieberman user** option, i.e., *domain\user*.	no
Lieberman Client Certificate	The file that contains the PEM certificate used to communicate with the Lieberman host. **Note:** If you use this option, you do not have to enter information in the **Lieberman user**, **Lieberman password**, and **Lieberman Authenticator** fields.	no
Lieberman Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
Lieberman Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	no
Use SSL	If Lieberman is configured to support SSL through IIS, check for secure communication.	no

Option	Description	Required
Verify SSL Certificate	If Lieberman is configured to support SSL through IIS and you want to validate the certificate, check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.	no
System Name	In the rare case your organization uses one default Lieberman entry for all managed systems, enter the default entry name.	no

Wallix Bastion (Tenable Nessus Manager only)

Tip: To view whether your Wallix Bastion credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
WALLIX Host	The IP address for the WALLIX Bastion host.	yes
WALLIX Port	The port on which the WALLIX Bastion API communicates. By default, Tenable uses 443.	yes
Authentication Type	**Basic** authentication (with WALLIX Bastion user interface username and Password requirements) or **API Key** authentication (with username and WALLIX Bastion-generated API key requirements).	no
WALLIX User	Your WALLIX Bastion user interface login username.	yes
WALLIX Password	Your WALLIX Bastion user interface login password. Used for **Basic** authentication to the API.	yes
WALLIX API Key	The API key generated in the WALLIX Bastion	yes

Option	Description	Required
	user interface. Used for **API Key** authentication to the API.	
Get Credential by Device Account Name	The account name associated with a **Device** you want to log in to the target systems with. **Note:** If your device has more than one account you must enter the specific device name for the account you want to retrieve credentials for. Failure to do this may result in credentials for the wrong account returned by the system.	Required only if you have a target and/or device with multiple accounts.
HTTPS	This is enabled by default. **Caution:** The integration fails if you disable **HTTPS**.	yes
Verify SSL Certificate	This is disabled by default and is not supported in WALLIX Bastion PAM integrations.	no
Elevate privileges with	This enables WALLIX Bastion Privileged Access Management (PAM). Use the drop-down menu to select the privilege elevation method. To bypass this function, leave this field set to **Nothing**. **Caution:** In your WALLIX Bastion account, the WALLIX Bastion super admin must have enabled "credential recovery" on your account for PAM to be enabled. Otherwise, your scan may not return any results. For more information, see your WALLIX Bastion documentation. **Note:** Multiple options for privilege escalation are supported, including *su*, *su+sudo* and *sudo*. For example, if you select **sudo**, more fields for **sudo user**, **Escalation Account Name**, and **Location of su and sudo** (directory) are provided and can be completed to support authentication and privilege	Required if you wish to escalate privileges.

Option	Description	Required
	escalation through WALLIX Bastion PAM. The **Escalation Account Name** field is then required to complete your privilege escalation. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Tenable Nessus User Guide.	
Database Port	The TCP port that the Oracle database instance listens on for communications from. The default is port 1521.	no
Auth Type	The type of account you want Tenable to use to access the database instance: • **SYSDBA** • **SYSOPER** • **NORMAL**	no
Service Type	The Oracle parameter you want to use to specify the database instance: **SID** or **SERVICE_NAME**.	no
Service	The SID value or SERVICE_NAME value for your database instance. The **Service** value you enter must match your parameter selection for the **Service Type** option.	yes
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works	no

Option	Description	Required
	against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	

HashiCorp Vault (Tenable Nessus Manager only)

Tip: To view whether your HashiCorp credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Windows and SSH Credentials		
Option	Description	Required
Hashicorp Vault host	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Hashicorp Vault port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate**(Required) and **Hashicorp Client Certificate Private Key** (Required) appear. Select the appropriate files for the client certificate and private key.	yes

Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The path/subdirectory to the authentication endpoint. This is not the full URL. For example: `/v1/auth/approle/login`	yes
Namespace	The name of a specified team in a multi-team environment.	no
Vault Type	The Tenable Nessus version: KV1, KV2, AD, or LDAP. For additional information about Tenable Nessus versions, see the Tenable Nessus documentation.	yes
KV1 Engine URL	(KV1) The URL Tenable Nessus uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL Tenable Nessus uses to access the KV2 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL Tenable Nessus uses to access the Active Directory engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the AD **Vault Type**
LDAP Engine URL	(LDAP) The URL Tenable Nessus uses to access the LDAP engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the LDAP **Vault Type**
Username Source	(KV1 and KV2) A drop-down box to specify if the	yes

	username is input manually or pulled from Hashicorp Vault.	
Username Key	(KV1 and KV2) The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	(KV1 and KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Domain Key (Windows)	(Required if Kerberos Target Authentication is enabled.) The key name that the domain is stored under in the secret.	yes
Secret Name	(KV1, KV2, and AD) The key secret you want to retrieve values for.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled.) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Domain (Windows)	(Required if Kerberos Target Authentication is enabled.) The domain to which Kerberos Target Authentication belongs, if applicable.	yes
Realm (SSH)	(Required if Kerberos Target Authentication is enabled.) The Realm is the authentication domain,	yes

	usually noted as the domain name of the target (for example, example.com).	
Use SSL	If enabled, Tenable Nessus Manager uses SSL for secure communications. Configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, Tenable Nessus Manager validates the SSL certificate. Configure SSL in Hashicorp Vault before enabling this option.	no
Enable for Tenable Nessus	Enables/disables IBM DataPower Gateway use with Tenable Nessus.	yes
Elevate privileges with (SSH)	Use a privilege escalation method such as su or sudo to use extra privileges when scanning. **Note:** Tenable supports multiple options for privilege escalation, including su, su+sudo and sudo. For example, if you select sudo, more fields for sudo user, Escalation account secret name, and Location of sudo (directory) are provided and can be completed to support authentication and privilege escalation through Tenable Nessus. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide and the Tenable Vulnerability Management User Guide.	Required if you wish to escalate privileges.
Escalation account secret name (SSH)	If the escalation account has a different username or password from the least privileged user, enter the credential ID or identifier for the escalation account credential here.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma	no

	or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	

Centrify (Tenable Nessus Manager only)

Option	Default Value
Centrify Host	(Required) The Centrify IP address or DNS address. **Note:** If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type *`IP address or hostname/subdirectory path`*.
Centrify Port	The port on which Centrify listens.
API User	(Required) The API user provided by Centrify
API Key	(Required) The API key provided by Centrify.
Tenant	The name of a specified team in a multi-team environment.
Authentication URL	The URL Tenable Nessus Manager uses to access Centrify.
Password Engine URL	The name of a specified team in a multi-team environment.
Username	(Required) The username to log in to the hosts you want to scan.

Option	Default Value
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in Centrify. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Nessus Manager scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Centrify so that password changes do not disrupt your Tenable Nessus Manager scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL	When enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

Arcon (Tenable Nessus Manager only)

Tip: To view whether your Arcon credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Default Value
Arcon host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon port	The port on which Arcon listens.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	The URL Tenable Nessus Manager uses to access Arcon.
Password Engine URL	The URL Tenable Nessus Manager uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Arcon Target Type	(Optional) The name of the target type. . Depending on the Arcon PAM version you are using and the system type the SSH credential has been created with, this is set to **linux** by default. Refer to the Arcon PAM Specifications document (provided by Arcon) for target type/system type mapping for the correct target type value.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Vulnerability Management scans. If Arcon changes a password during a scan, the scan fails.
Kerberos Target	If enabled, Kerberos authentication is used to log in to the specified

Option	Default Value
Authentication	Linux or Unix target.
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target.
Use SSL	When enabled, Tenable Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	When enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

Miscellaneous Credentials

This section includes information and settings for credentials in the **Miscellaneous** section.

ADSI

ADSI requires the domain controller information, domain, and domain admin and password.

ADSI allows Tenable Nessus to query an ActiveSync server to determine if any Android or iOS-based devices are connected. Using the credentials and server information, Tenable Nessus authenticates to the domain controller (not the Exchange server) to directly query it for device information. These settings are required for mobile device scanning.

Tenable Nessus supports obtaining the mobile information from Exchange Server 2010 and 2013 only.

Option	Description	Default
Domain Controller	(Required) The name of the domain controller for ActiveSync.	-
Domain	(Required) The name of the NetBIOS domain for ActiveSync.	-
Domain Admin	(Required) The domain administrator's username.	-
Domain Password	(Required) The domain administrator's password.	-

Nessus supports obtaining the mobile information from Exchange Server 2010 and 2013 only; Nessus cannot retrieve information from Exchange Server 2007.

Cisco Meraki

Option	Description	Required
Cisco Meraki API Host	Hostname or IP address to the Cisco Meraki Dashboard API host. **Note:** If your Cisco Meraki API Host requires you to use your own direct/unique URL, refer to Cisco Meraki Credential Fields, Usage, and Limitations in the *Tenable and Cisco Meraki Integration Guide* for guidance.	Yes

Option	Description	Required
Cisco Meraki API Port	Port of the Cisco Meraki Dashboard API. (Default 443)	Yes
Cisco Meraki API Key	API Key for authentication to the Cisco Meraki API.	Yes
CIsco Meraki Organization Name	Enter a single organization per credential.	Yes
CIsco Meraki Network Name	Enter one or more comma-separated network names.	No
Cisco Meraki Product Type	Enter one or more comma-separated product types. Valid product types: **appliance**, **camera**, **cellularGateway**, **secureConnect**, **sensor**, **switch**, **systemManager**, **wireless**, and **wirelessController**.	No
Cisco Meraki Tag	Enter one or more comma-separated tags used to filter device searches within an organization.	No
Cisco Meraki Device Name	Enter a single Cisco Meraki device name. (e.g., "Meraki MS120-8")	No
Cisco Meraki Device Model	Enter one or more comma-separated Cisco Meraki device models. (e.g., "MS120-8")	No
Device Serial Number	Enter one or more comma-separated device serial numbers.	No
Device MAC Address	Enter one or more comma-separated device MAC Addresses.	No
Discover Devices	Adds any discovered Cisco Meraki devices to the targets to scan. (Default Off)	No
HTTPS	When set to On, the field expands with the option to enable **Verification of SSL Client Certificate if a Custom CA is**	No

Option	Description	Required
	configured. (Default Off)	

F5

Option	Description	Default
Username	(Required) The username for the scanning F5 account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the F5 user.	-
Port	(Required) The TCP port that F5 listens on for communications from Tenable Nessus.	443
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	enabled

IBM iSeries

Option	Description	Default
Username	(Required) The username for the IBM iSeries account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the IBM iSeries user.	-

Netapp API

Option	Description	Default

Username	(Required) The username for the Netapp API account with HTTPS access that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the Netapp API user.	-
vFiler	The vFiler nodes to scan for on the target systems. To limit the audit to a single vFiler, type the name of the vFiler. To audit for all discovered Netapp virtual filers (vFilers) on target systems, leave the field blank.	-
Port	(Required) The TCP port that Netapp API listens on for communications from Tenable Nessus.	443

Nutanix Prism

Tip: To view whether your Nutanix Prism credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins

Option	Description	Default
Nutanix Host	(Required) Hostname or IP address of the Nutanix Prism Central host.	-
Nutanix Port	(Required) The TCP port that the Nutanix Prism Central host listens on for communications from Tenable.	9440
Nutanix Prism Central Authentication Method	(Required) The user can choose from a list of authentication methods: • Username and Password (manual entry) • Privileged Access Management (PAM) Integration. Use a specific PAM to gather vCenter API Authentication Credentials from the available list.	Username and Password
Discover Hosts	When enabled, Tenable adds all discovered Nutanix	enabled

Option	Description	Default
	hosts to the list of scan targets.	
Discover Virtual Machines	When enabled. Tenable adds all discovered Nutanix Virtual Machines to the list of scan targets.	enabled
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	disabled

OpenStack

Option	Description	Default
Username	(Required) The username for the OpenStack account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the OpenStack user.	-
Tenant Name for Authentication	(Required) The name of the specific tenant the scan uses to authenticate.	admin
Port	(Required) The TCP port that OpenStack listens on for communications from Tenable Nessus.	443
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA.	enabled

	Tip: If you are using a self-signed certificate, disable this setting.	

Palo Alto Networks PAN-OS

Option	Description	Default
Username	(Required) The username for the PAN-OS account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the PAN-OS user.	-
Port	(Required) The TCP port that PAN-OS listens on for communications from Tenable Nessus.	443
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	enabled

Red Hat Enterprise Virtualization (RHEV)

Option	Description	Default
Username	(Required) The username for RHEV account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the RHEV user.	-
Port	(Required) The TCP port that the RHEV server listens on for communications from Tenable Nessus.	443
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA.	enabled

Option	Description	Default
	Tip: If you are using a self-signed certificate, disable this setting.	

VMware ESX SOAP API

Access to VMware servers is available through its native SOAP API. VMware ESX SOAP API allows you to access the ESX and ESXi servers via username and password. Also, you have the option of not enabling SSL certificate verification:

For more information on configuring VMWare ESX SOAP API, see Configure vSphere Scanning.

Tip: To view whether your ESXi SOAP API credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Tenable can access VMware servers through the native VMware SOAP API.

Option	Description	Default
ESX SOAP API Authentication Method	(Required) The user can choose from a list of authentication methods: • Username and Password (manual entry) • PAM Integration (Use a specific PAM to gather vCenter API Authentication Credentials from the available list.)	Username and Password
Do not verify SSL Certificate	Do not validate the SSL certificate for the ESXi server.	disabled

VMware vCenter

For more information on configuring VMWare vCenter SOAP API, see Configure vSphere Scanning.

Tip: To view whether your VMware vCenter credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Tenable can access vCenter through the native VMware vCenter SOAP API. If available, Tenable uses the vCenter REST API to collect data in addition to the SOAP API.

Note: Tenable supports VMware vCenter/ESXi versions 7.0.3 and later for authenticated scans. This does not impact vulnerability checks for VMware vCenter/ESXi, which do not require authentication.

Note: The SOAP API requires a vCenter account with read permissions and settings privileges. The REST API requires a vCenter admin account with general read permissions and required Lifecycle Manager privileges to enumerate VIBs.

Option	Description	Default
vCenter Host	(Required) The name of the vCenter host.	-
vCenter Port	(Required) The TCP port that vCenter listens on for communications from Tenable.	443
Username	(Required) The username for the vCenter server account with admin read/write access that Tenable uses to perform checks on the target system.	-
Password	(Required) The password for the vCenver server user.	-
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	enabled
Auto Discover Managed VMware ESXi Hosts	This option adds any discovered VMware ESXi hypervisor hosts to the scan targets you include in your scan.	disabled
Auto Discover Managed VMware	This option adds any discovered VMware ESXi hypervisor virtual machines to the scan targets you	disabled

Option	Description	Default
ESXi Virtual Machines	include in your scan.	

X.509

Option	Description	Default
Client certificate	(Required) The client certificate.	-
Client key	(Required) The client private key.	-
Password for key	(Required) The passphrase for the client private key.	-
CA certificate to trust	(Required) The trusted Certificate Authority's (CA) digital certificate.	-

Mobile Credentials

Tenable Nessus Manager can leverage credentials for patch management systems to perform patch auditing on systems for which credentials may not be available.

Note: Patch management integration is not available on Tenable Nessus Essentials, Tenable Nessus Professional, Tenable Nessus Expert, or managed Tenable Nessus scanners.

ActiveSync

Option	Default	Description
Domain Controller	--	The domain controller for ActiveSync.
Domain	--	The Windows domain for ActiveSync.
Domain Username	--	The username for the domain administrator's account that Tenable Nessus uses to authenticate to ActiveSync.
Domain Password	--	The password for the domain administrator user.

Option	Default	Description
Scanner	--	Specifies which scanner Tenable Nessus uses when scanning the server. Tenable Nessus can only use one scanner to add data to a mobile repository.
Update Schedule	Every day at 12:30 -04:00	Specifies when Tenable Nessus scans the server to update the mobile repository. On each scan, Tenable Nessus removes the current data in the repository and replaces it with data from the latest scan.

AirWatch

Tip: To view whether your AirWatch credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Default Value	Description	Required
AirWatch Environment API URL	–	The Workspace ONE API URL endpoint. (e.g., https://xxx.awmdm.com/api)	yes
Port	443	The TCP port that AirWatch listens on for communications from Tenable.	yes
Username	–	The username for the AirWatch user account Tenable uses to authenticate to Workspace One's API.	yes
Password	–	The password for the AirWatch user.	yes
API Key	–	The API key for the VMware	yes

		Workspace ONE API.	
HTTPS	Enabled	Enable for Tenable Nessus to authenticate over an encrypted (HTTPS) or an unencrypted (HTTP) connection.	no
Verify SSL Certificate	Enabled	Enable for Tenable Nessus to verify if the SSL Certificate on the server is signed by a trusted CA.	no

Blackberry UEM

Tip: To view whether your Blackberry UEM credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description
Hostname	The server URL to authenticate with Blackberry UEM.
Port	The port to use to authenticate with Blackberry UEM.
Tenant	The SRP ID in Blackberry UEM. **Note:** To locate the SRP ID in Blackberry UEM: 1. In the Blackberry UEM top navigation bar, click the **Help** drop-down. 2. Click **About Blackberry UEM.** An information window containing the SRP ID appears. 3. Copy the SRP ID.
Domain	The domain name for Blackberry UEM.
Username	The username for the account you want Tenable Nessus to use

	to authenticate to Blackberry UEM.
Password	The password for the account you want Tenable Nessus to use to authenticate to Blackberry UEM.
HTTPS	When enabled, Tenable Nessus uses an encrypted connection to authenticate with Blackberry UEM.
Verify SSL Certificate	When enabled, Tenable Nessus verifies that the SSL Certificate on the server is signed by a trusted CA.

Intune

Tip: To view whether your Intune credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description
Tenant	The Microsoft Azure Directory (tenant) ID visible in your App registration.
Client	The Microsoft Azure Application (client) ID generated during your App registration.
Secret	The secret key generated when you created your client secret key in Microsoft Azure.
Username	The username for the account you want Tenable Nessus to use to authenticate to Intune.
Password	The password for the account you want Tenable Nessus to use to authenticate to Intune.

Ivanti

Option	Description	Default Value	Required
VSP Admin	The server URL Tenable uses to authenticate	-	yes

Option	Description	Default Value	Required
Portal URL	to the Ivanti administrator portal.		
VSP Admin Portal Port	The port Tenable uses to authenticate to the Ivanti administrator portal.	443	no
Port	The port Tenable uses to authenticate to Ivanti.	443	yes
Username	The username for the account you want Tenable to use to authenticate to Ivanti.	-	yes
Password	The password for the account you want Tenable to use to authenticate to Ivanti.	-	yes
HTTPS	When enabled, Tenable uses an encrypted connection to authenticate to Ivanti.	Enabled	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	Enabled	no

MaaS360

Tip: To view whether your MaaS360 credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
Username	The username to authenticate.	yes
Password	The password to authenticate.	yes
Root URL	The server URL to authenticate with MaaS360.	yes
Platform ID	The Platform ID provided for MaaS360.	yes

Billing ID	The Billing ID provided for MaaS360.	yes
App ID	The App ID provided for MaaS360.	yes
App Version	The App Version of MaaS360.	yes
App access key	The App Access Key provided for MaaS360.	yes
Collect All Device Data	When enabled, the scan collects all data types. When disabled, the scan collects one or more types of data to decrease the scan time. When disabled, choose one or more of the following collection options: • **Collect Device Summary** • **Collect Device Applications** • **Collect Device Compliance** • **Collect Device Policies**	no

MobileIron

Tip: To view whether your MobileIron credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Description	Required
VSP Admin Portal URL	The server URL Tenable Nessus uses to authenticate to the MobileIron administrator portal.	yes
VSP Admin Portal Port	The port Tenable Nessus uses to authenticate to the MobileIron administrator portal (typically, port 443 or 8443). The system assumes port 443 by default.	no

Port	The port Tenable Nessus uses to authenticate to MobileIron (typically, port 443).	no
Username	The username for the account you want Tenable Nessus to use to authenticate to MobileIron.	yes
Password	The password for the account you want Tenable Nessus to use to authenticate to MobileIron.	yes
HTTPS	When enabled, Tenable Nessus uses an encrypted connection to authenticate to MobileIron.	no
Verify SSL Certificate	When enabled, Tenable Nessus verifies that the SSL Certificate on the server is signed by a trusted CA.	no

Workspace ONE

Tip: To view whether your Workspace ONE credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Option	Default Value	Description	Required
Workspace ONE Environment API URL	–	The Workspace ONE API url endpoint. (e.g., https://xxx.awmdm.com/api)	yes
Port	443	The TCP port that Workspace ONE listens on for communications from Tenable.	yes
Workspace ONE Username	–	The username for the	yes

		Workspace ONE user account Tenable uses to authenticate to Workspace ONE's API.	
Workspace ONE Password	–	The password for the Workspace ONE user.	yes
API Key	–	The API key for the VMware Workspace ONE API.	yes
HTTPS	Enabled	Enable for Tenable Nessus to authenticate over an encrypted (HTTPS) or an unencrypted (HTTP) connection.	no
Verify SSL Certificate	Enabled	Enable for Tenable Nessus to verify if the SSL Certificate on the server is signed by a trusted CA. **Tip**: If you are using a self-signed certificate, disable this setting.	no
Collect All Device Data	Yes	Collects all device data required for plugin checks.	no
Collect Device Applications	Yes	(Enabled if Collect All Device Data is set to "No") Collects applications installed on mobile devices.	no

Patch Management Credentials

Tenable Nessus can leverage credentials for patch management systems to perform patch auditing on systems for which credentials may not be available.

Note: Patch management integration is not available on Tenable Nessus Essentials, Tenable Nessus Professional, Tenable Nessus Expert, or managed Tenable Nessus scanners.

Tenable Nessus Manager supports:

- Dell KACE K1000
- HCL BigFix
- Microsoft System Center Configuration Manager (SCCM)
- Microsoft Windows Server Update Services (WSUS)
- Red Hat Satellite Server
- Symantec Altiris

You can configure patch management options in the **Credentials** section while creating a scan, as described in Create a Scan.

IT administrators are expected to manage the patch monitoring software and install any agents required by the patch management system on their systems.

Note: If the credential check sees a system but it is unable to authenticate against the system, it uses the data obtained from the patch management system to perform the check. If Tenable Nessus is able to connect to the target system, it performs checks on that system and ignores the patch management system output.

Note: The data returned to Tenable Nessus by the patch management system is only as current as the most recent data that the patch management system has obtained from its managed hosts.

Scanning with Multiple Patch Managers

If you provide multiple sets of credentials to Tenable Nessus for patch management tools, Tenable Nessus uses all of them.

If you provide credentials for a host and for one or more patch management systems, Tenable Nessus compares the findings between all methods and report on conflicts or provide a satisfied finding. Use the Patch Management Windows Auditing Conflicts plugins to highlight patch data differences between the host and a patch management system.

Dell KACE K1000

KACE K1000 is available from Dell to manage the distribution of updates and hotfixes for Linux, Windows, and macOS systems. Tenable Nessus can query KACE K1000 to verify whether or not

patches are installed on systems managed by KACE K1000 and display the patch information through the Tenable Nessus user interface.

Tenable Nessus supports KACE K1000 versions 6.x and earlier.

KACE K1000 scanning uses the following Tenable plugins: 76867, 76868, 76866, and 76869.

Option	Description	Default
Server	(Required) The KACE K1000 IP address or system name.	-
Database Port	(Required) The TCP port that KACE K1000 listens on for communications from Tenable Nessus.	3306
Organization Database Name	(Required) The name of the organization component for the KACE K1000 database (e.g., ORG1).	ORG1
Database Username	(Required) The username for the KACE K1000 account that Tenable Nessus uses to perform checks on the target system.	R1
K1000 Database Password	(Required) The password for the KACE K1000 user.	-

HCL Tivoli Endpoint Manager (BigFix)

Tip: To view whether your HCL BigFix credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

HCL Bigfix is available to manage the distribution of updates and hotfixes for desktop systems.Tenable Nessus can query HCL Bigfix to verify whether or not patches are installed on systems managed by HCL Bigfix and display the patch information.

Package reporting is supported by RPM-based and Debian-based distributions that HCL Bigfix officially supports. This includes Red Hat derivatives such as RHEL, CentOS, Scientific Linux, and Oracle Linux, as well as Debian and Ubuntu. Other distributions may also work, but unless HCL Bigfix officially supports them, there is no support available.

For local check plugins to trigger, only RHEL, CentOS, Scientific Linux, Oracle Linux, Debian, Ubuntu, and Solaris are supported. Plugin 160250 must be enabled.

Tenable Nessus supports HCL Bigfix 9.5 and later and 10.x and later.

HCL Bigfix scanning uses the following Tenable plugins: 160247, 160248, 160249, 160250, and 160251.

Option	Description	Default
Web Reports Server	(Required) The name of HCL Bigfix Web Reports server.	-
Web Reports Port	(Required) The TCP port that the HCL Bigfix Web Reports server listens on for communications from Tenable Nessus.	-
Web Reports Username	(Required) The username for the HCL Bigfix Web Reports administrator account that Tenable Nessus uses to perform checks on the target system.	-
Web Reports Password	(Required) The password for the HCL Bigfix Web Reports administrator user.	-
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled
Verify SSL certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	Enabled

HCL Bigfix Server Configuration

In order to use these auditing features, you must make changes to the HCL Bigfix server. You must import a custom analysis into HCL Bigfix so that detailed package information is retrieved and made available to Tenable Nessus.

From the HCL BigFix Console application, import the following `.bes` files.

BES file:

```
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
    <Analysis>
        <Title>Tenable</Title>
        <Description>This analysis provides SecurityCenter with the data it needs for vulnerability
reporting. </Description>
        <Relevance>true</Relevance>
        <Source>Internal</Source>
        <SourceReleaseDate>2013-01-31</SourceReleaseDate>
        <MIMEField>
            <Name>x-fixlet-modification-time</Name>
            <Value>Thu, 13 May 2021 21:43:29 +0000</Value>
        </MIMEField>
        <Domain>BESC</Domain>
        <Property Name="Packages - With Versions (Tenable)" ID="74"><![CDATA[if (exists true whose
(if true then (exists object repository) else false)) then unique values of (lpp_name of it & "|" &
version of it as string & "|" & "fileset" & "|" & architecture of operating system) of filesets of
products of object repository else if (exists true whose (if true then (exists debianpackage) else
false)) then unique values of (name of it & "|" & version of it as string & "|" & "deb" & "|" &
architecture of it & "|" & architecture of operating system) of packages whose (exists version of it)
of debianpackages else if (exists true whose (if true then (exists rpm) else false)) then unique
values of (name of it & "|" & version of it as string & "|" & "rpm" & "|" & architecture of it & "|"
& architecture of operating system) of packages of rpm else if (exists true whose (if true then
(exists ips image) else false)) then unique values of (full name of it & "|" & version of it as
string & "|" & "pkg" & "|" & architecture of operating system) of latest installed packages of ips
image else if (exists true whose (if true then (exists pkgdb) else false)) then unique values of
(pkginst of it & "|" & version of it & "|" & "pkg10") of pkginfos of pkgdb else
"<unsupported>"]]></Property>
        <Property Name="Tenable AIX Technology Level" ID="76">current technology level of operating
system</Property>
        <Property Name="Tenable Solaris - Showrev -a" ID="77"><![CDATA[if ((operating system as
string as lowercase contains "SunOS 5.10" as lowercase) AND (exists file "/var/opt/BESClient/showrev_
patches.b64")) then lines of file "/var/opt/BESClient/showrev_patches.b64" else
"<unsupported>"]]></Property>
    </Analysis>
</BES>
```

BES file:

```
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
    <Task>
        <Title>Tenable - Solaris 5.10 - showrev -a Capture</Title>
        <Description><![CDATA[&lt;enter a description of the task here&gt; ]]></Description>
        <GroupRelevance JoinByIntersection="false">
            <SearchComponentPropertyReference PropertyName="OS" Comparison="Contains">
                <SearchText>SunOS 5.10</SearchText>
                <Relevance>exists (operating system) whose (it as string as lowercase contains "SunOS
5.10" as lowercase)</Relevance>
            </SearchComponentPropertyReference>
        </GroupRelevance>
        <Category></Category>
        <Source>Internal</Source>
        <SourceID></SourceID>
        <SourceReleaseDate>2021-05-12</SourceReleaseDate>
        <SourceSeverity></SourceSeverity>
```

```
        <CVENames></CVENames>
        <SANSID></SANSID>
        <MIMEField>
            <Name>x-fixlet-modification-time</Name>
            <Value>Thu, 13 May 2021 21:50:58 +0000</Value>
        </MIMEField>
        <Domain>BESC</Domain>
        <DefaultAction ID="Action1">
            <Description>
                <PreLink>Click </PreLink>
                <Link>here</Link>
                <PostLink> to deploy this action.</PostLink>
            </Description>
            <ActionScript MIMEType="application/x-sh"><![CDATA[#!/bin/sh
/usr/bin/showrev -a > /var/opt/BESClient/showrev_patches
/usr/sfw/bin/openssl base64 -in /var/opt/BESClient/showrev_patches -out /var/opt/BESClient/showrev_
patches.b64

]]></ActionScript>
        </DefaultAction>
    </Task>
</BES>
```

Microsoft System Center Configuration Manager (SCCM)

Tip: To view whether your Microsoft SCCM credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Microsoft System Center Configuration Manager (SCCM) is available to manage large groups of Windows-based systems. Tenable Nessus can query the SCCM service to verify whether or not patches are installed on systems managed by SCCM and display the patch information through the scan results.

Tenable Nessus connects to the server that is running the SCCM site (e.g., credentials must be valid for the SCCM service, so the selected user must have privileges to query all the data in the SCCM MMC). This server may also run the SQL database, or the database and the SCCM repository can be on separate servers. When leveraging this audit, Tenable Nessus must connect to the SCCM server via WMI and HTTPS.

Note: SCCM scanning with Tenable products requires one of the following roles: **Read-only Analyst**, **Operations Administrator**, or **Full Administrator**. For more information, see Setting Up SCCM Scan Policies.

SCCM scanning uses the following Tenable plugins: 57029, 57030, 73636, and 58186.

Note: SCCM patch management plugins support versions from SCCM 2007 up to and including Configuration Manager version 2309.

Credential	Description	Default
Server	(Required) The SCCM IP address or system name.	-
Domain	(Required) The name of the SCCM server's domain.	-
Username	(Required) The username for the SCCM user account that Tenable Nessus uses to perform checks on the target system. The user account must have privileges to query all data in the SCCM MMC.	-
Password	(Required) The password for the SCCM user with privileges to query all data in the SCCM MMC.	-

Windows Server Update Services (WSUS)

Tip: To view whether your Microsoft WSUS credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Windows Server Update Services (WSUS) is available from Microsoft to manage the distribution of updates and hotfixes for Microsoft products. Tenable Nessus can query WSUS to verify whether or not patches are installed on systems managed by WSUS and display the patch information through the Tenable Nessus user interface.

WSUS scanning uses the following Tenable plugins: 57031, 57032, and 58133.

Option	Description	Default
Server	(Required) The WSUS IP address or system name.	-
Port	(Required) The TCP port that Microsoft WSUS listens on for communications from Tenable Nessus.	8530
Username	(Required) The username for the WSUS administrator account that Tenable Nessus uses to perform checks on	-

Option	Description	Default
	the target system.	
Password	(Required) The password for the WSUS administrator user.	-
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	Enabled

Red Hat Satellite 6 Server

Tip: To view whether your Red Hat Satellite 6 Server credentials were successfully authenticated, view the plugin output of the `integration_status.nasl` plugin once the scan is complete. For more information, see Plugins.

Red Hat Satellite 6 is a systems management platform for Linux-based systems. Tenable Nessus can query Satellite to verify whether or not patches are installed on systems managed by Satellite and display the patch information.

Although not supported by Tenable, the Red Hat Satellite 6 plugin also works with Spacewalk Server, the Open Source Upstream Version of Red Hat Satellite. Spacewalk can manage distributions based on Red Hat (RHEL, CentOS, Fedora) and SUSE. Tenable supports the Satellite server for Red Hat Enterprise Linux.

Red Hat Satellite 6 scanning uses the following Tenable plugins: 84236, 84235, 84234, 84237, 84238, 84231, 84232, and 84233.

Option	Description	Default
Satellite server	(Required) The Red Hat Satellite 6 IP address or system	-

Option	Description	Default
	name.	
Port	(Required) The TCP port that Red Hat Satellite 6 listens on for communications from Tenable Nessus.	443
Username	(Required) The username for the Red Hat Satellite 6 account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the Red Hat Satellite 6 user.	-
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	Enabled

Symantec Altris

Altiris is available from Symantec to manage the distribution of updates and hotfixes for Linux, Windows, and macOS systems. Tenable Nessus has the ability to use the Altiris API to verify whether or not patches are installed on systems managed by Altiris and display the patch information through the Tenable Nessus user interface.

Tenable Nessus connects to the Microsoft SQL server that is running on the Altiris host. When leveraging this audit, if the MSSQL database and Altiris server are on separate hosts, Tenable Nessus must connect to the MSSQL database, not the Altiris server.

Altiris scanning uses the following Tenable plugins: 78013, 78012, 78011, and 78014.

Credential	Description	Default
Server	(Required) The Altiris IP address or system name.	-

Credential	Description	Default
Database Port	(Required) The TCP port that Altiris listens on for communications from Tenable Nessus.	5690
Database Name	(Required) The name of the MSSQL database that manages Altiris patch information.	Symantec_CMDB
Database Username	(Required) The username for the Altiris MSSQL database account that Tenable Nessus uses to perform checks on the target system. Credentials must be valid for a MSSQL databas account with the privileges to query all the data in the Altiris MSSQL database.	-
Database Password	(Required) The password for the Altiris MSSQL database user.	-
Use Windows Authentication	When enabled, use NTLMSSP for compatibility with older Windows Servers. When disabled, use Kerberos.	Disabled

Plaintext Authentication Credentials

Caution: Tenable does not recommend using plaintext credentials. Use encrypted authentication methods when possible.

If a secure method of performing credentialed checks is not available, users can force Nessus to try to perform checks over unsecure protocols; use the Plaintext Authentication options.

This menu allows the Nessus scanner to use credentials when testing HTTP , NNTP, FTP, POP2, POP3, IMAP, IPMI, telnet/rsh/rexec, and SNMPv1/v2c.

By supplying credentials, Nessus can perform more extensive checks to determine vulnerabilities. Nessus uses the supplied HTTP credentials for Basic and Digest authentication only.

Credentials for FTP, IPMI, NNTP, POP2, and POP3 require only a username and password.

HTTP

There are four different types of HTTP Authentication methods: Automatic authentication, Basic/Digest authentication, HTTP login form, and HTTP cookies import.

HTTP Global Settings

Option	Default	Description
Login method	POST	Specify if the login action is performed via a GET or POST request.
Re-authenticate delay (seconds)	0	The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.
Follow 30x redirections (# of levels)	0	If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.
Invert authenticated regex	Disabled	A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (for example, Authentication failed!).
Use authenticated regex on HTTP headers	Disabled	Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to determine the authentication state more accurately.
Use authenticated regex on HTTP headers	Disabled	The regex searches are case sensitive by default. This instructs Nessus to ignore case.

Authentication methods

Automatic authentication

Username and Password Required

Basic/Digest authentication

Username and Password Required

HTTP Login Form

The HTTP login page settings provide control over where authenticated testing of a custom web-based application begins.

Option	Description
Username	Login user's name.
Password	Password of the user specified.
Login page	The absolute path to the login page of the application (for example, /login.html).
Login submission page	The action parameter for the form method. For example, the login form for <form method="POST" name="auth_form" action="/login.php"> would be /login.php.
Login parameters	Specify the authentication parameters (for example, login=%USER%&password=%PASS%). If you use the keywords %USER% and %PASS%, they are substituted with values supplied on the Login configurations drop-down box. You can use this field to provide more than two parameters if required (for example, a group name or some other piece of information is required for the authentication process).
Check authentication on page	The absolute path of a protected web page that requires authentication, to assist Nessus in determining authentication status (for example, /admin.html).
Regex to verify successful authentication	A regex pattern to look for on the login page. Simply receiving a 200-response code is not always sufficient to determine session state. Nessus can attempt to match a given string such as "Authentication successful!"

HTTP cookies import

To facilitate web application testing, Nessus can import HTTP cookies from another piece of software (for example, browser, web proxy, etc.) with the HTTP cookies import settings. You can

upload a cookie file so that Nessus uses the cookies when attempting to access a web application. The cookie file must be in Netscape format.

NNTP

Setting	Description	Default
Username	(Required) The username for the NNTP account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the NNTP user.	-

FTP

Setting	Description	Default
Username	(Required) The username for the FTP account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the FTP user.	-

POP2

Setting	Description	Default
Username	(Required) The username for the POP2 account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the POP2 user.	-

POP3

Setting	Description	Default
Username	(Required) The username for the POP3 account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the POP3 user.	-

IMAP

Setting	Description	Default
Username	(Required) The username for the IMAP account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the IMAP user.	-

IPMI

Setting	Description	Default
Username	(Required) The username for the IMPI account that Tenable Nessus uses to perform checks on the target system.	-
Password (sent in clear)	(Required) The password for the IPMI user.	-

telnet/rsh/rexec

The telnet/rsh/rexec authentication section is also username and password, but there are more Global Settings for this section that can allow you to perform patch audits using any of these three protocols.

SNMPv1/v2c

SNMPv1/v2c configuration allows you to use community strings for authentication to network devices. You can configure up to four SNMP community strings.

Setting	Description	Default
Community string	(Required) The community string Tenable Vulnerability Management uses to authenticate on the host device.	public
Global Credential Settings		

UDP Port	(Required) The TCP ports that SNMPv1/v2c listens on for communications from Tenable Nessus.	161
Additional UDP port #1		
Additional UDP port #2		
Additional UDP port #3		

Web Authentication Credentials

The following are the available Web Authentication credentials in Tenable Nessus **Web App** templates:

> **Note:** The following settings only apply to web application scanning in Tenable Nessus. To view settings for the Tenable Web App Scanning product, see Tenable Web App Scanning Scan Settings.

HTTP Server Authentication

In a web application scan, you can configure the following settings for HTTP server-based authentication credentials.

Option	Action
Username	Type the username that Tenable Nessus should use to authenticate to the HTTP-based server.
Password	Type the password that Tenable Nessus should use to authenticate to the HTTP-based server.
Authentication Type	In the drop-down list, select one of the following authentication types: • **Basic** • **NTLM** • **Kerberos**
Kerberos Realm	(Required when enabling the Kerberos Authentication Type) Type the

	realm to which Kerberos Target Authentication belongs.
Key Distribution Center (KDC)	(Required when enabling the Kerberos Authentication Type) Type the host that supplies the user session tickets.

Web Application Authentication

In a web application scan, you can configure one of the following types of **Web Application Authentication** credentials:

- Login Form Authentication
- Cookie Authentication
- Selenium Authentication

Login Form Authentication

Option	Action
Authentication Method	In the drop-down box, select **Login Form**.
Login Page	Type the URL of the login page for the web application you want to scan.
Login Parameters	Type the login parameters for the web application you want to scan. Enter the parameters as JSON key value pairs (for example, `{"username": "example_user","password": "example_password"}`).
Pattern to Verify Successful Authentication	Type a word, phrase, or regular expression that appears on the website only if the authentication is successful (for example, **`Welcome, *your username*!`**). Note that leading slashes will be escaped and `.*` is not required at the beginning or end of the pattern.
Page to Verify Active Session	Type the URL that Tenable Nessus can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, **`Hello, *your username*.`**).

	Note that leading slashes will be escaped and `.*` is not required at the beginning or end of the pattern.

Cookie Authentication

Option	Action
Authentication Method	In the drop-down box, select **Cookie Authentication**.
Cookies	Enter the cookie key and value pairs as a comma-separated list. The pairs must be unencoded and in valid JSON formatting. For example: `{"name" : "value","name2" : "value2","name3" : "value3"}`
Page to Verify Active Session	Type the URL that Tenable Nessus can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, **`Hello, *your username*.`**). Note that leading slashes will be escaped and `.*` is not required at the beginning or end of the pattern.

Selenium Authentication

Option	Action
Authentication Method	Select **Selenium Authentication**.
Selenium Script (.side)	Do the following: a. In the Selenium IDE extension, record your authentication credentials in the Selenium IDE extension. b. Click **Add File**. The file manager for your operating system appears. c. Navigate to and select your Selenium credentials `.side` file.

	Tenable Nessus imports the credentials file.
Page to Verify Active Session	Type the URL that Tenable Nessus can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, **`Hello, *your username*.`**). Note that leading slashes will be escaped and `.*` is not required at the beginning or end of the pattern.

Compliance

Note: This feature is not available in Tenable Nessus Essentials or Essentials Plus. For information about upgrading to Tenable Nessus Professional, see Tenable Nessus Professional.

Note: If a scan is based on a user-defined policy, you cannot configure **Compliance** settings in the scan. You can only modify these settings in the related user-defined policy.

Tenable Nessus can perform vulnerability scans of network services as well as log in to servers to discover any missing patches.

However, a lack of vulnerabilities does not mean the servers are configured correctly or are "compliant" with a particular standard.

You can use Tenable Nessus to perform vulnerability scans and compliance audits to obtain all of this data at one time. If you know how a server is configured, how it is patched, and what vulnerabilities are present, you can determine measures to mitigate risk.

At a higher level, if this information is aggregated for an entire network or asset class, security and risk can be analyzed globally. This allows auditors and network managers to spot trends in non-compliant systems and adjust controls to fix these on a larger scale.

When configuring a scan or policy, you can include one or more compliance checks, also known as audits. Each compliance check requires specific credentials.

Some compliance checks are preconfigured by Tenable, but you can also create and upload custom audits.

For more information on compliance checks and creating custom audits, see the Compliance Checks Reference.

Note: The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements.

Compliance Check	Required Credentials
Adtran AOS	SSH
Alcatel TiMOS	SSH
Amazon AWS	Amazon AWS
Arista EOS	SSH
ArubaOS	SSH
Blue Coat ProxySG	SSH
Brocade FabricOS	SSH
Check Point GAiA	SSH
Cisco ACI	SSH
Cisco Firepower	SSH
Cisco IOS	SSH
Cisco Viptela	SSH
Citrix Application Delivery	Citrix NITRO API
Database	Database
Extreme ExtremeXOS	SSH
F5	F5
FireEye	SSH
Fortigate FortiOS	SSH
Generic SSH	SSH
Google Cloud Platform	Google Cloud Platform

Compliance Check	Required Credentials
HP ProCurve	SSH
Huawei VRP	SSH
IBM DB2 DB	Database
IBM iSeries	IBM iSeries or SSH
Juniper Junos	SSH
Microsoft Azure	Microsoft Azure
Mobile Device Manager	AirWatch or Mobileiron
MongoDB	MongoDB
Microsoft SQL DB	Database
MySQL DB	Database
NetApp API	NetApp API
NetApp Data ONTAP	SSH
OpenShift Container Platform	OpenShift Container Platform
OpenStack	OpenStack
Oracle DB	Database
Palo Alto Networks PAN-OS	PAN-OS
PostgreSQL DB	Database
Rackspace	Rackspace
RHEV	RHEV
Salesforce.com	Salesforce SOAP API
Snowflake	Snowflake API
SonicWALL SonicOS	SSH

Compliance Check	Required Credentials
Splunk	Splunk API
Sybase DB	Database
Unix	SSH
Unix File Contents	SSH
VMware vCenter/vSphere	VMware vCenter API or VMware ESX SOAP API
WatchGuard	SSH
Windows	Windows
Windows File Contents	Windows
Zoom	Zoom
ZTE ROSNG	SSH

Note: Plugins sometimes produce errors that fall into one of the following scenarios:

- Something should be notified as a concern, but not at the risk of impacting the results of a large scan
- Something happened where the plugin was unable to report issues

In either one of these scenarios, a compliance result with the name `Compliance Plugin Errors: <plugin name>` is posted as a WARNING. The output of the compliance results identifies the issue that should be reviewed. These results are posted by the plugin 214001 Compliance Status.

Upload a Custom Audit File

Note: This feature is not available in Tenable Nessus Essentials or Essentials Plus. For information about upgrading to Tenable Nessus Professional, see Tenable Nessus Professional.

When you configure the Compliance settings of a Nessus scan, you can upload the following custom audit files:

- A Tenable-created audit file downloaded from the Tenable downloads page.
- A Security Content Automation Protocol (SCAP) Data Stream file downloaded from a SCAP repository (for example, https://ncp.nist.gov/repository).

  The file must contain full SCAP content (Open Vulnerability and Assessment Language (OVAL) and Extensible Configuration Checklist Description Format (XCCDF) content) or OVAL standalone content.
- A custom audit file created or customized for a specific environment. For more information, see the Nessus Compliance Checks Reference.

Before you begin:

- Download or prepare the file you intend to upload.

  Note: Unlike standard audit files, you cannot configure custom audit file variable parameters in the Tenable Nessus user interface. To do this, you must edit the parameters directly in the audit file before uploading to Tenable Nessus.

  For example, when you upload a standard **CIS CentOS 6 Server L1 v3.0.0** audit file to Tenable Nessus, the user interface allows you to configure a parameter named **Network Time**.

  If you want to change **Network Time** from its default value in a custom audit file, search for that field in the custom audit file. You will find the field's variable name: **NTP_SERVER**.

  Next, search for **@NTP_SERVER@**. Enclose the variable name with "@"s when performing this search.

  You will find four locations:

  - `regex : "^[\\s]*server[\\s]+@NTP_SERVER@[\\s]*$"`
  - `expect: "^[\\s]*server[\\s]+@NTP_SERVER@[\\s]*$"`
  - `regex : "^[\\s]*server[\\s]+@NTP_SERVER@"`
  - `expect: "^[\\s]*server[\\s]+@NTP_SERVER@"`

  Update the value you want to change directly in the audit file (**192.0.2.0** in this example):

  - `regex : "^[\\s]*server[\\s]+192.0.2.0[\\s]*$"`
  - `expect: "^[\\s]*server[\\s]+192.0.2.0[\\s]*$"`

- `regex : "^[\\s]*server[\\s]+192.0.2.0"`
- `expect: "^[\\s]*server[\\s]+192.0.2.0"`

Perform this search and replace process for all variables that you want to change from the default values.

To upload a custom audit file:

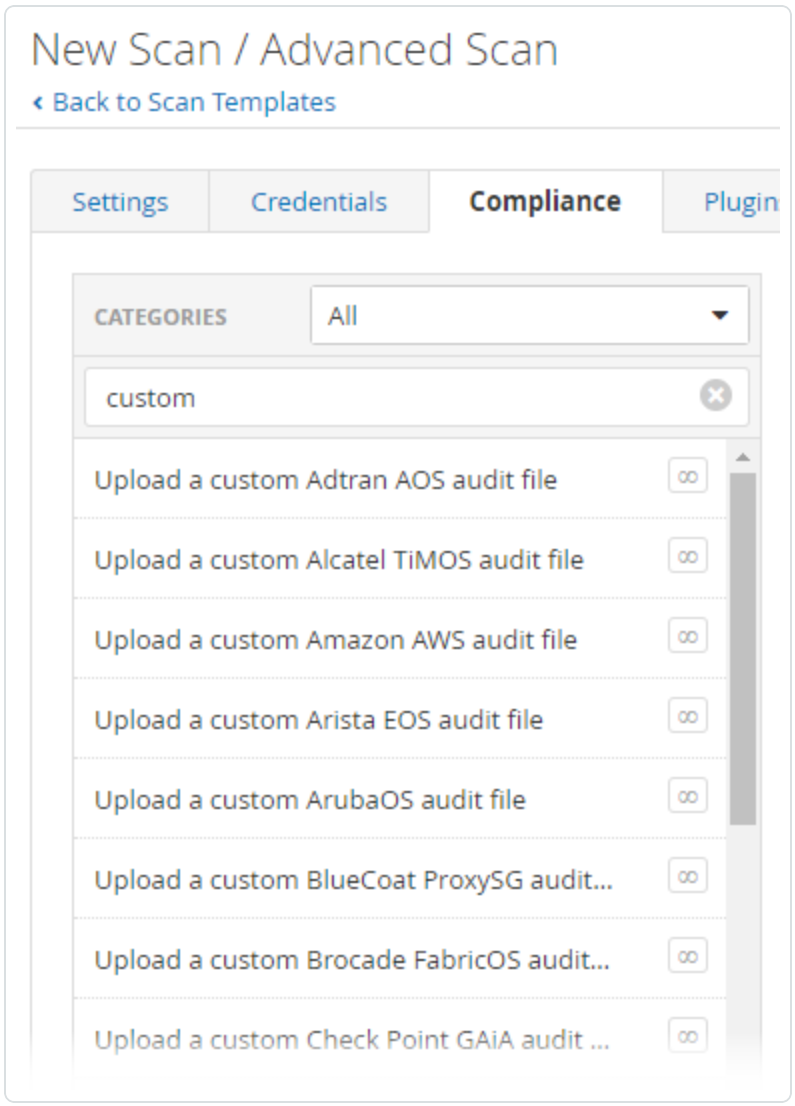
1. Log in to the Tenable Nessus user interface.
2. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.
3. In the upper right corner, click the **New Scan** button.

   The **Scan Templates** page appears.
4. Click the scan template that you want to use.

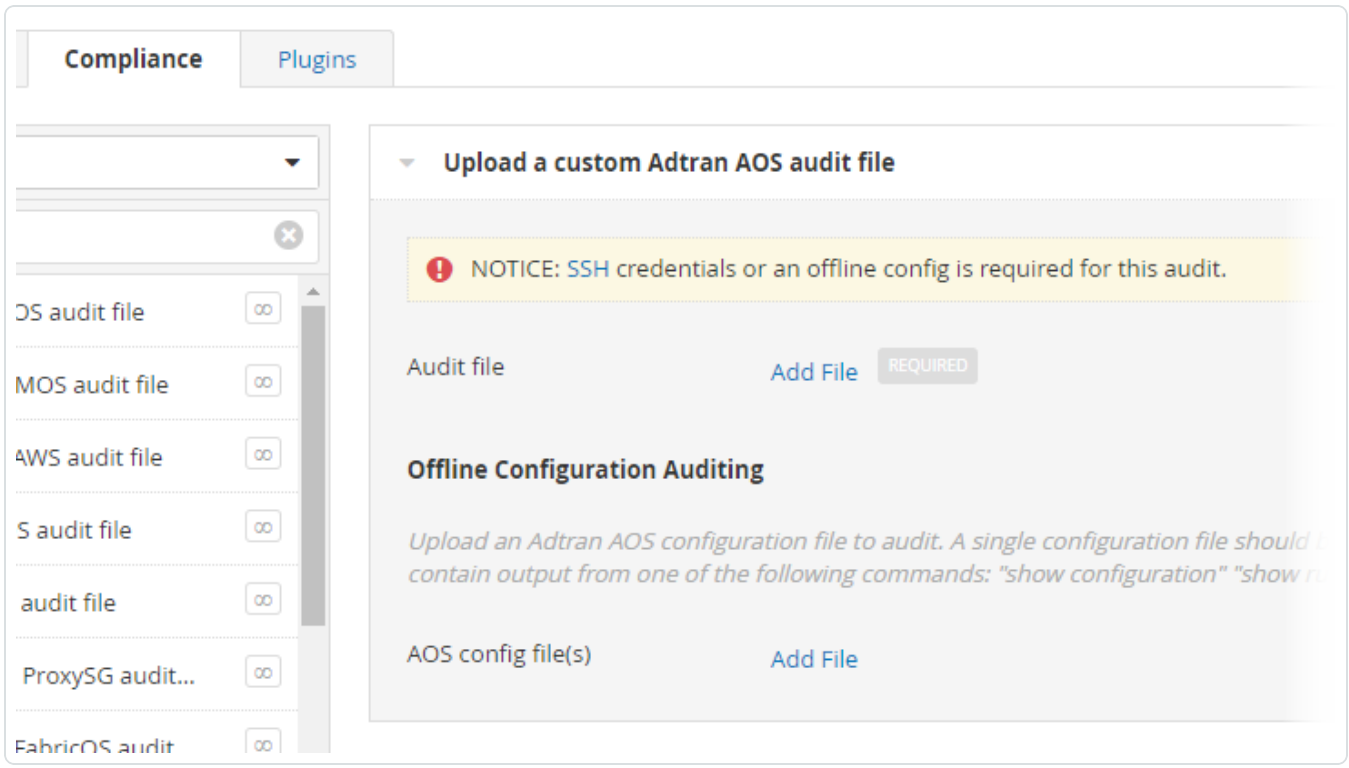
   The scan settings page appears.
5. Open the **Compliance** tab.
6. In the **Filter Compliance** box, type `custom`.

   A list of the custom audit file types that you can upload appears.



7. Select the custom audit file type that you want to upload.

   An **Upload a custom audit file** pane appears.



8. Click **Add File**. Select the custom audit file to upload from your machine.

   Depending on the audit type, you may need to configure additional settings once you upload the custom audit.

9. Do one of the following:

   - To launch the scan immediately, click the button, and then click **Launch**.

     Tenable Nessus saves and launches the scan.

   - To launch the scan later, click the **Save** button.

     Tenable Nessus saves the scan.

SCAP Settings

Security Content Automation Protocol (SCAP) is an open standard that enables automated management of vulnerabilities and policy compliance for an organization. It relies on multiple open standards and policies, including OVAL, CVE, CVSS, CPE, and FDCC policies.

When you select the **SCAP and OVAL Auditing** template, you can modify SCAP settings.

Note: The **SCAP and OVAL Auditing** scan template is retained for backward compatibility. This template supports SCAP version 1.2 and earlier, which is not compatible with modern operating systems such as Windows 10 and Windows 11 that require SCAP version 1.3 or later.

You can select **Linux (SCAP)**, **Linux (OVAL)**, **Windows (SCAP)**, or **Windows (OVAL)**. The following table describes the settings for each option.

Setting	Default Value	Description
Linux (SCAP) or **Windows (SCAP)**		
SCAP File	None	A valid zip file that contains full SCAP content (XCCDF, OVAL, and CPE for versions 1.0 and 1.1; DataStream for version 1.2).
SCAP Version	1.2	The SCAP version that is appropriate for the content in the uploaded SCAP file.
SCAP Data Stream ID	None	(SCAP Version 1.2 only) The Data Stream ID that you copied from the SCAP XML file. Example: `<data-stream id="scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip">`
SCAP Benchmark ID	None	The Benchmark ID that you copied from the SCAP XML file. Example: `<xccdf:Benchmark id="xccdf_gov.nist_benchmark_USGCB-Windows-7">`
SCAP Profile ID	None	The Profile ID that you copied from the SCAP XML file.

		Example: `<xccdf:Profile id="xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1">`
OVAL Result Type	Full results w/ system characteristics	The information you want the results file to include. The results file can be one of the following types: full results with system characteristics, full results without system characteristics, or thin results.
Linux (OVAL) or **Windows (OVAL)**		
OVAL definitions file	None	A valid zip file that contains OVAL standalone content.

Plugins

Some Tenable Nessus templates include **Plugin** options.

Plugins options enable you to select security checks by **Plugin Family** or individual plugins checks.

For more information on specific plugins, see the Tenable plugins site. For more information on plugin families, see About Plugin Families on the Tenable plugins site.

Note: When you create and save a scan or policy, it records all the plugins that you select initially. When Tenable Nessus receives new plugins via a plugin update, Nessus enables the new plugins automatically if the family they are associated with is enabled. If the family was disabled or partially enabled, Nessus also disables the new plugins in that family.

Plugin Families

Clicking on the **Plugin Family** allows you to enable (**green**) or disable (**gray**) the entire family. Selecting a family shows the list of its plugins. You can enable or disable individual plugins to create specific scans.

A family with some plugins disabled is purple and shows **Mixed** to indicate only some plugins are enabled. Clicking on the plugin family loads the complete list of plugins, and allow for granular selection based on your scanning preferences.

Mixed plugin families have a padlock icon that is locked or unlocked.

- Locked — New plugins added to the plugin family via plugin feed updates are *disabled* in the policy automatically.
- Unlocked — New plugins added to the plugin family via plugin feed updates are *enabled* in the policy automatically.

Click the padlock to lock or unlock the plugin family.

Caution: The **Denial of Service** family contains some plugins that could cause outages on a network if you do not enable the Safe Checks option, in addition to some useful checks that do not cause any harm. You can use the **Denial of Service** family with Safe Checks to ensure that Tenable Nessus does not run any potentially dangerous plugins. However, Tenable recommends that you do not use the **Denial of Service** family on a production network unless scheduled during a maintenance window and with staff ready to respond to any issues.

View Plugin Output Details

Selecting a specific **Plugin Name** shows the plugin output that you would see in a report.

The plugin details include the information described in the following table. Some plugins do not provide all the listed information.

Section	Description
Synopsis	View an overview of the plugin.
Description	View a detailed description of the plugin and its related vulnerability.
Solution	View the plugin vulnerability's solution.
See Also	View security advisories related to the plugin.
Plugin Information	View the following plugin information: • **ID** — The plugin's numeric ID. • **Version** — The plugin's current version.

	• **Type** — The plugin's type, which specifies how the plugin operates when run by a scanner.
	  • **remote** — The plugin does not attempt or require authentication to the local host. Instead, it remotely collects information through banner checks, testing for a patch, or exploiting a vulnerability. Some plugins may attempt to sign in to a service, but do not require local host credentials.
	  • **local** — The plugin authenticates to a target through a service (for example, SMB or SSH) and extracts information.
	  • **combined** — The plugin collects information via remote and local checks. If local checks are unavailable, the plugin still gathers what it can from the remote checks within the plugin.
	  • **settings** — The plugin defines one or more settings used by other plugins throughout the scan.
	  • **summary** — The plugin summarizes data collected by other plugins.
	  • **third party** — The plugin runs a third-party application (for example, nmap).
	  • **reputation** — Uses a third-party reputation service.
	• **Published** — The date on which the plugin was published.
	• **Modified** — The date on which the plugin was last modified.

Risk Information	View the plugin's following vulnerability risk information: • **Vulnerability Priority Rating (VPR)** — The vulnerability's numeric VPR rating. For more information about VPR, see CVSS Scores vs. VPR. • **Exploit Prediction Scoring System (EPSS)** — The vulnerability's numeric EPSS rating. • **Risk Factor** — The vulnerability's VPR severity level. For more information about VPR, see CVSS Scores vs. VPR.

	• **CVSS v4.0 Base Score** — The vulnerability's base CVSS v4.0 score. A vulnerability's base score is determined when the vulnerability is initially discovered and does not change over time. • **CVSS v4.0 Vector** — A textual representation of the metric values used to determine the vulnerability's CVSS v4.0 base score. • **CVSS v4.0 Temporal Vector** — A textual representation of the metric values used to determine the vulnerability's CVSS v4.0 temporal score. • **CVSS v4.0 Temporal Score** — The vulnerability's temporal CVSS v4.0 score. Temporal scores, unlike base scores, are updated over time based on activities conducted both by software vendors and hackers. • **CVSS v3.0 Base Score** — The vulnerability's base CVSS v3.0 score. A vulnerability's base score is determined when the vulnerability is initially discovered and does not change over time. • **CVSS v3.0 Vector** — A textual representation of the metric values used to determine the vulnerability's CVSS v3.0 base score. • **CVSS v3.0 Temporal Vector** — A textual representation of the metric values used to determine the vulnerability's CVSS v3.0 temporal score. • **CVSS v3.0 Temporal Score** — The vulnerability's temporal CVSS v3.0 score. Temporal scores, unlike base scores, are updated over time based on activities conducted both by software vendors and hackers. • **CVSS v2.0 Base Score** — The vulnerability's base CVSS v2.0 score. A vulnerability's base score is determined when the vulnerability is initially discovered and does not change over time. • **CVSS v2.0 Vector** — A textual representation of the metric values used to determine the vulnerability's CVSS v2.0 base score. • **CVSS v2.0 Temporal Vector** — A textual representation of the metric values used to determine the vulnerability's CVSS v2.0 temporal score. • **CVSS v2.0 Temporal Score** — The vulnerability's temporal CVSS v2.0 score. Temporal scores, unlike base scores, are updated over time

	based on activities conducted both by software vendors and hackers. • **IAVM Severity** — The vulnerability's Information Assurance Vulnerability Management (IAVM) severity level.
Vulnerability Information	View the plugin's following vulnerability information: • **CPE** — The plugin's Common Platform Enumeration (CPE). • **Exploit Available** — Specifies whether there is currently a publicly known exploit available against the plugin. If there are exploits available, Tenable Nessus lists the exploits in the **Exploitable With** subsection. • **Exploitability Ease** — Specifies how exploitable the plugin is. • **Patch Published** — Specifies the last date on which there was a patch published for the plugin. • **Vulnerability Published** — Specifies the last date on which the plugin's vulnerability became publicly known.
Reference Information	View the plugin's related reference material (CVE, CWE, CERT, IAVA, BID, SECUNIA, or other related information).

To view more detailed information about the plugin, search for the plugin on the Tenable Plugins website.

Note: When viewing plugins on the Tenable Plugins website, some plugins are documented with the following note: *"Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number."* This note means that Tenable does not have a complete resolution for the plugin's vulnerability and must manually validate whether the vulnerability is resolved.

Configure Dynamic Plugins

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

With the **Advanced Dynamic Scan** template, you can create a scan or policy with dynamic plugin filters instead of manually selecting plugin families or individual plugins. As Tenable releases new plugins, any plugins that match your filters are added to the scan or policy automatically. This

allows you to tailor your scans for specific vulnerabilities while ensuring that the scan stays up to date as new plugins are released.

For more information on specific plugins, see the Tenable plugins site. For more information on plugin families, see About Plugin Families on the Tenable plugins site.

To configure dynamic plugins:

1. Do one of the following:
   - Create a Scan.
   - Create a Policy.
2. Click the **Advanced Dynamic Scan** template.
3. Click the **Dynamic Plugins** tab.
4. Specify your filter options:
   - **Match Any or Match All:** If you select **All**, only results that match all filters appear. If you select **Any**, results that match any one of the filters appear.
   - **Plugin attribute:** See the Plugin Attributes table for plugin attribute descriptions.
   - **Filter argument:** Select **is equal to**, **is not equal to**, **contains**, **does not contain**, **greater than**, or **less than** to specify how the filter should match for the selected plugin attribute.
   - **Value:** Depending on the plugin attribute you selected, enter a value or select a value from the drop-down menu.
5. (Optional) Click ⊕ to add another filter.
6. Click **Preview Plugins**.

   Tenable Nessus lists the plugins that match the specified filters.
7. Click **Save**.

   Tenable Nessus creates the scan or policy, which automatically updates when Tenable adds new plugins that match the dynamic plugin filters.

Create a Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

Note: You cannot create and launch scans, create or view policies or plugin rules, or use the upgrade assistant while Tenable Nessus compiles plugins.

Note: If you are scanning a Linux machine with Tenable Nessus, the Linux machine's shell configuration file must have a `PS1` variable of four or more characters (for example, `PS1='\u@\h:~\$ '`). Having a `PS1` variable of less than four characters (for example, `PS1='\$ '`) can drastically increase the overall scan time.

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

   The **My Scans** page appears.

2. In the upper right corner, click the **New Scan** button.

   The **Scan Templates** page appears.

3. Click the scan template that you want to use.

4. Configure the scan's settings.

5. Do one of the following:

   - To launch the scan immediately, click the button, and then click **Launch**.

     Tenable Nessus saves and launches the scan.

   - To launch the scan later, click the **Save** button.

     Tenable Nessus saves the scan.

Create a Host Discovery Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

Knowing what hosts are on your network is the first step to any vulnerability assessment. Launch a host discovery scan to see what hosts are on your network (and associated information such as IP address, FQDN, operating systems, and open ports, if available). After you have a list of hosts, you can choose what hosts you want to target in a specific vulnerability scan.

The following overview describes a typical workflow of creating and launching a host discovery scan, then creating a follow-up scan that target-discovered hosts that you choose.

Create and launch a host discovery scan

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

   The **My Scans** page appears.

2. In the upper right corner, click the **New Scan** button.

   The **Scan Templates** page appears.

3. Under **Discovery**, click the **Host Discovery** template.

4. Configure the host discovery scan:

   - For **Name**, enter a name for the scan.
   - For **Targets**, enter targets as hostnames, IPv4 addresses, or IPv6 addresses.

     > **Tip:** For IP addresses, you can use CIDR notation (for example, 192.168.0.0/24), a range (for example, 192.168.0.1-192.168.0.255), or a comma-separated list (for example, 192.168.0.0,192.168.0.1). For more information, see Scan Targets.

   - (Optional) Configure the remaining settings.

5. To launch the scan immediately, click the button, and then click **Launch**.

   Tenable Nessus runs the host discovery scan, and the **My Scans** page appears.

6. In the scans table, click the row of a completed host discovery scan.

   The scan's results page appears.

7. In the **Hosts** tab, view the hosts that Tenable Nessus discovered, and any available associated information, such as IP address, FQDN, operating system, and open ports.

Create and launch a scan on one or more discovered hosts

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

   The **My Scans** page appears.

2. In the scans table, click the row of your completed host discovery scan.

   The scan's results page appears.

3. Click the **Hosts** tab.

   Tenable Nessus displays a table of scanned hosts.

4. Select the check box next to each host you want to scan in your new scan.

   At the top of the page, the **More** button appears.

5. Click the **More** button.

   A drop-down box appears.

6. Click **Create Scan**.

   The **Scan Templates** page appears.

7. Select a scan template for your new scan.

   Tenable Nessus automatically populates the **Targets** list with the hosts you previously selected.

8. Configure the rest of the scan settings, as described in Scan and Policy Settings.

9. To launch the scan immediately, click the button, and then click **Launch**.

   Tenable Nessus saves and launches the scan.

Create an Agent Scan

> **Required user role when using Tenable Nessus Manager:** Standard, Administrator, or System Administrator

To create an agent scan:

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

   The **My Scans** page appears.

2. In the upper-right corner, click the **New Scan** button.

   The **Scan Templates** page appears.

3. Click the **Agent** tab.

   The **Agent** scan templates page appears.

4. Click the scan template that you want to use.

   Tip: Use the search box in the top navigation bar to filter templates on the tab currently in view.

5. Configure the scan's settings.

6. (Optional) Configure compliance checks for the scan.

7. (Optional) Configure security checks by plugin family or individual plugin.

8. Do one of the following:

   - If you want to launch the scan later, click the **Save** button.

     Tenable Nessus saves the scan.

   - If you want to launch the scan immediately:

     a. Click the button.

     b. Click **Launch**.

     Tenable Nessus saves and launches the scan.

Create a Web Application Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

Use the following procedure to create and launch a web application scan in Tenable Nessus Expert. For more information on web application scanning with Tenable Nessus, see Web Application Scanning in Tenable Nessus.

Note: Tenable Nessus Expert only allows one concurrent web application scan at a time.

Before you begin:

Install Tenable Web App Scanning in Tenable Nessus. Doing so gives you access to the **Web App** scan templates.

To create a WAS scan:

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

   The **My Scans** page appears.

2. In the upper-right corner, click the **New Scan** button.

   The **Scan Templates** page appears.

3. Click the **Web App** tab.

   The **Web App** scan templates page appears.

4. Click the **Web App** scan template that you want to use.

5. Configure the scan:

   - Configure the Basic, Scope, Assessment, and Advanced settings. Depending on the scan template you choose, some of these settings may not be available for configuration.

     For WAS scans, you must at least name the scan and configure a **Target URL**. The **Target URL** specifies the URL for the target you want to scan. Targets must start with the `http://` or `https://` protocol identifier; regular expressions and wildcards are not allowed.

     > **Note:** If the URL you type in the **Target URL** box has a different FQDN host from the URL that appears on your license, and your scan runs successfully, the new URL you type counts as an additional asset on your license.

     > **Note:** If you create a user-defined scan template, the **Target URL** setting is not saved to the template. Type a target each time you create a new scan.

   - (Optional) Configure web authentication credentials for the scan.

   - (Optional) Enable or disable individual plugins.

6. Do one of the following:

   - If you want to launch the scan later, click the **Save** button.

     Tenable Nessus saves the web application scan.

   - If you want to launch the scan immediately:

a. Click the button.

b. Click **Launch**.

Tenable Nessus saves and launches the web application scan.

For information on viewing and interpreting web application scan results, see the following video: Web App Vulnerability Analysis in Nessus Expert 10.6.

Create an Attack Surface Discovery Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

Note: The Attack Surface Discovery scan template is only available in Tenable Nessus Expert.

You can use Tenable Nessus's integration with Tenable Attack Surface Management to create an attack surface discovery scan. This scan type allows you to scan top-level domains and generate DNS records based on the scan findings. Tenable Nessus Expert allows you to scan up to five different licensed domains.

To create an attack surface discovery scan:

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

   The **My Scans** page appears.

2. In the upper right corner, click the **New Scan** button.

   The **Scan Templates** page appears.

3. Under **Discovery**, click the **Attack Surface Discovery** template.

4. Configure the scan:

   a. For **Basic**, enter the scan name, description, schedule, and the folder to save the scan in.

   b. For **Discovery**, enter the top-level domains you want to scan. You can enter up to five domains.

> **Note:** You can only enter two-part domains (for example, you can enter `tenable.com`, but you cannot enter `docs.tenable.com`). If you need to scan multiple domains, list them in a comma-separated list (for example, `tenable.com, test.com, example.com`).

5. Do one of the following:

   - To save the scan configuration for later, click **Save**. You can launch it from the folder you selected in step 4.
   - To launch the scan immediately, click the button, and then click **Launch**.

     Tenable Nessus runs the attack surface discovery scan, and the **My Scans** page appears.

What to do next:

- Launch the scan.
- View the scan results.
- Modify the scan settings.
- Create a scan report.

  > **Note:** Tenable Nessus only offers two report templates for attack surface discovery scans: **Complete List of Vulnerabilities by Host** and **Detailed Vulnerabilities By Host**.

- Export the scan results.

  > **Note:** Only the **Nessus DB** export option is available for attack surface discovery scans.

Import a Scan

> **Required user role when using Tenable Nessus Manager:** Standard, Administrator, or System Administrator

You can import an exported Tenable Nessus (`.nessus`) or Tenable Nessus DB (`.db`) scan. With an imported scan, you can view scan results, export new reports for the scan, rename the scan, and update the description. You cannot launch imported scans or update policy settings.

You can also import `.nessus` files as policies. For more information, see Import a Policy.

Tip: You can export a WAS scan from Tenable Security Center to generate a `scan.db`. You can then import the `scan.db` into Tenable Nessus using the following steps.

To import a scan:

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

   The **My Scans** page appears.

2. In the upper-right corner, click **Import**.

   Your browser's file manager window appears.

3. Browse to and select the scan file that you want to import.

   Note: The supported file types are exported Nessus (`.nessus`) and Nessus DB (`.db`) files.

   The **Scan Import** window appears.

4. If the file is encrypted, type the **Password**.

5. Click **Upload**.

   Tenable Nessus imports the scan and its associated data.

Modify Scan Settings

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

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

   The **My Scans** page appears.

2. Optionally, in the left navigation bar, click a different folder.

3. In the scans table, select the check box on the row corresponding to the scan that you want to configure.

   In the upper-right corner, the **More** button appears.

4. Click the **More** button.

5. Click **Configure**.

The **Configuration** page for the scan appears.

6. Modify the settings.
7. Click the **Save** button.

   Tenable Nessus saves the settings.

Configure vSphere Scanning

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

You can configure a scan to scan the following virtual environments:

- ESXi/vSphere that vCenter manages
- ESXi/vSphere that vCenter does not manage
- Virtual machines

Note: You must provide an IPv4 address when scanning an ESXi host. Otherwise, the scan fails.

About VMware Credentialed Checks

Configuring the vCenter API or ESXi API credentials enables the collection of VMware Installation Bundle (VIB) package details for ESXi servers, which are used in the ESX Local Security Checks plugin family. Both of these credentials enable the collection of ESXi VIBs. Configuring an SSH credential to a targeted ESXi server also enables the collection of VIBs.

In addition to collection of ESXi VIBs, the vCenter credential enables auto-discovery of ESXi servers and vCenter compliance checks. In the case of vCenter compliance checks, the vCenter server must be configured as a target.

These credentials do not collect any host-level data about the vCenter server. To collect host-level data, configure an additional credential to the vCenter server (for example, SSH or Windows).

Tenable also collects ESXi and vCenter versions by detecting the software on the targeted hosts using remote, unauthenticated checks. Current vCenter and ESXi vulnerability results are based on this data.

For more information on VMware/vCenter, refer to the VMware integration documentation.

Scenario 1: Scanning ESXi/vSphere Not Managed by vCenter

To configure an ESXi/vSphere scan that vCenter does not manage:

1. Create a scan.
2. In the **Basic** scan settings, in the **Targets** section, type the IP address or addresses of the ESXi host or hosts.
3. Click the **Credentials** tab.

   The **Credentials** options appear.
4. From the **Categories** drop-down, select **Miscellaneous**.

   A list of miscellaneous credential types appears.
5. Click **VMware ESX SOAP API**.

   The VMware ESX SOAP API options appear. For more information, see VMware ESX SOAP API.
6. In the **Username** box, type the username associated with the local ESXi account.
7. In the **Password** box, type the password associated with the local ESXi account.
8. If your vCenter host includes an SSL certificate (not a self-signed certificate), deselect the **Do not verify SSL Certificate** checkbox. Otherwise, select the checkbox.
9. Click **Save**.

Scenario 2: Scanning vCenter-Managed ESXi/vSpheres

> **Note:** The SOAP API requires a vCenter admin account with read and write permissions. The REST API requires a vCenter admin account with read permissions, and a VMware vSphere Lifecycle manager account with read permissions.

To configure an ESXi/vSphere scan managed by vCenter:

1. Create a scan.
2. In the **Basic** scan settings, in the **Targets** section, type the IP addresses of:
    - the vCenter host.
    - the ESXi host or hosts.

    > **Note:** Listing the vCenter as a target results in the scan collecting the vCenter version and its vulnerabilities, but not operating system-level details. Listing the vCenter server as a target is also required for vCenter compliance scanning.
3. Click the **Credentials** tab.

    The **Credentials** options appear.
4. From the **Categories** drop-down, select **Miscellaneous**.

    A list of miscellaneous credential types appears.
5. Click **VMware vCenter SOAP API**.

    The VMware vCenter SOAP API options appear. For more information, see VMware vCenter SOAP API.
6. In the **vCenter Host** box, type the IP address of the vCenter host.
7. In the **vCenter Port** box, type the port for the vCenter host. By default, this value is 443.
8. In the **Username** box, type the username associated with the vCenter account.
9. In the **Password** box, type the password associated with the vCenter account.
10. If the vCenter host is SSL enabled, enable the **HTTPS** toggle.
11. If your vCenter host includes an SSL certificate (not a self-signed certificate), select the **Verify SSL Certificate** checkbox. Otherwise, deselect the checkbox.
12. Click **Save**.

Scenario 3: Scanning Virtual Machines

You can scan virtual machines just like any other host on the network. Be sure to include the IP address or addresses of your virtual machine in your scan targets. Note that virtual machines are

like any other host: you must configure credentials for each guest operating system that you want to scan. For more information, see Create a Scan.

VMware vCenter Support Matrix

Feature	Requires Authentication	Supported vCenter Version
Vulnerability Management	No	7.x, 8.x
Auto Discovery	Yes	7.0.3+, 8.x
Audit / Compliance	Yes	6.x, 7.x, 8.x
VIB Enumeration	Yes	7.0.3+, 8.x
Active / Inactive VMs	Yes	7.0.3+, 8.x

Configure Email Notifications for a Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

You can configure a scan to automatically send an email notification to specified recipients when the scan completes. This helps you and your stakeholders stay informed about scan results without needing to manually check the scan status in Tenable Nessus.

Before you begin:

- Ensure you or your administrator have configured an SMTP server in **Tenable Nessus**. For more information, see SMTP Server.

To configure email notifications for a scan:

1. In the top navigation bar, click **Scans**.
2. Do one of the following:
   - In the upper-right corner of the page, click **New Scan**.
   - Open an existing scan. Then, click **Configure**.
3. In the scan settings menu, click **Basic** > **Notifications**.

4. Configure the following settings:

Setting	Default Value	Description
Email Recipient(s)	None	Specifies zero or more email addresses, separated by commas, that are alerted when a scan completes and the results are available.
Attach Report	Off	(Tenable Nessus Professional and Tenable Nessus Expert only) Specifies whether you want to attach a report to each email notification. This option toggles the **Report Type** and **Max Attachment Size** settings.
Report Type	Nessus	(Tenable Nessus Professional and Tenable Nessus Expert only) Specifies the report type (CSV, Nessus, or PDF) that you want to attach to the email.
Max Attachment Size	25	(Tenable Nessus Professional and Tenable Nessus Expert only) Specifies the maximum size, in megabytes (MB), of any report attachment. If the report exceeds the maximum size, then it is not attached to the email. Tenable Nessus does not support report attachments larger than 50 MB.
Result Filters	None	Defines the type of information to be emailed.

5. Click **Save**.

   Tenable Nessus sends an email notification to the specified recipients after the scan completes.

Configure a Least-Privilege SSH Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

You can use an iterative process in Tenable Nessus to identify the exact permissions required for a complete and accurate credentialed SSH scan, allowing you to create a least-privilege account that avoids the security risks of granting full root access. This process relies on a scan setting and four informational plugins that report on command execution.

You can use this process to resolve the common challenge of negotiating scan credentials with server administrators, which often leads to delays or the assignment of a limited account that produces incomplete scan data.

How It Works

When you enable the **Attempt Least Privilege** scan setting, Tenable Nessus plugins first try to run commands without privilege escalation. If a command fails, Tenable Nessus retries it using privilege escalation (for example, `sudo`) and records the results in the output of four plugins:

- **Plugin ID 102094 (SSH Commands Require Privilege Escalation)** — Lists all commands that failed to run as a standard user and required elevated privileges. The output is in a simple YAML format that you can use to update the `/etc/sudoers` file.

  Example output:

  ```
  Login account : <username>
  Commands failed due to lack of privilege escalation :
   - Escalation account : (none)
   Escalation method  : (none)
   Plugins :
   - Plugin Filename : host_tag_nix.nbin
   Plugin ID       : 87414
   Plugin Name     : Host Tagging (Linux)
   - Command  : "cat /etc/tenable_tag"
   Response : null
   Error    : "\ncat: /etc/tenable_tag: Permission denied"
   - Plugin Filename : nessus_agent_installed_linux.nbin
   Plugin ID       : 110230
   Plugin Name     : Tenable Nessus Agent Installed (Linux)
   - Command  : "strings '/opt/nessus_agent/var/nessus/agent.version' 2>&1"
   Response : "strings: /opt/nessus_agent/var/nessus/agent.version: Permission
  ```

```
denied"
 Error    : ""
```

- **Plugin ID 102095 (SSH Commands Ran With Privilege Escalation)** — Lists all commands that ran successfully with escalated privileges. You can use this output to verify that only authorized commands are running with `sudo`.

  Example output:

```
Login account      : <username>
Escalation account : root
Escalation method  : su
Commands required privilege escalation :
 Plugins :
 - Plugin Filename : bios_get_info_ssh.nasl
 Plugin ID       : 34098
 Plugin Name     : BIOS Info (SSH)
 - Command : "LC_ALL=C dmidecode"
 - Plugin Filename : linux_kernel_speculative_execution_detect.nbin
 Plugin ID       : 125216
 Plugin Name     : Processor Speculative Execution Vulnerabilities (Linux)
 - Command : "head /sys/kernel/debug/x86/pti_enabled"
 - Command : "head /sys/kernel/debug/x86/retp_enabled"
 - Command : "head /sys/kernel/debug/x86/ibrs_enabled"
Command forced to use privilege escalation :
 Plugins :
 - Plugin Filename : netstat_portscan.nasl
 Plugin ID       : 14272
 Plugin Name     : Netstat Portscanner (SSH)
 - Command : "netstat -a -n"
```

- **Plugin ID 100158 (SSH Combined Host Command Logging)** — Shows the log file of the commands that were run. This plugin provides a downloadable debug log file that describes the SSH commands that Tenable Nessus ran during the scan.
- **Plugin ID 84239 (Debugging Log Report)** — Gathers the logs written by other plugins and reports them. This plugin provides an attachment with *all* plugin debug log files available at the end of a scan.

Note that plugins 100158 and 84239 are advanced diagnostic tools and require you enable plugin debugging in the scan configuration. Use these plugins to investigate unexpected scan results, particularly in environments with sophisticated, granular access controls (for example, TACACS).

While plugins 102094 and 102095 report that a command failed or succeeded, the debugging logs from 100158 and 84239 provide the exact command syntax Tenable Nessus passed to the host and the complete error response.

This additional detail can help diagnose complex access issues, such as a security module that allows a base command but blocks that command when used with a specific flag. Because enabling debugging is resource-intensive, Tenable recommends using these plugins only to troubleshoot a specific endpoint.

Example Process to Determine Account Configuration

The following is a workflow you can use to determine the necessary account configuration for a least-privilege SSH scan.

Before you begin:

- The following steps assume the scan target is a Linux server, using `sudo` for command escalation.
- The following steps assume you already know how to create and configure a scan in Tenable Nessus. For more information, see Create a Scan.

To determine permissions for a least-privilege SSH scan:

1. On the target host, create a standard user account for scanning.
2. Log in as the root user.
3. Run the `visudo` command to edit the `/etc/sudoers` file. Configure the new user account with basic `sudo` permissions.
4. In Tenable Nessus, begin creating an advanced scan.
5. Navigate to the **Credentials** tab.
6. Select **SSH**.

7. In the **Elevate privileges with** drop-down box, select **sudo**.
8. Select the **Attempt Least Privilege** check box.

   > **Note:** Enabling **Attempt Least Privilege** may increase scan times by 10–30% because Tenable Nessus attempts some commands twice.

9. Configure the remaining scan settings as needed and save the scan.
10. Launch the scan against the target host.
11. After the scan completes, review the scan results for **Plugin ID 102094 (SSH Commands Require Privilege Escalation)**.
12. (Optional) Review the output of **Plugin ID 102095 (SSH Commands Ran With Privilege Escalation)** to verify which commands are running with escalated privileges.
13. On the target host, edit the `/etc/sudoers` file again. Add the commands reported by plugin 102094 to grant the necessary permissions to the scan account.
14. Relaunch the scan.
15. Repeat steps 11-14 until plugin 102094 no longer reports any failed commands. At this point, the scan account has the precise privileges required for an accurate authenticated scan.

Troubleshoot Complex Access Issues

If you follow the procedure above (reviewing 102094, updating `sudoers`, and relaunching) but plugin 102094 still reports failed commands, you may have a complex access issue. You can use the debugging plugins to investigate further.

1. In the Tenable Nessus scan configuration, enable plugin debugging.
2. Relaunch the scan against the single target host.
3. After the scan completes, review the output of **Plugin ID 100158 (SSH Combined Host Command Logging)** and **Plugin ID 84239 (Debugging Log Report)**. Use the detailed logs from these plugins to identify the exact command syntax or error message causing the failure.

4. Update your host's access control configuration (for example, `/etc/sudoers` or TACACS rules) with the corrected permissions.
5. Disable plugin debugging in the scan configuration and relaunch the scan to confirm the issue is resolved.

Configure an Audit Trail

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

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

   The **My Scans** page appears.
2. (Optional) In the left navigation bar, click a different folder.
3. On the scans table, click the scan for which you want to configure an audit trail.

   The scan results appear.
4. In the upper right corner, click the **Audit Trail** button.

   The **Audit Trail** window appears.
5. In the **Plugin ID** box, type the plugin ID used by one or more scans.

   and/or

   In the **Host** box, type the hostname for a detected host.
6. Click the **Search** button.

   A list appears and shows the results that match the criteria that you entered in one or both boxes.

Launch a Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

In addition to configuring Schedule settings for a scan, you can manually start a scan.

Note: You cannot create and launch scans, create or view policies or plugin rules, or use the upgrade assistant while Tenable Nessus compiles plugins.

Note: If you are scanning a Linux machine with Tenable Nessus, the Linux machine's shell configuration file must have a `PS1` variable of four or more characters (for example, `PS1='\u@\h:~\$ '`). Having a `PS1` variable of less than four characters (for example, `PS1='\$ '`) can drastically increase the overall scan time.

To launch a scan:

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

   The **My Scans** page appears.

2. In the scans table, in the row of the scan you want to launch, click the ▶ button.

   Tenable Nessus launches the scan.

What to do next:

If you need to stop a scan manually, see Stop a Running Scan.

Pause or Resume a Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

You can pause scans that you want to stop temporarily. When you pause a scan, Tenable Nessus pauses all active scan tasks for that scan. Paused scans do no consume scanner resources.

You can also resume a scan that you previously paused. When you resume a scan, Tenable Nessus starts the scan tasks from the point at which you paused the scan.

Note: You cannot pause or resume web application or attack surface discovery scans.

If you want to stop and terminate a scan, see Stop a Running Scan.

To pause or resume a scan:

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

   The **My Scans** page appears.

2. In the scans table, in the row of the scan you want to pause or resume, do one of the following:

   - To pause the scan, click the ⏸ button.
   - To resume the scan, click the ▷ button.

   Depending on the button you click, Tenable Nessus pauses or resumes the scan.

Stop a Running Scan

> **Required user role when using Tenable Nessus Manager:** Standard, Administrator, or System Administrator

When you stop a scan, Tenable Nessus terminates all tasks for the scan and categorizes the scan as canceled. The Tenable Nessus scan results associated with the scan reflect only the completed tasks. You cannot stop individual tasks, only the scan as a whole.

For local scans (that is, not a scan run by Tenable Agent or a linked scanner in Tenable Nessus Manager), you can force stop the scan to stop the scan quickly and terminate all in-progress plugins. Tenable Nessus may not get results from any plugins that were running when you force stopped the scan.

If you want to temporarily stop a running scan, see Pause or Resume a Scan.

To stop a running scan:

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

   The **My Scans** page appears.

2. In the scans table, in the row of the scan you want to stop, click the ■ button.

   The **Stop Scan** dialog box appears.

3. To stop the scan, click **Stop**.

   Nessus begins terminating the scan processes.

4. (Optional) For local scans, to force stop the scan, click the ■ button.

   Nessus immediately terminates the scan and all its processes.

Delete a Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

Note: Moving and deleting scans are tag-based, user-specific actions. For example, when one user deletes a scan, it will only move to the trash folder for that user. For other users, the scan remains in the original folder and is updated with a trash tag.

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

   The **My Scans** page appears.

2. Optionally, in the left navigation bar, click a different folder.

3. On the scans table, on the row corresponding to the scan that you want to delete, click the ✕ button.

   The scan moves to the **Trash** folder.

   Note: Keep the following in mind when viewing the All Scans folder, which includes scan configurations that have been moved to the trash folder:

   If you move a triggered agent scan configuration to the trash folder, it no longer creates new scan histories and it does not show in the local scanner's scan list.

   Scan configurations that have been moved to the trash folder do not execute scans, regardless of whether they are enabled (Tenable Nessus Manager allows you enable and disable trashed scan configurations from the All Scans folder).

4. To delete the scan permanently, in the left navigation bar, click the **Trash** folder.

   The **Trash** page appears.

5. On the scans table, on the row corresponding to the scan that you want to delete permanently, click the ✕ button.

   A dialog box appears, confirming your selection to delete the scan.

6. Click the **Delete** button.

   Tenable Nessus deletes the scan.

Tip: On the **Trash** page, in the upper right corner, click the **Empty Trash** button to delete all scans in the **Trash** folder permanently.

Scan Folders

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

On the **Scans** page, the left navigation bar is divided into the **Folders** and Resources sections. The **Folders** section always includes the following default folders that you cannot remove:

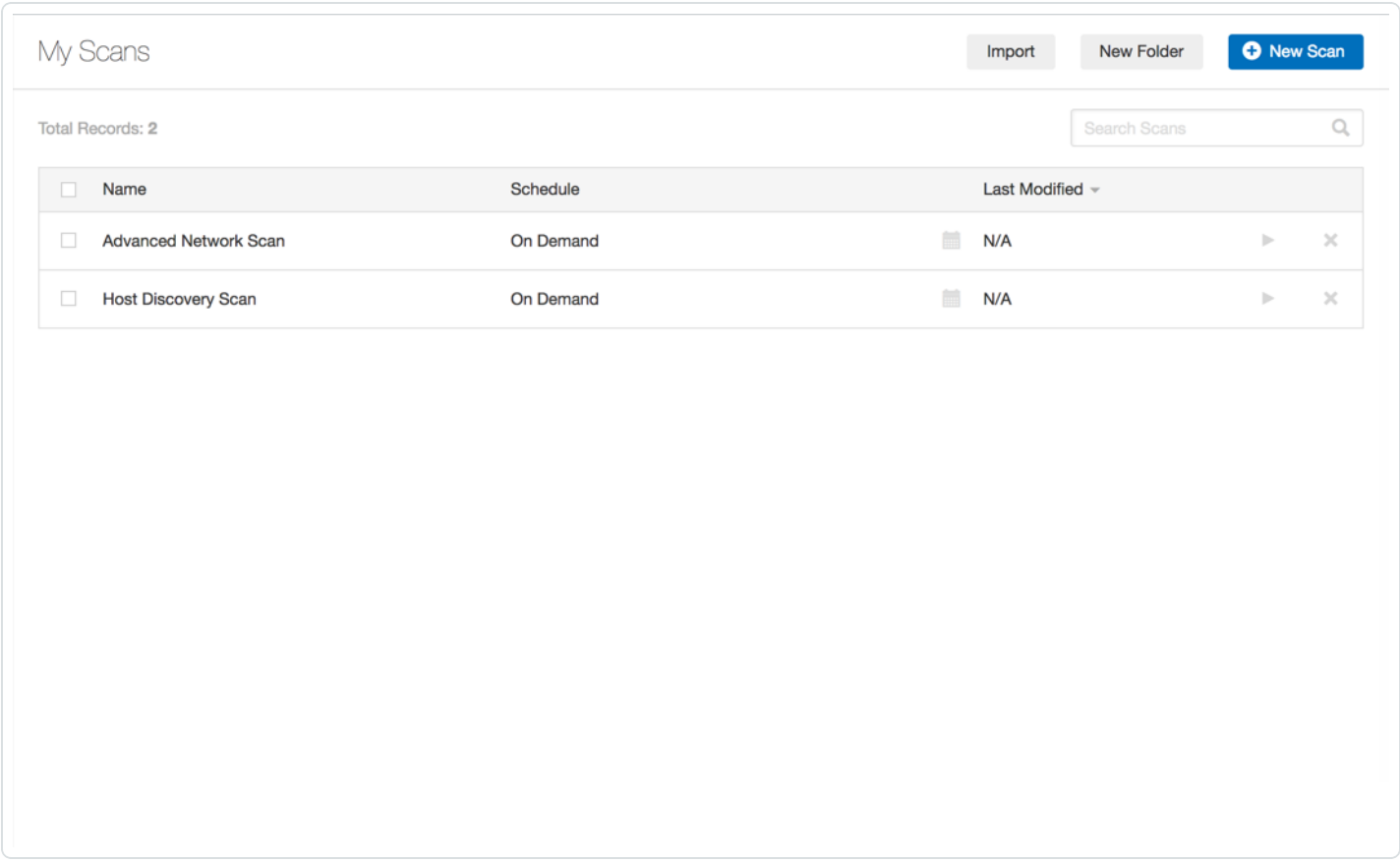
- My Scans
- All Scans
- Trash

Note: All scan folders and related actions (for example, moving and deleting scans) are user-specific and tag-based. For example, when one user deletes a scan, it only moves to the trash folder for that user. For other users, the scan remains in the original folder and Tenable Nessus updates it with a trash tag.

When you access the **Scans** page, the **My Scans** folder appears. When you create a scan, it appears by default in the **My Scans** folder.

The **All Scans** folder shows all scans you have created as well as any scans with which you have permission to interact. You can click on a scan in a folder to view scan results.

The **Trash** folder shows scans that you have deleted. In the **Trash** folder, you can permanently remove scans from your Tenable Nessus instance, or restore the scans to a selected folder. If you delete a folder that contains scans, Tenable Nessus moves all scans in that folder to the **Trash** folder. Tenable Nessus deletes the scans stored in the **Trash** folder automatically after 30 days.



Use the following procedures to manage scan folders:

Create a folder

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

   The **My Scans** page appears.

2. In the upper-right corner, click the **New Folder** button.

   The **New Folder** window appears.

3. In the **Name** box, type a name for the folder.

4. Click the **Create** button.

   Tenable Nessus creates the folder and shows it in the left navigation bar.

Move a scan to a folder

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

   The **My Scans** page appears.

2. If the scan you want to move is not in the **My Scans** folder, on the left navigation bar, click the folder that contains the scan you want to move.

3. On the scans table, select the check box on the row corresponding to the scan that you want to configure.

   In the upper-right corner, the **More** button appears.

4. Click **More**. Point to **Move To**, and click the folder that you want to move the scan to.

   The scan moves to that folder.

Rename a folder

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

   The **My Scans** page appears.

2. In the left navigation bar, next to the folder that you want to rename, click the ▼ button, and then click **Rename**.

   The **Rename Folder** window appears.

3. In the **Name** box, type a new name.

4. Click the **Save** button.

   The folder name changes.

Delete a folder

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

   The **My Scans** page appears.

2. In the left navigation bar, next to the folder that you want to rename, click the ▼ button, and then click **Delete**.

   The **Delete Folder** dialog box appears.

3. Click the **Delete** button.

   Tenable Nessus deletes the folder. If the folder contained scans, Tenable Nessus moves those scans to the **Trash** folder.

Scan Results

You can view scan results to help you understand your organization's security posture and vulnerabilities. Color-coded indicators and customizable viewing options allow you to customize how you view your scan's data.

You can view scan results in one of several views:

Page	Description
Dashboard	In Tenable Nessus Manager, the default scan results page shows the **Dashboard** view.
Scan Summary	View a summary of any completed scan in Tenable Nessus Professional, Nessus Expert, or any non-Tenable Agent scan in Tenable Nessus Manager.
Hosts	The **Hosts** page shows all scanned targets.
Vulnerabilities	List of identified vulnerabilities, sorted by severity. **Tip:** To view vulnerabilities by VPR, click ⚙ in the table header, click **Disable Groups**, and sort the table by **VPR Score**.
Compliance	If the scan includes compliance checks, this list shows counts and details sorted by vulnerability severity. If you configure the scan for compliance scanning, the ⇄ button allows you to navigate between the **Compliance** and **Vulnerability** results.
Remediations	If the scan's results include **Remediation** information, this list shows suggested remediations that address the highest number of vulnerabilities.
Notes	The **Notes** page shows additional information about the scan and the scan's results.

Page	Description
History	The **History** shows a listing of scans: **Start Time**, **End Time**, and the **Scan Statuses**. **Notes:** • Only the scan owner can delete a scan's history. • Scan histories are unavailable for imported scans and configured scans that Tenable Nessus has not executed. • Triggered scan histories do not appear in Tenable Nessus Manager and are designed to be viewed in Tenable Security Center. For Tenable Nessus triggered scan histories, Tenable Security Center shows a scan history for each 12-hour window of the past seven days. Tenable Security Center only retains up to 15 triggered scan histories at a time for each scan.
Summary (cluster configurations only)	View a scan summary of all agents targeted in your scan configuration, organized by cluster node. The summary table shows a row for each cluster node with the following details: • **Node** — The name of the node. • **Not Started** — The number of agents that have not started scanning. • **In Progress** — The number of agents currently scanning. • **Completed** — The number of agents that finished scanning and sent results to Tenable Nessus. • **Aborted** — The number of agents whose scans aborted. An agent appears as **Aborted** when it reports to Tenable Nessus that the scan did not complete. The scan may not launch (for example, if the agent cannot download the policy), or it may start but stop early (for example, if the scan window ends, the agent restarts, or another condition prevents completion). • **Failed** — The number of agents whose scans failed.

Page	Description
	An agent appears as **Failed** when it receives the scan job, but Tenable Nessus does not receive a completion status from the agent. This state typically occurs if the host goes offline or loses connectivity before the agent can return results. • **Total** — The total number of agents included in the scan job
Summary (Attack Surface Discovery scan template only)	View a summary of your attack surface discovery scan configuration. The summary table shows a row for each scanned domain with the following details: • **Domain** — The scanned domain name. • **First Complete Pull** — The date and time the scanned domain data was, or will be, available. • **Data Refreshed** — The date and time that Tenable Attack Surface Management last updated the domain data that Tenable Nessus pulls. Tenable Attack Surface Management refreshes the data that Tenable Nessus pulls every 90 days. • **Next Data Refresh** — The date and time of the next refresh of this domain's data in Tenable Attack Surface Management. Tenable Attack Surface Management refreshes the data that Tenable Nessus pulls every 90 days. • **Ages Out from License** — The data and time the domain ages out from your Tenable Nessus license. • **Record Count** — The number of subdomain records generated.
Records (Attack Surface Discovery scan template only)	View a list of the DNS records identified during the last attack surface discovery scan. The list only shows a maximum of 2,500 records across all scanned domains, but you can filter the table and only view certain record types or records from a specific domain. Tenable Nessus provides the following information for each record: • **Hostname** — The record's hostname.

Page	Description

	• **IP Address** — The IP address related to the record.
	• **Ports** — The discovered open ports on the scanned IP, if applicable.
	• **Type** — The DNS record type. Some of the most common record types are:
	  • A — Host address
	  • AAAA — IPv6 host address
	  • CNAME — Canonical name for an alias
	  • MX — Mail exchange
	  • NS — Name server
	  • PTR — Pointer
	  • SOA — Start of authority
	  • SRV — Location of service
	  • TXT — Text
	• **Target Hostname** — The hostname targeted by the DNS record. This is often the same as the **Hostname**.
	
	The **Records** page also shows details about the latest attack surface discovery scan:
	
	• **Policy** — The scan policy used for the scan (**Domain Discovery**).
	• **Status** — The current scan status.
	• **Severity Base** — The severity base used in the scan (for example, **CVSS v3.0**).
	• **Scanner** — The scanner used for the scan.
	• **Start** — The scan start time and date.
	• **End** — The scan end time and date.

Page	Description
	• **Elapsed** — The time elapsed between the **Start** and **End** times.

Severity

Severity is a categorization of the risk and urgency of a vulnerability.

For more information, see CVSS Scores vs. VPR.

CVSS-based Severity

When you view vulnerabilities in scan results, Tenable Nessus shows severity based on CVSSv2, CVSSv3, or CVSSv4 scores, depending on your configuration.

- You can choose whether Tenable Nessus calculates the severity of vulnerabilities using CVSSv2, CVSSv3, or CVSSv4 scores by configuring your default severity base setting. For more information, see Configure Your Default Severity Base.
- You can also configure individual scans to use a particular severity base, which overrides the default severity base for those scan results. For more information, see Configure the Severity Base for an Individual Scan.

VPR

When you view vulnerabilities in scan results, Tenable Nessus shows severity based on VPR.

EPSS-based Severity

When you view vulnerabilities in scan results, Tenable Nessus shows severity based on the Exploit Prediction Scoring System (EPSS).

CVSS Scores vs. VPR

Tenable uses CVSS scores and a dynamic Tenable-calculated Vulnerability Priority Rating (VPR) to quantify the risk and urgency of a vulnerability.

CVSS

Tenable uses and displays third-party Common Vulnerability Scoring System (CVSS) values retrieved from the National Vulnerability Database (NVD) to describe risk associated with vulnerabilities. CVSS scores power a vulnerability's **Severity** and **Risk Factor** values.

> **Note:** If a vulnerability's related plugin has CVSS vectors, the **Risk Factor** is calculated based on the CVSSv2 vector and equates to the CVSSv2 score **Severity**. If a plugin does not have CVSS vectors, Tenable independently calculates the **Risk Factor**.

CVSS-Based Severity

Tenable assigns all vulnerabilities a severity (**Info**, **Low**, **Medium**, **High**, or **Critical**) based on the vulnerability's static CVSS score (the CVSS version depends on your configuration). For more information, see Configure Default Severity.

Tenable Nessus analysis pages provide summary information about vulnerabilities using the following CVSS categories.

Severity	CVSSv2 Range	CVSSv3 Range	CVSSv4 Range
Critical	The plugin's highest vulnerability CVSSv2 score is 10.0.	The plugin's highest vulnerability CVSSv3 score is between 9.0 and 10.0.	The plugin's highest vulnerability CVSSv4 score is between 9.0 and 10.0.
High	The plugin's highest vulnerability CVSSv2 score is between 7.0 and 9.9.	The plugin's highest vulnerability CVSSv3 score is between 7.0 and 8.9.	The plugin's highest vulnerability CVSSv4 score is between 7.0 and 8.9.
Medium	The plugin's highest vulnerability CVSSv2 score is between 4.0 and 6.9.	The plugin's highest vulnerability CVSSv3 score is between 4.0 and 6.9.	The plugin's highest vulnerability CVSSv4 score is between 4.0 and 6.9.
Low	The plugin's highest vulnerability CVSSv2 score is between 0.1 and 3.9.	The plugin's highest vulnerability CVSSv3 score is between 0.1 and 3.9.	The plugin's highest vulnerability CVSSv4 score is between 0.1 and 3.9.

Info	The plugin's highest vulnerability CVSSv2 score is 0. - or - The plugin does not search for vulnerabilities.	The plugin's highest vulnerability CVSSv3 score is 0. - or - The plugin does not search for vulnerabilities.	The plugin's highest vulnerability CVSSv3 score is 0. - or - The plugin does not search for vulnerabilities.

CVSS-Based Risk Factor

For each plugin, Tenable interprets CVSS scores for the vulnerabilities associated with the plugin and assigns an overall risk factor (**Low**, **Medium**, **High**, or **Critical**) to the plugin. The **Vulnerability Details** page shows the highest risk factor value for all the plugins associated with a vulnerability.

Note: Detection (non-vulnerability) plugins and some automated vulnerability plugins do not receive CVSS scores. In these cases, Tenable determines the risk factor based on vendor advisories.

Tip: **Info** plugins receive a risk factor of **None**. Other plugins without associated CVSS scores receive a custom risk factor based on information provided in related security advisories.

Vulnerability Priority Rating

Tenable calculates a dynamic VPR for most vulnerabilities. The VPR is a dynamic companion to the data provided by the vulnerability's CVSS score, since Tenable updates the VPR to reflect the current threat landscape. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit.

VPR Category	VPR Range
Critical	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1 to 3.9

Note: Vulnerabilities without CVEs (for example, many vulnerabilities with the **Info** severity) do not receive a VPR. Tenable recommends remediating these vulnerabilities according to their CVSS-based severity.

Note: You cannot edit VPR values.

Note: VPR scores shown in Nessus are static and do not update dynamically. You have to rescan to view the latest and most accurate VPR scores.

Tenable Nessus provides a VPR value the first time you scan a vulnerability on your network.

Tenable recommends resolving vulnerabilities with the highest VPRs first. You can view VPR scores and summary data in:

- The **VPR Top Threats** for an individual scan, as described in View VPR Top Threats.
- The **Top 10 Vulnerabilities** report for an individual scan. For information on creating the report, see Create a Scan Report.

VPR Key Drivers

Some key drivers that you can view to explain a vulnerability's VPR include, but are not limited to:

Note: Tenable does not customize these values for your organization; VPR key drivers reflect a vulnerability's global threat landscape.

Key Driver	Description
Age of Vuln	The number of days since the National Vulnerability Database (NVD) published the vulnerability.
CVSSv3 Impact Score	The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable Nessus displays a Tenable-predicted score.
Exploit Code Maturity	The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (e.g., Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (**High**, **Functional**, **PoC**, or **Unproven**) parallel the CVSS Exploit Code Maturity categories.

Product Coverage	The relative number of unique products affected by the vulnerability: **Low**, **Medium**, **High**, or **Very High**.
Threat Sources	A list of all sources (e.g., social media channels, the dark web, etc.) where threat events related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system displays **No recorded events**.
Threat Intensity	The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability: **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Threat Recency	The number of days (0-180) since a threat event occurred for the vulnerability.

Threat Event Examples

Common threat events include:

- An exploit of the vulnerability
- A posting of the vulnerability exploit code in a public repository
- A discussion of the vulnerability in mainstream media
- Security research about the vulnerability
- A discussion of the vulnerability on social media channels
- A discussion of the vulnerability on the dark web and underground
- A discussion of the vulnerability on hacker forums

Configure Your Default Severity Base

Note: This setting does not apply to Tenable Nessus Manager. Vulnerability scoring for Tenable Nessus Manager data is managed within Tenable Security Center via the **Vulnerability Scoring System** setting.

Note: By default, new installations of Tenable Nessus use CVSSv3 scores (when available) to calculate severity for vulnerabilities. Preexisting, upgraded installations retain the previous default of CVSSv2 scores.

In Tenable Nessus scanners and Tenable Nessus Professional, you can choose whether Tenable Nessus calculates the severity of vulnerabilities using CVSSv2 or CVSSv3 scores (when available) by configuring your default severity base setting. In Tenable Nessus scanners and Tenable Nessus Professional, you can choose whether Tenable Nessus calculates the severity of vulnerabilities using CVSSv2, CVSSv3, or CVSSv4 scores (when available) by configuring your default severity base setting. When you change the default severity base, the change applies to all existing scans that are configured with the default severity base. Future scans also use the default severity base.

You can also configure individual scans to use a particular severity base, which overrides the default severity base for that scan, as described in Configure the Severity Base for an Individual Scan.

For more information about CVSS scores and severity ranges, see CVSS Scores vs. VPR.

To configure your default severity base:

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

   The **About** page appears.

2. In the left navigation bar, click **Advanced**.

   The **Advanced Settings** page appears.

3. Click the **Scanning** tab.

   The scanning advanced settings appear.

4. In the table, click the row for the **System Default Severity Basis** setting.

   > **Tip:** Use the search bar to search for any part of the setting name.

   The setting configuration window appears.

5. In the Value drop-down box, select **CVSS v2.0**, **CVSS v3.0**, or **CVSS v4.0** for your default severity base.

6. Click **Save**.

   Tenable Nessus updates the default severity base for your instance. Existing scans with the default severity base update to reflect the new default. Individual scans with overridden severity bases do not change.

Configure the Severity Base for an Individual Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

You can configure individual scans to use a particular severity base, which overrides the default severity base for that scan. If you change the default severity base, scans with overridden severity bases do not change.

To change the default severity base across the Tenable Nessus instance, see Configure Your Default Severity Base.

For more information about CVSS scores and severity ranges, see CVSS Scores vs. VPR.

Note: By default, new installations of Tenable Nessus use CVSSv3 scores (when available) to calculate severity for vulnerabilities. Preexisting, upgraded installations retain the previous default of CVSSv2 scores.

To configure the severity base for an individual scan:

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

   The **My Scans** page appears.

2. In the scan table, click the scan for which you want to change the severity base.

   The scan page appears. The **Scan Details**, including the scan's current severity base, appear on the right side of the page.

3. Under **Scan Details**, next to the current **Severity Base**, click the button.

   The **Change Severity Rating Base** window appears.

4. From the **Severity Rating Base** drop-down box, select one of the following:

   - **CVSS v2.0** — The severity for vulnerabilities found by the scan is based on CVSSv2 scores. This setting overrides the default severity base set on the Tenable Nessus instance.
   - **CVSS v3.0** — The severity for vulnerabilities found by the scan is based on CVSSv3 scores. This setting overrides the default severity base set on the Tenable Nessus

instance.

- **CVSS v4.0** — The severity for vulnerabilities found by the scan is based on CVSSv4 scores. This setting overrides the default severity base set on the Tenable Nessus instance.
- **Default** — The severity for vulnerabilities found by the scan use the Tenable Nessus default severity base, which appears in parentheses. If you change the default severity base later, the scan automatically uses the new default severity base.

5. Click **Save**.

   Tenable Nessus updates the severity base for your scan. The scan results update to reflect the updated severity.

Create a New Scan from Scan Results

> **Required user role when using Tenable Nessus Manager:** Standard, Administrator, or System Administrator

When you view scan results, you can select scanned hosts that you want to target in a new scan. When you create a new scan, Tenable Nessus automatically populates the targets with the hosts that you selected.

To create a new scan from scan results:

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

   The **My Scans** page appears.

2. In the scans table, click the row of a completed scan.

   The scan's results page appears.

3. Click the **Hosts** tab.

   Tenable Nessus displays a table of scanned hosts.

4. Select the check box next to each host you want to scan in your new scan.

   At the top of the page, the **More** button appears.

5. Click the **More** button.

   A drop-down box appears.

6. Click **Create Scan**.

   The **Scan Templates** page appears.

7. Select a scan template for your new scan.

   Tenable Nessus automatically populates the **Targets** list with the hosts you previously selected.

8. Configure the rest of the scan settings, as described in Scan and Policy Settings.

9. Do one of the following:

   - To launch the scan immediately, click the button, and then click **Launch**.

     Tenable Nessus saves and launches the scan.

   - To launch the scan later, click the **Save** button.

     Tenable Nessus saves the scan.

Search and Filter Results

Required user role when using Tenable Nessus Manager: Basic, Standard, Administrator, or System Administrator

You can search or use filters to view specific scan results. You can filter hosts and vulnerabilities, and you can create detailed and customized scan result views by using multiple filters.

Search for hosts

1. In scan results, click the **Hosts** tab.

   If you are working with an attack surface discovery scan, click the **Records** tab.

2. In the **Search Hosts** box above the hosts table, type text to filter for matches in hostnames.

   As you type, Nessus automatically filters the results based on your text.

Search for vulnerabilities

1. Do one of the following:
    - In scan results, in the **Hosts** tab, click a specific host to view its vulnerabilities.
    - In scan results, click the **Vulnerabilities** tab to view all vulnerabilities.
2. In the **Search Vulnerabilities** box above the vulnerabilities table, type text to filter for matches in vulnerability titles.

    As you type, Nessus automatically filters the results based on your text.

Create a filter

1. Do one of the following:
    - In scan results, click the **Hosts** tab.
    - In scan results, in the **Hosts** tab, click a specific host to view its vulnerabilities.
    - In scan results, click the **Vulnerabilities** tab to view all vulnerabilities.
    - In attack surface discovery scan results, click the **Records** tab to view all DNS records.
2. Click **Filters** next to the search box.
    - If you have saved filters, a list of your saved filters appears. Click **Custom** to open the **Filters** window and create a new filter, or click a saved filter to apply it to the table.
    - If you do not have saved filters, the **Filters** window appears.
3. Specify your filter rule options:
    - **Match Any or Match All:** If you select **All**, only results that match all filters appear. If you select **Any**, results that match any one of the filters appear.
    - **Plugin attribute:** See the Plugin Attributes table for plugin attribute descriptions.
    - **Filter argument:** Select **is equal to**, **is not equal to**, **contains**, or **does not contain** to specify how the filter should match for the selected plugin attribute.
    - **Value:** Depending on the plugin attribute you selected, enter a value or select a value from the drop-down menu.
4. (Optional) Click ⊕ to add another filter rule.

5. (Optional) Save the filter for future use by performing the following steps:

    a. Select the **Save this filter** checkbox to save the filter or filters.

    The **Filter name** box appears.

    b. Enter a name for the filter.

    c. Click **Save**.

    The saved filter is now available to select when you click the table **Filter** button.

    > **Note:** You can only save filters for the **Hosts**, **Vulnerabilities**, and **Records** tables.

6. Click **Apply**.

    Tenable Nessus applies your filters and the table shows vulnerabilities or records that match your filters.

Manage saved filters

1. Do one of the following:

    - In scan results, click the **Hosts** tab.
    - In scan results, in the **Hosts** tab, click a specific host to view its vulnerabilities.
    - In scan results, click the **Vulnerabilities** tab to view all vulnerabilities.

2. Click **Filter** next to the search box.

    A list of your saved filters appears.

3. Do one of the following:

    - Click the filter name to apply the filter to the table.
    - Click the button to edit the filter criteria.

      The **Filters** window appears. Edit the criteria, and click **Save**.
    - Click the button to create a duplicate saved filter.

      You can now select and edit a copy of the saved filter from the table **Filter** button.

- Click the ✕ button to delete the saved filter.

  The **Delete Filter** window appears. Click **Continue** to confirm the deletion.

Clear an applied filter

1. Click **Filter** next to the search box.

   The **Filter** window appears.

2. To remove a single filter, click ✕ next to the filter entry.

3. To remove all filters, click **Clear Filters**.

   Tenable Nessus removes the filters from the vulnerabilities shown in the table.

Plugin Attributes

The following table lists plugins attributes you can use to filter results.

Tip: Many Tenable Nessus plugin attributes relate to severity and vulnerability scores. To learn more about severity and vulnerability scores, see Severity and CVSS Scores vs. VPR.

Option	Description
Bugtraq ID	Filter results based on if a Bugtraq ID is equal to, is not equal to, contains, or does not contain a given string (for example, 51300).
CANVAS Exploit Framework	Filter results based on if the presence of an exploit in the CANVAS exploit framework is equal to or is not equal to true or false.
CANVAS Package	Filter results based on which CANVAS exploit framework package an exploit exists for. Options include CANVAS, D2ExploitPack, or White_ Phosphorus.
CERT Advisory ID	Filter results based on if a CERT Advisory ID (now called Technical Cyber Security Alert) is equal to, is not equal to, contains, or does not contain a given string (for example, TA12-010A).
CORE Exploit Framework	Filter results based on if the presence of an exploit in the CORE exploit framework is equal to or is not equal to true or false.

Option	Description
CPE	Filter results based on if the Common Platform Enumeration (CPE) is equal to, is not equal to, contains, or does not contain a given string (for example, Solaris).
CVE	Filter results based on if a Common Vulnerabilities and Exposures (CVE) v2.0 reference is equal to, is not equal to, contains, or does not contain a given string (for example, 2011-0123).
CVSS Base Score	Filter results based on if a Common Vulnerability Scoring System (CVSS) v2.0 base score is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (for example, 5). You can use this filter to select by risk level. The severity ratings are derived from the associated CVSS score, where 0 is Info, less than 4 is Low, less than 7 is Medium, less than 10 is High, and a CVSS score of 10 is Critical.
CVSS Temporal Score	Filter results based on if a CVSS v2.0 temporal score is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (for example, 3.3).
CVSS Temporal Vector	Filter results based on if a CVSS v2.0 temporal vector is equal to, is not equal to, contains, or does not contain a given string (for example, E:F).
CVSS Vector	Filter results based on if a CVSS v2.0 vector is equal to, is not equal to, contains, or does not contain a given string (for example, AV:N).
CVSS 3.0 Base Score	Filter results based on if a Common Vulnerability Scoring System (CVSS) v3.0 base score is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (for example, 5). You can use this filter to select by risk level. The severity ratings are derived from the associated CVSS score, where 0 is Info, less than 4 is Low, less than 7 is Medium, less than 10 is High, and a CVSS score of 10 is Critical.
CVSS 3.0	Filter results based on if a CVSS v3.0 temporal score is less than, is more

Option	Description
Temporal Score	than, is equal to, is not equal to, contains, or does not contain a string (for example, 3.3).
CVSS 3.0 Temporal Vector	Filter results based on if a CVSS v3.0 temporal vector is equal to, is not equal to, contains, or does not contain a given string (for example, E:F).
CVSS 3.0 Vector	Filter results based on if a CVSS v3.0 vector is equal to, is not equal to, contains, or does not contain a given string (for example, AV:N).
CVSS 4.0 Base Score	Filter results based on if a Common Vulnerability Scoring System (CVSS) v4.0 base score is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (for example, 5). You can use this filter to select by risk level. The severity ratings are derived from the associated CVSS score, where 0 is Info, less than 4 is Low, less than 7 is Medium, less than 10 is High, and a CVSS score of 10 is Critical.
CVSS 4.0 Temporal Score	Filter results based on if a CVSS v4.0 temporal score is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (for example, 3.3).
CVSS 4.0 Temporal Vector	Filter results based on if a CVSS v4.0 temporal vector is equal to, is not equal to, contains, or does not contain a given string (for example, E:F).
CVSS 4.0 Vector	Filter results based on if a CVSS v4.0 vector is equal to, is not equal to, contains, or does not contain a given string (for example, AV:N).
CWE	Filter results based on Common Weakness Enumeration (CWE) if a CVSS vector is equal to, is not equal to, contains, or does not contain a CWE reference number (for example, 200).
EPSS Score	Filter results based on if a vulnerability EPSS score is equal to, is not equal to, contains, does not contain, is less than, or is more than a value.
Exploit Available	Filter results based on the vulnerability having a known public exploit.
Exploit	Filter results based on if an Exploit Database ID (EBD-ID) reference is equal

Option	Description
Database ID	to, is not equal to, contains, or does not contain a given string (for example, 18380).
Exploitability Ease	Filter results based on if the exploitability ease is equal to or is not equal to the following values: Exploits are available, No exploit is required, or No known exploits are available.
Exploited by Malware	Filter results based on if the presence of a vulnerability is exploitable by malware is equal to or is not equal to true or false.
Exploited by Nessus	Filter results based on whether a plugin performs an actual exploit, usually an ACT_ATTACK plugin.
Hostname	Filter results if the host is equal to, is not equal to, contains, or does not contain a given string (for example, 192.168 or lab). For agents, you can search by the agent target name. For other targets, you can search by the target's IP address or DNS name, depending on how you configured the scan.
IAVA	Filter results based on if an IAVA reference is equal to, is not equal to, contains, or does not contain a given string (for example, 2012-A-0008).
IAVB	Filter results based on if an IAVB reference is equal to, is not equal to, contains, or does not contain a given string (for example, 2012-A-0008).
IAVM Severity	Filter results based on the IAVM severity level (for example, IV).
In The News	Filter results based on whether the vulnerability covered by a plugin has had coverage in the news.
Malware	Filter results based on whether the plugin detects malware; usually ACT_GATHER_INFO plugins.
Metasploit Exploit Framework	Filter results based on if the presence of a vulnerability in the Metasploit Exploit Framework is equal to or is not equal to true or false.
Metasploit	Filter results based on if a Metasploit name is equal to, is not equal to,

Option	Description
Name	contains, or does not contain a given string (for example, xslt_password_reset).
Microsoft Bulletin	Filter results based on Microsoft security bulletins like MS17-09, which have the format MSXX-XXX, where X is a number.
Microsoft KB	Filter results based on Microsoft knowledge base articles and security advisories.
OSVDB ID	Filter results based on if an Open Source Vulnerability Database (OSVDB) ID is equal to, is not equal to, contains, or does not contain a given string (for example, 78300).
Patch Publication Date	Filter results based on if a vulnerability patch publication date is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (for example, 12/01/2011).
Plugin Description	Filter results if the Plugin Description contains, or does not contain a given string (for example, remote).
Plugin Family	Filter results if the Plugin Name is equal to or is not equal to one of the designated Nessus plugin families. Tenable Nessus provides the possible matches via a drop-down menu.
Plugin ID	Filter results if the plugin ID is equal to, is not equal to, contains, or does not contain a given string (for example, 42111).
Plugin Modification Date	Filter results based on if a Nessus plugin modification date is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (for example, 02/14/2010).
Plugin Name	Filter results if Plugin Name is equal to, is not equal to, contains, or does not contain a given string (for example, windows).
Plugin Output	Filter results if Plugin Description is equal to, is not equal to, contains, or does not contain a given string (for example, PHP)
Plugin	Filter results based on if a Nessus plugin publication date is less than, is

Option	Description
Publication Date	more than, is equal to, is not equal to, contains, or does not contain a string (for example, 06/03/2011).
Plugin Type	Filter results if Plugin Type is equal to or is not equal to one of the two types of plugins: local or remote.
Port	Filter results based on if a port is equal to, is not equal to, contains, or does not contain a given string (for example, 80).
Protocol	Filter results if a protocol is equal to or is not equal to a given string (for example, HTTP).
Risk Factor	Filter results based on the risk factor of the vulnerability (for example, Low, Medium, High, Critical).
Secunia ID	Filter results based on if a Secunia ID is equal to, is not equal to, contains, or does not contain a given string (for example, 47650).
See Also	Filter results based on if a Nessus plugin see also reference is equal to, is not equal to, contains, or does not contain a given string (for example, seclists.org).
Solution	Filter results if the plugin solution contains or does not contain a given string (for example, upgrade).
Synopsis	Filter results if the plugin solution contains or does not contain a given string (for example, PHP).
VPR Score	Filter results based on if a vulnerability VPR score is equal to, is not equal to, contains, does not contain, is less than, or is more than a value (for example, VPR Score is more than 8.0).
Vulnerability Publication Date	Filter results based on if a vulnerability publication date earlier than, later than, on, not on, contains, or does not contain a string (for example, 01/01/2012). **Note:** Pressing the button next to the date brings up a calendar interface for easier date selection.

Compare Scan Results

Required user role when using Tenable Nessus Manager: Basic, Standard, Administrator, or System Administrator

You can compare two scan results to see differences between them. This comparison is not a true differential of the two results; it shows the new vulnerabilities that Tenable Nessus detected between the older baseline scan and the newer scan.

Comparing scan results helps you see how a given system or network has changed over time. This information is useful for compliance analysis by showing how vulnerabilities are being remediated, if systems are patched as Tenable Nessus finds new vulnerabilities, or how two scans may not be targeting the same hosts.

Note: You cannot compare imported scans or more than two scans.

To compare two scan results:

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

   The **My Scans** page appears.

2. Click a scan.

3. Click the **History** tab.

4. In the row of both scan results you want to compare, select the check box.

5. In the upper-right corner, click **Diff**.

   The **Choose Primary Result** window appears.

6. In the drop-down box, select which of the scan results is the primary result.

   The primary result is your differential baseline. The scan differential shows the vulnerabilities that Tenable Nessus detected in the non-baseline scan.

   Tip: To see a true differential of the two scan results, Tenable recommends generating the differential twice: once using the older scan result as the baseline, and once using the newer scan result as the baseline. Doing so allows you to see the vulnerabilities that were only detected in one of the scan results.

7. Click **Continue**.

   The scan differential appears. The differential shows the hosts on which the non-baseline scan detected vulnerabilities since the baseline scan under the **Hosts** tab and a list of the vulnerabilities detected under the **Vulnerabilities** tab.

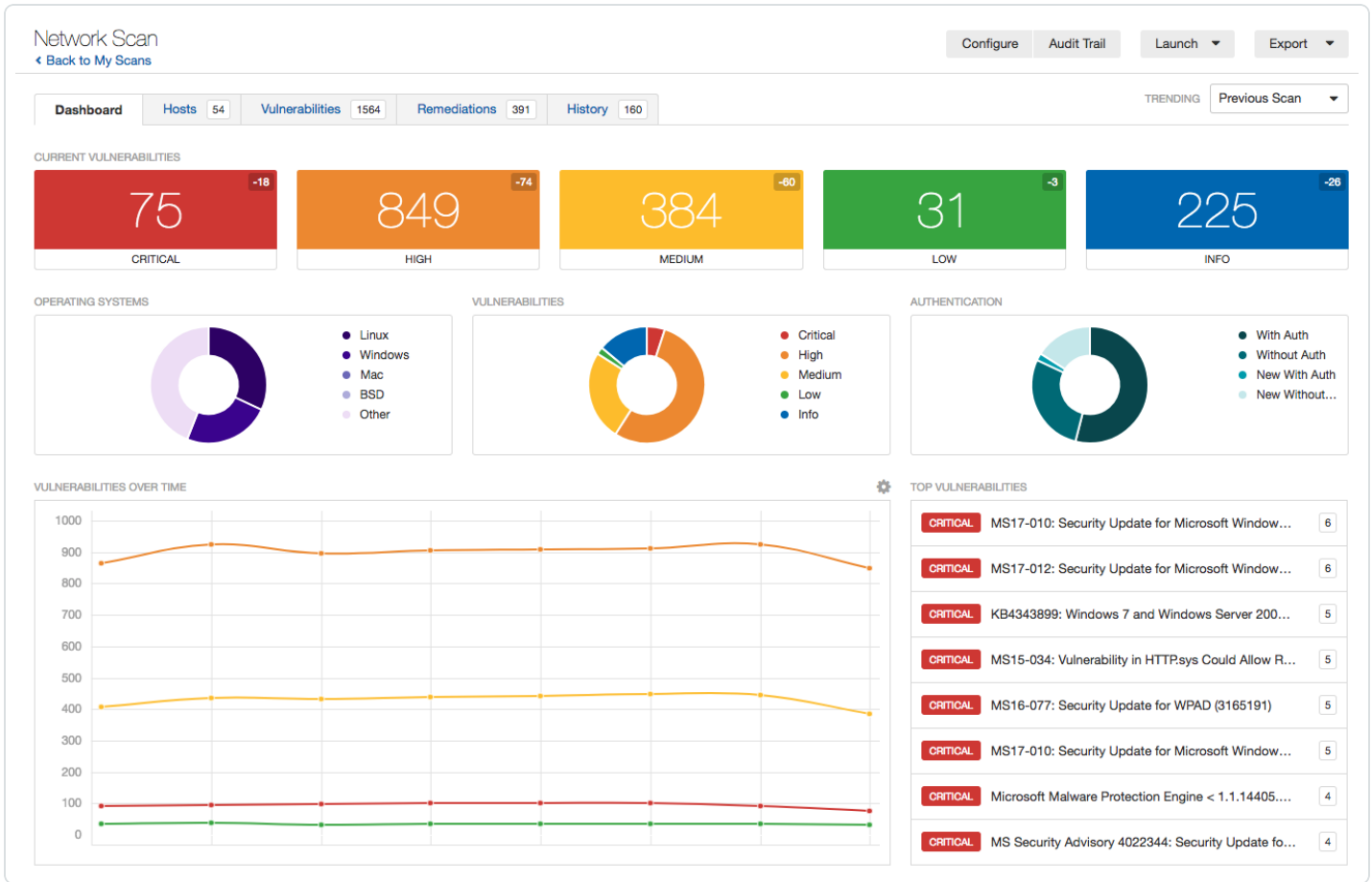
   You can generate a report of the scan differential. For more information, see step four of Create a Scan Report.

Dashboard

In Tenable Nessus Manager, you can configure a scan to show the scan's results in an interactive dashboard view.

> **Note:** This feature is only available for non-clustered Manager configurations.

Based on the type of scan performed and the type of data collected, the dashboard shows key values and trending indicators.



Dashboard View

Based on the type of scan performed and the type of data collected, the dashboard shows key values and a trending indicator.

Dashboard Details

Name	Description
Current Vulnerabilities	The number of vulnerabilities identified by the scan, by severity.
Operating System Comparison	The percentage of operating systems identified by the scan.
Vulnerability Comparison	The percentage of all vulnerabilities identified by the scan, by severity.
Host Count Comparison	The percentage of hosts scanned by credentialed and non-credentialed authorization types: without authorization, new without authorization, with authorization, and new with authorization.
Vulnerabilities Over Time	Vulnerabilities found over a period of time. You must complete at least two scans for this chart to appear.
Top Hosts	Top 8 hosts that had the highest number of vulnerabilities found in the scan.
Top Vulnerabilities	Top 8 vulnerabilities based on severity.

View Scan Summary

> **Required user role when using Tenable Nessus Manager:** Basic, Standard, Administrator, or System Administrator

You can view a summary of any non-agent scan in Tenable Nessus Manager, or any scan in Tenable Nessus Professional or Tenable Nessus Expert. The scan summary provides the following information:

Summary Section	Description
Scan Details	The number of critical, high, medium, and low-severity vulnerabilities detected during the scan.
Details	The scan name, the plugin set the scan used, the scan's CVSS score (for more information, see CVSS Scores vs. VPR), the scan's template, and the times at which the scan started and ended.
Authentication/Credential Info (Hosts)	The number of hosts that succeeded and failed to authenticate during the scan.
Scan Durations	The scan duration, median scan time per host, and maximum scan time.
Plugin Families Enabled/Disabled	A list of the plugin families that Tenable Nessus enabled or disabled for the scan. **Note:** This section does not appear for basic network scans.
Plugin Rules Applied	A list of the plugin rules that were applied for the scan. If Tenable Nessus did not apply plugin rules, this section does not appear.
Policy Details	The scan's basic, assessment, report, advanced, credential, port scanner, and fragile devices settings configurations. • For more information about basic, assessment, report, and advanced scan settings, see Scan and Policy Settings. • For more information about port scanner and fragile device settings, see Discovery Scan Settings.

Note: The **Scan Summary** tab does not appear while the scan is in progress.

To view a scan's summary:

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

   The **My Scans** page appears.

2. Click the scan for which you want to view a summary.

   The scan's results page appears.

3. Click the **Scan Summary** tab.

   The **Scan Summary** page appears.

Vulnerabilities

Vulnerabilities are instances of a potential security issue found by a plugin. In your scan results, you can choose to view all vulnerabilities found by the scan, or vulnerabilities found on a specific host.

Vulnerability view	Path
All vulnerabilities detected by a scan	**Scans** > *[scan name]* > **Vulnerabilities**
Vulnerabilities detected by a scan on a specific host	**Scans** > **Hosts** > *[scan name]*

Use the following procedures to manage vulnerabilties:

View vulnerabilities

Required user role when using Tenable Nessus Manager: Basic, Standard, Administrator, or System Administrator

You can view all vulnerabilities found by a scan, or vulnerabilities found on a specific host by a scan. When you drill down on a vulnerability, you can view information such as plugin details, description, solution, output, risk information, vulnerability information, and reference information.

Tip: To view vulnerabilities by VPR, click ⚙ in the table header, click **Disable Groups**, and sort the table by **VPR Score**.

To view vulnerabilities:

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

   The **My Scans** page appears.

2. Click the scan for which you want to view vulnerabilities.

   The scan's results page appears.

3. Do one of the following:

   - To view vulnerabilities on a specific host, click the host.
   - To view all vulnerabilities, click the **Vulnerabilities** tab.

     The **Vulnerabilities** tab appears.

4. (Optional) To sort the vulnerabilities, click an attribute in the table header row to sort by that attribute.

5. To view details for the vulnerability, click the vulnerability row.

   The vulnerability details page appears and shows plugin information and output for each instance on a host.

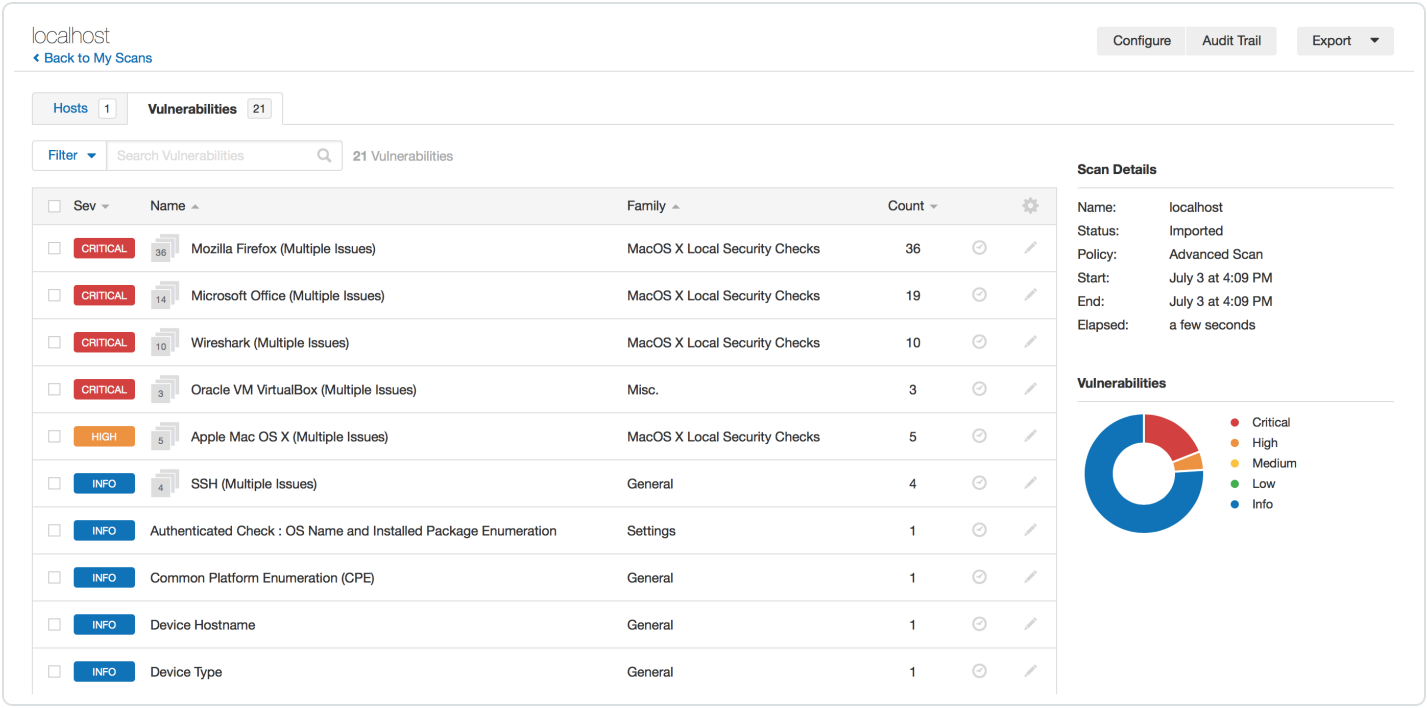
Group vulnerabilities

Required user role when using Tenable Nessus Manager: Basic, Standard, Administrator, or System Administrator

When you group vulnerabilities, plugins with common attributes such as Common Platform Enumeration (CPE), service, application, and protocol nest under a single row in scan results. Grouping vulnerabilities gives you a shorter list of results, and shows your related vulnerabilities together.

When you enable groups, the number of vulnerabilities in the group appears next to the severity indicator, and the group name says **(Multiple Issues)**.

The severity indicator for a group is based on the vulnerabilities in the group. If all the vulnerabilities in a group have the same severity, Tenable Nessus shows that severity level. If the vulnerabilities in a group have differing severities, Tenable Nessus shows the **Mixed** severity level.



To group vulnerabilities

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

   The **My Scans** page appears.

2. Click on the scan for which you want to view vulnerabilities.

   The scan's results page appears.

3. Do one of the following:

   - Click a specific host to view vulnerabilities found on that host.

     -or-

   - Click the **Vulnerabilities** tab to view all vulnerabilities.

   The **Vulnerabilities** tab appears.

4. In the header row of the vulnerabilities table, click ⚙.

   Note: The cog icon (⚙) only appears when there are vulnerabilities that can be grouped.

5. Click **Enable Groups**.

Tenable Nessus groups similar vulnerabilities in one row.

To ungroup vulnerabilities

1. In the header row of the vulnerabilities table, click ⚙.

   Note: The cog icon (⚙) only appears when there are vulnerabilities that can be grouped.

2. Click **Disable Groups**.

   Vulnerabilities appear on their own row.

To view vulnerabilities within a group

- In the vulnerabilities table, click the vulnerability group row.

  A new vulnerabilities table appears and shows the vulnerabilities in the group.

To set group severity types to the highest severity within the group

- Set the advanced setting `scans_vulnerability_groups_mixed` to `no`.

Modify a vulnerability

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

You can modify a vulnerability to change its severity level or hide it. This allows you to re-prioritize the severity of results to better account for your organization's security posture and response plan. When you modify a vulnerability from the scan results page, the change only applies to that vulnerability instance for that scan unless you indicate that the change should apply to all future scans. To modify severity levels for all vulnerabilities, use Plugin Rules.

To modify a vulnerability:

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

   The **My Scans** page appears.

2. Click the scan for which you want to view vulnerabilities.

   The scan's results page appears.

3. Do one of the following:

    - Click a specific host to view vulnerabilities found on that host.
    - Click the **Vulnerabilities** tab to view all vulnerabilities.

      The **Vulnerabilities** tab appears.

4. In the row of the vulnerability you want to modify, click .

   The **Modify Vulnerability** window appears.

5. In the **Severity** drop-down box, select a severity level or **Hide this result**.

   > **Note:** If you hide a vulnerability, you cannot recover it and you accept its associated risks. To hide a vulnerability temporarily, use Snooze a vulnerability.

6. (Optional) Select **Apply this rule to all future scans**.

   If you select this option, Tenable Nessus modifies this vulnerability for all future scans. Tenable Nessus does not modify vulnerabilities found in past scans.

7. Click **Save**.

   Tenable Nessus updates the vulnerability with your setting.

Snooze a vulnerability

> **Required user role when using Tenable Nessus Manager:** Basic, Standard, Administrator, or System Administrator

When you snooze a vulnerability, it does not appear in the default view of your scan results. You choose a period of time for which the vulnerability is snoozed – once the snooze period age outs, the vulnerability awakes and appears in your list of scan results. You can also manually wake a vulnerability or choose to show snoozed vulnerabilities. Snoozing affects all instances of the vulnerability in a given scan, so you cannot snooze vulnerabilities only on a specific host.

When you snooze a vulnerability, you only snooze the vulnerability for the scan result that you are working in. The vulnerability still appears in other existing scan results, and in future scan results.

To snooze a vulnerability:

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

   The **My Scans** page appears.

2. Click on the scan for which you want to view vulnerabilities.

   The scan's results page appears.

3. Do one of the following:

   - Click a specific host to view vulnerabilities found on that host.

     -or-

   - Click the **Vulnerabilities** tab to view all vulnerabilities.

     The **Vulnerabilities** tab appears.

4. In the row of the vulnerability you want to snooze, click .

   The **Snooze for** drop-down box appears.

5. Choose the period of time you want the vulnerability to snooze:

   - Click **1 Day**, **1 Week**, or **1 Month**.

     -or-

   - Click **Custom**.

   The **Snooze Vulnerability** window appears.

6. In the **Snooze Vulnerability** window:

   - If you selected a preset snooze period, click **Snooze** to confirm your selection.
   - If you selected a custom snooze period, select the date you want the vulnerability to snooze until, then click **Snooze**.

   Tenable Nessus snoozes the vulnerability for the selected period of time and does not appear in the default view of scan results.

To show snoozed vulnerabilities

1. In the header row of the vulnerabilities table, click ⚙.

   A drop-down box appears.

2. Click **Show Snoozed**.

   Snoozed vulnerabilities appear in the list of scan results.

To wake a snoozed vulnerability

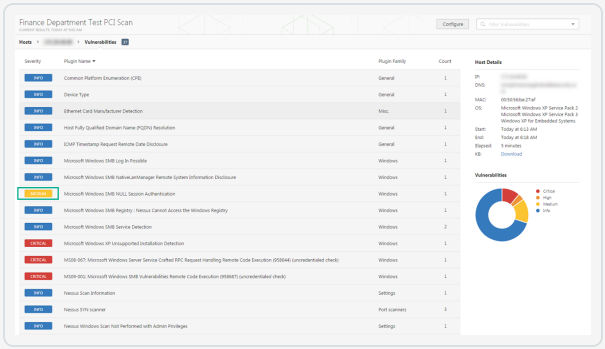
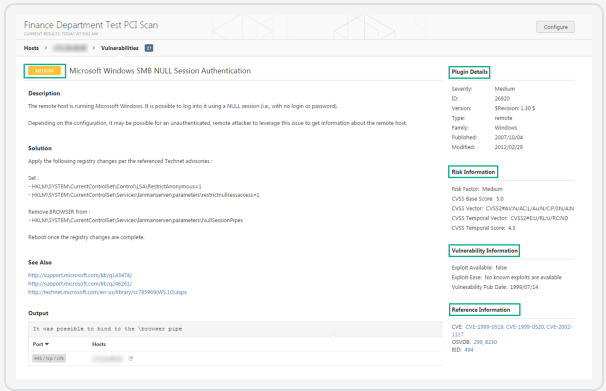
1. In the row of the snoozed vulnerability click ⏰.

   The **Wake Vulnerability** window appears.

2. Click **Wake**.

   The vulnerability is no longer snoozed, and appears in the default list of scan results.

Example Vulnerability Information

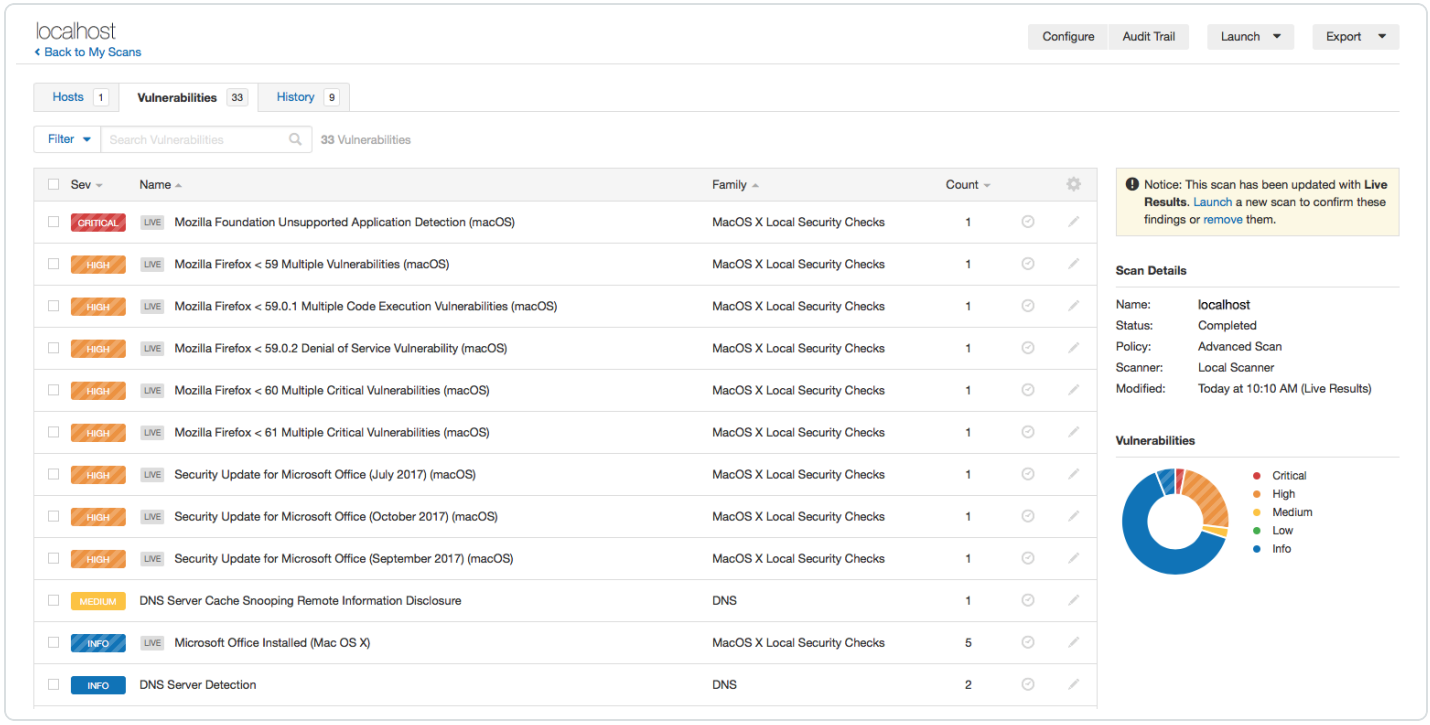
List of a single host's scan results by plugin severity and plugin name	Details of a single host's plugin scan result
	

Live Results

Tenable Nessus updates with new plugins automatically, which allows you to assess your assets for new vulnerabilities. However, if your scan is on an infrequent schedule, the scan may not run new plugins until several days after the plugin update. This gap could leave your assets exposed to vulnerabilities that you are not aware of.

In Nessus Professional and Nessus Expert, you can use *live results* to view scan results for new plugins based on a scan's most recently collected data, without running a new scan. Live results allow you to see potential new threats and determine if you need to launch a scan manually to confirm the findings. Live results are not results from an active scan; they are an assessment based on already-collected data. Live results don't produce results for new plugins that require active detection, like an exploit, or that require data that was not previously collected.

Live results appear with striped coloring in scan results. In the **Vulnerabilities** tab, the severity indicator is striped, and the **Live** icon appears next to the plugin name.



The results page shows a note indicating that the results include live results. Tenable recommends that you manually launch a scan to confirm the findings. The longer you wait between active scans, the more outdated the data may be, which lessens the effectiveness of live results.

To manage live results, see the following:

- Enable or Disable Live Results
- Remove Live Results

Enable or Disable Live Results

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

The first time you enable live results on a scan, the scan results update to include findings for plugins that were enabled since the last scan. The scan then updates with live results whenever there is a new plugin update. Live results are not results from an active scan; they are an assessment based on a scan's most recently collected data. Live results do not produce results for new plugins that require active detection, like an exploit, or that require data that was not previously collected. To learn more, see Live Results.

To enable or disable live results:

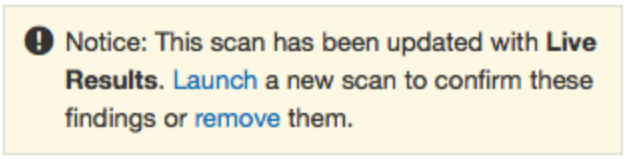
1. In Tenable Nessus Professional or Tenable Nessus Expert, create a new scan or edit an existing scan.
2. Go to the **Settings** tab.
3. Under **Post-Processing**, enable or disable **Live Results**:
   - To enable, select the **Live Results** check box.
   - To disable, clear the **Live Results** check box.
4. Click **Save**.

   Tenable Nessus enables or disables live results for this scan.

Remove Live Results

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

In Nessus Professional and Nessus Expert, if a scan includes live results, Tenable Nessus shows the following notice on the scan results page.



If you remove live results, they no longer appear on the scan results page. However, live results will re-appear the next time Nessus updates the plugins (unless you disable the feature for the scan).

Tip: To launch the scan and confirm the live results findings, click **Launch** in the notice before you remove the findings.

To remove Live Results findings from the scan results page:

- In the notice, click **remove**.

Scan Exports and Reports

Note: You cannot create scan exports or reports when using Tenable Nessus Essentials. If you are using Tenable Nessus Essentials Plus, you can create PDF and HTML reports. For information about upgrading to Tenable Nessus Professional, see Tenable Nessus Professional.

You can export scans as a Tenable Nessus file or a Tenable Nessus DB file, as described in Export a Scan. You can then import these files as a scan or policy, as described in Import a Scan and Import a Policy.

You can also create a scan report in several different formats. For more information, see Create a Scan Report.

User report templates to define the content of a report, based on chapter selection and ordering. Once you define your custom templates custom (for more information, see Create a Custom Report Template), you can use them to generate HTML or PDF reports for scan results. In addition to custom templates, Nessus provides some predefined system templates. To view custom and system report templates, see Customized Reports. For more information on the system templates, see https://www.tenable.com/nessus-reports.

Format	Description
Exports	
Nessus	A .nessus file in XML format that contains the list of targets, policies defined by the user, and scan results. Nessus strips the password credentials so they are not exported as plain text in the XML. If you import a .nessus file as a policy, you must re-apply your passwords to any credentials.
Nessus DB	A proprietary encrypted database format that contains all the information in a scan, including the audit trails and results. When you export in this format, you must enter a password to encrypt the results of the scan.

Policy	An informational JSON file that contains the scan policy details.
Timing Data	An informational comma-separated values (CSV) file that contains the scan hostname, IP, FQDN, scan start and end times, and the scan duration in seconds.
Reports	
PDF	A report generated in PDF format. Depending on the size of the report, PDF generation may take several minutes. You need either Oracle Java or OpenJDK for PDF reports.
HTML	A report generated using standard HTML output. This report opens in a new tab in your browser.
CSV	A CSV export that you can use to import into many external programs such as databases, spreadsheets, and more.

Export a Scan

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

You can export a scan from one Tenable Nessus scanner and import it to a different Tenable Nessus scanner. This helps you manage your scan results, compare reports, back up reports, and facilitates communication between groups within an organization. For more information, see Import a Scan.

You can export scan results as a Tenable Nessus file or as a Tenable Nessus DB file. For more information, see Scan Exports and Reports.

Note: For Tenable Nessus files, if you modified scan results using plugin rules or by modifying a vulnerability (for example, you hid or changed the severity of a plugin), the exported scan does not reflect these modifications..

Tip: If you need to export the results of a scan for vulnerability and remediation analysis, see Create a Scan Report.

Tip: For information about the encryption strength that Tenable Nessus uses for exports, see Encryption Strength.

To export a scan:

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

   The **My Scans** page appears.

2. Click a scan.

   The scan's results page appears.

3. In the upper-right corner, click **Export**.

4. From the drop-down box, select the format in which you want to export the scan results.

   - If you select **Tenable Nessus**, Tenable Nessus exports the *.nessus* XML file.
   - If you select **Tenable Nessus DB**, the **Export as Tenable Nessus DB** dialog box appears.

     a. Type a password to protect the file.

        When you import the Tenable Nessus DB file to another scanner, you must enter this password.

     b. Click **Export**.

        Tenable Nessus exports the Tenable Nessus Manager DB file.

   - If you select **Policy**, Tenable Nessus exports an informational JSON file that contains the scan policy details.
   - If you select **Timing Data**, Tenable Nessus exports an information CSV file that contains the scan hostname, IP, FQDN, scan start and end times, and the scan duration in seconds.

Create a Scan Report

> **Required user role when using Tenable Nessus Manager:** Standard, Administrator, or System Administrator

You can create a scan report to help you analyze the vulnerabilities and remediations on affected hosts. You can create a scan report in PDF, HTML, or CSV format, and customize it to contain only certain information.

When you create a scan report, it includes the results that are currently visible on your scan results page. You can also select certain hosts or vulnerabilities to specify your report.

To create a scan report:

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

   The **My Scans** page appears.

2. Click a scan.

   The scan's results page appears.

3. (Optional) To create a scan report that includes specific scan results, do the following:

   - Use search to narrow your scan results.
   - Use filters to narrow your scan results.
   - In the **Hosts** tab, select the checkbox in each row of a host you want to include in the scan report.
   - In the **Vulnerabilities** tab, select the checkbox in each row of each vulnerability or vulnerability group that you want to include in the scan report.

   Note: You can make selections in either **Hosts** or **Vulnerabilities**, but not across both tabs.

4. In the upper-right corner, click **Report**.

   The **Generate Report** window appears.

5. Select the format in which you want to export the scan results.

6. Configure the report for your selected format:

   PDF or HTML

   a. Click the **Report Template** you want to use.

      A description of the report template and a list of the template's applied filters appear.

      Tip: Select **Hide system templates** to view a list of your custom report templates only.

b. (Optional) If available for the report template you selected, you can enable or disable the **Include page breaks between vulnerability results** option.

c. (Optional) To save the selected report template as the default for PDF or HTML reports (depending on which format you selected), select the **Preferred Format** checkbox.

d. Click **Generate Report**.

   Tenable Nessus creates the scan report.

CSV

a. Select the checkboxes for the columns you want to appear in the CSV report.

   Tip: To select all columns, click **Select All**. To clear all columns, click **Clear**. To reset columns to the system default, click **System**.

b. (Optional) To save your current configuration as the default for CSV reports, select the **Preferred Format** checkbox.

c. Click **Generate Report**.

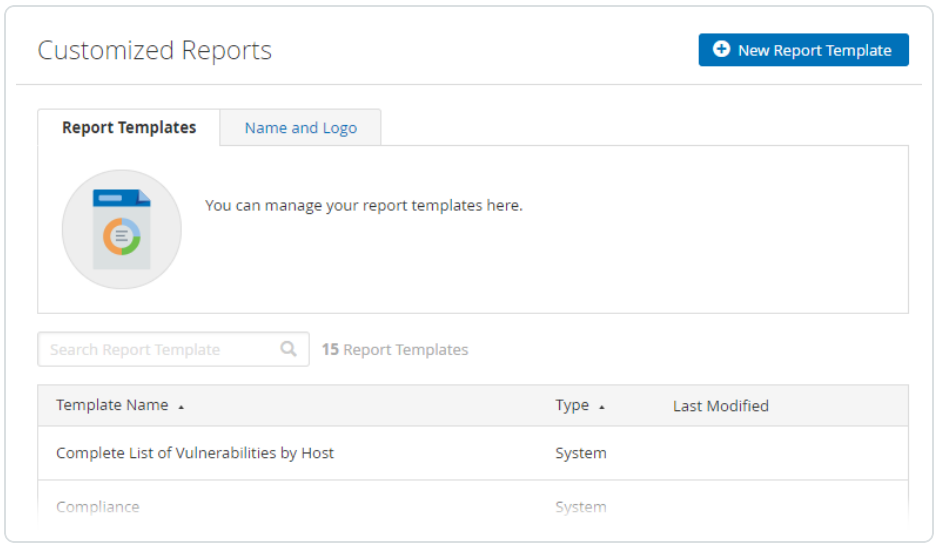
   Tenable Nessus creates the scan report.

Customized Reports

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

Note: This feature is only available for Tenable Nessus Manager, Tenable Nessus Professional, and Tenable Nessus Expert.

On the **Customized Reports** page, you can customize the title and logo that appear on each report and manage report templates.



Use the following procedures to manage customized reports:

Customize report title and logo

In Tenable Nessus, you can customize the title and logo that appear on each report. This allows you to prepare reports for different stakeholders.

To customize the report title and logo:

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Customized Reports**.

3. Click the **Name and Logo** tab.

4. In the **Custom Name** box, type the name that you want to appear on the report.

5. To upload a custom logo, click the **Upload** button.

   A window appears in which you can select a file to upload.

6. Click the **Save** button.

   Tenable Nessus saves your custom title and logo.

Create a custom report template

Tenable Nessus allows you to create custom report templates on the **Customized Reports** page in addition to the standard system report templates.

To create a custom report template:

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Customized Reports**.

   The **Report Templates** page appears.

3. In the top-right corner, click **New Report Template**.

   The **New Report Template** page appears.

4. In the **Name** texbox, enter the template name.

5. In the **Description** textbox, enter the template description.

6. Add report **Chapters** to the template. Chapters determine what information and statistics appear on the report.

   a. Click **Add a Chapter**.

      The **Add a Report Chapter** window appears.

   b. Click the chapter you want to add to the template. A description of the chapter appears below the chapter list.

   c. Click **Add** to add the selected chapter to the template.

      The **Add a Report Chapter** window closes, and Tenable Nessus adds the new chapter to the **Chapters** section. Repeat steps a-c to add another chapter.

7. Edit the selected template chapters.

   - Depending on the chapters selected, edit the chapter details. This may involve selecting or clearing check boxes or changing values.
   - Click the ↑↓ buttons to re-order the chapters.
   - Click ✕ to remove a chapter from the template.

8. Click **Save**. Tenable Nessus saves your report template. You can select and edit the template from the **Report Templates** tab.

Copy a report template

Tenable Nessus allows you to copy custom and system report templates to create a new report template.

To copy a custom report template:

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Customized Reports**.

   The **Report Templates** page appears.

3. In the row of the template you want to copy, click the button.

   The **Copy Report Template** window appears.

4. In the **Template Name** text box, enter the new template's name.

5. Click **Copy**. Tenable Nessus saves the new scan template. You can select and edit the template from the **Report Templates** tab.

Edit a custom report template

> **Note:** You can only edit custom templates.

To edit a custom report template:

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Customized Reports**.

   The **Report Templates** page appears.

3. Click the row for the custom template you want to edit.

   The template's detail page appears.

4. Edit the **Name**, **Description**, and **Chapters** as needed.
5. Click **Save**.

   Tenable Nessus saves your template changes.

Delete a custom report template

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

   The **My Scans** page appears.
2. In the left navigation bar, click **Customized Reports**.

   The **Report Templates** page appears.
3. In the report template table, in the row for the custom template you want to delete, click the ✕ button.

   The **Delete Report Template** window appears.
4. Click **Delete**.

   Tenable Nessus deletes your custom template.

Plugins

As information about new vulnerabilities is discovered and released into the general public domain, Tenable, Inc. research staff designs programs to enable Tenable Nessus to detect them.

These programs are called *plugins*. Tenable writes plugins in the Tenable Nessus proprietary scripting language called *Tenable Nessus Attack Scripting Language* (NASL).

Plugins contain vulnerability information, a generic set of remediation actions, and the algorithm to test for the presence of the security issue.

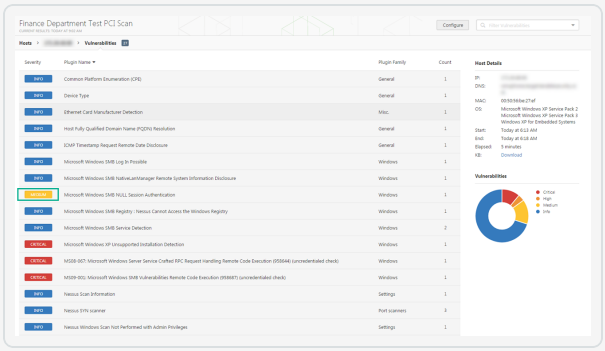
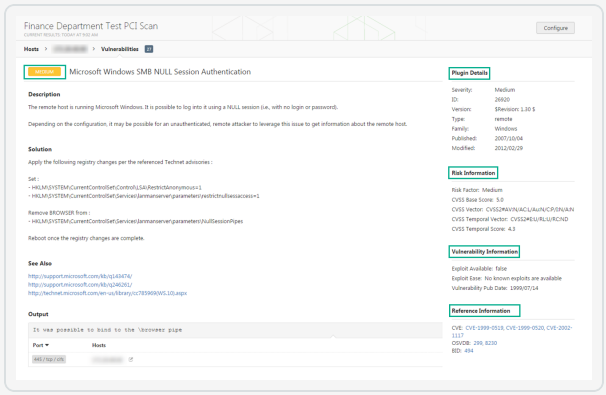
Tenable Nessus supports the Common Vulnerability Scoring System (CVSS) and supports v2, v3, and v4 values simultaneously. If CVSS2, CVSS3, and CVSS4 attributes are present, Tenable Nessus calculates all three scores.

Note: By default, new installations of Tenable Nessus use CVSSv3 scores (when available) to calculate severity for vulnerabilities. Preexisting, upgraded installations retain the previous default of CVSSv2 scores.

Tenable Nessus also uses plugins to obtain configuration information from authenticated hosts, which Tenable Nessus uses for configuration audit purposes against security best practices.

To view plugin information, see a list of newest plugins, view all Tenable Nessus plugins, and search for specific plugins, see the **Tenable Nessus Plugins** home page.

Example Plugin Information

List of a single host's scan results by plugin severity and plugin name	Details of a single host's plugin scan result
	

How do I get Tenable Nessus plugins?

By default, Tenable Nessus automatically updates plugins and checks for updated components and plugins every 24 hours.

During the **Product Registration** portion of the browser portion of the Tenable Nessus install, Tenable Nessus downloads all plugins and compiles them into an internal database.

You can also use the `nessuscli fetch –register` command to download plugins manually. For more details, see the command line section of this guide.

Optionally, during the **Registration** portion of the browser portion of the Tenable Nessus install, you can choose the **Custom Settings** link and provide a hostname or IP address to a server which hosts your custom plugin feed.

How do I update Tenable Nessus plugins?

By default, Tenable Nessus checks for updated components and plugins every 24 hours.

You can trigger a manual update on an individual Tenable Nessus scanner by navigating to the **Settings** > **About** page and clicking ↻ next to the **Last Updated** section. You can check the current installed plugin set in the same section. In Tenable Nessus Manager, you can perform these same actions for linked scanners in each linked scanner's details section.

You can also use the `nessuscli update --plugins-only` command to update plugins manually. For more details, see Nessuscli.

Tip: To install plugins when Tenable Nessus is offline or air-gapped, see Install Plugins Manually.

Create a Limited Plugin Policy

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

In addition to using the Tenable Nessus preset scan templates, you can create a limited plugin policy to scan with a custom selection of plugins.

Note: If your organization has any limited plugin policies or plans to create them, Tenable highly recommends keeping the **Auto Enable Plugin Dependencies** advanced setting enabled. This setting automatically enables any supporting plugins that your selected plugins may need to collect scan data. For more information, see Scanning (Advanced Settings).

To create a limited plugin policy:

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.

3. In the upper right corner, click the **New Policy** button.

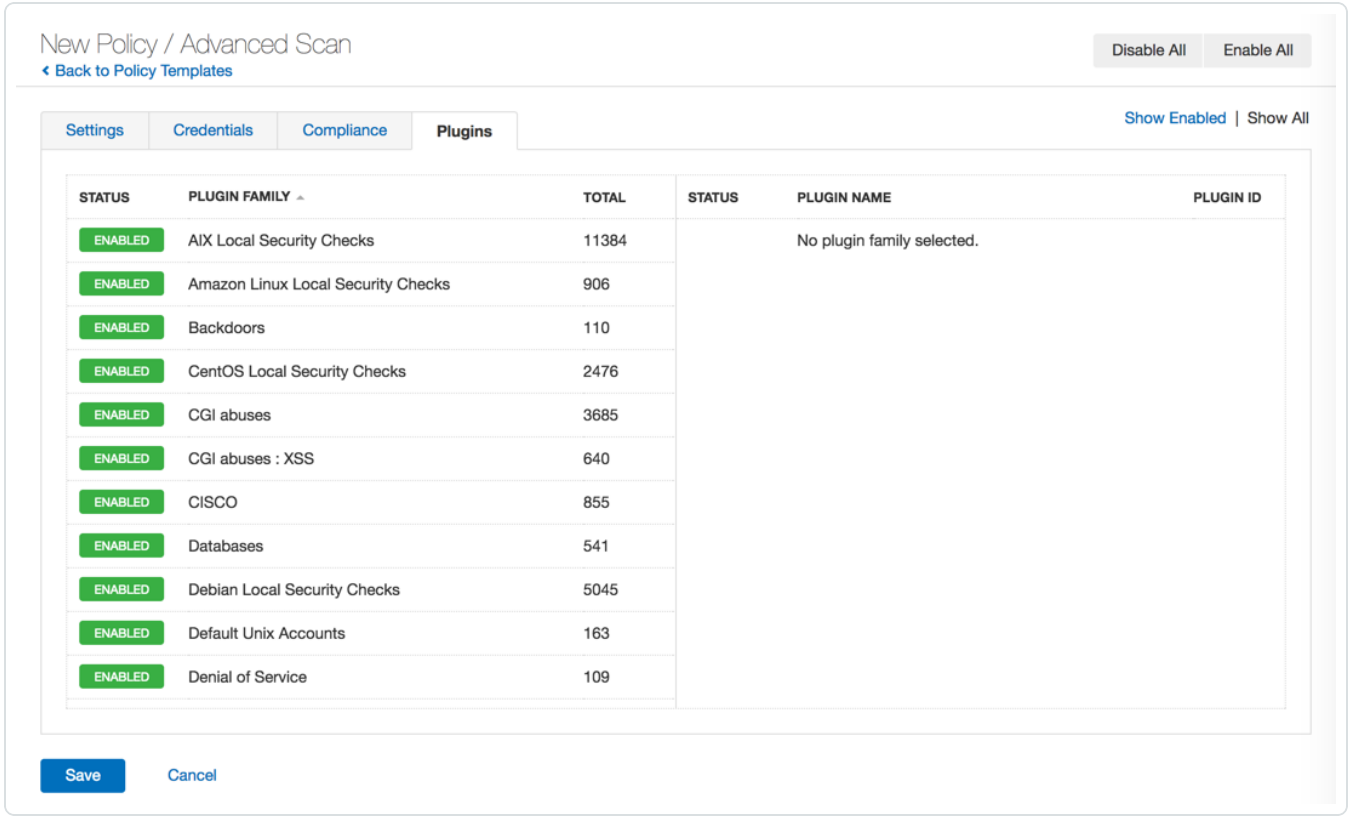
   The **Policy Templates** page appears.

4. Click the **Advanced Scan** template.

   The **Advanced Scan** page appears.

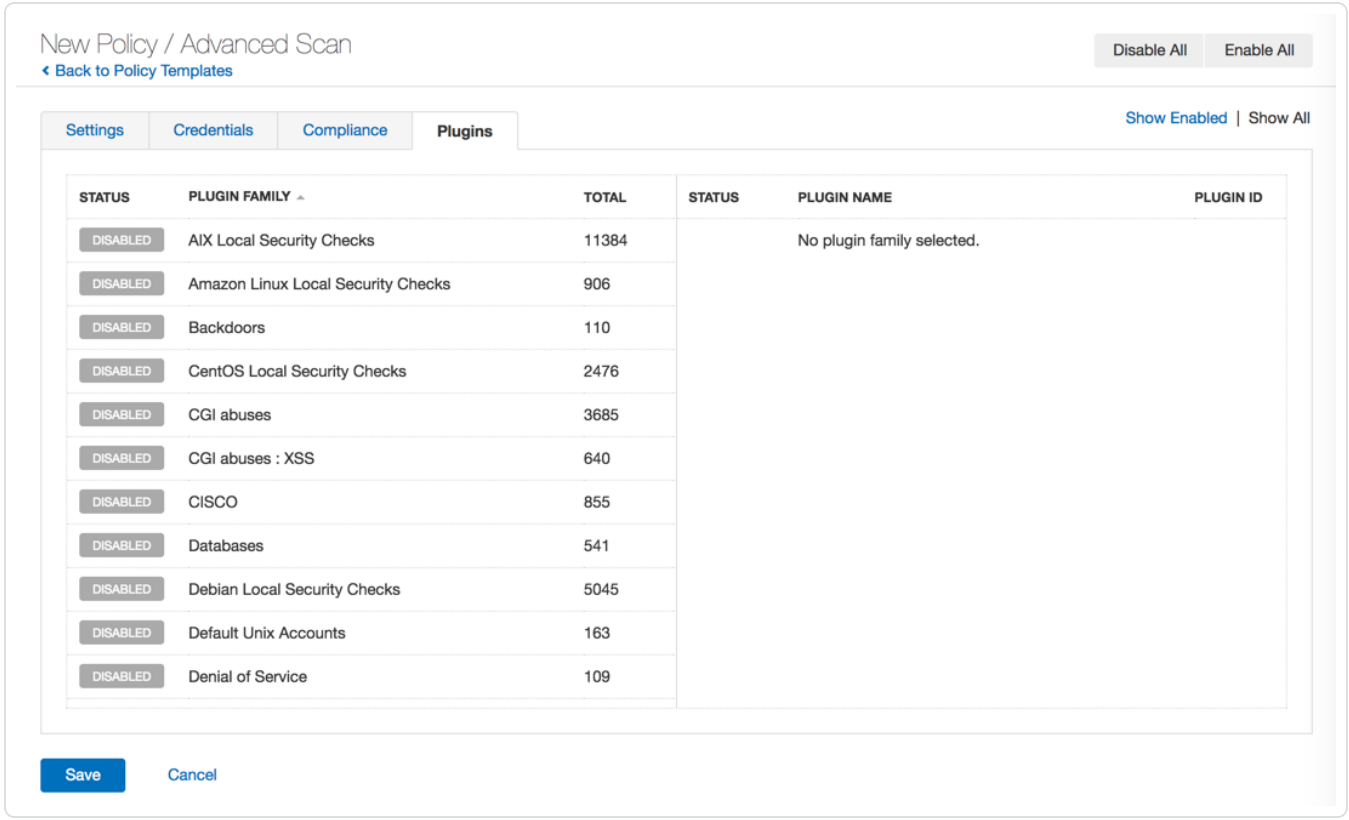
5. Click the **Plugins** tab.

   The list of plugin families appears, and by default, Tenable Nessus enables all the plugin families.



6. In the upper right corner, click the **Disable All** button.

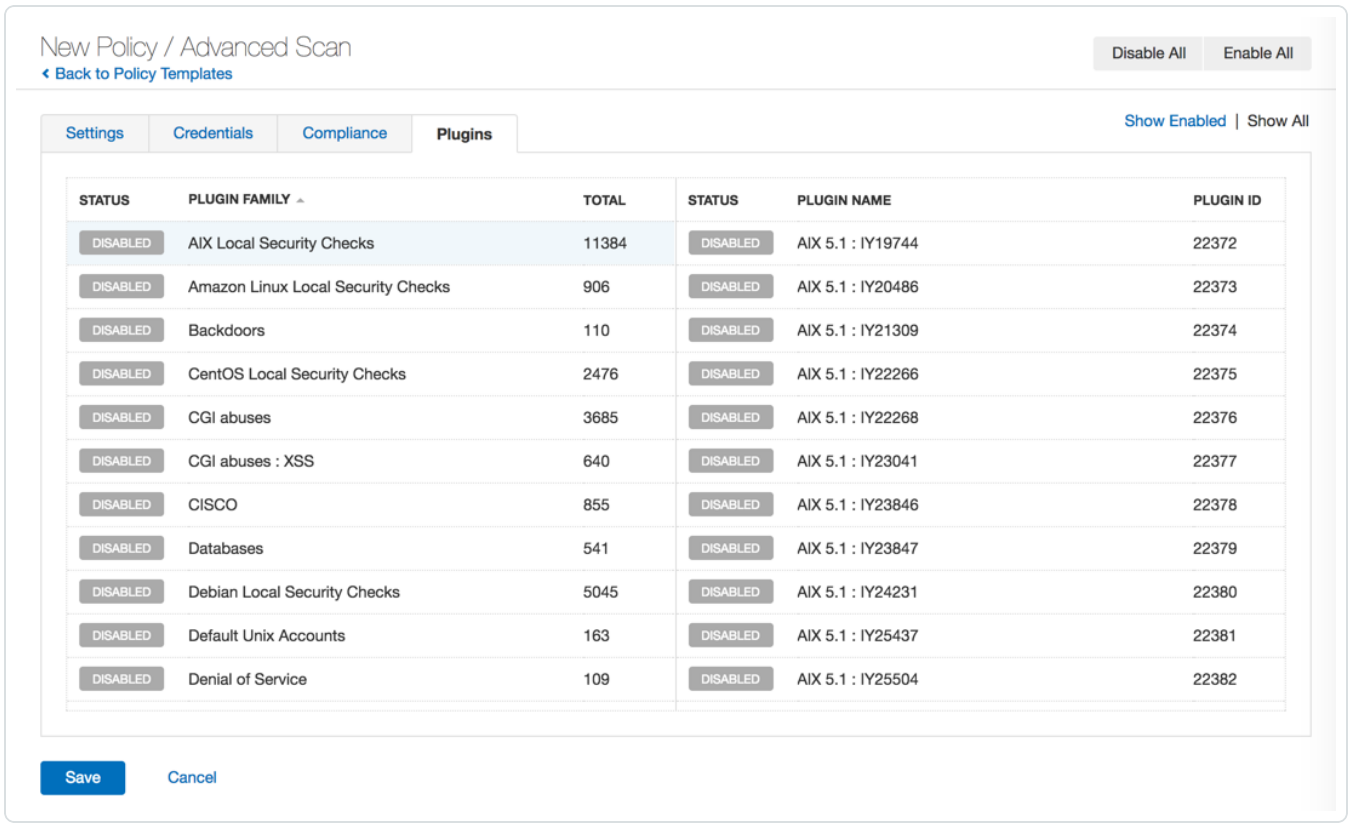
   Tenable Nessus disables all the plugin families.



Tip: To enable or disable all plugins quickly, click the **Enable All** and **Disable All** buttons in the upper right corner. If you only need to enable one or a few individual plugins, Tenable recommends disabling all plugins. Then, you can select individual plugins as described in step 8.

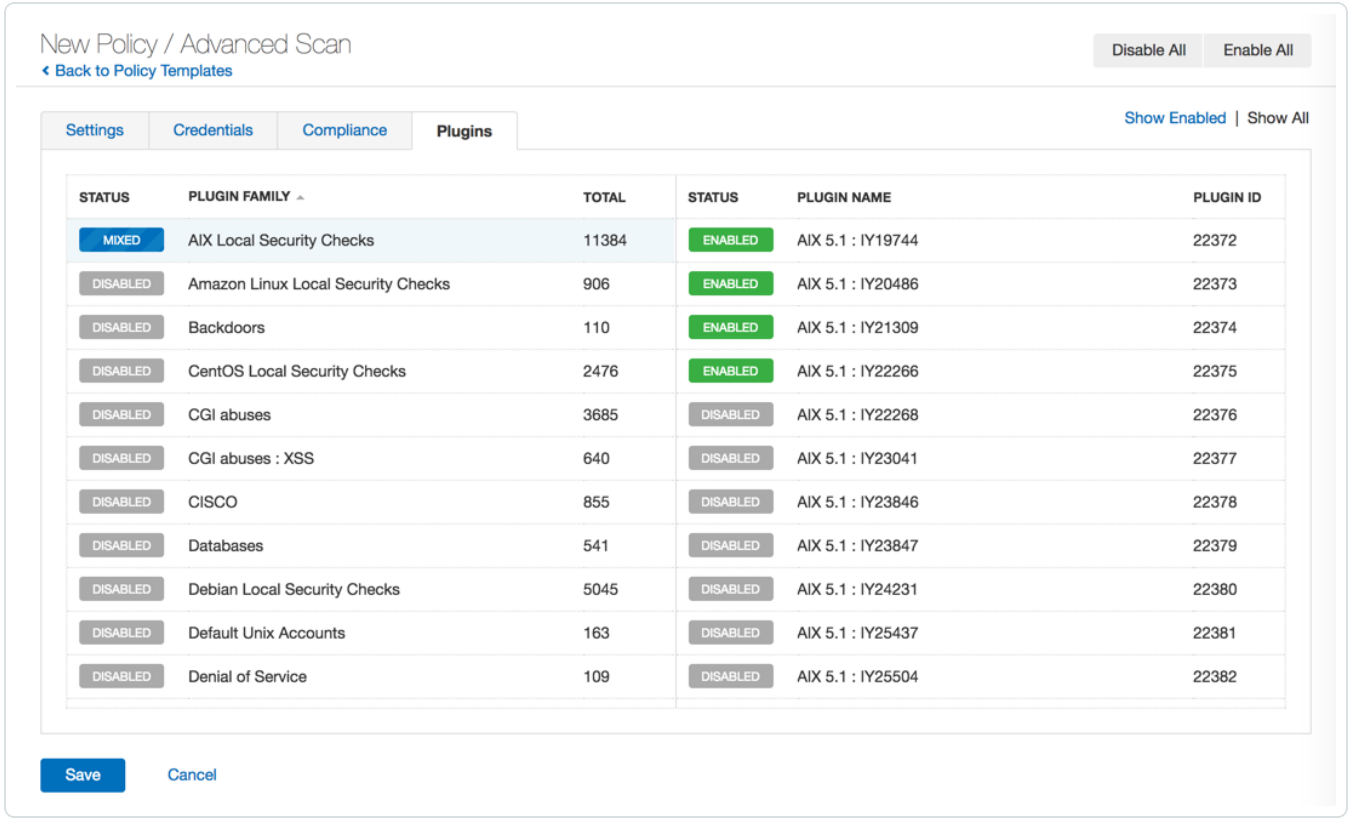
7. Click the plugin family that you want to include.

   The list of plugins appears in the left navigation bar.



8. For each plugin that you want to enable, click the **Disabled** button.

   Tenable Nessus enables each plugin.



Tip: You can search for plugins and plugin families using the **Filter** option in the upper right corner. This can help you search for individual plugins in large plugin families more quickly. For example, if you need to find an individual plugin, set the filter to `Match All of the following: Plugin ID is equal to <plugin ID>`. For more information, see Search and Filter Results.

9. Click the **Save** button.

   Tenable Nessus saves the policy.

Install Plugins Manually

Required user role when using Tenable Nessus Manager: System Administrator

You can manually update plugins on an offline Tenable Nessus system in two ways: the user interface or the command line interface.

Before you begin:

- Download and copy the Nessus plugins compressed TAR file to your system.

To install plugins manually using the Tenable Nessus user interface:

Note: You cannot use this procedure to update Tenable Vulnerability Management or Tenable Security Center-managed scanners. For more information about how linked scanners receive plugin updates, see Tenable Nessus Plugin and Software Updates.

1. On the **offline** system running Nessus (**A**), in the top navigation bar, click **Settings**.

   The **About** page appears.

2. Click the **Software Update** tab.

3. In the upper-right corner, click the **Manual Software Update** button.

   The **Manual Software Update** dialog box appears.

4. In the **Manual Software Update** dialog box, select **Upload your own plugin archive**, and then select **Continue**.

5. Navigate to the compressed TAR file you downloaded, select it, then click **Open**.

   Nessus updates with the uploaded plugins.

To install plugins manually using the command line interface:

1. On the **offline** system running Nessus (**A**), open a command prompt.

2. Use the `nessuscli update <tar.gz filename>` command specific to your operating system.

Platform	Command
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe update <tar.gz filename>`
macOS	`# /Library/Nessus/run/sbin/nessuscli update <tar.gz filename>`
Linux	`# /opt/nessus/sbin/nessuscli update <tar.gz filename>`

Plugin Rules

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

Plugin rules allow you to re-prioritize the severity of plugin results to better account for your organization's security posture and response plan.

The **Plugin Rules** page allows you to hide or change the severity of any given plugin. In addition, you can limit rules to a specific host or specific timeframe. From this page you can view, create, edit, and delete your rules.

> **Note:** You cannot apply custom plugin rules to PCI templates.

You can configure the following options for a plugin rule:

Option	Description
Host	The host that the plugin rule applies to. You can enter a single IP address or DNS address, or you can leave the box blank to apply the rule to all hosts. The **Host** option must follow the same formatting as the Designate hosts by their DNS name setting. In other words, if you disabled the setting, enter an IP address for **Host**. If you have the setting enabled, enter a DNS address for **Host**. **Note:** If the plugin is enabled in two different scan configurations that have conflicting Designate hosts by their DNS name settings, Tenable recommends creating two separate plugin rules for the plugin: one rule for the IP address, and one rule for the DNS address.
Plugin ID	The plugin that the plugin rule applies to.
Expiration Date	(Optional) The date on which the plugin rule ages out.
Severity	The severity that Nessus assigns the plugin while the plugin rule is active.

Use the following procedures to manage plugin rules:

Create a plugin rule

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Plugin Rules**.
3. In the upper right corner, click the **New Rule** button.

   The **New Rule** window appears.
4. Configure the settings.
5. Click the **Save** button.

   Tenable Nessus saves the plugin rule.

Modify a plugin rule

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

   The **My Scans** page appears.
2. In the left navigation bar, click **Plugin Rules**.
3. On the plugin rules table, select the plugin rule that you want to modify.

   The **Edit Rule** window appears.
4. Modify the settings as necessary.
5. Click the **Save** button.

   Tenable Nessus saves the settings.

Delete a plugin

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

   The **My Scans** page appears.
2. In the left navigation bar, click **Plugin Rules**.
3. On the plugin rules table, in the row for the plugin that you want to modify, click the ✕ button.

   A dialog box appears, confirming your selection to delete the plugin rule.
4. Click the **Delete** button.

   Tenable Nessus deletes the plugin rule.

Example Plugin Rule

Host: 192.168.0.6

Plugin ID: 79877

Expiration Date: 12/31/2022

Severity: Low

This example rule applies to scans performed on IP address 192.168.0.6. Once saved, this plugin rule changes the default severity of plugin ID 79877 (CentOS 8: rpm (CESA-2014:1976) to a severity of low until 12/31/2022. After 12/31/2022, the results of plugin ID 79877 returns to its critical severity.

Web Application Scanning in Tenable Nessus

Web application scanning (WAS) is available in Tenable Nessus Expert. Web application scanning in Tenable Nessus allows you to scan and address web application vulnerabilities that Tenable Nessus scanners, Tenable Agents, or Tenable Network Monitor cannot scan.

Note: The following platforms do not support web application scanning in Tenable Nessus:

- Any host system that does not support Docker
- Any host that uses an ARM-based processor (for example, AArch64 Linux distributions and Apple Silicon systems)

For more information about Docker support on virtualized hosts, see the Docker documentation.

Note: Tenable Nessus Expert only allows one concurrent web application scan at a time.

Licensing

If you license web application scanning in Tenable Nessus Expert, you can scan up to five different web application URLs per 90 days.

Tenable Nessus uses only the hostname and port (`FQDN:port`) to track against WAS licenses instead of the full URL. For example, all of the following targets count for a single license FQDN:

- https://example.com/welcome
- https://example.com/welcome/get-started
- https://example.com/welcome/get-started/create-new-user

If you do not perform a web application scan on a target URL for 90 days, Tenable Nessus removes the URL from your license and it no longer counts towards your URL limit. You cannot delete web application scan data to remove the URL from your license.

You can purchase additional URLs by contacting your Tenable representative.

Prerequisites

Before you enable web application scanning in Tenable Nessus Expert, you must install Docker version 20.0.0 or later on your Tenable Nessus host. Tenable Nessus Expert only supports Dock installations that follow the Docker install documentation.

Enable web application scanning

1. Under **Resources** in the left-side navigation pane, click **Web App Scanning**.

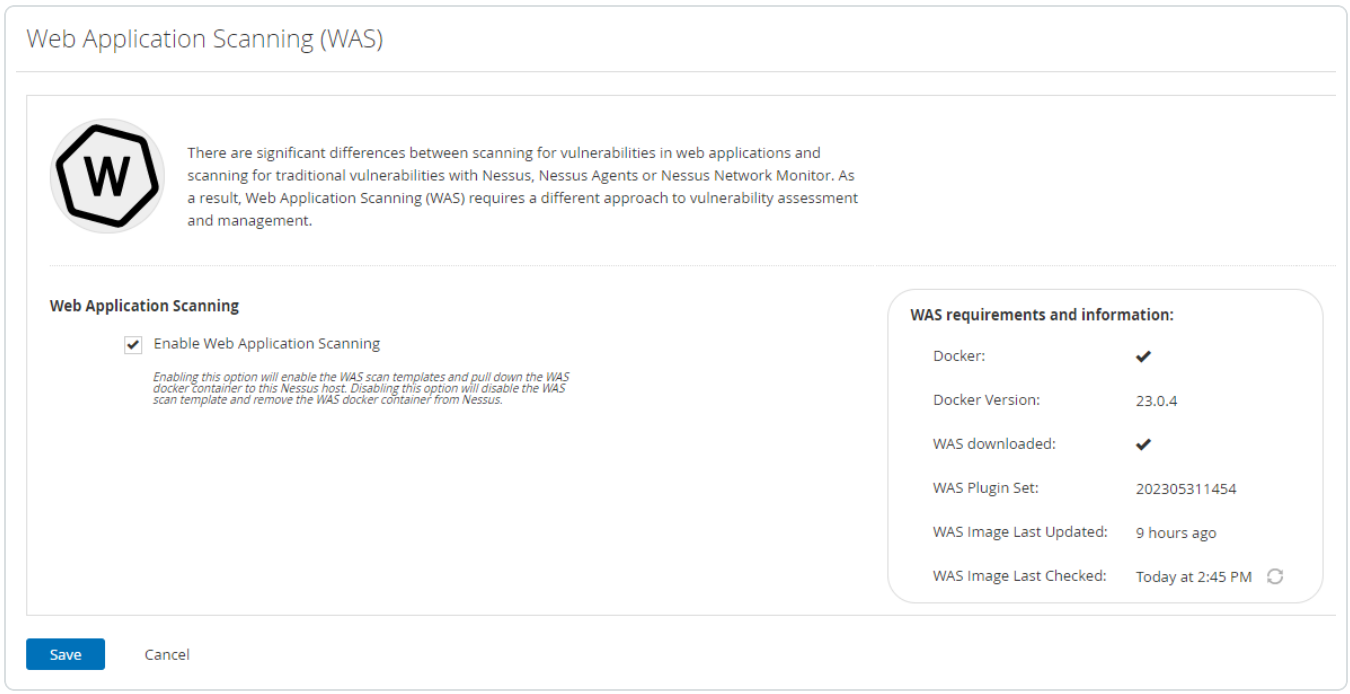
   The **Web Application Scanning (WAS)** page appears. The **WAS requirements and information** section shows whether Docker is installed on your Tenable Nessus host, the Docker version, whether web application scanning is downloaded on your Tenable Nessus host, and the current web application scanning plugin set.

2. Select the **Enable Web Application Scanning** checkbox.

3. Click **Save**.

   Tenable Nessus starts to download the latest web application scanning image.

   Once the web application scanning download completes, the **WAS requirements and information** section indicates that web application scanning is downloaded (as shown in the following image). You can now view **Web App** scan templates in the Tenable Nessus scanning user interface and perform web application scans.



Tip: With web application scanning installed, you can click next to the **WAS Image Last Checked** field to update Tenable Nessus with the latest Tenable Web App Scanning version.

For more information on how to install Tenable Nessus Expert and web application scanning, see the following video: Web App Scanning in Nessus Expert 10.6.

Web application scanning in offline mode

You can still perform web application scanning when Tenable Nessus is in offline mode.

After you perform the Enable web application scanning in Tenable Nessus steps, Tenable Nessus will not be able to automatically download the latest web application scanning image if it is in offline mode. Instead, you can upload the image manually using the following steps:

To upload the image manually and enable web application scanning in offline mode:

1. Find and save the Tenable web application scanning image as a tarball file in the Tenable Docker hub. For more information, see the Docker image save documentation.
2. Do one of the following:

- To upload the image in the Tenable Nessus user interface:

  a. Navigate to the **Web Application Scanning** page in Tenable Nessus.

  b. Click **Upload WAS Image** upper-right corner.

     The file explorer opens.

  c. Select the saved web application tarball file.

     Tenable Nessus begins downloading the tarball file. Once the download completes, you can proceed to scan with a web application scanning template.

- To upload the image from `nessuscli`:

  a. From `nessuscli`, enter the following command:

     ```
     nessuscli was --upload-image <image tarball file>
     ```

     Tenable Nessus begins downloading the tarball file. Once the command finishes running, you can proceed to scan with a web application scanning template.

What to do next:

- Create a scan with a web application scanning template.

Triggered Agent Scans (Tenable Nessus Manager)

When you configure a Tenable Agent scan in Tenable Nessus Manager, Tenable Nessus Manager offers two agent scan types: **Scan Window** and **Triggered Scan**.

For scan window scans, Tenable Nessus Manager creates a timeframe (for example, the default is three hours) in which an agent group must report in order to be included in the scan results. You must schedule Tenable Nessus Manager to launch window scan at a scheduled time, or you must manually launch the scan from the Tenable Nessus Manager user interface (for example, if you schedule a three-hour agent window scan for every Monday, Tenable Nessus Manager pulls data updates from the agent group for three hours every Monday).

Agents can be triggered to launch scans using three different methods:

- Interval trigger — Configure agents to scan at a certain time interval (for example, every 12 hours or every 24 hours).
- File Name trigger — Configure agents to scan whenever a file with a specific file name is added to the agent trigger directory. One trigger file correlates to one scan launch; when you launch a scan with this method, the file is removed. The agent trigger directory location varies by operating system:

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

- `nessuscli` trigger — Launch an existing triggered scan manually by running the following command in the Tenable Agent `nessuscli` utility:

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

You can also set multiple triggers for a single scan, and the scan searches for the triggers in their listed order (in other words, if the first trigger does not trigger the scan, it searches for the second trigger).

Note: Triggered scans are not affected by freeze windows.

Triggers vs. Scan Windows

Tenable recommends using triggered scans over scan window scans in many cases. Due to the scanning independence from Tenable Nessus Manager or user intervention and the multiple trigger options, triggered scanning offers more flexibility to meet the needs of your workflow, especially if you have a mobile workforce in multiple time zones.

Triggered scans can provide more consistent coverage than window scans and help overcome connectivity issues between Tenable Nessus Manager and linked agents. While scan window scans can create gaps in data coverage due to unresponsive or offline agents, triggered scans allow agents to scan and send data to Tenable Nessus Manager whenever the triggers occur; Tenable Nessus Manager accepts and processes data from triggered scans at any time.

Find Triggered Scan Details

In addition to managing triggered scans from Tenable Nessus Manager, you can view triggered scan details by running the following command in the Tenable Agent `nessuscli` utility:

```
# nessuscli scan-triggers --list
```

The `--list` command returns the agent's triggered scan details. These details include:

- Scan name
- Status (for example, **uploaded**)
- Time of last activity (shown next to the status)
- Scan description
- Time of last policy modification
- Time of last run
- Scan trigger description
- Scan configuration template

For more information about the Tenable Agent `nessuscli` utility, see Nessuscli Agent.

You can also view your agent trigger information in the agent trigger directory:

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

Error Messages

The following table lists the error messages that you may see while scanning in Tenable Nessus, and how Tenable recommends that you resolve each error. For more information about creating, modifying, and launching scans, see Scans.

Warning	Description	Recommended Action
Auto configuration	This warning indicates that occurred during the JSON deployment process. The following are examples of possible descriptions: • `Maximum number of retries reached; linking has failed.` • `Linking failed; will retry after X seconds.` • `Could not create user; forbidden username.` • `Invalid 'permissions' field` • `Username exceeds limit` • `Duplicate username` • `Failed to create user.`	Verify that the JSON deployment is configured correctly. Then, attempt to redeploy. Contact Tenable Support for further assistance.
Your Tenable Nessus global configuration database is corrupt. You can repair the database using the nessuscli system `--config-optimization` command or restore Tenable Nessus from a backup file. Contact Tenable Support for further assistance.	The Tenable Nessus configuration database became corrupt and may result in unwanted errors.	You can repair the database using the nessuscli system `--config-optimization` command or restore Tenable Nessus from a backup file. Contact Tenable Support for further assistance.
No valid targets in list	There were no valid targets in the scan's target list.	Verify that the scan's target list contains

Warning	Description	Recommended Action
		one or more targets in valid Tenable Nessus Scan Target format. Check your target rules file to determine whether the targets are prohibited. Adjust the scan's target list to ensure at least one valid, permitted target is present and re-scan.
Can't resolve target [target name]	Tenable Nessus could not resolve the target IP address.	Verify the target name is correct, then verify that a DNS entry exists and is correct for the target. Once the target name and DNS entries are correct, re-scan.
Unparseable target [target name]	Tenable Nessus did not scan the target because the name did not match any valid target specification.	Correct the target name to conform to one of the valid Tenable Nessus Scan Target formats.
Restricted target [target name]	Tenable Nessus did not scan the target because the IP address is not scannable (for example, 0.0.0.0).	Remove the target from the scan's target list.
Rejected attempt to scan [target], as it	Tenable Nessus cannot scan the target due to user-specified scanning	Remove the target from the scan's target

Warning	Description	Recommended Action
violates user-defined rules	restrictions.	list or adjust the target rules file.
The allowed number of live hosts scanned with Nessus Essentials has been reached - please contact Tenable to upgrade your license.	Tenable Nessus did not scan the target because the number of targets for a single scan exceeded the maximum allowed under the Tenable Nessus Essentials licensing terms.	Reduce the number of targets in the scan, or upgrade Tenable Nessus.
The licensed number of live hosts scanned has been reached - please contact Tenable to upgrade your license.	Tenable Nessus did not scan the target because the number of targets for a single scan exceeded the maximum allowed under the Tenable Nessus licensing terms.	Reduce the number of targets in the scan, or upgrade Tenable Nessus.
Your current Nessus scanner license limits your scans to [count] live IP addresses. You've now scanned over [count] different IP addresses over time, and Nessus will not let you scan any additional hosts. In order to increase this limit, please contact Tenable to upgrade your license.	Tenable Nessus did not scan the target because the cumulative number of unique targets across all scans exceeded the maximum allowed under the Tenable Nessus Essentials licensing terms.	Remove targets from the scan to conform to the licensing terms, or upgrade Tenable Nessus.
Your current Nessus scanner license limits your scans to [count] live IP addresses. You've	Tenable Nessus did not scan the target because the cumulative number of unique targets across all scans exceeded the maximum allowed under the Tenable Nessus evaluation license	Remove targets from the scan to conform to the licensing terms, or upgrade Tenable Nessus.

Warning	Description	Recommended Action
now scanned over [count] different IP addresses over time, and Nessus will not let you scan any additional hosts. In order to increase this limit, please contact Tenable to upgrade your license.	terms.	
Your current Nessus scanner license limits your scans to [count] live IP addresses. You've now scanned over [count] different IP addresses, and Nessus will not let you scan any additional hosts. In order to increase this limit, please contact Tenable.	Tenable Nessus did not scan the target because the cumulative number of unique targets across all scans exceeded the maximum allowed under the Nessus license terms.	Remove targets from the scan to conform to the licensing terms, or upgrade Tenable Nessus.
The network interface [interface] does not support packet forgery This prevents Nessus from determining whether some of the target hosts are alive and from performing a full port scan against them.	Tenable Nessus attempted to establish a session for sending or receiving raw IP packets, but failed.	Tenable recommends scanning over a different network interface. You may be able to resolve this problem by disabling the Ping the remote host scan setting and providing Tenable Nessus with

Warning	Description	Recommended Action
		credentials to the remote host to prevent a port scan from taking place.
VMware Fusion does not support packet forgery from the host OS to the target OSs. This prevents Nessus from determining whether some of the target hosts are alive and from performing a full port scan against them. If you want to scan your targets within VMware Fusion, either scan them from a different host or install Nessus in a Fusion VM and scan them from there.	The Tenable Nessus scanner was installed in an unsupported VMWare Fusion configuration.	Install Tenable Nessus on a different host.
The network interface [interface] was not always available for packet forgery, which may lead to incomplete results. This is likely to be a transient error due to a lack of resources on this host. To correct this error, reduce the number of scans and/or	Packet forgery succeeded at least once on the reported interface, but a subsequent attempt to open a packet forgery session failed.	Verify the current values of, and adjust, the Tenable Nessus Advanced Settings related to scanner performance. If the problem persists, report the issue to Tenable. Include the full

Warning	Description	Recommended Action
hosts scanned in parallel.		contents of the scanner logs nessusd.messages and nessusd.dump in the report.
A packet with actual length of [length] bytes was truncated to [truncated length] bytes. The current snapshot length of [snapshot length] for interface [interface name] is too small. Consider either setting the pcap.snaplen preference to at least [%] or ensuring your network is configured so that packets received by the OS are not greater than the device's MTU	Tenable Nessus attempts to capture raw IP packets for analysis during a scan. This error can occur when the received packet is larger than expected and is truncated. In rare circumstances, this may affect the accuracy of scan results.	Verify the current values of, and adjust, the Tenable Nessus Advanced Settings related to scanning.
[target] has been turned off, crashed or became unreachable during the audit – scan was interrupted prior to completion	Tenable Nessus determined that the target was alive, and began scanning. During the scan, the target stopped responding, and the scanner terminated the scan for that target only. The scan results may be incomplete. This may be the result of a temporary network disruption, a service that failed or restarted on the target, or the target	Verify that the target is active and running. Check any running services and start or restart as needed. Once the target is determined to be active, re-scan.

Warning	Description	Recommended Action
	may have crashed or been removed from the network.	
Some network congestion was detected during the scan. This may indicate that one or more of the remote hosts are connected through a connection that does not have enough bandwidth to cope with this scan. To reduce the risk of congestion: - Reduce 'max hosts' to a lower value - Increase the 'network read timeout' in your policy	There were intermittent failures to connect to a target port that is known to be open.	Verify the current values of, and adjust, the Tenable Nessus Advanced Settings related to scanner performance. Increase the Network timeout setting in the scan policy, then re-scan.
Scan not started for Nessus Agent [agent name]	During an agent scan, the agent did not start the scan.	Check whether the agent is present on the network. Verify network connectivity between the agent and the Tenable Nessus Manager/Tenable Vulnerability Management. Re-run the agent scan once you verify the agent is online.

Warning	Description	Recommended Action
[count] Nessus Agents didn't start scan: [agent names]	During an agent scan, the agent did not start the scan.	Check whether each agent is present on the network. Verify network connectivity between the agents and the Tenable Nessus Manager/Tenable Vulnerability Management. Re-run the agent scan once you verify the agents are online.
Scan not completed for Nessus Agent [agent name] at [agent IP]	During an agent scan, the agent did not report a scan result.	Check whether the agent is present on the network. Verify network connectivity between the agent and the Tenable Nessus Manager/Tenable Vulnerability Management. Re-run the agent scan once you verify the agent is online.
[count] Nessus Agents didn't complete scan: [agent names]	During an agent scan, the agents did not report a scan result.	Check whether each agent is present on the network. Verify network connectivity between the agents

Warning	Description	Recommended Action
		and the Tenable Nessus Manager/Tenable Vulnerability Management. Re-run the agent scan once you verify the agents are online.
[count] Nessus Agents aborted scan: [agent names]	During an agent scan, the agents aborted the scan.	
Failed to import scan results from remote scanner	A managed Tenable Nessus scanner uploaded a scan result to Tenable Nessus Manager, but Tenable Nessus Manager could not process the scan result.	Check if Tenable Nessus Manager has enough disk space, or if the scan result uploaded by the scanner is corrupted due to network or disk errors.
Failed to import scan results from remote Nessus Agent [agent name] at [agent IP] - [error]	An agent uploaded a scan result to either a cluster child node or Tenable Nessus Manager, but the scan result could not be processed.	Check if Tenable Nessus Manager has enough disk space, or if the scan result uploaded by the scanner is corrupted due to network or disk errors.
Failed to import scan results from remote node	In a clustered scan, a cluster "child node" is a Tenable Nessus scanner that manages agents, and is managed by a	Check if Tenable Nessus Manager has enough disk space, or

Warning	Description	Recommended Action
	Tenable Nessus Manager. This error happens when a scan result is uploaded by a child node to a Tenable Nessus Manager, but the result processing fails.	if the scan result uploaded by the scanner is corrupted due to network or disk errors.
The scan report file was not found	A plugin attempted to attach a file to a scan result, but the file does not exist.	Check the disk space on the scanner. If there is insufficient space, make room by removing unneeded files, or by adding disk space.
The scan report was [size] which is greater than the [max size] threshold for attaching.	A plugin attempted to attach a file to a scan result, but the file is too large.	Try adjusting the attached_report_maximum_size setting. If it is over 50MB, try to filter out the results in the report to reduce the size.
This audit has been deprecated and was not executed: [audit file name]	A Tenable Nessus Compliance Audit scan specified an audit file that is no longer supported. The scan will proceed, but the deprecated audit file will be skipped.	Remove the deprecated audit from the scan settings.
It was not possible to email this scan: [error]	Tenable Nessus has been configured to email scan results when a scan has completed, but the attempt to email the results failed.	Check that the configured email address and server are correct, and that the server is online

Warning	Description	Recommended Action
		and can be reached from the scanner.
Unenforceable Rules	Some dynamic rules are disabled because IP address resolution. Rules containing the following host names are affected: [rules]	Verify that the host names are correct and check your DNS configuration.
[varies]	A plugin reported an error.	
Portscanner max ports exceeded	Warning: portscanners have found more than [number of ports] open for [target], and the number of reported ports has been truncated to [number of ports] (threshold controlled by scanner preference portscanner.max_ports). Usually this is due to intervening network equipment intercepting and responding to connection requests as a countermeasure against port scanning or other potentially malicious activity. Since this negatively impacts both scan accuracy and performance, you may want to adjust your network security configuration to disable this behavior for vulnerability scans.	Adjust your network security configuration or the portscanner.max_ports preference.
Report max ports exceeded	Warning: [ports] were found to be open for [target] - since this exceeds the threshold of [number of ports] (controlled by scanner preference report.max_ports), these results have been removed from the scan report. Usually this is due to intervening	Adjust your network security configuration or the report.max_ports preference.

Warning	Description	Recommended Action
	network equipment intercepting and responding to connection requests as a countermeasure against portscanning or other potentially malicious activity. Since this negatively impacts both scan accuracy and performance, you may want to adjust your network security configuration to disable this behavior for vulnerability scans.	
SYN scanner timeout	The SYN port scan against [targets] timed out after [number of seconds] - TCP port results may be incomplete.	The SYN port scanners can run slowly under certain circumstances. The most frequent causes are poor network connectivity between the scanner and the host being scanned, and the configuration of boundary devices such as firewalls. Take one of the following actions: • Modify boundary device settings • Reduce the number of ports scanned • Increase the port scanner timeout

Warning	Description	Recommended Action
		Contact Tenable Support for guidance on how to increase the timeout.
TCP scanner timeout	The TCP port scan against [targets] timed out after [number of seconds] - TCP port results may be incomplete.	The TCP port scanners can run slowly under certain circumstances. The most frequent causes are poor network connectivity between the scanner and the host being scanned, and the configuration of boundary devices such as firewalls. Take one of the following actions: • Modify boundary device settings • Reduce the number of ports scanned • Increase the port scanner timeout Contact Tenable Support for guidance on how to increase the timeout.

Warning	Description	Recommended Action
UDP scanner timeout	The UDP port scan against [targets] timed out after [number of seconds] - UDP port results may be incomplete.	The UDP port scanner is known to run for more than 24 hours under some circumstances. Therefore, Tenable recommends using the SYN scanner instead. If you cannot use the SYN scanner due to policy or technical reasons, either reduce the number of ports scanned or increase the UDP port scanner timeout. Contact Tenable Support for guidance on how to increase the timeout. **Note:** For scans executed on Tenable cloud scanners, the UDP port timeout is fixed at eight hours to prevent scan timeouts and other undesirable performance effects.

Sensors (Tenable Nessus Manager)

In Tenable Nessus Manager, the **Sensors** page provides a centralized interface for viewing and managing all of your linked Tenable Agents and Tenable Nessus scanners.

From the **Sensors** page, you can perform several key management tasks:

- Quickly check the connection status (online, offline, or disabled) for all linked agents and scanners.
- Access the necessary information and controls to link new agents or scanners to Tenable Nessus Manager.
- Select individual sensors to view detailed properties, manage group memberships (for agents), or unlink sensors that are no longer needed.

For detailed instructions on managing specific sensor types, see the following topics:

Agents — Learn how to link, manage, and configure Tenable Agents.

Scanners — Learn how to link and manage Tenable Nessus scanners.

Agents

Agents increase scan flexibility by making it easy to scan assets without needing ongoing host credentials or assets that are offline. Additionally, agents enable large-scale concurrent scanning with little network impact.

Once linked, you must add an agent to an agent group to use when configuring scans. Linked agents automatically download plugins from the manager upon connection. Agents are automatically unlinked after a period of inactivity.

> **Note:** Agents must download plugins before they return scan results. This process can take several minutes.

To manage agents, see the following:

- Modify Agent Settings
- Filter Agents

- Export Agents
- Download Linked Agent Logs
- Restart an Agent
- Unlink an Agent
- Delete an Agent

Agent groups

You can use agent groups to organize and manage the agents linked to your scanner. You can add each agent to any number of groups and you can configured scans to use these groups as targets.

> **Note:** Agent group names are case-sensitive. When you link agents using System Center Configuration Manager (SCCM) or the command line, you must use the correct case.

For more information, see Agent Groups.

Agent updates

You can configure the Tenable Agent version that Tenable Nessus Manager offers to its linked Tenable Agents.

For more information, see Agent Updates.

Freeze windows

Freeze windows allow you to schedule times where Tenable Nessus suspends certain activities for all linked agents.

For more information, see Freeze Windows .

Agent clustering

With Tenable Nessus Manager clustering, you can deploy and manage large numbers of agents from a single Tenable Nessus Manager instance.

For more information, see Clustering.

Install Tenable Agents

Before you begin the Tenable Agents installation process, you must retrieve the agent linking key from the Tenable Nessus Manager user interface.

Once you retrieve the linking key, use the procedures described in the *Tenable Agent User Guide* to install the agent and link it to Tenable Nessus Manager.

Once installed and linked, Tenable Agents are linked to Tenable Nessus Manager 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. Linked agents automatically download plugins from the manager upon connection; this process can take several minutes and you must perform it before an agent can return scan results.

Retrieve the Tenable Nessus Linking Key

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

Before you begin the Tenable Agents installation process, you must retrieve the agent linking key from Tenable Nessus Manager.

Note: You can also retrieve your agent linking key from the `nessuscli`. For more information, see `nessuscli fix --secure --get agent_linking_key` in the nessuscli Fix Commands section.

To retrieve the agent linking key:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. (Optional) To modify the **Linking Key**, click the button next to the linking key.

   You may want to modify a linking key if:

   - You regenerated your linking key and want to revert to a previous linking key.
   - You have a mass deployment script where you want to predefine your linking key.

   Note: The linking key must be a 64-character-alphanumeric string.

3. Record or copy the **Linking Key**.

What to do next:

- Install and link Tenable Nessus.

Link an Agent to Tenable Nessus Manager

After you install Tenable Agent, link the agent to Tenable Nessus Manager.

Before you begin:

- Retrieve the linking key from Tenable Nessus Manager.
- Install Tenable Agent.

To link Tenable Agent to Tenable Nessus Manager:

1. Log in to the Tenable Agent from a command terminal.
2. At the agent command prompt, use the command `nessuscli agent link` using the supported arguments.

   For example:

   Linux:

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

   macOS:

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

   Windows:

   ```
   # C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
   --key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
   --name=WindowsAgent --groups=All --host=yourcompany.com --port=8834
   ```

The following table lists the supported arguments for `nessuscli agent link`:

Argument	Required	Value
`--key`	yes	The linking key that you retrieved from the manager.
`--host`	yes	The static IP address or hostname you set during the Tenable Nessus Manager installation.
`--port`	yes	8834 or your custom port.
`--name`	no	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.
`--ca-path`	no	A custom CA certificate to use to validate the manager's server certificate.
`--groups`	no	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. List multiple groups in a comma-separated list. If any group names have spaces, use quotes around the whole list. For example: `--groups="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"`).
`--offline-install`	no	When enabled, the agent periodically attempts to link to Tenable Nessus Manager, even if the agent is not online. 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. If you do not use this flag, the agent immediately attempts to link with Tenable Nessus Manager (the agent only attempts once).

Argument	Required	Value
`--proxy-host`	no	The hostname or IP address of your proxy server.
`--proxy-port`	no	The port number of the proxy server.
`--proxy-password`	no	The password of the user account that you specified as the username.
`--proxy-username`	no	The name of a user account that has permissions to access and use the proxy server.
`--proxy-agent`	no	The user agent name, if your proxy requires a preset user agent.

Modify Agent Settings

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

In Tenable Nessus Manager, you can configure global agent settings to specify agent settings for all your linked agents. You can configure advanced settings for individual agents remotely. You can also set up agent freeze windows and configure the manager's agent update plan.

To modify agent settings in Tenable Nessus Manager:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. Do any of the following:

   - To modify global agent settings:

     a. Click the **Settings** tab.

     b. Modify the settings as described in Global Agent Settings.

     c. Click **Save**.

   - To modify individual agent settings remotely, see Remote Agent Settings.

- To modify your manager's agent update plan, see Configure Agent Update Plan.
- To modify agent freeze window settings, see Modify Global Freeze Window Settings.

Global Agent Settings

The following table describes the global agent settings you can configure in Tenable Nessus Manager:

Option	Description
Manage Agents	
Track unlinked agents	When this setting is enabled, agents that are unlinked without manual intervention (due to an inactivity timeout) are preserved in the manager along with the corresponding agent data. This option can also be set using the `nessuscli` utility. **Note:** This option does not allow the manager to track *deleted* agents. When you delete an agent, the manager and/or cluster no longer tracks or recognizes the agent.
Unlink inactive agents after *X* days	Specifies the number of days an agent can be inactive before the manager unlinks the agent. Inactive agents that were automatically unlinked by Tenable Nessus Manager automatically relink if they come back online. Requires that **Track unlinked agents** is enabled.
Remove agents that have been inactive for *X* days	Specifies the number of days an agent can be inactive before the manager removes the agent.
Remove bad agents	When this setting is enabled, agents with one or more of the following criteria are removed from Tenable Nessus Manager: • The agent was previously deleted or removed by a user.

Option	Description
	• The agent does not provide a valid access token. • The agent was blocklisted. **Note:** This setting only applies to Tenable Nessus environments with clustering enabled.
Freeze Windows	
Configure global freeze windows as described in Modify Freeze Window Settings.	

Remote Agent Settings

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

All agent advanced settings can be set via the agent's command line interface, as described in Advanced Settings in the *Tenable Agent Deployment and User Guide*. However, you can modify some settings remotely via Tenable Nessus Manager.

To modify remote agent settings:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. Do one of the following:

   To modify a single agent:

   a. In the agents table, click the row for the agent you want to configure.

      The agent detail page appears. By default, the **Agent Details** tab is open.

   b. Click the **Remote Settings** tab.

      The **Remote Settings** page appears.

   c. Modify the agent settings:

Setting	Description	Default	Values
Scan Performance	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 in the *Tenable Agent User Guide*.	`high`	`low`, `medium`, or `high`
Plugin Compilation Performance	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	Tenable Agent 10.8.3 and later — `medium` Tenable Agent 10.8.2 and earlier — `high`	`low`, `medium`, or `high`

	medium or high means that plugin compilation completes more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control in the *Tenable Agent User Guide*.		
Nessus Agent Log Level	The logging level of the `backend.log` log file, as indicated by a set of log tags that determine what information to include in the log. If you manually edited `log.json` to set a custom set of log tags for `backend.log`, this setting overwrites that content. For more information, see Manage Logs.	`normal`	• `normal` - Changes the backend.log logging level to `normal` and sets log tags to `"log", "info", "warn", "error", "trace"` • `debug` - Changes the backend.log logging level to `debug` and sets log tags to `"log", "info", "warn",`

			`"error"`, `"trace"`, `"debug"` • `verbose` - Changes the backend.log logging level to `verbose`and sets log tags to `"log"`, `"info"`, `"warn"`, `"error"`, `"trace"`, `"debug"`, `"verbose"`
Maximum Scans Per Day	Specifies the maximum number of scans to run on the agent per day.	10	Integers 1 or more
Automatic Hostname Update	When enabled, when the hostname on the endpoint is modified the new hostname will be updated in the agent's manager. This feature is disabled by default to prevent custom agent names from being overridden.	`no`	`yes` or `no`

To modify multiple agents:

a. Do one of the following:

   - In the agents table, select the check box next to each agent you want to edit.
   - In the table header, select the check box to select the entire page.

b. In the upper-right corner, click the **Manage** button.

   A drop-down menu appears.

c. Click the **Remote Settings** button.

   The **Remote Settings** page appears.

d. Modify the agent settings:

Setting	Description	Default	Values
Scan Performance	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 in the *Tenable Agent User Guide*.	`high`	`low`, `medium`, or `high`

Plugin Compilation Performance	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 consumes more CPU. For more information, see Agent CPU Resource Control in the *Tenable Agent User Guide*.	Tenable Agent 10.8.3 and later — `medium` Tenable Agent 10.8.2 and earlier — `high`	`low`, `medium`, or `high`
Nessus Agent Log Level	The logging level of the `backend.log` log file, as indicated by a set of log tags that determine what information to include in the log. If you manually edited `log.json` to set a custom set of log tags	`normal`	• `normal` - Changes the backend.log logging level to `normal` and sets log tags to `"log", "info", "warn", "error",`

	for `backend.log`, this setting overwrites that content. For more information, see Manage Logs.		`"trace"` • `debug` - Changes the backend.log logging level to `debug` and sets log tags to `"log", "info", "warn", "error", "trace", "debug"` • `verbose` - Changes the backend.log logging level to `verbose`and sets log tags to `"log", "info", "warn", "error", "trace", "debug", "verbose"`
Maximum Scans Per Day	Specifies the maximum number of scans to run on the agent per day.	10	Integers 1 or more

Automatic Hostname Update	When enabled, when the hostname on the endpoint is modified the new hostname will be updated in the agent's manager. This feature is disabled by default to prevent custom agent names from being overridden.	no	yes or no

3. Do one of the following:

   - To save and immediately apply the setting, click **Save and Apply**.

     Note: For some settings, applying the setting requires an agent soft (backend) restart or full service restart.

   - To save the setting but not yet apply settings, click the **Save** button.

     Note: For the setting to take effect on the agent, you must apply the setting. In the banner that appears, click **Apply all changes now**. For some settings, applying the setting requires an agent soft (backend) restart or full service restart.

Agent Updates

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

You can configure the Tenable Agent version that Tenable Nessus Manager offers to its linked Tenable Agents to update to from the **Agent Updates** page.

The **Agent Updates** page also allows you to manually update the offered Tenable Agent version directly from the Tenable Nessus feed and shows what Tenable Agent versions correspond to the **GA**, **Early Access**, and **Stable** update plans, when Tenable Nessus Manager last checked the feed for new available versions, the version that your Tenable Nessus Manager instance currently offers, and the time at which Tenable Nessus Manager last updated its version offering from the feed.

Note: The **Agent Updates** page is not available when Tenable Nessus is managed by Tenable Security Center or Tenable Nessus Manager.

Note: The **Agent Updates** page only affects Tenable Agent version updates, and does not affect plugin updates.

To manage the agent update settings, use the following procedures:

Configure the agent update plan

You can configure the Tenable Agent version that Tenable Nessus Manager offers to its linked Tenable Agents to update to from the **Agent Updates** page.

You can choose from one of the three agent update plans:

Agent Update Plan	Description
GA releases	(Default) Tenable Nessus Manager allows its Tenable Agents to update to the latest generally available (GA) version automatically.
Early Access releases	Tenable Nessus Manager allows its Tenable Agents to update to the latest version automatically when it is released for Early Access (typically a few weeks before GA).
Stable releases	Tenable Agents do not automatically update to the latest version and remain on an earlier version set by Tenable (usually one release older than the current generally available version).

To configure the agent update plan:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Updates**.

   The **Agent Updates** page appears.

3. Under **Agent Update Plan**, select the plan you want to use for updating Tenable Agents.

4. Click **Save**.

   After saving, Tenable recommends updating the Tenable Agent version that Tenable Nessus Manager offers from the Tenable Nessus feed.

Configure the agent version offered by Tenable Nessus Manager

The **Automatic Updates** setting allows Tenable Nessus Manager to automatically update the Tenable Agent version it offers to its linked agents to upgrade to based on the manager's update plan. Alternatively, you can turn off **Automatic Updates** and configure the offered Tenable Agent version manually.

> **Note:** If you want to prevent linked agents from downloading any software updates, you need to create a permanent freeze window in addition to disabling **Automatic Updates**. Disabling **Automatic Updates** only blocks Tenable Nessus Manager from updating the version it offers the linked agents. If Tenable Nessus Manager already downloaded a new agent version to offer the linked agents, the linked agents upgrade or downgrade to that new version. To avoid this, create and enable a permanent freeze window with the **Prevent software updates** setting turned on. For more information, see Create a Freeze Window.

To enable or disable the **Automatic Updates** setting:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Updates**.

   The **Agent Updates** page appears.

3. Under **Automatic Updates**, select or clear the **Enable Agent Updates** check box.

4. Click the **Save** button.

   Tenable Nessus Manager saves the setting.

Sometimes, such as after you configure the agent update plan or after you turn off **Automatic Updates**, you may want to update the Tenable Agent version that Tenable Nessus Manager offers manually.

To update the offered Tenable Agent version manually:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Updates**.

   The **Agent Updates** page appears.

3. In the upper-left corner of the page, click the **Manual Software Updates** button.

   The **Update Provided Agent Version Now** window appears.

   > **Note:** The **Manual Software Update** button updates the offered Tenable Agent version based on the saved agent update plan. For example, if you set the plan to **GA releases**, save, and click the button, your offered Tenable Agent version updates to the latest GA version. The button does not show if you selected **Disable agent version updates**.

4. Click the **Continue** button.

   Tenable Nessus Manager updates the version it offers to Tenable Agents from the Tenable Nessus feed.

Filter Agents

Use this procedure to filter agents in Tenable Nessus Manager.

To filter agents in the agents table:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. Above the agents table, click the **Filter** button.

   The **Filter** window appears.

3. Configure the filters as necessary. For more information, see Agent Filters.

4. Click **Apply**.

   Tenable Nessus Manager filters the list of agents to include only those that match your configured options.

Agent Filters

Parameter	Operator	Expression
IP Address	is equal to is not equal to contains does not contain	In the text box, type the IPv4 or IPv6 addresses on which you want to filter.
Last Connection Last Plugin Update Last Scanned	earlier than later than on not on	In the text box, type the date on which you want to filter.
Member of Group	is equal to is not equal to	From the drop-down list, select from your existing agent groups.
Name	is equal to is not equal to contains does not contain	In the text box, type the agent name on which you want to filter.
Platform	contains does not contain	In the text box, type the platform name on which you want to filter.
Status	is equal to	In the drop-down list, select an agent status. For more

Parameter	Operator	Expression
	is not equal to	information, see Agent Status in the *Tenable Agent Deployment and User Guide*.
Version	is equal to is not equal to contains does not contain	In the text box, type the version you want to filter.

Export Agents

Required user role when using Tenable Nessus Manager: Standard, Administrator, or System Administrator

To export agent data in Tenable Nessus Manager:

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

   The **Linked Agents** page appears.

2. (Optional) Click the **Filter** button to apply a filter to the agents list.

3. In the upper right corner, click **Export**. If a drop-down appears, click **CSV**.

   Your browser's download manager appears.

4. Click **OK** to save the `agents.csv` file.

The `agents.csv` file exported from Tenable Nessus Manager contains the following data:

Field	Description
Agent Name	The name of the agent.
Status	The status of the agent at the time of export. Possible values are `unlinked`, `online`, or `offline`.

IP Address	The IPv4 or IPv6 address of the agent.
Platform	The platform the agent is installed on.
Groups	The names of any groups the agent belongs to.
Version	The version of the agent.
Last Plugin Update	The date (in ISO-8601 format) the agent's plugin set was last updated.
Last Scanned	The date (in ISO-8601 format) the agent last performed a scan of the host.

Download Linked Agent Logs

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

As an administrator in Tenable Nessus Manager, you can request and download a log file containing logs and system configuration data from any of your managed scanners and agents. This information can help you troubleshoot system problems, and also provides an easy way to gather data to submit to Tenable Support.

You can store a maximum of five log files from each agent in Tenable Nessus Manager. Once the limit is reached, you must remove an old log file to download a new one.

To download logs from a linked agent:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the agents table, click the agent for which you want to download logs.

   The **Agents** page for that agent appears.

3. Click the **Logs** tab.

4. In the upper-right corner, click **Request Logs**.

> **Note:** If you have reached the maximum of five log files, the **Request Logs** button is disabled. Remove an existing log before downloading a new one.

Tenable Nessus Manager requests the logs from the agent the next time it checks in, which may take several minutes. You can view the status of the request in the user interface until the download is complete.

5. To download the log file, click the file name.

   Your system downloads the log file.

To remove an existing log:

- In the row of the log you want to remove, click the 🗑 button.

To cancel a pending or failed log download:

- In the row of the pending or failed log download that you want to cancel, click the ⊘ button.

Restart an Agent

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

In Tenable Nessus, you can restart linked agents on the **Linked Agents** page.

To restart an agent:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. Do one of the following:

   To restart a single agent:

   a. In the agents table, click the row for the agent you want to configure.

      The agent detail page appears. By default, the **Agent Details** tab is open.

   b. Click the **Remote Settings** tab.

The **Remote Settings** page appears.

c. In the upper-right corner, click the **Restart Agent** button.

The **Restart Agent** window appears.

To restart multiple agents:

a. Do one of the following:

- In the agents table, select the check box next to each agent you want to restart.
- In the table header, select the check box to select all the agents listed on the page.

b. In the upper-right corner, click the **Manage** button.

A drop-down menu appears.

c. Click the **Restart** button.

The **Restart Agent** window appears.

> **Note:** The **Restart** button does not show in the drop-down menu if none of agents you selected are online.

3. In the drop-down menu, select the restart type you want the agent to perform:

- **Soft restart the agent service (No service restart)** — This restart occurs the next time the agent checks in to Tenable Nessus Manager.
- **Restart the agent service when the agent is idle** — This restart occurs the next time the agent checks in to Tenable Nessus Manager.
- **Immediately restart the agent service (Stops all running scans)** — This restart occurs immediately.

4. Click the **Restart** button.

The window closes, and a message appears confirming your selected restart type.

Unlink an Agent

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

When you unlink an agent manually, the agent disappears from the Tenable Nessus **Agents** page, but the system retains related data for the period of time specified in agent settings. When you unlink an agent manually, the agent does *not* automatically relink to Tenable Nessus Manager.

> **Tip**: You can configure agents to unlink automatically if they are inactive for some days, as described in agent settings.

To unlink agents in Tenable Nessus Manager manually:

Run the `# nessuscli agent unlink` command or use the following steps to unlink the agents in Tenable Nessus.

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

   The **My Scans** page appears.

2. In the left navigation bar, click **Agents**.

   The **Agents** page appears.

3. Do one of the following:

   To unlink a single agent:

   a. In the agents table, in the row for the agent that you want to unlink, click the button.

      A confirmation window appears.

   To unlink one agent or multiple agents:

   a. In the agents table, select the check box in each row for each agent you want to unlink.

   b. In the upper-right corner, click the **Manage** button.

      A drop down menu appears.

   c. Click the **Unlink** button.

      A confirmation window appears.

      > **Note:** The **Unlink** button does not show in the drop down menu if none of the agents you selected are linked.

4. Click the **Unlink** button.

   Tenable Nessus Manager unlinks the agent or agents.

Delete an Agent

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

Tenable Nessus Manager allows you to delete your linked agents from the **Linked Agents** page.

To delete agents from Tenable Nessus Manager:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. Do one of the following:

   To delete a single agent:

   a. In the row of the agent you want to delete, click the ✕ button.

      A confirmation window appears.

   To delete multiple agents:

   a. Select the check boxes of the agents that you want to delete.

   b. In the upper-right corner, click the **Manage** button.

      A drop-down menu appears.

   c. Click the **Delete** button.

      A confirmation window appears.

3. Click the **Delete** button.

   Tenable Nessus Manager deletes the agent or agents.

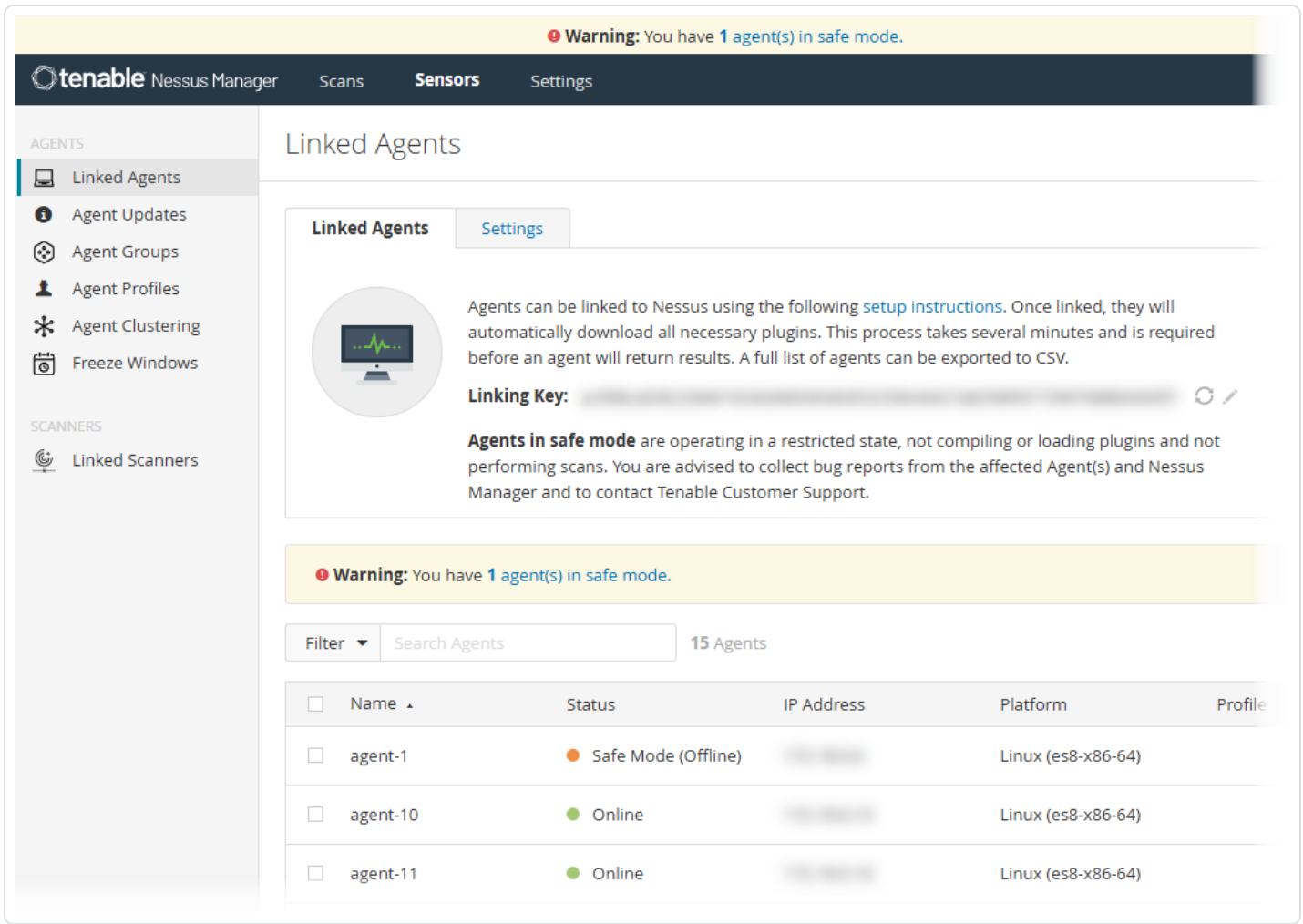
Agent Safe Mode

When Tenable Agent experiences an internal error that it cannot recover from, the agent automatically enters safe mode. While the agent is in safe mode, it does not compile plugins or run scans, but it maintains connection with its Tenable agent management platform, such as Tenable Vulnerability Management or Tenable Nessus Manager. Safe mode maximizes the likelihood that the agent stays connected to its manager and allows your organization or Tenable to execute remote agent commands to correct the error and return the agent to normal operations.

For a deeper explanation of agent safe mode, see Safe Mode in the *Tenable Agent User Guide*.

> **Note:** Agents on an earlier version than 10.9.0 do not have safe mode capabilities.

When a linked agent enters safe mode, Tenable Nessus Manager notifies you with a warning banner at the top of the application and on the **Linked Agents** page, and each agent in safe mode is marked with **Safe Mode (Offline)** status in the agents table.



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 at least 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.

Report agents that are in safe mode

1. Generate a debug file for at least one of the agents that are in safe mode by running the following command:

   ```
   # nessuscli bug-report-generator
   ```

   For more information about `bug-report-generator`, see Nessuscli Agent.

2. Go to connect.tenable.com and open a ticket. Be sure to include the collected debug information.

   Await instruction from Tenable Support.

Self-remediate agents that are in safe mode

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.

1. Go to **Sensors** > **Linked Agents**.

2. Attempt to remediate the issue using one of the following methods: restarting the agent, rebuilding or resetting the agent plugins, or upgrading/downgrading the agent version.

   Generally, the agent re-enters safe mode within 90 minutes of restarting the agent if the issue is not solved. If your remediation action fixed the issue, the agent exits safe mode and remains out of safe mode. If you cannot remediate the issue, follow the *Report agents that are in safe mode* steps.

Restart the agents

Restarting the agent can remediate the issue if a previously undiscovered bug caused the agent to enter safe mode. You can restart an agent by simply exiting safe mode in the **Linked Agents** menu.

To restart the agent:

a. In the **Linked Agents** table, select the checkbox of each agent you want to restart.

b. Click **Manage** in the upper-right corner.

   A drop-down menu appears.

c. Click **Exit Safe Mode**.

   The **Exit Safe Mode** window appears.

d. Click **Exit Safe Mode**.

   The agent or agents restart and exit safe mode the next time they check in with Tenable Nessus Manager, which may be up to 30 minutes after clicking **Confirm**.

Rebuild or reset the agent plugins

Rebuild or resetting the agent's plugins can remediate the issue if the agent enters safe mode after a plugin update.

Rebuilding agent plugins instructs the agent to locally rebuild its current plugin set. Resetting the agent plugins instructs the agent to download the latest plugins from Tenable Nessus Manager and build them. Therefore, the plugin reset process may not complete until up to 12 hours later (the next time the agents connect with Tenable Nessus Manager).

Once either process completes, the agent restarts and exits safe mode.

Generally, Tenable recommends attempting to rebuild agent plugins before attempting to reset agent plugins. This is because rebuilding plugins has a much smaller impact on network traffic.

> **Note:** If you rebuild plugins on many agents in a shared host environment, you may notice a CPU usage spike in that environment. If you reset plugins on many agents, you may notice a significant CPU usage spike.

To rebuild or reset the agent plugins:

a. In the **Linked Agents** table, select the checkbox of each agent you want to restart.

b. Click **Manage** in the upper-right corner.

   A drop-down menu appears.

c. Depending on the action you want to perform, click **Rebuild Plugins** or **Reset Plugins**.

   A confirmation window appears.

d. Click **Confirm**.

   The agent or agents perform a plugin rebuild or plugin reset the next time they check in with Tenable Nessus Manager, which may be up to 30 minutes after clicking **Confirm**.

Upgrade or downgrade the agent version

Upgrading or downgrading the agent can remediate the issue if a software version update caused the agent to enter safe mode. Once the upgrade or downgrade process is complete, the agent restarts and exits safe mode.

If you choose to upgrade or downgrade agents, the process may not complete until up to 12 hours later (the next time the agents connect with Tenable Nessus Manager).

Agent Profiles

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

In Tenable Nessus Manager, you can create agent profiles to customize and manage the behavior of your linked agents. An agent profile allows you to configure a range of settings for a specific group of agents.

You can use a profile to:

- Assign a specific agent version for testing or standardization purposes.
- Limit the amount of host CPU processing that agents can use.

By assigning agents to different profiles, you can apply distinct configurations to various segments of your environment, which provides granular control over agent operations.

There are two types of agent profile:

- **Default** — The profile to which an agent or agent group belongs to unless you assign it to a custom profile. You cannot copy, delete, or edit the name and description of the **Default** profile.
- Custom profiles — A custom profile that you create. Custom profiles allow you to associate and configure different agents and agent groups based on your business needs.

Note: You can only assign an agent to one profile.

Note: The agent profile version overrides the agent's update plan setting. If you assign the agent a freeze window, the freeze window overrides both the agent update plan and the agent profile. In this case, the agent remains on its current version and no software updates occur for that agent as long as the agent is assigned to the freeze window.

To manage agent profiles:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Profiles**.

   The **Agent Profiles** page appears.

Use the following procedures to manage your agent profiles:

Create an agent profile

Note: You cannot create an agent profile for an end-of-life (EOL) Tenable Agent version.

To create an agent profile:

1. On the **Agent Profiles** page, click ⊕ **Add Agent Profile**.

   The **New Agent Profile** page appears.

2. Enter a **Name** for the agent profile.

3. Select the agent profile's **Version**. This is the version that agents assigned to the profile are upgraded or downgraded to. The default value is the oldest version available in the drop-down menu.

You can set the agent profile to stay on the latest major version release (for example, 10.x) or the latest minor version release (for example, 10.4.x), or you can set the agent profile to a specific patch release (for example, 10.4.1). If you do not configure a **Version**, the agents assigned to the profile follow the configured agent update plan.

> **Note:** Before a version can be applied to agents, the version package must be present in Tenable Nessus Manager's `remote/agent_versions` directory, which can be found in the following parent directories:
>
> - Linux — `/opt/nessus/var/nessus`
> - Windows — `C:\ProgramData\Tenable\Nessus\nessus`
> - macOS — `/Library/Nessus/run/var/nessus`
>
> You can download missing version packages by enabling the **Enable Agent Updates** setting or performing a manual software update.

4. (Optional) For **CPU Limit %**, enter an integer from 1 to 100 to set the maximum percentage of the host's CPU that the agent can use.

   > **Note:** This setting only affects agents on version 11.1.0 or later.

5. (Optional) Enter a **Description** for the agent profile.

6. Click **Add**. Tenable Nessus Manager adds the new profile to the **Agent Profiles** page.

   > **Note:** Unless you perform a manual software update, Tenable Nessus Manager does not download the packages for agents added to an agent profile until the next update interval. In turn, agents will not receive and apply those packages until their next update interval, which is every 24 hours by default. Therefore, it may take up to 48 hours to complete an agent profile version change.
   >
   > You can run the `nessuscli fix --set auto_update_delay=1` command on Tenable Nessus Manager and a pilot group of agents to reduce the update interval to one hour, after which it may take up to two hours to complete an agent profile version change, providing there are no environmental issues.

Add or remove an agent from agent profiles

Use the following procedures to add an agent to an agent profile or remove an agent from an agent profile in Tenable Nessus Manager.

In addition to using the Tenable Nessus Manager user interface, you can link an agent to a profile by running the `nessuscli agent link` command and specifying the optional `--profile-uuid` argument. You can link an agent to a profile during deployment by specifying the `profile-uuid` in the *config.json file*. To find a profile's `profile-uuid`, see View an agent profile ID.

Note: The agent profile version overrides the agent's update plan setting. If you assign the agent a freeze window, the freeze window overrides both the agent update plan and the agent profile. In this case, the agent remains on its current version and no software updates occur for that agent as long as the agent is assigned to the freeze window.

Apply an agent profile to an agent

To apply an agent profile to an agent in the **Linked Agents** user interface:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. Click the row of the agent that you want to assign to the profile.

   The **Agent Details** page appears.

3. Next to **Profile**, click ⊕.

   The **Add to Profile** window appears.

4. In the table, select the check box of the agent profile that you want to assign the agent to.

5. Click **Apply**.

   Tenable Nessus Manager assigns the agent to the agent profile.

To apply an agent profile to an agent in the **Agent Profiles** user interface:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Profiles**.

   The **Agent Profiles** page appears.

3. Click the agent profile to manage.

   The agent profile details page appears.

4. Click the **Agents** tab.

5. In the upper-right corner, click ⊕ **Add Agents**.

   The **Add Agents** window appears.

6. Do one of the following:

   - In the agents table, select the check box next to each agent you want to add to the profile.
   - In the table header, select the check box to select all agents.

7. Click **Add**. Tenable Nessus Manager adds the agent or agents to the profile.

Remove an agent profile from an agent

To remove an agent profile from an agent in the **Linked Agents** user interface:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. Click the row of the agent that you want to remove a profile from.

   The **Agent Details** page appears.

3. Next to **Profile**, click ✕ on the profile you want to remove from the agent.

   The **Remove Profile** window appears.

4. Click **Remove** to confirm.

   Tenable Nessus Manager removes the profile from the agent.

To remove an agent profile from an agent in the **Agent Profiles** user interface:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Profiles**.

   The **Agent Profiles** page appears.

3. Click the agent profile to manage.

   The agent profile details page appears.

4. Open the **Agents** tab.

5. Select the checkbox or checkboxes of the agent or agents that you want to remove the profile from.

6. In the upper-right corner, click the **Remove** button.

   The **Remove Agent** window appears.

7. Click **Remove**.

   The agent profile is removed from the agent or agents.

View an agent profile ID

You can link an agent to a profile by running the `nessuscli agent link` command and specifying the optional `--profile-uuid` argument. You can also link an agent to a profile during deployment by specifying the `profile-uuid` in the *config.json file*. Use the following procedure to view a profile's `--profile-uuid`.

To view an agent profile ID:

1. On the **Profiles** page, click the agent profile that you want to view the ID of.

   The agent profile details page appears.

2. In the **Profile Details** tab, the `--profile-uuid` is listed as **UUID**.

Edit an agent profile

To edit an agent profile:

1. On the **Agent Profiles** page, click ✎ in the row of the profile that you want to edit.

   The **Edit Agent Profile** window appears.

2. Edit the agent profile name, version, agent CPU limit, and description as needed.

   > **Note:** Before a version can be applied to agents, the version package must be present in Tenable Nessus Manager's `remote/agent_versions` directory, which can be found in the following parent directories:
   >
   > - Linux — `/opt/nessus/var/nessus`
   > - Windows — `C:\ProgramData\Tenable\Nessus\nessus`
   > - macOS — `/Library/Nessus/run/var/nessus`
   >
   > You can download missing version packages by enabling the **Enable Agent Updates** setting or performing a manual software update.

3. Click **Save**.

   Tenable Nessus Manager saves your changes.

   > **Note:** Unless you perform a manual software update, Tenable Nessus Manager does not download the packages for agents added to an agent profile until the next update interval. In turn, agents will not receive and apply those packages until their next update interval, which is every 24 hours by default. Therefore, it may take up to 48 hours to complete an agent profile version change.
   >
   > You can run the `nessuscli fix --set auto_update_delay=1` command on Tenable Nessus Manager and a pilot group of agents to reduce the update interval to one hour, after which it may take up to two hours to complete an agent profile version change, providing there are no environmental issues.

Delete an agent profile

Delete an agent profile if you no longer need the agent profile. You cannot undo an agent profile deletion.

To delete an agent profile:

1. On the **Agent Profiles** page, click ✕ in the row of the profile that you want to delete.

   The **Delete Agent Profile** window appears.

2. Click **Delete** to confirm the deletion.

   Tenable Nessus Manager deletes the agent profile and removes all the linked agents from the profile.

Manage agent profiles in offline mode

Use the following process to add a new agent profile **Version** option while Tenable Nessus Manager is in offline mode.

1. Download the `nessus-agent-updates-<agent version>.tar.gz` file from the Tenable Agent Downloads page.

2. In the nessuscli tool, run the following command to upload the tar.gz file to Tenable Nessus Manager:

   ```
   nessuscli update <tar.gz filename> --agent-version
   ```

   The tar.gz file uploads to Tenable Nessus Manager.

   Once Tenable Nessus Manager downloads the file, the new agent version is available to choose in the **Version** dropdown when creating or updating an agent version. For example, if you uploaded `nessus-agent-updates-10.9.1.tar.gz`, you can now set your agent profile versions to 10.9.1.

Agent Groups

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

You can use agent groups to organize and manage the agents linked to Tenable Nessus Manager. You can add an agent to more than one group, and configure scans to use these groups as targets. This will happen.

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

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 you must import into Tenable Security Center. The `.nessus` file size affects hard drive space and bandwidth.

Use the following processes to create and manage agent groups:

Create an agent group

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. Select the check boxes of the agents that you want to add to the new agent group.

3. In the upper-right corner, click the **Manage** button.

   A drop-down menu appears.

4. In the drop-down menu, click **New Group**.

   The **New Agent Group** window appears.

5. Enter a name for the new agent group.

6. Click **Add**.

   Tenable Nessus Manager creates the new agent group and adds the agents you selected to the new group.

Add agents to an agent group

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. Select the check boxes of the agents that you want to add to the agent group.

3. In the upper-right corner, click the **Manage** button.

   A drop-down menu appears.

4. In the drop down menu, click **Add to Group(s)**.

   The **Add to Group(s)** window appears.

5. In the window, select the groups you want to add the agents to.

6. Click **Add**.

   Tenable Nessus Manager adds the selected agents to the agent group or groups.

Modify an agent group

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Groups**.

   The **Agent Groups** page appears.

3. Do any of the following:

   - Modify the group name

     a. In the row for the agent group that you want to modify, click the button.

        The **Edit Agent Group** window appears.

     b. In the **Name** box, type a new name for the agent group.

     c. Click **Save**.

        The manager saves your changes.

   - Add agents to the agent group

     a. In the agent groups table, click the agent group you want to modify.

        The agent group details page appears.

b. In the upper-right corner of the page, click the **Add Agents** button.

   The **Add Agents** window appears. This window contains a table of available agents.

c. (Optional) In the **Search** box, type the name of an agent, then click **Enter**.

   The table of agents refreshes to display the agents that match your search criteria.

d. Click the check box next to each agent you want to add to the group.

e. Click **Add**.

   The manager adds the selected agent or agents to the group.

- Remove agents from the agent group

  a. In the agent groups table, click the agent group you want to modify.

     The agent group details page appears. By default, the **Group Details** tab is active.

  b. (Optional) Filter the agent groups in the table.

  c. (Optional) Search for an agent by name.

  d. Select the agent or agents you want to remove:

     - For an individual agent, click the ✕ button next to the agent.
     - For multiple agents, select the check box next to each, then click the **Remove** button in the upper-right corner of the page.

     A confirmation window appears.

  e. In the confirmation window, confirm the removal.

- Modify the user permissions for the agent group

  1. In the agent groups table, click the agent group for which you want to configure permissions.

     The agent group details page appears.

2. Click the **Permissions** tab.

   The **Permissions** tab appears.

3. Do any of the following:

   > **Tip**: Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

   - Add permissions for a new user or user group:

     a. In the **Add users or groups** box, type the name of a user or group.

        As you type, a filtered list of users and groups appears.

     b. Select a user or group from the search results.

        Tenable Vulnerability Management adds the user to the permissions list, with a default permission of **Can Use**.

   - Change the permissions for an existing user or user group:

     > **Note:** The **Default** user represents any users who have not been specifically added to the agent group.

     a. Next to the permission drop-down for the **Default** user, click the ▼ button.

     b. Select a permissions level.

     c. Click **Save**.

   - Remove permissions for a user or user group:

     - For the **Default** user, set the permissions to **No Access**.
     - For any other user or user group, click the ✕ button next to the user or user group for which you want to remove permissions.

4. Click **Save**.

Tenable Vulnerability Management saves the changes you made to the agent group.

Delete an agent group

1. In the row for the agent group that you want to delete, click the ✕ button.

   A confirmation window appears.

2. To confirm, click **Delete**.

   The manager deletes the agent group.

Freeze Windows

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

Freeze windows allow you to schedule times when Tenable Nessus Manager suspends certain agent activities for all linked agents. This activity includes:

- Receiving and applying software updates
- Receiving plugin updates
- Installing or executing agent scans (this does not include triggered agent scans)

To manage freeze windows, use the following procedures:

Create a freeze window

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Freeze Windows**.

   The **Freeze Windows** page appears.

3. In the upper-right corner, click the **New Window** button.

   The **New Freeze Window** page appears.

4. Configure the freeze window options as necessary:

Option	Description
Name	The name of the freeze window.
Enabled	Indicates whether the freeze window is enabled. • If the switch is turned on, the freeze window is enabled and any agents assigned to the freeze window are blocked from certain activities based on its schedule. • If the switch is turned off, the freeze window is disabled and any agents assigned to the freeze window ignore its schedule.
Frequency	Indicates how often the freeze window occurs. The possible values are: • Once • Daily • Weekly • Monthly • Yearly
Window	Determines the start and end time of the freeze window using the 24-hour format. You can specify the time window in 30-minute intervals (for example, 9:00 to 17:30).
Effective	Determines the date range during which the freeze window is effective (for example, 2025-06-01 to 2025-07-01). After the **Effective** date range expires, agents stop following the freeze window schedule.
Timezone	The timezone of the **Window** range.

A summary of the freeze window schedule appears next to **Summary**.

5. Click **Save**.

   The freeze window goes into effect and appears on the **Freeze Windows** tab.

Modify a freeze window

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Freeze Windows**.

   The **Freeze Windows** page appears.

3. In the freeze windows table, click the freeze window you want to modify.

   The freeze window details page appears.

4. Modify the options as necessary:

Option	Description
Name	The name of the freeze window.
Enabled	Indicates whether the freeze window is enabled. • If the switch is turned on, the freeze window is enabled and any agents assigned to the freeze window are blocked from certain activities based on its schedule. • If the switch is turned off, the freeze window is disabled and any agents assigned to the freeze window ignore its schedule.
Frequency	Indicates how often the freeze window occurs. The possible values are: • Once • Daily • Weekly • Monthly • Yearly
Window	Determines the start and end time of the freeze window using the 24-hour format. You can specify the time window in 30-minute intervals (for example, 9:00 to 17:30).

Effective	Determines the date range during which the freeze window is effective (for example, 2025-06-01 to 2025-07-01). After the **Effective** date range expires, agents stop following the freeze window schedule.
Timezone	The timezone of the **Window** range.

A summary of the freeze window schedule appears next to **Summary**.

5. Click **Save** to save your changes.

Delete a freeze window

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Freeze Windows**.

   The **Freeze Windows** page appears.

3. In the freeze window table, in the row for the freeze window that you want to delete, click the ✕ button.

   A dialog box appears, confirming your selection to delete the freeze window.

4. Click **Delete** to confirm the deletion.

   Tenable Nessus Manager deletes the freeze window.

Modify global freeze window settings

In Tenable Nessus Manager, you can configure a permanent freeze window and global settings for how freeze windows work on linked agents.

To modify global freeze window settings:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Freeze Windows**.

The **Freeze Windows** page appears.

3. Click the **Settings** tab.
4. Modify any of the following settings:

Freeze Windows	
Enforce a permanent freeze window schedule	When enabled, Tenable Nessus Manager creates a permanent freeze window that prevents agents from updating software. The permanent freeze window takes effect immediately after you save the settings (step 5), and it overrides any other existing freeze windows. **Note:** Disabling this setting is the only way to end the permanent freeze window. The following freeze window settings also apply during the permanent freeze window.
Prevent software updates	When enabled, agents do not receive software updates during scheduled freeze windows.
Prevent plugin updates	When enabled, agents do not receive plugin updates during scheduled freeze windows.
Prevent agent scans	When enabled, the system does not run agent scans during scheduled freeze windows.

5. Click **Save**.

   Tenable Nessus Manager saves your changes.

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.

Definitions

Parent node — The Tenable Nessus Manager instance with clustering enabled, which child nodes link to.

Child node — A Tenable Nessus instance that acts as a node that Tenable Agents connect to.

Tenable Nessus Manager cluster — A parent node, its child nodes, and associated agents.

For more information, see the following topics:

- Clustering System Requirements
- Enable Clustering
- Get Linking Key from Node
- Link a Node
- Migrate Agents to a Cluster
- Link Agents to a Cluster
- Enable or Disable a Node
- Rebalance Nodes
- View or Edit a Node
- Delete a Node
- Cluster Groups

Clustering System Requirements

The following are system requirements for the parent node and child nodes. These estimations assume that the KB and audit trail settings are disabled. If those settings are enabled, the size required can significantly increase. In these cases, Tenable recommends increasing the standard system requirements by at least 50%.

Note: All Tenable Nessus nodes in a cluster must be on the same Tenable Nessus version. Otherwise, the cluster deployment is unsupported.

Note: If you notice slow performance in your clustering environments, Tenable highly recommends reviewing Hardware Requirements and ensuring that your parent and child node configurations are properly configured.

Caution: Tenable highly recommends not using shared resources in Tenable Nessus clustering environments. Doing so can cause significant performance issues.

Parent Node (Tenable Nessus Manager with Clustering Enabled)

Tenable supports connecting up to 20,000 agents per one Tenable Nessus Manager child node.

Note: The amount of disk space needed depends on how many agent scan results you keep and for how long. For example, if you run a single 5,000 agent scan result once per day and keep scan results for seven days, the estimated disk space used is 35 GB. The disk space required per scan result varies based on the consistency, number, and types of vulnerabilities detected.

- **CPU** — 8 core minimum for all implementations, with an additional 8 cores for every three child nodes
- **RAM** — 16 GB minimum for all implementations, with an additional 4 GB for every additional child node
- **Disk**
  - 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) **+** 500 MB

    For example, if a standalone Tenable Nessus Manager is scanning daily with 100 agents, the disk space requirement is 5 MB x 100 agents x 7 scans over seven days + 500 MB = **4,000 MB** (**4 GB**).
  - Environments without triggered agent scanning — 5 GB per 5,000 agents per scan per day

Note: The parent node must have the cumulative amount of disk space used for all child nodes. For example, if the parent node has three child nodes that need 1 GB of disk space each, the parent node requires 3 GB of disk space in addition to its own disk space requirement.

Child Node (Tenable Nessus Scanner Managed by Tenable Nessus Manager Parent Node)

Note: Disk space is used to store agent scan results temporarily, both individual and combined, before uploading the results to the parent node.

Child node with 0-10,000 agents:

- **CPU** — 4 cores
- **RAM** — 16 GB

- **Disk**
    - 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) **+** 500 MB

      For example, if a standalone Tenable Nessus Manager is scanning daily with 100 agents, the disk space requirement is 5 MB x 100 agents x 7 scans over seven days + 500 MB = **4,000 MB** (**4 GB**).
    - Environments without triggered agent scanning — 5 GB per 5,000 agents per concurrent scan

Child node with 10,000-20,000 agents:

A child node can support a maximum of 20,000 agents.

- **CPU** — 8 cores
- **RAM** — 32 GB
- **Disk**
    - 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) **+** 500 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 agents x 7 scans over seven days + 500 MB = **39,000 MB** (**39 GB**).
    - Environments without triggered agent scanning — 5 GB per 5,000 agents per concurrent scan

Agents

Linked agents must be on a supported Tenable Agent version.

Enable Clustering

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

When you enable clustering on Tenable Nessus Manager it becomes a *parent node*. You can then link *child nodes*, each of which manages Tenable Agents. Once you enable clustering on a parent node, you cannot undo the action and turn Tenable Nessus Manager into a regular scanner or Tenable Agent manager.

Note: To enable Tenable Nessus Manager clustering in Tenable Nessus 8.5.x or 8.6.x, you must contact your Tenable representative. In Tenable Nessus Manager 8.7.x and later, you can enable clustering using the following procedure.

Note: All Tenable Nessus nodes in a cluster must be on the same version. Otherwise, the cluster deployment is unsupported.

To enable clustering in Tenable Nessus Manager:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Setup** page appears and displays the **Settings** tab.

3. Select **Enable Cluster**.

   Caution: Once you enable clustering on a parent node, you cannot undo the action and turn Tenable Nessus Manager into a regular scanner or Tenable Agent manager.

4. Click **Save**.

   Your Tenable Nessus Manager becomes a parent node of a cluster.

What to do next:

- Link child nodes to the parent node.
- Manage cluster groups.

Migrate Agents to a Cluster

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

If you have a non-clustered instance of Tenable Nessus Manager with linked agents, you can migrate the linked agents to an existing cluster. After the agents successfully migrate to the cluster, the agents are then unlinked from their original Tenable Nessus Manager. Any agents that did not successfully migrate remain linked to the original Tenable Nessus Manager. The original Tenable Nessus Manager remains as a Tenable Nessus Manager instance and does not become part of the cluster.

Before you begin

- Ensure there is a functional cluster available for the agents to migrate to. The cluster should meet the Tenable Nessus Clustering System Requirements. If you do not have a functional cluster, enable clustering on the Tenable Nessus Manager instance you want to act as the parent node for the cluster.
- Get the linking key from the **Linked Agents** page of the Tenable Nessus Manager parent node for the cluster you want the agents to migrate to.

To migrate agents to a cluster:

1. Access a non-clustered instance of Tenable Nessus Manager with linked agents.
2. In the top navigation bar, click **Sensors**.

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.
3. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Setup** page appears and displays the **Settings** tab.
4. Click the **Cluster Migration** tab.
5. Complete the **Cluster Information**:
   - **Parent Node Hostname** — Type the hostname or IP address of the Tenable Nessus Manager parent node of the cluster to which you are migrating.
   - **Parent Node Port** — Type the port for the specified parent node host. The default is 8834.
   - **Parent Node Linking Key** — Paste or type the linking key that you copied from the Tenable Nessus Manager parent node, as described in Get Linking Key from Node.

- **Enable Agent Migration** — Select this checkbox to migrate agents to the cluster. Disable the checkbox to stop migrating agents, if agents are currently in the process of migrating.

6. Click **Save**.

   Tenable Nessus Manager begins or stops migrating agents to the cluster, depending on whether you have selected **Enable Agent Migration**.

What to do next:

Log in to the Tenable Nessus Manager parent node to manage linked Tenable Agents.

Link Agents to a Cluster

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

Depending on your cluster group configuration, you can link an agent to a parent node or a child node. Usually, Tenable recommends linking to a parent node. However, linking to a child node may be helpful if you have geographically distributed cluster groups and want to ensure that an agent is linked to a particular cluster group.

For general information about clusters, see Clustering.

Before you begin:

- Get Linking Key from Node. You need the node's linking key for the agent link command's **--key** argument.

To link an agent to a parent node:

In this scenario, the agent links to the cluster's parent node, receives a list of child nodes, and attempts to connect to a child node within the cluster.

1. Log in to the Tenable Agent from the command terminal.
2. At the agent command prompt, use the command `nessuscli agent link` with the supported arguments to link to the parent node.

   For example:

Linux:

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

macOS:

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

Windows:

```
# C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=WindowsAgent --groups=All --host=yourcompany.com --port=8834
```

To view a list of the supported agent-linking arguments, see Nessus CLI Agent Commands

To link an agent to a child node:

In this scenario, the agent links to a child node in a specific cluster group and receives a list of all the child nodes within that cluster group. The agent then attempts to connect to a child node within the cluster group.

1. Log in to the Tenable Agent from the command terminal.
2. At the agent command prompt, use the command `nessuscli agent link` with the supported arguments to link to the child node.

   For example:

   Linux:

   ```
   /opt/nessus_agent/sbin/nessuscli agent link
   ```

```
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=LinuxAgent --groups=All --host=yourcompany.com --port=8834
```

macOS:

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

Windows:

```
# C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name=WindowsAgent --groups=All --host=yourcompany.com --port=8834
```

To view a list of the supported agent-linking arguments, see Nessus CLI Agent Commands

Upgrade a Cluster

Required user role when using Tenable Nessus Manager: System Administrator

If your cluster is not configured to update automatically and you need to update it to a new Tenable Nessus version, use the following steps to update the cluster parent node and child nodes manually. When you update cluster node versions manually, it is important to stop, update, and start the nodes in the documented order. Doing so ensures that, as long as the child nodes are running, they have access to the parent node and can continue to deliver scan results and other data.

To configure a cluster to update automatically, configure the **Nessus Update Plan** of each node as described in Update Tenable Nessus Software.

To learn more about clustering in Tenable Nessus, see Clustering and Clustering System Requirements.

To update a Tenable Nessus cluster manually:

1. Stop Tenable Nessus on the child nodes.
2. Stop Tenable Nessus on the parent node.
3. Update the parent node to desired version.
4. Update the child nodes to desired version.
5. Start Tenable Nessus on the parent node.
6. Start Tenable Nessus on the child nodes.

   Once you start all the nodes using the new version, the upgrade process is complete.

Manage Nodes

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

To manage cluster nodes, see the following topics:

- Get Linking Key from Node
- Link a Node
- View or Edit a Node
- Enable or Disable a Node
- Rebalance Nodes
- View or Edit a Node
- Delete a Node

To manage cluster groups, see Cluster Groups .

Get Linking Key from Node

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

You need the linking key from the cluster parent node to link child nodes or migrate agents to the cluster. Similarly, you need the linking key from the cluster child node to link an agent to the child node directly.

Note: You can also retrieve your child node linking key from the `nessuscli`. For more information, see `nessuscli fix --secure --get child_node_linking_key` in the nessuscli Fix Commands section.

Before you begin:

- Enable Clustering on the node that you want to link to.

To get the linking key from the node:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.

3. Copy or make note of the **Linking Key**.

What to do next:

- Link a child node to the cluster.
- Link new agents to the cluster.
- Migrate existing agents to the cluster.

Link a Node

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

To link a child node to a cluster, you install an instance of Tenable Nessus as a cluster child node, then configure the node to link to the parent node of the cluster.

Note: Before you begin, you must get the linking key from the cluster parent node. This is because you have to complete the Link the child node to the parent node process in one session. Starting the process and then navigating away from the user interface before completing the process can disable the child node user interface prematurely.

To install and configure Tenable Nessus as a child node:

1. Install Tenable Nessus as described in the appropriate Install Tenable Nessus procedure for your operating system.
2. On the **Welcome to Nessus**, select **Link Nessus to another Tenable product**.
3. Click **Continue**.

   The **Managed Scanner** screen appears.
4. From the **Managed by** drop-down box, select **Nessus Manager (Cluster Node)**.
5. Click **Continue**.

   The **Create a user account** screen appears.
6. Create a Tenable Nessus administrator user account, which you use to log in to Tenable Nessus:

   a. In the **Username** box, enter a username.

   b. In the **Password** box, enter a password for the user account.
7. Click **Submit**.

   Tenable Nessus finishes the configuration process, which may take several minutes.

To link the child node to the parent node:

1. In the Tenable Nessus child node, use the administrator user account you created during initial configuration to sign in to Tenable Nessus.

   The **Agents** page appears. By default, the **Node Settings** tab is open.
2. Enable the toggle to **On**.
3. Configure the **General Settings**:

   - **Node Name** — Type a unique name that identifies this Tenable Nessus child node on the parent node.
   - (Optional) **Node Host** — Type the hostname or IP address that Tenable Agents should use to access the child node. If you do not provide a host node, Tenable Agent uses the system hostname. If Tenable Agent cannot detect the hostname, the link fails.
   - (Optional) **Node Port** — Type the port for the specified host.

4. Configure the **Cluster Settings**:

    - **Cluster Linking Key** — Paste or type the linking key that you copied from the Tenable Nessus Manager parent node.
    - **Parent Node Host** — Type the hostname or IP address of the Tenable Nessus Manager parent node to which you are linking.
    - **Parent Node Port** — Type the port for the specified host. The default is 8834.
    - (Optional) **Use Proxy** — Select the checkbox if you want to connect to the parent node via the proxy settings set in Proxy Server.

5. Click **Save**.

    A confirmation window appears.

6. To confirm linking the node to the parent node, click **Continue**.

    The Tenable Nessus child node links to the parent node. Tenable Nessus logs you out of the user interface and disables the user interface.

    > **Note:** Once you disable the child node user interface, subsequent attempts to access the child node user interface result in the following error: `error: The requested file was not found`.

What to do next:

- Log in to the Tenable Nessus Manager parent node to manage linked Tenable Agents and nodes.
- Link or migrate agents to the cluster.
- On the Tenable Nessus Manager parent node, manage cluster groups to organize your nodes into groups that conform to your network topology. You must segment your network with cluster groups when certain agents only have access to certain child nodes. By default, Nessus assigns the node to the default cluster group.

View or Edit a Node

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

On Tenable Nessus Manager with clustering enabled, you can view the list of child nodes currently linked to the parent node. Tenable Nessus assigns these child nodes to cluster groups. You can

view details for a specific node, such as its status, IP address, number of linked agents, software information, and plugin set. If agents on the node are currently running a scan, a scan progress bar appears.

You can edit a node's name or the maximum number of agents that can be linked to the child node.

To view or edit a child node:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.

3. In the cluster groups table, click the row of a cluster group that contains child nodes.

   The **Cluster Nodes** tab appears. The **Cluster Nodes** table describes the following information about each cluster node:

Column	Description
Name	The child node name.
Status	The child node's current state: • **Idle** — The node is inactive and is not scanning or rebalancing. • **Idle (disabled)** — The node is manually disabled via the button. • **Scanning** — The node is scanning.
Scans	The count of in-progress scans the child node is participating in.
Usage	This column indicates how many agents are currently linked to the node compared to its maximum capacity. **Note:** You can configure the maximum agents per node later in step 8.
Last	The last day and time the child node communicated with the parent

Connected	node.
Link	Click disable or enable the child node in the cluster group.
Delete	Click to remove the child node from the cluster group.

4. Click the row of the child node you want to view.

   Tenable Nessus Manager shows the **Node Details** tab.

5. In the **Node Details** tab, view detailed information for the selected node.

6. To move the node to another cluster group, do the following:

   a. Next to **Cluster Group**, click the button.

      The **Change Cluster Group** dialog box appears.

   b. In the drop-down menu, select a different cluster group.

   c. Click **Save**.

      The node moves to another cluster group.

7. To edit node settings, click the **Settings** tab.

8. Edit any of the following:

   - **Node Name** — Type a unique name to identify the node.
   - **Max Agents** — Type the maximum number of agents that can be linked to the child node. The default value is 10,000 and the maximum value is 20,000.

9. Click **Save**.

   Tenable Nessus Manager updates the node settings.

Enable or Disable a Node

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

If you disable a child node, its linked Tenable Agents relink to another available child node in the same cluster group. If you re-enable a child node, Tenable Agents may become unevenly distributed, at which point you can choose to Rebalance Nodes.

To enable or disable child nodes:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.

3. In the cluster groups table, click the row of a cluster group that contains child nodes.

4. In the row of a child node, do one of the following:

   - To disable a node:

     a. Hover over the button, which becomes .

     b. Click the button.

        Tenable Nessus Manager disables the child node.

   - To enable a node:

     a. Hover over the . button, which becomes .

     b. Click the button.

        Tenable Nessus Manager enables the child node.

Rebalance Nodes

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

Tenable Agents may become unevenly distributed across child nodes for various reasons: a child node or multiple child nodes may be temporarily unavailable, disabled, deleted, or recently added. Events such as these negatively impact the cluster's performance. When the imbalance passes a certain threshold, Tenable Nessus Manager gives you the option to rebalance child nodes. This threshold is passed when one or both of the following criteria are met:

- 10% of your agents are not ideally distributed, based on your nodes' ideal capacity.
- A single node has at least 5% more agents than the node's ideal capacity.

  Example:

Your organization has four nodes and 100 linked agents. To evenly distribute linked agents across four nodes, Tenable Nessus Manager should assign each node 25% of the total linked agents which, in this case, would be 25 linked agents per node.

Tenable Nessus Manager gives you the option to rebalance child nodes if either:

- *Tenable Nessus Manager can redistribute 10% or more of your linked agents (in this example, 10 linked agents or more) for better results. For example, if two of your nodes have 20 linked agents and two of your nodes have 30 linked agents, Tenable Nessus Manager would allow you to rebalance the nodes to reach the ideal 25-25-25-25 distribution.*
- *One of your nodes reaches 30% of its capacity (in this example, ~33 linked agents)*

When you rebalance child nodes, Tenable Agents get redistributed more evenly across child nodes within a cluster group. Tenable Agents unlink from an overloaded child node and relink to a child node with more availability.

To rebalance child nodes:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.

3. In the cluster groups table, click the row of a cluster group.

4. In the upper-right corner of the page, click **Rebalance Nodes**.

   Tenable Nessus Manager rebalances the Tenable Agent distribution across child nodes.

Delete a Node

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

When you delete a child node, linked Tenable Agents eventually relink to another available child node in the same cluster group. The agents may take longer to relink if you delete a node compared to if you disable the node instead.

If the node you want to delete is the last node in a cluster group with linked agents, you must first move those agents to a different cluster group. If you only want to disable a child node temporarily, see Enable or Disable a Node.

To delete a child node:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.

3. In the cluster groups table, click the row of a cluster group that contains child nodes.

4. In the row of the child node you want to delete, click the ✕ button.

   The **Delete Agent Node** dialog box appears.

   Note: If you delete a node, you cannot undo this action.

5. To confirm you want to delete the child node, click **Delete**.

   Tenable Nessus Manager deletes the child node.

Cluster Groups

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

Clusters are divided into cluster groups that allow you to deploy and link agents in a way that conforms to your network topology. For example, you could create cluster groups for different regions of where your nodes and agents are physically located, which could minimize network traffic and control where your agents' connections occur.

Cluster child nodes must belong to a cluster group, and can only belong to one cluster group at a time. Agents in each cluster group only link to nodes in the same cluster group.

A cluster group is different from an agent group, which is a group of agents that you designate to scan a target. You use cluster groups to manage the nodes that agents link to within a cluster.

To manage your cluster groups and their assigned nodes and agents, see the following:

Create a cluster group

By default, Tenable Nessus assigns new nodes and agents to the default cluster group. You can create cluster groups that conform to your network topology. For example, you could create cluster groups for different regions of where your nodes and agents are physically located, which could minimize network traffic and control where your agents' connections occur.

A cluster group is different from an agent group, which is a group of agents that you designate to scan a target. You can use cluster groups to manage the nodes that agents link to within a cluster.

Note: If cluster child nodes have automatic software updates disabled, you must manually update them to Nessus 8.12 or later to use agent cluster groups. If cluster child nodes have automatic software updates enabled, nodes can take up to 24 hours to update. To ensure correct linking and configuration, wait for all child nodes to update to a supported Nessus version before configuring custom cluster groups. All child nodes must be on the same Nessus version and operating system.

Before you begin:

- Enable Clustering on the Tenable Nessus Manager parent node.

To create a cluster group:

1. Log in to the Tenable Nessus Manager parent node.
2. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.
3. In the upper-right corner, click ⊕ **New Cluster Group**.

   The **New Cluster Group** window appears.
4. Type a **Name** for the cluster group.
5. Click **Add**.

   Tenable Nessus Manager creates a new cluster group.

Modify a cluster group

You can edit a cluster group name or set a cluster group as the default cluster group. Tenable Nessus assigns the new linked nodes to the default cluster group.

To modify a cluster group:

1. Log in to the Tenable Nessus Manager parent node.
2. In the top navigation bar, click **Sensors**.

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.
3. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.
4. In the cluster groups table, in the row of the cluster group you want to modify, click the button.

   The **Edit Cluster Group** window appears.
5. Edit any of the following settings:

   - **Name** — Type a new name for the cluster group.
   - **Set as Default** — Select this check box to set this cluster group as the default cluster group that Tenable Nessus adds new linked nodes to.
6. Click **Save**.

   Tenable Nessus Manager updates the cluster group settings.

Add a node to a cluster group

By default, Tenable Nessus assigns new linked nodes to the default cluster group. You can also add a node to a different cluster group manually; for example, you could add nodes that are in a similar location to the same cluster group. A node can only belong to one cluster group at a time.

When you move a node that belonged to another cluster group, any agents that were linked to that node remain in their original cluster group and relink to another node in the original cluster group.

Note: If cluster child nodes have automatic software updates disabled, you must manually update them to Nessus 8.12 or later to use agent cluster groups. If cluster child nodes have automatic software updates enabled, nodes can take up to 24 hours to update. To ensure correct linking and configuration, wait for all child nodes to update to a supported Nessus version before configuring custom cluster groups. All child nodes must be on the same Nessus version and operating system.

Before you begin:

- Ensure you have added at least one child node to the cluster, as described in Link a Node.
- If you want to add a node to a cluster group other than the default cluster group, create a cluster group first.

To add a child node to a cluster group:

1. Log in to the Tenable Nessus Manager parent node.
2. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.
3. In the cluster groups table, click the row of the cluster group to which you want to add a node.

   The cluster group details page appears and shows the **Cluster Nodes** tab by default.
4. In the upper-right corner, click **Add Nodes**.

   The **Add Nodes** window appears and shows the available nodes.
5. (Optional) Search for a node by name to filter the results.
6. In the nodes table, select the check box next to each node you want to add.

   Note: A node can only belong to one cluster group at a time. When you move a node that belonged to another cluster group, any agents that were linked to that node remain in their original cluster group and relink to another node in the original cluster group.
7. Click **Add**.

   Tenable Nessus Manager moves the node to the cluster group.

Add an agent to a cluster group

By default, Tenable Nessus assigns new agents to the default cluster group. You can also add agents to a different cluster group manually; for example, you could add agents that are in a similar location to the same cluster group. An agent can only belong to one cluster group at a time.

When you add an agent to a cluster group, the agent relinks to an available node in the cluster group.

Before you begin:

- Ensure you have added at least one child node to the cluster, as described in Link a Node.
- Ensure the cluster group you want to add an agent to has at least one node.

To add an agent to a cluster group:

1. Log in to the Tenable Nessus Manager parent node.
2. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.
3. In the cluster groups table, click the row of the cluster group to which you want to add an agent.

   The cluster group details page appears and shows the **Cluster Nodes** tab by default.
4. Click the **Agents** tab.

   The agents assigned to the cluster group appear in a table.
5. In the upper-right corner, click **Add Agents**.

   The **Add Agents** window appears and shows available agents.
6. (Optional) Search for an agent by name to filter the results.
7. In the agents table, select the check box next to each agent you want to add.

   Note: Agents can only belong to one cluster group at a time. If you move the agent to a different group, it relinks to an available node in the new cluster group.
8. Click **Add**.

   Tenable Nessus Manager adds the agent to the cluster group.

Move a node to a cluster group

By default, Tenable Nessus assigns new linked nodes to the default cluster group. You can manually add a node to a different cluster group; for example, you could add nodes that are in a similar location to the same cluster group. A node can only belong to one cluster group at a time.

When you move a node that belonged to another cluster group, any agents that were linked to that node remain in their original cluster group and relink to another node in the original cluster group.

Before you begin:

- Ensure you have added at least one child node to the cluster, as described in Link a Node.
- If you want to move a node to a cluster group other than the default cluster group, create a cluster group first.

To move a child node to a different cluster group:

1. Log in to the Tenable Nessus Manager parent node.
2. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.
3. In the cluster groups table, click the row of the cluster group that contains the agent you want to move.

   The cluster group details page appears and shows the **Cluster Nodes** tab by default.
4. In the cluster nodes table, select the check box for each node that you want to move to a different cluster group.

   > **Note:** If there are agents assigned to the cluster group, you must leave at least one node in the cluster group.
5. In the upper-right corner, click **Move**.

   The **Move Node** window appears.
6. In the drop-down box, select the cluster group to which you want to move the node.

   > **Note:** A node can only belong to one cluster group at a time. When you move a node that belonged to another cluster group, any agents that were linked to that node remain in their original cluster group and relink to another node in the original cluster group.
7. Click **Move**.

   Tenable Nessus Manager moves the node to the selected cluster group.

Move an agent to a cluster group

By default, Tenable Nessus assigns new agents to the default cluster group. You can manually add agents to a different cluster group; for example, you could add agents that are in a similar location to the same cluster group. An agent can only belong to one cluster group at a time.

When you move an agent to a cluster group, the agent relinks to an available node in the cluster group. There may be a mismatch in the number of agents listed for the cluster group and actual usage when an agent is moving or relinking.

Before you begin:

- Ensure you have added at least one child node to the cluster, as described in Link a Node.
- Ensure the cluster group you want to add an agent to has at least one node.

To move an agent to a different cluster group:

1. Log in to the Tenable Nessus Manager parent node.
2. In the top navigation bar, click **Sensors**.

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.
3. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.
4. In the cluster groups table, click the row of the cluster group that contains the agent you want to move.

   The cluster group details page appears and shows the **Cluster Nodes** tab by default.
5. Click the **Agents** tab.

   The agents assigned to the cluster group appear in a table.
6. In the agents table, select the check box for each agent that you want to move to a different cluster group.
7. In the upper-right corner, click **Move**.

The **Move Agent** window appears.

8. In the drop-down box, select the cluster group to which you want to move the agent.

   Note: Agents can only belong to one cluster group at a time. If you move the agent to a different group, it relinks to an available node in the new cluster group.

9. Click **Move**.

   Tenable Nessus Manager moves the agent to the cluster group.

Delete a cluster group

You can delete a cluster group that does not have any assigned nodes or agents. You cannot delete the default cluster group.

Before you begin:

- Move or delete the nodes in the cluster group.

To delete a cluster group:

1. Log in to the Tenable Nessus Manager parent node.
2. In the top navigation bar, click **Sensors**.

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

3. In the left navigation bar, click **Agent Clustering**.

   The **Cluster Groups** page appears.

4. In the cluster groups table, in the row of the cluster group you want to delete, click the ✕ button.

   The **Delete Cluster Group** window appears.

5. To confirm that you want to delete the cluster group, click **Delete**.

   Note: You cannot undo this action.

   Tenable Nessus Manager deletes the cluster group.

Scanners

In Tenable Nessus Manager, you can view the instance's linking key and a list of linked remote scanners. You can click on a linked scanner to view details about that scanner.

Scanners are identified by scanner type and indicate whether the scanner has **Shared** permissions.

You can link remote scanners to Nessus Manager with the Linking Key or valid account credentials. Once linked, you can manage scanners locally and select them when configuring scans.

For more information, see:

- Link Nessus Scanner
- Unlink Nessus Scanner
- Enable or Disable a Scanner
- Remove a Scanner
- Download Managed Scanner Logs
- Tenable Nessus Plugin and Software Updates

Link Nessus Scanner

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

To link your Tenable Nessus scanner during initial installation, see Configure Nessus.

If you choose not to link the scanner during initial installation, you can link Tenable Nessus scanner later. You can link a Tenable Nessus scanner to a manager such as Tenable Nessus Manager or Tenable Vulnerability Management.

Note: You cannot link to Tenable Security Center from the user interface after initial installation. If your scanner is already linked to Tenable Security Center, you can unlink and then link the scanner to Tenable Vulnerability Management or Tenable Nessus Manager, but you cannot relink to Tenable Security Center from the interface.

To link a Tenable Nessus scanner to a manager:

1. In the user interface of the manager you want to link to, copy the **Linking Key**, found on the following page:

   - Tenable Vulnerability Management: **Settings** > **Sensors** > **Linked Scanners** > ⊕ **Add Nessus Scanner**
   - Tenable Nessus Manager: **Sensors** > **Linked Scanners**

   > **Note:** You can also retrieve your scanner linking key from the `nessuscli`. For more information, see `nessuscli fix --secure --get scanner_linking_key` in the nessuscli Fix Commands section.

2. In the Tenable Nessus scanner you want to link, in the top navigation bar, click **Settings**.

   The **About** page appears.

3. In the left navigation bar, click **Remote Link**.

   The **Remote Link** page appears.

4. Fill out the linking settings for your manager as described in Remote Link.

5. Click **Save**.

   Tenable Nessus links to the manager.

Unlink Nessus Scanner

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

You can unlink your Tenable Nessus scanner from a manager so that you can relink it to another manager.

> **Note:** You cannot link to Tenable Security Center from the user interface after initial installation. If your scanner is already linked to Tenable Security Center, you can unlink and then link the scanner to Tenable Vulnerability Management or Tenable Nessus Manager, but you cannot relink to Tenable Security Center from the interface.

To unlink a Tenable Nessus scanner from a manager:

1. In the Tenable Nessus scanner you want to unlink, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **Remote Link**.

   The **Remote Link** page appears.

3. Switch the toggle to **Off**.

4. Click **Save**.

   Tenable Nessus unlinks from the manager.

What to do next

- If you unlinked Tenable Nessus from Tenable Security Center, delete the scanner from Tenable Security Center.

Enable or Disable a Scanner

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

To enable a linked scanner:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Linked Scanners**.

3. In the scanners table, in the row for the scanner that you want to enable, hover over the button, which becomes .

4. Click the button.

   Tenable Nessus enables the scanner.

To disable a linked scanner:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Linked Scanners**.

3. In the scanners table, in the row for the scanner that you want to disable, hover over the button, which becomes .
4. Click the button.

   Tenable Nessus disables the scanner.

Remove a Scanner

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.
2. In the left navigation bar, click **Linked Scanners**.
3. Do one of the following:

   - To remove a single scanner:
     - In the scanners table, in the row for the scanner that you want to remove, click the button.

       A confirmation window appears.
   - To remove multiple scanners:
     a. In the scanners table, select the check box in the row for each scanner that you want to remove.

     b. In the upper-right corner, click the **Remove** button.

        A confirmation window appears.
4. In the confirmation window, click **Remove**.

   Tenable Nessus Manager removes the scanner or scanners.

Download Managed Scanner Logs

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

As an administrator in Tenable Nessus Manager, you can request and download a log file containing logs and system configuration data from any of your managed scanners and Tenable Agents. This information can help you troubleshoot system problems, and also provides an easy way to gather data to submit to Tenable Support.

You can store a maximum of five log files from each managed scanner in Tenable Nessus Manager. Once the limit is reached, you must remove an old log file to download a new one.

> **Note:** You can only request logs from Nessus scanners running 8.1 and later.

To download logs from a managed scanner:

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

   The **Linked Agents** page appears. By default, **Linked Agents** is selected in the left navigation menu and the **Linked Agents** tab is active.

2. In the left navigation bar, click **Linked Scanners**.

   The **Scanners** page appears and displays the linked scanners table.

3. In the linked scanners table, click the scanner for which you want to download logs.

   The detail page for that scanner appears.

4. Click the **Logs** tab.

5. In the upper-right corner, click **Request Logs**.

   > **Note:** If you have reached the maximum of five log files, the **Request Logs** button is disabled. Remove an existing log before downloading a new one.

   Tenable Nessus Manager requests the logs from the managed scanner the next time it checks in, which may take several minutes. You can view the status of the request in the user interface until the download is complete.

6. To download the log file, click the file name.

   Your system downloads the log file.

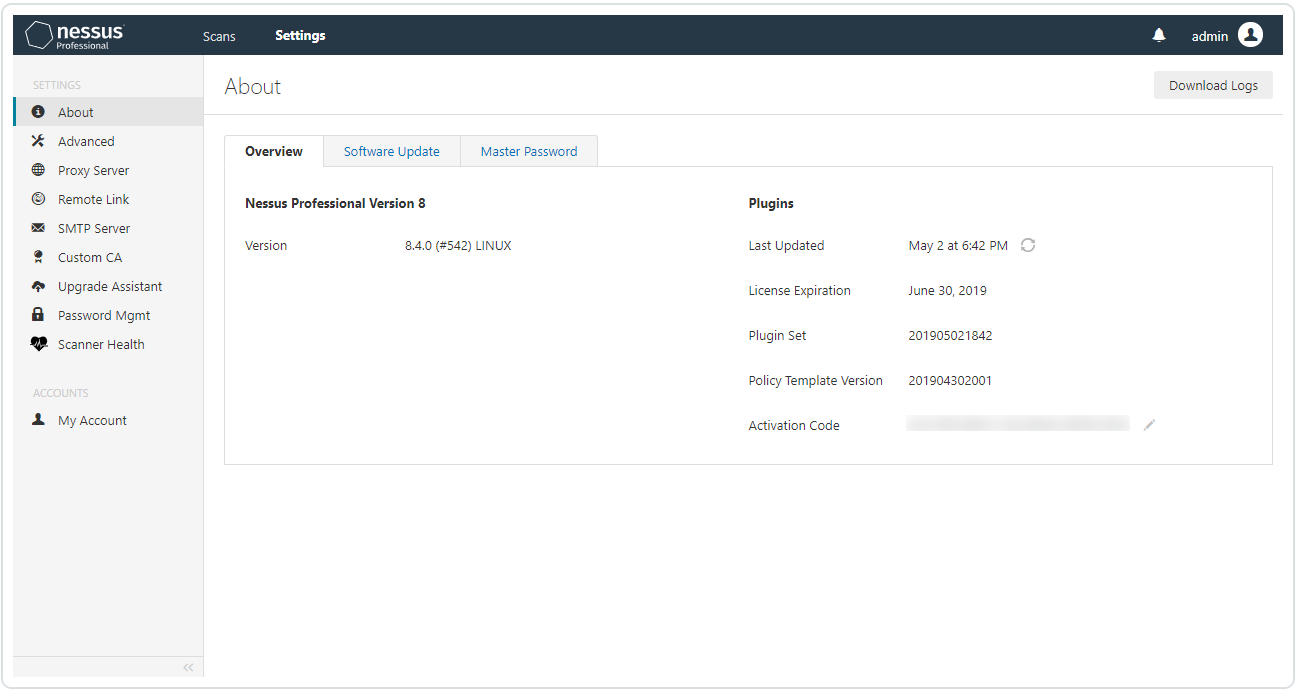
To remove an existing log:

- In the row of the log you want to remove, click the 🗑 button.

To cancel a pending or failed log download:

- In the row of the pending or failed log download that you want to cancel, click the ⊘ button.

Settings



The **Settings** page contains the following sections:

- About
- Advanced
- Proxy Server
- Remote Link
- SMTP Server
- Custom CA
- My Account
- Users

About

Required user role when using Tenable Nessus Manager: System Administrator

The **About** page shows an overview of Tenable Nessus licensing and plugin information. When you access the product settings, the **About** page appears. By default, Tenable Nessus shows the **Overview** tab, which contains information about your Tenable Nessus instance, as described in the **Overview** table.

On the **Software Update** tab, you can set your automatic software update preferences or manually update Tenable Nessus software.

On the **Plugin Detail Locale** tab, you can select the language you want plugin details to appear in.

On the **Encryption Password** tab, you can set an encryption password.

On the **Events** tab, you can view a history of Tenable Nessus system events that have occurred.

Basic users cannot view the **Software Update** or **Encryption Password** tabs. Standard users can only view the product version and basic information about the current plugin set.

To download logs, click the **Download Logs** button in the upper-right corner of the page. For more information, see Download Logs.

Overview

Value	Description
Nessus Professional and Nessus Expert	
Version	The version of your Nessus instance.
Licensed Domains	(Tenable Nessus Expert only) The number of unique domains you have scanned with the attack surface discovery template over the past 90 days. Tenable Nessus Expert allows up to five licensed domains. Once you have not scanned a domain for 90 days, Tenable Nessus removes it from the **Licensed Domains** count. If your organization wants to purchase more domains, contact your Tenable Customer Success Manager (CSM). For more information, see Create an Attack Surface Discovery Scan.
Licensed URLs	(Tenable Nessus Expert only) The number of unique URLs you have scanned with Tenable Nessus web application scanning over the past 90 days. Tenable Nessus Expert allows up to five licensed URLs. Once you have not scanned a URL for 90 days, Tenable Nessus removes it from the **Licensed URLs** count. If

Value	Description
	your organization wants to purchase more URLs, contact your Tenable Customer Success Manager (CSM). For more information, see Licensing.
Last Updated	The date on which the plugin set was last refreshed. This date can indicate the last time that Tenable Nessus updated the plugins based on its automatic plugin update cycle or the last time you clicked the update plugins button ( ).
Expiration	The date on which your license age outs. **Note:** You cannot run scans or download new plugins after your license age outs. You can still access your system and scan reports for 30 days after expiration.
Plugin Set	The ID of the current plugin set.
Policy Template Version	The ID of the current version of the policy template set.
Activation Code	The activation code for your instance of Nessus.
Nessus Manager	
Version	The version of your Nessus instance.
Licensed Hosts	The number of hosts you can scan, depending on your license.
Licensed Scanners	The number of scanners that you have licensed that are currently in use.
Licensed Agents	The number of agents that you have licensed that are currently in use.
Last Updated	The date on which the plugin set was last refreshed.

Value	Description
Expiration	The date on which your license age outs.
Plugin Set	The ID of the current plugin set.
Policy Template Version	The ID of the current version of the policy template set.
Activation Code	The activation code for your instance of Nessus.

Download Logs

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

As an administrator, you can download a log file containing local logs and system configuration data for Tenable Nessus instance you are currently logged into. This information can help you troubleshoot system problems, and also provides an easy way to gather data to submit to Tenable Support.

You can choose to download two types of log files: **Basic** or **Extended**. The **Basic** option contains recent Tenable Nessus log data and system information, including operating system version, CPU statistics, available memory and disk space, and other data that can help you troubleshoot. The **Extended** option also includes recent Tenable Nessus web server log records, system log data, and network configuration information.

For information on managing individual Tenable Nessus log files, see Manage Logs.

To download logs:

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

   The **About** page appears.

2. In the upper-right corner, click **Download Logs**.

   The **Download Logs** window appears.

3. Select the **Debug Log Type**:

- **Basic**: Standard Tenable Nessus log data and system configuration information.
- **Extended**: All information in the **Basic** option, Tenable Nessus web server log data, and more system logs.

4. (Optional) Select **Sanitize IPs** to hide the first two octets of IPv4 addresses in the logs.
5. Click **Download**.

   Tip: To cancel the download, click **Cancel**.

   Tenable Nessus generates the file *nessus-bug-report-XXXXX.zip*, which downloads and appears in your browser window.

Configure the Plugin Detail Locale

Required user role when using Tenable Nessus Manager: System Administrator

Use the **Plugin Detail Locale** tab in Tenable Nessus to choose what language (*locale*) plugin metadata appears in. This tab configures the language for any plugin metadata that appears in the following user interface and report fields:

- **Synopsis**
- **Description**
- **Script Name**
- **Solution**

Tip: English is the default plugin detail locale. You only have to configure the plugin detail locale if you want plugin details to appear in a language that is not English.

Note: This feature is not available for managed scanners, Tenable Nessus Manager, and when Tenable Nessus is in offline mode.

To configure the plugin detail locale:

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. Select the **Plugin Detail Locale** tab.
3. Select the **Enable Plugin Locales** checkbox.
4. Next to the **Locales** label, select the languages to download. When you select a language, Tenable Nessus adds it to the **Default Plugin Detail Locale** list.

   You can choose any combination of Japanese, Simplified Chinese, and Traditional Chinese; English is already available by default.
5. Select your **Default Plugin Detail Locale**. The default locale determines what language your plugin details appear in. You can select from any of the languages that you selected in the previous step.
6. Click **Save**. Tenable Nessus notifies you that it is downloading your selected language packs.

   Once the download completes, Tenable Nessus applies your default locale selection, and the plugin metadata in the Tenable Nessus user interface and reports show in the selected language.

Set an Encryption Password

Required user role when using Tenable Nessus Manager: System Administrator

If you set an encryption password, Nessus encrypts all policies, scans results, and scan configurations. You must enter the password when Tenable Nessus restarts.

Caution: If you lose your encryption password, it cannot be recovered by an administrator or Tenable Support.

To set an encryption password in the Tenable Nessus user interface:

1. In Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.
2. Click the **Encryption Password** tab.
3. In the **New Password** box, type your encryption password.
4. Click the **Save** button.

   Tenable Nessus saves the encryption password.

To set an encryption password in the command-line interface:

1. Access Tenable Nessus from the CLI.
2. Type the following command specific to your operating system:
   - Linux:

     ```
     /opt/nessus/sbin/nessusd --set-encryption-passwd
     ```

   - Windows:

     ```
     C:\Program Files\Tenable\Nessus\nessusd --set-encryption-passwd
     ```

   - macOS:

     ```
     /Library/Nessus/run/sbin/nessusd --set-encryption-passwd
     ```

3. When prompted, type a new password.

   Note: The password does not appear when you are typing.

   ```
   /opt/nessus/sbin/nessusd --set-encryption-passwd
   New password :
   Again :
   New password is set
   ```

   If your password is valid, a success message appears.

View Tenable Nessus System Events

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

You can view a history of backend and system-level events that occur in Tenable Nessus from the **About** > **Events** tab in the user interface.

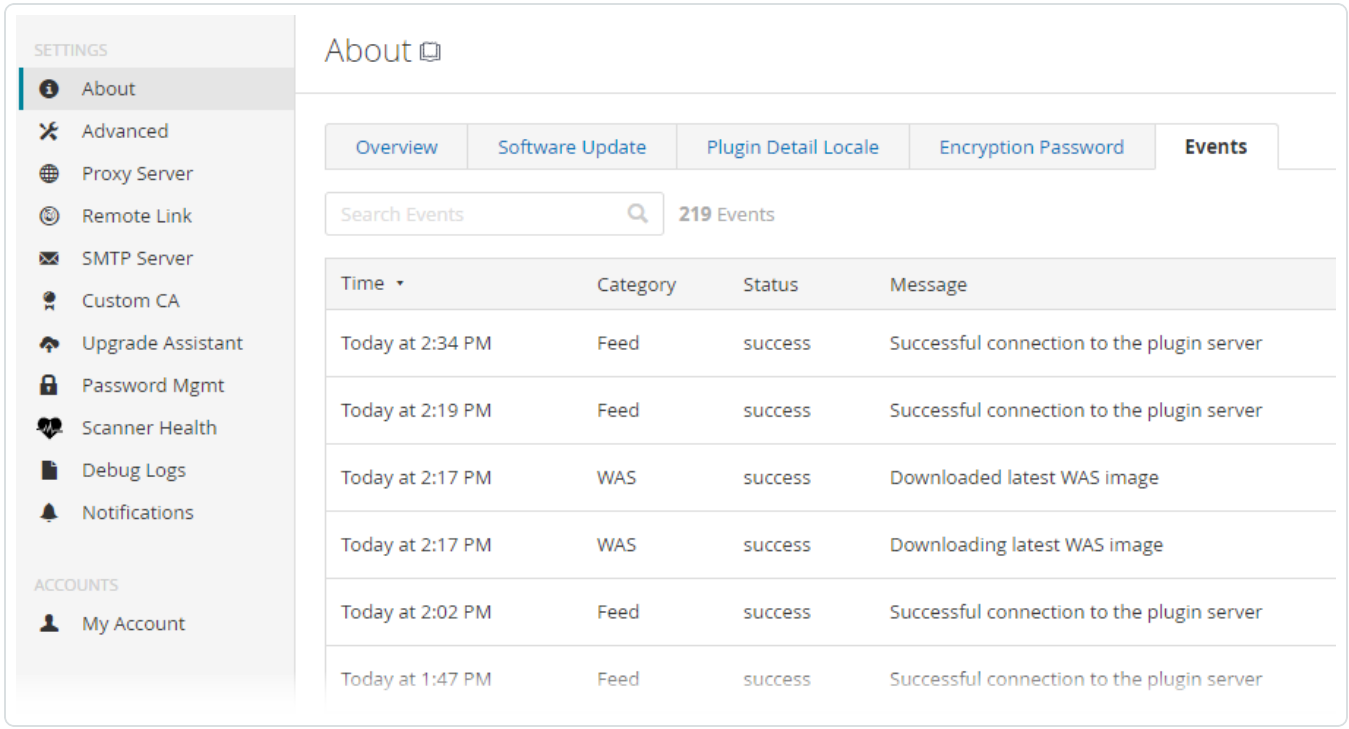
You can use the **Events** tab to view feed and web app scanning (WAS) events, such as when Tenable Nessus successfully connects to the plugin server, when Tenable Nessus begins and finishes plugin downloads, and when Tenable Nessus downloads the latest WAS image.

To view Tenable Nessus backend events:

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. Select the **Events** tab.



   The table of system events appears. For each event, the table lists the date and time the event occurred on, the event category, status, and a description message. You can filter the table by each column in ascending or descending order by clicking the column headers, or you can search for a specific event in the **Search Events** search bar.

Advanced Settings

> **Required user role when using Tenable Nessus Manager:** System Administrator

The **Advanced Settings** page allows you to configure Tenable Nessus manually. You can configure advanced settings from the Tenable Nessus user interface, or from the command-line interface. Tenable Nessus validates your input values to ensure only valid configurations.

Tenable Nessus groups the advanced settings into the following categories:

- User Interface
- Scanning
- Logging
- Performance
- Security
- Agents and Scanners
- Cluster
- Miscellaneous
- Custom

Details

- Advanced settings apply globally across your Tenable Nessus instance.
- To configure advanced settings, you must use a Tenable Nessus administrator user account.
- Tenable Nessus does not automatically update all advanced settings.
- Changes may take several minutes to take effect.
- Tenable Nessus indicates the settings that require restarting for the change to apply with the ℹ icon.
- Custom policy settings supersede the global advanced settings.

User Interface

Setting	Description	Default	Valid Values	Restart Required?
Allow Post-Scan Editing (allow_post_scan_editing)	Allows a user to make edits to scan results after the scan is complete.	yes	yes or no	no

Setting	Description	Default	Valid Values	Restart Required?
Disable API (disable_api)	Disables the API, including inbound HTTP connections. Users cannot access Tenable Nessus via the user interface or the API.	no	yes or no	yes
Disable Frontend (disable_ frontend)	Disables the Tenable Nessus user interface. Users can still use the API.	no	yes or no	yes
Login Banner (login_banner)	A text banner that appears after you attempt to log in to Tenable Nessus. **Note:** The banner only appears the first time you log in on a new browser or computer.	None	String	no
Maximum Concurrent Web Users (global.max_ web_users)	Maximum web users who can connect simultaneously.	1024	Integers. If set to 0, there is no limit.	no
Nessus Web Server IP (listen_address)	IPv4 address to listen for incoming connections. If set to 127.0.0.1, this restricts access to local	0.0.0.0	String in the format of an IP address	yes

Setting	Description	Default	Valid Values	Restart Required?
	connections only.			
Nessus Web Server Port (xmlrpc_listen_port)	The port that the Tenable Nessus web server listens on.	8834	Integers	yes
UI Theme (ui_theme)	When enabled, changes user interface color theme to dark mode. **Note:** The UI Theme setting may not function properly if you have SELinux enabled.	`Track Os Setting`	`Light`, `Dark`, or `Track Os Setting`	no
Use Mixed Vulnerability Groups (scan_vulnerability_groups_mixed)	When enabled, Tenable Nessus shows the severity level as **Mixed** for vulnerability groups, unless all the vulnerabilities in a group have the same severity. When disabled, Tenable Nessus shows the highest severity indicator of a vulnerability in a group	`yes`	`Yes` or `No`	no
Use Vulnerability Groups (scan_vulnerability_	When enabled, Tenable Nessus groups vulnerabilities	`yes`	`yes` or `no`	no

Setting	Description	Default	Valid Values	Restart Required?
groups)	in scan results by common attributes, giving you a shorter list of results.			

Scanning

Setting	Description	Default	Valid Values	Restart Required?
Audit Trail Verbosity (audit_trail)	Controls verbosity of the plugin audit trail. Full audit trails include the reason why Tenable Nessus did not include certain plugins in the scan.	`full`	`full`, `partial`, `none`	no
Auto Enable Plugin Dependencies (auto_enable_dependencies)	Automatically activates the plugins that are depended on by other plugins. The setting does not enable plugins that are depended on by scan template settings. If disabled, not all plugins may run despite being selected in a scan policy.	`yes`	`yes` or `no`	no
CGI Paths for Web Scans (cgi_path)	A colon-delimited list of CGI paths to use for web server scans.	/cgi-bin:/scripts	String	no
Engine Thread Idle Time (engine.idle_wait)	Number of seconds a scan engine remains idle before shutting itself down.	60	Integers 0-600	no

Max Plugin Output Size (plugin_output_max_size_kb)	The maximum size, in KB, of plugin output that Tenable Nessus includes in the exported scan results with the `.nessus` format. If the output exceeds the maximum size, Tenable Nessus truncates the output in the report.	1000	Integers. If set to 0, there is no limit.	no
Maximum Ports in Scan Reports (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	no
Maximum Ports Reported by Portscanner Plugins (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	no
Maximum Size for E-mailed Reports (attached_report_maximum_size)	Specifies the maximum size, in MB, of any report attachment. If the report exceeds the maximum size, then it is not attached to the email. Tenable Nessus does not support report attachments larger than 50 MB.	25	Integers 0-50	no
Nessus	Location of the Tenable Nessus rules file	*Nessus*	String	no

Rules File Location (rules)	(`nessusd.rules`).
	
	The following are the defaults for each operating system:
	
	Linux:
	
	`/opt/nessus/etc/nessus/nessusd.rules`
	
	macOS:
	
	`/Library/Nessus/run/var/nessus/conf/nessusd.rules`
	
	Windows:
	
	`C:\ProgramData\Tenable\Nessus\nessus\conf\nessusd.rules`
		config directory for your operating system		

Non-Simultaneous Ports (non_simult_ports)	Specifies ports against which two plugins you cannot run simultaneously.	139, 445, 3389	String	no
Paused Scan Timeout (paused_scan_timeout)	The duration, in minutes, that a scan can remain in the paused state before Tenable Nessus terminates it.	0	Integers 0-10080	no
PCAP Snapshot Length (pcap.snaplen)	The snapshot size used for packet capture; the maximum size of a captured network packet. Typically, Tenable Nessus sets this value automatically based on the scanner's NIC. However, depending on your network configuration, Tenable Nessus may truncate the packages, resulting in the following	0	Integers 0-262144	no

	message in your scan report: "The current snapshot length of ### for interface *X* is too small." You can increase the length to avoid packet truncation.			
Port Range (port_range)	The default range of ports that the scanner plugins probe.	`default`	`default`, `all`, a range of ports, a comma-separated list of ports and/or port ranges. Specify UDP and TCP ports by prefixing each range by `T:` or `U:`.	no

Reverse DNS Lookups (reverse_lookup)	When enabled, Tenable Nessus identifies targets by their fully qualified domain name (FQDN) in the scan report. When disabled, the report identifies the target by hostname or IP address.	no	yes or no	no
Safe Checks (safe_checks)	When enabled, Tenable Nessus uses safe checks, which use banner grabbing rather than active testing for a vulnerability.	yes	yes or no	no
Silent Plugin Dependencies (silent_dependencies)	When enabled, Tenable Nessus does not include the list of plugin dependencies and their output in the report. You can select a plugin as part of a policy that depends on other plugins to run. By default, Tenable Nessus runs those plugin dependencies, but does not include their output in the report. When disabled, Tenable Nessus includes both the selected plugin and any plugin dependencies in the report.	yes	yes or no	no
Slice Network Addresses (slice_network_addresses)	If you set this option, Tenable Nessus does not scan a network incrementally (10.0.0.1, then 10.0.0.2, then 10.0.0.3, and so on) but attempts to slice the workload throughout the whole network (for example, it scans 10.0.0.1, then 10.0.0.127, then 10.0.0.2, then 10.0.0.128, and so on).	no	yes or no	no
System Default Severity Basis (severity_basis)	In Tenable Nessus scanners and Tenable Nessus Professional, you can choose whether Tenable Nessus calculates the severity of vulnerabilities using CVSSv2 or CVSSv3 scores (when available) by configuring your default severity base setting. In Tenable Nessus scanners and	On a new installation of Tenable Nessus: cvss_v3	cvss_v2, cvss v3, or cvss_v4	no

	Tenable Nessus Professional, you can choose whether Tenable Nessus calculates the severity of vulnerabilities using CVSSv2, CVSSv3, or CVSSv4 scores (when available) by configuring your default severity base setting. When you change the default severity base, the change applies to all existing scans that are configured with the default severity base. Future scans also use the default severity base. For more information about CVSS scores and severity ranges, see CVSS Scores vs. VPR. **Note:** This setting is not available for Tenable Nessus Manager.	On preexisting upgraded instance: `cvss_v2`		

Logging

Setting	Description	Default	Valid Values	Restart Required?
Log Additional Scan Details (log_details)	When enabled, scan logs include the username, scan name, and current plugin name in addition to the base information. You may not see these additional details unless you also enable `log_whole_attack`.	no	`yes` or `no`	no
Log Verbose Scan	Logs verbose details of the scan. Helpful for debugging issues with the scan, but this may be disk intensive. To add more details, enable	no	`yes` or `no`	no

Setting	Description	Default	Valid Values	Restart Required?
Details (log_whole_attack)	`log_details`.			

Nessus Dump File Location (dumpfile)	Location of `nessusd.dump`, a log file for debugging output if generated.
	The following are the defaults for each operating system:
	Linux:
	`/opt/nessus/var/nessus/logs/nessusd.dump`
	macOS:
	`/Library/Nessus/run/var/nessus/logs/nessusd.dump`
	Windows:
	`C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.dump`
		Nessus log directory for your operating system	String	yes

Nessus Dump File Log Level (nasl_log_type)	The type of NASL engine output in `nessusd.dump`.	`normal`	`normal`, `none`, `trace`, or `full`.	yes
Nessus Dump File Max Files (dumpfile_	The maximum number of the `nessusd.dump` files kept on disk. If the number exceeds the specified value, Tenable Nessus deletes the oldest dump file.	100	Integers 1-1000	yes

Setting	Description	Default	Valid Values	Restart Required?
max_files)				
Nessus Dump File Max Size (dumpfile_max_size)	The maximum size of the `nessusd.dump` files in MB. If file size exceeds the maximum size, Tenable Nessus creates a new dump file.	512	Integers 1-2048	yes
Nessus Dump File Rotation Time (dumpfile_rotation_time)	Determines how often Tenable Nessus dump files are rotated in days.	1	Integers 1-365	yes
Nessus Dump File Rotation (dumpfile_rot)	Determines whether Tenable Nessus rotates dump files based on maximum rotation size or rotation time.	`size`	`size` — Tenable Nessus rotates dump files based on size, as specified in `dumpfile_max_size`. `time` — Tenable	yes

Setting	Description	Default	Valid Values	Restart Required?
			Nessus rotates dump files based on time, as specified in `dumpfile_rotation_time`.	
Nessus Log Level (backend_log_level)	The logging level of the `backend.log` log file, as indicated by a set of log tags that determine what information to include in the log. If you manually edited `log.json` to set a custom set of log tags for `backend.log`, this setting overwrites that content. For more information, see Manage Logs.	`normal`	• `normal` — sets log tags to `log, info, warn, error, tra`	yes

Setting	Description	Default	Valid Values	Restart Required?
			ce • debug — sets log tags to log, info, warn, error, trace, debug • verbose — sets log tags to	

Setting	Description	Default	Valid Values	Restart Required?
			`log`, `info`, `warn`, `error`, `trace`, `debug`, `verbose`	

Nessus Scanner Log Location (logfile)	Location where Tenable Nessus stores its scanner log file.
	The following are the defaults for each operating system:
	Linux:
	`/opt/nessus/var/nessus/logs/nessusd.messages`
	macOS:
	`/Library/Nessus/run/var/nessus/logs/nessusd.messages`
	Windows:
		Nessus log directory for your operating system	String	yes

Setting	Description	Default	Valid Values	Restart Required?
	`C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.messages`			
Log File Maximum Files (logfile_max_files)	Determines the maximum number of `nessusd.messages` files that Tenable Nessus keeps on the disk. If the number of `nessusd.messages` log files exceeds the specified value, Tenable Nessus deletes the oldest log files.	Tenable Nessus — 100 Tenable Agent — 2	Integers 1-1000	yes
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 Nessus creates a new messages log file.	Tenable Nessus —512 Tenable Agent — 10	Integers 1-2048	yes
Log File Rotation Time (logfile_rotation_time)	Determines how often Tenable Nessus messages log files are rotated in days.	1	Integers 1-365	yes
Log File Rotation	Determines whether Tenable Nessus rotates messages log files based on maximum	`size`	`size` — Tenable	yes

Setting	Description	Default	Valid Values	Restart Required?
(logfile_rot)	rotation size or rotation time.		Nessus rotates log files based on size, as specified in `logfile_max_size`. `time` — Tenable Nessus rotates log files based on time, as specified in `logfile_rotation_time`.	
Scanner Metric Logging (scanner.metrics)	Enables scanner performance metrics data gathering.	0	0 (off), 0x3f (full data except plugin metrics),	no

Setting	Description	Default	Valid Values	Restart Required?
			0x7f (full data including plugin metrics) **Note:** Including plugin metrics greatly increases the size of the log file. Tenable Nessus does not automatically clean up log files.	
Use Milliseconds in Logs (logfile_msec)	When enabled, `nessusd.messages` and `nessusd.dump` log timestamps are in milliseconds. When disabled, log timestamps are in seconds.	no	yes or no	yes

Performance

Setting	Description	Default	Valid Values	Restart Required?
Database Synchronous Setting (db_synchronous_setting)	Control how database updates are synchronized to disk. `NORMAL` is faster, with some risk of data loss during unexpected system shutdowns (for example, during a power outage or crash). `FULL` is safer, with some performance cost.	`NORMAL`	`NORMAL` or `FULL`	yes
Engine Logging (global.log.engine_details)	When enabled, logs additional information about which scan engine you assigned each target to during scanning.	`no`	`yes` or `no`	no
Global Max Hosts Concurrently Scanned (global.max_hosts)	Maximum number of hosts that Tenable Nessus can scan simultaneously across all scans.	Varies depending on hardware	Integers	no

Setting	Description	Default	Valid Values	Restart Required?
Global Max Port Scanners (global.max_portscanners)	Maximum number of port scanners.	100	Integers 0-1024	no
Global Max TCP Sessions (global.max_simult_tcp_sessions)	Maximum number of simultaneous TCP sessions across all scans.	50 for desktop operating systems (for example, Windows 10). 50000 for other operating systems (for example, Windows Server 2016).	Integers	no
Max Concurrent Checks Per Host (max_checks)	Maximum number of simultaneous plugins that can run concurrently on each host.	5	Integers	no
Max Concurrent Hosts Per Scan (max_hosts)	Maximum number of hosts checked at one time during a scan.	256	Integers If set to 0, defaults to 256	no

Setting	Description	Default	Valid Values	Restart Required?
Max Concurrent Scans (global.max_scans)	Maximum number of simultaneous scans that the scanner can run.	0	Integers 0-1000 If set to 0, there is no limit.	no
Max Engine Checks (engine.max_checks)	Maximum number of simultaneous plugins that can run concurrently on a single scan engine.	64	Integers	no
Max Engine Threads (engine.max)	Maximum number of scan engines that run in parallel. Each scan engine scans multiple targets concurrently from one or more scans (see `engine.max_hosts`).	8 times the number of CPU cores on the machine	Integers	no
Max Hosts Per Engine Thread (engine.max_hosts)	Maximum number of targets that run concurrently on a single scan engine.	16	Integers	no
Max HTTP Connections (max_http_connections)	The number of simultaneous connection attempts before the web server responds with HTTP code 503 (Service	600	Integers	yes

Setting	Description	Default	Valid Values	Restart Required?
	Unavailable, Too Many Connections).			
Max HTTP Connections Hard (max_http_connections_hard)	The number of simultaneous connection attempts before the web server does not allow further connections.	3000	Integers	yes
Max TCP Sessions Per Host (host.max_simult_tcp_sessions)	Maximum number of simultaneous TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner sends, which is 10 times the number of TCP sessions. For example, if you set this option to 15, the SYN scanner sends 150 packets per second at most.	0	Integers. If set to 0, there is no limit.	no
Max TCP Sessions Per Scan (max_simult_tcp_sessions)	Maximum number of simultaneous TCP sessions for the entire scan,	0	Integers 0-2000. If set to 0, there is no	no

Setting	Description	Default	Valid Values	Restart Required?
	regardless of the number of hosts the scanner is scanning.		limit.	
Engine Thread Pool Minimum Size (thread_pool.min)	The minimum size of the pool of threads available for use by the scan engine. You can defer asynchronous tasks to these threads, and this value controls the maximum number of threads.	2	Integers 0-100	no
Engine Thread Pool Maximum Size (thread_pool.max)	The maximum size of the pool of threads available for use by the scan engine. You can defer asynchronous tasks to these threads, and this value controls the maximum number of threads.	200	Integers 0-500	no
Minimum Engine Threads (engine.min)	The number of scan engines that start initially as Tenable Nessus scans the targets. After the	2 times the number of CPU cores on the machine	Integers	no

Setting	Description	Default	Valid Values	Restart Required?
	engine reaches `engine.optimal_hosts` number of targets, Tenable Nessus adds more scan engines up to `engine.max`.			
Optional Hosts Per Engine Thread (engine.optimal_hosts)	The minimum number of targets that are running on each scan engine before Tenable Nessus adds more engines (up to `engine.max`).	2	Integers	no
Plugin Check Optimization Level (optimization_level)	Determines the type of check that Tenable Nessus performs before a plugin runs. If you set this setting to `open_ports`, then Tenable Nessus checks that required ports are open; if they are not, the plugin does not run. If you set this setting to	None	`open_ports` or `required_keys`	no

Setting	Description	Default	Valid Values	Restart Required?
	`required_keys`, then Tenable Nessus performs the open port check, and also checks that required keys (KB entries) exist, ignoring the excluded key check.			
Plugin Timeout (plugins_timeout)	Maximum lifetime of a plugin's activity in seconds.	320	Integers 0-1000	no
QDB Memory Usage (qdb_mem_usage)	Directs Tenable Nessus to use more or less memory when idle. If Tenable Nessus is running on a dedicated server, setting this to high uses more memory to increase performance. If Tenable Nessus is running on a shared machine, setting this to low uses considerably less memory, but has a moderate performance	`low`	`low` or `high`	no

Setting	Description	Default	Valid Values	Restart Required?
	impact.			
Reduce TCP Sessions on Network Congestion (reduce_connections_on_congestion)	Reduces the number of TCP sessions in parallel when the network appears to be congested.	no	yes or no	no
Remediations Limit (remediations_limit)	Limits the number of remediations that Tenable Nessus generates and shows in a scan result.	500	Integers > 0	no
Scan Check Read Timeout (checks_read_timeout)	Read timeout for the sockets of the tests.	5	Integers 0-1000	no
Stop Scan on Host Disconnect (stop_scan_on_disconnect)	When enabled, Tenable Nessus stops scanning a host that disconnects during the scan.	no	yes or no	no
XML Enable Plugin Attributes (xml_enable_plugin_attributes)	When enabled, Tenable Nessus includes plugin attributes in exported scans to Tenable Security Center.	no	yes or no	no
Webserver Thread Pool	The minimum	2	Integers 0-	no

Setting	Description	Default	Valid Values	Restart Required?
Minimum Size (www.thread_pool.min)	thread pool size for the webserver/backend.		100	
Webserver Thread Pool Maximum Size (www.thread_pool.max)	The maximum thread pool size for the webserver/backend.	200	Integers 0-500	no

Security

Setting	Description	Default	Valid Values	Restart Required?
Always Validate SSL Server Certificates (strict_certificate_validation)	Always validate SSL server certificates, even during initial remote link (requires manager to use a trusted root CA).	no	yes or no	no
Cipher Files on Disk (cipher_files_on_disk)	Encipher files that Tenable Nessus writes.	yes	yes or no	yes
Force Public Key Authentication (force_pubkey_auth)	Force logins for Tenable Nessus to use public key authentication.	no	yes or no	yes
Max	Maximum	0	Integers 0-2000.	no

Setting	Description	Default	Valid Values	Restart Required?
Concurrent Sessions Per User (max_sessions_per_user)	concurrent sessions per user		If set to 0, there is no limit.	
SSL Cipher List (ssl_cipher_list)	Cipher list to use for Tenable Nessus backend connections. You can use a preconfigured list of cipher strings, or enter a custom cipher list or cipher strings. **Note:** This setting only sets ciphers for TLS 1.2.	`compatible`	• `legacy` - A list of ciphers that can integrate with older and insecure browsers and APIs. • `compatible` - A list of secure ciphers that is compatible with all browsers, including Internet Explorer 11. May not include all the latest ciphers. • `modern` - A list of the latest and most secure ciphers. May not be compatible with older browsers, such as Internet Explorer 11. • `custom` - A	yes

Setting	Description	Default	Valid Values	Restart Required?
			custom OpenSSL cipher list. For more information on valid cipher list formats, see the OpenSSL documentation. • `niap` - A list of ciphers that conforms to NIAP standards. `ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384` **Tip**: For a list of Tenable-supported ciphers, see System Requirements in the *Tenable Vulnerability Management User Guide*.	
SSL Mode (ssl_	Minimum	`tls_1_2`	• `compat` -	yes

Setting	Description	Default	Valid Values	Restart Required?
mode)	supported version of TLS.		TLS v1.0+ • `ssl_3_0` - SSL v3+ • `tls_1_1` - TLS v1.1+ • `tls_1_2` - TLS v1.2+ • `tls_1_3` - TLS v1.3+ • `niap` - TLS v1.2	

Agents & Scanners

Note: The following settings are only available in Tenable Nessus Manager.

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

Setting	Description	Default	Valid Values	Restart Required?
	inactive agents are automatically deleted if `agent_auto_delete` is set to `yes`.			
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`. **Note:** This value must be less than the `agent_auto_delete_threshold`.	30	Integers 30-90	no
agents_progress_viewable	When a scan	100	Integers.	no

Setting	Description	Default	Valid Values	Restart Required?
	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.		If set to 0, this defaults to 100.	
agent_updates_from_feed	When enabled, new Tenable Agent software updates are automatically downloaded.	`yes`	`yes` or `no`	yes
cloud.manage.download_max	The maximum concurrent agent update downloads.	10	Integers	no
agent_merge_audit_trail	Controls whether or not agent scan result audit trail	`false`	`true` or `false`	no

Setting	Description	Default	Valid Values	Restart Required?
	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`.			
agent_merge_kb	Includes the agent scan result KB data in the main agent database. Excluding KB data can significantly improve agent result processing performance. If this setting is set to false, the **Include the KB**	`false`	`true` or `false`	no

Setting	Description	Default	Valid Values	Restart Required?
	setting in an individual scan or policy defaults to `Exclude KB`.			

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 corrupted scan result in the event of a crash. For more details, refer to the sqlite3 documentation.	`DELETE`	`MEMORY`
			`TRUNCATE`
			`DELETE`
				no

agent_merge_synchronous_setting	Sets the filesystem sync mode to use when processing agent results. Turning this off will significantly	`FULL`	`OFF`
			`NORMAL`
			`FULL`
				no

Setting	Description	Default	Valid Values	Restart Required?
	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.			
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

Cluster

Note: The following settings are only available in Tenable Nessus Manager with clustering enabled.

Setting	Description	Default	Valid Values
Agent Blacklist Duration Days (agent_blacklist_duration_days)	The number of days that an agent remains blocked from relinking to a cluster node. For example, Tenable Nessus blocks an agent if it tries to link with a UUID that matches an existing agent in a cluster. **Note:** Tenable Nessus blocks an agent after Tenable Nessus deletes or removes the agent due to inactivity. However, Tenable Nessus places the agent back in good standing if an administrator manually unlinks and relinks the agent.	7	Integers > 0
Agent Clustering Scan Cutoff (agent_cluster_scan_cutoff)	Tenable Nessus aborts scans after running this many seconds without a child node update.	3600	Integers > 299
Agent Node Global Maximum Default (agent_node_global_max_default)	The global default maximum number of agents allowed per cluster node. If you set an individual maximum for a child node, that setting overrides this setting.	10000	Integers 0-20000

Miscellaneous

Setting	Description	Default	Valid Values	Restart Required?
Allow Special Characters in User Names (allow_special_chars_in_username)	Determines whether Tenable Nessus usernames can include parentheses: **(** and **)**.	`true`	`true` or `false`	no
Automatic Update Delay (auto_update_delay)	Number of hours that Tenable Nessus waits between automatic updates.	24	Integers > 0	no
Automatic Updates (auto_update)	Automatically updates plugins. If you enable this setting and register Tenable Nessus, Tenable Nessus automatically gets the newest plugins from Tenable when they are available. If your scanner is on an isolated network that is not able to reach the internet, disable this setting. **Note:** This setting does not work for Tenable Nessus scanners that you connected to Tenable Vulnerability Management. Scanners linked to Tenable Vulnerability Management automatically receive updates from cloud.tenable.com. For more information, see the knowledge base article.	`yes`	`yes` or `no`	yes

Setting	Description	Default	Valid Values	Restart Required?
Automatically Update Nessus (auto_update_ui)	Automatically download and apply Tenable Nessus updates. **Note:** This setting does not work for Tenable Nessus scanners that you connected to Tenable Vulnerability Management. Scanners linked to Tenable Vulnerability Management automatically receive updates from cloud.tenable.com. For more information, see the knowledge base article.	yes	yes or no	no
Backups to keep (backup_days_to_keep)	Tenable Nessus automatically creates a backup file every 24 hours. Use this setting to determine how many days Tenable Nessus keeps the backup files before discarding them. For example, if you keep this setting at the default 30 days, Tenable Nessus stores daily backup files for the past 30 days. For more information about Tenable Nessus backup files, see Back Up Tenable Nessus.	30	Integers > 0	no
Child Node Port (child_node_listen_port)	Allows Tenable Nessus child nodes to communicate to the parent node on a different port.	none	Any valid port value	yes
Initial Sleep	(Tenable Nessus Manager only) Sleep time between managed scanner and agent	30	Integers 5-3300	no

Setting	Description	Default	Valid Values	Restart Required?
Time (ms_agent_sleep)	requests. You can override this setting in Tenable Nessus Manager or Tenable Vulnerability Management.			
Java Heap Size (java_heap_size)	Determines Java heap size (the system memory used to store objects instantiated by applications running on the Java virtual machine) Tenable Nessus uses when exporting PDF reports.	`auto`	`auto` or Integers > 0	yes
Max HTTP Client Requests (max_http_client_requests)	Determines the maximum number of concurrent outbound HTTP connections on managed scanners and agents.	4	Integers > 0	yes
Nessus Debug Port (dbg_port)	The port on which `nessusd` listens for `ndbg` client connections. If left empty, Tenable Nessus does not establish a debug port.	None	String in one of the following formats: *port* or *localhost*:*port* or *ip*:*port*	no
Nessus Preferences Database (config_	Location of the configuration file that contains the engine preference settings. The following are the defaults for each operating system:	*Tenable Nessus database director*	String	yes

Setting	Description	Default	Valid Values	Restart Required?

file)	Linux:
	`/opt/nessus/etc/nessus/nessusd.db`
	macOS:
	`/Library/Nessus/run/etc/nessus/conf/nessusd.db`
	Windows:
	`C:\ProgramData\Tenable\Nessus\conf\nessusd.db`
		y for your operating system		

Non-User Scan Result Cleanup Threshold (report_cleanup_threshold_days)	The age threshold (in days) for removing old system-user scan reports.	30	Integers > 0	no
Old User Files Cleanup (old_user_files_cleanup_hours)	The number of hours after which Tenable Nessus removes old user files from the file system. If set to 0, Tenable Nessus does not perform a cleanup.	0	Integers > 0	no
Orphaned Scan History	The number of days after which Tenable Nessus removes orphaned Tenable Security Center scans. For example, an	30	Integers > 0	no

Setting	Description	Default	Valid Values	Restart Required?
Cleanup (orphaned_scan_cleanup_days)	orphaned scan could be a scan executed via Tenable Security Center that was not properly removed. If set to 0, Tenable Nessus does not perform a cleanup. **Note:** This setting only applies to network scans launched from Tenable Security Center. It does not apply to agent or web application scans.			
Packet Capture Archive Cleanup (packet_capture_archive_cleanup_days)	The number of days after which Tenable Nessus removes packet capture archives from the filesystem. If set to 0, Tenable Nessus does not perform a cleanup.	30	Integers > 0	no
Plugin Integrity Check Frequency (Minutes) (plugin_healthcheck_frequency)	Determines the frequency, in minutes, at which Tenable Nessus runs a full plugin integrity check.	10080	Integers 1440-10080	yes
Remote Scanner	This setting allows Tenable Nessus to	None	Integer	yes

Setting	Description	Default	Valid Values	Restart Required?
Port (remote_listen_port)	operate on different ports: one dedicated to communicating with remote agents and scanners (comms port) and the other for user logins (management port). By adding this setting, you can link your managed scanners and agents a different port (for example, 9000) instead of the port defined in `xmlrpc_listen_port` (default 8834).			
Report Crashes to Tenable (report_crashes)	When enabled, Tenable Nessus sends crash information to Tenable, Inc. automatically to identify problems. Tenable Nessus does not send personal or system-identifying information to Tenable, Inc..	`yes`	`yes` or `no`	no
Scan Source IP(s) (source_ip)	Source IPs to use when running on a multi-homed host. If you provide multiple IPs, Tenable Nessus cycles through them whenever it performs a new connection.	None	IP address or comma-separated list of IP addresses.	yes
Send Telemetry (send_telemetry)	When enabled, Tenable Nessus periodically and securely sends non-confidential product usage data to Tenable. Usage statistics include, but are not limited to, data about your visited pages within the Tenable Nessus interface, your	`yes`	`yes` or `no`	yes

Setting	Description	Default	Valid Values	Restart Required?
	used reports and dashboards, your Tenable Nessus license, and your configured features. Tenable uses the data to improve your user experience in future Tenable Nessus releases. You can disable this option at any time to stop sharing usage statistics with Tenable.			
User Scan Result Deletion Threshold (scan_history_expiration_days)	The number of days after which Tenable Nessus deletes the scan history and data for completed scans permanently. **Note:** This setting affects any scanner, agent, and web application scans launched from Tenable Security Center.	0	Integers > 0 If set to 0, Tenable Nessus retains the history.	no
Windows Minidump (windows_minidump)	Determines whether Tenable Nessus generates a Windows minidump file in the log folder if Tenable Nessus for Windows crashes.	no	yes or no	no

Custom

Not all advanced settings are populated in the Tenable Nessus user interface, but you can set some settings in the command-line interface. If you create a custom setting, it appears in the **Custom** tab.

Use the following procedures to manage custom advanced settings:

Create a new setting

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **Advanced**.

   The **Advanced Settings** page appears.

3. In the upper right corner, click the **New Setting** button.

   The **Add Setting** window appears.

4. In the **Name** box, type the key for the new setting.

5. In the **Value** box, type the corresponding value.

6. Click the **Add** button.

   The new setting appears in the list.

Modify a setting

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

   The **About** page appears.

2. In the left navigation bar, click **Advanced**.

   The **Advanced Settings** page appears.

3. In the settings table, click the row for the setting you want to modify.

   The **Edit Setting** box appears.

4. Modify the settings as needed.

5. Click the **Save** button.

   Tenable Nessus saves the setting.

Delete a setting

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **Advanced**.

   The **Advanced Settings** page appears.

3. In the settings table, in the row for the setting you want to delete, click the ✕ button.

   A dialog box appears, confirming your selection to delete the setting.

4. Click **Delete**.

   Tenable Nessus deletes the setting.

The following table lists the advanced settings that you can configure, even though Tenable Nessus does not list them by default.

Identifier	Description	Default	Valid Values
acas_classification	Adds a classification banner to the top and bottom of the Tenable Nessus user interface, and turns on last successful and failed login notification.	None	• `UNCLASSIFIED` - Green banner • `CLASSIFIED` - Purple banner • `CONFIDENTIAL` - Blue banner • `SECRET` - Red banner • `TOP SECRET` - Orange banner • TOP SECRET/SCI - Yellow banner with black font color)
multi_scan_same_host	When disabled, to avoid overwhelming a host, Tenable Vulnerability Management prevents a single scanner from	`no`	`yes` or `no`

Identifier	Description	Default	Valid Values
	simultaneously scanning multiple targets that resolve to a single IP address. Instead, Tenable Vulnerability Management scanners serialize attempts to scan the IP address, whether it appears more than once in the same scan task or in multiple scan tasks on that scanner. Scans may take longer to complete. When enabled, a Tenable Vulnerability Management scanner can simultaneously scan multiple targets that resolve to a single IP address within a single scan task or across multiple scan tasks. Scans complete more quickly, but scan targets could potentially become overwhelmed, causing timeouts and incomplete results.		
merge_plugin_results	Supports merging plugin results for plugins that generate multiple findings with the same host, port, and protocol. Tenable recommends enabling this option for scanners linked to	no	yes or no

Identifier	Description	Default	Valid Values
	Tenable Security Center.		
nessus_syn_scanner.global_throughput.max	Sets the max number of SYN packets that Tenable Nessus sends per second during its port scan (no matter how many hosts Tenable Nessus scans in parallel). Adjust this setting based on the sensitivity of the remote device to large numbers of SYN packets.	65536	Integers
login_banner	A text banner shows that appears after you attempt to log in to Tenable Nessus. The banner only appears the first time you log in on a new browser or computer.	None	String
timeout.*<plugin ID>*	Enter the plugin ID in place of *<plugin ID>*. The maximum time, in seconds, that Tenable Nessus permits the *<pluginID>* to run before Tenable Nessus stops it. If you set this option for a plugin, this value supersedes `plugins_timeout`.	None	Integers 0-86400

Scan Engine Settings

Every Tenable Nessus deployment — whether it is a standalone Tenable Nessus Professional or Tenable Nessus Expert, or a Tenable Nessus scanner managed by Tenable Vulnerability

Management or Tenable Security Center — is equipped with advanced settings. Some of these settings, known as *scan engine settings*, control the Tenable Nessus scan engine's scanning performance. You can adjust scan engine settings in the **Performance Options** section of the scan policy **Settings**.

Tenable Nessus Scanner Settings

The following table is not an exhaustive list of all advanced settings. It is a list of the settings that affect scan engine performance. For a full list of the advanced settings, see Advanced Scan Settings.

Setting	Identifier	Definition
Global Max Hosts Concurrently Scanned	**global.max_hosts**	The total number of targets that the scanner processes simultaneously across all running scans. This value limits the total number of targets running in the scan engine. The scan engine does not process more targets than the value assigned to **global.max_hosts**.
Max Concurrent Scans	**global.max_scans**	The total number of scans the scan engine runs concurrently.
Global Max TCP Sessions	**global.max_simult_tcp_sessions**	The maximum number of concurrent TCP sessions allowed for all scans.
Global Max Port Scanners	**global.max_portscanners**	The maximum number of threads allocated to the port scanner task thread pool. This value represents the maximum number of port scanners the engine runs simultaneously across all scans.
Max Concurrent Hosts Per Scan	**max_hosts**	The maximum number of targets that the scan engine processes simultaneously for a given scan.
Max Concurrent Checks Per Host	**max_checks**	The maximum number of plugins that can run concurrently for a given target. This setting's value determines the number of plugins that each engine thread runs for a target.

Max TCP Sessions Per Scan	**max_simult_tcp_sessions**	The maximum number of concurrent TCP sessions allowed for a given scan.
Max TCP Sessions Per Host	**host.max_simult_tcp_sessions**	The maximum number of concurrent TCP sessions allowed for a single target.
Max Hosts Per Engine Thread	**engine.max_hosts**	The maximum number targets than an engine thread processes.
Optimal Hosts Per Engine Thread	**engine.optimal_hosts**	The number of targets the scan engine assigns to an engine thread before starting a new engine thread.
Max Engine Checks	**engine.max_checks**	The total number of plugins allowed to run for an engine thread across all the targets running in that thread.
Max Engine Threads	**engine.max**	The maximum number of engine threads that the scan engine starts.
Minimum Engine Threads	**engine.min**	The minimum number of engine threads that the scan engine starts to handle a scan.

The following sections provide brief explanations of precedence and caveats regarding how some of the settings affect the scan engine's processing of targets.

Max Host Settings

The following settings affect the scan engine's processing of targets:

- **global.max_hosts**
- **max_hosts**
- **engine.max_hosts**
- **engine.max**

In the majority of scenarios, **global.max_hosts** takes precedence over the other settings in determining maximum numbers of concurrent targets, but it is possible to engineer a situation

where it does not. For example, you could limit the maximum number of targets a scanner would scan concurrently by manipulating **engine.max_hosts** and **engine.max**. If the **engine.max_hosts** and **engine.max values** are configured such that the following occurs:

(**engine.max_hosts** x **engine.max**) < **global.max_hosts**

In this case, the scanner applies the more stringent limit, which is the value from **engine.max_hosts** multiplied by **engine.max**.

Max Simultaneous TCP Sessions Settings

Three advanced settings affect the number of concurrent TCP sessions in the scan engine:

- **global.max_simult_tcp_sessions**
- **max_simult_tcp_sessions**
- **host.max_simult_tcp_sessions**

The **global.max_simult_tcp_sessions** setting is an absolute cap that applies across all running scans on a scanner. The **max_simult_tcp_sessions** value caps the concurrent TCP sessions for a specific scan, and the **host.max_simult_tcp_**sessions setting limits the concurrent TCP sessions per host.

Max Checks Settings

Two settings control the number of plugins allowed to run concurrently by the scan engine:

- **max_checks**
- **engine.max_checks**

The **engine.max_checks** setting takes precedence over the **max_checks** setting so that the total number of concurrent plugins the engine runs at any given time does not exceed (**engine.max_checks** x **engine.max**).

Tenable Vulnerability Management and Tenable Security Center Policy Settings

When you launch a scan in Tenable Vulnerability Management or Tenable Security Center, they do not assign a single scan to a single scanner. Instead, to utilize multiple scanners effectively, they break up a single scan into smaller chunks (referred to as *tasks*) and distribute the tasks to multiple scanners. This allows multiple scanners to execute a single overall scan in parallel, but it also

affects how the scan engine settings are applied. The Tenable Nessus scan engine interprets each individual *task* as an entire scan.

For example, assume there is a single scan targeting 1,000 IPs. Tenable Vulnerability Management and Tenable Security Center process the scan in the following ways:

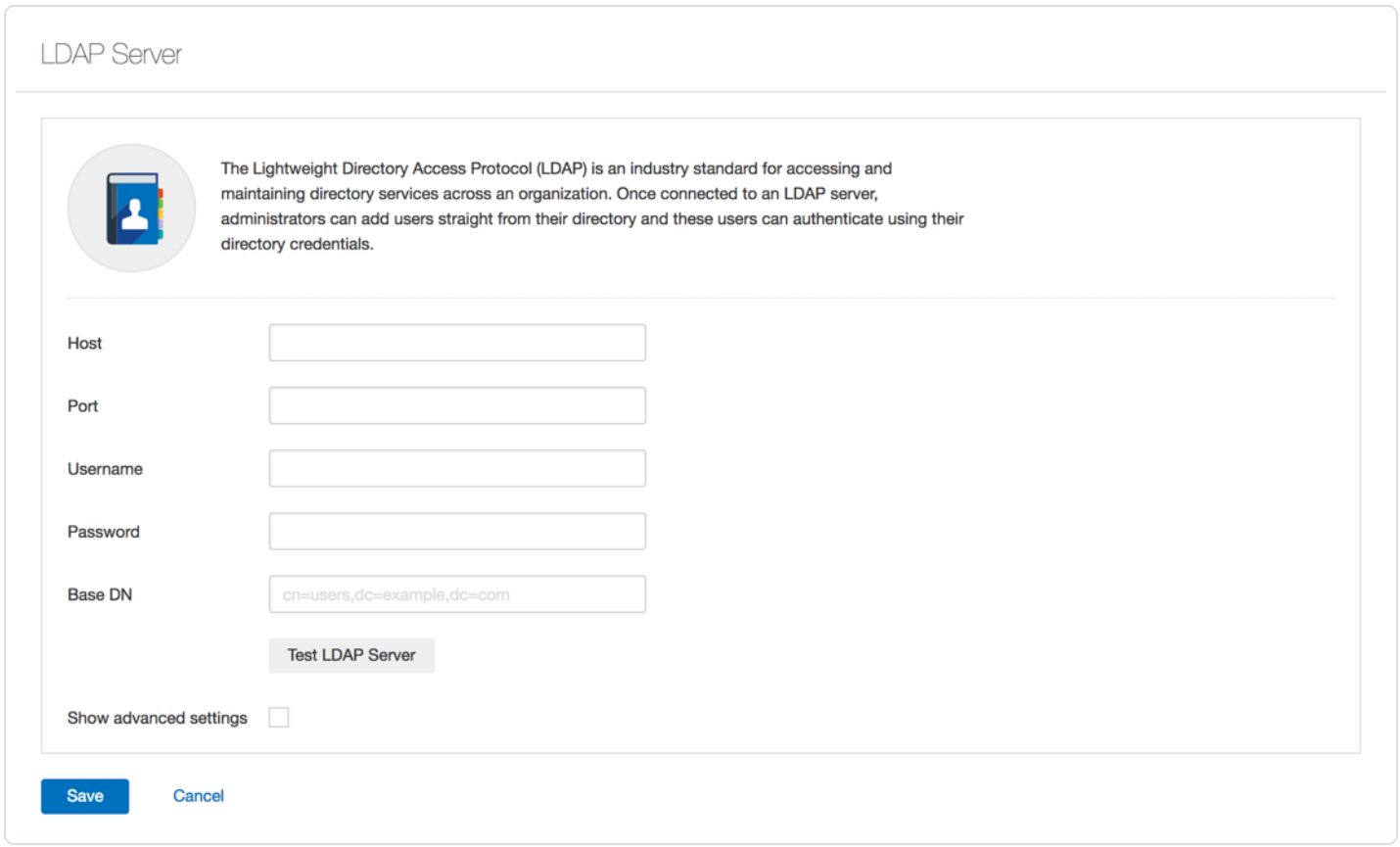
- **Tenable Vulnerability Management** — Tenable Vulnerability Management turns the scan targets into 8 tasks of 120 IPs each and a 9th task with 40 IPs, and assume that the scan policy has **max_hosts** (**Max simultaneous hosts per scan** in the user interface) set to 5. In this scenario, a given scanner would get 5 of those 9 tasks and execute a max of 25 hosts in parallel — 5 per scan, according to the scan engine — not a max of 5 hosts in parallel. Once the scanner completes the 5 tasks, it may receive a new batch of tasks from Tenable Vulnerability Management and continues scanning until the entire scan job is complete.
- **Tenable Security Center** — Tenable Security Center turns the scan targets into 125 tasks of 8 IPs each, and assume that the scan policy has **max_hosts** (**Max simultaneous hosts per scan** in the user interface) set to the default value of 30. In this scenario, a given scanner would get 4 of those 125 tasks and execute a max of 30 hosts in parallel — 8 in the first 3 tasks and 6 in the final task, according to the scan engine. Once the scanner completes a task, it receives a new task from Tenable Security Center and continues scanning until the entire scan job is complete.

Each "per scan" setting applies to the individual Tenable Vulnerability Management or Tenable Security Center tasks rather than the overall scan. This can sometimes lead to confusion and unanticipated scanner behavior when setting those performance tuning parameters in the scan policy.

LDAP Server (Tenable Nessus Manager)

Required user role when using Tenable Nessus Manager: System Administrator

In Tenable Nessus Manager, the **LDAP Server** page shows options that allow you to configure a Lightweight Directory Access Protocol (LDAP) server to import users from your directory.



To configure an LDAP server:

1. In Tenable Nessus Manager, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **LDAP Server**.

   The **LDAP Server** page appears.

3. Configure the settings as necessary:

Setting	Description
Host	The LDAP server host.
Port	The LDAP server port. Confirm the selection with your LDAP server administrators.
Username	The username for an account on the LDAP server with credentials to

	search for user data. Format the username as provided by the LDAP server.
Password	The password for an account on the LDAP server with credentials to search for user data.
Base DN	The LDAP search base used as the starting point to search for the user data.
Show advanced settings	Click the **Show advanced settings** checkbox to show or hide the advanced LDAP settings.
Advanced Settings (Optional)	
Username Attribute	The attribute name on the LDAP server that contains the username for the account. This is often specified by the string `sAMAccountName` in servers that may be used by LDAP. Contact your LDAP server administrator for the correct value.
Email Attribute	The attribute name on the LDAP server that contains the email address for the account. This is often specified by the string `mail` in servers that may be used by LDAP. Contact your LDAP server administrator for the correct value.
Name Attribute	The attribute name on the LDAP server that contains the name associated with the account. This is often specified by the string `CN` in servers that may be used by LDAP. Contact your LDAP server administrator for the correct value.
CA (PEM Format)	The LDAP server's certificate authority (CA) certificate, if applicable. Enter the certificate in PEM format.

4. (Optional) Click the **Test LDAP Server** button to verify the LDAP configuration you entered.

A message appears on the top-right corner of the page that confirms whether your LDAP configuration is valid. If the configuration is not valid, review the settings and adjust them as needed.

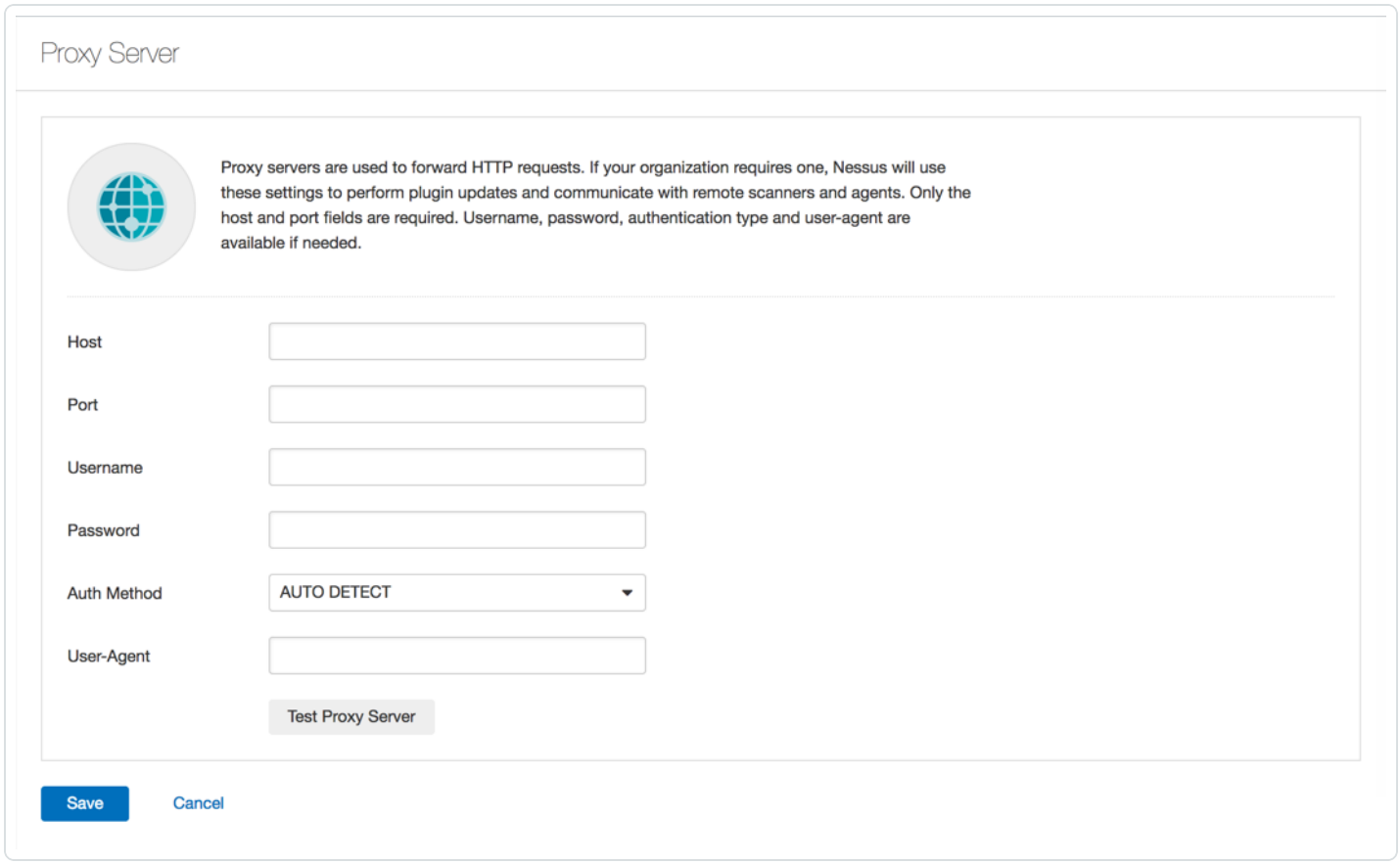
5. Click the **Save** button.

   Tenable Nessus Manager saves the LDAP server configuration.

Proxy Server

Required user role when using Tenable Nessus Manager: System Administrator

The **Proxy Server** page allows you to configure a proxy server. If the proxy you use filters specific HTTP user agents, you can type a custom user-agent string in the **User-Agent** box.



To configure a proxy server:

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **Proxy Server**.

   The **Proxy Server** page appears.

3. Configure the settings as necessary:

Setting	Description
Host	The proxy server host.
Port	The proxy server port.
Username	The username for an account on the proxy server with credentials to search for user data. Format the username as provided by the proxy server.
Password	The password for an account on the proxy server with credentials to search for user data.
Auth Method	The authentication method Nessus uses to connect to the proxy server: • **AUTO DETECT** — Tenable Nessus secures the connection with authentication based on what you entered for the previous settings. Tenable recommends selecting this option if you do not know what to select. • **NONE** — Tenable Nessus does not authenticate. • **BASIC** — Tenable Nessus secures the connection with basic authentication. • **DIGEST** — Tenable Nessus secures the connection with digest authentication. • **NTLM** — Tenable Nessus secures the connection with NTLM authentication.

	Note: Tenable Nessus only supports NTLMv2.
User-Agent	The user agent for the proxy server, if your proxy requires a preset user agent.

4. Click the **Save** button.

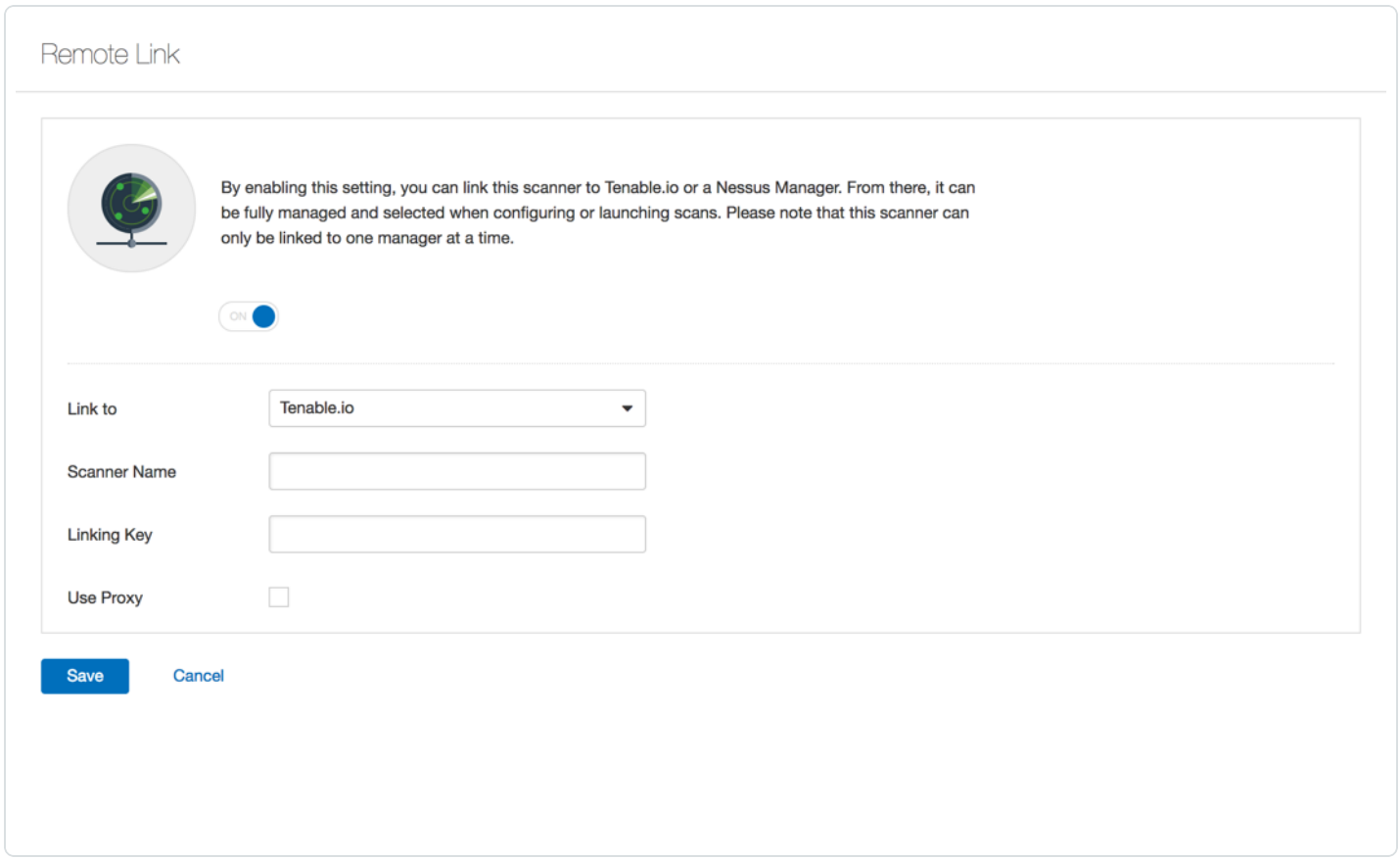
   Tenable Nessus saves the proxy server.

Remote Link

Required user role when using Tenable Nessus Manager: System Administrator

The **Remote Link** page allows you to link your Tenable Nessus scanner to a licensed Tenable Nessus Manager or Tenable Vulnerability Management.

Note: You cannot link to Tenable Security Center from the user interface after initial installation. If your scanner is already linked to Tenable Security Center, you can unlink and then link the scanner to Tenable Vulnerability Management or Tenable Nessus Manager, but you cannot relink to Tenable Security Center from the interface.



Enable or disable the toggle to link a scanner or unlink a scanner.

Remote Link Settings

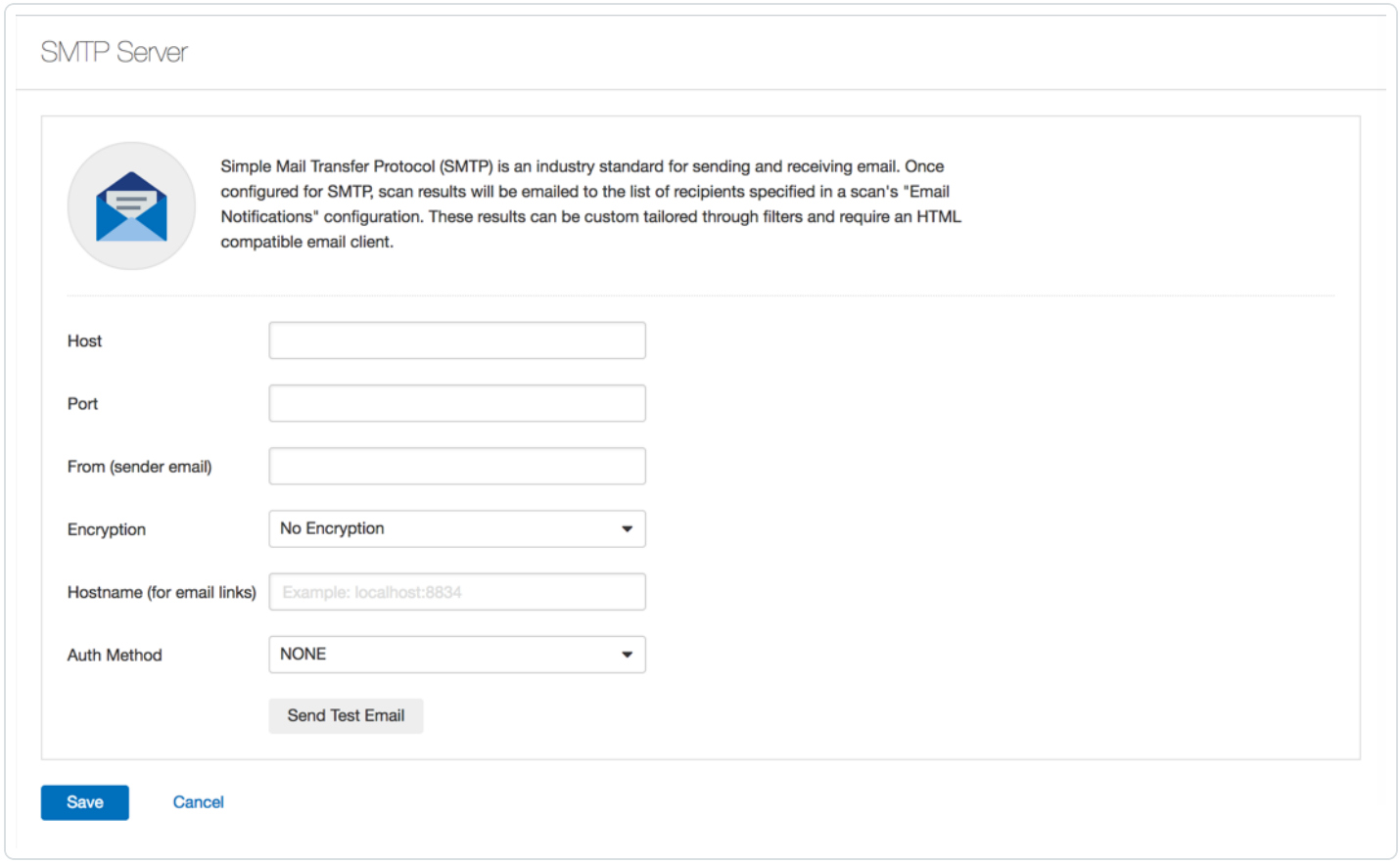
Option	Set To
Link Tenable Nessus to Tenable Nessus Manager	
Link to	**Nessus Manager**
Scanner Name	The name you want to use for this Tenable Nessus scanner.
Manager Host	The static IP address or hostname of the Tenable Nessus Manager instance you want to link to.
Manager Port	Your Tenable Nessus Manager port, or the default 8834.
Linking Key	The key specific to your instance of Tenable Nessus Manager.

Option	Set To
Use Proxy	Select or deselect the check box depending on your proxy settings. If you select **Use Proxy**, you must also configure: • **Host** — The hostname or IP address of the proxy server. • **Port** — The port number of the proxy server. • **Username** — The username for an account that has permissions to access and use the proxy server. • **Password** — The password associated with the username you provided.
Link Tenable Nessus to Tenable Vulnerability Management	
Link to	**Tenable.io**
Scanner Name	**cloud.tenable.com**
Linking Key	The key specific to your instance of Tenable Vulnerability Management. The key looks something like the following string: *2d38435603c5b59a4526d39640655c3288b00324097a08f7a93e5480940d1cae*
Use Proxy	Select or deselect the check box depending on your proxy settings. If you select **Use Proxy**, you must also configure: • **Host** — The hostname or IP address of the proxy server. • **Port** — The port number of the proxy server. • **Username** — The username for an account that has permissions to access and use the proxy server. • **Password** — The password associated with the username you provided.

SMTP Server

Required user role when using Tenable Nessus Manager: System Administrator

The **SMTP Server** page allows you to configure a Simple Mail Transfer Protocol (SMTP) server. Once you configure an SMTP server, Nessus can email HTML scan results to the list of recipients that you specify in the scan settings.



Note: The **SMTP Server** page is not available when Tenable Nessus is linked to Tenable Vulnerability Management.

To configure an SMTP server:

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **SMTP Server**.

   The **SMTP Server** page appears.

3. Configure the settings as necessary.

Setting	Description
Host	The SMTP server host.
Port	The SMTP server port.
From (sender email)	The email address that shows as the sender in the scan results email.
Encryption	The email encryption type: • **No Encryption** — Tenable Nessus does not encrypt the email. • **Force SSL** — Tenable Nessus forces SSL encryption for the email. • **Force TLS** — Tenable Nessus forces TLS encryption for the email. • **Use TLS if available** — Tenable Nessus uses TLS encryption if the receiving server is compatible.
Hostname (for email links)	The hostname that shows for the sender host and port in the email.
Auth Method	The authentication method Nessus uses to connect to the STMP server: • **NONE** — Tenable Nessus does not authenticate the connection. • **PLAIN** — Tenable Nessus secures the connection with plain (username/password) authentication. • **LOGIN** — Tenable Nessus secures the connection with login authentication. • **NTLM** — Tenable Nessus secures the connection with NTLM authentication.

	• **CRAM-MD5** — Tenable Nessus secures the connection with CRAM-MD5 authentication.

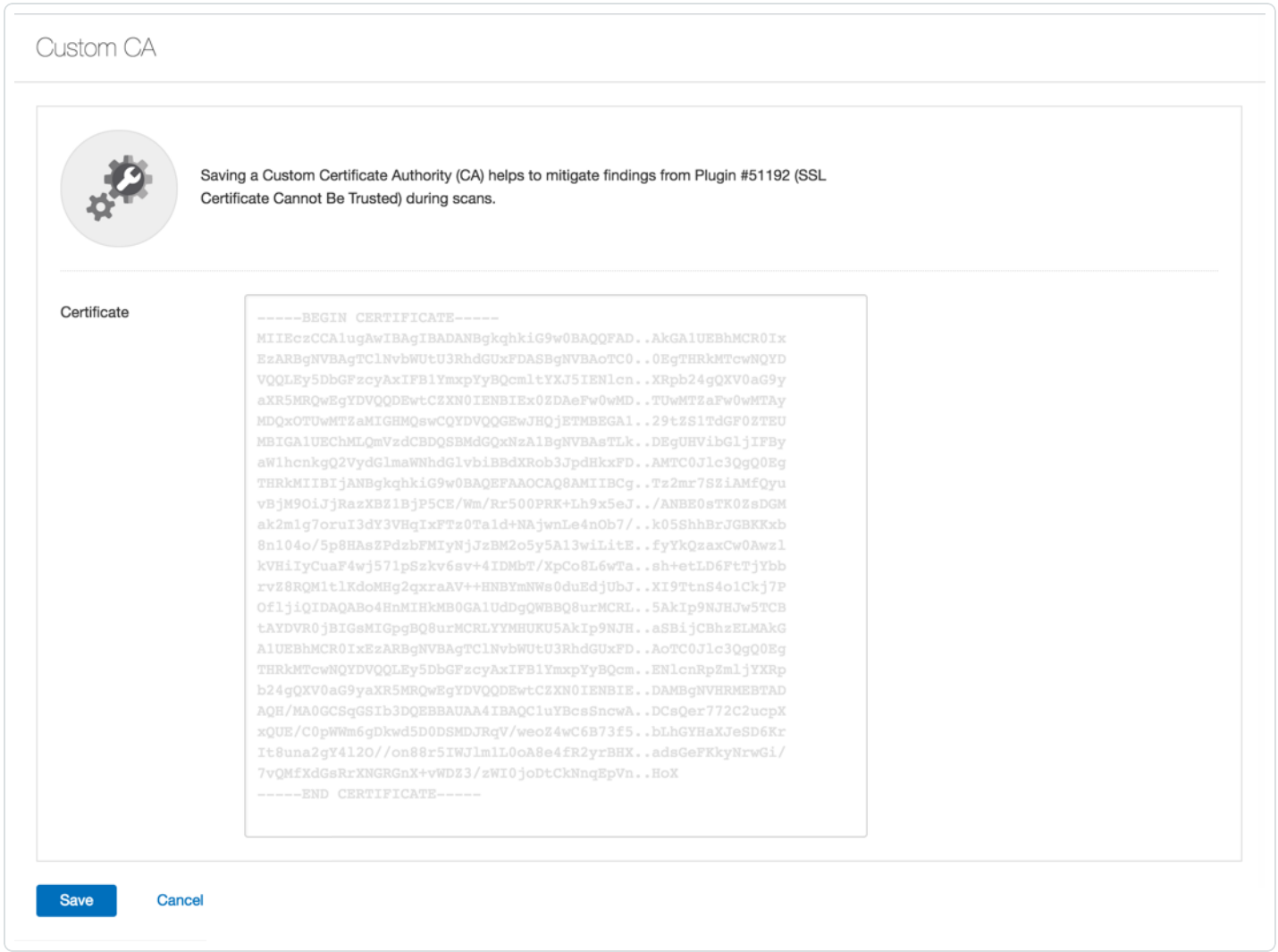
4. Click the **Save** button.

   Tenable Nessus saves the SMTP server.

Custom CA

Required user role when using Tenable Nessus Manager: System Administrator

The **Custom CA** page shows a text box that you can use to upload a custom certificate authority (CA) in Nessus. For more information, see Certificates and Certificate Authorities.



Note: Include the beginning text `-----BEGIN CERTIFICATE-----` and ending text `-----END CERTIFICATE-----`.

Tip: You can save more than one certificate in a single text file, including the beginning and ending text for each one.

Upgrade Assistant

Required user role when using Tenable Nessus Manager: System Administrator

The following feature is not supported in Federal Risk and Authorization Manage Program (FedRAMP) environments. For more information, see the FedRAMP Product Offering.

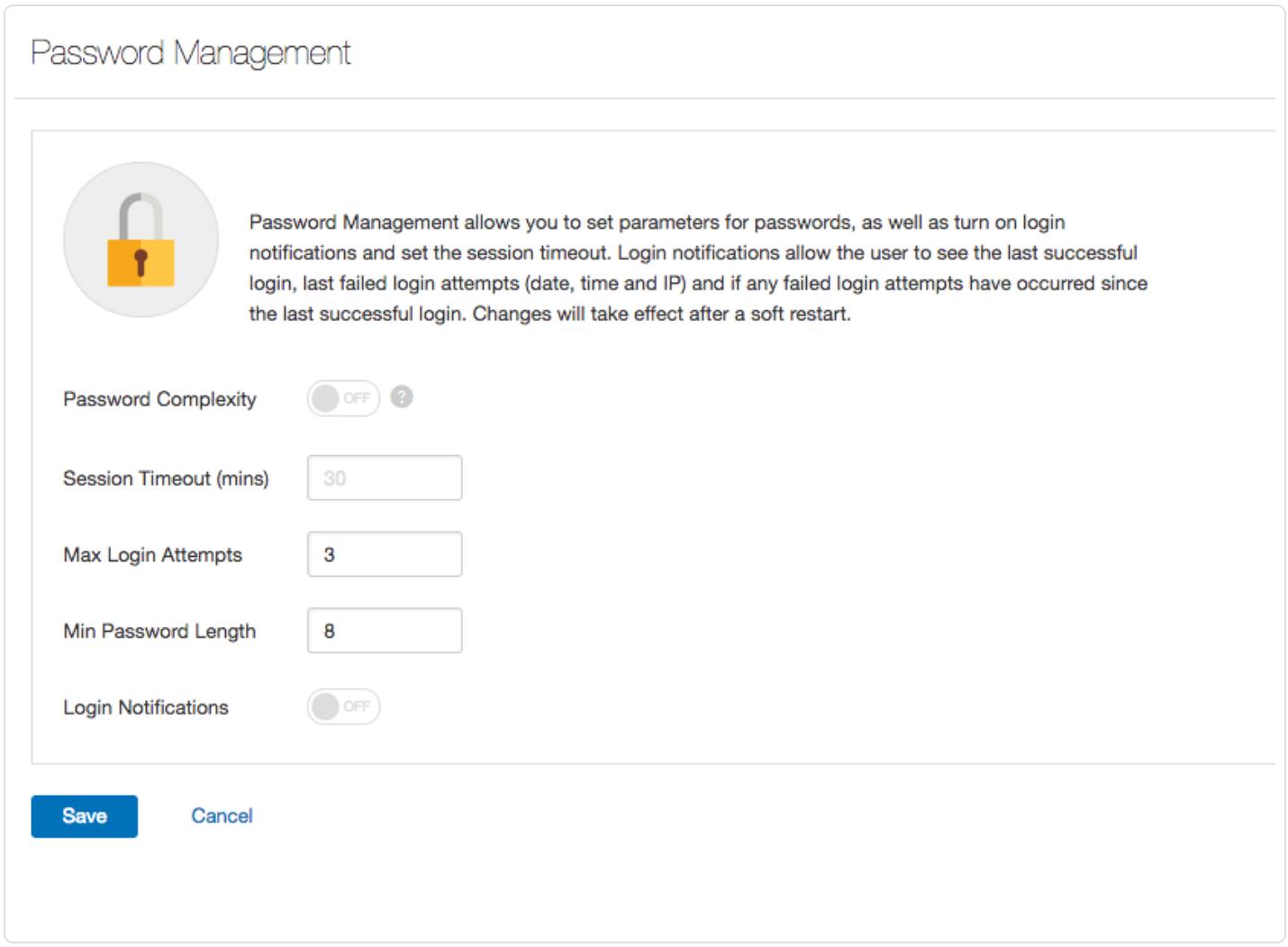
The **Upgrade Assistant** tool is not available in Tenable Nessus clustering environments.

You can upgrade data from Tenable Nessus to Tenable Vulnerability Management via the **Upgrade Assistant** tool. For more information, see Tenable Nessus to Tenable Vulnerability Management Upgrade Assistant.

Password Management

Required user role when using Tenable Nessus Manager: System Administrator

The **Password Management** page allows you to set parameters for passwords, login notifications, and the session timeout.



Tip: You can configure the password management settings from the `nessuscli`. For more information, see `nessuscli fix --set <password_setting>=<value>` in the Nessuscli topic.

Tip: For information on the security Tenable uses to store and protect passwords, see Encryption Strength.

To configure password management:

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **Password Mgmt**.

   The **Password Management** page appears.

3. Configure the settings as necessary:

Setting	Default	Description
Password Complexity	Off	Determines whether Tenable Nessus passwords must have a minimum of eight characters, and at least three of the following: an upper case letter, a lower case letter, a special character, and a number.
Session Timeout (mins)	30	Defines the web session timeout in minutes. Tenable Nessus logs users out automatically if their session is idle for longer than this timeout value.
Max Login Attempts	5	Defines the maximum number of user login attempts allowed by Tenable Nessus before the application locks the account out. Setting this value to 0 disables this feature.
Min Password Length	8	Defines the minimum number of characters for passwords of accounts.
Login Notifications	Off	Determines whether Tenable Nessus can see login notifications. Login notifications allow the user to see the last successful login and failed login attempts (date, time, and IP), and if any failed login attempts have occurred since the last successful login.

4. Click the **Save** button.

   Tenable Nessus saves the password setting.

   Note: Changes to the **Session Timeout** and **Max Login Attempts** settings require a restart to take effect.

Scanner Health

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

The **Scanner Health** page provides you with information about the performance of your Tenable Nessus scanner. You can monitor real-time health and performance data to help troubleshoot scanner issues. Scanner alerts provide information about system errors that may cause your scanner to malfunction.

Tenable Nessus removes alerts as you address them (for example, if your receive an alert about low disk space, deleting unneeded files to increase disk space removes the alert). Tenable Nessus updates the information every 30 seconds.

Tenable Nessus organizes the scanner health information into three categories: Overview, Network, and Alerts.

Overview

Widget	Description	Actions
Current Health	Widgets showing Nessus memory used in MB, CPU load, and the number of hosts Tenable Nessus is scanning.	None
Scanner Alerts	Alerts about areas where your Tenable Nessus scanner performance may be suffering. Alerts can have a severity level of Info, Low, Medium, or High.	Click an alert to see more details. If there are more than five alerts, click **More Alerts** to see the full list of alerts.
System Memory	Chart showing how much of your system memory Tenable Nessus is using.	None
Nessus Data Disk Space	Chart showing the percentage of free and used disk space on the disk where you installed Tenable Nessus's data directory.	None
Memory Usage History	Graph showing how many MB of memory Tenable Nessus used over time.	Hover over a point on the graph to see

		detailed data.
CPU Usage History	Graph showing the percentage of CPU load Tenable Nessus used over time.	Hover over a point on the graph to see detailed data.
Scanning History	Graph showing the number of scans Tenable Nessus ran and active targets Tenable Nessus scanned over time.	Hover over a point on the graph to see detailed data.

Network

Widget	Description	Actions
Scanning History	Graph showing the number of scans Tenable Nessus ran and active targets Tenable Nessus scanned over time.	Hover over a point on the graph to see detailed data.
Network Connections	Graph showing the number of TCP sessions Tenable Nessus creates during scans over time.	Hover over a point on the graph to see detailed data.
Network Traffic	Graph showing how much traffic Tenable Nessus is sending and receiving over the network over time.	Hover over a point on the graph to see detailed data.
Number of DNS Lookups	Graph showing how many reverse DNS (rDNS) and DNS lookups Tenable Nessus performs over time.	Hover over a point on the graph to see detailed data.
DNS Lookup Time	Graph showing the average time that Tenable Nessus takes to perform rDNS and DNS lookups over time.	Hover over a point on the graph to see detailed data.

Alerts

Widget	Description	Actions

Scanner Alerts	List of alerts about areas where your Tenable Nessus scanner performance may be suffering. Alerts can have a severity level of Info, Low, Medium, or High.	Click an alert to see more details.

For information, see Monitor Scanner Health.

Monitor Scanner Health

Required user role when using Tenable Nessus Manager: Administrator or System Administrator

The **Scanner Health** page provides you with information about the performance of your Tenable Nessus scanner. For more information about performance data, see Scanner Health.

To monitor scanner health:

1. In Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **Scanner Health**.

3. (Optional) To adjust the time scale on a graph, on the **Overview** tab, from the drop-down box, select a time period.

   The graphs on both the **Overview** and **Network** tabs reflect the selected time period.

4. (Optional) To hide an item from a time graph, click the item in the legend.

   Tip: Hiding items automatically adjusts the scale to the visible items and allows you to view one dataset at a time.

5. Click the **Overview**, **Network** or **Alerts** tab.

Advanced Debugging - Packet Capture

Required user role when using Tenable Nessus Manager: System Administrator

When working with Tenable Nessus to understand scanner results, it may be necessary to understand the communications between a scanner and the host that was scanned. When this occurs, Tenable support may request a capture of network traffic between the scanner and the

target host. Tenable Nessus now supports the ability to generate and download such a capture through the Tenable Nessus user interface.

Note: This feature has the following limitations:

- Packet capture does not apply to Tenable Nessus scanners that are linked to Tenable Security Center.
- Packet capture is limited to TCP and UDP traffic only. Other protocols such as ICMP (ping) are not captured.
- The **Target to capture** field must match a host in the scan's target list, or no capture will occur.
- Tenable Nessus limits the amount of disk space that can be allocated to packet capture data. The total disk space that may be used by the packet capture subsystem is the lesser of the following two parameters: 10% of the partition size on which Tenable Nessus is installed or 20GB.
- The maximum size of a single packet capture file is the lesser of the following two parameters: 10% of the packet capture total disk space value or 1GB.
- If, during a capture session, the amount of data exceeds the limit for a single capture file, the capture is terminated and the partial result is saved. These limits may be adjusted by a Tenable Nessus administrator using the `global.network_capture.max_disk_mb` and/or `global.network_capture.max_file_mb` advanced preferences.
- Tenable Nessus must be restarted for these changes to take effect.

To enable packet capture for a scan in the Tenable Nessus user interface:

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

   The **My Scans** page appears.

2. In the upper right corner, click the **New Scan** button.

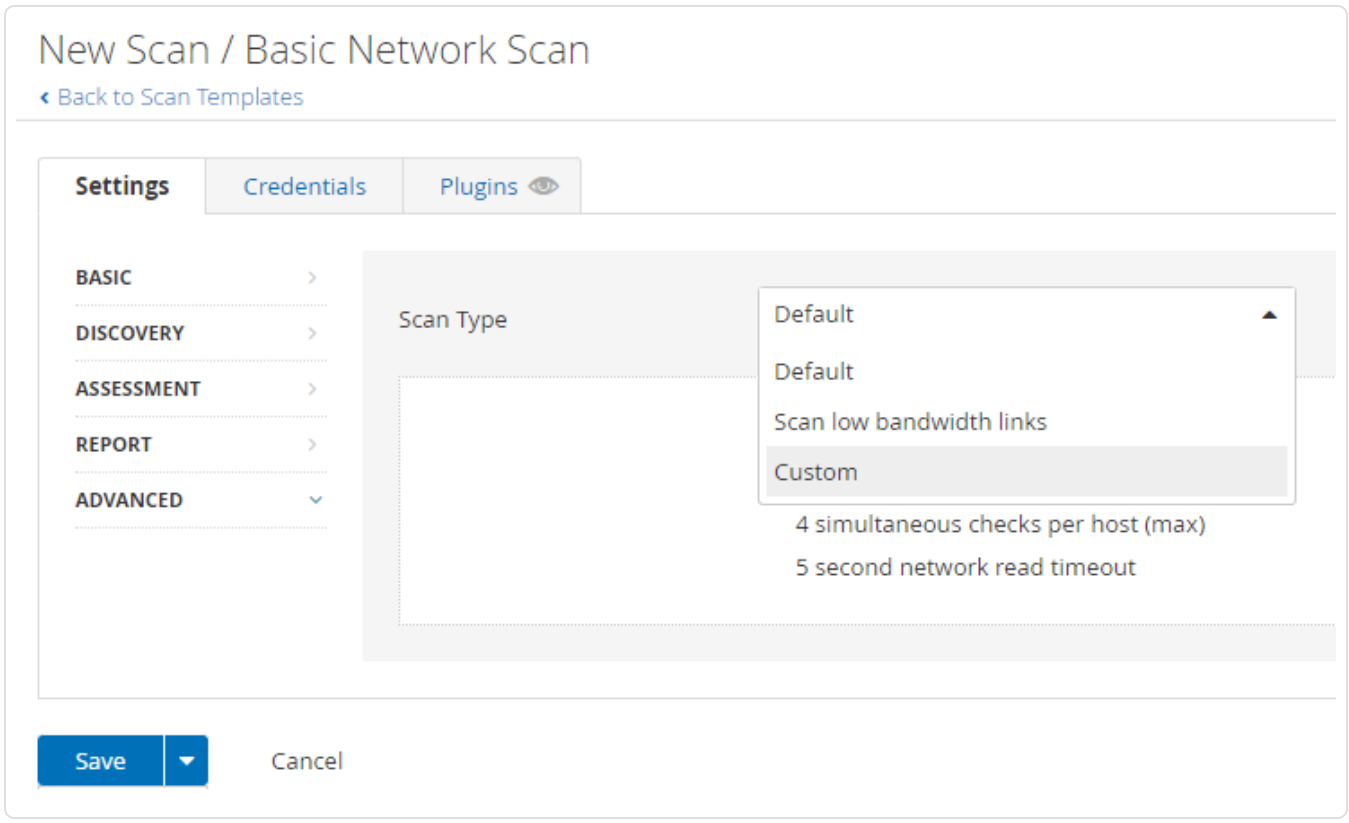
   The **Scan Templates** page appears.

3. Click the scan template that you want to use.

   The **New Scan** page appears.

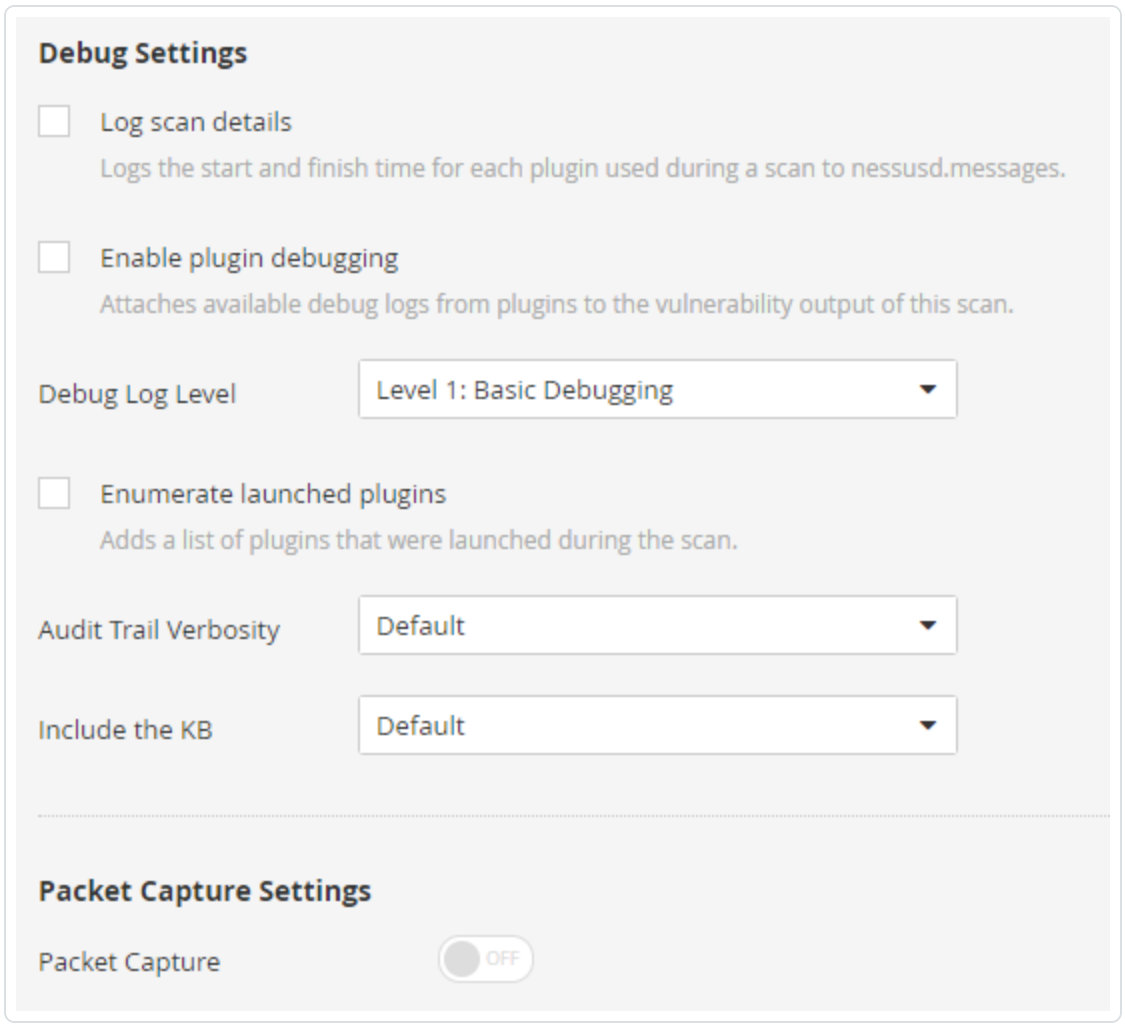
4. Click the **Advanced** settings tab.

5. Select **Custom** from the **Scan Type** drop-down.

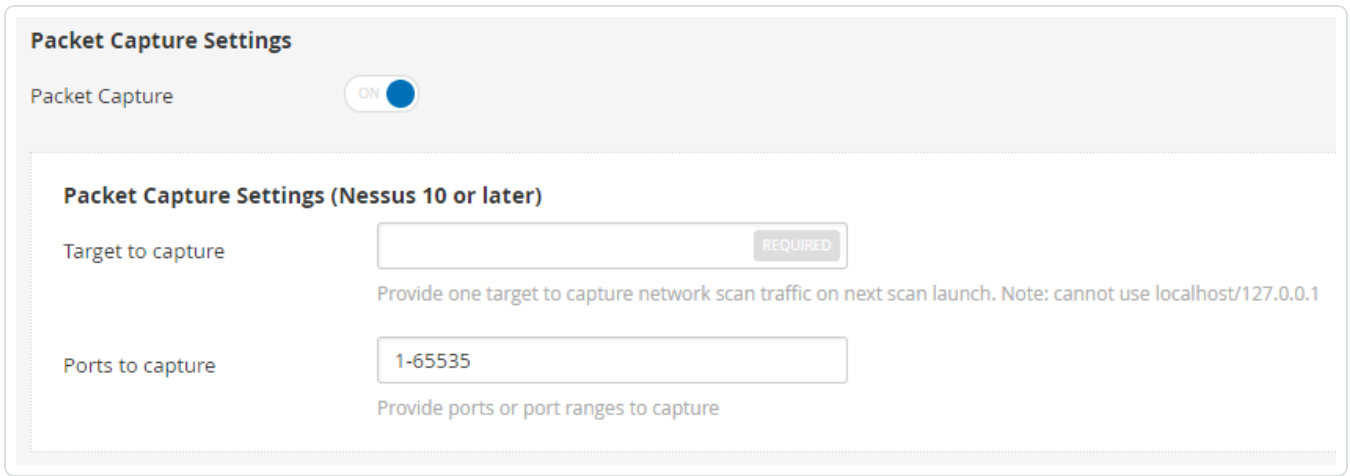


Note: This step is only necessary if you are configuring a Basic Network Scan. If you are configuring an Advanced Network Scan, skip this step.

6. Click **General**.
7. Scroll to the bottom of the **General** settings window and set **Packet Capture** to **ON**.



8. In the **Target to capture** field, enter the IP address or hostname of a single host.



9. In the **Ports to capture** field, enter a port or range of ports.

10. Click the **Save** button.
11. Launch the scan.

To retrieve a packet capture:

After the scan is complete, a compressed archive containing the packet capture will be available for download.

To download the capture:

1. Select **Settings** from the top navigation bar.
2. Select **Debug Logs** from the side navigation bar.

   The **Debug Logs** window will show a list of packet captures. For example, `pcap_SCANNAME_SCANID.zip`.
3. Select the archive that matches your scan.
4. Click the **Download** button.

   The file downloads from the scanner to your local host.

Notifications

Tenable Nessus may periodically show notifications such as login attempts, errors, system information, and license expiration information. These notifications appear after you log in, and you can choose to acknowledge or dismiss each notification.

The following table describes the two ways you can view notifications:

Notification View	Location	Description
Current notifications	The bell icon in the top navigation bar ()	Shows notifications that appeared during this session. When you acknowledge a notification, it no longer appears in your current notification session, but remains listed in the notification history.
Notification history	**Settings** >	Shows all notifications from the past 90

	Notifications	days. The notifications table shows each notification and the time and date it appeared, whether you acknowledged it, the severity, and the message. Unacknowledged notifications appear in bold. You cannot acknowledge a notification from the notification history view.

Use the following procedures to manage notifications:

View notifications

You can view outstanding notifications from your current session, and you can also view a history of notifications from the past 90 days.

To view your current notifications:

In the top navigation bar, click  .

To view your notification history:

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

   The **About** page appears.

2. In the left navigation bar, click **Notifications**.

   The **Notifications** page appears and shows the notifications table.

3. (Optional) Filter or search the notifications to narrow results in the notifications table.

Acknowledge notifications

When you acknowledge a notification, it no longer appears in your current notification session, but remains listed in the notification history. You cannot acknowledge notifications from the notification history view.

If you choose not to acknowledge a notification, it appears the next time you log in. You cannot acknowledge some notifications – instead, you must take the recommended action.

To acknowledge a notification:

- For a notification window, click **Acknowledge**.
- For a notification banner, click **Dismiss**.
- For a notification in the upper-right corner, click 🗑.

To clear current notifications:

1. In the top navigation bar, click  .
2. Click **Clear Notifications**.

> **Note:** Clearing notifications does not acknowledge notifications. It removes them from your current notifications.

Accounts

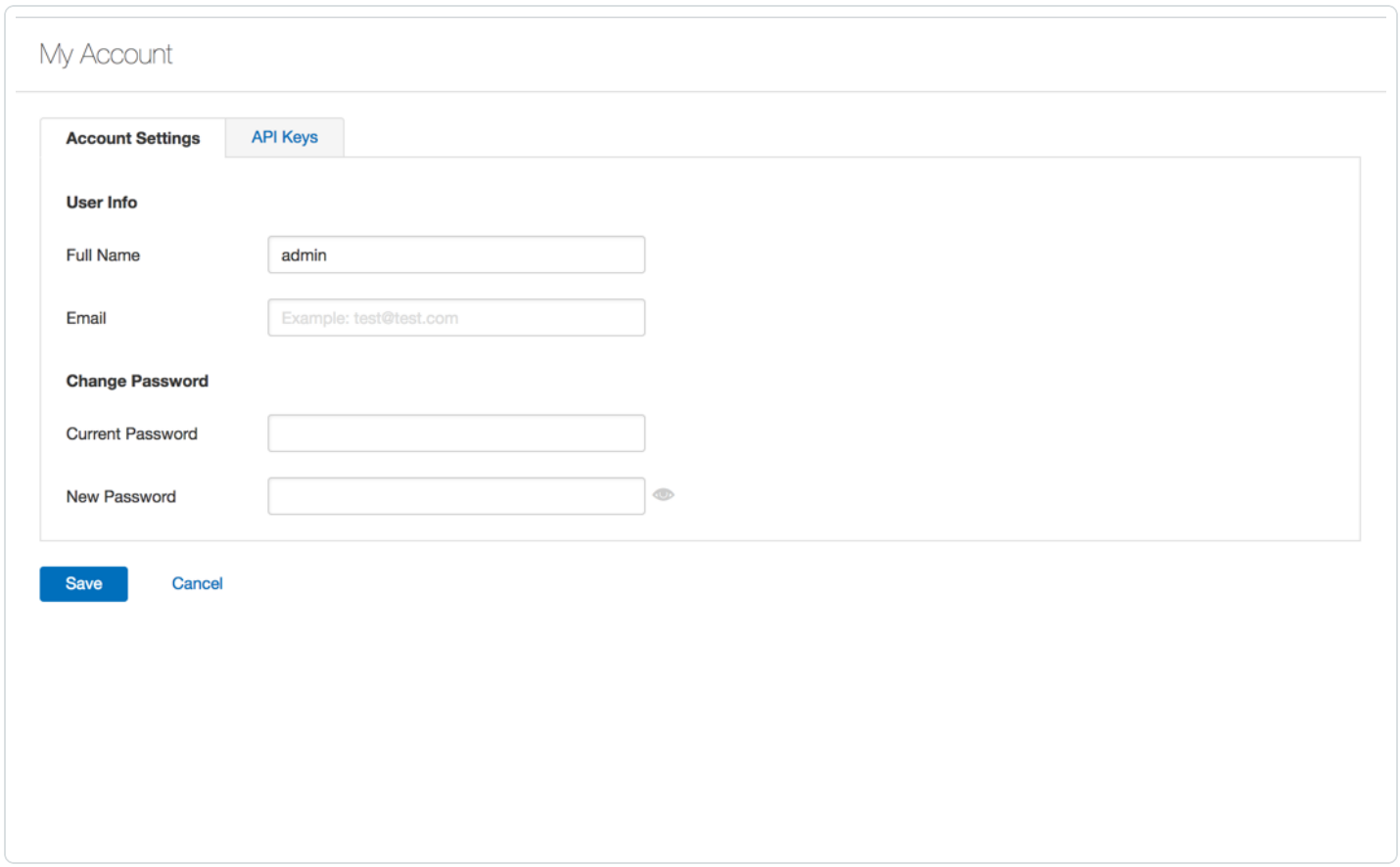
This section contains the following tasks available in the **Accounts** section of the **Settings** page.

- Modify Your User Account
- Generate an API Key
- Create a User Account
- Modify a User Account
- Delete a User Account

My Account

The **Account Settings** page shows settings for the current authenticated user.

> **Note:** Once created, you cannot change a username.



API Keys

An API Key consists of an access key and a secret key. API Keys authenticate with the **Nessus REST API** and pass with requests using the `X-ApiKeys` HTTP header.

Note:

- Nessus only presents API Keys upon initial generation. Store API keys in a safe location.
- Tenable Nessus cannot retrieve API Key. If you lose your API Key, you must generate a new API Key.
- Regenerating an API Key immediately deauthorizes any applications currently using the key.

Modify Your User Account

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

   The **About** page appears.

2. In the left navigation bar, click **My Account**.

The **My Account** page appears.

3. Modify your name, email, or password as needed.

   Note: You cannot modify a username after you create the account.

   Note: Passwords cannot contain Unicode characters.

4. Click **Save**.

   Tenable Nessus saves your account settings.

Generate an API Key

Required user role when using Tenable Nessus Manager: System Administrator

In Tenable Nessus Manager, you can generate an API key from the **API Keys** tab in the Tenable Nessus user interface. Generating an API key can help you automate various tasks and integrate Tenable Nessus with other security tools and systems within your organization. The API key does not expire until you generate a new API key.

In addition to Tenable Nessus Manager, the **API Keys** tab may also be available in Tenable Nessus Professional and Tenable Nessus Expert, depending on your license and configuration. For more information, contact your Tenable Customer Success Manager.

Note: You may not directly access Tenable Nessus scanning APIs to configure or launch scans, except as permitted as part of the Tenable Security Center and Tenable Vulnerability Management enterprise solutions.

Caution: Generating a new API key replaces any existing keys and deauthorizes any linked applications.

To generate an API key:

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **My Account**.

   The **My Account** page appears.

3. Click the **API Keys** tab.

4. Click **Generate**.

   A dialog box appears, confirming your selection to generate a new API key.

5. Click **Generate**.

   Your new API key appears.

   > **Tip:** To access the Tenable Nessus API documentation, navigate to ***<Tenable Nessushost>:<port>/api#/overview***.

Users (Tenable Nessus Manager)

> **Required user role when using Tenable Nessus Manager:** Administrator or System Administrator

> **Note:** The **Users** page is only available in Tenable Nessus Manager. All users in Tenable Nessus Professional, Tenable Nessus Expert, and Tenable Nessus Essentials have System Administrator permissions.

The **Users** page shows a table of all Tenable Nessus Manager user accounts. This documentation refers to that table as the *users table*. Each row of the users table includes the username, the date of the last login, and the role assigned to the account.

User accounts are assigned roles that dictate the level of access a user has in Tenable Nessus Manager. You can disable or change the role of a user account at any time. The following table describes the roles that you can assign to users:

Name	Description
Basic	Basic user can read scan results.
Standard	Standard users can create scans and policies. A scan created by a Standard user cannot be edited by other Standard users unless they are given editing permissions from the scan creator.
Administrator	Administrators have the same privileges as Standard users, but can also manage users, user groups, and scanners and view scans that are shared by other users.
System	System Administrators have the same privileges as Administrators, but

Name	Description
Administrator	can also manage and modify system configuration settings.
Disabled	Disabled user accounts cannot be used to log in to Tenable Nessus.

Use the following procedures to manage user accounts:

Create a user account

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

   The **About** page appears.

2. In the left navigation bar, click **Users**.

   The **Users** page appears.

3. In the upper right corner, click the **New User** button.

   The **Account Settings** tab appears.

4. Type in the settings as necessary, and select a role for the user.

   Note: You cannot modify a username after you save the account.

5. Click **Save**.

   Tenable Nessus saves the user account.

Modify a user account

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

   The **About** page appears.

2. In the left navigation bar, click **Users**.

   The **Users** page appears.

3. In the users table, click the user whose account you want to modify.

   The **<Username>** page appears, where <Username> is the name of the selected user.

4. Modify the user's name, email, role, or password as needed.

Note: You cannot modify a username after you create the account.

Note: Passwords cannot contain Unicode characters.

5. Click **Save**.

   Tenable Nessus saves your account settings.

Delete a user account

1. In Tenable Nessus, in the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **Users**.

   The **Users** page appears.

3. In the users table, in the row for the user that you want to delete, click the ✕ button.

   A dialog box appears, confirming your selection to delete the user.

4. Click **Delete**.

   Tenable Nessus deletes the user.

Transfer user data

In Tenable Nessus Manager, you can transfer a user's data to a system administrator. When you transfer user data, you transfer ownership of all policies, scans, scan results, and plugin rules to a system administrator account. Transferring user data is useful if you need to remove a user account but do not want to lose their associated data in Tenable Nessus.

To transfer user data:

1. Log in to Tenable Nessus with the system administrator account to which you want to transfer user data.

2. In the top navigation bar, click **Settings**.

   The **About** page appears.

3. In the left navigation bar, under **Accounts**, click **Users**.

The **Users** page appears and shows the users table.

4. In the users table, select the check box for each user whose data you want to transfer to your account.
5. In the upper-right corner, click **Transfer Data**.

   A warning window appears.

   > **Note:** Once you transfer user data, you cannot undo the action.

6. To transfer the data, click **Transfer**.

   Tenable Nessus transfers ownership of the selected user's policies, scans, scan results, and plugin rules to the administrator account.

Additional Resources

This section contains the following resources:

- Plugins
- Amazon Web Services
- Command Line Operations
- Configure Tenable Nessus for NIAP Compliance
- Create a Limited Plugin Policy
- Default Data Directories
- Manage Logs
- Tenable Nessus Credentialed Checks
- Offline Update Page Details
- Run Tenable Nessus as Non-Privileged User
- Scan Targets

Amazon Web Services

For information on integrating Tenable Nessus with Amazon Web Services, see the following:

- Tenable Nessus BYOL Scanner on Amazon Web Services
- Link a BYOL Scanner to with Pre-Authorized Scanner Features

Certificates and Certificate Authorities

Tenable Nessus includes the following defaults:

- The default Tenable Nessus SSL certificate and key, which consists of two files: `servercert.pem` and `serverkey.pem`.
- A Tenable Nessus certificate authority (CA), which signs the default Tenable Nessus SSL certificate. The CA consists of two files: `cacert.pem` and `cakey.pem`.

The default certificate files are located in the following directory, depending on your operating system:

Operating System	Directory
Windows	`C:\ProgramData\Tenable\Nessus\nessus\CA`
macOS	`/Library/Nessus/run/com/nessus/CA`
Linux	`/opt/nessus/com/nessus/CA`

However, you may want to upload your own certificates or CAs for advanced configurations or to resolve scanning issues. For more information, see:

- Custom SSL Server Certificates — View an overview of Tenable Nessus SSL server certificates and troubleshoot common certificate problems.
    - Create a New Server Certificate and CA Certificate — If you do not have your own custom CA and server certificate, you can use Tenable Nessus to create a new server certificate and CA certificate.
    - Upload a Custom Server Certificate and CA Certificate — Replace the default certificate that ships with Tenable Nessus.
- Trust a Custom CA — Add a custom root CA to the list of CAs that Tenable Nessus trusts.
- Create SSL Client Certificates for Login — Create an SSL client certificate to log in to Tenable Nessus instead of using a username and password.
- Tenable Nessus Manager Certificates and Tenable Agent — Understand the certificate chain between Tenable Nessus Manager and Tenable Agents and troubleshoot issues.

Custom SSL Server Certificates

By default, Tenable Nessus uses an SSL certificate signed by the Tenable Nessus certificate authority (CA), *Nessus Certification Authority*. During installation, Tenable Nessus creates two files that make up the certificate: `servercert.pem` and `serverkey.pem`. This certificate allows you to access Tenable Nessus over HTTPS through port 8834.

Because Nessus Certification Authority is not a trusted valid certificate authority, the certificate is untrusted, which can result in the following:

- Your browser may produce a warning regarding an unsafe connection when you access Tenable Nessus via HTTPS through port 8834.
- Plugin 51192 may report a vulnerability when scanning the Tenable Nessus scanner host.

To resolve these issues, you can use a custom SSL certificate generated by your organization or a trusted CA.

To configure Tenable Nessus to use custom SSL certificates, see the following:

- Create a New Server Certificate and CA Certificate. — If your organization does not have a custom SSL certificate, create your own using the built-in Tenable Nessus `mkcert` utility.
- Upload a Custom Server Certificate and CA Certificate — Replace the default certificate that ships with Tenable Nessus.
- Trust a Custom CA — Add a custom CA to the list of CAs that Tenable Nessus trusts.

Troubleshooting

To troubleshoot common problems with using the default CA certificate with Tenable Nessus, see the following table:

Problem	Solution
Your browser reports that the Tenable Nessus server certificate is untrusted.	Do any of the following: • Get the Tenable Nessus self-signed certificate signed by a trusted root CA, and upload that trusted CA to your browser. • Use the `/getcert` path to install the root CA in your browsers. Go to the following address in your browser: `https://[IP address]:8834/getcert`. • Upload your own custom certificate and custom CA to your browser: a. Upload a Custom Server Certificate and CA Certificate. b. If Tenable Nessus does not trust the CA for your certificate, configure Tenable Nessus to Trust a Custom CA.

	Note: These workarounds do not work with some browsers. Tenable plans to update Tenable Nessus soon so that all browsers trust Tenable Nessus server certificates. In the meantime, Tenable recommends using a third-party custom server certificate.
Plugin 51192 reports that the Tenable Nessus server certificate is untrusted. For example: • The certificate expired • The certificate is self-signed and therefore untrusted	Do any of the following: • Replace the Tenable Nessus server certificate with one that has been signed by a CA that Tenable Nessus already trusts. • Upload your own custom certificate and custom CA to your browser: a. Upload a Custom Server Certificate and CA Certificate. b. If Tenable Nessus does not trust the CA for your certificate, configure Tenable Nessus to Trust a Custom CA.
Plugin 51192 reports that an unknown CA was found at the top of the certificate chain.	Add your custom root CA to the list of CAs that Tenable Nessus trusts, as described in Trust a Custom CA.

Create a New Server Certificate and CA Certificate

If you do not have your own custom certificate authority (CA) and server certificate (for example, a trusted certificate that your organization uses), you can use Tenable Nessus to create a new server certificate and CA certificate.

The Tenable Nessus CA signs this server certificate, which means your browser may report that the server certificate is untrusted.

Note: You need to be an administrator user or have root privileges to create a new custom CA and server certificate.

Note: The following steps are applicable to both Tenable Nessus scanners and Tenable Nessus Manager.

To create a new custom CA and server certificate:

1. Access the Tenable Nessus CLI as an administrator user or a user with root privileges.
2. Run the `nessuscli mkcert` command:

   Linux

   ```
   # /opt/nessus/sbin/nessuscli mkcert
   ```

   Windows

   ```
   C:\Program Files\Tenable\Nessus\nessuscli.exe mkcert
   ```

   macOS

   ```
   # /Library/Nessus/run/sbin/nessuscli mkcert
   ```

   This command places the certificates in their correct directories.
3. When prompted for the hostname, enter the DNS name or IP address of the Tenable Nessus server in the browser such as https://hostname:8834/ or https://ipaddress:8834/. The default certificate uses the hostname.

What to do next:

- Because Nessus Certification Authority is not a trusted valid certificate authority, the certificate is untrusted, which can result in the following:
  - Your browser may produce a warning regarding an unsafe connection when you access Tenable Nessus via HTTPS through port 8834.
  - Plugin 51192 may report a vulnerability when scanning the Tenable Nessus scanner host.

  To resolve either of those issues, Trust a Custom CA. For more information about how Tenable Nessus uses custom SSL server certificates and CAs, see Custom SSL Server Certificates.

Upload a Custom Server Certificate and CA Certificate

These steps describe how to upload a custom server certificate and certificate authority (CA) certificate to the Nessus web server through the command line.

You can use the `nessuscli import-certs` command to validate the server key, server certificate, and CA certificate, check that they match, and copy the files to the correct locations. Alternatively, you can manually copy the files.

Before you begin:

- Ensure you have a valid server certificate and custom CA. If you do not already have your own, create a custom CA and server certificate using the built-in Tenable Nessus `mkcert` utility.

To upload a custom CA certificate using a single command:

1. Access Tenable Nessus from the CLI.
2. Type the following, replacing the server key, server certificate, and CA certificate with the appropriate path and file names for each file.

   ```
   nessuscli import-certs --serverkey=<server key path> --servercert=<server certificate path> --cacert=<CA certificate path>
   ```

   Tenable Nessus validates the files, checks that they match, and copies the files to the correct locations.

To upload a custom server certificate and CA certificate manually using the CLI:

1. Stop the Nessus server.
2. Back up the original Nessus CA and server certificates and keys.

   Tip: For the location of the default certificate files for your operating system, see The default certificate files are located in the following directory, depending on your operating system:.

   Linux example

   ```
   cp /opt/nessus/com/nessus/CA/cacert.pem /opt/nessus/com/nessus/CA/cacert.pem.orig
   cp /opt/nessus/var/nessus/CA/cakey.pem /opt/nessus/var/nessus/CA/cakey.pem.orig
   cp /opt/nessus/com/nessus/CA/servercert.pem
   /opt/nessus/com/nessus/CA/servercert.pem.orig
   ```

```
cp /opt/nessus/var/nessus/CA/serverkey.pem
/opt/nessus/var/nessus/CA/serverkey.pem.orig
```

Windows example

```
copy C:\ProgramData\Tenable\Nessus\nessus\CA\cacert.pem
C:\ProgramData\Tenable\Nessus\nessus\CA\cacert.pem.orig
copy C:\ProgramData\Tenable\Nessus\nessus\CA\cakey.pem
C:\ProgramData\Tenable\Nessus\nessus\CA\cakey.pem.orig
copy C:\ProgramData\Tenable\Nessus\nessus\CA\servercert.pem
C:\ProgramData\Tenable\Nessus\nessus\CA\servercert.pem.orig
copy C:\ProgramData\Tenable\Nessus\nessus\CA\serverkey.pem
C:\ProgramData\Tenable\Nessus\nessus\CA\serverkey.pem.orig
```

macOS example

```
cp /Library/NessusAgent/run/com/nessus/CA/cacert.pem
/Library/NessusAgent/run/com/nessus/CA/cacert.pem.orig
cp /Library/NessusAgent/run/var/nessus/CA/cakey.pem
/Library/NessusAgent/run/var/nessus/CA/cakey.pem.orig
cp /Library/NessusAgent/run/com/nessus/CA/servercert.pem
/Library/NessusAgent/run/com/nessus/CA/servercert.pem.orig
cp /Library/NessusAgent/run/var/nessus/CA/serverkey.pem
/Library/NessusAgent/run/var/nessus/CA/serverkey.pem.orig
```

3. Replace the original certificates with the new custom certificates:

Note: The certificates must be unencrypted, and you must name them `servercert.pem` and `serverkey.pem`.

Note: If your certificate does not link directly to the root certificate, add an intermediate certificate chain, a file named `serverchain.pem`, in the same directory as the `servercert.pem` file. This file contains the 1-n intermediate certificates (concatenated public certificates) necessary to construct the full certificate chain from the Nessus server to its ultimate root certificate (one trusted by the user's browser).

Linux example

```
cp customCA.pem /opt/nessus/com/nessus/CA/cacert.pem
cp cakey.pem /opt/nessus/var/nessus/CA/cakey.pem
cp servercert.pem /opt/nessus/com/nessus/CA/servercert.pem
cp serverkey.pem /opt/nessus/var/nessus/CA/serverkey.pem
```

Windows example

```
copy customCA.pem C:\ProgramData\Tenable\Nessus\nessus\CA\cacert.pem
copy cakey.pem C:\ProgramData\Tenable\Nessus\nessus\CA\cakey.pem
copy servercert.pem C:\ProgramData\Tenable\Nessus\nessus\CA\servercert.pem
copy serverkey.pem C:\ProgramData\Tenable\Nessus\nessus\CA\serverkey.pem
```

macOS example

```
cp customCA.pem /Library/NessusAgent/run/com/nessus/CA/cacert.pem
cp cakey.pem /Library/NessusAgent/run/var/nessus/CA/cakey.pem
cp servercert.pem /Library/NessusAgent/run/com/nessus/CA/servercert.pem
cp serverkey.pem /Library/NessusAgent/run/var/nessus/CA/serverkey.pem
```

4. If prompted, overwrite the existing files.
5. Start the Tenable Nessus server.
6. In a browser, log in to the Tenable Nessus user interface as a user with administrator permissions.
7. When prompted, verify the new certificate details.

   Subsequent connections should not show a warning if a browser-trusted CA generated the certificate.

What to do next:

- If Tenable Nessus does not already trust the CA, configure Tenable Nessus to Trust a Custom CA.

Trust a Custom CA

Required user role when using Tenable Nessus Manager: System Administrator

By default, Tenable Nessus trusts certificate authorities (CAs) based on root certificates in the *Mozilla Included CA Certificate* list. Tenable Nessus lists the trusted CAs in the `known_CA.inc` file in the Tenable Nessus directory. Tenable updates `known_CA.inc` when updating plugins.

If you have a custom root CA that is not included in the known CAs, you can configure Tenable Nessus to trust the custom CA to use for certificate authentication.

You can use either the Tenable Nessus user interface or the command-line interface (CLI).

Note: You can also configure individual scans to trust certain CAs. For more information, see Trusted CAs.

Note: For information about using custom SSL certificates, see Create SSL Client Certificates for Login.

Note: `known_CA.inc` and `custom_CA.inc` are used for trusting certificates in your network, and are not used for Nessus SSL authentication.

Before you begin:

- If your organization does not already have a custom CA, use Tenable Nessus to create a new custom CA and server certificate, as described in Create a New Server Certificate and CA Certificate.
- Ensure your CA is in PEM (Base64) format.

To configure Tenable Nessus to trust a custom CA using the Tenable Nessus user interface:

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

   The **About** page appears.

2. In the left navigation bar, click **Custom CA**.

   The **Custom CA** page appears.

3. In the **Certificate** box, enter the text of your custom CA.

> **Note:** Include the beginning text `-----BEGIN CERTIFICATE-----` and ending text `-----END CERTIFICATE-----`.

> **Tip:** You can save more than one certificate in a single text file, including the beginning and ending text for each one.

4. Click **Save**.

   The CA is available for use in Nessus.

To configure Tenable Nessus to trust a custom CA using the CLI:

1. Save your PEM-formatted CA as a text file.

   > **Note:** Include the beginning text `-----BEGIN CERTIFICATE-----` and ending text `-----END CERTIFICATE-----`.

   > **Tip:** You can save more than one certificate in a single text file, including the beginning and ending text for each one.

2. Rename the file `custom_CA.inc`.

3. Move the file to your plugins directory:

   Linux

   `/opt/nessus/lib/nessus/plugins`

   Windows

   `C:\ProgramData\Tenable\Nessus\nessus\plugins`

   macOS

   `/Library/Nessus/run/lib/nessus/plugins`

   The CA is available for use in Nessus.

Create SSL Client Certificates for Login

You can configure Tenable Nessus to use SSL client certificate authentication for users to log in to Tenable Nessus when accessing Tenable Nessus on port 8834. After you enable certificate authentication, you can no longer log in using a username and password.

Caution: Tenable Nessus does not support connecting agents, remote scanners, or managed scanners after you enable SSL client certificate authentication. Configure an alternate port to enable supporting remote agents and scanners using the advanced setting `remote_listen_port`. For more information, see Advanced Settings.

If you configure SSL client certificate authentication, Tenable Nessus also supports:

- Smart cards
- Personal identity verification (PIV) cards
- Common Access Cards (CAC)

To configure SSL client certificate authentication for Tenable Nessus user accounts:

1. Access the Tenable Nessus CLI as an administrator user or a user with equivalent privileges.
2. Create a client certificate for each user you want to be able to log in to Tenable Nessus via SSL authentication.
    a. On the Tenable Nessus server, run the `nessuscli mkcert-client` command.

    Linux

    ```
    # /opt/nessus/sbin/nessuscli mkcert-client
    ```

    macOS

    ```
    # /Library/Nessus/run/sbin/nessuscli mkcert-client
    ```

    Windows

    ```
    C:\Program Files\Tenable\Nessus\nessuscli.exe mkcert-client
    ```

    b. Complete the fields as prompted.

> **Note:** The answers you provided in the initial prompts remain as defaults if you create subsequent client certificates during the same session. However, you can change the values for each client certificate you create.

Tenable Nessus creates the client certificates and places them in the Tenable Nessus temporary directory:

- Linux: `/opt/nessus/var/nessus/tmp/`
- macOS: `/Library/Nessus/run/var/nessus/tmp/`
- Windows: `C:\ProgramData\Tenable\Nessus\tmp`

c. Combine the two files (the certificate and the key) and export them into a format that you can import into the browser, such as `.pfx`.

In the previous example, the two files were *`key_sylvester`*`.pem` and *`cert_sylvester.pem`*.

For example, you can combine the two files by using the `openssl` program and the following command:

```
# openssl pkcs12 -export -out combined_sylvester.pfx -inkey key_sylvester.pem
-in cert_sylvester.pem -chain -CAfile /opt/nessus/com/nessus/CA/cacert.pem -
passout 'pass:password' -name 'Nessus User Certificate for: sylvester'
```

Tenable Nessus creates the resulting file `combined_sylvester.pfx` in the directory where you launched the command.

3. Upload the certificate to your browser's personal certificate store.

   Refer to the documentation for your browser.

4. Set Tenable Nessus to allow SSL client certificate authentication.

   Linux

   ```
   # /opt/nessus/sbin/nessuscli fix --set force_pubkey_auth=yes
   ```

   Windows

```
C:\Program Files\Tenable\Nessus\nessuscli.exe fix --set force_pubkey_
auth=yes
```

macOS

```
# /Library/Nessus/run/sbin/nessuscli fix --set force_pubkey_auth=yes
```

5. Log in to Tenable Nessus via `https://<Tenable Nessus IP address or hostname>:8834` and select the username you created.

What to do next:

- If you are using a custom CA, configure Tenable Nessus plugins to trust certificates from your CA, as described in Trust a Custom CA.

Tenable Nessus Manager Certificates and Tenable Agent

When you link an agent to Tenable Nessus Manager, you can optionally specify the certificate that the agent should use when it links with Tenable Nessus Manager. This allows the agent to verify the server certificate from Tenable Nessus Manager when the agent links with Tenable Nessus Manager, and secures subsequent communication between the agent and Tenable Nessus Manager. For more information on linking Tenable Agent, see Nessuscli.

If you do not specify the certificate authority (CA) certificate at link time, the agent receives and trusts the CA certificate from the linked Tenable Nessus Manager. This ensures that subsequent communication between the agent and Tenable Nessus Manager is secure.

> **Note:** If you use a self-signed or untrusted certificate for your Tenable Nessus Manager certificate, it needs to be trusted by any linked agents. Otherwise, the agents lose connection to Tenable Nessus Manager. For more information, see Trust a Custom CA.

The CA certificate the agent receives at linking time saves in the following location:

Linux

```
/opt/nessus_agent/var/nessus/users/nessus_ms_agent/ms_cert.pem
```

Windows

```
C:\ProgramData\Tenable\Nessus Agent\nessus\users\nessus_ms_agent\ms_cert.pem
```

macOS

`/Library/NessusAgent/run/var/nessus/users/nessus_ms_agent/`

Troubleshooting

If the agent cannot follow the complete certificate chain, an error occurs and the agent stops connecting with the manager. You can see an example of this event in the following sensor logs:

- **nessusd.messages** - Example: Server certificate validation failed: unable to get local issuer certificate
- **backend.log** - Example: [error][msmanager] SSL error encountered when negotiating with <Manager_IP>:<PORT>. Code 336134278, unable to get local issuer certificate, error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed

Scenario: Agent can't communicate to manager due to broken certificate chain

A common reason your certificate chain may break is that you change the server certificate on Tenable Nessus Manager but do not update the CA certificate. The agent is then unable to communicate to the manager upon restart. To resolve this issue, do one of the following:

- Unlink and relink the agent to Tenable Nessus Manager, which resets the certificate so the agent gets the correct CA certificate from Tenable Nessus Manager.
- Manually upload the correct `cacert.pem` file from Tenable Nessus Manager into the `custom_CA.inc` file in the agent plugin directory:
  - **Linux**

    `/opt/nessus_agent/lib/nessus/plugins`
  - **Windows**

    `C:\ProgramData\Tenable\Nessus Agent\nessus\plugins`
  - **macOS**

    `/Library/NessusAgent/run/lib/nessus/plugins`

- Generate a new server certificate on Tenable Nessus Manager using the CA for which the agent already has the CA certificate, so that the certificate chain is still valid.

Command Line Operations

This section includes command line operations for Tenable Nessus and Tenable Agents.

Tip: During command line operations, prompts for sensitive information, such as a password, do not show characters as you type. However, the command line records the data and accepts it when you press the **Enter** key.

This section includes the following topics:

- Start or Stop Tenable Nessus
- Start or Stop Tenable Agent
- Nessus-Service
- Nessuscli
- Nessuscli Agent
- Update Tenable Nessus Software (CLI)

Start or Stop Tenable Nessus

The following represent best practices for starting and stopping the Nessus service on your machine.

Note: This topic refers to starting or stopping the Nessus service that runs on host machines. To launch or stop an individual scan, see Launch a Scan and Stop a Running Scan.

Windows

1. Navigate to **Services**.
2. In the **Name** column, click **Tenable Nessus**.
3. Do one of the following:

- To stop the **Nessus** service, right-click **Tenable Nessus**, and then click **Stop**.
- To restart the **Nessus** service, right-click **Tenable Nessus**, and then click **Start**.

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

Note: You must have root permissions to run the start and stop commands.

Linux

Use the following commands:

Start or Stop	Linux Command-Line Operation
RedHat, CentOS, and Oracle Linux	
Start	`# systemctl start nessusd`
Stop	`# systemctl stop nessusd`
SUSE	
Start	`# systemctl start nessusd`
Stop	`# systemctl stop nessusd`
Debian, Kali, and Ubuntu	
Start	`# systemctl start nessusd`
Stop	`# systemctl stop nessusd`

Note: You must have root permissions to run the start and stop commands.

macOS

1. Navigate to **System Preferences**.
2. Click the button.
3. Click the button.
4. Type your username and password.
5. Do one of the following:
    - To stop the Nessus service, click the **Stop Nessus** button.
    - To start the Nessus service, click the **Start Nessus** button.

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

Note: You must have root permissions to run the start and stop commands.

Start or Stop a Tenable Agent

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`

Nessus-Service

If necessary, whenever possible, you should start and stop Tenable Nessus services using Tenable Nessus service controls in your operating system's interface.

However, there are many **nessus-service** functions that you can perform through a command line interface.

Unless otherwise specified, you can use the **nessusd** command interchangeably with **nessus-service** server commands.

You can use the **# killall nessusd** command to stop all Tenable Nessus services and in-process scans.

Note: You must have administrative privileges to run the following commands.

Nessus-Service Syntax

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

Nessusd Commands

Option	Description
-c <config-file>	When starting the **nessusd** server, this option specifies 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, this option specifies the source IP of Tenable Nessus during scanning. This setting relates to the source IP address of the device that hosts Tenable Nessus, not the scan target IP address. This option is only useful if you have a multi-homed 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

Option	Description
	these IP addresses set.
-D	When starting the `nessusd` server, this option forces the server to run in the background (daemon mode).
-v	Show the version number and exit.
-l	Show a list of those third-party software licenses.
-h	Show a summary of the commands and exit.
--ipv4-only	Only listen on the IPv4 socket.
--ipv6-only	Only listen on the IPv6 socket.
-q	Operate in "quiet" mode, suppressing all messages to `stdout`.
-R	Force a reprocessing of the plugins.
-t	Check the time stamp of each plugin when starting up to compile newly updated plugins only.
-K	Set a parent password for the scanner. If you set a parent password, Tenable Nessus encrypts all policies and credentials contained in the policy. When you set a password, the Tenable Nessus user interface prompts you for the password. **Caution:** If you set your parent password and lose it, neither your administrator nor Tenable Support can recover it.

Suppress Command Output Example

You can suppress command output by using the **-q** option. For example:

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

Considerations

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, run the following command:

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

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

Nessuscli

You can administer some Tenable Nessus functions through a command-line interface (CLI) using the `nessuscli` utility.

This allows the user to manage user accounts, modify advanced settings, manage digital certificates, report bugs, update Tenable Nessus, and fetch necessary license information.

Note: You must run all commands with administrative privileges.

Nessuscli Syntax

Operating System	Command
Windows	`C:\Program Files\Tenable\Nessus\nessuscli.exe <cmd> <arg1> <arg2>`
macOS	`# /Library/Nessus/run/sbin/nessuscli <cmd> <arg1> <arg2>`
Linux	`# /opt/nessus/sbin/nessuscli <cmd> <arg1> <arg2>`

This topic describes the following command types:

- Help Commands
- System Commands
- Backup Commands

- Bug Reporting Commands
- User Commands
- Fetch Commands
- Fix Commands
- Certificate Commands
- Software Update Commands
- Manager Commands
- Managed Scanner Commands
- Web Application Scanning Command
- Dump Command
- Node Commands

Nessuscli Commands

Command	Description
Help Commands	
`nessuscli help`	Shows a list of Tenable Nessus commands. The help output may vary, depending on your Tenable Nessus license.
`nessuscli <cmd> help`	Shows more help information for specific commands identified in the nessuscli help output.
System Commands	
`nessuscli system --config-optimization`	Optimizes the size and structure of your global configuration database. This optimization typically lasts for a few seconds. However, in cases such as a Tenable Nessus Manager that manages many agents, the process can take a few minutes. You must stop Tenable Nessus before running this command.

Command	Description
Backup Commands	
`nessuscli backup --create <backup_filename>`	Creates a backup file of your Tenable Nessus instance, which includes your license and settings, and appends it with *<Unix epoch timestamp>*.zip. The command does not back up scan results. Example: If you run `nessuscli backup --create <december-backup>`, Tenable Nessus creates the following backup file: *december-backup.1671720758.zip*. For more information, see Back Up Tenable Nessus.
`nessuscli backup --restore <path/to/backup_filename>`	Restores a previously saved backup of Tenable Nessus. For more information, see Restore Tenable Nessus.
Bug Reporting Commands The bug reporting commands create an archive that you can send to Tenable, Inc. to help diagnose issues. By default, the script runs in interactive mode.	
`nessuscli bug-report-generator`	Generates an archive of system diagnostics. Running this command without arguments prompts for values. `--quiet:` run the bug report generator without prompting user for feedback. `--scrub:` when in quiet mode, bug report generator sanitizes the last two octets of the IPv4 address. `--full:` when in quiet mode, bug report generator collects extra data.
User Commands	
`nessuscli rmuser`	Allows you to remove a Tenable Nessus user.

Command	Description
<username>	
`nessuscli chpasswd` *<username>*	Allows you to change a user's password. The CLI prompts to enter the Tenable Nessus user's name. The CLI does not echo passwords on the screen.
`nessuscli adduser` *<username>*	Allows you to add a Tenable Nessus user account. The CLI prompts you for a username, password, and opted to allow the user to have an administrator type account. Also, the CLI prompts to add Users Rules for this new user account. **Note:** If this is your first time creating a user with this command in your Tenable Nessus Manager instance, Tenable recommends restarting Tenable Nessus to ensure that the user interface properly updates with the new user's information.
`nessuscli lsuser`	Shows a list of Tenable Nessus users.
Fetch Commands Manage Tenable Nessus registration and fetch updates	
`nessuscli fetch --register` *<Activation Code>*	Uses your Activation Code to register Tenable Nessus online. Example: `# /opt/nessus/sbin/nessuscli fetch --register` *xxxx-xxxx-xxxx-xxxx*
`nessuscli fetch --register-only` *<Activation Code>*	Uses your Activation Code to register Tenable Nessus online, but does not automatically download plugin or core updates. Example: `# /opt/nessus/sbin/nessuscli fetch --register-only` *xxxx-xxxx-xxxx-xxxx*
`nessuscli fetch --`	Registers Tenable Nessus with the nessus.license file

Command	Description
`register-offline nessus.license`	obtained from https://plugins.nessus.org/v2/offline.php and sets Tenable Nessus in offline mode. **Caution:** Starting Tenable Nessus in offline mode disables all `nessuscli` commands that require connection to the Tenable Nessus feed (for example, `nessuscli update` and `nessuscli fix --set_scanner_update_channel=`). If Tenable Nessus is in offline mode, you cannot use a `fix` command to deactivate offline mode.
`nessuscli fetch --check`	Shows whether Tenable Nessus is properly registered and is able to receive updates.
`nessuscli fetch --code-in-use`	Shows the Activation Code that Tenable Nessus is using.
`nessuscli fetch --challenge`	Shows the challenge code needed to use when performing an offline registration. Example challenge code: aaaaaa11b2222cc33d44e5f6666a777b8cc99999
`nessuscli fetch --security-center`	Prepares Tenable Nessus to be connected to Tenable Security Center. **Caution:** *Do not use this command if you do not want to switch your Tenable Nessus instance to Tenable Security Center.* This command irreversibly changes the Tenable Nessus scanner or Manager to a Tenable Security Center-managed scanner, resulting in several user interface changes (for example, the site logo changes, and you do not have access to the **Sensors** page).
Fix Commands	

Command	Description
`nessuscli fix`	Reset registration, show network interfaces, and list advanced settings that you have set. Using the `--secure` option acts on the encrypted preferences, which contain information about registration. You can use `--list`, `--set`, `--get`, and `--delete` to modify or view preferences.
`nessuscli fix [--secure] --list`	
`nessuscli fix [--secure] --set <setting=value>`	
`nessuscli fix [--secure] --get <setting>`	
`nessuscli fix [--secure] --delete <setting>`	
`nessuscli fix --list-interfaces`	List the network adapters on this machine.
`nessuscli fix --set listen_address=<address>`	Tell the server to only listen to connections on the address `<address>` that is an IP, not a machine name. This option is useful if you are running nessusd on a gateway and if you do not want people on the outside to connect to your nessusd.
`nessuscli fix --show`	List all advanced settings, including those you have not set. If you have not set an advanced setting, the CLI shows the default value. **Note:** This command only lists settings that are shared by all Tenable Nessus license types. In other words, the command does not list any settings specific to Tenable Nessus Expert, Tenable Nessus Professional, or Tenable Nessus Manager.
`nessuscli fix --reset`	This command deletes all your registration information and preferences, causing Tenable Nessus to run in a non-registered state. Tenable Nessus Manager retains the same linking key after resetting. Before running `nessuscli fix --reset`, verify running scans have completed, then stop the nessusd daemon or

Command	Description
	service, as described in Start or Stop Tenable Nessus.
`nessuscli fix --reset-all`	This command resets Tenable Nessus to a fresh state, deleting all registration information, settings, data, and users. **Caution:** You cannot undo this action. Contact Tenable Support before performing a full reset.
`nessuscli fix --set agent_update_channel=<value>`	(Tenable Nessus Manager-linked agents only) Sets the agent update plan to determine what version the agent automatically updates to. Values: • **ga** — Automatically updates to the latest Tenable Agent version when it is made generally available (GA). • **ea** — Automatically updates to the latest Tenable Nessus 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 Nessus version. Remains on an earlier version of Tenable Nessus set by Tenable, usually one release older than the current generally available version, but no earlier than 8.10.0. When Tenable Nessus releases a new version, your Tenable Nessus instance updates software versions, but stays on a version prior to the latest release. **Note:** For agents linked to Tenable Nessus Manager, you need to run the `agent_update_channel` command from the Tenable Nessus Manager `nessuscli` utility. For agents linked to Tenable Vulnerability Management, you need to run the `agent_update_channel` command from the agent `nessuscli` utility.

Command	Description
`nessuscli fix --secure --get agent_linking_key`	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.
`nessuscli fix --secure --get child_node_linking_key`	Retrieve your unique child node linking key. **Note**: You can only use this linking key to link a child node. You cannot use it to link an agent or a scanner.
`nessuscli fix --secure --get scanner_linking_key`	Retrieve your unique scanner linking key. **Note**: You can only use this linking key to link a scanner. You cannot use it to link an agent or a child node.
`nessuscli fix --set niap_mode=enforcing`	Enforces NIAP mode for Tenable Nessus. For more information about NIAP mode, see Configure Tenable Nessus for NIAP Compliance.
`nessuscli fix --set niap_mode=non-enforcing`	Disables NIAP mode for Tenable Nessus. For more information about NIAP mode, see Configure Tenable Nessus for NIAP Compliance.
`nessuscli fix --set fips_mode=enforcing`	Enforces the current validated FIPS module for Tenable Nessus communication and database encryption. The FIPS module does not affect scanning encryption. **Note:** Tenable Nessus also enforces the FIPS module when you enforce NIAP mode. For more information, see Configure Tenable Nessus for NIAP Compliance.
`nessuscli fix --set fips_mode=non-enforcing`	Disables the FIPS module for Tenable Nessus communication and database encryption. **Note:** Tenable Nessus also disables the FIPS module when you disable NIAP mode. For more information, see Configure Tenable Nessus for NIAP Compliance.

Command	Description
`nessuscli fix --set path_to_java=<custom file path>`	Sets a custom file path to Java for PDF exports. If not set, Tenable Nessus uses the system path. You must use an absolute file path that contains the Java binary. For example, if the Tenable Nessus installation is in `/usr/lib/jvm/java-17-openjdk-amd64`, the custom file path must be **`/usr/lib/jvm/java-17-openjdk-amd64/bin`**.
`nessuscli fix --set global.path_to_docker=<custom path>`	Sets the custom file path to Docker for web application scans in Tenable Nessus Expert. Tenable Nessus Expert uses the Docker system path by default (for example, `/usr/bin/docker`). You must use an absolute file path.
`nessuscli fix --set old_user_files_cleanup_hours=`	Sets the interval of time, in hours, after which Tenable Nessus deletes old user files (located in the `/nessus/users/<user>/files` directory). You may find this setting useful if you are experiencing scan errors due to an excess of user files. The default and minimum value for this setting is **0**. The setting does not have a maximum value. When the setting is set to zero, Tenable Nessus does not perform the file cleanup.
`nessuscli fix --set <password_setting>=<value>`	Sets parameters and limitations for user passwords. You can use this command to edit the following settings: • **Password Complexity** (`passwd_complexity`)– Determines whether Tenable Nessus passwords must have a minimum of eight characters, and at least three of the following: an upper case letter, a lower case letter, a special character, and a number. This setting is turned off by default.

Command	Description
	• **Session Timeout** (`xmlrpc_idle_session_timeout`)— Defines the web session timeout in minutes. Tenable Nessus logs users out automatically if their session is idle for longer than this timeout value. This setting is set to 30 by default. • **Max Login Attempts** (`user_max_login_attempt`) — Defines the maximum number of user login attempts allowed by Tenable Nessus before the application locks the account out. Setting this value to 0 disables this feature. This setting is set to 5 by default. • **Min Password Length** (`min_password_len`) — This setting is set to 8 by default. Defines the minimum number of characters for passwords of accounts. • **Login Notifications** (`passwd_notifications`) — Determines whether Tenable Nessus can see login notifications. Login notifications allow the user to see the last successful login and failed login attempts (date, time, and IP), and if any failed login attempts have occurred since the last successful login. This setting is turned off by default. **Note:** You need the System Administrator role to configure password settings. For more information, see Users (Tenable Nessus Manager). **Tip:** You can also manage these settings on the **Password Management** page. To view the default and valid values of each password settings, see Password Management.
Certificate Commands	
`nessuscli mkcert-client`	Creates a certificate for the Tenable Nessus server.
`nessuscli mkcert [-q]`	Creates a certificate with default values.

Command	Description
	`-q` for quiet creation.
`nessuscli import-certs --serverkey=<server key path> --servercert=<server certificate path> --cacert=<CA certificate path> [--serverchain=<server chain pem path>]`	Validates the server key, server certificate, the CA certificate, and the `serverchain.pem` file and checks that they match. Then, copies the files to the correct locations. The `serverchain` parameter is optional.
Software Update Commands	
`nessuscli update`	By default, this tool updates based on the software update options selected through the Tenable Nessus user interface. **Note**: This command only works for standalone Tenable Nessus scanners. The command does not work for scanners managed by Tenable Vulnerability Management or Tenable Security Center.
`nessuscli update --all`	Forces updates for all Tenable Nessus components. **Note**: This command only works for standalone Tenable Nessus scanners. The command does not work for scanners managed by Tenable Vulnerability Management or Tenable Security Center.
`nessuscli update --plugins-only`	Forces updates for Tenable Nessus plugins only. **Note**: This command only works for standalone Tenable Nessus scanners. The command does not work for scanners managed by Tenable Vulnerability Management or Tenable Security Center.
`nessuscli update <tar.gz filename>`	Updates Tenable Nessus plugins by using a TAR file instead of getting the updates from the plugin feed. You obtain the

Command	Description
	TAR file when you Manage Tenable Nessus Offline - Download and Copy Plugins steps.
`nessuscli update <tar.gz filename> --agent-version`	(Tenable Nessus Manager only) Adds the agent version of the tar.gz file to the **Agent Profiles** menu to be selectable while creating or updating agent profiles. For more information, see Agent Profiles.
`nessuscli fix --set scanner_update_channel=<value>`	(Tenable Nessus Professional and Tenable Vulnerability Management-managed scanners only) Sets the Tenable Nessus to determine what version Tenable Nessus automatically updates to. **Note:** If you change your update plan and have automatic updates enabled, Tenable Nessus may immediately update to align with the version represented by your selected plan. Tenable Nessus may either upgrade or downgrade versions. Values: • **ga** — Automatically updates to the latest Tenable Nessus version when it is made generally available (GA). **Note:** This date is the same day the version is made generally available. • **ea** — Automatically updates to the latest Tenable Nessus 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 Nessus version. Remains on an earlier version of Tenable Nessus set by Tenable, usually one release older than the current generally available version, but

Command	Description
	no earlier than 8.10.0. When Tenable Nessus releases a new version, your Tenable Nessus instance updates software versions, but stays on a version prior to the latest release.
Manager Commands Used for generating plugin updates for your managed scanners and agents connected to a manager.	
`nessuscli manager download-core`	Downloads core component updates for remotely managed agents and scanners.
`nessuscli manager generate-plugins`	Generates plugins archives for remotely managed agents and scanners.
Managed Scanner Commands Used for linking, unlinking, and viewing the status of remote managed scanners.	
`nessuscli managed help`	Shows nessuscli-managed commands and syntax.
`nessuscli managed link --key=<key> --host=<host> --port=<port> [optional parameters]`	Link an unregistered scanner to a manager. **Note:** You cannot link a scanner via the CLI if you have already registered the scanner. You can either link via the user interface, or reset the scanner to unregister it (however, you lose all scanner data). **Optional Parameters:** • `--name` — A name for the scanner. • `--ca-path` — A custom CA certificate to use to validate the manager's server certificate. • `--groups` — One or more existing scanner groups where you want to add the scanner. List multiple groups in a comma-separated list. If any group names have spaces, use quotes around the whole list.

Command	Description
	For example: `--groups="Atlanta,Global Headquarters"` **Note:** The scanner group name is case-sensitive and must match exactly. • `--profile-uuid` — The UUID of the scanner profile that you want to assign the scanner to (for example, `12345678-9abc-4ef0-9234-56789abcdef0`) • `--proxy-host` — The hostname or IP address of your proxy server. • `--proxy-port` — The port number of the proxy server. • `--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. • `--proxy-agent` — The user agent name, if your proxy requires a preset user agent. • `--aws-scanner` — Indicates that the Tenable Nessus scanner links with pre-authorized AWS scanner capabilities. Pre-auth AWS scanners differ from Tenable Nessus scanners in that they do not provide **Targets** or **Upload Targets** scan configuration options. Instead, they provide a **Select Targets** button. Click to **Select Targets** to query AWS IMDSv2 and generate a list of visible network targets on a new page. Use this page to select the AWS targets to scan, then click **Confirm**.

Command	Description
	Note: The Tenable Nessus scanner must already be running on an AWS instance for this option to take effect. **Note:** `--aws-scanner` is not supported in Amazon Linux 2023 AMI environments. **Caution:** Only include the `--aws-scanner` parameter if you want to link Tenable Nessus with pre-authorized AWS scanner capabilites.
`nessuscli managed unlink`	Unlink a managed scanner from its manager.
`nessuscli managed status`	Identifies the status of the managed scanner.
Web Application Scanning Command	
`nessuscli was --upload-image <image tarball file>`	Uploads a local web application scanning image tarball file to Tenable Nessus. You can use this command to enable web application scanning in Tenable Nessus when it is in offline mode. For more information, see Web application scanning in offline mode.
Dump Command	
`nessuscli dump --plugins`	Adds a `plugins.xml` file in the `sbin` directory. For example, running the `/opt/nessus/sbin/nessuscli dump --plugins` on Linux adds a `plugins.xml` file to the `/opt/nessus/sbin/plugins` directory.
Node Commands Used for viewing and changing node links in a cluster environment.	
`nessuscli node link --key=<key> --host=<host> --port=<port>`	Links the child node to the parent node in a clustering environment. For more information on `key`, `host`, and `port`, see Link a

Command	Description
	Node.
`nessuscli node unlink`	Unlinks the child node from the parent node.
`nessuscli node status`	Shows whether the child node is linked to parent node and the number of agents that are linked.

Nessuscli Agent

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 <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.

Command	Description
`# 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.
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).

Command	Description
	• 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:** • `--key` — The linking key that you retrieved from the manager. • `--host` — The static IP address or hostname you set during the Tenable Nessus Manager installation. **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.

Command	Description
	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. **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 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. List multiple groups in a comma-separated list. If any group names have spaces, use quotes around the

Command	Description
	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. • `--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

Command	Description
	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> --port=<new_port>`	Relinks the linked agent from Tenable Vulnerability Management to Tenable Sensor 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

Command	Description
	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 • 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 --`	(Tenable Vulnerability Management-linked agents only)

Command	Description
`UUID=<scan-uuid>`	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 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

Command	Description
	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` — (Default behavior) 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). • `--offline` — Provides the most recently cached agent status when it cannot connect to Tenable Nessus Manager or Tenable Vulnerability Management.

Command	Description
	• `--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` • `Total compiled plugins size` • `Total plugins attributes data` • `Total plugin size on disk`

Command	Description
`# 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`, you need to enter a `proxy_address`. • `proxy_basic_login` — The proxy login username. If you enter a

Command	Description
	`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 in the *Tenable Agent User Guide*.
`# nessuscli fix --set update_hostname="<value>"`	Updates agent hostnames automatically in Tenable Vulnerability Management or Tenable Nessus Manager. You can set the `update_hostname` parameter to `yes` or `no`. By default, this preference is disabled.

Command	Description
	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 Tenable Nessus version when it is made generally available (GA). **Note:** This date is the same day the version is made generally available. • **ea** — Automatically updates to the latest Tenable Nessus 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 Nessus version. Remains on an earlier version of Tenable Nessus set by Tenable, usually one release older than the current generally available version, but no earlier than 8.10.0. When Tenable Nessus releases a new version, your Tenable Nessus instance updates software versions, but stays on a version prior to the

Command	Description
	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 the second try, and 4.5 seconds after the third try.

Command	Description
	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. **Note:** Tenable Agent also disables the FIPS

Command	Description
	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 in the *Tenable Agent User Guide*.
`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 in the *Tenable Agent Deployment and User Guide* for <value> preference options.

Update Tenable Nessus Software (CLI)

When updating Tenable Nessus components, you can use the nessuscli update commands, also found in the command-line section.

Note: If you are working with Tenable Nessus offline, see Manage Tenable Nessus Offline.

Note: You must run the following commands with administrator privileges.

Operating System	Command
Linux	`# /opt/nessus/sbin/nessuscli <cmd> <arg1> <arg2>`
Windows	`C:\Program Files\Tenable\Nessus <cmd> <arg1> <arg2>`
macOS	`# /Library/Nessus/run/sbin/nessuscli <cmd> <arg1> <arg2>`
Software Update Commands	
`nessuscli update`	By default, this tool respects the software update options selected through the Nessus user interface.
`nessuscli update --all`	Forces updates for all Nessus components.
`nessuscli update --plugins-only`	Forces updates for Nessus plugins only.

Configure Tenable Nessus for NIAP Compliance

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

Caution: When installing Tenable Nessus 10.5.8 on Windows, you must install Tenable Nessus in the default directory to be NIAP compliant and avoid the CVE-2025-36625 vulnerability.

Before you begin:

- If you are using SSL certificates to log in SSL certificates to log in to Tenable Nessus, ensure your server and client certificates are NIAP-compliant. You can either use your own certificates signed by a CA, or you can Create SSL Client Certificates for Login using Tenable Nessus.
- Confirm you have enabled the full disk encryption capabilities provided by the operating system on the host where you installed Tenable Nessus.

To configure Tenable Nessus for NIAP compliance:

1. Log in to your instance of Tenable Nessus.
2. Enable NIAP mode using the command line interface:
    a. Access Tenable Nessus from a command line interface.
    b. In the command line, enter the following command:

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

    Linux example:

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

    Tenable Nessus does the following:

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

- Overrides the **SSL Mode** (`ssl_mode_preference`) with the **TLS 1.2** (`niap`) option.
- Overrides the **SSL Cipher List** (`ssl_cipher_list`) setting with the **NIAP Approved Ciphers** (`niap`) setting, 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 Tenable Nessus marks the certificate as invalid. If there is no response, then Tenable Nessus does not mark the certificate as invalid.
  - Ensure 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 you want to use a custom CA certificate that is not in known_CA.inc, copy it to custom_CA.inc in the plugins directory.
- Enforces the current validated FIPS module for Tenable Nessus communication and database encryption. The FIPS module does not affect scanning encryption.

  Note: You can enforce the FIPS module from the `nessuscli` without enforcing NIAP mode. For more information, see Fix Commands.

Database encryption

You can convert encrypted databases from the default format (OFB-128) to NIAP-compliant encryption (XTS-AES-128).

Tenable Nessus in NIAP mode can read databases with the default format (OFB-128).

To convert encrypted databases to NIAP-compliant encryption:

1. Stop Tenable Nessus.
2. Enable NIAP mode, as described in the previous procedure.
3. Enter the following command:

   ```
   nessuscli security niapconvert
   ```

   Tenable Nessus converts encrypted databases to XTS-AES-128 format.

Default Data Directories

The default Tenable Nessus data directory contains logs, certificates, temporary files, database backups, plugins databases, and other automatically generated files.

Refer to the following table to determine the default data directory for your operating system.

Operating System	Directory
Linux	**`/opt/nessus/var/nessus`**
Windows	**`C:\ProgramData\Tenable\Nessus\nessus`**
macOS	**`/Library/Nessus/run/var/nessus`**

Note: Tenable Nessus does not support using symbolic links for `/opt/nessus/`.

Encryption Strength

Tenable Nessus uses the following default encryption for storage and communications.

Function	Default Encryption
Storing user account	SHA-512 and the PBKDF2 function with a 512-bit key

passwords	
Storing user and service accounts for scan credentials, as described in Credentials	AES-128
Scan results and scan exports	AES-128
Communications between Tenable Nessus and clients (GUI/API users)	TLS 1.3 (fallback to TLS 1.2 or earlier, as configured) with the strongest encryption method supported by Tenable Nessus and your browser or API program
Communications between Tenable Nessus and Tenable Agents	TLS 1.3 (fallback to TLS 1.2 if forced by the environment)
Communications between Tenable Nessus and the Tenable plugin update server	TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384
Communications between Tenable Nessus and the Tenable product registration server	TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384

File and Process Allowlist

Tenable recommends allowing the following Tenable Nessus 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 Agent processes, see File and Process Allowlist in the *Tenable Agent 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
Note: If your Windows installation uses a non-standard drive or folder structure, use the %PROGRAMFILES% and %PROGRAMDATA% environment variables.
C:\Program Files\Tenable\Nessus*
C:\Program Files (x86)\Tenable\Nessus*
Processes
C:\ProgramData\Tenable\Nessus\nessus\tmp
C:\Program Files\Tenable\Nessus\nessuscli.exe
C:\Program Files\Tenable\Nessus\nessusd.exe
C:\Program Files\Tenable\Nessus\nasl.exe
C:\Program Files\Tenable\Nessus\nessus-service.exe
C:\Program Files\Tenable\Nessus\openssl.exe
C:\Program Files (x86)\Tenable\Nessus\nasl.exe
C:\Program Files (x86)\Tenable\Nessus\nessuscli.exe
C:\Program Files (x86)\Tenable\Nessus\nessusd.exe
C:\Program Files (x86)\Tenable\Nessus\nessus-service.exe
C:\Program Files (x86)\Tenable\Nessus\openssl.exe
Linux
Folders
/opt/nessus/bin/*
/opt/nessus/bin/openssl
/opt/nessus/sbin/*
/opt/nessus/lib/nessus/*

/opt/nessus/etc/nessus
Processes
/opt/nessus/bin/nasl
/opt/nessus/sbin/nessusd
/opt/nessus/sbin/nessuscli
/opt/nessus/sbin/nessus-service
macOS
Folders
/Library/Nessus/run/sbin/*
/Library/Nessus/run/bin/*
Processes
/Library/Nessus/run/bin/nasl
/Library/Nessus/run/bin/openssl
/Library/Nessus/run/sbin/nessus-service
/Library/Nessus/run/sbin/nessuscli
/Library/Nessus/run/sbin/nessusd
/Library/Nessus/run/sbin/nessusmgt

Get Started with Web Application Scanning in Tenable Nessus Expert

With the release of Tenable Nessus 10.6, Tenable brings its web application scanning functionality to Tenable Nessus Expert. The following overview provides you with everything you need to know to get started using web application scanning in Tenable Nessus Expert. Even if you are already familiar with Tenable's cloud-based application scanner, read this overview in its entirety, as it contains information you must know to use this functionality successfully.

For more information about web application scanning in the Tenable Nessus Expert user interface, see Web Application Scanning in Tenable Nessus and Create a Web Application Scan.

System and Hardware Requirements

While Tenable Nessus itself is installed directly on the host operating system, the web scanner portion of Tenable Nessus Expert is installed as a Docker image on the same host. To do this, your host must have Docker version 20.0.0 or later installed. The web application scanner cannot run if the host does not have Docker installed (all other Tenable Nessus functionality works as expected without Docker being installed).

To install Docker and view Docker system requirements on your host, see https://docs.docker.com/. Once Docker is installed on the host, you can install or upgrade to Tenable Nessus 10.6 or later on the host (you can also install Docker after you install or upgrade to Tenable Nessus).

The following table describes the hardware requirements for web application scanning in Tenable Nessus Expert:

Hardware	Minimum Requirement
Processor	> 8 2GHz cores
RAM	> 12 GB Tenable recommends using 16 GB RAM for the best results.
Disk Space	> 40 GB Your overall usage (scan results, plugin updates, logging) increase the amount of disk space needed over time.

Note: The following platforms do not support web application scanning in Tenable Nessus:

- Any host that does not support Docker
- Any host that uses an ARM-based processor (for example, AArch64 Linux distributions and Apple Silicon systems)

For more information about Docker support on virtualized hosts, see the Docker documentation.

Installation Notes

To install web application scanning in Tenable Nessus Expert, see Web Application Scanning in Tenable Nessus.

In addition to the following installation notes, see the following video on how to install Tenable Nessus Expert and web application scanning: Web App Scanning in Nessus Expert 10.6.

- Tenable Nessus Expert only supports Dock installations that follow the Docker install documentation.
- Tenable Nessus Expert must be able to detect that Docker is installed on the host before you can enable web application scanning.

  On Windows systems, you must run the Docker Desktop as administrator (right-click the Docker Desktop icon and select **Run as administrator**) for Tenable Nessus Expert to detect the presence of Docker. In the event you installed Docker Desktop in a custom directory path, Tenable Nessus Expert on Windows may not be able to detect the instance. In this case, use the `Nessuscli` utility to tell Tenable Nessus Expert where in the host system's directory path the Docker binary lives. For example, if you are running a Windows host and your Docker executable is stored here:

  ```
  C:\Program Files\Docker\Docker\Resources\bin\docker.exe
  ```

  Run the following command as administrator:

  ```
  nessuscli fix --set global.path_to_docker="C:\Program
  Files\Docker\Docker\resources\bin\docker.exe"
  ```

  You can use this same command on Linux systems by adding the Linux file path to the Docker binary.

  Then, restart the Tenable Nessus service and log in to finish enabling web application scanning.
- Do not attempt to install Tenable Nessus web application scanning on an existing Docker image. The web application scanner already resides on a Docker image, and running a Docker application within another docker image is not supported and results in poor performance.
- Tenable Nessus web application scanning does not run on ARM processors (for example, AArch64 Linux or macOS Apple Silicon processors).

Best Practices

- Web applications, whether complex or simple, require knowledge of the application to configure the scanner to perform to the best of its capabilities successfully. Tenable recommends working with web application developers to ensure that you use the proper scan configuration settings for the specific applications architecture.
- Because web application scanning can be invasive depending on how the scan is configured, Tenable recommends first scanning against a mirror image of the web application, if available. This allows you to determine the impact of using various scan configurations against the application.
- When scanning a production application directly, Tenable recommends only performing web scans during your organization's scheduled maintenance windows.
- In most cases, security practitioners identify specific web applications to assess for vulnerabilities. However, they may not be aware of all the potential web applications deployed in their environment. Tenable recommends running an initial scan to identify potential web applications. Doing so allows you to compile a list of potential web application targets. You can use the list to engage with system administrators and web application developers and determine whether these hosts require a full web application vulnerability assessment. For more information, see the following video on identifying web application hosts in your network: How to Detect Web Applications with Nessus.

Web Application Scanning Templates

The web application scanner in Tenable Nessus Expert includes seven scan templates:

- An API scanning template
- A web application configuration audit template
- A Log4Shell detection template
- A web application overview template
- A PCI ASV template
- A general web application scan template
- An SSL TLS audit scan
- A quick web application scan template

In most circumstances, Tenable recommends using the following scan templates in their listed order to generate scan results that meet most organization's security requirements:

1. **SSL TLS**

   For information about setting up and launching an **SSL TLS** scan against a web application, see the following video: Web App SSL and TLS Scanning in Nessus Expert 10.6.

2. **Web App Config Audit**

   For information about setting up and launching a **Web App Config Audit** scan against a web application, see the following video: Web App Config Audit Scanning in Nessus Expert 10.6.

3. **Web App Overview**

   For information about setting up and launching a **Web App Overview** scan against a web application, see the following video: Web App Overview Scanning in Nessus Expert 10.6.

4. **Scan**

   For information about scanning a web application with the **Scan** template, see the following video: Web App Scan in Nessus Expert 10.6.

For information on viewing and interpreting web application scan results, see the following video: Web App Vulnerability Analysis in Nessus Expert 10.6.

For more documentation on each Tenable Nessus web application scan template, see Scan Templates.

Helpful Knowledge Base Articles

The web application scanner in Tenable Nessus Expert uses the same engine as Tenable's web application scanner found in Tenable Vulnerability Management and Tenable Core + Tenable Web App Scanning. While the following knowledge base articles may reference these other products, the topics discussed in the articles are applicable to web application scanning in Tenable Nessus:

- Can Tenable Vulnerability Management WAS assess Flash-based websites?
- Can Tenable Vulnerability Management WAS log in to sites using CAPTCHA?
- Can Tenable Vulnerability Management Web Application Scanning integrate into a CI/CD?

- Does Scanning a Single sign-on (SSO) page using Selenium capture all the URLs in the sitemap?
- Does Tenable Core + WAS use the host file for name resolution?
- Limitations of Selenium in Web Application Scanning
- Troubleshooting OpenAPI/Swagger Specification File is Invalid
- WAS Scan Time Limit Reached
- What is the maximum number of results published in a Web Application Scan?
- What to do when a Tenable Web Application Scanning scan never finishes or times out

Manage Logs

Tenable Nessus has the following default log files:

- `nessusd.dump` — Nessus dump log file used for debugging output.

  Configure `nessusd.dump`

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

Name	Description	Default	Valid Values
Nessus Dump File Location (dumpfile)	Location of `nessusd.dump`, a log file for debugging output if generated. The following are the defaults for each operating system: Linux: `/opt/nessus/var/nessus/logs/nessusd.dump`	*Nessus log directory for your operating system*	String

	macOS:
	`/Library/Nessus/run/var/nessus/logs/nessusd.dump`
	Windows:
	`C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.dump`		

Nessus Dump File Log Level (nasl_log_type)	The type of NASL engine output in `nessusd.dump`.	`normal`	`normal`, `none`, `trace`, or `full`.
Nessus Dump File Max Files (dumpfile_max_files)	The maximum number of the `nessusd.dump` files kept on disk. If the number exceeds the specified value, Tenable Nessus deletes the oldest dump file.	100	Integers 1-1000
Nessus Dump File Max Size (dumpfile_max_size)	The maximum size of the `nessusd.dump` files in MB. If file size exceeds the maximum size, Tenable Nessus creates a new dump file.	512	Integers 1-2048
Nessus Dump	Determines how often Tenable Nessus dump files are rotated in days.	1	Integers 1-365

File Rotation Time (dumpfile_rotation_time)			
Nessus Dump File Rotation (dumpfile_rot)	Determines whether Tenable Nessus rotates dump files based on maximum rotation size or rotation time.	`size`	`size` — Tenable Nessus rotates dump files based on size, as specified in `dumpfile_max_size`. `time` — Tenable Nessus rotates dump files based on time, as

			specified in `dumpfile_rotation_time`.
Use Milliseconds in Logs	When enabled, `nessusd.messages`and `nessusd.dump`log timestamps are in milliseconds. When disabled, log timestamps are in seconds.	`no`	`yes` or `no`

For more information, see Advanced Settings.

Alternatively, you can configure log locations and rotation strategies for `nessusd.dump` 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 modify log settings using log.json:

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

Operating System	Log Location
Windows	`C:\ProgramData\Tenable\Nessus\nessus\logs\<filename>`
macOS	`/Library/Nessus/run/var/nessus`
Linux	`/opt/nessus/var/nessus`

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

Note: The following describe parameters in the log.json file, and whether Tenable recommends that you modify the parameter. Some parameters are advanced and you do not need to modify them often. If you are an advanced user who wants to configure a custom log file with advanced parameters, see the knowledge base article for more information.

Parameter	Default value	Can be modified?	Description
`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_`

Parameter	Default value	Can be modified?	Description
			`strategy` is `daily`.
`max_size`	Tenable Nessus : 536870912 (512 MB) Agent: 10485760 (10 MB)	yes	Rotation size in bytes. Only used if `rotation_strategy` is `size`.
`max_files`	Tenable Nessus: 10 Agent: 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 operating system and log file	yes	The location and name of the log file. See Default Log Locations. If you change the name of a default Tenable Nessus log file, some advanced

Parameter	Default value	Can be modified?	Description
			settings may not be able to modify the log settings.

The following are examples of a log.json file.

Linux example

```
{
      "reporters": [
      {
      "tags": [
            "response"
      ],
      "reporter": {
            "type": "file",
            "rotation_strategy": "daily",
            "rotation_time": "86400",
            "max_size": "536870912",
            "max_files": "1024",
            "file": "/opt/nessus/var/nessus/logs/www_server.log"
      },
      "format": "combined"
      },
      {
      "tags": [
            "log",
            "info",
            "warn",
            "error",
            "trace"
      ],
      "reporter": {
      "type": "file",
      "file": "/opt/nessus/var/nessus/logs/backend.log"
```

```
        },
        "context": true,
        "format": "system"
        }
        ]
}
```

Windows example

Note: The backslash (\) is a special character in JSON. To enter a backslash in a path string, you must escape the first backslash with a second backslash so the path parses correctly.

```
{
        "reporters": [
        {
        "tags": [
                "response"
        ],
        "reporter": {
                "type": "file",
                "rotation_strategy": "daily",
                "rotation_time": "86400",
                "max_size": "536870912",
                "max_files": "1024",
                "file": "C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\www_
server.log"
        },
        "format": "combined"
        },
        {
        "tags": [
                "log",
                "info",
                "warn",
                "error",
                "trace"
```

```
      ],
      "reporter": {
      "type": "file",
      "file": "C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\backend.log"
      },
      "context": true,
      "format": "system"
      }
      ]
}
```

macOS example

```
{
      "reporters": [
      {
      "tags": [
            "response"
      ],
      "reporter": {
            "type": "file",
            "rotation_strategy": "daily",
            "rotation_time": "86400",
            "max_size": "536870912",
            "max_files": "1024",
            "file": "/Library/Nessus/run/var/nessus/logs/www_server.log"
      },
      "format": "combined"
      },
      {
      "tags": [
            "log",
            "info",
            "warn",
            "error",
            "trace"
```

```
        ],
        "reporter": {
        "type": "file",
        "file": /Library/Nessus/run/var/nessus/logs/backend.log"
        },
        "context": true,
        "format": "system"
        }
        ]
}
```

3. Save the `log.json` file.
4. Restart the Tenable Nessus service.

   The Tenable Nessus updates the log settings.

- `nessusd.messages` — Nessus scanner log.

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	Description	Default	Valid Values
Nessus Scanner Log Location (logfile)	Location where Tenable Nessus stores its scanner log file. The following are the defaults for each operating system: Linux: `/opt/nessus/var/nessus/logs/nessusd.messages` macOS:	*Nessus log directory for your operating system*	String

	`/Library/Nessus/run/var/nessus/logs/nessusd.messages`
	
	Windows:
	
	`C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.messages`		

Log File Maximum Files (logfile_max_files)	Determines the maximum number of `nessusd.messages` files that Tenable Nessus keeps on the disk. If the number of `nessusd.messages` log files exceeds the specified value, Tenable Nessus deletes the oldest log files.	Tenable Nessus — 100 Tenable Agent — 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 Nessus creates a new messages log file.	Tenable Nessus —512 Tenable Agent — 10	Integers 1-2048
Log File Rotation Time (logfile_rotation_time)	Determines how often Tenable Nessus messages log files are rotated in days.	1	Integers 1-365

Log File Rotation (logfile_rot)	Determines whether Tenable Nessus rotates messages log files based on maximum rotation size or rotation time.	`size`	`size` — Tenable Nessus rotates log files based on size, as specified in `logfile_max_size`. `time` — Tenable Nessus rotates log files based on time, as specified in `logfile_rotation_time`.
Use Milliseconds in	When enabled, `nessusd.messages`and `nessusd.dump`log timestamps are in milliseconds. When disabled, log timestamps	`no`	`yes` or `no`

Logs (logfile_msec)	are in seconds.		

For more information, see Advanced Settings.

- `www_server.log` — Nessus web server log.

Configure `www_server.log`

You can configure log locations and rotation strategies for `www_server.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 modify log settings using log.json:

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

Operating System	Log Location
Windows	`C:\ProgramData\Tenable\Nessus\nessus\logs\ <filename>`
macOS	`/Library/Nessus/run/var/nessus`
Linux	`/opt/nessus/var/nessus`

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

Note: The following describe parameters in the log.json file, and whether Tenable recommends that you modify the parameter. Some parameters are advanced and you do not need to modify them often. If you are an advanced user who wants to configure a custom log file with advanced parameters, see the knowledge base article for more information.

Parameter	Default value	Can be modified?	Description
`tags`	`response`	no	Determines what log information the log includes. • `response` — Web server activity logs **Note:** `response` is the only valid tag for `www_server.log`.
`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

Parameter	Default value	Can be modified?	Description
			`rotation_time`.
`rotation_time`	86400 (1 day)	yes	Rotation time in seconds. Only used if `rotation_strategy` is `daily`.
`max_size`	Tenable Nessus: 536870912 (512 MB) Tenable Agent: 10485760 (10 MB)	yes	Rotation size in bytes. Only used if `rotation_strategy` is `size`.
`max_files`	Tenable Nessus: 10 Tenable Agent: 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 operating system and log	yes	The location and name of the log file. See Default Log Locations.

Parameter	Default value	Can be modified?	Description
	file		If you change the name of a default Tenable Nessus log file, some advanced settings may not be able to modify the log settings.
`context`	`true`	not recommended	Enables more context information for logs in the `system` format, such as `backend.log`.
`format`	`combined`	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.

The following are examples of a log.json file.

Linux example

```
{
      "reporters": [
```

```
      {
      "tags": [
            "response"
      ],
      "reporter": {
            "type": "file",
            "rotation_strategy": "daily",
            "rotation_time": "86400",
            "max_size": "536870912",
            "max_files": "1024",
            "file": "/opt/nessus/var/nessus/logs/www_server.log"
      },
      "format": "combined"
      },
      {
      "tags": [
            "log",
            "info",
            "warn",
            "error",
            "trace"
      ],
      "reporter": {
      "type": "file",
      "file": "/opt/nessus/var/nessus/logs/backend.log"
      },
      "context": true,
      "format": "system"
      }
      ]
}
```

Windows example

Note: The backslash (\) is a special character in JSON. To enter a backslash in a path string, you must escape the first backslash with a second backslash so the path parses correctly.

```
{
	"reporters": [
	{
	"tags": [
		"response"
	],
	"reporter": {
		"type": "file",
		"rotation_strategy": "daily",
		"rotation_time": "86400",
		"max_size": "536870912",
		"max_files": "1024",
		"file": "C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\www_
server.log"
	},
	"format": "combined"
	},
	{
	"tags": [
		"log",
		"info",
		"warn",
		"error",
		"trace"
	],
	"reporter": {
	"type": "file",
	"file": "C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\backend.log"
	},
	"context": true,
	"format": "system"
	}
	]
}
```

macOS example

```
{
	"reporters": [
	{
	"tags": [
		"response"
	],
	"reporter": {
		"type": "file",
		"rotation_strategy": "daily",
		"rotation_time": "86400",
		"max_size": "536870912",
		"max_files": "1024",
		"file": "/Library/Nessus/run/var/nessus/logs/www_server.log"
	},
	"format": "combined"
	},
	{
	"tags": [
		"log",
		"info",
		"warn",
		"error",
		"trace"
	],
	"reporter": {
	"type": "file",
	"file": /Library/Nessus/run/var/nessus/logs/backend.log"
	},
	"context": true,
	"format": "system"
	}
	]
}
```

3. Save the `log.json` file.
4. Restart the Tenable Nessus service.

   The Tenable Nessus updates the log settings.

- `backend.log` — Nessus backend log.

  Configure `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 modify log settings using log.json:

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

Operating System	Log Location
Windows	`C:\ProgramData\Tenable\Nessus\nessus\logs\ <filename>`
macOS	`/Library/Nessus/run/var/nessus`
Linux	`/opt/nessus/var/nessus`

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

     Note: The following describe parameters in the log.json file, and whether Tenable recommends that you modify the parameter. Some parameters are advanced and you do not need to modify them often. If you are an advanced user who wants to configure a custom log file with advanced parameters, see the knowledge base article for more information.

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

Parameter	Default value	Can be modified?	Description
			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

Parameter	Default value	Can be modified?	Description
			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`	Tenable Nessus : 536870912 (512 MB) Tenable Agent: 10485760 (10 MB)	yes	Rotation size in bytes. Only used if `rotation_strategy` is `size`.

Parameter	Default value	Can be modified?	Description
`max_files`	Tenable Nessus: 10 Tenable Agent: 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 operating system and log file	yes	The location and name of the log file. See Default Log Locations. If you change the name of a default Tenable Nessus log file, some advanced settings may not be able to modify the log settings.
`context`	`true`	not recommended	Enables more context information for logs in the `system` format, such as `backend.log`.

`format`	`combined`
	
	`system`
		not recommended	Determines the format of the output.

Parameter	Default value	Can be modified?	Description
			• `combined` — Presents output in a format used for web server logs. • `system` — Presents output in the default operating system log format.

The following are examples of a log.json file.

Linux example

```
{
      "reporters": [
      {
      "tags": [
            "response"
      ],
      "reporter": {
            "type": "file",
            "rotation_strategy": "daily",
            "rotation_time": "86400",
            "max_size": "536870912",
            "max_files": "1024",
            "file": "/opt/nessus/var/nessus/logs/www_server.log"
      },
      "format": "combined"
      },
      {
```

```
      "tags": [
            "log",
            "info",
            "warn",
            "error",
            "trace"
      ],
      "reporter": {
      "type": "file",
      "file": "/opt/nessus/var/nessus/logs/backend.log"
      },
      "context": true,
      "format": "system"
      }
      ]
}
```

Windows example

Note: The backslash (\) is a special character in JSON. To enter a backslash in a path string, you must escape the first backslash with a second backslash so the path parses correctly.

```
{
      "reporters": [
      {
      "tags": [
            "response"
      ],
      "reporter": {
            "type": "file",
            "rotation_strategy": "daily",
            "rotation_time": "86400",
            "max_size": "536870912",
            "max_files": "1024",
            "file": "C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\www_
server.log"
```

```
      },
      "format": "combined"
      },
      {
      "tags": [
            "log",
            "info",
            "warn",
            "error",
            "trace"
      ],
      "reporter": {
      "type": "file",
      "file": "C:\\ProgramData\\Tenable\\Nessus\\nessus\\logs\\backend.log"
      },
      "context": true,
      "format": "system"
      }
      ]
}
```

macOS example

```
{
      "reporters": [
      {
      "tags": [
            "response"
      ],
      "reporter": {
            "type": "file",
            "rotation_strategy": "daily",
            "rotation_time": "86400",
            "max_size": "536870912",
            "max_files": "1024",
            "file": "/Library/Nessus/run/var/nessus/logs/www_server.log"
```

```
        },
        "format": "combined"
        },
        {
        "tags": [
              "log",
              "info",
              "warn",
              "error",
              "trace"
        ],
        "reporter": {
        "type": "file",
        "file": /Library/Nessus/run/var/nessus/logs/backend.log"
        },
        "context": true,
        "format": "system"
        }
        ]
}
```

3. Save the `log.json` file.
4. Restart the Tenable Nessus service.

   The Tenable Nessus updates the log settings.

- `nessuscli.log` — Nessuscli log.

Default Log Locations

The following table describes the default log file locations for each operating system.

Operating System	Log Location
Windows	`C:\ProgramData\Tenable\Nessus\nessus\logs\<filename>`
macOS	`/Library/Nessus/run/var/nessus/logs/<filename>`
Linux	`/opt/nessus/var/nessus/logs/<filename>`

Mass Deployment Support

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

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

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

For more information, see the following:

- Tenable Nessus Environment Variables
- Deploy Tenable Nessus using JSON

Tenable Nessus Environment Variables

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

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

User Configuration

Use the following environment variables for initial user configuration:

- `NCONF_USER_USERNAME` - Tenable Nessus username.
- `NCONF_USER_PASSWORD` - Tenable Nessus user password.

  > **Note:** If you create a user but leave the `NCONF_USER_PASSWORD` value empty, Tenable Nessus automatically generates a password. To log in as the user, use `nessuscli` to change the user's password first.

- `NCONF_USER_ROLE` - Tenable Nessus user role.

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 scanner 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 Tenable Nessus should retry linking.
- `NCONF_LINK_PROFILE_UUID` - (Optional) The UUID of the scanner profile to assign the scanner to.
- `NCONF_LINK_GROUPS` - (Optional) One or more existing scanner groups where you want to add 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"`

Deploy Tenable Nessus using JSON

You can automatically configure and deploy Tenable Nessus scanners using a JSON file, `config.json`. To determine the location of this file on your operating system, see Default Data Directories.

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

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

Location of config.json File

Place the config.json file in the following location:

- Linux: `/opt/nessus/var/nessus/config.json`
- Windows: `C:\ProgramData\Tenable\Nessus\nessus\config.json`

Example Tenable Nessus 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"
	},
	"user": {
		"username": "admin",
		"password": "password",
		"role": "system_administrator",
		"type": "local"
	}
}
```

`config.json` Details

The following describes the format of the different settings in each section of `config.json`.

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

Linking

The `link` section sets preferences to link Tenable Nessus to a manager.

Setting	Description
`name`	(Optional) A name for the scanner.
`host`	The hostname or IP address of the manager you want to link to.
`port`	The port for the manager you want to link to. For Tenable Nessus Manager: 8834 or your custom port.
`key`	The linking key that you retrieved from the manager.
`ms_cert`	(Optional) A custom CA certificate to use to validate the manager's server certificate.
`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. `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.

`aws_scanner`	(Optional) Set `aws_scanner` to **`true`** to link the Tenable Nessus scanner as an AWS scanner. **Note:** The Tenable Nessus scanner must already be running on an AWS instance for the option to take effect. **Caution:** `aws_scanner` is not supported in Amazon Linux 2023 AMI environments.

Preferences

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

User

The `user` section creates a Tenable Nessus user.

Setting	Description
`username`	Username for the Tenable Nessus user.
`password`	(Optional but recommended) Password for the Tenable Nessus user. If you create a user but leave the `password` value empty, Tenable Nessus automatically generates a password. To log in as the user, use `nessuscli` to change the user's password first.
`role`	The role for the user. Set to `disabled`, `basic`, `standard`, `administrator`, or `system_administrator`. For more information, see Users.
`type`	Set to `local`.

Migrate Tenable Nessus to a New Linux Server

Required user role when using Tenable Nessus Manager: System Administrator

During the lifecycle of a Tenable Nessus scanner or Tenable Nessus Manager installed on Linux, you may need to perform a migration from one server to another. The following topic outlines the migration steps for same-to-same, cross-platform, and/or cross-architecture migrations and provides some considerations.

Prerequisites

Ensure your target server has an operating system that is supported for the target version of Tenable Nessus and that it meets all other system and hardware requirements.

Next, ensure the Tenable Nessus version is the same on the source and target servers.

Run the `/opt/nessus/sbin/nessusd -v` command to determine the version on both servers. If the source version is lower than the target version, do one of the following:

- Upgrade the source server Tenable Nessus to the same version as the target server's.
- Downgrade the target server Tenable Nessus to the same version as the source server's.
    - To downgrade Tenable Nessus on Tenable Core, run the `pkexec /usr/libexec/tenablecore/backup/applicationDowngrade.sh` command on the target server, select the Tenable Nessus version to downgrade to, then press **Enter**.

      Note: Due to a Cockpit limitation in Tenable Core Oracle Linux 8 (OL8), it is not possible to run this command in Tenable Core OL8's terminal. You must run it in a Secure Shell (SSH) session instead.
    - To downgrade Tenable Nessus on any other operating system, uninstall Tenable Nessus, then install the version matching the source server's.

Transfer the Data

Transfer the data from the source to the target server using one of the following two options. Both options exclude specific directories (including backups and logs) that are non-essential to the migration. Back these up separately, if needed. A remote sync is the faster option, as it does not require to create, transfer and restore a backup.

Notes:

- All commands must be run as root.
- If you have a non-root user (providing sudo privilege escalation is allowed for your account), you may switch to a root prompt by using the `sudo -i` command and entering your non-root user password again.
- Some operating systems may show a *"tar: invalid option --* ' error when copying and pasting a tar command. Manually entering the command resolves this issue.

Option 1: Backup and Restore

1. Before you begin, ensure sufficient disk space is available on the source server to create a backup. Run the following command to estimate both the time and disk space required for a backup without creating a file.

```
time tar --exclude=
{'bin*','lib*','sbin*','var/nessus/backups*','var/nessus/logs*','var/nessus/plugin-
*','var/nessus/remote*','var/nessus/report-
engine*','var/nessus/templates/tmp*','var/nessus/tmp*','var/nessus/tools*','var/ne-
ssus/www*'} -Ppczf - /opt/nessus | wc -c | numfmt --to=iec-i
```

Example output

```
[root@ness01 ~]# time tar --exclude=
{'bin*','lib*','sbin*','var/nessus/backups*','var/nessus/logs*','var/nessus/plugin-
*','var/nessus/remote*','var/nessus/report-
engine*','var/nessus/templates/tmp*','var/nessus/tmp*','var/nessus/tools*','var/ne-
ssus/www*'} -Ppczf - /opt/nessus | wc -c | numfmt --to=iec-i
43Mi

real    0m7.158s
user    0m7.074s
sys     0m0.362s
```

2. Run the following command to determine if any of the available mount points have sufficient disk space to store a backup of the estimated size.

```
df -h
```

3. Providing sufficient disk space is available, run the following command to generate the backup on the source server at a suitable time. Change `/path/to` to a path you determined to have sufficient disk space to store the backup:

```
service nessusd stop
tar --exclude=
{'bin*','lib*','sbin*','var/nessus/backups*','var/nessus/logs*','var/nessus/plugin-
*','var/nessus/remote*','var/nessus/report-
engine*','var/nessus/templates/tmp*','var/nessus/tmp*','var/nessus/tools*','var/ne-
ssus/www*'} -Ppczf /path/to/nessus_backup.tar.gz /opt/nessus
```

4. Transfer nessus_backup.tar.gz to a location on the target server with sufficient disk space by running the following command:

```
scp /path/to/nessus_backup.tar.gz root@:/path/to
```

Example output

```
[root@ness01 ~]# scp /tmp/nessus_backup.tar.gz root@ness01_target:/tmp
The authenticity of host 'ness01_target (1.2.3.4)' can't be established.
ECDSA key fingerprint is SHA256:oarLiSLC4L+z8ts5/qAwhV9JYtqLNy8Eia1IBqh8gso.
ECDSA key fingerprint is MD5:32:3d:4b:3d:4b:e4:78:ce:4b:87:16:ce:f0:ac:f5:82.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ness01_target' (ECDSA) to the list of known hosts.
root@ness01_target's password:
nessus_backup.tar.gz
                                        100% 3049MB 186.2MB/s   00:16
```

5. On the target server, extract the backup by running the following command. Change `/path/to` to reflect the transferred backup path on the target server:

```
tar -xvf /path/to/nessus_backup.tar.gz -C /
```

Option 2: Remote Sync

1. Ensure rsync is available on both the source and the target server, and that you are able to log in as root to the target server from the source server. If the rsync command does not return output on either server, you can install it by running the `yum install rsync` command on Red Hat-based operating systems, or `dpkg -i rsync` on Debian-based operating systems.

2. On the source server, run the following command to determine the amount of disk space consumed by Tenable Nessus, excluding the directories that will not be synced:

```
du -sh --exclude
{"bin*","lib*","sbin*","var/nessus/backups*","var/nessus/logs*","var/nessus/plugin-
*","var/nessus/remote*","var/nessus/report-
engine*","var/nessus/templates/tmp*","var/nessus/tmp*","var/nessus/tools*","var/ne-
ssus/www*"} /opt/nessus
```

3. Ensure at least the same amount of space is available on the target server, then stop the service on the both the source and target server by running the following command:

```
service nessusd stop
```

4. Run the following command on the source server to synchronize the files to the target server. Change `<target IP address>` to the actual target IP address.

```
rsync -ravz --exclude=
{'bin*','lib*','sbin*','var/nessus/backups*','var/nessus/logs*','var/nessus/plugin-
*','var/nessus/remote*','var/nessus/report-
engine*','var/nessus/templates/tmp*','var/nessus/tmp*','var/nessus/tools*','var/ne-
ssus/www*'} /opt/nessus/* root@<target IP address>:/opt/nessus/
```

Example output

```
[root@ness01 ~]# rsync -ravz --exclude=
{'bin*','lib*','sbin*','var/nessus/backups*','var/nessus/logs*','var/nessus/plugin-
*','var/nessus/remote*','var/nessus/report-
engine*','var/nessus/templates/tmp*','var/nessus/tmp*','var/nessus/tools*','var/ne-
ssus/www*'} /opt/nessus/* root@1.2.3.4:/opt/nessus/
root@1.2.3.4's password:
sending incremental file list
```

```
etc/nessus/
etc/nessus/nessus-fetch.db
etc/nessus/nessus-fetch.db-shm
etc/nessus/nessus-fetch.db-wal
etc/nessus/nessusd.db
etc/nessus/nessusd.db-journal
var/nessus/
var/nessus/.__db_ok
var/nessus/global.db
var/nessus/global.db-shm
var/nessus/global.db-wal
var/nessus/nessus-service.version
var/nessus/nessus.version
var/nessus/tenable_links.json
var/nessus/tenable_rss_feeds.json
var/nessus/upgrades.db
var/nessus/users/
var/nessus/users/admin/
var/nessus/users/admin/policies.db
var/nessus/users/admin/auth/
var/nessus/users/admin/auth/admin
var/nessus/users/admin/auth/hash
var/nessus/users/admin/auth/rules
var/nessus/users/admin/reports/
var/nessus/users/admin/reports/361da43c-fda9-960c-49e8-
d52d3b60280b1d615196a27e8acb
var/nessus/users/admin/reports/361da43c-fda9-960c-49e8-
d52d3b60280b1d615196a27e8acb.name
var/nessus/users/admin/reports/361da43c-fda9-960c-49e8-
d52d3b60280b1d615196a27e8acb.ts
var/nessus/users/nessus_ms_agent/
var/nessus/users/nessus_ms_agent/tmp/
var/nessus/users/nessus_ms_agent/tmp/e5a9ba0be43e72ab/
var/nessus/users/test/
var/nessus/users/test/policies.db
var/nessus/users/test/auth/
var/nessus/users/test/auth/hash
var/nessus/users/test/auth/rules
```

```
var/nessus/users/test/files/
var/nessus/users/test/reports/
sent 2,317,224 bytes  received 5,953 bytes  172,087.19 bytes/sec
total size is 335,189,932  speedup is 144.28
```

Adjustments

Perform the following steps on the target server to ensure a consistent, working state after you have transferred or restored the data:

1. To prevent a FIPS module error from being shown when running nessuscli and ensure the correct platform-specific binaries are in place, perform a forced Tenable Nessus upgrade with the appropriate command for Red Hat or Debian-based operating systems.

   Red Hat-based operating systems

   ```
   rpm -Uvh --force /tmp/Nessus-<version>.x86_64.rpm
   ```

   Note: On Oracle Linx 8 instances of Tenable Core, you can run the `yum download Nessus` command to download the latest Tenable Nessus RPM file to the present working directory. On older instances of Tenable Core, you can run `yumdownloader Nessus` to achieve the same result.

   Debian-based operating systems

   ```
   dpkg --force-all -I /tmp/Nessus-<version>.amd64.deb
   ```

2. Start the Tenable Nessus service on the target server:

   ```
   service nessusd start
   ```

3. To allow the download of plugins and prevent a *"Could not validate this preference file. Have installation files been copied from another system?"* error, log in to Tenable Nessus, then navigate to **Settings** > **Overview** and apply the license again. To re-use the same license, first reset it in https://support.tenable.com. After applying the license, Tenable Nessus signs you out.

   Notes:

- If configured to update online, Tenable Nessus attempts to update shortly thereafter, with the login screen showing *"Plugins are compiling, Nessus functionality will be limited until compilation is complete"* for up to 20 minutes. During that time, backend.log shows *"<[info][globaldb] Waiting for Nessus to be ready>"*. While you will be able to log in and check your data is all there, it will not be possible to run scans until after this completes. When done, the user interface shows *"Plugins are done compiling"*, while backend.log shows *"[info][globaldb] cleanup is starting"* and other activity.

  You can use the `tail -f /opt/nessus/var/nessus/logs/backend.log` command to monitor the progress in backend.log.

  If applicable, Tenable Nessus Manager also starts generating agent DB files, which will take an additional 10 minutes. Next, Tenable Nessus Manager checks if the feed offers a new agent core version. If so, it downloads the new agent core version.

- Air-gapped Tenable Nessus installations require a manual plugins update. You can force the generation of agent DB files for Tenable Nessus Manager after a plugins update using the following command:

  ```
  /opt/nessus/sbin/nessuscli manager generate-plugins –force
  ```

- Information exchange between Tenable Nessus Manager cluster nodes is dependent on a pre-shared secret. If, for example, you run `nessuscli fix --reset` was performed, a new certificate was generated, or a custom CA uploaded to the Tenable Nessus Manager parent, an *"Invalid certificate signature"* error may appear in a child node's backend.log. If so, follow Invalid Certificate signature on cluster nodes to reset the pre-shared secret and re-enable communication between the nodes.

Configure the Hostname and IP address

A stand-alone Tenable Nessus may use a different hostname and/or IP address. However, as agents will have been linked to one or the other, a Tenable Nessus Manager target server should have the same IP address and hostname as the source server. After transferring the data, make note of the source server hostname and IP address, then shut down the source server and assign the same to the target server.

Notes:

- If a different hostname and/or IP address is used for the Tenable Nessus Manager target server, agents linked to the previous hostname or IP address will have an Offline status in the console. To correct this, you must remove each agent's Tenable tag (/etc/tenable_tag or HKLM\SOFTWARE\Tenable\TAG) before relinking them to the target server.
    - Not removing the Tenable tag before attempting to relink the agent results in a 409 error, as the Tenable Nessus Manager will already have an agent with the same Tenable tag.
    - After deleting the Tenable tag, restart the agent service using `service nessusagent restart` to create a new one.
    - The relinking of an agent with a new Tenable tag results in an update of the agent in the Tenable Nessus Manager console.

Configure the hostname using one of the following two options:

Option 1: Re-use the source server's hostname on the target server

1. Shut down the source server
2. On the target server, run the following command as root to change the hostname:

    ```
    hostname <hostname>
    ```

    Note: The changed hostname is not immediately reflected in the command prompt. Enter `exit`, then log in again, after which the new hostname should be shown. If it does not persist after a reboot, change the name in /etc/hostname directly.

Option 2: Use a new hostname on the target server

1. Run the below command as root on the target server to set the desired hostname.

    ```
    hostname <new hostname>
    ```

2. Enter exit, then log in again, after which the new hostname should be shown.

To change the target server's IP address, determine the interface name associated with the IP address to be changed in the `ip a` output, then update the IP address in /etc/sysconfig/network-

scripts/ifcfg-*<network interface name>* in a Red Hat-based operating system, or in /etc/network/interfaces in a Debian-based operating system, and then reboot the server.

Offline Mode

You can set new or existing Tenable Nessus scanners to *offline mode*. Offline mode automatically disables any features that require a connection to the Tenable Nessus feed. For this reason, Tenable recommends using offline mode for any scanner that is offline or air-gapped.

Activate or Deactivate Offline Mode

- To register Tenable Nessus in offline mode during installation, select the **Register Offline** option in the installation user interface.
- To activate offline mode on an existing Tenable Nessus scanner, run `nessuscli fetch --register-offline nessus.license` from the command line.
- To deactivate offline mode on an existing Tenable Nessus scanner, run `nessuscli fetch --register <activation-code>` from the command line.

For more information about `nessuscli fetch` commands, see Fetch Commands.

Offline Mode Functionality

The following features and elements are disabled in offline mode:

- All functionality that requires connection to the Tenable Nessus feed and:
  - Core and plugin updates
  - `nessuscli` commands that require connection to the Tenable Nessus feed (for example, `nessuscli update`)
  - Feed status updates in the Events tab
  - License registration checks
- Upgrade Assistant
- The ability to update the plugin detail locale
- The ability to link Tenable Nessus to Tenable Vulnerability Management

- In-application product updates
- Context-sensitive help documentation icons

Note: In Tenable Nessus versions 10.9.0 and later, web application scanning and declaring agent versions via agent profiles are both supported in offline mode. However, you need to run the following commands while online before going into offline mode for the features to work properly:

- Web application scanning — `nessuscli --upload-was <image-tarball path>`

  Running this command uploads a local web application scanning image tarball file to Tenable Nessus. For more information, see Web application scanning in offline mode.

- Agent versioning via agent profiles — `nessuscli update <tar.gz filename> --agent-version`

  Running this command adds the agent version of the tar.gz file to the **Agent Profiles** menu to be selectable while creating or updating agent profiles. For more information, see Manage agent profiles in offline mode.

Run Tenable Nessus as Non-Privileged User

Tenable Nessus can run as a non-privileged user.

Limitations

- When scanning localhost, Nessus plugins assume that they are running as root. Therefore, certain types of scans may fail. For example, because Nessus is now running as a non-privileged user, file content Compliance Audits may fail or return erroneous results since the plugins are not able to access all directories.
- `nessuscli` does not have a `--no-root` mode. Running commands with `nessuscli` as root could potentially create files in the Nessus install directory owned by root, which can prohibit Nessus from accessing them successfully. Use care when running `nessuscli`, and potentially fix permissions with `chown` after using it.

Run Nessus on Linux with Systemd as a Non-Privileged User

Limitations

- When scanning localhost, Nessus plugins assume that they are running as root. Therefore, certain types of scans may fail. For example, because Nessus is now running as a non-privileged user, file content Compliance Audits may fail or return erroneous results since the plugins are not able to access all directories.
- `nessuscli` does not have a `--no-root` mode. Running commands with `nessuscli` as root could potentially create files in the Nessus install directory owned by root, which can prohibit Nessus from accessing them successfully. Use care when running `nessuscli`, and potentially fix permissions with `chown` after using it.

Steps

1. Do one of the following:
   - If you have not already, install Nessus.
   - If you already installed Nessus and are running it, stop `nessusd`.
2. Create a non-root account to run the Nessus service.

   ```
   sudo useradd -r -m nonprivuser
   ```

3. Remove `world` permissions on Nessus binaries in the `/sbin` directory.

   ```
   sudo chmod 750 /opt/nessus/sbin/*
   ```

4. Change ownership of `/opt/nessus` to the non-root user.

   ```
   sudo chown nonprivuser:nonprivuser -R /opt/nessus
   ```

   Note: You need to complete steps 3 and 4 every time Tenable Nessus is updated.

5. Set capabilities on `nessusd` and `nessus-service`.

   Tip: Use **cap_net_admin** to put interface in promiscuous mode.
   Use **cap_net_raw** to create raw sockets for packet forgery.
   Use **cap_sys_resource** to set resource limits.

If this is only a manager, and you do not want this instance of Nessus to perform scans, you need to provide it only with the capability to change its resource limits.

```
sudo setcap "cap_sys_resource+eip" /opt/nessus/sbin/nessusd
sudo setcap "cap_sys_resource+eip" /opt/nessus/sbin/nessus-service
```

If you want this instance of Nessus to perform scans, you need to add more permissions to allow packet forgery and enabling promiscuous mode on the interface.

```
sudo setcap "cap_net_admin,cap_net_raw,cap_sys_resource+eip"
/opt/nessus/sbin/nessusd
sudo setcap "cap_net_admin,cap_net_raw,cap_sys_resource+eip"
/opt/nessus/sbin/nessus-service
```

6. Create an override configuration file by running the following two commands:

```
mkdir -p /etc/systemd/system/nessusd.service.d/
printf '[Service]\nExecStart=\nExecStart=/opt/nessus/sbin/nessus-service -q --no-
root\nUser=nonprivuser\n' > /etc/systemd/system/nessusd.service.d/override.conf
```

This file overrides the ExecStart and User options in the `nessusd` service unit file (/usr/lib/systemd/system/nessusd.service) with the non-privileged settings.

7. Reload the `systemd` manager configuration to include the override configuration file by running the following command:

```
sudo systemctl daemon-reload
```

8. Start `nessusd` by running the following command:

```
sudo service nessusd start
```

9. Verify Tenable Nessus is running as a non-privileged user by running the following command:

```
service nessusd status
```

If Tenable Nessus is running as a non-privileged user, `override.conf` shows under `/etc/systemd/system/nessusd.service.d` and `CGroup` (Control Group) shows that you started both `nessus-service` and `nessusd` with the `--no-root` parameter.

Run Nessus on Linux with init.d Script as a Non-Privileged User

Limitations

When scanning localhost, Nessus plugins assume that they are running as root. Therefore, certain types of scans may fail. For example, because Nessus is now running as a non-privileged user, file content Compliance Audits may fail or return erroneous results since the plugins are not able to access all directories.

Because `nessuscli` does not have a `--no-root` mode, running commands with `nessuscli` as root could potentially create files in the Nessus install directory owned by root, which can prohibit Nessus from accessing them successfully. Use care when running `nessuscli`, and potentially fix permissions with `chown` after using it.

Steps

1. If you have not already, install Nessus.
2. Create a non-root account to run the Nessus service.

   ```
   sudo useradd -r -m nonprivuser
   ```

3. Remove 'world' permissions on Nessus binaries in the /sbin directory.

   ```
   sudo chmod 750 /opt/nessus/sbin/*
   ```

4. Change ownership of /opt/nessus to the non-root user.

   ```
   sudo chown nonprivuser:nonprivuser -R /opt/nessus
   ```

5. Set capabilities on nessusd and nessus-service.

   Tip:

Use **cap_net_admin** to put the interface in promiscuous mode.

Use **cap_net_raw** to create raw sockets for packet forgery.

Use **cap_sys_resource** to set resource limits.

If this is only a manager, and you do not want this instance of Nessus install to perform scans, you need to provide it only with the capability to change its resource limits.

```
sudo setcap "cap_sys_resource+eip" /opt/nessus/sbin/nessusd
sudo setcap "cap_sys_resource+eip" /opt/nessus/sbin/nessus-service
```

If you want this instance of Nessus to perform scans, you need to add extra permissions to allow packet forgery and enabling promiscuous mode on the interface.

```
sudo setcap "cap_net_admin,cap_net_raw,cap_sys_resource+eip"
/opt/nessus/sbin/nessusd
sudo setcap "cap_net_admin,cap_net_raw,cap_sys_resource+eip"
/opt/nessus/sbin/nessus-service
```

6. Add the following line to the **/etc/init.d/nessusd** script:

CentOS

```
daemon --user=nonprivuser /opt/nessus/sbin/nessus-service -q -D --no-root
```

Debian

```
start-stop-daemon --start --oknodo --user nonprivuser --name nessus --
pidfile --chuid nonprivuser --startas /opt/nessus/sbin/nessus-service -- -q
-D --no-root
```

Depending on your operating system, the resulting script should appear as follows:

CentOS

```
start() {
```

```
    KIND="$NESSUS_NAME"
    echo -n $"Starting $NESSUS_NAME : "
    daemon --user=nonprivuser /opt/nessus/sbin/nessus-service -q -D --no-root
    echo "."
    return 0
}
```

Debian

```
start() {
    KIND="$NESSUS_NAME"
    echo -n $"Starting $NESSUS_NAME : "
    start-stop-daemon --start --oknodo --user nonprivuser --name nessus --pidfile
--chuid nonprivuser --startas /opt/nessus/sbin/nessus-service -- -q -D --no-root
    echo "."
    return 0
}
```

7. Start `nessusd`.

   In this step, Nessus starts as `root`, but `init.d` starts it as `nonprivuser`.

   ```
   sudo service nessusd start
   ```

   Note: If you are running Nessus on Debian, after starting Nessus, run the `chown -R nonprivuser:nonprivuser /opt/nessus` command to regain ownership of directories created at runtime.

Run Nessus on macOS as a Non-Privileged User

Limitations

- When scanning localhost, Nessus plugins assume that they are running as root. Therefore, certain types of scans may fail. For example, because Nessus is now running as a non-privileged user, file content Compliance Audits may fail or return erroneous results since the plugins are not able to access all directories.

- nessuscli does not have a `--no-root` mode. Running commands with `nessuscli` as root could potentially create files in the Nessus install directory owned by root, which could cause Nessus to be unable to access them appropriately. Use care when running `nessuscli`, and potentially fix permissions with `chown` after using it.

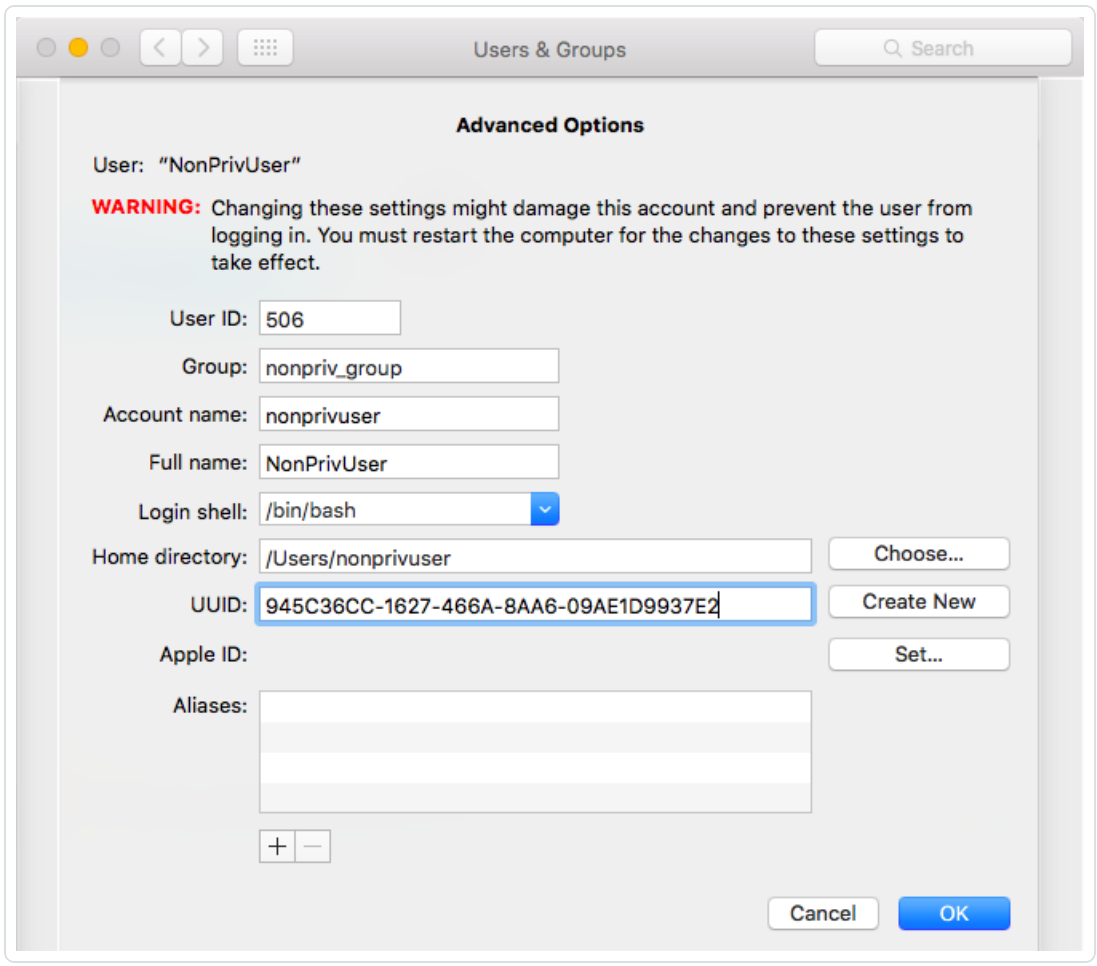
Steps

1. If you have not already done so, Install Nessus on MacOSX.
2. Since the Nessus service is running as root, you need to unload it.

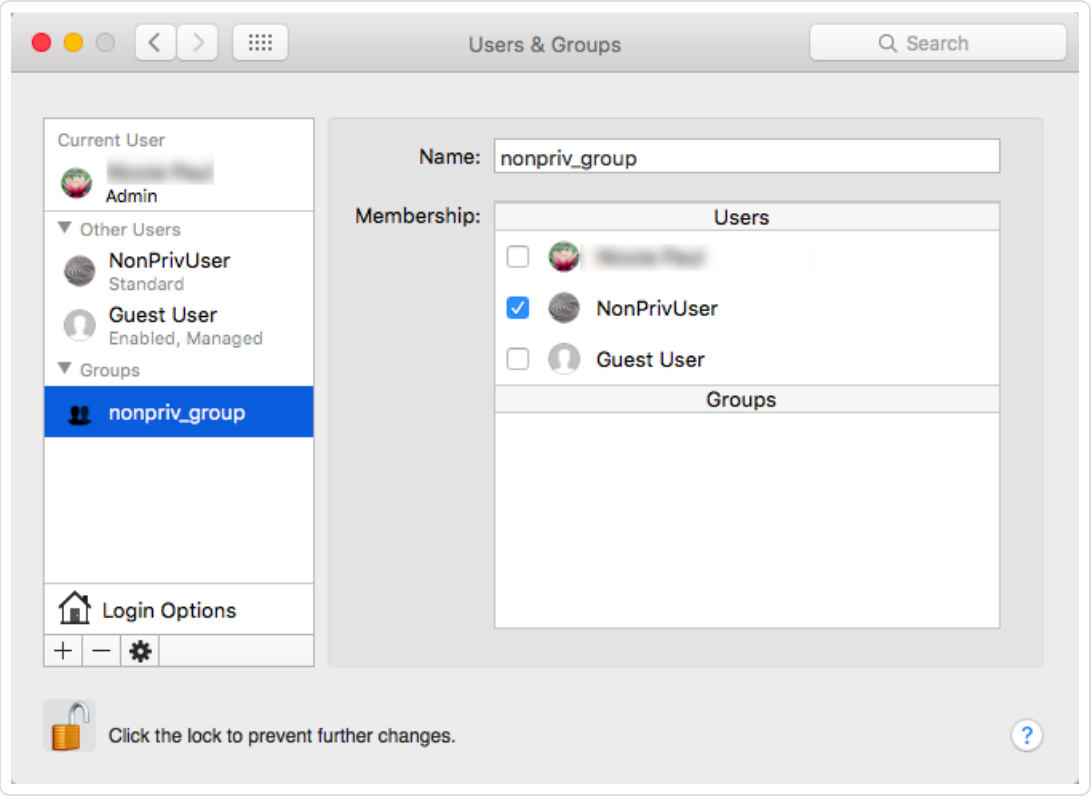
   Use the following command to unload the Nessus service:

   ```
   sudo launchctl unload /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
   ```

3. On the Mac, in **System Preferences > Users & Groups**, create a new **Group**.
4. Next, in **System Preferences > Users & Groups**, create the new **Standard User**. Configure this user to run as the Nessus non-privileged account.



5. Add the new user to the group you created in Step 1.



6. Remove 'world' permissions on Nessus binaries in the /sbin directory.

```
sudo chmod 750 /Library/Nessus/run/sbin/*
```

7. Change ownership of `/Library/Nessus/run` directory to the non-root (Standard) user you created in Step 2.

```
sudo chown -R nonprivuser:nonprivuser /Library/Nessus/run
```

8. Give that user read/write permissions to the `/dev/bpf*` devices. A simple way to do this is to install Wireshark, which creates a group called `access_bpf` and a corresponding launch daemon to set appropriate permissions on `/dev/bpf*` at startup. In this case, you can simply assign the `nonpriv` user to be in the `access_bpf` group. Otherwise, you need to create a launch daemon giving the "nonpriv" user, or a group that it is a part of, read/write permissions to all /dev/bpf*.

9. For Step 8. changes to take effect, reboot your system.

10. Using a text editor, modify the Nessus **/Library/LaunchDaemons/com.tenablesecurity.nessusd.plist** file and add the following lines. **Do not modify any of the existing lines.**

```
<string>--no-root</string>
<key>UserName</key>
<string>nonprivuser</string>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Disabled</key>
        <true/>
        <key>Label</key>
        <string>com.tenablesecurity.nessusd</string>
        <key>ProgramArguments</key>
        <array>
                <string>/Library/Nessus/run/sbin/nessus-service</string>
                <string>-q</string>
                <string>--no-root</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
      <key>UserName</key>
      <string>nonprivuser</string>
</dict>
</plist>
```

11. Using **`sysctl`**, verify the following parameters have the minimum values:

```
$ sysctl debug.bpf_maxdevices
debug.bpf_maxdevices: 16384
$ sysctl kern.maxfiles
kern.maxfiles: 12288
$ sysctl kern.maxfilesperproc
kern.maxfilesperproc: 12288
$ sysctl kern.maxproc
kern.maxproc: 1064
$ sysctl kern.maxprocperuid
kern.maxprocperuid: 1064
```

12. If any of the values in Step 9. do not meet the minimum requirements, take the following steps to modify values.

Create a file called **/etc/sysctl.conf**.
Using a text editor, edit the **systctl.conf** file with the correct values found in Step 9.

Example:

```
$ cat /etc/sysctl.conf
kern.maxfilesperproc=12288
kern.maxproc=1064
kern.maxprocperuid=1064
```

13. Next, using the **launchctl limit** command, verify your OS default values.

    Example: MacOSX 10.10 and 10.11 values.

```
$ launchctl limit
cpu         unlimited      unlimited
filesize    unlimited      unlimited
data        unlimited      unlimited
stack       8388608        67104768
core        0              unlimited
rss         unlimited      unlimited
memlock     unlimited      unlimited
maxproc     709            1064
maxfiles    256            unlimited
```

14. If you do not set any of the values in Step 11 to the default OSX values above, take the following steps to modify values.

    Using a text editor, edit the **launchd.conf** file with the correct, default values as shown in Step 11.

    Example:

```
$ cat /etc/launchd.conf
limit maxproc 709 1064
```

    Note: Some older versions of OSX have smaller limits for **maxproc**. If your version of OSX supports increasing the limits through **/etc/launchctl.conf**, increase the value.

15. For all changes to take effect either reboot your system or reload the launch daemon.

```
sudo launchctl load /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
```

Tenable Nessus Credentialed Checks

In addition to remote scanning, you can use Tenable Nessus to scan for local exposures. For information about configuring credentialed checks, see Credentialed Checks on Windows and Credentialed Checks on Linux.

Purpose

External network vulnerability scanning is useful to obtain a snapshot in time of the network services offered and the vulnerabilities they may contain. However, it is only an external perspective. It is important to determine what local services are running and to identify security exposures from local attacks or configuration settings that could expose the system to external attacks that an external scan might not detect.

A typical network vulnerability assessment performs a remote scan against the external points of presence and an on-site scan is performed from within the network. Neither of these scans can determine local exposures on the target system. Some of the information gained relies on the banner information shown, which may be inconclusive or incorrect. By using secured credentials, you can grant the Nessus scanner local access to scan the target system without requiring an agent. This can facilitate scanning of a large network to determine local exposures or compliance violations.

The most common security problem in an organization is that security patches are not applied in a timely manner. A Nessus credentialed scan can quickly determine which systems are out of date on patch installation. This is especially important when a new vulnerability is made public and executive management wants a quick answer regarding the impact to the organization.

Another major concern for organizations is to determine compliance with site policy, industry standards (such as the Center for Internet Security (CIS) benchmarks) or legislation (such as Sarbanes-Oxley, Gramm-Leach-Bliley, or HIPAA). Organizations that accept credit card information must demonstrate compliance with the Payment Card Industry (PCI) standards. There have been quite a few well-publicized cases where the credit card information for millions of customers was breached. This represents a significant financial loss to the banks responsible for covering the

payments and heavy fines or loss of credit card acceptance capabilities by the breached merchant or processor.

Access Level

Credentialed scans can perform any operation that a local user can perform. The level of scanning depends on the privileges granted to the user account that you configure Tenable Nessus to use.

Non-privileged users with local access on Linux systems can determine basic security issues, such as patch levels or entries in the /etc/passwd file. For more comprehensive information, such as system configuration data or file permissions across the entire system, you need an account with "root" privileges.

Tenable Nessus needs to use a local administrator account for credentialed scans on Windows systems. Several bulletins and software updates by Microsoft have made reading the registry to determine software patch level unreliable without administrator privileges. Tenable Nessus needs local administrative access to perform direct reading of the file system. This allows Nessus to attach to a computer and perform direct file analysis to determine the true patch level of the systems that Tenable Nessus evaluates.

Detecting When Credentials Fail

If you are using Nessus to perform credentialed audits of Linux or Windows systems, analyzing the results to determine if you had the correct passwords and SSH keys can be difficult. You can detect if your credentials are not working using plugin 21745.

This plugin detects if either SSH or Windows credentials did not allow the scan to log into the remote host. When a login is successful, this plugin does not produce a result.

Credentialed Checks on Windows

Follow the steps in this document to configure Windows systems for local security checks.

> **Note:** To run some local checks, Tenable Nessus requires that the host runs PowerShell 5.0 or newer.

Prerequisites

Before you begin this process, ensure that there are no security policies in place that block credentialed checks on Windows, such as:

- Windows security policies
- Local computer policies (for example, *Deny access to this computer from the network*, *Access this computer from the network*)
- Antivirus or endpoint security rules
- IPS/IDS

Configure an Account for Authenticated Scanning

The most important aspect of Windows credentials is that the account used to perform the checks needs privileges to access all required files and registry entries which, often, means administrative privileges. If you do not provide Tenable Nessus with credentials for an administrative account, at best, you can use it to perform registry checks for the patches. While this is still a valid method to find installed patches, it is incompatible with some third-party patch management tools that may neglect to set the key in the policy. If Tenable Nessus has administrative privileges, it checks the version of the dynamic-link library (`.dll`) on the remote host, which is considerably more accurate.

The following drop-down sections describe how to configure a domain or local account to use for Windows credentialed checks, depending on your use case.

Note: You can only use Domain Administrator accounts to scan Domain Controllers.

Use Case #1: Configure a Domain Account for Local Audits

To create a domain account for remote, host-based auditing of a Windows server, the server must be a supported version of Windows and part of a domain. To configure the server to allow logins from a domain account, use the Classic security model, as described in the following steps:

1. Open the **Start** menu and select **Run**.
2. Enter `gpedit.msc` and select **OK**.
3. Select **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.
4. In the list, select **Network access: Sharing and security model for local accounts**.

   The **Network access: Sharing and security model for local accounts** window appears.

5. In the Local Security Setting section, in the drop-down box, select **Classic - local users authenticate as themselves**.

   This allows local users of the domain to authenticate as themselves, even though they are not physically local on the particular server. Without doing this, all remote users, even real users in the domain, authenticate as guests and do not have enough credentials to perform a remote audit.

6. Click **OK**.

Note: To learn more about protecting scanning credentials, see 5 Ways to Protect Scanning Credentials for Windows Hosts.

Use Case #2: Configure a Local Account

To configure a standalone (in other words, not part of a domain) Windows server with credentials you plan to use for credentialed checks, create a unique account as the administrator.

Do not set the configuration of this account to the default of **Guest only: local users authenticate as guest**. Instead, switch this to **Classic: local users authenticate as themselves**.

Note: A common mistake is to create a local account that does not have enough privileges to log on remotely and do anything useful. By default, Windows assigns new local accounts Guest privileges if they are logged into remotely. This prevents remote vulnerability audits from succeeding. Another common mistake is to increase the amount of access that the Guest users obtain. This reduces the security of your Windows server.

Create the "Nessus Local Access" Security Group

1. Log in to a Domain Controller and open **Active Directory Users and Computers**.
2. To create a security group, select **Action** > **New** > **Group**.
3. Name the group **Nessus Local Access**. Set **Scope** to **Global** and **Type** to **Security**.
4. Add the account you plan to use to perform Tenable Nessus Windows Authenticated Scans to the Tenable Nessus Local Access group.

Create the "Nessus Scan GPO" Group Policy

1. Open the Group Policy Management Console.
2. Right-click **Group Policy Objects** and select **New**.
3. Type the name of the policy **Nessus Scan GPO**.

Add the "Nessus Local Access" Group to the "Nessus Scan GPO" Policy

1. Right-click **Nessus Scan GPO Policy**, then select **Edit**.
2. Expand **Computer configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Restricted Groups**.
3. In the left navigation bar on **Restricted Groups**, right-click and select **Add Group**.
4. In the **Add Group** dialog box, select **browse** and enter **Nessus Local Access**.
5. Select **Check Names**.
6. Select **OK** twice to close the dialog box.
7. Select **Add** under **This group is a member of:**
8. Add the **Administrators** Group.
9. Select **OK** twice.

Tenable Nessus uses Server Message Block (SMB) and Windows Management Instrumentation (WMI). Ensure Windows Firewall allows access to the system.

Allow WMI on Windows

1. Right-click **Nessus Scan GPO Policy**, then select **Edit**.
2. Expand **Computer configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Windows Firewall with Advanced Security** > **Windows Firewall with Advanced Security** > **Inbound Rules**.
3. Right-click in the working area and choose **New Rule...**.
4. Choose the **Predefined** option, and select **Windows Management Instrumentation (WMI)** from the drop-down box.
5. Select **Next**.

6. Select the checkboxes for:
    - Windows Management Instrumentation (ASync-In)
    - Windows Management Instrumentation (WMI-In)
    - Windows Management Instrumentation (DCOM-In)
7. Select **Next**.
8. Select **Finish**.

> **Tip:** Later, you can edit the predefined rule created and limit the connection to the ports by IP Address and Domain User to reduce any risk for abuse of WMI.

Link the GPO

1. In the Group policy management console, right-click the domain or the OU and select **Link an Existing GPO**.
2. Select the **Nessus Scan GPO**.

Configure Windows

Once you create an appropriate account for credentialed checks, there are several Windows options that you must configure before scanning:

(Local accounts only) User Account Control (UAC)

Disable Windows User Account Control (UAC), or you must change a specific registry setting to allow Tenable Nessus audits. To disable UAC, open the Control Panel, select **User Accounts**, and set **Turn User Account Control** to **Off**.

Alternatively, instead of disabling UAC, Tenable recommends adding a new registry DWORD named **LocalAccountTokenFilterPolicy** and setting its value to **1**. Create this key in the following registry: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy`. For more information on this registry setting, see the MSDN 766945 KB.

> **Tip:** To turn off UAC completely, open the **Control Panel**, select **User Accounts**, and then set Turn User Account Control to off. Alternatively, you can add a new registry key named LocalAccountTokenFilterPolicy and set its value to 1.

You must create this key in the registry at the following location: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy`.

For more information on this registry setting, consult the MSDN 766945 KB. In Windows 7 and 8, if you disable UAC, then you must set EnableLUA to **0** in `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System` as well.

Host Firewall

- Using the **Run** prompt, run `gpedit.msc` and enable **Group Policy Object Editor**. Navigate to **Local Computer Policy** > **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall** > **Standard Profile** > **Windows Firewall: Allow inbound file and printer exception** and enable it.

  While in the **Group Policy Object Editor**, navigate to **Local Computer Policy** > **Administrative Templates** > **Network** > **Network Connections** > **Prohibit use of Internet connection firewall on your DNS domain**. Set this option to either **Disabled** or **Not Configured**.

- Under **Windows Firewall** > **Windows Firewall Settings**, enable **File and Printer Sharing**. Open any host firewalls to allow connections from Tenable Nessus to **File and Printer Sharing** on TCP ports **139** and **445**. If you want Tenable Nessus to pick up any open ports or services on the host, those ports also need to be accessible to the scanner.

Remote Registry

Enable the **Remote Registry** (it is disabled by default). You can enable it for a one-time audit, or leave it enabled permanently if you perform frequent audits.

Note: Enabling this option configures Tenable Nessus to attempt to start the remote registry service before starting the scan.

The Windows credentials provided in the Tenable Nessus scan policy must have administrative permissions to start the Remote Registry service on the host being scanned.

If the service is set to *manual* (rather than *enabled*), plugin IDs 42897 and 42898 only enable the registry during the scan.

Note: For information on enabling the Remote Registry during scans, see How to enable the "Start the Remote Registry service during the scan" option in a scan policy.

Administrative Shares

Using either the **AutoShareServer** (Windows Server) or **AutoShareWks** (Windows Workstation), enable the following default administrative shares:

- **IPC$**
- **ADMIN$**

  > **Note:** Windows 10 disables **ADMIN$** by default. For all other operating systems, the three shares are enabled by default and can cause other issues if disabled by default. For more information, see Overview of problems that may occur when administrative shares are missing in the Windows documentation.

- **C$**

What to do next:

- Configure a Tenable Nessus scan for Windows logins.

Configure a Tenable Nessus Scan for Windows Logins

Tenable Nessus allows you to configure your scan configurations with the credentials needed for Windows logins. You can do so during the Create a Scan process, or you can add credentials to an existing scan configuration.

Before you begin, configure your Windows system for authenticated scanning as described in Credentialed Checks on Windows.

To configure a Tenable Nessus scan configuration for Windows logins:

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

   The My Scans page appears.

2. Do one of the following:

   - Click **New Scan** to create a new scan and select a template.
   - Click **My Scans** in the left navigation bar, choose an existing scan, then click the **Configure** button.

3. In the scan settings, click the **Credentials** tab.

The Credentials menu opens.

4. In the Categories drop-down menu, select **Host**.
5. In the Host category, click **Windows**.

   A Windows credentials pane appears.
6. Select an authentication method. Depending on the method, the remaining Windows settings change.
7. Depending on the authentication method, specify the SMB account username, password or hash, and domain.

   To view the Windows credential setting descriptions, see Windows.
8. Click **Save**. Tenable Nessus saves the new Windows credentials.

Credentialed Checks on macOS

Follow the steps in this document to configure macOS systems for local security checks. You can enable local security checks using an SSH private/public key pair or user credentials and `sudo` or `su` access.

OpenSSH is the example SSH daemon used in this document. If you have a commercial variant of SSH, your procedure may differ slightly.

Prerequisites

Configuration requirements for SSH

You can configure an SSH server to accept certain types of encryption. However, some commercial SSH variants do not support blowfish-cbc. Check that your SSH server supports the algorithm you want to use.

Tenable Nessus supports the blowfish-cbc, aesXXX-cbc (aes128, aes192, and aes256), 3des-cbc, and aes-ctr algorithms.

User privileges

For maximum effectiveness, the SSH user must be able to run any command on the system. On macOS systems, the SSH user must be a member of the **Administrator** group and have full disk access. While it is possible to run some checks (such as patch levels) with non-privileged access, full compliance checks that audit system configuration and file permissions require full disk access. For this reason, Tenable recommends that you use SSH keys instead of credentials when possible.

Configuration requirements for Kerberos

If you use Kerberos, you must configure `sshd` with Kerberos support to verify the ticket with the KDC. You must properly configure reverse DNS lookups for this to work. The Kerberos interaction method must be `gssapi-with-mic`.

Generate SSH Public and Private Keys

Generate a private/public key pair for the Tenable Nessus scanner. You can generate this key pair from the Tenable Nessus scanner. This document assumes that the scanner is running on Linux, but you can also perform the same steps on any of your macOS systems, using any user account.

Note: The defined Tenable Nessus user must own the generated keys.

To generate the key pair, use `ssh-keygen` and save the key in a safe place. See the following example:

```
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter the file in which to save the key (/Users/test/.ssh/id_dsa):
/home/test/Nessus/ssh_key
Enter the passphrase (empty for no passphrase):
Enter the same passphrase again:
Your identification has been saved in
/home/test/Nessus/ssh_key.
Your public key has been saved in
/home/test/Nessus/ssh_key.pub.
The key fingerprint is:
06:4a:fd:76:ee:0f:d4:e6:4b:74:84:9a:99:e6:12:ea
#
```

Do not transfer the private key to any system other than the one running the Tenable Nessus server. When `ssh-keygen` asks you for a passphrase, enter a strong passphrase or press the **Return** key

twice (that is, do not set any passphrase). If you specify a passphrase, you must specify it in **Policies** > **Credentials** > **SSH settings** for your Tenable Nessus scan configuration to use key-based authentication.

Create a User Account

On every target system that you want to scan using local security checks, create a new user account dedicated to Tenable Nessus. This user account must have the same name on all systems. You must grant the account **Administrator** and **Remote Login** privileges to allow Tenable Nessus to run remote credentialed scans.

Configure macOS Remote Login

On the host macOS system, enable **Allow full disk access for the remote users** under the **Remote Login** System setting. This enables full disk access to `sshd-keygen-wrapper`, which you need in the following steps.

Then, grant **Full disk access** under **Privacy and Security** to any related system services to allow plugins to search across the file system. Ensure that the following the services are included:

- `/Library/NessusAgent/run/sbin/nessus-service`
- `/usr/libexec/sshd-keygen-wrapper`

Set Up the SSH Key

From the system containing the keys, secure copy the public key to the system that you want to scan for host checks as shown in the following example. This document refers to the user as `nessus`, but you can use any name.

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
#
```

You can also copy the file from the system on which you installed Tenable Nessus using the secure ftp command, **`sftp`**. You must name the file on the target system `authorized_keys`.

Return to the Public Key System

Set the permissions on both the `/home/nessus/.ssh` directory and the `authorized_keys` file.

```
# chown -R nessus:nessus ~nessus/.ssh/
# chmod 0600 ~nessus/.ssh/authorized_keys
# chmod 0700 ~nessus/.ssh/
#
```

Repeat this process on all systems that you want to test for SSH checks (starting at the Create a User Account steps).

Test the SSH Key

Next, test to make sure that the accounts and networks are configured correctly. Using the simple command `id`, from the Tenable Nessus scanner, run the following command:

```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

If the Tenable Nessus scanner successfully returns information about the Tenable Nessus user, the setup was successful.

What to do next:

- Configure Tenable Nessus for macOS logins.

Credentialed Checks on Linux

Follow the steps in this document to configure Linux systems for local security checks. The SSH daemon used in the following examples is OpenSSH. If you have a commercial variant of SSH, your procedure may be slightly different.

You can enable local security checks using an SSH private/public key pair or user credentials and `sudo` or `su` access.

> **Note:** If you are scanning a Linux machine with Tenable Nessus, the Linux machine's shell configuration file must have a `PS1` variable of four or more characters (for example, `PS1='\u@\h:~\$ '`). Having a `PS1` variable of less than four characters (for example, `PS1='\$ '`) can drastically increase the overall scan time.

Prerequisites

Configuration requirements for SSH

Tenable Nessus supports the blowfish-cbc, aesXXX-cbc (aes128, aes192, and aes256), 3des-cbc, and aes-ctr algorithms.

Some commercial variants of SSH do not have support for the blowfish cipher, possibly for export reasons. It is also possible to configure an SSH server to accept certain types of encryption only. Check that your SSH server supports the correct algorithm.

User privileges

For maximum effectiveness, the SSH user must be able to run any command on the system. On Linux systems, the SSH user must have `root` privileges. While it is possible to run some checks (such as patch levels) with non-privileged access, full compliance checks that audit system configuration and file permissions require root access. For this reason, Tenable recommends that you use SSH keys instead of credentials when possible.

Configuration requirements for Kerberos

If you use Kerberos, you must configure `sshd` with Kerberos support to verify the ticket with the KDC. You must properly configure reverse DNS lookups for this to work. The Kerberos interaction method must be **`gssapi-with-mic`**.

Enable SSH Local Security Checks

This section provides a high-level procedure for enabling SSH between the systems involved in the Tenable Nessus credential checks. It is not an in-depth tutorial on SSH, and assumes the reader has the prerequisite knowledge of Linux system commands.

Generate SSH Public and Private Keys

The first step is to generate a private/public key pair for the Tenable Nessus scanner to use. You can generate this key pair from any of your Linux systems, using any user account. However, it is important that the defined Tenable Nessus user owns the keys.

To generate the key pair, use `ssh-keygen` and save the key in a safe place (see the following Red Hat ES 3 installation example).

```
# ssh-keygen -t ecdsa -b 521
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/test/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/test/.ssh/id_ecdsa
Your public key has been saved in /home/test/.ssh/id_ecdsa.pub
The key fingerprint is:
SHA256:xL27sSSquFGQ2jhemuZGDdtt8lXL3nuUcOVrDIHtfi0 test@ubuntu2204-test
The key's randomart image is:
+---[ECDSA 521]---+
|            o    |
|   .   . . . o . |
|  o     o . . +  |
| = .   . . o + . |
|+ *.o   S o + + o|
|.++= o . o . +E=.|
|.=. + . o = . o. |
|o. o . . + = .   |
|..o....   o.o    |
+----[SHA256]-----+
#
```

Note: If you experience SSH key compatibility issues when authenticating to an SSH server, you can generate a key using the `dsa` command instead of `ecdsa`:

```
ssh-keygen -t dsa
```

Do not transfer the private key to any system other than the one running the Tenable Nessus server. When `ssh-keygen` asks you for a passphrase, enter a strong passphrase or press the **Return** key twice (that is, do not set any passphrase). If you specify a passphrase, you must specify it in **Policies** > **Credentials** > **SSH settings** for Tenable Nessus to use key-based authentication.

Create a User Account and Set Up the SSH Key

On every target system that you want to scan using local security checks, create a new user account dedicated to Tenable Nessus. This user account must have exactly the same name on all systems. For this document, we call the user `nessus`, but you can use any name.

Once you create the user account, make sure that the account has no valid password set. On Linux systems, new user accounts are locked by default, unless you explicitly set an initial password. If you are using an account where someone had set a password, use the `passwd -l` command to lock the account.

You must also create the directory under this new account's home directory to hold the public key. For this exercise, the directory is `/home/nessus/.ssh`. See the following Linux systems example:

```
# passwd -l nessus
# cd /home/nessus
# mkdir .ssh
#
```

For Solaris 10 systems, Sun has enhanced the `passwd(1)` command to distinguish between locked and non-login accounts. This is to ensure that you cannot use a locked user account to execute commands (for example, cron jobs). You can only use non-login accounts to execute commands, and they do not support an interactive login session. These accounts have the "NP" token in the password field of `/etc/shadow`. To set a non-login account and create the SSH public key directory in Solaris 10, run the following commands:

```
# passwd -N nessus
# grep nessus /etc/shadow
nessus:NP:13579::::::
# cd /export/home/nessus
# mkdir .ssh
#
```

Now that you have created the user account, you must transfer the key to the system, place it in the appropriate directory, and set the correct permissions.

Example

From the system containing the keys, secure-copy the public key to the system that you want to scan for host checks as shown in the following example.

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
#
```

You can also copy the file from the system on which you installed Tenable Nessus using the secure ftp command, **sftp**. You must name the file on the target system `authorized_keys`.

Return to the Public Key System

Set the permissions on both the `/home/nessus/.ssh` directory and the `authorized_keys` file.

```
# chown -R nessus:nessus ~nessus/.ssh/
# chmod 0600 ~nessus/.ssh/authorized_keys
# chmod 0700 ~nessus/.ssh/
#
```

Repeat this process on all systems that you want to test for SSH checks (starting at Create a User Account and Set Up the SSH Key).

Test to make sure that the accounts and networks are configured correctly. Using the simple Linux command `id`, from the Tenable Nessus scanner, run the following command:

```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

If it successfully returns information about the Tenable Nessus user, the key exchange was successful.

What to do next:

- Configure Tenable Nessus for SSH host-based checks.

Configure a Tenable Nessus Scan for SSH Host-Based Checks

> **Required user role when using Tenable Nessus Manager:** Standard, Administrator, or System Administrator

Tenable Nessus allows you to configure your scan configurations with the credentials needed for local macOS or Linux checks. You can do so during the Create a Scan process, or you can add credentials to an existing scan configuration.

If you have not already done so, configure the host system for credentialed scanning by completing the steps in Credentialed Checks on macOS or Credentialed Checks on Linux, depending on the host's operating system.

To configure SSH host-based checks in the Tenable Nessus user interface:

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

   The My Scans page appears.

2. Do one of the following:

   - Click **New Scan** to create a new scan and select a template.
   - Click **My Scans** in the left navigation bar, choose an existing scan, then click the **Configure** button.

3. Click the **Credentials** tab.
4. Select **SSH**.
5. In the **Authentication method** drop-down box, select an authentication method.
6. Configure the remaining settings.
7. Click the **Save** button.