



Tenable Nessus 10.5.x User Guide

Last Updated: May 19, 2023



Table of Contents

Welcome to Tenable Nessus 10.5.x	14
Get Started with Tenable Nessus	18
Navigate Tenable Nessus	20
System Requirements	21
Hardware Requirements	22
Software Requirements	26
Customize SELinux Enforcing Mode Policies	28
Licensing Requirements	29
Deployment Considerations	31
Port Requirements	32
Host-Based Firewalls	34
IPv6 Support	35
Network Address Translation (NAT) Limitation	36
Antivirus Software	37
Security Warnings	38
Certificates and Certificate Authorities	39
Custom SSL Server Certificates	41
Create a New Server Certificate and CA Certificate	43
Upload a Custom Server Certificate and CA Certificate	45
Trust a Custom CA	49
Create SSL Client Certificates for Login	51
Tenable Nessus Manager Certificates and Tenable Nessus Agent	54
Install Nessus	56



Download Nessus	57
Install Nessus	58
Install Nessus on Linux	59
Install Nessus on Windows	61
Install Nessus on macOS	63
Install Nessus on Raspberry Pi	66
Deploy Nessus as a Docker Image	67
Install Tenable Nessus Agents	73
Retrieve the Nessus Agent Linking Key	74
Link an Agent to Tenable Nessus Manager	75
Upgrade Nessus and Nessus Agents	78
Upgrade Nessus	79
Upgrade from Evaluation	80
Update Nessus Software	81
Upgrade Nessus on Linux	84
Upgrade Nessus on Windows	85
Upgrade Nessus on macOS	86
Update a Nessus Agent	87
Downgrade Nessus Software	88
Configure Nessus	91
Install Nessus Essentials, Professional, Expert, or Manager	93
Activate a Nessus Professional or Expert Trial	96
Link to Tenable Vulnerability Management	98
Link to Nessus Manager	103



Link to Tenable Security Center	105
Manage Activation Code	107
View Activation Code	108
Reset Activation Code	109
Update Activation Code	110
Transfer Activation Code	112
Manage Tenable Nessus Offline	114
Install Nessus Offline	116
Generate Challenge Code	119
Generate Your License	121
Download and Copy License File (nessus.license)	122
Register Your License with Nessus	123
Download and Copy Plugins	124
Install Plugins Manually	125
Update the Audit Warehouse Manually	127
Update Nessus Manager Manually on an Offline System	129
Offline Update Page Details	131
Back Up Nessus	132
Restore Nessus	133
Remove Nessus and Nessus Agents	134
Remove Nessus	135
Uninstall Nessus on Linux	136
Uninstall Nessus on Windows	138
Uninstall Nessus on macOS	139



Remove Nessus as a Docker Container	140
Remove Nessus Agent	141
Uninstall a Nessus Agent on Linux	142
Uninstall a Nessus Agent on Windows	143
Uninstall a Nessus Agent on macOS	145
Warning Messages	146
Scans	158
Scan Templates	160
Scan and Policy Settings	170
Basic Settings for Scans	172
Scan Targets	178
Basic Settings for Policies	181
Discovery Scan Settings	183
Preconfigured Discovery Scan Settings	193
Assessment Scan Settings	216
Preconfigured Assessment Scan Settings	233
Report Scan Settings	242
Advanced Scan Settings	244
Preconfigured Advanced Scan Settings	252
Credentials	259
Cloud Services Credentials	261
Database Credentials	264
Database Credentials Authentication Types	271
Host Credentials	285



SNMPv3	286
SSH	288
Windows	307
Miscellaneous Credentials	327
Mobile Credentials	334
Patch Management Credentials	339
Plaintext Authentication Credentials	349
Compliance	354
Upload a Custom Audit File	357
SCAP Settings	360
Plugins	362
Configure Dynamic Plugins	363
Create and Manage Scans	365
Example: Host Discovery	366
Create a Scan	368
Create an Attack Surface Discovery Scan with Bit Discovery	369
Import a Scan	371
Create an Agent Scan	372
Modify Scan Settings	373
Configure vSphere Scanning	374
Configure an Audit Trail	376
Launch a Scan	377
Stop a Running Scan	378
Delete a Scan	379



Scan Folders	380
Manage Scan Folders	382
Scan Results	384
Severity	387
CVSS Scores vs. VPR	388
Configure Your Default Severity Base	392
Configure Severity Base for an Individual Scan	394
Create a New Scan from Scan Results	396
Search and Filter Results	398
Compare Scan Results	406
Dashboard	408
View Scan Summary	410
Vulnerabilities	412
View Vulnerabilities	413
Modify a Vulnerability	414
Group Vulnerabilities	415
Snooze a Vulnerability	417
Live Results	419
Enable or Disable Live Results	421
Remove Live Results	422
Scan Exports and Reports	423
Export a Scan	425
Policies	427
Create a Policy	429



Import a Policy	430
Modify Policy Settings	431
Delete a Policy	432
About Nessus Plugins	433
Create a Limited Plugin Policy	435
Install Plugins Manually	439
Plugin Rules	441
Create a Plugin Rule	443
Modify a Plugin Rule	444
Delete a Plugin Rule	445
Customized Reports	446
Create a Scan Report	447
Customize Report Title and Logo	449
Create a Custom Report Template	450
Copy a Report Template	452
Edit a Custom Report Template	453
Delete a Custom Report Template	454
Terrascan	455
Create a Terrascan Scan Configuration	457
Launch a Terrascan Scan	461
Download Terrascan Results	462
Terrascan Scan History	463
View Terrascan Violations	465
Export a Summary of Violations	467



View Terrascan Passed Rules	468
Edit a Terrascan Scan Configuration	470
Delete a Terrascan Scan Configuration	474
Sensors (Nessus Manager)	475
Agents	476
Modify Agent Settings	478
Global Agent Settings	479
Remote Agent Settings	481
Filter Agents	489
Export Agents	491
Download Linked Agent Logs	492
Restart an Agent	494
Unlink an Agent	496
Delete an Agent	498
Agent Groups	499
Create a New Agent Group	500
Configure User Permissions for an Agent Group	502
Add Agents to an Agent Group	504
Modify an Agent Group	505
Delete an Agent Group	507
Agent Updates	508
Configure Agent Update Plan	509
Configure the Offered Nessus Agent Version	510
Freeze Windows	512



Create a Freeze Window	513
Modify a Freeze Window	514
Delete a Freeze Window	515
Modify Global Freeze Window Settings	516
Clustering	518
Clustering System Requirements	520
Enable Clustering	522
Migrate Agents to a Cluster	523
Link Agents to a Cluster	525
Manage Nodes	528
Get Linking Key from Node	529
Link a Node	530
View or Edit a Node	533
Enable or Disable a Node	535
Rebalance Nodes	536
Delete a Node	538
Cluster Groups	539
Create a Cluster Group	540
Add a Node to a Cluster Group	541
Add an Agent to a Cluster Group	543
Move an Agent to a Cluster Group	545
Move a Node to a Cluster Group	547
Modify a Cluster Group	549
Delete a Cluster Group	550



Scanners	551
Link Nessus Scanner	552
Unlink Nessus Scanner	553
Enable or Disable a Scanner	554
Remove a Scanner	555
Download Managed Scanner Logs	556
Settings	558
About	559
Download Logs	561
Set an Encryption Password	562
Advanced Settings	564
Create a New Setting	607
Modify a Setting	608
Delete a Setting	609
LDAP Server (Nessus Manager)	610
Configure an LDAP Server	612
Proxy Server	614
Configure a Proxy Server	616
Remote Link	618
SMTP Server	621
Configure an SMTP Server	623
Custom CA	625
Upgrade Assistant	626
Password Management	627



Configure Password Management	629
Scanner Health	630
Monitor Scanner Health	633
Advanced Debugging - Packet Capture	634
Notifications	638
Acknowledge Notifications	639
View Notifications	640
Accounts	641
My Account	642
Modify Your User Account	643
Generate an API Key	644
Users	645
Create a User Account	647
Modify a User Account	648
Delete a User Account	649
Transfer User Data	650
Additional Resources	651
Amazon Web Services	652
Command Line Operations	653
Start or Stop Nessus	654
Start or Stop a Nessus Agent	656
Nessus-Service	658
Nessuscli	661
Nessuscli Agent	673



Update Nessus Software (CLI)	683
Configure Tenable Nessus for NIAP Compliance	684
Default Data Directories	687
Encryption Strength	688
File and Process Allowlist	689
Manage Logs	692
Mass Deployment Support	700
Nessus Environment Variables	701
Deploy Tenable Nessus using JSON	703
Nessus Credentialed Checks	707
Credentialed Checks on Windows	709
Prerequisites	713
Enable Windows Logins for Local and Remote Audits	714
Configure a Nessus Scan for Windows Logins	717
Credentialed Checks on Linux	718
Prerequisites	719
Enable SSH Local Security Checks	720
Configure Nessus for SSH Host-Based Checks	723
Run Nessus as Non-Privileged User	724
Run Nessus on Linux with Systemd as a Non-Privileged User	725
Run Nessus on Linux with init.d Script as a Non-Privileged User	728
Run Nessus on macOS as a Non-Privileged User	731
Run Nessus on FreeBSD as a Non-Privileged User	736
Upgrade Assistant	740



Welcome to Tenable Nessus 10.5.x

If you are new to Tenable Nessus®, see [Get Started with Tenable Nessus](#).

To get started with creating a scan, see [Create a Scan](#).

- To create a compliance scan, configure [Compliance](#) settings for the scan.
- To create a host discovery scan, see [Example: Host Discovery](#).

Nessus Solutions

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 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 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 Nessus knowledge base and support ticket creation

[Tenable Vulnerability Management Product Page](#)

[Tenable Vulnerability Management User Manual](#)

Tenable Nessus Professional

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

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, Nessus sets the standard for vulnerability scanning speed and accuracy.

[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 stand-



ard 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 Nessus Agent deployment options, easily extends to mobile, transient, and other hard-to-reach environments.

Tenable Nessus Agent

For Tenable Nessus Agent documentation, see the [Tenable Nessus Agent User Guide](#).

Nessus 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 Nessus Agents are lightweight, low-footprint programs that you install locally on hosts to supplement traditional network-based scanning or to provide visibility into gaps that traditional scanning misses. Tenable Nessus Agents collect vulnerability, compliance, and system data, and



report that information back to a manager for analysis. With Tenable Nessus 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 Nessus Agents help you address the challenges of traditional network-based scanning, specifically for the assets where it's impossible or nearly impossible to consistently collect information about your organization's security posture. Traditional 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 Nessus 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 Nessus 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 Nessus Agents with Tenable Nessus Manager or Tenable Vulnerability Management.

[Nessus Agents Product Page](#)



Get Started with Tenable Nessus

Prepare

- Ensure that your setup meets the minimum system requirements:
 - [Hardware Requirements](#)
 - [Software Requirements](#)
- Obtain your [Activation Code for Nessus](#).

Install and configure Tenable Nessus

- Follow the installation steps depending on your Nessus software and operating system, as described in [Install Nessus](#).
- 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.

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. Tenable sometimes refers to a user-defined template as a *policy*.

- 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 .



System Requirements

You can run Tenable Nessus in the following environments.

Environment			More Information
Tenable Core	Virtual	VMware	Requirements in the <i>Tenable Core User Guide</i>
		Microsoft Hyper-V	
	Cloud	Microsoft Azure	
	Hardware		
Other plat- forms	Virtual	VMware	Virtual Machine 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 Nessus deployments include raw network speed, the size of the network, and the configuration of Nessus.

Note: 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 about Tenable Core + Nessus, see [Requirements](#) in the *Tenable Core User Guide*.

Storage Requirements

You must install Tenable Nessus on direct-attached storage (DAS) devices. Tenable Nessus does not support storage area networks (SANs) or network-attached storage (NAS) configurations.

Tenable recommends a minimum of 1,000 MB of temporary space for the Nessus scanner to run properly.

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.

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	<p>CPU: 4 2GHz cores</p> <p>Memory: 4 GB RAM (8 GB RAM recommended)</p> <p>Disk space: 30 GB, not including space used by the host operating system</p> <p>Note: Your usage (e.g., scan results, plugin updates, and logs) increases the amount of disk space needed over time.</p>
Scanning more than 50,000 hosts per scan	<p>CPU: 8 2GHz cores</p> <p>Memory: 8 GB RAM (16 GB RAM recommended)</p> <p>Disk space: 30 GB, not including space used by the host operating system</p> <p>Note: Your usage (e.g., scan results, plugin updates, and logs) increases the amount of disk space needed over time.</p>

Tenable Nessus Manager

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

Scenario	Minimum Recommended Hardware
Nessus Manager with 0-10,000 agents	<p>CPU: 4 2GHz cores</p> <p>Memory: 16 GB RAM</p> <p>Disk space: 5 GB per 5,000 agents per concurrent scan</p> <p>Note: Scan results and plugin updates require more disk space over time.</p>
Nessus Manager with 10,001-20,000	<p>CPU: 8 2GHz cores</p>



Scenario	Minimum Recommended Hardware
agents	<p>Memory: 32 GB RAM</p> <p>Disk space: 5 GB per 5,000 agents per concurrent scan</p> <p>Note: Scan results and plugin updates require more disk space over time.</p> <p>Note: Engage with your Tenable representative for large deployments.</p>

Virtual Machine

You can install Tenable Nessus on a Virtual Machine that meets the same requirements.

Note: Using Network Address Translation (NAT) to connect your virtual machine to the network negatively affects many of the Tenable Nessus vulnerability checks, host enumeration, and operating system identification.

Nessus Agents

Tenable Nessus Agents are lightweight and only minimal system resources. Generally, a Tenable Nessus Agent uses 40 MB of RAM (all pageable). A Tenable Nessus Agent uses almost no CPU while idle, but is designed to use up to 100% of CPU when available during jobs.

For more information on Tenable Nessus Agent resource usage, see [Agent Software Footprint](#).

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

Hardware	Minimum Requirement
Processor	1 Dual-core CPU
Processor Speed	> 1 GHz
RAM	> 1 GB



Hardware	Minimum Requirement
Disk Space	<ul style="list-style-type: none">• Agents 7.7.x and earlier: > 1 GB, not including space used by the host operating system• Agents 8.0.x and later: > 3 GB, not including space used by the host operating system• Agents 10.0.x and later: > 2 GB, not including space used by the host operating system <p>The agent may require more space during certain processes, such as a <code>plugins-code.db</code> defragmentation operation.</p>
Disk Speed	15-50 IOPS

Note: You can control the priority of the Tenable Nessus Agent relative to the priority of other tasks running on the system. For more information see [Agent CPU Resource Control](#) in the *Tenable Nessus Agent Deployment and User Guide*.



Software Requirements

Tenable Nessus supports Mac, Linux, and Windows operating systems.

Tip: For information about Tenable Core + Nessus, see [System Requirements](#) in the *Tenable Core User Guide*.

Tenable Nessus Scanner, Tenable Nessus Manager, and Tenable Nessus Professional

For Tenable Nessus software requirements, see the [Nessus Software Requirements](#) in the *General Requirements User Guide*.

Nessus Agents

For Tenable Nessus Agent software requirements, see the [Agent Software Requirements](#) in the *General Requirements User Guide*.

Supported Browsers

Nessus supports the following browsers:

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

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.

PDF Report Requirements

The Nessus .pdf report generation feature requires the latest version of **Oracle Java** or **OpenJDK**.

Install **Oracle Java** or **OpenJDK** *prior* to installing Nessus.

Note: If you install **Oracle Java** or **OpenJDK** *after* you install Nessus, you must reinstall Nessus to enable PDF report generation.



Customize SELinux Enforcing Mode Policies

Security-Enhanced Linux (SELinux) enforcing mode policies require customization to interact with 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 Nessus.
4. Run the `sealert` tool again to confirm you resolved the error alerts.



Licensing Requirements

Nessus is available to operate either as a subscription or managed by Tenable Security Center. Tenable Nessus requires a plugin feed Activation Code to operate in subscription mode. This code identifies which version of Tenable Nessus that Tenable licensed you to install and use, and if applicable, how many IP addresses you can scan, how many remote scanners you can link to Tenable Nessus, and how many Nessus 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.

Tenable recommends that you obtain the Activation Code before starting the installation process, as it is required before you can set up Tenable Nessus.

Your activation code:

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

Note: For more information about managing Tenable Nessus offline, refer to the [Nessus User Guide](#).

You may purchase a Tenable Nessus subscription through the Tenable, Inc. online store at <https://store.tenable.com/> or via a purchase order through [Authorized Nessus Partners](#). You will then receive an Activation Code from Tenable, Inc.. This code will be used when configuring your copy of Tenable Nessus for updates.

Note: See the [Obtain an Activation Code page](#) to obtain an Activation Code.

If you are using Tenable Security Center to manage your Nessus scanners, the Activation Code and plugin updates are managed from Tenable Security Center. You must start Nessus before it communicates with Tenable Security Center, which it normally does not do without a valid Activation Code and plugins. To have 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**.



Deployment Considerations

When deploying 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 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 Nessus scan.

Certain network devices that perform stateful inspection, such as firewalls, load balancers, and Intrusion Detection/Prevention Systems, may react negatively when Nessus conducts a scan through them. 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 Nessus Manager for agent management, Tenable does not recommend using 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 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](#)



Port Requirements

Tenable Nessus port requirements include Tenable Nessus Manager, Tenable Nessus Professional, Tenable Nessus Expert, Tenable Nessus Essentials, and Tenable Nessus scanner-specific requirements and Tenable Nessus Agent-specific requirements.

- [Tenable Nessus Manager, Tenable Nessus Professional, Tenable Nessus Expert, Tenable Nessus Essentials, and Tenable Nessus Scanners](#)
- [Tenable Nessus Agents](#)

Tenable Nessus Manager, Tenable Nessus Professional, Tenable Nessus Expert, Tenable Nessus Essentials, and Tenable Nessus Scanners

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. Communicating with the <code>plugins.nessus.org</code> server for plugin updates.
UDP 53	Performing DNS resolution.



Tenable Nessus Agents

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

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 443	Communicating with Tenable Vulnerability Management.
TCP 8834	Communicating with Tenable Nessus Manager. Note: The default Tenable Nessus Manager port is TCP 8834. However, this port is configurable and may be different for your organization.
UDP 53	Performing DNS resolution.



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 on RHEL 7, CentOS 7, and Fedora 20+ systems 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 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 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 Nessus folders, files, and processes in security products, see [File and Process Allowlist](#).



Security Warnings

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

During the web-based portion of the 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 Nessus user interface ([https://\[server IP\]:8834](https://[server IP]:8834)).

Example Security Warning

- a connection privacy problem
- an untrusted site
- an unsecure connection

Because 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 Nessus login page.

Browser	Instructions
Google Chrome	Select Advanced , and then Proceed to example.com (unsafe) . Note: Some instances of Google Chrome 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 .



Certificates and Certificate Authorities

Tenable Nessus includes the following defaults:

- The default Tenable Nessus SSL certificate and key, which consists of two files: `server-cert.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`.

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.
- [Create SSL Client Certificates for Login](#) – Create an SSL client certificate to log in to Tenable Nessus instead of using a username and password.
- [Trust a Custom CA](#) – Add a custom root CA to the list of CAs that Tenable Nessus trusts.
- [Tenable Nessus Manager Certificates and Tenable Nessus Agent](#) – Understand the certificate chain between Tenable Nessus Manager and Tenable Nessus Agents and troubleshoot issues.

Location of Certificate Files

Operating System	Directory
Linux	<code>/opt/nessus/com/nessus/CA/servercert.pem</code> <code>/opt/nessus/var/nessus/CA/serverkey.pem</code> <code>/opt/nessus/com/nessus/CA/cacert.pem</code> <code>/opt/nessus/var/nessus/CA/cacert.key</code>



Operating System	Directory
FreeBSD	<code>/usr/local/nessus/com/nessus/CA/servercert.pem</code> <code>/usr/local/nessus/var/nessus/CA/serverkey.pem</code> <code>/usr/local/nessus/com/nessus/CA/cacert.pem</code> <code>/usr/local/nessus/var/nessus/CA/cacert.key</code>
Windows	<code>C:\ProgramData\Tenable\Nessus\nessus\CA\servercert.pem</code> <code>C:\ProgramData\Tenable\Nessus\nessus\CA\serverkey.pem</code> <code>C:\ProgramData\Tenable\Nessus\nessus\CA\cacert.pem</code> <code>C:\ProgramData\Tenable\Nessus\nessus\CA\cacert.key</code>
macOS	<code>/Library/Nessus/run/com/nessus/CA/servercert.pem</code> <code>/Library/Nessus/run/var/nessus/CA/serverkey.pem</code> <code>/Library/Nessus/run/com/nessus/CA/cacert.pem</code> <code>/Library/Nessus/run/var/nessus/CA/cacert.key</code>



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, 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: <ul style="list-style-type: none">• Get the Tenable Nessus self-signed certificate signed by a trusted root CA, and upload that trusted CA to your browser.



	<ul style="list-style-type: none">• Use the /getcert path to install the root CA in your browsers. Go to the following address in your browser: <code>https://[IP address]:8834/getcert</code>.• Upload your own custom certificate and custom CA to your browser:<ol style="list-style-type: none">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.
<p>Plugin 51192 reports that the Tenable Nessus server certificate is untrusted.</p> <p>For example:</p> <ul style="list-style-type: none">• The certificate expired• The certificate is self-signed and therefore untrusted	<p>Do any of the following:</p> <ul style="list-style-type: none">• 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:<ol style="list-style-type: none">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.
<p>Plugin 51192 reports that an unknown CA was found at the top of the certificate chain.</p>	<p>Add your custom root CA to the list of CAs that Nessus trusts, as described in Trust a Custom CA.</p>



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 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
```

macOS

```
# /Library/Nessus/run/sbin/nessuscli mkcert
```

Windows

```
C:\Program Files\Tenable\Nessus\nessuscli.exe 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 also 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.

For the location of the default certificate files for your operating system, see [Location of Certificate Files](#).

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/com/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.em 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.em /Library/NessusAgent/run/var/nessus/CA/cakey.em
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 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

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: 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)

Before you begin:

- If you are using a custom CA, configure Nessus to trust certificates from your CA, as described in [Trust a Custom CA](#).

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. Set Nessus to allow SSL client certificate authentication.

Linux

```
# /opt/nessus/sbin/nessuscli fix --set force_pubkey_auth=yes
```

macOS

```
# /Library/Nessus/run/sbin/nessuscli fix --set force_pubkey_auth=yes
```

Windows

```
C:\Program Files\Tenable\Nessus\nessuscli.exe fix --set force_pubkey_auth-h=yes
```



3. Create a client certificate for each user you want to be able to log in to Tenable Nessus via SSL authentication.

a. On the 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.

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.

4. Upload the certificate to your browser's personal certificate store.

Refer to the documentation for your browser.

5. [Restart](#) the Nessus service.
6. Log in to Tenable Nessus via `https://<Nessus IP address or hostname>:8834` and select the username you created.



Tenable Nessus Manager Certificates and Tenable Nessus 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 Nessus 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.

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_certificate.pem
```

- **macOS**

```
/Library/NessusAgent/run/lib/nessus/users/nessus_ms_agent/ms_cert.pem
```

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.



Install Nessus

This section includes information and steps required for installing Nessus on all supported operating systems.

- [Install Nessus on macOS](#)
- [Install Nessus on Linux](#)
- [Install Nessus on Windows](#)
- [Install Nessus on Raspberry Pi](#)
- [Deploy or Install Tenable Core + Nessus](#)
- [Deploy Nessus as a Docker Image](#)



Download Nessus

You can download Nessus from the [Tenable Downloads site](#).

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

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



Install Nessus

This section describes how to install Nessus Manager, Nessus Professional, and Nessus Expert on the following operating systems:

- [Linux](#)
- [Windows](#)
- [macOS](#)
- [Raspberry Pi](#)
- [Deploy Nessus as a Docker Image](#)



Install Nessus on Linux

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

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

To install Nessus on Linux:

1. [Download](#) the Nessus package file.
2. From the command line, run the Nessus installation command specific to your operating system.

Example Nessus install commands:

Red Hat version 6

```
# yum install Nessus-<version number>-es6.x86_64.rpm
```

Debian version 6

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

FreeBSD version 10

```
# pkg add Nessus-<version number>-fbsd10-amd64.txz
```

3. From the command line, restart the `nessusd` daemon.

Example Nessus daemon start commands:

Red Hat, CentOS, Oracle Linux, Fedora, SUSE, FreeBSD

```
# systemctl start nessusd
```

Debian/Kali and Ubuntu

```
# systemctl start nessusd
```



4. 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>.

5. Perform the remaining [Nessus installation steps](#) in your browser.



Install Nessus on Windows

Caution: If you install a Nessus Agent, Manager, or Scanner on a system with an existing Nessus Agent, Manager, or Scanner running `nessusd`, the installation process will kill 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

For details, refer to the [Product Download](#) topic.

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. 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, Inc. 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 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 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>.

Perform the remaining [Nessus installation steps](#) in your web browser.



Install Nessus on macOS

Caution: If you install a Nessus Agent, Manager, or Scanner on a system with an existing Nessus Agent, Manager, or Scanner running `nessusd`, the installation process will kill 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 Nessus Package File

For details, refer to the [Product Download](#) topic.

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-<Nessus_Version>.dmg`
 - 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 Nessus on Raspberry Pi

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

1. Download the Nessus package file. For details, see [Download Nessus](#).
2. From a command prompt or terminal window, run the Nessus installation command:

```
dpkg -i Nessus-10.0.0-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 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>.
5. Perform the remaining [Nessus installation steps](#) in your browser.



Deploy 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 and Ubuntu. 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 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 2 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. 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 Nessus as a Docker image:

- To stop and remove the container, see [Remove Nessus as a Docker Container](#).

Operators

Operator	Description
<code>--name</code>	Sets the name of the container in Docker.
<code>-d</code>	Starts a container in detached mode.
<code>-p</code>	<p>Publishes to the specified port in the format <i>host port:container port</i>. By default, the port is 8834:8834.</p> <p>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.</p>
<code>-e</code>	<p>Precedes an environment variable.</p> <p>For descriptions of environment variables you can set to configure settings in your Tenable Nessus instance, see Environment Variables.</p>

Environment Variables

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



Deploying a 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 to appear 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.
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.
Nessus Settings		
AUTO_UPDATE	No	<p>Sets whether Tenable Nessus should automatically receive updates.</p> <p>Valid values are as follows:</p> <ul style="list-style-type: none">• <code>all</code> – (Default) Automatically update plugins and Tenable Nessus software.• <code>plugins</code> – 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.io linking key> -e USERNAME=admin -e PASSWORD=admin -e MANAGER_HOST=cloud.tenable.com -e MANAGER_PORT=443 tenable/nessus:<version-OS>
```

Deploying a 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.sc 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 to appear in the manager. By default, the name is the container ID.
GROUPS	No	The name of the existing scanner group or groups that you want to add the scanner to. 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"
CA-PATH	No	The location of the CA certificate related to the scanner.
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 -e PASSWORD=admin -e PROXY-HOST=cloud.tenable.com -e PROXY-PORT=443 -e AWS-SCANNER=true 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 Nessus images

Variable	Required?	Description
USERNAME	No	Creates the administrator user.



PASSWORD	No	Creates the password for the user.
----------	----	------------------------------------



Install Tenable Nessus Agents

To install agents, use the procedures described in the [Nessus Agent User Guide](#).

Once installed, Tenable Nessus Agents are linked to 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.

Once installed, an agent links 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. Agents automatically download plugins from the manager upon linking; this process can take several minutes and you before an agent can return scan results.



Retrieve the Nessus Agent Linking Key

Before you begin the Tenable Nessus 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 Nessus Agent](#)



Link an Agent to Tenable Nessus Manager

After you install Tenable Nessus Agent, link the agent to Tenable Nessus Manager.

Before you begin:

- [Retrieve the linking key](#) from Tenable Nessus Manager.
- [Install Tenable Nessus Agent](#).

To link Tenable Nessus Agent to Tenable Nessus Manager:

1. Log in to the Tenable Nessus 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=00abcd0000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00
--name=LinuxAgent --groups=All --host=yourcompany.com --port=8834
```

macOS:

```
# /Library/NessusAgent/run/sbin/nessuscli agent link
--key=00abcd0000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00
--name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
```

Windows:

```
# C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
--key=00abcd0000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00
--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	<p>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.</p> <p>List multiple groups in a comma-separated list. If any group names have spaces, use quotes around the whole list.</p> <p>For example: <code>--groups="Atlanta, Global Headquarters"</code></p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: The agent group name is case-sensitive and must match exactly.</p></div>
--offline-install	no	<p>When enabled (set to "yes"), installs Tenable Nessus Agent on the system, even if it is offline. Tenable Nessus Agent periodically attempts to link itself to its manager.</p> <p>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.</p>
--proxy-host	no	The hostname or IP address of your proxy server.
--proxy-port	no	The port number of the proxy server.



<code>--proxy-pass-word</code>	no	The password of the user account that you specified as the username.
<code>--proxy-user-name</code>	no	The name of a user account that has permissions to access and use the proxy server.
<code>--proxy-agent</code>	no	The user agent name, if your proxy requires a preset user agent.



Upgrade Nessus and Nessus Agents

This section included information for upgrading Nessus and Nessus Agents on all supported operating systems.

- [Upgrade Nessus](#)
 - [Upgrade from Evaluation](#)
 - [Update Nessus Software](#)
 - [Upgrade Nessus on macOS](#)
 - [Upgrade Nessus on Linux](#)
 - [Upgrade Nessus on Windows](#)
- [Update a Nessus Agent](#)
- [Downgrade Nessus Software](#)



Upgrade Nessus

This section includes information for upgrading Nessus.


- [Upgrade from Evaluation](#)
- [Update Nessus Software](#)
- [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 Nessus, type your full-version activation code on the **Settings** page, on the **About** tab.

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 Nessus Software

Note: For information about upgrading an offline Tenable Nessus Manager that manages Tenable Nessus scanners, see [Update Nessus Manager Manually 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 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 Nessus to download plugins.

7. Click the **Save** button.

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.

Nessus downloads any available updates.



Upgrade Nessus on Linux

Download Nessus

From the [Tenable Downloads Page](#), download the latest, full-license version of Nessus.

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, SUSE

```
# dnf upgrade 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, FreeBSD

```
# 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

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.

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

The process of upgrading Nessus on a Mac using the Nessus installation GUI is the same process as a new [Mac Install](#).



Update a Nessus Agent

After you install an agent, Tenable Nessus Manager automatically updates the agent software based on the agent update plan. For more information on configuring the agent update plan, see [Agent Updates](#).

Note: In addition to using the agent update plan, you can manually update agents through the command line. For more information, see the [Tenable Nessus Agent User Guide](#).



Downgrade Nessus Software

Tenable Nessus 8.10.0 and later supports the ability to downgrade Tenable Nessus to a previous version of Tenable Nessus. You cannot downgrade to a version before 8.10.0.

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 Nessus backup file](#).
- If Tenable Nessus has an encryption password, you cannot downgrade by changing the 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 Nessus encryption password, see the [How to remove the encryption password \(formerly master password\) through the command-line](#) knowledge base article. To set the Nessus encryption password after downgrading, see [Set an Encryption Password](#).

To downgrade Nessus manually on Linux or macOS:

Note: To manually downgrade 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 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 Nessus version you want to install.
- b. Manually [install](#) the Nessus version. Force install the new Nessus rpm file over the current rpm file.



macOS

- a. [Download](#) the Nessus version you want to install.
- b. Manually [install](#) the Nessus version. Replace the current 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 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.

Nessus saves the update plan.



Configure Nessus

When you access 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. 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 + Nessus, see [Deploy or Install Tenable Core](#) in the *Tenable Core + Nessus User Guide*.

Before you begin:

- [Install Nessus](#).

To configure Tenable Nessus:

1. Follow the [Install 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 Nessus to the Internet for installation.
 - (Optional) Click **Settings** to configure the following Nessus settings manually.
 - [Proxy Server](#) – Configure a proxy server.

Note: You must enter a proxy server if you want to link the 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 Nessus plugin feed.
- [Encryption Password](#) – Enter a Nessus encryption 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 Nessus online, follow the configuration steps for your selected product:
 - [Install Nessus Essentials, Professional, Expert, or Manager](#)
 - [Activate a Nessus Professional or Expert Trial](#)
 - [Link to Tenable Vulnerability Management](#)
 - [Link to Tenable Security Center](#)
 - [Link to Nessus Manager](#)
 - [Link a Node](#) (Tenable Nessus Manager cluster)
- If you are installing Nessus offline, continue at step 1 of [Install Nessus Offline](#).



Install 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 Nessus Professional or 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 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 Nessus 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. Nessus functionality will be limited until compilation is complete.* You cannot create scans, view policies or plugin rules, or use the upgrade assistant while Tenable Nessus compiles plugins.



Activate a Nessus Professional or Expert Trial

This option activates 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 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. Enter the email address of your Tenable community account, or the email address you want to connect to your Tenable community account.

- If Nessus recognizes the email address, a page appears saying that Nessus found your account.
- If Nessus does not recognize the email address, the **Create Account** page appears.
 - a. Enter your new account information.

4. Click **Start Trial**.

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.

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 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. Nessus functionality will be limited until compilation is complete.* You cannot create scans, view 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.

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

Note: Once you link Tenable Nessus to Tenable Vulnerability Management, it remains linked until you [unlink it](#).

Before you begin:

- Configure Tenable Nessus as described in [Configure 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 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.io**.
4. In the **Linking Key** box, type the linking key of your Tenable Vulnerability Management instance.
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 Nessus](#).

Note: When running the `adduser` command in the following steps, create the user as a full administrator/system administrator when prompted.

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
```

```
# ./nessuscli adduser
```

3. Do one of the following:

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

```
# /opt/nessus/sbin/nessuscli managed link --key=<key> --host-t=fedcloud.tenable.com --port=443
```

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

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

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
```

```
> nessuscli adduser
```

3. Do one of the following:

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

```
> \opt\nessus\sbin\nessuscli managed link --key=<key> --host-t=fedcloud.tenable.com --port=443
```

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

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

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
```

```
# /Library/Nessus/run/sbin/nessuscli adduser
```



3. Do one of the following:

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

```
# /opt/nessus/sbin/nessuscli managed link --key=<key> --host-  
t=fedcloud.tenable.com --port=443
```

- 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
```

4. Run the following command:

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



Link to Nessus Manager

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

To manage your activation code, use the following topics:

- [View Activation Code](#)
- [Reset 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**.

View from Command Line

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

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



Reset Activation Code

You do not need to reset your activation code for the latest Tenable Nessus versions, and you are able to re-register the same license with your original activation code.

In Nessus Professional 7.x and earlier versions, if you uninstall and reinstall Nessus, you need to reset your activation code. Reset your activation code on the [Tenable Community site](#), as described in the [Tenable Community Guide](#).

Note: Reset codes have a 10-day waiting period before you can reset your code again.




Update Activation Code

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

Note: If you are working with Nessus offline, see [Manage Tenable Nessus Offline](#).

User Interface

1. In 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 Nessus.

Command Line Interface

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

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

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



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



Transfer Activation Code

In Nessus Professional 7.0 or later and 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 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 Nessus.

Nessus User Interface


Activate a new Nessus instance

1. [Install 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**.

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

Update an existing Nessus instance



1. Access the system on which you want to activate 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 Nessus.

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

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

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



Manage Tenable Nessus Offline

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

Scenario 1: New Nessus Install

If you want to install Nessus, but, for security purposes, the server is not connected to the internet, then follow the steps to [install Nessus while offline](#). This process downloads and installs Nessus plugins on the offline Nessus server.

Scenario 2: Update Nessus Licensing

If you have an existing Nessus server that is offline, and you want to update Nessus with the new license/activation code, then complete the following steps:

Caution: Tenable recommends saving the custom-offline plugin download URL described in step 5 before continuing to step 6. The URL appears only once after registration. If you close the registration window and forget the URL, you have to restart the registration process to generate a new URL.

1. [Generate Challenge Code](#).
2. [Generate Your License](#).
3. [Download and copy the license file \(nessus.license\)](#).
4. [Register Your License with Nessus](#).
5. [Download and copy plugins to Nessus](#).
6. [Install Plugins Manually](#).
7. [Update Nessus Manager Manually on an Offline System](#).

Scenario 3: Update Nessus Plugins

You have an existing Nessus server that is offline and you need to update Nessus plugins. In this scenario, you have already completed steps to [Install Nessus Offline](#) but you need to install the latest plugins.

In this case, perform the following operations:



1. Use the Custom URL that you saved and copied during your first offline [Download and Copy Plugins](#) operation.
2. [Download and Copy Plugins](#)
3. [Install Plugins Manually](#)

Nessus Offline Operations

For explanation purposes, we provide computers **A** (offline Nessus server) and **B** (online computer) to demonstrate operations performed when managing Nessus offline.

Operation	Computer A (Offline Nessus)	Computer B (Online Computer)
Generate Challenge Code	X	
Generate Your License		X
Download and Copy License File (nessus.license)		X
Download and Copy Plugins		X
Download and Copy Plugins	X	
Register Your License with Nessus	X	
Install Plugins Manually	X	



Install Nessus Offline

A Nessus **Offline** registration is suitable for computers that run Nessus, but are not connected to the internet. To ensure that Nessus has the most up-to-date plugins, Nessus servers not connected to the internet must perform these specific steps to register Nessus.

This process requires the use of two computers: the computer where you are installing 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 Nessus server) and **B** (online computer) as examples.

1. During the [browser portion](#) of the Nessus installation, on the **Welcome to Nessus** page, select **Register Offline**.
2. Click **Continue**.
3. Select the Nessus type that you want to deploy: Nessus Expert, Nessus Professional, 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 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:
aaaaaa1b2222cc33d44e5f6666a777b8cc99999.

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: aaaaaa1b2222cc33d44e5f6666a777b8cc99999

3. Next, where prompted, type your Nessus activation code.



Example Activation Code: AB-CDE-1111-F222-3E4D-55E5-CD6F

4. Click the **Submit** button.

The [Offline Update Page Details](#) 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.
- **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 still using the computer with internet access (**B**), select the on-screen, custom URL.

A compressed TAR file downloads.

Tip: This custom URL is specific to your Nessus license. Save it and use it each time you need to update plugins.

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

Use the directory specific to your operating system:

Platform	Command
Linux	<code># /opt/nessus/sbin/</code>
FreeBSD	<code># /usr/local/nessus/sbin/</code>
Windows	<code>C:\Program Files\Tenable\Nessus</code>
macOS	<code># /Library/Nessus/run/sbin/</code>

Copy and Paste License Text



1. While still using the computer with internet access (**B**), copy 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**.

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

4. Using the System Administrator account you created during setup, **Sign In** to Nessus.



Generate Challenge Code

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

Whereas you use an activation code when performing 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.

To generate a challenge code in Nessus:

1. Log in to Tenable Nessus.
2. Click **Settings**.
3. Click the pencil icon next to the activation code.

The **Update Activation Code** window appears.

4. In the **Registration** drop-down menu, select **Offline**.
5. Click **Activate**.

The challenge code appears in the window.

To generate a challenge code from the command line:

1. On the **offline** system running Nessus (**A**), open a command prompt.
2. Use the `nessuscli fetch --challenge` command specific to your operating system.

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

3. Copy the alphanumeric challenge code.

Example Challenge Code:



aaaaaa11b2222cc33d44e5f6666a777b8cc99999

4. Use the copied challenge code to [Generate Your License](#).



Generate Your License

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

However, if your 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 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 [generated challenge code](#).

1. On a system *with* internet access (**B**), navigate to the [Nessus Offline Registration Page](#).
2. Where prompted, type in your [challenge code](#).

Example Challenge Code: aaaaaa11b2222cc33d44e5f6666a777b8cc99999

3. Next, where prompted, enter your Nessus activation code.

Example Activation Code: AB-CDE-1111-F222-3E4D-55E5-CD6F

4. Select **Submit**.

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

5. Next, [Download and Copy License File \(nessus.license\)](#).



Download and Copy License File (nessus.license)

After you have [generated your Nessus license](#), you now need to download and then copy the license to the **offline** system (**A**) running Nessus.

1. At the [Nessus Offline Registration Page](#), while still using the computer with internet access (**B**), select the on-screen **nessus.license** link.
The link downloads the **nessus.license** file.
2. Copy the **nessus.license** file to the **offline** system (**A**) running Nessus 6.3 and newer.

Use the directory specific to your operating system:

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

3. Next, [register your license with Nessus](#).



Register Your License with Nessus

When you receive a new license and Activation Code, you must re-register the license with Nessus.

When your Nessus server is offline, you must [generate](#) a license, [download](#) the license, and then register your license with Nessus.

Once [downloaded and copied](#) to your offline Nessus server, use the **nessuscli fetch -- register** command that corresponds to your operating system.

1. On the **offline** system running Nessus (**A**), open a command prompt.
2. Use the **nessuscli fetch --register-offline** command specific to your operating system.

Platform	Command
Linux	<pre># /opt/nessus/sbin/nessuscli fetch --register-offline /opt/nessus/etc/nessus/nessus.license</pre>
FreeBSD	<pre># /usr/local/nessus/sbin/nessuscli fetch --register-offline /usr/local/nessus/etc/nessus/nessus.license</pre>
Windows	<pre>C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register-offline "C:\ProgramData\Tenable\Nessus\conf\nessus.license"</pre>
macOS	<pre># /Library/Nessus/run/sbin/nessuscli fetch --register-offline /Library/Nessus/run/etc/nessus/nessus.license</pre>



Download and Copy Plugins

Note: The following process is only intended for organizations that do not want to enable automatic plugin updates in their Nessus environment, or organizations that use offline environments. For information about automatic plugin updates and how to enable them, see [Update Nessus Software](#).

After submitting the required information on the [Offline Update Page Details](#), download the **Nessus Plugins** compressed TAR file.

Download Plugins

1. Using the computer with internet access (**B**), copy and save the on-screen custom URL link.

Note: This custom URL is specific to your Nessus license and you must use it each time you need to download and update plugins again.

Caution: Tenable recommends saving the custom URL before continuing. The URL is only shown once after registration. If you close the registration window and forget the URL, you have to restart the registration process to generate a new URL.

2. Click the on-screen custom URL link.
The link downloads the compressed TAR file.

Copy Plugins to Nessus

3. Copy the compressed TAR file to the **offline (A)** system.
Use the directory specific to your operating system:

Platform	Directory
Linux	# /opt/nessus/sbin/
FreeBSD	# /usr/local/nessus/sbin/
macOS	# /Library/Nessus/run/sbin/
Windows	C:\Program Files\Tenable\Nessus

4. Next, on the **offline (A)** system running Nessus, [Install Plugins Manually](#).



Install Plugins Manually

You can manually update Nessus plugins 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.

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, then click **Open**.

Tenable Nessus updates with the uploaded plugins.

To install plugins 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
Linux	<code># /opt/nessus/sbin/nessuscli update <tar.gz filename></code>
FreeBSD	<code># /usr/local/nessus/sbin/nessuscli update <tar.gz filename></code>
macOS	<code># /Library/Nessus/run/sbin/nessuscli update <tar.gz filename></code>
Windows	<code>C:\Program Files\Tenable\Nessus>nessuscli.exe update <tar.gz filename></code>

Tenable Nessus updates with the uploaded plugins.

Note: If you receive a signature check failure error, check the integrity of your plugins archive, download the plugins again, and retry the process. If the error persists, re-register Nessus or contact Tenable Support.



Update the Audit Warehouse Manually

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 filename>` command specific to your operating system.



Platform	Command
Linux	<code># /opt/nessus/sbin/nessuscli update <tar.gz filename></code>
FreeBSD	<code># /usr/local/nessus/sbin/nessuscli update <tar.gz filename></code>
Windows	<code>C:\Program Files\Tenable\Nessus>nessuscli.exe update <tar.gz filename></code>
macOS	<code># /Library/Nessus/run/sbin/nessuscli update <tar.gz filename></code>

Tenable Nessus updates with the uploaded audit files.



Update Nessus Manager Manually on an Offline System

Note: Use the following steps to upgrade an offline Tenable Nessus Manager that manages Tenable Nessus scanners. When upgrading other forms of Tenable Nessus offline (for example, Tenable Nessus Professional, a Tenable Nessus Manager not managing Tenable Nessus scanners, or Tenable Nessus scanners managed by Tenable Security Center), use the steps described in [Update Nessus Software](#).

On Nessus Manager, you can manually update software on an offline system in two ways.

- **Option 1:** Use the **Manual Software Update** feature in the Nessus 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 Nessus (**A**), in the top navigation bar, select **Settings**.
3. From the left navigation menu, select **Software Update**.
4. Select the **Manual Software Update** button.
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**.

Nessus 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 Nessus (**A**), open a command prompt.
3. Use the `nessuscli update <tar.gz filename>` command specific to your operating system.



Platform	Command
Linux	# /opt/nessus/sbin/nessuscli update <tar.gz filename>
FreeBSD	# /usr/local/nessus/sbin/nessuscli update <tar.gz filename>
Windows	C:\Program Files\Tenable\Nessus>nessuscli.exe update <tar.gz filename>
macOS	# /Library/Nessus/run/sbin/nessuscli update <tar.gz filename>



Offline Update Page Details

When you are working with Nessus offline, use the <https://plugins.nessus.org/v2/offline.php> page.

Based on the steps you are using to [Manage Tenable Nessus Offline](#), the resulting web page 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.
- **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.



Back Up Nessus

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

What to do next:

- [Restore Nessus](#)



Restore Nessus

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.

On Tenable Nessus 8.11.1 and later, 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 8.11.1, you can restore a backup from Tenable Nessus 8.10.0.

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.

Before you begin:

- [Back Up 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 Nessus and Nessus Agents

This section includes information for removing Nessus and Nessus Agents.

- [Remove Nessus](#)
 - [Uninstall Nessus on macOS](#)
 - [Uninstall Nessus on Linux](#)
 - [Uninstall Nessus on Windows](#)
 - [Remove Nessus as a Docker Container](#)
- [Remove Nessus Agent](#)
 - [Uninstall a Nessus Agent on macOS](#)
 - [Uninstall a Nessus Agent on Linux](#)
 - [Uninstall a Nessus Agent on Windows](#)



Remove Nessus

This section includes information for uninstalling and removing Nessus.

- [Uninstall Nessus on Linux](#)
- [Uninstall Nessus on Windows](#)
- [Uninstall Nessus on macOS](#)
- [Remove Nessus as a Docker Container](#)



Uninstall Nessus on Linux

Optional: Export your Scans and Policies

1. Go to the folder or folders where you store your scans.
2. Double-click the scan to view its dashboard.
3. In the upper right corner, select the **Export** button, and then choose the Nessus DB option.

Stop Nessus Processes

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

Examples: Nessus Daemon Stop Commands

Red Hat, CentOS, and Oracle Linux

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

SUSE

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

FreeBSD

```
# service nessusd stop
```

Debian/Kali and Ubuntu

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

Remove Nessus

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

Examples: Nessus Remove Commands



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, SUSE

```
# dnf remove Nessus
```

Debian/Kali and Ubuntu

```
# dpkg -r Nessus
```

FreeBSD

```
# pkg delete Nessus
```

2. 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
```

FreeBSD

```
# rm -rf /usr/local/nessus/bin
```

This completes the process of uninstalling the **Nessus** on the **Linux** operating systems.



Uninstall Nessus on Windows

1. (Optional) [Export](#) your scans and policies.
2. [Stop Nessus](#).
3. Uninstall Nessus from the Windows user interface or the CLI following the steps below:

To uninstall 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 Nessus.

4. Click **Yes**.

Windows uninstalls Nessus.

To uninstall Nessus from the Windows CLI:

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

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

Note: For information about optional `msiexec /x` parameters, see [msiexec](#) in the Microsoft documentation.



Uninstall Nessus on macOS

Stop Nessus

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.

Remove the following Nessus directories, subdirectories, or files

```
/Library/Nessus  
/Library/LaunchDaemons/com.tenablesecurity.nessusd.plist  
/Library/PreferencePanels/Nessus Preferences.prefPane  
/Applications/Nessus
```

Disable the Nessus service

1. To prevent the macOS from trying to start the now non-existent service, type the following command from a command prompt.

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

2. If prompted, provide the administrator password.



Remove 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>
```



Remove Nessus Agent

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

- [Uninstall a Nessus Agent on Linux](#)
- [Uninstall a Nessus Agent on Windows](#)
- [Uninstall a Nessus Agent on macOS](#)

Note: For instructions on how to remove an agent from a manager while leaving the agent installed on the host, see [Unlink an Agent](#).



Uninstall a Nessus Agent on Linux

Before you begin:

- [Unlink the agent](#) from the manager.

To uninstall Tenable Nessus Agent on Linux:

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

Example Nessus Agent Remove Commands

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, SUSE

```
# dnf remove Nessus
```

Debian/Kali and Ubuntu

```
# dpkg -r NessusAgent
```

FreeBSD

```
# pkg delete NessusAgent
```

What to do next:

- If you plan on reinstalling the Tenable Nessus Agent on the system, see the [knowledge base](#) article on how to avoid linking errors.



Uninstall a Nessus Agent on Windows

Before you begin:

- [Unlink the agent](#) from the manager.

To uninstall Tenable Nessus Agent from the Windows user interface:

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

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

4. Click **Yes**.

Windows deletes all Nessus related files and folders.

Note: On Windows, the Tenable Nessus Agent uninstall process automatically creates a [backup](#) file in the %TEMP% directory. If you reinstall Tenable Nessus Agent within 24 hours, Tenable Nessus Agent uses that backup file to [restore](#) the installation. If you want to reinstall Tenable Nessus Agent within 24 hours without using the backup, manually delete the backup file in the %TEMP% directory beforehand.

To uninstall Tenable Nessus Agent from the Windows CLI:

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

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

Note: For information about optional `msiexec /x` parameters, see [msiexec](#) in the Microsoft documentation.

What to do next:



- If you plan on reinstalling the Tenable Nessus Agent on the system, see the [knowledge base](#) article on how to avoid linking errors.



Uninstall a Nessus Agent on macOS

Before you begin:

- [Unlink the agent](#) from the manager.

To uninstall Tenable Nessus Agent on macOS:

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

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

2. Disable the Nessus Agent service:

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

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

b. If prompted, provide the administrator password.

What to do next:

- If you plan on reinstalling the Tenable Nessus Agent on the system, see the [knowledge base](#) article on how to avoid linking errors.



Warning Messages

The following table lists the warning 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
No valid targets in list	There were no valid targets in the scan's target list.	Verify that the scan's target list contains one or more targets in valid 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]	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]	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 Nessus Scan Target formats.



Restricted target [target name]	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 violates user-defined rules	Nessus cannot scan the target due to user-specified scanning restrictions.	Remove the target from the scan's target 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.	Nessus did not scan the target because the number of targets for a single scan exceeded the maximum allowed under the Nessus Essentials licensing terms.	Reduce the number of targets in the scan, or upgrade Nessus .
The licensed number of live hosts scanned has been reached - please contact Tenable to upgrade your license.	Nessus did not scan the target because the number of targets for a single scan exceeded the maximum allowed under the Nessus licensing terms.	Reduce the number of targets in the scan, or upgrade 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.	Nessus did not scan the target because the cumulative number of unique targets across all scans exceeded the maximum allowed under the Nessus Essentials licensing terms.	Remove targets from the scan to conform to the licensing terms, or upgrade Nessus .



<p>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.</p>	<p>Nessus did not scan the target because the cumulative number of unique targets across all scans exceeded the maximum allowed under the Nessus evaluation license terms.</p>	<p>Remove targets from the scan to conform to the licensing terms, or upgrade Nessus.</p>
<p>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</p>	<p>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.</p>	<p>Remove targets from the scan to conform to the licensing terms, or upgrade Nessus.</p>
<p>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</p>	<p>Nessus attempted to establish a session for sending or receiving raw IP packets, but failed.</p>	<p>Tenable recommends scanning over a different network interface.</p> <p>You may be able to resolve this problem by disabling the Ping the</p>



<p>port scan against them.</p>		<p>remote host scan setting and providing Nessus with credentials to the remote host to prevent a port scan from taking place.</p>
<p>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.</p>	<p>The Nessus scanner was installed in an unsupported VMWare Fusion configuration.</p>	<p>Install Nessus on a different host.</p>
<p>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</p>	<p>Packet forgery succeeded at least once on the reported interface, but a subsequent attempt to open a packet forgery session failed.</p>	<p>Verify the current values of, and adjust, the Nessus Advanced Settings related to scanner performance.</p> <p>If the problem persists, report the issue to Tenable. Include the full contents of the scanner logs <code>nessusd.messages</code></p>



number of scans and/or hosts scanned in parallel.		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	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 Nessus Advanced Settings related to scanning.
[target] has been turned off, crashed or became unreachable during the audit - scan was interrupted prior to completion	<p>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.</p> <p>This may be the result of a temporary network disruption, a service that failed or restarted on the target, or the target may have crashed or been removed from the network.</p>	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.
Some network con-	There were intermittent failures to con-	Verify the current val-



<p>gestion 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</p>	<p>nect to a target port that is known to be open.</p>	<p>ues of, and adjust, the Nessus Advanced Settings related to scanner performance.</p> <p>Increase the Network timeout setting in the scan policy, then re-scan.</p>
<p>Scan not started for Nessus Agent [agent name]</p>	<p>During an agent scan, the agent did not start the scan.</p>	<p>Check whether the agent is present on the network. Verify network connectivity between the agent and the Nessus Manager/Tenable.io.</p> <p>Re-run the agent scan once you verify the agent is online.</p>
<p>[count] Nessus Agents didn't start scan: [agent names]</p>	<p>During an agent scan, the agent did not start the scan.</p>	<p>Check whether each agent is present on the network. Verify network connectivity between the agents and the Nessus Manager/Tenable.io.</p>



		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 Nessus Manager/Tenable.io. 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 and the Nessus Manager/Tenable.io. 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 Nessus scanner uploaded a scan result to Nessus Manager, but Nessus Manager could not process the scan result.	Check if the Nessus Manager has enough disk space, or if the scan result uploaded by the scanner is cor-



		rupted 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 Nessus Manager, but the scan result could not be processed.	Check if the 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	<p>In a clustered scan, a cluster "child node" is a Nessus scanner that manages agents, and is managed by a Nessus Manager.</p> <p>This error happens when a scan result is uploaded by a child node to a Nessus Manager, but the result processing fails.</p>	Check if the Nessus Manager has enough disk space, or 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	A Nessus Compliance Audit scan spe-	Remove the deprecated



deprecated and was not executed: [audit file name]	cified an audit file that is no longer supported. The scan will proceed, but the deprecated audit file will be skipped.	audit from the scan settings.
It was not possible to email this scan: [error]	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 and can be reached from the scanner.
[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	Adjust your network security configuration or the report.max_ports preference.



	<p>been removed from the scan report. Usually this is due to intervening 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.</p>	
SYN scanner timeout	<p>The SYN port scan against [targets] timed out after [number of seconds] - TCP port results may be incomplete.</p>	<p>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:</p> <ul style="list-style-type: none">• Modify boundary device settings• Reduce the number of ports scanned• Increase the port scanner timeout <p>Contact Tenable Sup-</p>



		<p>port for guidance on how to increase the timeout.</p>
TCP scanner timeout	The TCP port scan against [targets] timed out after [number of seconds] - TCP port results may be incomplete.	<p>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:</p> <ul style="list-style-type: none">• Modify boundary device settings• Reduce the number of ports scanned• Increase the port scanner timeout <p>Contact Tenable Support for guidance on how to increase the timeout.</p>
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.



Scans

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.

<input type="checkbox"/>	Name ^	Schedule	Last Modified		
<input type="checkbox"/>	6.10.7 - Advance - 85 - Cred	On Demand	✓ June 16 at 6:36 PM	▶	✕
<input type="checkbox"/>	6.10.7 - Advance - Cred - 84	On Demand	✓ June 16 at 6:09 PM	▶	✕
<input type="checkbox"/>	Active sync	On Demand	✓ June 28 at 11:47 AM	▶	✕
<input type="checkbox"/>	Agent Scan	Disabled	↑ June 28 at 10:39 AM		✕
<input type="checkbox"/>	Agent Scan	Disabled	↑ June 28 at 10:35 AM		✕
<input type="checkbox"/>	AIX 7.1 - Borken Policy	On Demand	✓ June 30 at 11:07 AM	▶	✕
<input type="checkbox"/>	AIX 7.1 - working	On Demand	✓ June 30 at 10:04 AM	▶	✕
<input type="checkbox"/>	<script>alert('lol')</script>	Disabled	↑ June 28 at 4:31 PM		✕
<input type="checkbox"/>	<script>alert('lol')</script>	On Demand	✓ June 28 at 12:33 PM	▶	✕
<input type="checkbox"/>	apple PM	On Demand	✓ June 28 at 11:31 AM	▶	✕
<input type="checkbox"/>	Example 2	On Demand	✓ July 26 at 10:28 AM	▶	✕

For more information, see the following sections:

- [Scan Templates](#)
- [Create and Manage Scans](#)
- [Scan Results](#)
- [Scan Folders](#)
- [Policies](#)
- [Terrascan](#)
- [Plugins](#)
- [Customized Reports](#)



- [Scanners](#)
- [Agents](#)



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. Nessus provides separate templates for scanners and agents, depending on which sensor you want to use for scanning:

- [Scanner Templates](#)
- [Agent Templates \(Nessus Manager only\)](#) (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 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 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](#).

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 Nessus Manager for agent management, Tenable does not recommend using 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 Nessus Manager. These configurations can negatively impact agent scan performance. In most cases, use agent scan templates when working in Nessus Manager.

Template	Description
Discovery	
Attack Surface Discovery	(Tenable Nessus Expert only) Uses Bit Discovery 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 with Bit Discovery .
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 Nessus Network Monitor, run this scan weekly to



	<p>discover new assets on your network.</p> <p>Note: Assets identified by discovery scans do not count toward your license.</p>
Vulnerabilities	
Basic Network Scan	<p>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.</p>
Advanced Network Scan	<p>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.</p> <p>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.</p>
Advanced Dynamic Scan	<p>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.</p>
Malware Scan	<p>Scans for malware on Windows and Unix systems.</p> <p>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.</p>
Mobile Device Scan	<p>(Nessus Manager only)</p> <p>Assesses mobile devices via Microsoft Exchange or an MDM.</p> <p>Use this template to scan what is installed on the targeted mobile devices and report on the installed applications or application versions'</p>



	<p>vulnerabilities.</p> <p>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.</p> <ul style="list-style-type: none">• To query for information, the 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 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, Nessus retrieves information from phones that have been updated in the last 365 days.
Web Application Tests	Scan for published and unknown web vulnerabilities.
Credentialed Patch Audit	Authenticates hosts and enumerates missing updates. Use this template with credentials to give Nessus direct access to the host, scan the target hosts, and enumerate missing patch updates.
Intel AMT Security Bypass	Performs remote and local checks for CVE-2017-5689.
Spectre and Melt-down	Performs remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
WannaCry Ransomware	Scans for the WannaCry ransomware (MS17-010).



Ripple20 Remote Scan	Detects hosts running the Treck stack in the network, which may be affected by Ripple20 vulnerabilities.
Zerologon Remote Scan	Detects Microsoft Netlogon elevation of privilege vulnerability (Zerologon).
Solarigate	Detects SolarWinds Solorigate vulnerabilities using remote and local checks.
ProxyLogon: MS Exchange	Performs remote and local checks to detect Microsoft Exchange Server vulnerabilities related to CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065.
PrintNightmare	Performs local checks for CVE-2021-34527, the PrintNightmare Windows Print Spooler vulnerability.
Active Directory Starter Scan	<p>Scans for misconfigurations in Active Directory.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: Active Directory Starter Scans require ADSI credentials. For more information, see Miscellaneous.</p></div> <p>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.</p>
Log4Shell	Detects the Log4Shell vulnerability (CVE-2021-44228) in Apache Log4j via local checks.
Log4Shell Remote Checks	Detects the Log4Shell vulnerability (CVE-2021-44228) in Apache Log4j via remote checks.
Log4Shell Vulnerability Ecosystem	Detects the Log4Shell vulnerability (CVE-2021-44228) in Apache Log4j via local and remote checks. This template is dynamic and is regularly updated with new plugins as third-party vendors patch their software.
2022 Threat Landscape Retrospective (TLR)	Detects vulnerabilities featured in Tenable's 2022 Threat Landscape Retrospective report.



CISA Alerts AA22-011A and AA22-047A	Performs remote and local checks for vulnerabilities from CISA alerts AA22-011A and AA22-047A.
ContiLeaks	Performs remote and local checks for ContiLeaks vulnerabilities.
Ransomware Ecosystem	Performs remote and local checks for common ransomware vulnerabilities.
Compliance	
Audit Cloud Infrastructure	<p>Audits the configuration of third-party cloud services.</p> <p>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.</p>
Internal PCI Network Scan	<p>Performs an internal PCI DSS (11.2.1) vulnerability scan.</p> <p>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.</p> <div style="border: 1px solid blue; padding: 5px;"><p>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).</p></div>
MDM Config Audit	<p>Audits the configuration of mobile device managers.</p> <p>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.</p>
Offline Config Audit	<p>Audits the configuration of network devices.</p> <p>Offline configuration audits allow Nessus to scan hosts without the need to scan over the network or use credentials. Organizational policies may</p>



	<p>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.</p> <p>Tenable recommends using offline configuration audits to scan devices that do not support secure remote access and devices that scanners cannot access.</p>
Unofficial PCI Quarterly External Scan	<p>Performs quarterly external scans as required by PCI.</p> <p>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.io customers can submit their PCI scan results to Tenable for PCI ASV validation.</p>
Policy Compliance Auditing	<p>Audits system configurations against a known baseline.</p> <p>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.</p>
SCAP and OVAL Auditing	<p>Audits systems using SCAP and OVAL definitions.</p> <p>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.</p> <ul style="list-style-type: none">• SCAP compliance auditing requires sending an executable to the remote host.• Systems running security software (for example, McAfee Host Intru-



sion 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.

Agent Templates (Nessus Manager only)

There are two agent template categories in 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 con-



	<p>figuration, such as faster or slower checks, but misconfigurations can cause asset outages or network saturation. Use the advanced templates with caution.</p>
Malware Scan	<p>Scans for malware on Windows and Unix systems.</p> <p>Nessus 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.</p>
Agent Log4Shell	<p>Detects the Log4Shell vulnerability (CVE-2021-44228) in Apache Log4j via local checks.</p>
Compliance	
Policy Compliance Auditing	<p>Audits system configurations against a known baseline.</p> <p>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.</p>
SCAP and OVAL Auditing	<p>Audits systems using SCAP and OVAL definitions.</p> <p>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.</p> <ul style="list-style-type: none">• 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 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](#)
- [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:


- [General](#)
- [Schedule](#)
- [Notifications](#)
- [Permissions](#)

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 displayed on the 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 Window	1 hour	(Agent scans only) (Required) 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.
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 . <div style="border: 1px solid blue; padding: 5px;">Note: After scan creation, you cannot change the Tenable-provided template on which a scan is based.</div> 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 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	<p>(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 wild-cards are not allowed. Targets must start with the <code>http://</code> or <code>https://</code> protocol identifier.</p> <p>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.</p> <p>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.</p>
Targets	None	<p>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.</p> <p>Targets can be specified using a number of different formats.</p> <p>Tip: You can force Nessus to use a given host name for a server during a scan by using the <code>hostname[ip]</code> syntax (e.g., <code>www.example.com[192.168.1.1]</code>).</p>
Upload Targets	None	<p>Uploads a text file that specifies targets.</p> <p>The targets file must be formatted in the following manner:</p> <ul style="list-style-type: none">• 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	<p>Specifies how often the scan is launched.</p> <ul style="list-style-type: none">• Once: Schedule the scan at a specific time.• Daily: Schedule the scan to occur on a daily basis, at a specific time or to repeat up to every 20 days.• Weekly: Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks.• Monthly: Schedule the scan to occur every month, by time and day or week of month, for up to 20 months.• Yearly: Schedule the scan to occur every year, by time and day, for up to 20 years.
Starts	Varies	<p>Specifies the exact date and time when a scan launches.</p> <p>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 09/31/2018 at 9:12 AM, the default starting date and time is set to 09/31/2018 and 09:30.</p> <p>Note: If you schedule your scan to repeat monthly, Tenable</p>



		<p>recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (e.g., the 29th), Tenable Nessus cannot run the scan on those days.</p>
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 <i>Weekly</i> for Frequency . 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 <i>Monthly</i> 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 identifier	fe80:0:0:0:216:cbff:fe92:88d0%eth0	Tenable Nessus scans the single IPv6 address. Tenable Nessus does not 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	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,



Target Description	Example	Explanation
replaced with numeric ranges		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 notation	192.168.0.0/255.255.255.128	Tenable Nessus scans all addresses within the specified 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 target.



Target Description	Example	Explanation
able to an IPv4 address with netmask notation		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	<p>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 provide a IPv6 scope identifier, Tenable Nessus sends out the requests on all interfaces.</p> <p>Tenable Nessus does not support using the interface names instead of interface indexes for the scope identifier on Windows platforms.</p>
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](#)
- [Permissions](#)

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:

- [Host Discovery](#)
- [Port Scanning](#)
- [Service Discovery](#)
- [Identity](#)

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	Description
---------	---------	-------------



Value		
Ping the remote host	On	<p>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.</p> <p>If set to Off, the scanner does not ping remote hosts on multiple ports during the scan.</p> <div style="border: 1px solid blue; padding: 5px;">Note: To scan VMware guest systems, Ping the remote host must be set to Off.</div>
Scan unresponsive hosts	Disabled	<p>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.</p>
General Settings		
Test the local Nessus host	Enabled	<p>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.</p>
Use Fast Network Discovery	Disabled	<p>When disabled, if a host responds to ping, 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.</p> <p>When enabled, Nessus does not perform these checks.</p>
Ping Methods		
ARP	Enabled	<p>Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.</p>
TCP	Enabled	<p>Ping a host using TCP.</p>
Destination ports	built-in	<p>Destination ports can be configured to use specific</p>



(TCP)		<p>ports for TCP ping. This specifies the list of ports that are checked via TCP ping.</p> <p>Type one of the following: <code>built-in</code>, a single port, or a comma-separated list of ports.</p> <p>For more information about which ports <code>built-in</code> specifies, see the knowledge base article.</p>
ICMP	Enabled	<p>Ping a host using the Internet Control Message Protocol (ICMP).</p>
Assume ICMP unreachable from the gateway means the host is down	Disabled	<p>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.</p> <div style="border: 1px solid blue; padding: 5px;"><p>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.</p></div>
Maximum number of retries	2	<p>Specifies the number of attempts to retry pinging the remote host.</p>
UDP	Disabled	<p>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.</p>
Fragile Devices		
Scan Network Printers	Disabled	<p>When enabled, the scanner scans network printers.</p>



Scan Novell Net-ware hosts	Disabled	When enabled, the scanner scans Novell NetWare hosts.
Scan Operational Technology devices	Disabled	<p>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.</p> <p>When disabled, the scanner uses ICS/SCADA Smart Scanning to cautiously identify OT devices and stops scanning them once they are discovered.</p>
Wake-on-LAN		
List of MAC Addresses	None	<p>The Wake-on-LAN (WOL) menu controls which hosts to send WOL magic packets to before performing a scan.</p> <p>Hosts that you want to start prior to scanning are provided by uploading a text file that lists one MAC address per line.</p> <p>For example:</p> <pre>33:24:4C:03:CC:C7 FF:5C:2C:71:57:79</pre>
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	<p>Specifies the range of ports to be scanned.</p> <p>Supported keyword values are:</p> <ul style="list-style-type: none">• <code>default</code> instructs the scanner to scan approximately 4,790 commonly used ports. The list of ports can be found in the <code>nessus-services</code> file on the Nessus scanner.• <code>all</code> instructs the scanner to scan all 65,536 ports, including excluding port 0. <p>Additionally, you can indicate a custom list of ports by using a comma-separated list of ports or port ranges. For example, <code>21, 23, 25, 80, 110</code> or <code>1-1024, 8080, 9000-9200</code>. If you wanted to scan all ports excluding port 0, you would type <code>1-65535</code>.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: You cannot use a combination of <code>default</code>, <code>all</code>, single target IDs, and port ranges in a comma-separated list. In other words, you can only enter <code>default</code>, <code>all</code>, a single target ID, a list of target IDs, a single port range, or a list of port ranges.</p></div> <p>The custom range specified for a port scan is applied to the protocols you have selected in the Network Port Scan-</p>



Setting	Default Value	Description
		<p>ners group of settings.</p> <p>If scanning both TCP and UDP, you can specify a split range specific to each protocol. For example, if you want to scan a different range of ports for TCP and UDP in the same policy, you would type <code>T:1-1024,U:300-500</code>.</p> <p>You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate protocol. For example, <code>1-1024,T:1024-65535,U:1025</code>.</p>
Local Port Enumerators		
SSH (netstat)	Enabled	<p>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.</p>
WMI (netstat)	Enabled	<p>When enabled, the scanner uses netstat to determine open ports while performing a WMI-based scan.</p> <p>In addition, the scanner:</p> <ul style="list-style-type: none">• 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. <p>If any port enumerator (netstat or SNMP) is successful, the port range becomes <i>all</i>.</p>
SNMP	Enabled	<p>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,</p>



Setting	Default Value	Description
		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.
Only run network port scanners if local port enumeration failed	Enabled	If a local port enumerator runs, all network port scanners will be disabled for that asset.
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. TCP scans are only possible if you are using Linux or FreeBSD. On Windows or macOS, the scanner does not do a TCP scan and instead uses the SYN scanner to avoid performance issues native to those operating systems. 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



Setting	Default Value	Description
		<p>response.</p> <p>If you enable this option, you can also set the Override Automatic Firewall Detection option.</p>
Override automatic firewall detection	Disabled	<p>This setting can be enabled if you enable either the TCP or SYN option.</p> <p>When enabled, this setting overrides automatic firewall detection.</p> <p>This setting has three options:</p> <ul style="list-style-type: none">• 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	<p>This option engages the built-in Tenable Nessus UDP scanner to identify open UDP ports on the targets.</p> <p>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.</p>

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 to find services	Enabled	When enabled, the scanner attempts to map each open port 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 two options: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• None



Setting	Default Value	Description
		<ul style="list-style-type: none">• Known SSL/TLS ports• All TCP ports
Identify certificates expiring within x days	60	When enabled, the scanner identifies SSL and TLS certificates that are within the specified number of days of 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 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)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)
	OS Identification	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP
	Port scan (common ports)	<ul style="list-style-type: none">• General Settings:



		<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Port Scanner Settings:<ul style="list-style-type: none">◦ Scan common ports◦ Use netstat if credentials are provided◦ Use SYN scanner if necessary• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)
	Port scan (all ports)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Port Scanner Settings:<ul style="list-style-type: none">◦ Scan all ports (1-65535)◦ Use netstat if credentials are provided◦ Use SYN scanner if necessary• Ping hosts using:



		<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)
	Custom	All defaults
Vulnerabilities		
Basic Network Scan	Port scan (common ports) (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Port Scanner Settings:<ul style="list-style-type: none">◦ Scan common ports◦ Use netstat if credentials are provided◦ Use SYN scanner if necessary• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)
	Port scan (all ports)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Port Scanner Settings:



		<ul style="list-style-type: none">◦ Scan all ports (1-65535)◦ Use netstat if credentials are provided◦ Use SYN scanner if necessary• Ping hosts using:<ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)
	Host enumeration (include fragile hosts)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host



		<ul style="list-style-type: none">◦ Use fast network discovery• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)• Scan all devices, including:<ul style="list-style-type: none">◦ Printers◦ Novell Netware hosts
	Custom	All defaults
Mobile Device Scan	-	-
Web Application Tests	Port scan (common ports) (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Port Scanner Settings:<ul style="list-style-type: none">◦ Scan common ports◦ Use netstat if credentials are provided◦ Use SYN scanner if necessary• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP



	Port scan (all ports)	<ul style="list-style-type: none">◦ ICMP (2 retries) <ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Port Scanner Settings:<ul style="list-style-type: none">◦ Scan all ports (1-65535)◦ Use netstat if credentials are provided◦ Use SYN scanner if necessary• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)
	Custom	All defaults
Credentialed Patch Audit	Port scan (common ports) (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Port Scanner Settings:<ul style="list-style-type: none">◦ Scan common ports◦ Use netstat if credentials are provided



		<ul style="list-style-type: none">◦ Use SYN scanner if necessary• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)
	Port scan (all ports)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Port Scanner Settings:<ul style="list-style-type: none">◦ Scan all ports (1-65535)◦ Use netstat if credentials are provided◦ Use SYN scanner if necessary• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)
	Custom	All defaults
Badlock Detection	Normal (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host



		<ul style="list-style-type: none">◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan the default Nessus port range◦ Detect SSL/TLS on ports where it is commonly used
	Quick	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan TCP ports 23, 25, 80, and 443◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:



		<ul style="list-style-type: none">◦ Scan all TCP ports◦ Detect SSL on all open ports
	Custom	All defaults
Bash Shellshock Detection	Normal (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan the default Nessus port range◦ Detect SSL/TLS on ports where it is commonly used• Scan all devices, including:<ul style="list-style-type: none">◦ Printers◦ Novell Netware hosts
	Quick	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:



		<ul style="list-style-type: none">◦ Scan TCP ports 23, 25, 80, and 443◦ Detect SSL/TLS on ports where it is commonly used• Scan all devices, including:<ul style="list-style-type: none">◦ Printers◦ Novell Netware hosts
	Thorough	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan all TCP ports◦ Detect SSL on all open ports• Scan all devices, including:<ul style="list-style-type: none">◦ Printers◦ Novell Netware hosts
	Custom	All defaults
DROWN Detection	Normal (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host



		<ul style="list-style-type: none">◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan the default Nessus port range◦ Detect SSL/TLS on ports where it is commonly used
	Quick	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan TCP ports 23, 25, 80, and 443◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:



		<ul style="list-style-type: none">◦ Scan all TCP ports◦ Detect SSL on all open ports
	Custom	All defaults
Intel AMT Security Bypass	Normal (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan the default Nessus port range◦ Detect SSL/TLS on ports where it is commonly used
	Quick	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan TCP ports 16992, 16993, 623, 80, and 443◦ Detect SSL/TLS on ports where it is com-



		monly used
	Thorough	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan all TCP ports◦ Detect SSL on all open ports
	Custom	All defaults
Shadow Brokers Scan	Normal (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan the default Nessus port range◦ Detect SSL/TLS on ports where it is commonly used• Scan all devices, including:<ul style="list-style-type: none">◦ Printers



		<ul style="list-style-type: none">◦ Novell Netware hosts
	Thorough	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan all TCP ports◦ Detect SSL on all open ports• Scan all devices, including:<ul style="list-style-type: none">◦ Printers◦ Novell Netware hosts
	Custom	<u>All defaults</u>
Spectre and Meltdown	Normal (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan the default Nessus port range◦ Detect SSL/TLS on ports where it is com-



		monly used
	Thorough	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan all TCP ports◦ Detect SSL on all open ports
	Custom	All defaults
WannaCry Ransomware	Normal (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan the default Nessus port range◦ Detect SSL/TLS on ports where it is commonly used
	Quick	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host



		<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan TCP ports 139 and 445◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan all TCP ports◦ Detect SSL on all open ports
	Custom	<u>All defaults</u>
Log4Shell	Normal	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery



		<ul style="list-style-type: none">• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan the default Nessus port range◦ Detect SSL/TLS on ports where it is commonly used• Do not scan fragile devices.
	Quick	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan TCP ports 80 and 443◦ Detect SSL/TLS on ports where it is commonly used• Do not scan fragile devices.
	Thorough (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:



		<ul style="list-style-type: none">◦ Scan all TCP ports◦ Detect SSL on all open ports• Do not scan fragile devices.
	Custom	All defaults
Log4Shell Remote Checks	Normal (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan the default Nessus port range◦ Detect SSL/TLS on ports where it is commonly used• Do not scan fragile devices.
	Quick	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan TCP ports 80 and



		<p>443</p> <ul style="list-style-type: none">◦ Detect SSL/TLS on ports where it is commonly used <ul style="list-style-type: none">• Do not scan fragile devices.
	Thorough	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan all TCP ports◦ Detect SSL on all open ports• Do not scan fragile devices.
	Custom	All defaults
Log4Shell Vulnerability Ecosystem	Normal	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan the default Nessus port range



		<ul style="list-style-type: none">◦ Detect SSL/TLS on ports where it is commonly used• Do not scan fragile devices.
	Quick	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan TCP ports 80 and 443◦ Detect SSL/TLS on ports where it is commonly used• Do not scan fragile devices.
	Thorough (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host◦ Use fast network discovery• Service Discovery Settings:<ul style="list-style-type: none">◦ Scan all TCP ports◦ Detect SSL on all open ports



		<ul style="list-style-type: none">• Do not scan fragile devices.
	Custom	All defaults
Compliance		
Audit Cloud Infrastructure	-	-
Internal PCI Network Scan	Port scan (common ports) (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Port Scanner Settings:<ul style="list-style-type: none">◦ Scan common ports◦ Use netstat if credentials are provided◦ Use SYN scanner if necessary• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)
	Port scan (all ports)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host◦ Use fast network discovery• Port Scanner Settings:



		<ul style="list-style-type: none">◦ Scan all ports (1-65535)◦ Use netstat if credentials are provided◦ Use SYN scanner if necessary• Ping hosts using:<ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Ping the remote host◦ Always test the local Nessus host• Scan all devices, including:<ul style="list-style-type: none">◦ Printers◦ Novell Netware hosts
	Custom	All defaults
SCAP and OVAL Auditing	Host enumeration (default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Always test the local Nessus host



		<ul style="list-style-type: none">◦ Use fast network discovery• Ping hosts using:<ul style="list-style-type: none">◦ TCP◦ ARP◦ ICMP (2 retries)
	Custom	All defaults



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:

- [General](#)
- [Brute Force](#)
- [SCADA](#)
- [Web Applications](#)
- [Windows](#)
- [Malware](#)
- [Databases](#)

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 Nessus to allow for a specific grace time in reporting when antivirus signatures are considered out of date. By default, Nessus considers signatures out of date regardless of how long ago an update was available (for example, a few hours ago). You can configure this setting to allow for up to 7 days before reporting them out of date.
SMTP		
Third party domain		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 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	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, 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 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	Disabled	Enables Hydra whenever Nessus performs the scan.



Hydra (slow)		
Logins file		A file that contains usernames that Hydra uses during the scan.
Passwords file		A file that contains passwords for user accounts that Hydra uses during the scan.
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, Nessus only uses the usernames specified in the logins file for the scan. Otherwise, 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 ID (0 - 99)		The ID of the SAP R/3 client that you want Hydra to test.
Windows accounts to test	Local accounts	You can set this to <i>Local accounts</i> , <i>Domain Accounts</i> , or <i>Either</i> .
Interpret pass-	Disabled	If enabled, Hydra interprets passwords as NTLM hashes.



words 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 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 Register	0	The register at which to start scanning.
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



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.
		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. Nessus tries all values between the Start and Stop .

Web Applications

By default, 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
General Settings		
Use a custom User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	Specifies which type of browser Nessus impersonates while scanning.
Web Crawler		



Setting	Default Value	Description
Start crawling from	/	The URL of the first page that Nessus tests. If you want to test multiple pages, use a colon delimiter to separate them (for example, <code>/:/php4:/base</code>).
Excluded pages (regex)	<code>/server_privileges\.php <> log out</code>	Specifies portions of the web site to exclude from being crawled. For example, to exclude the <code>/manual</code> directory and all Perl CGI, set this field to: <code>(^/manual) <> (\.pl(\?.*)?\$/)</code> . 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 Nessus follows for each start page.
Follow dynamic pages	Disabled	If you enable this setting, 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.
Abort web application tests if HTTP login fails	Disabled	If Nessus cannot log in to the target via HTTP, then do not run any web application tests.



Setting	Default Value	Description
Try all HTTP methods	Disabled	This option instructs 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, 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 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	Disabled	This setting manages the combination of



Setting	Default Value	Description
than one parameter at a time per form		<p>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 <code>/test.php?arg1=XSS&b=1&c=1</code>, where b and c allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated.</p> <p>This setting has four options:</p> <ul style="list-style-type: none">• 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 variables. For example, Tenable Nessus would attempt <code>/test.php?a-a=XSS&b=1&c=1&d=1</code> and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as dis-



Setting	Default Value	Description
		<p>covered during the mirror process) and any other variables are given the first value. In this case, Tenable Nessus would never test for <code>/test.php?a=XSS&b=3&c=3&d=3</code> when the first value of each variable is 1.</p> <ul style="list-style-type: none">• 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 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	Disabled	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 injec-



Setting	Default Value	Description
		<p>tion, 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.</p> <p>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.</p> <p>If you enable this option, select one of the following options:</p> <ul style="list-style-type: none">• 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 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.



Setting	Default Value	Description
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, 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 Nessus attempts to enumerate domain users.
End UID	1200	The end of a range of IDs where 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 Nessus attempts to enumerate local users.
End UID	1200	The end of a range of IDs where Nessus attempts to enumerate local users.

Malware

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

- [General Settings](#)
- [Hash and Allowlist Files](#)
- [File System Scanning](#)



Setting	Default Value	Description
General Settings		
Disable DNS resolution	Disabled	Checking this option prevents Nessus from using the cloud to compare scan findings against known malware.
Hash and Allowlist Files		
Custom Netstat IP Threat List	None	<p>A text file that contains a list of known bad IP addresses that you want to detect.</p> <p>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.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: Tenable does not detect private IP ranges in the text file.</p></div>
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 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 Nessus finds any matches while scanning a target, and a



		<p>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.</p>
Hosts file allowlist	None	<p>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 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.</p>
Yara Rules		
Yara Rules	None	<p>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.</p>
File System Scanning		
Scan file system	Off	<p>Enabling this option allows you to scan system directories and files on host computers.</p> <div style="border: 1px solid red; padding: 5px;"><p>Caution: Enabling this setting in scans targeting 10 or more hosts could result in performance degradation.</p></div>
Windows Directories		
Scan %Systemroot%	Off	<p>Enables file system scanning to scan %Systemroot%.</p>
Scan %ProgramFiles%	Off	<p>Enables file system scanning to scan %ProgramFiles%.</p>
Scan %ProgramFiles (x86)%	Off	<p>Enables file system scanning to scan %ProgramFiles (x86)%.</p>



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. 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) loc-



ally. 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.



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)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid false alarms◦ Disable CGI scanning• Web Applications:<ul style="list-style-type: none">◦ Disable web application scanning
	Scan for known web vulnerabilities	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Enable CGI scanning• Web Applications:<ul style="list-style-type: none">◦ Start crawling from "/"◦ Crawl 1000 pages (max)◦ Traverse 6 directories (max)◦ Test for known vulnerabilities in commonly used web applications



		<ul style="list-style-type: none">◦ Generic web application tests disabled
	Scan for all web vulnerabilities (quick)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Enable CGI scanning• Web Applications:<ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Enable CGI scanning◦ Perform thorough tests• Web Applications:<ul style="list-style-type: none">◦ Start crawling from "/"◦ Crawl 1000 pages (max)◦ Traverse 6 directories (max)



		<ul style="list-style-type: none">◦ 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	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Enable CGI scanning• Web Applications:<ul style="list-style-type: none">◦ Start crawling from "/"◦ Crawl 1000 pages (max)◦ Traverse 6 directories (max)◦ Test for known vul-



		<p>nerabilities in commonly used web applications</p> <ul style="list-style-type: none">◦ Generic web application tests disabled
	Scan for all web vulnerabilities (quick) (Default)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Enable CGI scanning• Web Applications:<ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Enable CGI scanning◦ Perform thorough tests• Web Applications:<ul style="list-style-type: none">◦ Start crawling from "/"



		<ul style="list-style-type: none">◦ 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	<ul style="list-style-type: none">• General Settings<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Disable CGI scanning• Web Applications<ul style="list-style-type: none">◦ Disable web application scanning



Log4Shell Remote Checks	Default	<ul style="list-style-type: none">• General Settings<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Disable CGI scanning• Web Applications<ul style="list-style-type: none">◦ Disable web application scanning
Log4Shell Vulnerability Ecosystem	Default	<ul style="list-style-type: none">• General Settings<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Disable CGI scanning• Web Applications<ul style="list-style-type: none">◦ Disable web application scanning
Shadow Brokers Scan	–	–
Spectre and Melt-down	–	–
WannaCry Ransomware	–	–
Compliance		
Audit Cloud Infrastructure	–	–
Internal PCI Network Scan	Default	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid false alarms◦ Disable CGI scanning• Web Applications:



		<ul style="list-style-type: none">◦ Disable web application scanning
	Scan for known web vulnerabilities	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Enable CGI scanning• Web Applications:<ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Enable CGI scanning• Web Applications:<ul style="list-style-type: none">◦ Start crawling from "/"◦ Crawl 1000 pages (max)◦ Traverse 6 directories (max)◦ Test for known vul-



		<p>nerabilities in commonly used web applications</p> <ul style="list-style-type: none">◦ Perform each generic web app test for 5 minutes (max)
	Scan for all web vulnerabilities (complex)	<ul style="list-style-type: none">• General Settings:<ul style="list-style-type: none">◦ Avoid potential false alarms◦ Enable CGI scanning◦ Perform thorough tests• Web Applications:<ul style="list-style-type: none">◦ 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	<p>When disabled, provides the standard level of plugin activity in the report. The output does not include the informational plugins 56310, 64582, and 58651.</p> <p>When enabled, this setting has two options:</p> <ul style="list-style-type: none">• 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		



Setting	Default Value	Description
Allow users to edit scan results	Enabled	When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other 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](#)
- [Debug 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 scan.
Scan IP addresses	Disabled	By default, Tenable Nessus scans a list of IP addresses



Setting	Default Value	Description
in a random order		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	<p>When enabled, if a credentialed scan tries to connect via SSH to a FortiOS host that presents a disclaimer prompt, the scanner provides the necessary text input to accept the disclaimer prompt and continue the scan.</p> <p>The scan initially sends a bad ssh request to the target in order to retrieve the supported authorization methods. This allows you to determine how to connect to the target, which is helpful when you configure a custom ssh banner and then try to determine how to connect to the host.</p> <p>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.</p>
Scan targets with multiple domain names in parallel	Disabled	<p>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.</p> <p>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</p>



Setting	Default Value	Description
		multiple scan tasks. Scans complete more quickly, but hosts could potentially become overwhelmed, causing timeouts and incomplete results.
Trusted CAs	none	<p>Determines the certificate authorities (CAs) that Nessus allows for the scan. In the Trusted CAs box, enter the text of your CA or CAs.</p> <div data-bbox="706 583 1479 745" style="border: 1px solid blue; padding: 5px;"><p>Note: Include the beginning text -----BEGIN CERTIFICATE----- and ending text -----END CERTIFICATE-----.</p></div> <div data-bbox="706 768 1479 926" style="border: 1px solid green; padding: 5px;"><p>Tip: You can save more than one certificate in a single text file, including the beginning and ending text for each one.</p></div> <p>You can also determine trusted CAs at the scanner level. For more information, see Trust a Custom CA.</p>
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.



Setting	Default Value	Description
Max simultaneous hosts per scan	30, or the Tenable Nessus scanner advanced setting <code>max_hosts</code> , whichever is smaller.	Specifies the maximum number of hosts that a scanner scans at the same time.
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.
Unix find command exclusions		
Exclude Filepath	none	A plain text file containing a list of filepaths to exclude from all plugins that search using the <code>find</code> command on Unix systems. In the file, enter one filepath per line, formatted per patterns allowed by the Unix <code>find</code> command <code>-path</code> argument. For more information, see the <code>find</code> command man page .
Exclude Filesystem	none	A plain text file containing a list of filesystems to exclude from all plugins that search using the <code>find</code> command on Unix systems.



Setting	Default Value	Description
		<p>In the file, enter one filesystem per line, using filesystem types supported by the Unix <code>find</code> command - <code>fstype</code> argument. For more information, see the <code>find</code> command man page.</p>
Include Filepath	none	<p>A plain text file containing a list of filepaths to include from all plugins that search using the <code>find</code> command on Unix systems.</p> <p>In the file, enter one filepath per line, formatted per patterns allowed by the Unix <code>find</code> command <code>-path</code> argument. For more information, see the <code>find</code> command man page.</p> <p>Including filepaths increases the locations that are searched by plugins, which extends the duration of the scan. Make your inclusions as specific as possible.</p> <div style="border: 1px solid green; padding: 5px;"><p>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.</p></div>
Windows file search Options		
Windows Exclude Filepath	none	<p>A plain text file containing a list of filepaths to exclude from all plugins that search using Tenable's unmanaged software directory scans.</p> <p>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 <code>E:\</code>, <code>E:\Testdir\</code>, and <code>\Testdir\</code>.</p> <div style="border: 1px solid green; padding: 5px;"><p>Tip: The default exclusion paths include <code>\Win-</code></p></div>



Setting	Default Value	Description
		<p>dows\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.</p>
Windows Include Filepath	none	<p>A plain text file containing a list of filepaths to include from all plugins that search using Tenable's unmanaged software directory scans.</p> <p>In the file, enter one absolute or partial filepath per line, formatted as the literal strings you want to exclude. You can only include absolute directory names, examples such as E:\, E:\Testdir\, and C:\.</p> <p>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.</p>
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	<p>Controls verbosity of the plugin audit trail. All audit trail data includes the reason why plugins were not included in the scan.</p> <p>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_</p>



Setting	Default Value	Description
		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.
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, 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.
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



Setting	Default Value	Description
		that agents begin scanning at least 30 minutes before the scan window closes.



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)	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 30 simultaneous hosts (max)◦ 4 simultaneous checks per host (max)◦ 5 second network read timeout
	Scan low bandwidth links	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 30 simultaneous hosts (max)◦ 4 simultaneous checks per host (max)◦ 5 second network read timeout
	Scan low bandwidth links	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 30 simultaneous hosts (max)◦ 4 simultaneous checks per host (max)◦ 5 second network read



		timeout
	Scan low bandwidth links	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 30 simultaneous hosts (max)◦ 4 simultaneous checks per host (max)◦ 5 second network read timeout
	Scan low bandwidth links	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 30 simultaneous hosts (max)◦ 4 simultaneous checks per host (max)◦ 5 second network read timeout
	Scan low bandwidth links	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 2 simultaneous hosts



		<p>(max)</p> <ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 30 simultaneous hosts (max)◦ 4 simultaneous checks per host (max)◦ 5 second network read timeout
	Scan low bandwidth links	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 2 simultaneous hosts (max)◦ 2 simultaneous checks per host (max)◦ 15 second network read timeout◦ Slow down the scan when network con-



		gestion is detected
	Custom	All defaults
Policy Compliance Auditing	Default (default)	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 30 simultaneous hosts (max)◦ 4 simultaneous checks per host (max)◦ 5 second network read timeout
	Scan low bandwidth links	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 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)	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 30 simultaneous hosts (max)◦ 4 simultaneous checks per host (max)◦ 5 second network read timeout



	Scan low bandwidth links	<ul style="list-style-type: none">• Performance options:<ul style="list-style-type: none">◦ 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 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.

Nessus has the ability to log into remote Linux hosts via Secure Shell (SSH); and with Windows hosts, Nessus uses various Microsoft authentication technologies. Nessus also uses the Simple Network Management Protocol (SNMP) to make version and information queries to routers and switches.

The scan or policy's **Credentials** page allows you to configure the Nessus scanner to use authentication credentials during scanning. Configuring credentials allows 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, 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

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: 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.



Cloud Services Credentials

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	<p>For 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:</p> <ul style="list-style-type: none">• us-east-1• us-east-2• us-west-1• us-west-2• ca-central-1• eu-west-1• eu-west-2• eu-central-1



		<ul style="list-style-type: none">• 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 two 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

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 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 are available **Database** credentials:

- [DB2](#)
- [MySQL](#)
- [Oracle](#)
- [PostgreSQL](#)
- [SQL Server](#)
- [Sybase ASE](#)
- [MongoDB](#)
- [Cassandra](#)

DB2

The following table describes the additional options to configure for **IBM DB2** credentials.

Options	Description
Auth Type	<p>The authentication method for providing the required credentials.</p> <ul style="list-style-type: none">• Password• Import• CyberArk• Lieberman• Hashicorp Vault <p>For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.</p>
Database Port	<p>The TCP port that the IBM DB2 database instance listens on for communications from Tenable Nessus Manager. The default is port 50000.</p>
Database	<p>The name for your database (not the name of your instance).</p>



Options	Description
Name	
Options	Description
Username	The username for a user on the database.
	The password associated with the username you provided.
Port	The TCP port that the Informix/DRDA database instance listens on for communications from Tenable Security Center. The default is port 1526.

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. <ul style="list-style-type: none">• 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 Manager. The default is port 3306.

Oracle



The following table describes the additional options to configure for **Oracle** credentials.

Options	Description
Auth Type	<p>The authentication method for providing the required credentials.</p> <ul style="list-style-type: none">• Password• Import• CyberArk• Lieberman• Hashicorp Vault <p>For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.</p>
Database Port	<p>The TCP port that the Oracle database instance listens on for communications from Tenable Nessus Manager. The default is port 1521.</p>
Auth Type	<p>The type of account you want Tenable Nessus Manager to use to access the database instance:</p> <ul style="list-style-type: none">• Normal• System Operator• System Database Administrator• SYSDBA• SYSOPER• NORMAL
Service Type	<p>The Oracle parameter you want to use to specify the database instance: SID or Service NameSERVICE_NAME.</p>
Service	<p>The SID value or SERVICE_NAME value for your database instance.</p> <p>The Service value you enter must match your parameter selection for the Service Type option.</p>



PostgreSQL

The following table describes the additional options to configure for **PostgreSQL** credentials.

Options	Description
Auth Type	<p>The authentication method for providing the required credentials.</p> <ul style="list-style-type: none">• Password• Client Certificate• CyberArk• Lieberman• Hashicorp Vault <p>For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.</p>
Database Port	<p>The TCP port that the PostgreSQL database instance listens on for communications from Tenable Nessus Manager. The default is port 5432.</p>
Database Name	<p>The name for your database instance.</p>

SQL Server

The following table describes the additional options to configure for **SQL Server** credentials.

Options	Description
Auth Type	<p>The authentication method for providing the required credentials.</p> <ul style="list-style-type: none">• Password• Import• CyberArk• Lieberman• Hashicorp Vault



Options	Description
	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 Manager. The default is port 1433.
AuthType	The type of account you want Tenable Nessus Manager to use to access the database 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. <ul style="list-style-type: none">• 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 Manager. The default is port 3638.
Auth Type	The type of authentication used by the Sybase ASE database: RSA or Plain Text .

Cassandra



Option	Description
Auth Type	<p>The authentication method for providing the required credentials.</p> <ul style="list-style-type: none">• Password• CyberArk• Lieberman• Hashicorp Vault <p>For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.</p>
Port	<p>The port the database listens on. The default is port 9042.</p>

MongoDB

Option	Description
Auth Type	<p>The authentication method for providing the required credentials.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: This option is only available for non-legacy versions of the MongoDB authentication method.</p></div> <ul style="list-style-type: none">• Password• Client Certificate• CyberArk• Lieberman• Hashicorp Vault <p>For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.</p>
Username	<p>(Required) The username for the database.</p>
Password	<p>(Required) The password for the supplied username.</p>



Option	Description
Database	The name of the database to authenticate to. <div data-bbox="391 306 1479 384" style="border: 1px solid green; padding: 5px;">Tip: To authenticate via LDAP or saslauthd, type \$external.</div>
Port	(Required) The TCP port that the MongoDB database instance listens on for communications from Tenable Nessus Manager.



Database Credentials Authentication Types

Depending on the authentication type you select for your [database credentials](#), you must configure the following options.

- [Client Certificate](#)
- [Password](#)
- [Import](#)
- [CyberArk](#)
- [CyberArk \(Legacy\)](#)
- [HashiCorp Vault](#)
- [Lieberman](#)

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 Vulnerability Management 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 Vulnerability Management 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: <ul style="list-style-type: none">• Windows• SQL Oracle values include: <ul style="list-style-type: none">• SYSDBA• SYSOPER• NORMAL Sybase ASE values include: <ul style="list-style-type: none">• RSA• Plain Text	yes
Instance name	SQL Server	The name for your database instance.	no



Option	Database Types	Description	Required
Service type	Oracle	Valid values include: <ul style="list-style-type: none">• 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*.

CyberArk

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management 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.	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 Username , Identifier , or Address . 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	yes



Option	Description	Required
	<p>all targets have the same identifier.</p> <p>Note: The Username option also adds the Address parameter of the API query and assigns the target IP of the resolved host to the Address parameter. This may lead to failure to fetch credentials if the CyberArk Account Details Address field contains a value other than the target IP address.</p>	
Username	(If Get credential by is 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
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 Vulnerability Management can get credentials from CyberArk to use in a scan.

Option	Database Types	Description	Required
Username	All	The target system's username.	yes



Option	Database Types	Description	Required
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 <code>/AIMWebservice/v1.1/AIM.asmx</code> .	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 Password	All	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.	no
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 Cli-	All	The passphrase for the private key, if	no



Option	Database Types	Description	Required
ent Certificate Private Key Passphrase		your authentication implementation requires it.	
CyberArk Appld	All	The Appld 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
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



Option	Database Types	Description	Required
Database Name	DB2 PostgreSQL	The name of the database.	no
Auth type	Oracle SQL Server Sybase ASE	SQL Server values include: <ul style="list-style-type: none">• Windows• SQL Oracle values include: <ul style="list-style-type: none">• Normal• System Operator• System Database Administrator• SYSDBA• SYSOPER• NORMAL Sybase ASE values include: <ul style="list-style-type: none">• RSA• Plain Text	yes
Instance Name	SQL Server	The name for your database instance.	no
Service type	Oracle	Valid values include: <ul style="list-style-type: none">• 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	no



Option	Database Types	Description	Required
		option.	

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	Database Types	Description	Required
Hashicorp Vault host	All	The Hashicorp Vault IP address or DNS address. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">Note: If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type <i>IP address or hostname / subdirectory path</i>.</div>	yes
Hashicorp Vault port	All	The port on which Hashicorp Vault listens.	yes
Authentication Type	All	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. Click Add File to select the appropriate files for the client	yes



		certificate and private key.	
Role ID	All	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	All	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	All	The URL Tenable Nessus Manager uses to access Hashicorp Vault.	yes
Username Source	All	A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	All	The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	All	The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	All	The key secret you want to retrieve values for.	yes
Use SSL	All	When enabled, Tenable Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Hashicorp Vault before enabling this	no



		option.	
Verify SSL Certificate	All	When enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no
Database Port	All	The port on which Tenable Nessus Manager communicates with the database.	yes
Auth Type	Oracle	The authentication method for the database credentials. Valid values include: <ul style="list-style-type: none">• SYSDBA• SYSOPER• NORMAL	yes
Service Type	Oracle	Valid values include: <ul style="list-style-type: none">• 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	yes



the **Service Type** option.

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 <i>IP address or hostname / sub-directory path</i> .	yes
Lieberman port	All	The port on which Lieberman listens.	yes
Lieberman API URL	All	The URL Tenable Nessus Manager 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 domain to the Lieberman user option, i.e., <i>domain\user</i> .	no
Lieberman Client Certificate	All	The file that contains the PEM certificate used to communicate with the	no



Option	Database Type	Description	Required
		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.	
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
Database Port	All	The port on which Tenable Nessus Manager communicates with the database.	yes



Option	Database Type	Description	Required
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: <ul style="list-style-type: none">• Windows• SQL Oracle values include: <ul style="list-style-type: none">• SYSDBA• SYSOPER• NORMAL Sybase ASE values include: <ul style="list-style-type: none">• RSA• Plain Text	yes
Instance Name	SQL Server	The name for your database instance.	no
Service type	Oracle	Valid values include: <ul style="list-style-type: none">• 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



Host Credentials

Nessus supports the following forms of host authentication:

- [SNMPv3](#)
- [Secure Shell \(SSH\)](#)
- [Windows](#)



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: <ul style="list-style-type: none">• No authentication and no privacy• Authentication without privacy• Authentication and privacy	Authentication and privacy
Authentication algorithm	The algorithm the remote service supports: MD5 or SHA1 .	SHA1
Authentication password	(Required) The password associated with the User-name .	-
Privacy algorithm	The encryption algorithm to use for SNMP traffic:	AES



Option	Description	Default
	AES or DES .	
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.

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 1000 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 <code>known_hosts</code> file is available and provided as part of the Global Credential Settings of the scan policy in the known_hosts file field, 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 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 Nessus impersonates while scanning.
Attempt	Cleared	Enables or disables dynamic privilege escalation. When



Option	Default Value	Description
least privilege		enabled, 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, 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 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.

CyberArk (Nessus Manager only)

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.	yes
Port	The port on which the CyberArk API communicates.	yes



Option	Description	Required
	By default, Tenable uses 443.	
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.	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. 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 (for example, example.com). By default, Tenable Nessus uses 443.	yes



Option	Description	Required
Get credential by	<p>The method with which your CyberArk API credentials are retrieved. Can be Username, Identifier, or Address.</p> <p>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.</p> <p>Note: The Username option also adds the Address parameter of the API query and assigns the target IP of the resolved host to the Address parameter. This may lead to failure to fetch credentials if the CyberArk Account Details Address field contains a value other than the target IP address.</p>	yes
Username	(If Get credential by is 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 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) (Nessus Manager only)

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 Certificate Private Key	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Priv-	(Optional) The passphrase for the private key, if required.



Option	Description
ate Key Pass-phrase	
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.

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 Nessus implementation of Linux-based Kerberos authentication for SSH supports the aes-cbc and aes-ctr encryption algorithms. An overview of how 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 Nessus to connect to the KDC if it is running on a port other than 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.



Option	Description
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.

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.
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable.io receiving an unrecognized password prompt on the target host's interactive SSH shell.

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. Nessus supports both DSA and RSA key formats.

Like Public Key Encryption, Nessus supports RSA and DSA OpenSSH certificates. Nessus also requires the user certificate, which is signed by a Certificate Authority (CA), and the user's private key.



Note: Nessus supports the openssh SSH public key format (pre-7.8 OpenSSH). 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, 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, Nessus can escalate privileges on Cisco devices by selecting Cisco 'enable' or .k5login for Kerberos logins.

Note: 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.

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, 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	Allows for increasing privileges once authenticated.



Option	Description
with	

Thycotic Secret Server (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 <code>https://pw.mydomain.com/SecretServer/</code> . We parse this to know that HTTPS defines it is a ssl connection, <code>pw.mydomain.com</code> is the target address, <code>/SecretServer/</code> 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 (required)	Use this value in cloud instances of Thycotic to define which organization your query should hit.
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.

BeyondTrust (Nessus Manager only)

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 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 con-



	nections 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.

Lieberman (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 <i>IP address or hostname / subdirectory path</i> .	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., <i>domain\user</i> .	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	no



Option	Description	Required
	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

Wallix Bastion (Nessus Manager only)

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



Option	Description	Required
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 user interface. Used for API Key authentication to the API.	yes
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 .	Required if you wish to escalate privileges.



Option	Description	Required
	<p>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.</p> <p>Note: Multiple options for privilege escalation are supported, including <i>su</i>, <i>su+sudo</i> and <i>sudo</i>. 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 escalation through WALLIX Bastion PAM. The Escalation Account Name field is then required to complete your privilege escalation.</p> <p>Note: For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide.</p>	
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: <ul style="list-style-type: none">• 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	yes



Option	Description	Required
	<p>database instance.</p> <p>The Service value you enter must match your parameter selection for the Service Type option.</p>	

HashiCorp Vault (Nessus Manager only)

Option	Default Value	Required
Hashicorp Vault host	<p>(Required) The Hashicorp Vault IP address or DNS address.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: If your Hashicorp Vault installation is in a sub-directory, you must include the subdirectory path. For example, type <i>IP address or hostname/sub-directory path</i>.</p></div>	yes
Hashicorp Vault port	<p>(Required) The port on which Hashicorp Vault listens.</p>	yes
Hashicorp Vault API URL	<p>The URL Tenable Nessus Manager uses to access Hashicorp Vault.</p>	yes
Authentication Type	<p>Specifies the authentication type for connecting to the instance: App Role or Certificates.</p> <p>If you select Certificates, additional options for Hashicorp Client Certificate and Hashicorp Client Certificate Private Key appear. Click Add File to select files for the client certificate and private key.</p>	yes
Role ID	<p>Required if you select App Role for Authentication Type. The GUID provided by Hashicorp Vault when you configured your App Role.</p>	yes
Role Secret ID	<p>Required if you select App Role for Authentication Type. The GUID generated by Hashicorp Vault when you configured your App Role.</p>	yes



Authentication URL	The URL Tenable Nessus Manager uses to access Hashicorp Vault.	yes
Namespace	The name of a specified team in a multi-team environment. For more information about multi-team environments, see the Hashicorp documentation .	no
KV Engine URL	The URL Tenable Nessus Manager uses to access the Hashicorp Vault secrets engine.	yes
Username Source	Specifies if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	The key secret you want to retrieve values for.	yes
Use SSL	When enabled, Tenable Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no

Centrify (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 <i>IP address or hostname/sub-directory path</i> .



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	<p>The length of time, in minutes, that you want to keep credentials checked out in Centrify.</p> <p>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.</p> <div style="border: 1px solid blue; padding: 5px;"><p>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.</p></div>
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.

Arcon (Nessus Manager only)

Option	Default Value
Arcon host	(Required) The Arcon IP address or DNS address.



	<p>Note: If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type <i>IP address or hostname/subdirectory path</i>.</p>
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.
Checkout Duration	<p>(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon.</p> <p>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.</p> <p>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.</p>
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.



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 make use of 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 it is required by the remote Windows server. 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 will attempt to log in via NTLMSSP/LMv2 authentication. If that fails, Nessus will then attempt 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 will allow 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 will be 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 will not be 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 Tenable [blog 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	Enabled	If this option is disabled, then it is theoretically possible



Option	Default	Description
NTLMv1 authentication		to trick Nessus into attempting to log into a Windows server with domain credentials via the NTLM version 1 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 directly log into other servers. 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 http://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.



Option	Default	Description
		By default, Windows systems have the Windows Server service enabled, which means you do not need to enable 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)

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.	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	(Required if Kerberos Target Authentication is	yes



Option	Description	Required
Center (KDC)	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.	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	<p>The method with which your CyberArk API credentials are retrieved. Can be Username, Identifier, or Address.</p> <p>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.</p> <p>Note: The Username option also adds the Address parameter of the API query and assigns the target IP of the resolved host to the Address parameter. This may lead to failure to fetch credentials if the CyberArk Account Details Address field contains a value other than the target IP address.</p>	yes
Username	(If Get credential by is Username) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be	no



Option	Description	Required
	retrieved from.	
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 (Legacy) (Nessus Manager only)

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 <code>/AIMWebservice/v1.1/AIM.asmx</code> .
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.



Option	Description
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.
Appld	The Appld 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 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 cus-



Option	Description
	tom_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.

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.
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.

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 <i>https://pw.mydomain.com/SecretServer</i> , Tenable Nessus determines it is an SSL connection, that <i>pw.mydomain.com</i> is the target address, and that <i>/SecretServer</i> 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 con-



	nections instead of password authentication.
Verify SSL Certificate	<p>If enabled, Tenable Nessus verifies the SSL Certificate on the Thycotic server.</p> <p>For more information about using self-signed certificates, see Custom SSL Server Certificates.</p>

BeyondTrust (Tenable Nessus Manager only)

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.
BeyondTrust API key	(Required) The API key provided by BeyondTrust.
Checkout duration	<p>(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.</p> <div style="border: 1px solid blue; padding: 5px;"><p>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.</p></div>
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 <i>IP address or hostname / subdirectory path</i> .	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.,	no



Option	Description	Required
	<code>domain\user.</code>	
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
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)

Option	Description	Required
WALLIX Host	The IP address for the WALLIX Bastion host.	yes



Option	Description	Required
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 user interface. Used for API Key authentication to the API.	yes
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	Required if you



Option	Description	Required
	<p>Management (PAM). Use the drop-down menu to select the privilege elevation method. To bypass this function, leave this field set to Nothing.</p> <div data-bbox="514 411 1195 684" style="border: 1px solid red; padding: 5px;"><p>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.</p></div> <div data-bbox="514 705 1195 1100" style="border: 1px solid blue; padding: 5px;"><p>Note: Multiple options for privilege escalation are supported, including <i>su</i>, <i>su+sudo</i> and <i>sudo</i>. 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 escalation through WALLIX Bastion PAM. The Escalation Account Name field is then required to complete your privilege escalation.</p></div> <div data-bbox="514 1121 1195 1276" style="border: 1px solid blue; padding: 5px;"><p>Note: For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide.</p></div>	wish to escalate privileges.
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: <ul style="list-style-type: none">• SYSDBA• SYSOPER• NORMAL	no



Option	Description	Required
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

HashiCorp Vault (Tenable Nessus Manager only)

Option	Default Value	Required
Hashicorp Vault host	(Required) The Hashicorp Vault IP address or DNS address. Note: If your Hashicorp Vault installation is in a sub-directory, you must include the subdirectory path. For example, type <i>IP address or hostname/subdirectory path</i> .	yes
Hashicorp Vault port	The port on which Hashicorp Vault listens.	yes
Authenticaton 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. Click Add File to select files for the client certificate and private key.	yes
Role ID	Required if you select App Role for Authentication Type . The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	Required if you select App Role for Authentication Type . The GUID generated by Hashicorp Vault when you configured your App Role.	yes



Authentication URL	The URL Tenable Nessus Manager uses to access Hashicorp Vault.	yes
Namespace	The name of a specified team in a multi-team environment. For more information about multi-team environments, see the Hashicorp documentation .	no
KV Engine URL	The URL Tenable Nessus Manager uses to access the Hashicorp Vault secrets engine.	yes
Username Source	Specifies if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	(Required) The key secret you want to retrieve values for.	yes
Use SSL	When enabled, Tenable Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no

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 <i>IP address or hostname/sub-</i>



	<code>directory path.</code>
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	<p>The length of time, in minutes, that you want to keep credentials checked out in Centrify.</p> <p>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.</p> <p>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.</p>
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.

Arcon (Tenable Nessus Manager only)



Option	Default Value
Arcon host	<p>(Required) The Arcon IP address or DNS address.</p> <div data-bbox="634 310 1479 468" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type <i>IP address or hostname/subdirectory path</i>.</p></div>
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.
Checkout Duration	<p>(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon.</p> <p>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.</p> <div data-bbox="634 1377 1479 1570" style="border: 1px solid #0070C0; padding: 5px;"><p>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.</p></div>
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.



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 and Active Directory Starter Scans.

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.

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 Nessus connects using secure communication (HTTPS). When disabled, Tenable Nessus connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable Nessus 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

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
Username	(Required) Username used for authentication to the Nutanix Prism Central host.	-
Password	(Required) Password used for authentication to the Nutanix Prism Central host.	-
Discover Host	This option adds any discovered Nutanix Prism Central hosts to the scan targets to be scanned.	-
Discover Virtual Machines	This option adds any discovered Nutanix Prism Central Virtual Machines to the scan targets to be scanned.	-
HTTPS	When enabled, Tenable Nessus connects using secure communication (HTTPS). When disabled, Tenable Nessus connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable Nessus 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



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 Nessus connects using secure communication (HTTPS). When disabled, Tenable Nessus connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable Nessus 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

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 Nessus connects using secure communication (HTTPS). When disabled, Tenable Nessus connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable Nessus 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 Nessus 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

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](#).

Tenable Nessus can access VMware servers through the native VMware SOAP API.



Option	Description	Default
Username	(Required) The username for the ESXi server account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the ESXi user.	-
Do not verify SSL Certificate	Do not validate the SSL certificate for the ESXi server.	disabled

VMware vCenter Auto Discovery

For more information on configuring VMWare vCenter SOAP API, see [Configure vSphere Scanning](#).

Tenable Nessus can access vCenter through the native VMware vCenter SOAP API. If available, Tenable Nessus uses the vCenter REST API to collect data in addition to the SOAP API.

Note: You must use a vCenter admin account with read and write permissions.

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 Nessus.	443
Username	(Required) The username for the vCenter server account with admin read/write access that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the vCenter server user.	-
HTTPS	When enabled, Tenable Nessus connects using secure communication (HTTPS). When disabled, Tenable Nessus connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable Nessus 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.	
Auto Discover Managed VMware ESXi Hosts	This option adds any discovered VMware ESXi hypervisor hosts to the scan targets you include in your scan.	not enabled
Auto Discover Managed VMware ESXi Virtual Machines	This option adds any discovered VMware ESXi hypervisor virtual machines to the scan targets you include in your scan.	not enabled

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

AirWatch

Option	Description
AirWatch Environment API URL (required)	The URL of the SOAP or REST API.
Port	Set to use a different port to authenticate with Airwatch.
Username (required)	The username to authenticate with Airwatch's API.
Password (required)	The password to authenticate with Airwatch's API.
API Keys (required)	The API Key for the Airwatch REST API.
HTTPS	Set to use HTTPS instead of HTTP.
Verify SSL Certificate	Verify whether the SSL Certificate on the server is signed by a trusted CA.

Apple Profile Manager

Option	Description
Server (required)	The server URL to authenticate with Apple Profile Manager.
Port	Set to use a different port to authenticate with Apple Profile Manager.
Username (required)	The username to authenticate.
Password (required)	The password to authenticate.
HTTPS	Set to use HTTPS instead of HTTP.
Verify SSL Certificate	Verify whether the SSL Certificate on the server is signed by a trusted CA.

Global Credential Settings



Force device updates	Force devices to update with Apple Profile Manager immediately.
Device update timeout (minutes)	Number of minutes to wait for devices to reconnect with Apple Profile Manager

Good MDM

Option	Description
Server (required)	The server URL to authenticate with Good MDM.
Port (required)	Set the port to use to authenticate with Good MDM.
Domain (required)	The domain name for Good MDM.
Username (required)	The username to authenticate.
Password (required)	The password to authenticate.
HTTPS	Set to use HTTPS instead of HTTP.
Verify SSL Certificate	Verify whether the SSL Certificate on the server is signed by a trusted CA.

MaaS360

Option	Description
Username (required)	The username to authenticate.
Password (required)	The password to authenticate.
Root URL (required)	The server URL to authenticate with MaaS360.
Platform ID (required)	The Platform ID provided for MaaS360.
Billing ID	The Billing ID provided for MaaS360.



(required)	
App ID (required)	The App ID provided for MaaS360.
App Version (required)	The App Version of MaaS360.
App access key (required)	The App Access Key provided for MaaS360.
Collect All Device Data	<p>When enabled, the scan collects all data types.</p> <p>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:</p> <ul style="list-style-type: none">• Collect Device Summary• Collect Device Applications• Collect Device Compliance• Collect Device Policies

MobileIron

Option	Description
VSP Admin Portal URL	The server URL Tenable Nessus uses to authenticate to the MobileIron administrator portal.
VSP Admin Portal Port	(Optional) The port Tenable Nessus uses to authenticate to the MobileIron administrator portal (typically, port 443 or 8443). The system assumes port 443 by default.
Port	(Optional) The port Tenable Nessus uses to authenticate to MobileIron (typically, port 443).
Username	The username for the account you want Tenable Nessus to use to authenticate to MobileIron.



Password	The password for the account you want Tenable Nessus to use to authenticate to MobileIron.
HTTPS	(Optional) When enabled, Tenable Nessus uses an encrypted connection to authenticate to MobileIron.
Verify SSL Certificate	When enabled, Tenable Nessus verifies that the SSL Certificate on the server is signed by a trusted CA.

VMware Workspace One

Option	Description	Default	Required
VMware Workspace One Environment API URL	The SOAP URL or REST API URL you want to use to authenticate with VMware Workspace One.	--	Yes
Port	The TCP port that VMware Workspace One listens on for communications from Tenable.	443	Yes
Username	The username for the VMware Workspace One user account Tenable uses to authenticate to VMware Workspace One's REST API.	--	Yes
Password	The password for the VMware Workspace One user.	--	Yes
API Key	The API key for the VMware Workspace One REST API.	--	Yes
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled	No
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed	Enabled	No



Option	Description	Default	Required
	by a trusted CA. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;">Tip: If you are using a self-signed certificate, disable this setting.</div>		
Scanner	Specifies which Nessus scanner Tenable Security Center uses when scanning the server. Tenable Security Center can only use one Nessus scanner to add data to a mobile repository.	--	Yes
Update Schedule	Specifies when Tenable Security Center scans the server to update the mobile repository. On each scan, Tenable Security Center removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00	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 to Nessus Professional or managed scanners.

Note: Patch management integration is not available on Nessus Professional or managed scanners.

Tenable Nessus 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)

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 Nessus connects using secure communication (HTTPS). When disabled, Tenable Nessus connects using standard HTTP.	Enabled
Verify SSL certificate	When enabled, Tenable Nessus 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>BES</Domain>
    <Property Name="Packages - With Versions (Tenable)" ID="74"><![CDATA[if (exists true whose (if true then repository) else false)) then unique values of (lpp_name of it & "|" & version of it as string & "|" & "fileset"
    tecture of operating system) of filesets of products of object repository else if (exists true whose (if true then
    anpackage) else false)) then unique values of (name of it & "|" & version of it as string & "|" & "deb" & "|" &
    it & "|" & architecture of operating system) of packages whose (exists version of it) of debianpackages else if
    whose (if true then (exists rpm) else false)) then unique values of (name of it & "|" & version of it as string
    "|" & architecture of it & "|" & architecture of operating system) of packages of rpm else if (exists true whose
    (exists ips image) else false)) then unique values of (full name of it & "|" & version of it as string & "|" &
    architecture of operating system) of latest installed packages of ips image else if (exists true whose (if true
    pkgdb) else false)) then unique values of (pkginst of it & "|" & version of it & "|" & "pkg10") of pkginfos of pk
    "<unsupported>"]></Property>
    <Property Name="Tenable AIX Technology Level" ID="76">current technology level of operating system</Prop
    <Property Name="Tenable Solaris - Showrev -a" ID="77"><![CDATA[if ((operating system as string as lowerc
    "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>
  </Task>
</BES>
```



```
</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)

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.

SCCM scanning uses the following Tenable plugins: 57029, 57030, 73636, and 58186.

Note: SCCM patch management plugins support SCCM 2007, SCCM 2012, SCCM 2016, and SCCM 2019.



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)

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 the target system.	-
Password	(Required) The password for the WSUS administrator user.	-
HTTPS	When enabled, Tenable Nessus connects using secure communication (HTTPS).	Enabled



Option	Description	Default
	When disabled, Tenable Nessus connects using standard HTTP.	
Verify SSL Certificate	When enabled, Tenable Nessus 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 Server

Red Hat Satellite 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 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.

Satellite scanning uses the following Tenable plugins: 84236, 84235, 84234, 84237, and 84238.

Option	Description	Default
Satellite server	(Required) The Red Hat Satellite IP address or system name.	-
Port	(Required) The TCP port that Red Hat Satellite listens on for communications from Tenable Nessus.	443
Username	(Required) The username for the Red Hat Satellite account that Tenable Nessus uses to perform checks on the target system.	-
Password	(Required) The password for the Red Hat Satellite user.	-
Verify SSL	When enabled, Tenable Nessus verifies that the	Enabled



Option	Description	Default
Certificate	SSL certificate on the server is signed by a trusted CA. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;">Tip: If you are using a self-signed certificate, disable this setting.</div>	

Red Hat Satellite 6 Server

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 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 Nessus connects using secure communication (HTTPS). When disabled, Tenable Nessus connects using	Enabled



Option	Description	Default
	standard HTTP.	
Verify SSL Certificate	When enabled, Tenable Nessus 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 Altiris

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.	-
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 database account with the privileges to query all the data in the Altiris MSSQL database.	-



Credential	Description	Default
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!).



Option	Default	Description
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 <code><form method="POST" name="auth_form" action="/login.php"></code> would be /login.php.
Login parameters	Specify the authentication parameters (for example, login-n=%USER%&password=%PASS%). If you use the keywords %USER% and



Option	Description
	%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 IPMI 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		



Compliance

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](#).

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	SSH
Citrix XenServer	SSH
Database	Database
Dell Force10 FTOS	SSH
Extreme ExtremeXOS	SSH
F5	F5
FireEye	SSH
Fortigate FortiOS	SSH
Generic SSH	SSH
Google Cloud Platform	SSH
HP ProCurve	SSH
Huawei VRP	SSH
IBM iSeries	IBM iSeries
Juniper Junos	SSH
Microsoft Azure	Microsoft Azure
Mobile Device Manager	AirWatch, Apple Profile Manager, or Mobileiron
MongoDB	MongoDB



NetApp API	NetApp API
NetApp Data ONTAP	SSH
OpenStack	OpenStack
NetApp Data ONTAP	SSH
Palo Alto Networks PAN-OS	PAN-OS
Rackspace	Rackspace
RHEV	RHEV
Salesforce.com	Salesforce SOAP API
SonicWALL SonicOS	SSH
Splunk	Splunk API
Unix	SSH
Unix File Contents	SSH
VMware vCenter/vSphere	VMware ESX SOAP API or VMware vCenter SOAP API
WatchGuard	SSH
Windows	Windows
Windows File Contents	Windows
Zoom	Zoom
ZTE ROSNG	SSH



Upload a Custom Audit File

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://nvd.nist.gov/ncp/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.

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.

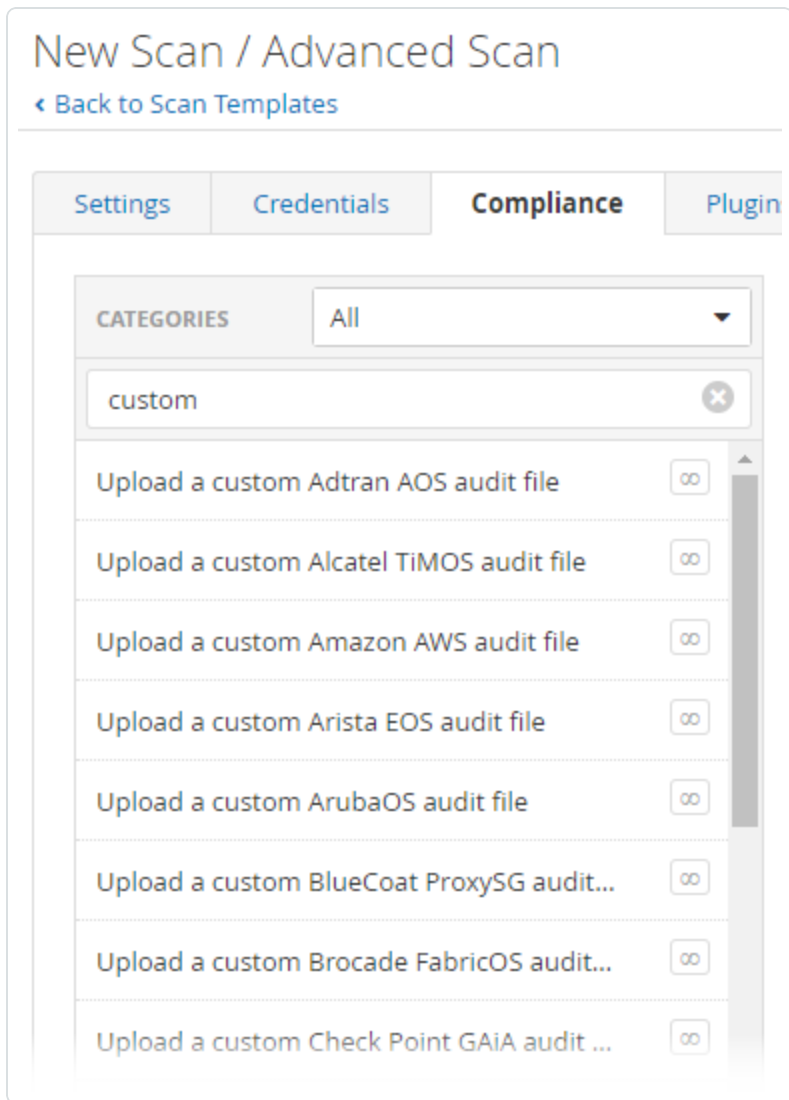
The **Scan Templates** page appears.

4. Click the [scan template](#) that you want to use.

The scan settings page appears.

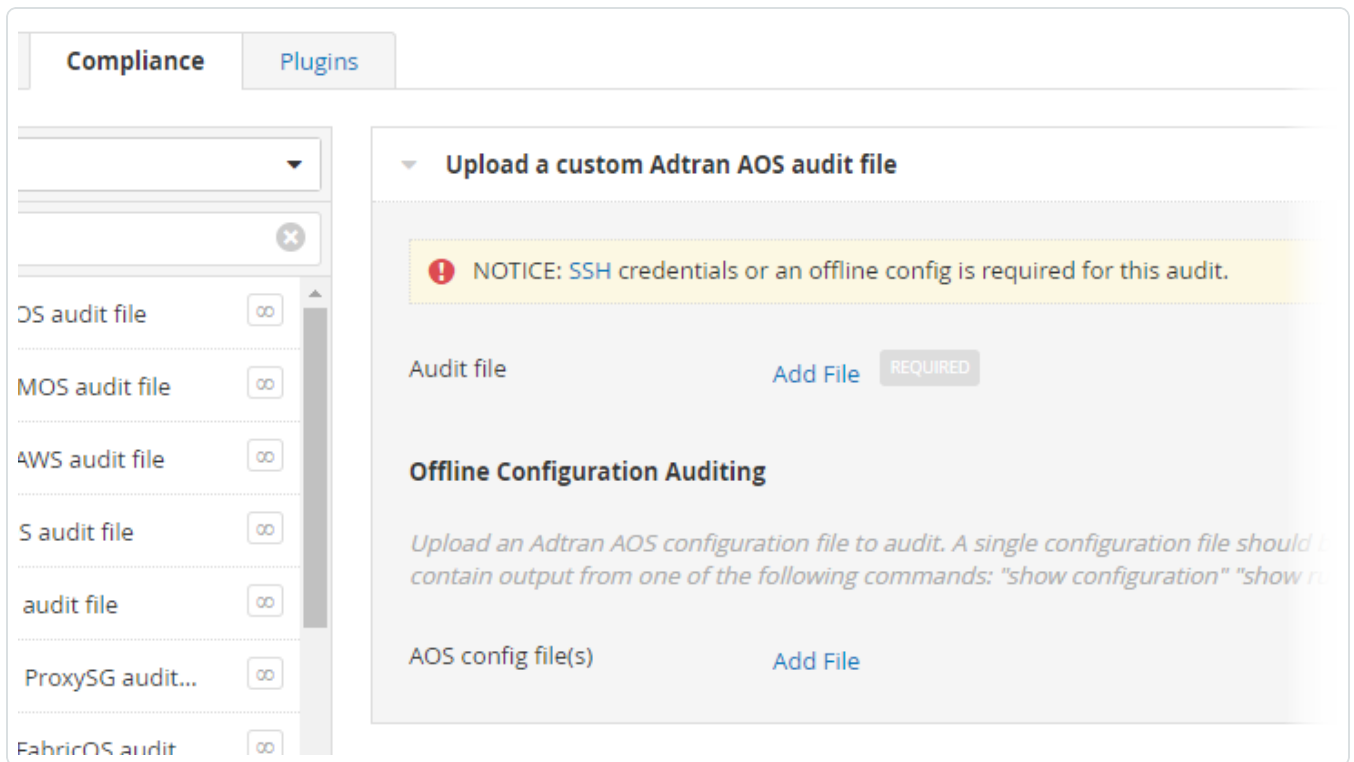
5. Open the **Compliance** tab.
6. In the **Filter Compliance** box, type custom.

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.

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: <pre><data-stream id="scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip"></pre>
SCAP Benchmark ID	None	The Benchmark ID that you copied from the SCAP XML file. Example: <pre><xccdf:Benchmark id="xccdf_gov.nist_benchmark_USGCB-Windows-7"></pre>



SCAP Profile ID	None	<p>The Profile ID that you copied from the SCAP XML file.</p> <p>Example:</p> <pre><xccdf:Profile id="xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1"></pre>
OVAL Result Type	Full results w/ system characteristics	<p>The information you want the results file to include.</p> <p>The results file can be one of the following types: full results with system characteristics, full results without system characteristics, or thin results.</p>
Linux (OVAL) or Windows (OVAL)		
OVAL definitions file	None	A valid zip file that contains OVAL standalone content.



Plugins

The **Advanced Scan** 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.

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 **blue** 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.

Selecting a specific **Plugin Name** shows the plugin output that you would see in a report.

The plugin details include a **Synopsis**, **Description**, **Solution**, **Plugin Information**, and **Risk Information**.

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.

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 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.



Configure Dynamic Plugins

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 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](#)



Example: Host Discovery

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 a Scan

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

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 an Attack Surface Discovery Scan with Bit Discovery

Note: The Attack Surface Discovery scan template is only available in Tenable Nessus Expert.

You can use Nessus's integration with Bit Discovery 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

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](#).

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: 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**.

Nessus imports the scan and its associated data.



Create an Agent Scan

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.



Modify Scan Settings

A standard user or administrator can perform this procedure.

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

Note: You need administrator permissions to complete the following procedures.

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

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**.
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** check box. Otherwise, select the check box.
9. Click **Save**.

Scenario 2: Scanning vCenter-Managed ESXi/vSpheres

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.
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**.
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 local ESXi account.
9. In the **Password** box, type the password associated with the local ESXi 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** check box. Otherwise, deselect the check box.
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. For more information, see [Create a Scan](#).



Configure an Audit Trail

A standard user or administrator can perform this procedure.

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

In addition to configuring [Schedule](#) settings for a scan, you can manually start a scan run.

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](#).



Stop a Running Scan

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 Nessus 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.

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

A standard user or administrator can perform this procedure.

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. For more information, see [Scan Folders](#).

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.

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

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.



My Scans

Import

New Folder

[+ New Scan](#)

Total Records: 2

Search Scans

<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	Advanced Network Scan	On Demand	N/A		
<input type="checkbox"/>	Host Discovery Scan	On Demand	N/A		



Manage Scan Folders

A standard user or administrator can complete the following procedures.

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. For more information, see [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 Nessus Agent scan in Tenable Nessus Manager.
Hosts	The Hosts page shows all scanned targets.
Vulnerabilities	List of identified vulnerabilities, sorted by severity. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;">Tip: To view vulnerabilities by VPR, click  in the table header, click Disable Groups, and sort the table by VPR Score.</div>
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.
History	The History shows a listing of scans: Start Time , End Time , and the Scan Statuses .
Summary (Attack Surface Dis-	View a summary of your attack surface discovery scan configuration. The summary table shows a row for each scanned domain with the following



covery scan template only)	<p>details:</p> <ul style="list-style-type: none">• 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 the domain data Tenable Nessus pulls was updated in Bit Discovery. Bit Discovery 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 Bit Discovery. Bit Discovery 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)	<p>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:</p> <ul style="list-style-type: none">• Hostname – The record's hostname.• 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:<ul style="list-style-type: none">• 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 v2.0**).
- **Scanner** – The scanner used for the scan.
- **Start** – The scan start time and date.
- **End** – The scan end time and date.
- **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 scores or CVSSv3 scores, depending on your configuration.

- You can choose whether Tenable Nessus calculates the severity of vulnerabilities using CVSSv2 or CVSSv3 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 Severity Base for an Individual Scan](#).

VPR

When you [view vulnerabilities](#) in scan results, Tenable Nessus also shows severity based on VPR.



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.

Tip: **Risk Factor** and **Severity** values are unrelated; they are calculated separately.

CVSS-Based Severity

Tenable assigns all vulnerabilities a severity (**Info**, **Low**, **Medium**, **High**, or **Critical**) based on the vulnerability's static CVSSv2 or CVSSv3 score, depending 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
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.
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.
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.
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.
Info	The plugin's highest vulnerability CVSSv2 score is 0. - or -	The plugin's highest vulnerability CVSSv3 score is 0. - or -



The plugin does not search for vulnerabilities.

The plugin does not search for vulnerabilities.

CVSS-Based Risk Factor

For each plugin, Tenable interprets the CVSSv2 or CVSSv3 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 in the National Vulnerability Database (NVD) (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

You can view the following key drivers to explain a vulnerability's VPR.

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: 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. 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 Severity Base for an Individual Scan](#).

For more information about CVSS scores and severity ranges, see [CVSS Scores vs. VPR](#).

Note: You cannot configure the default severity base in Tenable Nessus Manager.

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** or **CVSS v3.0** 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 Severity Base for an Individual Scan

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.

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](#).

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 scans 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.



- **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

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

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.

To 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.

To 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.

To 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.

To 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 table **Filter** button.


- Click the  button to delete the saved filter.

The **Delete Filter** window appears. Click **Continue** to confirm the deletion.

To 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.

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.
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	<p>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).</p> <p>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.</p>
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	Filter results based on if a CVSS v2.0 temporal vector is equal to, is not



Vector	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	<p>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).</p> <p>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.</p>
CVSS 3.0 Temporal Score	Filter results based on if a CVSS v3.0 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 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).
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).
Exploit Available	Filter results based on the vulnerability having a known public exploit.
Exploit Database ID	Filter results based on if an Exploit Database ID (EBD-ID) reference is equal 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 Name	Filter results based on if a Metasploit name is equal to, is not equal to, 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 Plugin Description contains, or does not contain a given string (for example, remote).
Plugin Family	Filter results if 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 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 Publication Date	Filter results based on if a Nessus plugin publication date is less than, is 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

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](#).

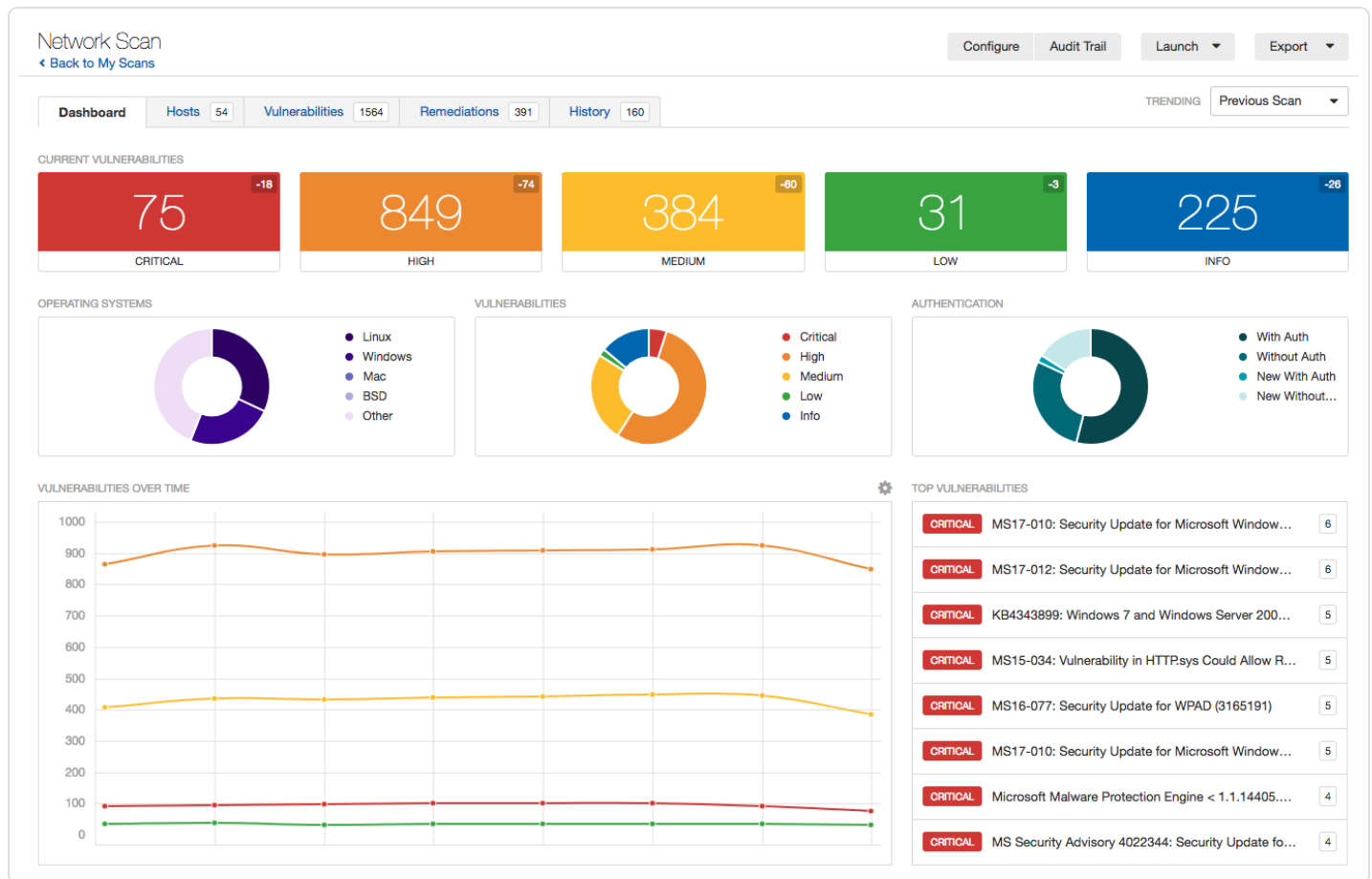


Dashboard

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

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. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;">Note: This section does not appear for basic network scans.</div>
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. <ul style="list-style-type: none">• 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]

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


For information on managing vulnerabilities, see:

- [View Vulnerabilities](#)
- [Search and Filter Results](#)
- [Modify a Vulnerability](#)
- [Group Vulnerabilities](#)
- [Snooze a Vulnerability](#)
- [Live Results](#)



View Vulnerabilities

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.



Modify a Vulnerability

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 [Vulnerability Snoozing](#).

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.



Group Vulnerabilities

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, Nessus shows the **Mixed** severity level.

localhost Configure Audit Trail Export

[Back to My Scans](#)

Hosts 1 Vulnerabilities 21

Filter Search Vulnerabilities 21 Vulnerabilities

Sev	Name	Family	Count	
CRITICAL	36 Mozilla Firefox (Multiple Issues)	MacOS X Local Security Checks	36	
CRITICAL	14 Microsoft Office (Multiple Issues)	MacOS X Local Security Checks	19	
CRITICAL	10 Wireshark (Multiple Issues)	MacOS X Local Security Checks	10	
CRITICAL	3 Oracle VM VirtualBox (Multiple Issues)	Misc.	3	
HIGH	5 Apple Mac OS X (Multiple Issues)	MacOS X Local Security Checks	5	
INFO	4 SSH (Multiple Issues)	General	4	
INFO	Authenticated Check : OS Name and Installed Package Enumeration	Settings	1	
INFO	Common Platform Enumeration (CPE)	General	1	
INFO	Device Hostname	General	1	
INFO	Device Type	General	1	

Scan Details

Name: localhost
Status: Imported
Policy: Advanced Scan
Start: July 3 at 4:09 PM
End: July 3 at 4:09 PM
Elapsed: a few seconds

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

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 .
5. Click **Enable Groups**.

Nessus groups similar vulnerabilities in one row.

To ungroup vulnerabilities:

1. In the header row of the vulnerabilities table, click .
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.



Snooze a Vulnerability

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.



Live Results

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 screenshot shows the Nessus interface for a scan on localhost. The 'Vulnerabilities' tab is active, showing 33 vulnerabilities. A table lists the following items:

Sev	Name	Family	Count
CRITICAL	Mozilla Foundation Unsupported Application Detection (macOS)	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 59 Multiple Vulnerabilities (macOS)	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 59.0.1 Multiple Code Execution Vulnerabilities (macOS)	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 59.0.2 Denial of Service Vulnerability (macOS)	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 60 Multiple Critical Vulnerabilities (macOS)	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 61 Multiple Critical Vulnerabilities (macOS)	MacOS X Local Security Checks	1
HIGH	Security Update for Microsoft Office (July 2017) (macOS)	MacOS X Local Security Checks	1
HIGH	Security Update for Microsoft Office (October 2017) (macOS)	MacOS X Local Security Checks	1
HIGH	Security Update for Microsoft Office (September 2017) (macOS)	MacOS X Local Security Checks	1
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS	1
INFO	Microsoft Office Installed (Mac OS X)	MacOS X Local Security Checks	5
INFO	DNS Server Detection	DNS	2

A notice states: "Notice: This scan has been updated with Live Results. Launch a new scan to confirm these findings or remove them." Scan details include: Name: localhost, Status: Completed, Policy: Advanced Scan, Scanner: Local Scanner, Modified: Today at 10:10 AM (Live Results). A donut chart shows the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

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

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

In Nessus Professional and Nessus Expert, if a scan includes live results, Tenable Nessus shows the following notice on the scan results page.

! Notice: This scan has been updated with **Live Results**. [Launch](#) a new scan to confirm these findings or [remove](#) them.

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

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 (see [Create a Custom Report Template](#) for more information), 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 host-name, 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

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](#) and [Import a Policy](#).

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](#).

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.

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 Nessus 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.




Policies

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: For information about default policy templates and settings, see [Scan Templates](#).

Policies

Import [+ New Policy](#)

 Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of [scan templates](#). From this page you can view, create, import, download, edit, and delete policies.

Total Records: 2

<input type="checkbox"/> Name ^	Template	Last Modified		
<input type="checkbox"/> Advanced Scan Policy	Advanced Scan	Today at 10:35 AM	↓	×
<input type="checkbox"/> Internal PCI Network Scan Policy	Internal PCI Network Scan	Today at 10:36 AM	↓	×

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.



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.



Import a Policy

You can import an [exported](#) Tenable Nessus (.nessus) scan or policy and import it as a policy. 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: Supported file type is an exported Nessus (.nessus) file.

Tenable Nessus imports the file as a policy.

5. (Optional) [Modify Policy Settings](#).



Modify Policy Settings

A standard user or administrator can perform this procedure.

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.



Delete a Policy

This procedure can be performed by a standard user or administrator.

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 **X** button.

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

4. Click the **Delete** button.

Tenable Nessus deletes the policy.



About Nessus 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 both v2 and v3 values simultaneously. If both CVSS2 and CVSS3 attributes are present, Tenable Nessus calculates both scores. However in determining the Risk Factor attribute, currently the CVSS2 scores take precedence.

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 Nessus plugins, and search for specific plugins, see the [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 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 Nessus install, 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 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 Nessus Plugins?

By default, Nessus checks for updated components and plugins every 24 hours. Alternatively, you can update plugins manually from the [Scanner Settings Page](#) in the user interface.

You can also use the `nessuscli update --plugins-only` command to update plugins manually.

For more details, see the [Command Line](#) section of this guide.



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.

New Policy / Advanced Scan

[Back to Policy Templates](#) Disable All Enable All

Settings Credentials Compliance **Plugins** Show Enabled | Show All

STATUS	PLUGIN FAMILY	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	AIX Local Security Checks	11384		No plugin family selected.	
ENABLED	Amazon Linux Local Security Checks	906			
ENABLED	Backdoors	110			
ENABLED	CentOS Local Security Checks	2476			
ENABLED	CGI abuses	3685			
ENABLED	CGI abuses : XSS	640			
ENABLED	CISCO	855			
ENABLED	Databases	541			
ENABLED	Debian Local Security Checks	5045			
ENABLED	Default Unix Accounts	163			
ENABLED	Denial of Service	109			

Save Cancel

6. In the upper right corner, click the **Disable All** button.



Tenable Nessus disables all the plugin families.

New Policy / Advanced Scan Disable All Enable All

[Back to Policy Templates](#)

Settings Credentials Compliance **Plugins** Show Enabled | Show All

STATUS	PLUGIN FAMILY ^	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
DISABLED	AIX Local Security Checks	11384		No plugin family selected.	
DISABLED	Amazon Linux Local Security Checks	906			
DISABLED	Backdoors	110			
DISABLED	CentOS Local Security Checks	2476			
DISABLED	CGI abuses	3685			
DISABLED	CGI abuses : XSS	640			
DISABLED	CISCO	855			
DISABLED	Databases	541			
DISABLED	Debian Local Security Checks	5045			
DISABLED	Default Unix Accounts	163			
DISABLED	Denial of Service	109			

Save Cancel

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.



New Policy / Advanced Scan Disable All Enable All

[Back to Policy Templates](#)

Settings Credentials Compliance **Plugins** Show Enabled | Show All

STATUS	PLUGIN FAMILY ^	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
DISABLED	AIX Local Security Checks	11384	DISABLED	AIX 5.1 : IY19744	22372
DISABLED	Amazon Linux Local Security Checks	906	DISABLED	AIX 5.1 : IY20486	22373
DISABLED	Backdoors	110	DISABLED	AIX 5.1 : IY21309	22374
DISABLED	CentOS Local Security Checks	2476	DISABLED	AIX 5.1 : IY22266	22375
DISABLED	CGI abuses	3685	DISABLED	AIX 5.1 : IY22268	22376
DISABLED	CGI abuses : XSS	640	DISABLED	AIX 5.1 : IY23041	22377
DISABLED	CISCO	855	DISABLED	AIX 5.1 : IY23846	22378
DISABLED	Databases	541	DISABLED	AIX 5.1 : IY23847	22379
DISABLED	Debian Local Security Checks	5045	DISABLED	AIX 5.1 : IY24231	22380
DISABLED	Default Unix Accounts	163	DISABLED	AIX 5.1 : IY25437	22381
DISABLED	Denial of Service	109	DISABLED	AIX 5.1 : IY25504	22382

Save Cancel

8. For each plugin that you want to enable, click the **Disabled** button.

Tenable Nessus enables each plugin.



New Policy / Advanced Scan Disable All Enable All

[Back to Policy Templates](#)

Settings Credentials Compliance **Plugins** [Show Enabled](#) | [Show All](#)

STATUS	PLUGIN FAMILY ^	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
MIXED	AIX Local Security Checks	11384	ENABLED	AIX 5.1 : IY19744	22372
DISABLED	Amazon Linux Local Security Checks	906	ENABLED	AIX 5.1 : IY20486	22373
DISABLED	Backdoors	110	ENABLED	AIX 5.1 : IY21309	22374
DISABLED	CentOS Local Security Checks	2476	ENABLED	AIX 5.1 : IY22266	22375
DISABLED	CGI abuses	3685	DISABLED	AIX 5.1 : IY22268	22376
DISABLED	CGI abuses : XSS	640	DISABLED	AIX 5.1 : IY23041	22377
DISABLED	CISCO	855	DISABLED	AIX 5.1 : IY23846	22378
DISABLED	Databases	541	DISABLED	AIX 5.1 : IY23847	22379
DISABLED	Debian Local Security Checks	5045	DISABLED	AIX 5.1 : IY24231	22380
DISABLED	Default Unix Accounts	163	DISABLED	AIX 5.1 : IY25437	22381
DISABLED	Denial of Service	109	DISABLED	AIX 5.1 : IY25504	22382

[Save](#) [Cancel](#)

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

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.

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
Linux	<code># /opt/nessus/sbin/nessuscli update <tar.gz filename></code>
FreeBSD	<code># /usr/local/nessus/sbin/nessuscli update <tar.gz file-</code>



Platform	Command
	<i>name</i> >
Windows	C:\Program Files\Tenable\Nessus>nessuscli.exe update <tar.gz filename>
macOS	# /Library/Nessus/run/sbin/nessuscli update <tar.gz file- name>



Plugin Rules

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	<p>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.</p> <p>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.</p> <p>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.</p>
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.

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 7: 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.



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

A standard user or administrator can perform this procedure.

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 Rule

A standard user or administrator can perform this procedure.

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 **X** button.

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

4. Click the **Delete** button.

Tenable Nessus deletes the plugin rule.




Customized Reports

On the **Customized Reports** page in Nessus, you can view report templates, [create custom report templates](#), [copy report templates](#), and [customize the title and logo](#) that appear on each report.

Customized Reports New Report Template

Report Templates Name and Logo

 You can manage your report templates here.

Search Report Template 15 Report Templates

Template Name	Type	Last Modified
Complete List of Vulnerabilities by Host	System	
Compliance	System	



Create a Scan Report

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 check box in each row of a host you want to include in the scan report.
- In the **Vulnerabilities** tab, select the check box 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. From the drop-down box, 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) To save the selected report template as the default for PDF or HTML reports (depending on which format you selected), select the **Save as default** check box.
- c. Click **Generate Report**.

Tenable Nessus creates the scan report.

CSV

- a. Select the check boxes 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 **Save as default** check box.
- c. Click **Generate Report**.

Tenable Nessus creates the scan report.



Customize Report Title and Logo

In 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.

What to do next:

- [Create a Scan Report](#)



Create a Custom Report Template

Note: This feature is only available for Nessus Manager, Nessus Professional, and Nessus Expert.

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** textbox, 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**. Nessus saves your report template. You can select and edit the template from the **Report Templates** tab (see [Edit a Custom Report Template](#) for more information).



Copy a Report Template

Note: This feature is only available for Nessus Manager, Nessus Professional, and Nessus Expert.

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**. Nessus saves the new scan template. You can select and edit the template from the **Report Templates** tab (see [Edit a Custom Report Template](#) for more information).



Edit a Custom Report Template

Note: This feature is only available for Nessus Manager, Nessus Professional, and Nessus Expert.

Nessus allows you to edit custom report templates on the **Customized Reports** page.

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.

Note: You can only edit custom templates.

The template's detail page appears.

4. Edit the **Name**, **Description**, and **Chapters** as needed (see [Create a Custom Report Template](#) for more information).

5. Click **Save**.

Nessus saves your template changes.



Delete a Custom Report Template

Note: This feature is only available for Nessus Manager, Nessus Professional, and Nessus Expert.

To 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 **X** button.

Note: You can only delete custom templates.

The **Delete Report Template** window appears.

4. Click **Delete**.

Nessus deletes your custom template.



Terrascan

Terrascan is a static code analyzer for Infrastructure as Code (IaC). You can install and run Terrascan in several different ways. Companies most commonly use Terrascan in automated pipelines to identify policy violations before they provision insecure infrastructure. For more information, see the [Terrascan documentation](#).

Note: Terrascan is not available for Raspberry Pi 4 versions of Nessus.

The **Terrascan > About** page allows you to install or uninstall the Terrascan executable in your Nessus instance. By default, Tenable Nessus does not have Terrascan installed.

The page also shows the following details for the Terrascan executable:

- Status (**Installed**, **Not Installed**, **Downloading**, or **Removing**)
- Version (for example, **1.13.2** or **N/A** if you have not installed Terrascan)
- Path (for example, **/opt/nessus/sbin/terrascan** or **N/A** if you have not installed Terrascan)

Note: The Terrascan feature is available in Nessus Professional, Tenable Nessus Expert, and Nessus Essentials for Nessus versions 10.1.2 and newer. You can only [create](#) and [launch](#) scans with Tenable Nessus Expert.

Note: When installed, Terrascan pulls policies from its GitHub repository, retrieves a scan target repository, and scans the scan target repository locally on the Nessus host. Running Terrascan causes the Nessus host to consume more CPU and network resources than normal Nessus scanning. For more information, see the [Terrascan documentation](#).

To install or uninstall Terrascan in your Nessus instance:

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **About** page appears.

2. Under **Terrascan Installation**, do one of the following:
 - Select the **Terrascan** check box to install Terrascan.
 - Deselect the **Terrascan** check box to uninstall Terrascan.
3. Click **Save**.



- If you selected the check box, Terrascan begins installing and the **Details for the Terrascan executable** pane updates the **Status** to **Downloading**.

Once you install Terrascan, Tenable Nessus updates the **Status** to **Installed** and shows the Terrascan executable's **Version** and file **Path**.

- If you deselected the check box, Terrascan begins uninstalling and the **Details for the Terrascan executable** pane updates the **Status** to **Removing**.

Once you uninstall Terrascan, Tenable Nessus updates the **Status** to **Not Installed** and removes the Terrascan executable's **Version** and file **Path**.

To update Terrascan in your Nessus instance:

Note: You can only update the Terrascan executable if you have already installed it.

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **Scans** page appears.

2. Click the **About** tab.

The **About** page appears.

3. In the top-right corner, click **Check for Updates**.

Note: The **Check for Updates** button is only available when you have Terrascan installed.

The **Download Terrascan** window appears.

4. Click **Continue**.

The window closes and the **Status** updates to **Downloading**.

Once the download completes, the **Status** updates to **Installed** and the **Details for the Terrascan executable** pane shows the Terrascan executable's new **Version**.

- [View Terrascan Violations](#)
- [Export a Summary of Violations](#)
- [View Terrascan Passed Rules](#)

Note: You need to have Terrascan version v1.15.1 IIRC installed for the **Scans** tab to appear.



Create a Terrascan Scan Configuration

Note: You can only create a Terrascan scan configuration in Tenable Nessus Expert. If you do not have Tenable Nessus Expert, you need to run the Terrascan executable from the command line interface (CLI) to gather scan results.

Tenable Nessus Expert allows you to create a Terrascan scan configuration, similar to other scan configurations in Nessus. However, you manage Terrascan scan configurations separately, under the **Terrascan** tab.

Before you begin:

- [Install Terrascan](#) on your Nessus instance.

To create a new scan configuration with Terrascan:

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **Scans** page appears.

2. In the upper-right corner, click the **New Scan** button.

The **New Terrascan Configuration** page appears.

3. Set up the new scan configuration:

Setting	Description
Configuration Name	The name of the Terrascan scan configuration.
Logging	
Command Output Format	Determines the output logging format (separate from the actual scan results). You can choose json or console .
Log Level	Determines the output verbosity level: <ul style="list-style-type: none">• info• debug



	<ul style="list-style-type: none">• warn• error• panic• fatal
Verbose Violations	Determines whether the scan logs violations with details.
Scanning	
IAC Type	Determines the Infrastructure as Code (IAC) type. <ul style="list-style-type: none">• all• arm• cft• docker• helm• k8s• kustomize• terraform• tfplan
Minimum Severity	Determines the minimum violation severity that Terrascan reports. You can choose low , medium , or high .
Non-recursive	Determines whether the scan recurses into subdirectories of the repository.
Output Format	Determines the scan result output format: <ul style="list-style-type: none">• human



	<ul style="list-style-type: none">• json• yaml• xml• junit-xml• sarif• github-sarif
Output Passed Rules	Determines whether the scan results show passed rules.
Policy Type	The policy type or types to include in the scan: <ul style="list-style-type: none">• all• aws• azure• docker• gcp• github• k8s
Remote Type	Determines the remote repository type: <ul style="list-style-type: none">• git• s3• gcs• http• terraform-registry <div style="border: 1px solid blue; padding: 5px;">Note: You need to make Git available on the Nessus host to select the</div>



	<input type="text" value="Git type."/>
Remote URL	The URL of the remote IAC registry.
Remote URL Branch	The branch of the remote IAC registry.

4. Click **Save**.

Tenable Nessus Expert saves the new scan configuration, and you can now select it from the **Terrascan > Scans** page.

What to do next:

- [Launch](#) a Terrascan scan.
- [Download](#) a Terrascan scan's results.
- [Manage](#) the Terrascan scan's histories and results.
- [Edit](#) a Terrascan scan configuration.
- [Delete](#) a Terrascan scan configuration.



Launch a Terrascan Scan

Note: You can only launch a Terrascan scan in Tenable Nessus Expert. If you do not have Tenable Nessus Expert, you need to run the Terrascan executable from the command line interface (CLI) to gather scan results.

Once you set up a Terrascan scan configuration, you can launch a scan from the Tenable Nessus Expert user interface.

Before you begin:

- [Install Terrascan](#) on your Nessus instance.

To launch a Terrascan scan:

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **Scans** page appears.

2. In the scan table, roll over the scan you want to edit.
3. In the scan row, click the ► button.

Nessus launches the scan. Once the scan completes, you can [download the scan results](#) from the scan's history page, view the scanned [violations](#) and [passed rules](#), or [export a summary of violations](#).



Download Terrascan Results

Once you complete a Terrascan scan in Nessus, you can download the scan results.

Note: If you complete a Terrascan scan while you have a Tenable Nessus Expert license and decide to downgrade from Tenable Nessus Expert, you can still download the scan's results. However, once you downgrade, you cannot launch any new Terrascan scans.

Before you begin:

- [Install Terrascan](#) on your Nessus instance.

To download Terrascan scan results:

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **Scans** page appears.

2. In the scan table, double-click the scan configuration.

The scan details page opens, and the **Violations** tab opens by default.

3. Click the **History** tab.

The scan history page appears.

4. In the scan history table under the **Results** column, click the output type to download the scan results as.

Note: You can download the results in JSON format and the output formats that you selected for the **Output Format** during the [scan configuration setup](#) process.

The scan results download to your machine in the output type that you selected.



Terrascan Scan History

The Terrascan user interface allows you to manage the Terrascan scan history in a few ways. You can use a scan's scan history page to launch the scan, edit the scan configuration, download scan results, download the command output of a scan, view the configuration used for a completed scan, and delete the scan's history and results.

Before you begin:

- [Install Terrascan](#) on your Nessus instance.

To navigate to the Terrascan scan history page:

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **Scans** page appears.

2. Click the row of the scan you want to view.

The scan details page appears, and the **Violations** tab opens by default.

3. Click the **History** tab.

The **History** page appears.

4. Do one of the following:

- [Launch](#) the scan.
- [Edit](#) the scan configuration.
- [Download](#) the scan results of a completed scan.
- [Export](#) the scan's summary of violations.

- **Download a scan's command output.**

a. Roll over the scan whose command output you want to download.

b. In the scan row, click the  button.

The command output downloads as a .txt file.



- **View the configuration used for a completed scan.**

- a. Roll over the scan whose command output you want to download.
- b. In the scan row, click the ⓘ button.

The **Config Details** window appears and shows the scan's configuration.

- **Delete a scan's history and results.**

- a. Roll over the scan whose history and results you want to delete.
- b. In the scan row, click the ✕ button.

The **Delete Result** window appears.

- c. Click **Delete**.

Nessus removes the scan history and related results from the scan history page.



View Terrascan Violations

Note: You can only launch a Terrascan scan in Tenable Nessus Expert. If you do not have Tenable Nessus Expert, you need to run the Terrascan executable from the command line interface (CLI) to gather scan results.

Once you [launch](#) a Terrascan scan and the scan completes, you can view the detected security violations in Tenable Nessus Expert. Violations represent all the scan policies that were checked and did not pass during the scan.

Before you begin:

- [Install Terrascan](#) on your Nessus instance.

To view Terrascan scan violations:

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **Scans** page appears.

2. Click the row of the scan you want to view.

The scan details page appears, and the **Violations** tab opens by default.

The **Violations** page shows the number of detected violations next to the tab header, the scan details, and a list of the found violations in a table.

Note: The tab header shows the number of unique violations, and the **Scan Details** section shows the number of total violations.

Tenable Nessus Expert shows the following information for each violation:

Column	Description
Severity	The severity level of the violation: <i>Low</i> , <i>Medium</i> , or <i>High</i> .
Category	The violation category: <ul style="list-style-type: none">• Compliance Validation• Configuration and Vulnerability Analysis• Data Protection



	<ul style="list-style-type: none">• Encryption and Key Management• Identity and Access Management• Infrastructure Security• Logging and Monitoring• Resilience• Security Best Practices
Description	The violation description.
Count	The number of times Terrascan detected the violation.



Export a Summary of Violations

Tenable Nessus Expert allows you to generate and export a summary of violations for a completed Terrascan scan as an HTML or PDF report.

Before you begin:

- [Install Terrascan](#) on your Nessus instance.

To generate and export a Terrascan summary of violations:

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **Scans** page appears.

2. Click the row of the scan that you want to generate a report for.

The scan details page appears, and the **Violations** tab opens by default.

3. In the upper-right corner, click the **Report** button.

The **Export Terrascan Results** window appears.

4. Choose the report format, **HTML** or **PDF**.

5. Choose the report template:

- **Summary of Violations** – Lists the detected violations by count.
- **Summary of Violations by File** – Lists the detected violations by file.

6. Click the **Generate Report** button.

Tenable Nessus Expert generates the report, and the report downloads to your machine.



View Terrascan Passed Rules

Note: You can only launch a Terrascan scan in Tenable Nessus Expert. If you do not have Tenable Nessus Expert, you need to run the Terrascan executable from the command line interface (CLI) to gather scan results.

Once you [launch](#) a Terrascan scan and the scan completes, you can view the detected passed rules in Tenable Nessus Expert. Passed rules represent all the scan policies that were checked and passed during the scan.

Before you begin:

- [Install Terrascan](#) on your Nessus instance.

To view Terrascan scan passed rules:

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **Scans** page appears.

2. Click the row of the scan you want to view.

The scan details page appears, and the **Violations** tab opens by default.

3. Click the **Passed Rules** tab.

The **Passed Rules** page opens.

The **Passed Rules** page shows the number of detected passed rules next to the tab header, the scan details, and a list of the found passed rules in a table.

Note: The tab header shows the number of unique passed rules, and the **Scan Details** section shows the number of total passed rules.

Tenable Nessus Expert shows the following information for each passed rule:

Column	Description
Severity	The severity level of the passed rule: Low, Medium, or High.
Category	The passed rule category: <ul style="list-style-type: none">• Compliance Validation



	<ul style="list-style-type: none">• Configuration and Vulnerability Analysis• Data Protection• Encryption and Key Management• Identity and Access Management• Infrastructure Security• Logging and Monitoring• Resilience• Security Best Practices
Description	The passed rule description.
Version	The scan policy version.



Edit a Terrascan Scan Configuration

Note: You can only edit a Terrascan scan configuration in Tenable Nessus Expert.

You can update the settings of a Terrascan scan configuration whenever you are not using it to perform a scan.


Before you begin:

- [Install Terrascan](#) on your Nessus instance.

To edit a Terrascan scan configuration:

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **Scans** page appears.

2. In the scan table, roll over the scan you want to edit.
3. In the scan row, click the  button.

The scan configuration page appears.

4. Edit the scan configuration settings:

Setting	Description
Configuration Name	The name of the Terrascan scan configuration.
Logging	
Command Output Format	Determines the output logging format (separate from the actual scan results). You can chose json or console .
Log Level	Determines the output verbosity level: <ul style="list-style-type: none">• info• debug• warn



	<ul style="list-style-type: none">• error• panic• fatal
Verbose Violations	Determines whether the scan logs violations with details.
Scanning	
IAC Type	Determines the Infrastructure as Code (IAC) type. <ul style="list-style-type: none">• all• arm• cft• docker• helm• k8s• kustomize• terraform• tfplan
Minimum Severity	Determines the minimum violation severity that Terrascan reports. You can choose low , medium , or high .
Non-recursive	Determines whether the scan recurses into subdirectories of the repository.
Output Format	Determines the scan result output format: <ul style="list-style-type: none">• human• json• yaml



	<ul style="list-style-type: none">• xml• junit-xml• sarif• github-sarif
Output Passed Rules	Determines whether the scan results show passed rules.
Policy Type	The policy type or types to include in the scan: <ul style="list-style-type: none">• all• aws• azure• docker• gcp• github• k8s
Remote Type	Determines the remote repository type: <ul style="list-style-type: none">• git• s3• gcs• http• terraform-registry <div style="border: 1px solid blue; padding: 5px;"><p>Note: You need to make Git available on the Nessus host to select the Git type.</p></div>
Remote URL	The URL of the remote IAC registry.
Remote URL	The branch of the remote IAC registry.



Branch

5. Click **Save**.

Tenable Nessus Expert saves the new configuration options.



Delete a Terrascan Scan Configuration

You can delete a scan configuration from the Nessus Terrascan user interface.

Note: If you create a Terrascan scan configuration while you have a Tenable Nessus Expert license and decide to downgrade from Tenable Nessus Expert, you can still delete the scan configuration after downgrading.

Before you begin:

- [Install Terrascan](#) on your Nessus instance.

To delete a Terrascan scan configuration:

1. Under **Resources** in the left-side navigation pane, click **Terrascan**.

The **Scans** page appears.

2. In the scan table, roll over the scan you want to edit.
3. In the scan row, click the **X** button.

The **Delete Configuration** window appears.

4. Click **Delete**.

Tenable Nessus deletes the scan configuration and removes it from the Terrascan scan table.



Sensors (Nessus Manager)

In Tenable Nessus Manager, you can manage linked agents and scanners from the **Sensors** page.

In the [Agents](#) section, you can do the following:

- [Modify Agent Settings](#)
- [Filter Agents](#)
- [Export Agents](#)
- [Download Linked Agent Logs](#)
- [Restart an Agent](#)
- [Unlink an Agent](#)
- [Delete an Agent](#)
- Manage [Agent Groups](#)
- Manage [Freeze Windows](#)
- Manage [Clustering](#)

In the [Scanners](#) section, you can do the following:

- [Link Nessus Scanner](#)
- [Unlink Nessus Scanner](#)
- [Enable or Disable a Scanner](#)
- [Remove a Scanner](#)
- [Download Managed Scanner Logs](#)



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 Nessus Agent version that Tenable Nessus Manager offers to its linked Tenable Nessus 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](#).



Modify Agent Settings

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	<p>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 <code>nessuscli</code> utility.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: This option does not allow the manager to track <i>deleted</i> agents. When you delete an agent, the manager and/or cluster no longer tracks or recognizes the agent.</p></div>
Unlink inactive agents after X days	<p>Specifies the number of days an agent can be inactive before the manager unlinks the agent.</p> <p>Inactive agents that were automatically unlinked by Tenable Nessus Manager automatically relink if they come back online.</p> <p>Requires that Track unlinked agents is enabled.</p>
Remove agents that have been inactive for X days	<p>Specifies the number of days an agent can be inactive before the manager removes the agent.</p>
Remove bad agents	<p>When this setting is enabled, agents with one or more of the following criteria are removed from Tenable Nessus Manager:</p> <ul style="list-style-type: none">• The agent was previously deleted or removed by a user.• The agent does not provide a valid access token.• The agent was blocklisted.



Option	Description
Freeze Windows	
	Configure global freeze windows as described in Modify Freeze Window Settings .



Remote Agent Settings

All agent advanced settings can be set via the agent's command line interface, as described in [Advanced Settings](#) in the *Tenable Nessus 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 com-	high	low, medium, or high



	<p>plete more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control in the <i>Tenable Nessus Agent Deployment and User Guide</i>.</p>		
Plugin Compilation Performance	<p>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 <i>Tenable Nessus Agent Deployment and User Guide</i>.</p>	high	low, medium, or high
Nessus Agent Log Level	<p>The logging level of the backend. <code>log log</code></p>	normal	<ul style="list-style-type: none">• normal - Changes the



	<p>file, as indicated by a set of log tags that determine what information to include in the log.</p> <p>If you manually edited <code>log.json</code> to set a custom set of log tags for <code>backend.log</code>, this setting overwrites that content.</p> <p>For more information, see log.json Format.</p>		<p><code>backend.log</code> logging level to normal and sets log tags to "log", "info", "warn", "error", "trace"</p> <ul style="list-style-type: none">• <code>debug</code> - Changes the <code>backend.log</code> logging level to debug and sets log tags to "log", "info", "warn", "error", "trace", "debug"• <code>verbose</code> - Changes the <code>backend.log</code> 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	<p>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 <i>Tenable Nessus Agent Deployment and User Guide</i>.</p>	high	low, medium, or high
Plugin Compilation Performance	<p>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 com-</p>	high	low, medium, or high



	<p>pilation completes more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control in the <i>Tenable Nessus Agent Deployment and User Guide</i>.</p>		
Nessus Agent Log Level	<p>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.</p> <p>If you manually edited log.json to set a custom set of log tags for backend.log, this setting overwrites that content.</p> <p>For more information, see log.json Format.</p>	normal	<ul style="list-style-type: none">• 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",



			<p>"debug"</p> <ul style="list-style-type: none">• 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.



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	earlier than later than	In the text box, type the date on which you want to filter.
Last Plugin Update	on	
Last Scanned	not on	



Parameter	Operator	Expression
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 is not equal to	In the drop-down list, select an agent status. For more information, see Agent Status in the <i>Tenable Nessus Agent Deployment and User Guide</i> .
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

To export agents data in 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 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 <code>unlinked</code> , <code>online</code> , or <code>offline</code> .
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

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

In Tenable Nessus, you can restart linked agents (versions 7.6 and later) 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

When you manually unlink an agent, the agent disappears from the **Agents** page, but the system retains related data for the period of time specified in [agent settings](#). When you manually unlink an agent, the agent does *not* automatically relink to Tenable Nessus Manager.

Tip: You can configure agents to automatically unlink if they are inactive for some days, as described in [agent settings](#).

To manually unlink agents in Tenable Nessus Manager:

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.

The manager unlinks the agent or agents.



Delete an Agent

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 Groups

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.

Tenable recommends that you size agent groups appropriately, particularly if you are managing scans in Nessus Manager and then importing the scan data into Tenable Security Center. You can size agent groups when you manage agents in 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 a New Agent Group](#)
- [Add Agents to an Agent Group](#)
- [Configure User Permissions for an Agent Group](#)
- [Modify an Agent Group](#)
- [Delete an Agent Group](#)



Create a New Agent Group

You can use agent groups to organize and manage the agents linked to your account. You can add an agent to more than one group, and configure scans to use these groups as targets.

Use this procedure to create an agent group in Tenable Nessus Manager.

To create a new 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. In the upper-right corner, click the **New Group** button.

The **New Agent Group** window appears.

4. In the **Name** box, type a name for the new agent group.

5. Click **Add**.

Tenable Nessus Manager adds the agent group and it appears in the table.

To create a new agent group in Tenable Nessus Manager 10.4 and later:

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 the **Add** button.

Tenable Nessus Manager creates the new agent group and adds the agents you selected to the new group.

What to do next:

- [Configure](#) user permissions for the agent group.
- [Use](#) the agent group in an agent scan configuration.



Configure User Permissions for an Agent Group

You can share an agent group with other users or user groups in your organization.

User permissions for agent groups include the following:

- **No access** – (Default user only) The user or user group cannot add the agent group to an agent scan. If a user or user group with this permission attempts to launch an existing scan that uses the agent group, the scan fails.
- **Can use** – The user or user group can add the agent group to an agent scan and can launch existing scans that use the agent group.

Use this procedure to configure permissions for an agent group in Tenable Nessus Manager.

To configure user permissions for an agent group:

1. [Create](#) or [modify](#) an agent group.
2. In the agent groups table, click the agent group for which you want to configure permissions.
The agent group details page appears.
3. Click the **Permissions** tab.
The **Permissions** tab appears.
4. 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.
5. Click **Save**.

Tenable Vulnerability Management saves the changes you made to the agent group.



Add Agents to an Agent Group

Tenable Nessus Manager allows you to add your linked agents to agent groups from the **Linked Agents** page.

Note: In addition to the following process, you can add agents to a group from the **Agent Groups** page. For more information, see [Create a New Agent Group](#).

To 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 the **Add** button.

Tenable Nessus Manager adds the selected agents to the agent group or groups.



Modify an Agent Group

Use this procedure to modify an agent group in Tenable Nessus Manager.

To 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 **X** 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.**

- a. In the agent groups table, click the agent group you want to modify.

The agent group details page appears.

- b. Click the **Permissions** tab.

The **Permissions** tab appears.

- c. [Configure](#) the user permissions for the group.



Delete an Agent Group

Use this procedure to delete an agent group in Tenable Nessus Manager.

To 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. In the row for the agent group that you want to delete, click the **X** button.

A confirmation window appears.

4. To confirm, click **Delete**.

The manager deletes the agent group.



Agent Updates

You can configure the Tenable Nessus Agent version that Tenable Nessus Manager offers to its linked Tenable Nessus Agents to update to from the **Agent Updates** page.

The **Agent Updates** page also allows you to manually update the offered Tenable Nessus Agent version directly from the Tenable Nessus feed and shows what Tenable Nessus 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 only affects Tenable Nessus Agent version updates, and does not affect plugin updates.

Note: The **Agent Updates** page is not available when Nessus is managed by Tenable Security Center or Tenable Nessus Manager.

To manage the agent update settings, use the following procedure:

- [Configure Agent Update Plan](#)
- [Configure the Offered Nessus Agent Version](#)



Configure Agent Update Plan

You can configure the Tenable Nessus Agent version that Tenable Nessus Manager offers to its linked Tenable Nessus 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 Nessus Agents to update to the latest generally available (GA) version automatically.
Early Access releases	Tenable Nessus Manager allows its Tenable Nessus Agents to update to the latest version automatically when it is released for Early Access (typically a few weeks before GA).
Stable releases	Tenable Nessus 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 Nessus Agents.
4. Click **Save**.

After saving, you might want to update the Tenable Nessus Agent version that Tenable Nessus Manager offers from the Tenable Nessus feed. For more information, see [Configure the Offered Nessus Agent Version](#).



Configure the Offered Nessus Agent Version

The **Automatic Updates** setting allows Tenable Nessus Manager can automatically update the Tenable Nessus 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 Nessus Agent version manually.

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. Select or clear the **Enable Agent Updates** checkbox.
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 Nessus Agent version that Tenable Nessus Manager offers manually.

To update the offered Tenable Nessus 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 Nessus 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 Nessus 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 Nessus Agents from the Nessus feed.



Freeze Windows

Freeze windows allow you to schedule times when 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

To manage freeze windows, use the following procedures:

- [Create a Freeze Window](#)
- [Modify a Freeze Window](#)
- [Delete a Freeze Window](#)
- [Modify Global Freeze Window Settings](#)



Create a Freeze Window

Freeze windows allow you to schedule times where certain agent activities are suspended for all linked agents. This activity includes:

- Receiving and applying software updates
- Receiving plugin updates
- Installing or executing agent scans

To create a freeze window for linked agents:

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 options as necessary.

5. Click **Save**.

The freeze window goes into effect and appears on the **Freeze Windows** tab.



Modify a Freeze Window

Use this procedure to modify a freeze window in Tenable Nessus Manager.

To configure global freeze window settings, see [Agent Settings](#) .

To 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.

5. Click **Save** to save your changes.



Delete a Freeze Window

Use this procedure to delete a freeze window in Tenable Nessus Manager.

To delete a freeze window for linked agents:

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 **X** 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	<p>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.</p> <div style="border: 1px solid #0070C0; padding: 5px;"><p>Note: Disabling this setting is the only way to end the permanent freeze window.</p></div> <p>The following freeze window settings also apply during the permanent freeze window.</p>
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, 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 Nessus 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 Nessus version. Otherwise, the cluster deployment is unsupported.

Parent Node (Tenable Nessus Manager with clustering enabled)

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.

- **Disk:** Estimated minimum of 5 GB per 5000 agents per scan per day
- **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

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:

- **Disk:** Estimated minimum of 5 GB per 5000 agents per concurrent scan.
- **CPU:** 4 cores
- **RAM:** 16 GB

Child node with 10,000-20,000 agents:



A child node can support a maximum of 20,000 agents.

- **Disk:** Estimated minimum of 5 GB per 5000 agents per concurrent scan.
- **CPU:** 8 cores
- **RAM:** 32 GB

Agents

- Linked agents must be on a [supported Nessus Agent version](#).



Enable Clustering

When you enable clustering on Tenable Nessus Manager it becomes a *parent node*. You can then link *child nodes*, each of which manages Tenable Nessus 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 Nessus 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 Nessus 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

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 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 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 check box to migrate agents to the cluster. Disable the check box 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 Nessus Agents.



Link Agents to a Cluster

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 Nessus 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=00abcd00000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00
--name=LinuxAgent --groups=All --host=yourcompany.com --port=8834
```

macOS:

```
# /Library/NessusAgent/run/sbin/nessuscli agent link
--key=00abcd00000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00
--name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
```



Windows:

```
# C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
--key=00abcd0000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00
--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 Nessus 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=00abcd0000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00
--name=LinuxAgent --groups=All --host=yourcompany.com --port=8834
```

macOS:

```
# /Library/NessusAgent/run/sbin/nessuscli agent link
--key=00abcd0000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00
--name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
```

Windows:

```
# C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
--key=00abcd0000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00
```



```
--name=WindowsAgent --groups=All --host=yourcompany.com --port=8834
```

To view a list of the supported agent-linking arguments, see [Nessus CLI Agent Commands](#)



Manage Nodes

To manage cluster nodes, see the following:

- [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

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

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: 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:

- [Get the linking key](#) from the cluster parent node.

To install and configure Tenable Nessus as a child node:

1. Install Tenable Nessus as described in the appropriate [Install 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 Nessus Agents should use to access the child node. If you do not provide a host node, Tenable Nessus Agent uses the system hostname. If Tenable Nessus 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 check box 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.

What to do next:



- Log in to the Tenable Nessus Manager parent node to manage linked Tenable Nessus 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

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.

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 10000 and the maximum value is 20000.

9. Click **Save**.

Tenable Nessus Manager updates the node settings.



Enable or Disable a Node

If you disable a child node, its linked Tenable Nessus Agents relink to another available child node in the same cluster group. If you re-enable a child node, Tenable Nessus 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

Tenable Nessus 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 Nessus Agents get redistributed more evenly across child nodes within a cluster group. Tenable Nessus 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 Nessus Agent distribution across child nodes.



Delete a Node

When you delete a child node, linked Tenable Nessus 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

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](#)
- [Modify a Cluster Group](#)
- [Add a Node to a Cluster Group](#)
- [Add an Agent to a Cluster Group](#)
- [Move a Node to a Cluster Group](#)
- [Move an Agent to a Cluster Group](#)
- [Delete a Cluster Group](#)



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.

What to do next:

- [Add a Node to a Cluster Group](#)
- [Add an Agent to a Cluster Group](#)



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, first [Create a Cluster Group](#).

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.

What to do next:

- [Add an Agent to a 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, as described in [Add a Node to a Cluster Group](#).

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 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, as described in [Add a Node to a Cluster Group](#).

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.



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, first [Create a Cluster Group](#).

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.



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.



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. To change the default cluster group, see [Modify a Cluster Group](#).

Before you begin:

- Move assigned agents to a different cluster group, as described in [Move an Agent to a Cluster Group](#).
- [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 **X** 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](#)



Link Nessus Scanner

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

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



A standard user or administrator in Tenable Nessus Manager can perform this procedure.

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

An administrator can perform the following procedure 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 **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 **X** 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

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 Nessus 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:



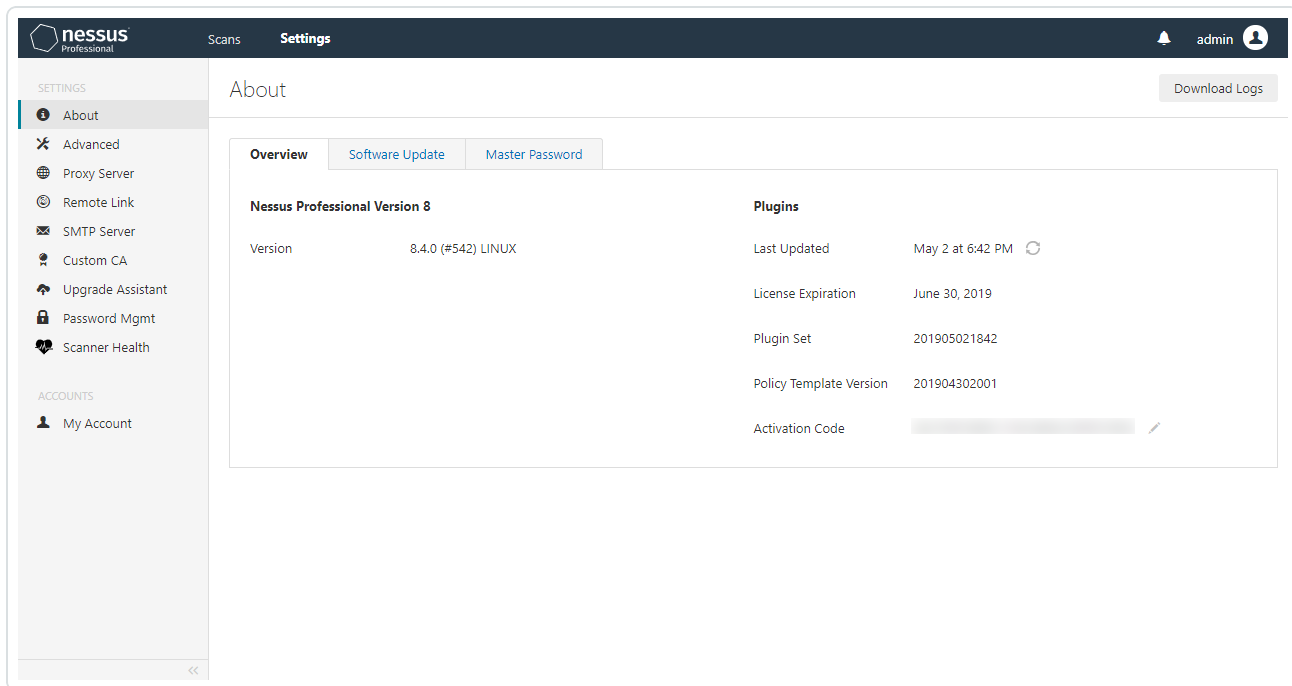
- In the row of the log you want to remove, click the  button.

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

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 **Encryption Password** tab, you can [set an encryption password](#).

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.
Last Updated	The date on which the plugin set was last refreshed.
Expiration	The date on which your license age outs. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">Note: For Tenable Nessus Professional 8.5 and later, 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.</div>
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.



Value	Description
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.
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

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 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 Nessus web server log records, system log data, and network configuration information.

For information on managing individual 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**.

Nessus generates the file *nessus-bug-report-XXXXX.tar.gz*, which downloads and appears in your browser window.



Set an Encryption Password

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.




Advanced Settings

The **Advanced Settings** page allows you to configure Nessus manually. You can configure advanced settings from the Tenable Nessus user interface, or from the command-line interface. 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 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  icon.
- Custom policy settings supersede the global advanced settings.

User Interface



Setting	Identifier	Description	Default	Valid Values
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
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
Disable Frontend	disable_frontend	Disables the Tenable Nessus user interface. Users can still use the API.	no	yes or no
Disable Tenable News	disable_rss	In Tenable Nessus Essentials or Tenable Nessus Professional trial, the left navigation bar shows a Tenable news widget. Use this setting to disable the widget.	no	yes or no
Disable UI	disable_ui	Disables the user interface on managed scanners.	no	yes or no
Login Banner	login_banner	A text banner that appears after you attempt to log in to	None	String



Setting	Identifier	Description	Default	Valid Values
		Nessus. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">Note: The banner only appears the first time you log in on a new browser or computer.</div>		
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.
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 connections only.	0.0.0.0	String in the format of an IP address
Nessus Web Server Port	xmlrpc_listen_port	The port that the Nessus web server listens on.	8834	Integers
UI Theme	ui_theme	When enabled, changes user interface color theme to dark mode.	Track Os Setting	Light, Dark, or Track Os Setting
Use Mixed Vulnerability Groups	scan_vulnerability_groups_mixed	When enabled, Nessus shows the severity level as Mixed for vulnerability groups,	yes	Yes or No



Setting	Identifier	Description	Default	Valid Values
		unless all the vulnerabilities in a group have the same severity. When disabled, Nessus shows the highest severity indicator of a vulnerability in a group		
Use Vulnerability Groups	scan_vulnerability_groups	When enabled, Tenable Nessus groups vulnerabilities in scan results by common attributes, giving you a shorter list of results.	yes	yes or no

Scanning

Setting	Identifier	Description	Default	Valid Values
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
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



Setting	Identifier	Description	Default	Valid Values
CGI Paths for Web Scans	cgi_path	A colon-delimited list of CGI paths to use for web server scans.	/cgi-bin:/scripts	String
Engine Thread Idle Time	engine.idle_wait	Number of seconds a scan engine remains idle before shutting itself down.	60	Integers 0-600
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.
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
Maximum Ports Reported by Portscanner Plugins	portscanner.max_ports	The maximum number of ports that the 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
Maximum	attached_	Specifies the maximum size, in MB, of any	25	Intege-



Setting	Identifier	Description	Default	Valid Values
Size for E-mailed Reports	report_maximum_size	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.		rs 0-50
Nessus Rules File Location	rules	<p>Location of the Nessus rules file (nessusd.rules).</p> <p>The following are the defaults for each operating system:</p> <p>Linux:</p> <pre>/opt/nessus/etc/nessus/nessusd.rules</pre> <p>macOS:</p> <pre>/Library/Nessus/run/var/nessus/conf/nessusd.rules</pre> <p>Windows:</p> <pre>C:\ProgramData\Tenable\Nessus\nessus\conf\nessusd.rules</pre>	<i>Nessus config directory for your operating system</i>	String
Non-Simultaneous Ports	non_simult_ports	Specifies ports against which two plugins you cannot run simultaneously.	139, 445, 3389	String
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



Setting	Identifier	Description	Default	Valid Values
PCAP Snapshot Length	pcap.snapshot	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 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.	0	Integers 0-262144
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



Setting	Identifier	Description	Default	Valid Values
				and TCP ports by prefixing each range by T: or U:.
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 host-name or IP address.	no	yes or no
Safe Checks	safe_checks	When enabled, Nessus uses safe checks, which use banner grabbing rather than active testing for a vulnerability.	yes	yes or 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, Nessus runs those plugin dependencies, but does not include their output in the report. When disabled, Nessus includes both the selected plugin and any plugin dependencies in the report.	yes	yes or no
Slice Network Addresses	slice_network_addresses	If you set this option, 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	no	yes or no



Setting	Identifier	Description	Default	Valid Values
s		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).		
System Default Severity Basis	severity_basis	<p>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.</p> <p>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.</p> <p>For more information about CVSS scores and severity ranges, see CVSS Scores vs. VPR.</p> <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p>Note: This setting is not available for Tenable Nessus Manager.</p> </div>	<p>On a new installation of Tenable Nessus : cvss_v3</p> <p>On preexisting upgraded instance: cvss_v2</p>	cvss_v2 or cvss_v3

Logging

Setting	Identifier	Description	Default	Valid Values
Log Additional Scan	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	no	yes or no



Setting	Identifier	Description	Default	Valid Values
Details		also enable <code>log_whole_attack</code> .		
Log Verbose Scan Details	<code>log_whole_attack</code>	Logs verbose details of the scan. Helpful for debugging issues with the scan, but this may be disk intensive. To add more details, enable <code>log_details</code> .	no	yes or no
Nessus Dump File Location	<code>dumpfile</code>	Location of <code>nessusd.dump</code> , a log file for debugging output if generated. The following are the defaults for each operating system: Linux: <code>/opt/nessus/var/nessus/logs/nessusd.dump</code> macOS: <code>/Library/Nessus/run/var/nessus/logs/nessusd.dump</code> Windows: <code>C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.dump</code>	<i>Nessus log directory for your operating system</i>	String
Nessus Dump File Log Level	<code>nasl_log_type</code>	The type of NASL engine output in <code>nessusd.dump</code> .	normal	normal, none, trace, or full.
Nessus Dump File Max	<code>dumpfile_max_files</code>	The maximum number of the <code>nessusd.dump</code> files kept on disk. If the number exceeds the specified value, Tenable Nessus deletes the	100	Integers 1-1000



Setting	Identifier	Description	Default	Valid Values
Files		oldest dump file.		
Nessus Dump File Max Size	dumpfile_max_size	The maximum size of the <code>nessusd.dump</code> files in MB. If file size exceeds the maximum size, Tenable Nessus creates a new dump file.	512	Integers 1-2048
Nessus Dump File Rotation Time	dumpfile_rotation_time	Determines how often Nessus dump files are rotated in days.	1	Integers 1-365
Nessus Dump File Rotation	dumpfile_rot	Determines whether Nessus rotates dump files based on maximum rotation size or rotation time.	size	size— Nessus rotates dump files based on size, as specified in <code>dumpfile_max_size</code> . time— Nessus rotates dump files based on



Setting	Identifier	Description	Default	Valid Values
				time, as specified in <code>dump-file-rotation-time</code> .
Nessus Log Level	<code>backend_log_level</code>	<p>The logging level of the <code>backend.log</code> log file, as indicated by a set of log tags that determine what information to include in the log.</p> <p>If you manually edited <code>log.json</code> to set a custom set of log tags for <code>backend.log</code>, this setting overwrites that content.</p> <p>For more information, see log.json Format.</p>	normal	<ul style="list-style-type: none">normalsets log tags tolog, info, warn, error, tracedebugset-



Setting	Identifier	Description	Default	Valid Values
				s log tag- s to lo- g, inf- o, war- n, err- or, tra- ce, deb- ug • ver- bos- e – set- s log tag- s to lo- g, inf- o, war- n, err-



Setting	Identifier	Description	Default	Valid Values
				or, trace, debug, verbose
Nessus Scanner Log Location	logfile	<p>Location where Tenable Nessus stores its scanner log file.</p> <p>The following are the defaults for each operating system:</p> <p>Linux:</p> <pre>/opt/nessus/var/nessus/logs/nessusd.messages</pre> <p>macOS:</p> <pre>/Library/Nessus/run/var/nessus/logs/nessusd.messages</pre> <p>Windows:</p> <pre>C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.messages</pre>	<i>Nessus log directory for your operating system</i>	String
Log File Maximum	logfile_max_files	Determines the maximum number of Nessus log files.	Integers 1-1000	Nessus-100



Setting	Identifier	Description	Default	Valid Values
Files				Nessus Agent-2
Log File Maximum Size	logfile_max_size	Determines the maximum Nessus log file size in MB.	Integers 1-2048	Nessus-512 Nessus Agent-10
Log File Rotation Time	logfile_rotation_time	Determines how often Nessus dump files are rotated in days.	1	Integers 1-365
Log File Rotation	logfile_rot	Determines whether Nessus rotates log files based on maximum rotation size or rotation time.	size	size- Nessus rotates log files based on size, as specified in logfile_max_size. time- Nessus rotates log files based on time, as specified in log-



Setting	Identifier	Description	Default	Valid Values
				file_rotation_time.
Scanner Metric Logging	scanner-metrics	Enables scanner performance metrics data gathering.	0	0 (off), 0x3f (full data except plugin metrics), 0x7f (full data including plugin metrics) Note: Including plugin metrics greatly increases the size of the log file. Tenable Nessus



Setting	Identifier	Description	Default	Valid Values
				does not automatically clean up log files.
Use Milliseconds in Logs	logfile_msec	When enabled, <code>nessusd.messages</code> and <code>nessusd.dump</code> log timestamps are in milliseconds. When disabled, log timestamps are in seconds.	no	yes or no

Performance

Setting	Identifier	Description	Default	Valid Values
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	NORMAL	NORMAL or FULL



Setting	Identifier	Description	Default	Valid Values
		cost.		
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
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
Global Max Port Scanners	global.max_ports-scanners	Maximum number of port scanners.	100	Integers 0-1024
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	Integers



Setting	Identifier	Description	Default	Valid Values
			example, Windows Server 2016).	
Max Concurrent Checks Per Host	max_checks	Maximum number of simultaneous plugins that can run concurrently on each host.	5	Integers
Max Concurrent Hosts Per Scan	max_hosts	Maximum number of hosts checked at one time during a scan.	Varies, up to 100.	Integers. If set to 0, defaults to 100.
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.
Max Engine Checks	engine.max_checks	Maximum number of simultaneous plugins that can run concurrently on a single scan engine.	64	Integers
Max Engine Threads	engine.max	Maximum number of scan engines that run in parallel. Each scan engine	8 times the number of CPU cores on	Integers



Setting	Identifier	Description	Default	Valid Values
		scans multiple targets concurrently from one or more scans (see <code>engine.max_hosts</code>).	the machine	
Max Hosts Per Engine Thread	<code>engine.max_hosts</code>	Maximum number of targets that run concurrently on a single scan engine.	16	Integers
Max HTTP Connections	<code>max_http_connections</code>	The number of simultaneous connection attempts before the web server responds with HTTP code 503 (Service Unavailable, Too Many Connections).	600	Integers
Max HTTP Connections Hard	<code>max_http_connections_hard</code>	The number of simultaneous connection attempts before the web server does not allow further connections.	3000	Integers
Max TCP Sessions Per Host	<code>host.max_simult_tcp_sessions</code>	Maximum number of simultaneous TCP sessions for a	0	Integers. If set to 0,



Setting	Identifier	Description	Default	Valid Values
		<p>single host.</p> <p>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.</p>		<p>there is no limit.</p>
Max TCP Sessions Per Scan	max_simult_tcp_sessions	Maximum number of simultaneous TCP sessions for the entire scan, regardless of the number of hosts the scanner is scanning.	0	<p>Integers 0-2000.</p> <p>If set to 0, there is no limit.</p>
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 asyn-	2	<p>Integers 0-100</p>



Setting	Identifier	Description	Default	Valid Values
		chronous tasks to these threads, and this value controls the maximum number of threads.		
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
Minimum Engine Threads	engine.min	The number of scan engines that start initially as Tenable Nessus scans the targets. After the engine reaches <code>engine.-optimal_hosts</code> number of targets, Nessus adds more scan engines up to <code>engine.max</code> .	2 times the number of CPU cores on the machine	Integers
Optional Hosts Per Engine Thread	engine.optimal_hosts	The minimum number of targets that	2	Integers



Setting	Identifier	Description	Default	Valid Values
		are running on each scan engine before Tenable Nessus adds more engines (up to <code>engine.max</code>).		
Optimize Tests	<code>optimize_test</code>	Optimizes the test procedure. If you disable this setting, scans may take longer and typically generate more false positives.	yes	yes or no
Plugin Check Optimization Level	<code>optimization_level</code>	Determines the type of check that Tenable Nessus performs before a plugin runs. If you set this setting to <code>open_ports</code> , then Tenable Nessus checks that required ports are open; if they are not, the plugin does not run. If you set this set-	None	<code>open_ports</code> or <code>required_keys</code>



Setting	Identifier	Description	Default	Valid Values
		ting to 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
QDB Memory Usage	qdb_mem_usage	Directs Nessus to use more or less memory when idle. If Nessus is running on a dedicated server, setting this to high uses more memory to increase performance. If Nessus is running on a shared machine, setting this to low uses considerably less memory, but has a moderate performance	low	low or high



Setting	Identifier	Description	Default	Valid Values
		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
Remediations Limit	remediations_limit	Limits the number of remediations that Tenable Nessus generates and shows in a scan result.	500	Integers > 0
Scan Check Read Timeout	checks_read_timeout	Read timeout for the sockets of the tests.	5	Integers 0-1000
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
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



Setting	Identifier	Description	Default	Valid Values
Webserver Thread Pool Minimum Size	www.thread_pool.min	The minimum thread pool size for the web-server/backend.	2	Integers 0-100
Webserver Thread Pool Maximum Size	www.thread_pool.max	The maximum thread pool size for the web-server/backend.	200	Integers 0-500

Security

Setting	Identifier	Description	Default	Valid Values
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
Cipher Files on Disk	cipher_files_on_disk	Encipher files that Nessus writes.	yes	yes or no
Force Public Key Authentication	force_public_key_auth	Force logins for Nessus to use public key authentication.	no	yes or no
Max Concurrent Sessions	max_sessions_per_	Maximum concurrent ses-	0	Integers 0-2000.



Setting	Identifier	Description	Default	Valid Values
sions Per User	user	sions per user		If set to 0, there is no limit.
SSL Cipher List	ssl_cipher_list	Cipher list to use for Nessus backend connections. You can use a pre-configured list of cipher strings, or enter a custom cipher list or cipher strings.	compatible	<ul style="list-style-type: none">• 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 custom OpenSSL cipher list. For more information



Setting	Identifier	Description	Default	Valid Values
				<p>on valid cipher list formats, see the OpenSSL documentation.</p> <ul style="list-style-type: none">• <code>niap</code> - A list of ciphers that conforms to NIAP standards. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><pre>ECDHE-RSA-AES128-SHA256:ECDH-E-RSA-AES128-GCM-SHA256:ECDH-E-RSA-AES256-SHA384:ECDH-E-RSA-AES256-GCM-SHA384</pre></div>
SSL Mode	<code>ssl_mode</code>	Minimum supported version of TLS.	<code>tls_1_2</code>	<ul style="list-style-type: none">• <code>compat</code> - TLS v1.0+• <code>ssl_3_0</code> - SSL v3+• <code>tls_1_1</code> - TLS v1.1+• <code>tls_1_2</code> - TLS v1.2+• <code>niap</code> - TLS v1.2

Agents & Scanners



Note: The following settings are only available in Tenable Nessus Manager.

Name	Setting	Description	Default	Valid Values
Agent Auto Delete	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
Agent Auto Delete Threshold	agent_auto_delete_threshold	The number of days after which inactive agents are automatically deleted if agent_auto_delete is set to yes.	30	Integers 1-365
Agent Auto Unlink	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



Name	Setting	Description	Default	Valid Values
Agent Auto Unlink Threshold	agent_auto_unlink_threshold	<p>The number of days after which inactive agents are automatically unlinked if agent_auto_unlink is set to yes.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: This value must be less than the agent_auto_delete_threshold.</p></div>	30	Integers 30-90
Agents Progress	agents_progress_viewable	<p>When a scan gathers information from agents, Tenable Nessus Manager does not show detailed agents information if the number of agents exceeds this setting. Instead, a message indicates that results are being gathered and will be viewable when the</p>	100	Integers. If set to 0, this defaults to 100.



Name	Setting	Description	Default	Valid Values
		scan is complete.		
Automatically Download Agent Updates	agent_updates_from_feed	When enabled, new Tenable Nessus Agent software updates are automatically downloaded.	yes	yes or no
Concurrent Agent Software Updates	cloud.manage.download_max	The maximum concurrent agent update downloads.	10	Integers
Include Audit Trail Data	agent_merge_audit_trail	<p>Controls whether or not agent scan result audit trail data is included in the main agent database. Excluding audit trail data can significantly improve agent result processing performance.</p> <p>If this setting is set to false, the Audit Trail Verbosity setting in an individual scan or policy</p>	false	true or false



Name	Setting	Description	Default	Valid Values
		defaults to No audit trail.		
Include KB Data	agent_merge_kb	<p>Includes the agent scan result KB data in the main agent database. Excluding KB data can significantly improve agent result processing performance.</p> <p>If this setting is set to false, the Include the KB setting in an individual scan or policy defaults to Exclude KB.</p>	false	true or false
Result Processing Journal Mode	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	DELETE	MEMORY TRUNCATE DELETE



Name	Setting	Description	Default	Valid Values
		also introduces a small risk of a corrupted scan result in the event of a crash. For more details, refer to the sqlite3 documentation .		
Result Processing Sync Mode	agent_merge_synchronous_setting	Sets the filesystem sync mode to use when processing agent results. Turning this off will significantly improve processing performance, but also introduces a small risk of a corrupted scan result in the event of a crash. For more details, refer to the sqlite3 documentation .	FULL	OFF NORMAL FULL
Track Unique Agents	track_unique_agents	When enabled, Tenable Nessus	no	yes or no



Name	Setting	Description	Default	Valid Values
		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.		

Cluster

Note: The following settings are only available in Tenable Nessus Manager with clustering enabled.

Setting	Identifier	Description	Default	Valid Values
Agent Blacklist Duration Days	agent_blacklist_duration_days	<p>The number of days that an agent remains blocked from relinking to a cluster node.</p> <p>For example, Tenable Nessus blocks an agent if it tries to link with a UUID that matches an existing agent in a cluster.</p> <p>Note: Tenable Nessus</p>	7	Integers > 0



Setting	Identifier	Description	Default	Valid Values
		<div style="border: 1px solid blue; padding: 5px;">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.</div>		
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_maximum_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	Identifier	Description	Default	Valid Values
Allow Special Characters in User Names	allow_special_chars_in_username	Determines whether Tenable Nessus usernames can include parentheses: (and).	true	true or false
Automatic Update	auto_update_	Number of hours that Tenable Nessus waits between automatic updates.	24	Integers > 0



Setting	Identifier	Description	Default	Valid Values
Delay	delay			
Automatic Updates	auto_update	<p>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.</p> <div style="border: 1px solid blue; padding: 5px;"><p>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.</p></div>	yes	yes or no
Automatically Update Nessus	auto_update_ui	<p>Automatically download and apply Nessus updates.</p> <div style="border: 1px solid blue; padding: 5px;"><p>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.</p></div>	yes	yes or no
Backups to keep	backup_days_to_keep	Nessus automatically creates a backup file every 24 hours. Use this setting to determine how many days Nessus keeps the backup files before discarding them.	30	Integers > 0



Setting	Identifier	Description	Default	Valid Values
		<p>For example, if you keep this setting at the default 30 days, Nessus stores daily backup files for the past 30 days.</p> <p>For more information about Nessus backup files, see Back Up Nessus.</p>		
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
Initial Sleep Time	ms_agent_sleep	(Tenable Nessus Manager only) Sleep time between managed scanner and agent requests. You can override this setting in Nessus Manager or Tenable.io.	30	Integers 5-3300
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
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
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: <i>port</i> or <i>localhost:port</i> or



Setting	Identifier	Description	Default	Valid Values
				<i>ip:port</i>
Nessus Preferences Database	config_file	<p>Location of the configuration file that contains the engine preference settings.</p> <p>The following are the defaults for each operating system:</p> <p>Linux:</p> <p><code>/opt/nessus/etc/nessus/nessusd.db</code></p> <p>macOS:</p> <p><code>/Library/Nessus/run/etc/nessus/conf/nessusd.db</code></p> <p>Windows:</p> <p><code>C:\ProgramData\Tenable\Nessus\conf\nessusd.db</code></p>	<i>Nessus database directory for your operating system</i>	String
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
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
Orphaned Scan His-	orphaned_scan_	The number of days after which Tenable	30	Integers > 0



Setting	Identifier	Description	Default	Valid Values
tory Cleanup	cleanup_days	Nessus removes orphaned scans. For example, an 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.		
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
Plugin Integrity Check Frequency (Minutes)	plugin_healthcheck_frequency	Determines the frequency, in minutes, at which Nessus runs a full plugin integrity check.	10080	Integers 1440-10080
Remote Scanner Port	remote_listen_port	This setting allows Nessus to 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 <code>xmlrpc_listen_port</code> (default 8834).	None	Integer
Report Crashes to Tenable	report_crashes	When enabled, Nessus sends crash information to Tenable, Inc. automatically to identify problems. Tenable	yes	yes or no



Setting	Identifier	Description	Default	Valid Values
		Nessus does not send personal or system-identifying information to Tenable, Inc..		
Scan Source IP (s)	source_ip	Source IPs to use when running on a multi-homed host. If you provide multiple IPs, Nessus cycles through them whenever it performs a new connection.	None	IP address or comma-separated list of IP addresses.
Send Telemetry	send_telemetry	<p>When enabled, Nessus periodically and securely sends non-confidential product usage data to Tenable.</p> <p>Usage statistics include, but are not limited to, data about your visited pages within the Tenable Nessus interface, your 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.</p>	yes	yes or no
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.	0	0 or integers larger than or equal to 3. If set to 0,



Setting	Identifier	Description	Default	Valid Values
				Tenable Nessus retains the history.
Windows Minidump	windows_minidump	Determines whether Nessus generates a Windows minidump file in the log folder if Nessus for Windows crashes.	no	yes or 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.

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 Nessus user interface, and turns on last successful and failed login notification.	None	UNCLASSIFIED (green banner), CONFIDENTIAL (blue banner), SECRET (red banner), or a custom value (orange banner).
multi_scan_same_host	When disabled, to avoid overwhelming a host, Tenable.io prevents a single scanner from simultaneously scanning multiple	no	yes or no



Identifier	Description	Default	Valid Values
	<p>targets that resolve to a single IP address. Instead, Tenable.io 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.</p> <p>When enabled, a Tenable.io 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.</p>		
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 Tenable Security Center.	no	yes or no
nessus_syn_scanner.global_throughput.max	Sets the max number of SYN packets that Nessus sends per second during its port scan (no matter how many hosts Tenable Nessus scans in parallel). Adjust	65536	Integers



Identifier	Description	Default	Valid Values
	this setting based on the sensitivity of the remote device to large numbers of SYN packets.		
login_banner	A text banner shows that appears after you attempt to log in to 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 <code>plugins_timeout</code> .	None	Integers 0-86400



Create a New Setting

1. In 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 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 **X** button.

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

4. Click **Delete**.


Tenable Nessus deletes the setting.



LDAP Server (Nessus Manager)

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.

LDAP Server



The Lightweight Directory Access Protocol (LDAP) is an industry standard for accessing and maintaining directory services across an organization. Once connected to an LDAP server, administrators can add users straight from their directory and these users can authenticate using their directory credentials.

Host	<input type="text"/>
Port	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
Base DN	<input type="text" value="cn=users,dc=example,dc=com"/>

Show advanced settings

The following table describes the **LDAP Server** fields:

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	<p>The attribute name on the LDAP server that contains the username for the account. This is often specified by the string <code>sAMAccountName</code> in servers that may be used by LDAP.</p> <p>Contact your LDAP server administrator for the correct value.</p>
Email Attribute	<p>The attribute name on the LDAP server that contains the email address for the account. This is often specified by the string <code>mail</code> in servers that may be used by LDAP.</p> <p>Contact your LDAP server administrator for the correct value.</p>
Name Attribute	<p>The attribute name on the LDAP server that contains the name associated with the account. This is often specified by the string <code>CN</code> in servers that may be used by LDAP.</p> <p>Contact your LDAP server administrator for the correct value.</p>
CA (PEM Format)	The LDAP server's certificate authority (CA) certificate, if applicable. Enter the certificate in PEM format.



Configure an LDAP Server

1. In 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 <code>sAMAccountName</code> 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 <code>mail</code> 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 <code>CN</code> 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.


Nessus Manager saves the LDAP server configuration.



Proxy Server

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, see [Configure a Proxy Server](#).

Proxy Server



Proxy servers are used to forward HTTP requests. If your organization requires one, Nessus will use these settings to perform plugin updates and communicate with remote scanners and agents. Only the host and port fields are required. Username, password, authentication type and user-agent are available if needed.

Host	<input type="text"/>
Port	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
Auth Method	AUTO DETECT ▼
User-Agent	<input type="text"/>

The following table describes the **Proxy Server** settings:

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	<p>The authentication method Nessus uses to connect to the proxy server:</p> <ul style="list-style-type: none">• 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.
User-Agent	The user agent for the proxy server, if your proxy requires a preset user agent.



Configure a Proxy Server

1. In 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: <ul style="list-style-type: none">• 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.



User-Agent	The user agent for the proxy server, if your proxy requires a preset user agent.
------------	--

4. Click the **Save** button.

Nessus saves the proxy server.




Remote Link

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.

Remote Link



By enabling this setting, you can link this scanner to Tenable.io or a Nessus Manager. From there, it can be fully managed and selected when configuring or launching scans. Please note that this scanner can only be linked to one manager at a time.

ON

Link to

Scanner Name

Linking Key

Use Proxy

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	



Option	Set To
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.
Use Proxy	Select or deselect the check box depending on your proxy settings. If you select Use Proxy , you must also configure: <ul style="list-style-type: none">• 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: <code>2d38435603c5b59a4526d39640655c3288b00324097a08f7a93e5480940d1cae</code>
Use Proxy	Select or deselect the check box depending on your proxy settings. If you select Use Proxy , you must also configure: <ul style="list-style-type: none">• Host – The hostname or IP address of the proxy server.




Option	Set To
	<ul style="list-style-type: none">• 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

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.

SMTP Server

 Simple Mail Transfer Protocol (SMTP) is an industry standard for sending and receiving email. Once configured for SMTP, scan results will be emailed to the list of recipients specified in a scan's "Email Notifications" configuration. These results can be custom tailored through filters and require an HTML compatible email client.

Host

Port

From (sender email)

Encryption

Hostname (for email links)

Auth Method

The following table describes the **SMTP Server** settings:

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: <ul style="list-style-type: none">• No Encryption – Tenable Nessus does not encrypt the email.



	<ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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.



Configure an SMTP Server

1. In 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: <ul style="list-style-type: none">• 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 SMTP server: <ul style="list-style-type: none">• 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.


Nessus saves the SMTP server.



Custom CA

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](#).

Custom CA



Saving a Custom Certificate Authority (CA) helps to mitigate findings from Plugin #51192 (SSL Certificate Cannot Be Trusted) during scans.

Certificate

```
-----BEGIN CERTIFICATE-----
MIIEczCCA1ugAwIBAgIBADANBgkqhkiG9w0BAQQFAD..AkGAlUEBhMCR0Ix
EzARBgNVBAgTClnvbwU3RhdGUxPDASBgNVBAoTC0..0EgTHRkMTcwNQYD
VQQLZy5DbGFzcyAxIFB1YmtpYyBQcm1tYXJ5IEN1cn..XRpb24gQXV0aG9y
aXR5MRQwEgYDVQDEwtCZXN0IENBIEExOZDAeFw0wMD..TUwMTZaPw0wMTAy
MDQxOTUwMTZaMIGHMQswCQYDVQGEWJHQjETMBEGA1..29tZS1TdGF0ZTEU
MBIGAlUEChMLQmVzdCBDQSBmdGQxNzAlBqNVBAAsTLk..DEgUHVibG1jIFBy
aW1hcnkgQ2VydgG1maWNhdG1vbiBBdXR0b3JpdHkxZD..AMTC0Jlc3QgQ0Eg
THRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg..Tz2mr7S2iAMfQyu
vBjM90iJjRazXBZlBjP5CE/Wm/Rr500PRK+Lh9x5eJ../ANBE0sTK0ZSDGM
ak2mlg7oruI3dY3VHqIxFTz0Tald+NAjwnLe4nOb7/.k05ShhBrJGBKxb
8n104o/5p8HAsZPdzbFMIyNjJzBM2o5y5A13wiLitE..fyYkQzaxCw0Awz1
kVHiIyCuaF4wj571pSzkv6sv+4IDMBT/XpCo8L6wTa..sh+etLD6FtTjYbb
rvZ8RQM1t1KdoMHg2qxraAV++HNBYmNws0duEdjUbJ..XI9TtnS4o1Ck7P
Of1jiQIDAQABo4HnMIHkMB0GA1UdDgQWBQB8urMCRL..5AkIp9NJHJw5TCB
tAYDVR0jB1GsmIGpgBQ8urMCRLYYMHUKU5AkIp9NJH..aSBijCBhzELMAkG
AlUEBhMCR0IxEzARBgNVBAgTClnvbwU3RhdGUxPD..AoTC0Jlc3QgQ0Eg
THRkMTcwNQYDVQQLZy5DbGFzcyAxIFB1YmtpYyBQcm..EN1cnRp2mljYXRp
b24gQXV0aG9yaXR5MRQwEgYDVQDEwtCZXN0IENBIE..DAMBqNVHRMEBTAD
AQH/MA0GCSqGSIb3DQEBAUAA4IBAQC1uYBcsSncwA..DCsQer772C2ucpX
xQUE/CopWw6gDkwd5D0DSMDJRqV/weo24wC6B73f5..bLhGYHaXJeSD6Kr
It8una2gy4120//on88r5IWJlm1L0oA8e4fr2yrBHX..adsGeFKkyNrwGi/
7vQMfXdGsRrXNGRgnX+vWDZ3/zWI0joDtCkNngEpVn..HoX
-----END CERTIFICATE-----
```

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

The following feature is not supported in Federal Risk and Authorization Manage Program (FedRAMP) environments. For more information, see the [FedRAMP Product Offering](#).

You can upgrade data from Tenable Nessus to Tenable Vulnerability Management via the **Upgrade Assistant** tool.


For more information, please refer to the Upgrade Assistant documentation: <https://docs.tenable.com/upgrade-assistant/nessus>



Password Management

The **Password Management** page allows you to set parameters for passwords, login notifications, and the session timeout.

Password Management



Password Management allows you to set parameters for passwords, as well as turn on login notifications and set the session timeout. Login notifications allow the user to see the last successful login, last failed login attempts (date, time and IP) and if any failed login attempts have occurred since the last successful login. Changes will take effect after a soft restart.

Password Complexity OFF ?

Session Timeout (mins)

Max Login Attempts

Min Password Length

Login Notifications OFF

Setting	Default	Description
Password Complexity	Off	Requires password to have a minimum of 8 characters, and at least 3 of the following: an upper case letter, a lower case letter, a special character, and a number.
Session Timeout (mins)	30	The web session timeout in minutes. Tenable Nessus logs users out automatically if their session is idle for longer than this timeout value.



Setting	Default	Description
Max Login Attempts	5	The maximum number of user login attempts allowed by Nessus before Tenable Nessus locks the account out. Setting this value to 0 disables this feature.
Min Password Length	8	This setting defines the minimum number of characters for passwords of accounts.
Login Notifications	Off	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.



Configure Password Management

1. In 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.

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

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 updates the information every 30 seconds.

For information, see [Monitor Scanner Health](#).

Tenable Nessus organizes the Scanner Health information into three categories:

- [Overview](#)
- [Network](#)
- [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	Graph showing how many MB of memory Tenable	Hover over a point on



Usage History	Nessus used over time.	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.



Monitor Scanner Health

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 data-set at a time.

5. Click the [Overview](#), [Network](#) or [Alerts](#) tab.



Advanced Debugging - Packet Capture

Note: Packet capture is only available in Tenable Nessus Professional and Tenable Nessus Expert.

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. Nessus now supports the ability to generate and download such a capture through the Nessus user interface.

Note: This feature has the following limitations:

- 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.
- 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 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 Nessus administrator using the `global.network_capture.max_disk_mb` and/or `global.network_capture.max_file_mb` advanced preferences.
- 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.

New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings | Credentials | Plugins

BASIC >
DISCOVERY >
ASSESSMENT >
REPORT >
ADVANCED ▾

Scan Type
Default
Default
Scan low bandwidth links
Custom
4 simultaneous checks per host (max)
5 second network read timeout

Save ▾ | Cancel

6. Click **General**.
7. Scroll to the bottom of the **General** settings window and set **Packet Capture** to **ON**.



Debug Settings

Log scan details
Logs the start and finish time for each plugin used during a scan to nessusd.messages.

Enable plugin debugging
Attaches available debug logs from plugins to the vulnerability output of this scan.

Debug Log Level

Enumerate launched plugins
Adds a list of plugins that were launched during the scan.

Audit Trail Verbosity

Include the KB

Packet Capture Settings

Packet Capture

8. In the **Target to capture** field, enter the IP address or hostname of a single host.

Packet Capture Settings

Packet Capture

Packet Capture Settings (Nessus 10 or later)

Target to capture REQUIRED
Provide one target to capture network scan traffic on next scan launch. Note: cannot use localhost/127.0.0.1

Ports to capture
Provide ports or port ranges to capture

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.tar.gz.

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. For more information, see [Acknowledge Notifications](#).

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 > Notifications	Shows all notifications from the past 90 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.

For more information, see [View Notifications](#).




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. For more information on viewing notification history, see [View Notifications](#).

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. You can still view cleared notifications in [notification history](#).



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. For information on managing notifications, see [Acknowledge Notifications](#).

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.



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.

My Account

Account Settings **API Keys**

User Info

Full Name

Email

Change Password

Current Password

New Password

Save **Cancel**

API Keys

An API Key consists of an Access Key and a Secret Key. API Keys authenticate with the **Nessus REST API** (version 6.4 or greater) 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

Caution: Generating a new API key replaces any existing keys and deauthorize any linked applications.

Note: Customers may not directly access Nessus scanning APIs to configure or launch scans, except as permitted as part of the Tenable Security Center and Tenable Vulnerability Management enterprise solutions.

1. In 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.



Users

Note: The **Users** page is only available in Tenable Nessus Manager.

The **Users** page shows a table of all Tenable Nessus 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. 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	<p>Basic user roles can read scan results.</p> <p>Note: This role is not available in Tenable Nessus Professional or Tenable Nessus Expert.</p>
Standard	<p>Standard users can create scans and policies.</p> <p>A scan created by a Standard user cannot be edited by other Standard users unless they're given editing permissions from the scan creator.</p> <p>Note: This role is not available in Tenable Nessus Professional or Tenable Nessus Expert.</p>
Administrator	<p>Administrators have the same privileges as Standard users, but can also manage users, user groups, and scanners. In Nessus Manager, Administrators can view scans that are shared by users.</p> <p>Tenable Nessus Professional and Tenable Nessus Expert users are Administrators by default.</p>
System Administrator	<p>System Administrators have the same privileges as Administrators, but can also manage and modify system configuration settings.</p> <p>Note: This role is not available in Tenable Nessus Professional or Tenable Nessus Expert.</p>



Name	Description
Disabled	Disabled user accounts cannot be used to log in to Tenable Nessus.



Create a User Account

Note: You can only perform this procedure in Tenable Nessus Manager. You cannot have multiple user accounts in Tenable Nessus Professional or Tenable Nessus Expert.

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

Note: You can only perform this procedure in Tenable Nessus Manager. You cannot have multiple user accounts in Tenable Nessus Professional or Tenable Nessus Expert.

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

Note: You can only perform this procedure in Tenable Nessus Manager. You cannot have multiple user accounts in Tenable Nessus Professional or Tenable Nessus Expert.

1. In 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 **X** 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.

Note: You can only perform this procedure in Tenable Nessus Manager. You cannot have multiple user accounts in Tenable Nessus Professional or Tenable Nessus Expert.

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:

- [About Nessus Plugins](#)
- [Amazon Web Services](#)
- [Command Line Operations](#)
- [Configure Tenable Nessus for NIAP Compliance](#)
- [Create a Limited Plugin Policy](#)
- [Default Data Directories](#)
- [Manage Logs](#)
- [Nessus Credentialed Checks](#)
- [Offline Update Page Details](#)
- [Run Nessus as Non-Privileged User](#)
- [Scan Targets](#)



Amazon Web Services

For information on integrating Nessus with Amazon Web Services, see the following:

- [Nessus BYOL Scanner on Amazon Web Services](#)
- [Nessus Pre-Authorized Scanner](#)
- [Link a BYOL Scanner to with Pre-Authorized Scanner Features](#)



Command Line Operations

This section includes command line operations for Nessus and Nessus 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 Nessus](#)
- [Start or Stop Nessus Agent](#)
- [Nessus-Service](#)
- [Nessuscli](#)
- [Nessuscli Agent](#)
- [Update Nessus Software \(CLI\)](#)



Start or Stop 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	<code>C:\Windows\system32>net start "Tenable Nessus"</code>
Stop	<code>C:\Windows\system32>net stop "Tenable Nessus"</code>

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	<code># /sbin/service nessusd start</code>
Stop	<code># /sbin/service nessusd stop</code>
SUSE	



Start or Stop	Linux Command-Line Operation
Start	<code># /etc/rc.d/nessusd start</code>
Stop	<code># /etc/rc.d/nessusd stop</code>
FreeBSD	
Start	<code># service nessusd start</code>
Stop	<code># service nessusd stop</code>
Debian, Kali, and Ubuntu	
Start	<code># /etc/init.d/service nessusd start</code>
Stop	<code># /etc/init.d/service nessusd stop</code>

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	<code># sudo launchctl start com.tenablesecurity.nessusd</code>
Stop	<code># sudo launchctl stop com.tenablesecurity.nessusd</code>

Note: You must have root permissions to run the start and stop commands.



Start or Stop a Nessus Agent

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

Windows

1. Navigate to **Services**.
2. In the **Name** column, click **Tenable Nessus Agent**.
3. To stop the service, right-click **Tenable Nessus Agent**, and then click **Stop**.

-or-

To restart the Nessus Agent service, right-click **Tenable Nessus Agent**, and then click **Start**.

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

Linux



Use the following commands:

Start or Stop	Linux Command Line Operation
RedHat, CentOS, and Oracle Linux	
Start	<code># /sbin/service nessusagent start</code>
Stop	<code># /sbin/service nessusagent stop</code>
SUSE	
Start	<code># /etc/rc.d/nessusagent start</code>
Stop	<code># /etc/rc.d/nessusagent stop</code>
FreeBSD	



Start or Stop	Linux Command Line Operation
Start	<code># service nessusagent start</code>
Stop	<code># service nessusagent stop</code>
Debian, Kali, and Ubuntu	
Start	<code># /etc/init.d/service nessusagent start</code>
Stop	<code># /etc/init.d/service nessusagent stop</code>

macOS

1. Navigate to **System Preferences**.
2. Click the  button.
3. Click the  button.
4. Type your username and password.
5. To stop the Nessus Agent service, click the **Stop Nessus Agent** button.

-or-

To start the Nessus Agent service, click the **Start Nessus Agent** button.

Start or Stop	macOS Command Line Operation
Start	<code># sudo launchctl start com.tenablesecurity.nessusagent</code>
Stop	<code># sudo launchctl stop com.tenablesecurity.nessusagent</code>



Nessus-Service

Unless otherwise specified, you can use **nessus-service** server commands interchangeably with **nessusd** commands.

If necessary, whenever possible, you should start and stop Nessus service using Nessus service controls in the operating system's interface. However, there are many **nessus-service** functions that you can perform through a command-line interface.

Tip: Use the `# killall nessusd` command to stop all Nessus services and in-process scans.

Note: You must run the following commands with administrative privileges.

Nessus-Service Syntax

Operating System	Command
Linux	<code># /opt/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]</code>
FreeBSD	<code># /usr/local/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]</code>
macOS	<code># /Library/Nessus/run/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]</code>
Windows	<code>C:\Program Files\Tenable\Nessus\nessus-service.exe [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]</code>

Suppress Command Output Examples

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

Linux

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

Nessus-Service or Nessusd Commands



Option	Description
-c <config-file>	When starting the nessusd server, use this option to specify the server-side nessusd configuration file to use. It allows for the use of an alternate configuration file instead of the standard db.
-S <ip[,ip2,...]>	When starting the nessusd server, force the source IP of the connections established by Nessus during scanning to <ip>. This option is only useful if you have a multihomed machine with multiple public IP addresses that you would like to use instead of the default one. For this setup to work, the host running nessusd must have multiple NICs with these IP addresses set.
-D	When starting the nessusd server, this option forces the server to run in the background (daemon mode).
-v	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 IPv4 socket.
--ipv6-only	Only listen on 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 only compile newly updated plugins.
-K or --set-encryption-passwd	<p>Set an encryption password for the scanner.</p> <p>If you set an encryption password, Nessus encrypts all policies, scans results, and scan configurations. You must enter the password when Tenable Nessus restarts.</p> <div style="border: 1px solid red; padding: 5px;"><p>Caution: If you lose your encryption password, it cannot be recovered by an administrator or Tenable Support.</p></div>

Notes



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

To set this setting, use the [Nessuscli](#) tool:

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

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



Nessuscli

You can administer some 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 Nessus, and fetch necessary license information.

Note: You must run all commands with administrative privileges.

Nessuscli Syntax

Operating System	Command
Linux	<code># /opt/nessus/sbin/nessuscli <cmd> <arg1> <arg2></code>
Windows	<code>C:\Program Files\Tenable\Nessus\nessuscli.exe <cmd> <arg1> <arg2></code>
macOS	<code># /Library/Nessus/run/sbin/nessuscli <cmd> <arg1> <arg2></code>

This topic describes the following command types:

- [Help Commands](#)
- [Backup Commands](#)
- [Bug Reporting Commands](#)
- [User Commands](#)
- [Fetch Commands](#)
- [Fix Commands](#)
- [Certificate Commands](#)
- [Software Update Commands](#)
- [Manager Commands](#)
- [Managed Scanner Commands](#)

- [Dump Command](#)
- [Node Commands](#)

Nessuscli Commands

Command	Description
Help Commands	
<code>nessuscli help</code>	Shows a list of Nessus commands. The help output may vary, depending on your Tenable Nessus license.
<code>nessuscli <cmd> help</code>	Shows more help information for specific commands identified in the <code>nessuscli help</code> output.
Backup Commands	
<code>nessuscli backup --create <backup_filename></code>	Creates a backup file of your Tenable Nessus instance, which includes your license and settings, and appends it with <i><Unix epoch timestamp>.tar.gz</i> . The command does not back up scan results. Example: If you run <code>nessuscli backup --create <december-backup></code> , Nessus creates the following backup file: <i>december-backup.1671720758.tar.gz</i> . For more information, see Back Up Nessus .
<code>nessuscli backup --restore <path/to/-backup_filename></code>	Restores a previously saved backup of Tenable Nessus. For more information, see Restore 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.	
<code>nessuscli bug-</code>	Generates an archive of system diagnostics.



Command	Description
<code>report-generator</code>	Running this command without arguments prompts for values. <code>--quiet</code> : run the bug report generator without prompting user for feedback. <code>--scrub</code> : when in quiet mode, bug report generator sanitizes the last two octets of the IPv4 address. <code>--full</code> : when in quiet mode, bug report generator collects extra data.
User Commands	
<code>nessuscli rmuser <username></code>	Allows you to remove a Nessus user.
<code>nessuscli chpasswd <username></code>	Allows you to change a user's password. The CLI prompts to enter the Nessus user's name. The CLI does not echo passwords on the screen.
<code>nessuscli adduser <username></code>	Allows you to add a 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.
<code>nessuscli lsuser</code>	Shows a list of Nessus users.
Fetch Commands	
Manage Nessus registration and fetch updates	
<code>nessuscli fetch --register <Activation Code></code>	Uses your Activation Code to register Nessus online. Example: <code># /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx</code>
<code>nessuscli fetch --register-only</code>	Uses your Activation Code to register Nessus online, but does not automatically download plugin or core updates.



Command	Description
<Activation Code>	Example: <pre># /opt/nessus/sbin/nessuscli fetch --register-only xxxx-xxxx-xxxx-xxxx</pre>
<pre>nessuscli fetch -- register-offline nessus.license</pre>	Registers Nessus with the <code>nessus.license</code> file obtained from https://plugins.nessus.org/v2/offline.php .
<pre>nessuscli fetch -- check</pre>	Shows whether Nessus is properly registered and is able to receive updates.
<pre>nessuscli fetch -- code-in-use</pre>	Shows the Nessus Activation Code that Tenable Nessus is using.
<pre>nessuscli fetch -- challenge</pre>	Shows the challenge code needed to use when performing an off-line registration. Example challenge code: <code>aaaaaa11b2222c-c33d44e5f6666a777b8cc99999</code>
<pre>nessuscli fetch -- security-center</pre>	Prepares Nessus to be connected to Security Center. <div style="border: 1px solid red; padding: 5px;">Caution: <i>Do not use this command if you do not want to switch your Nessus instance to Tenable.sc. This command irreversibly changes the Nessus scanner or Manager to a Tenable.sc-managed scanner, resulting in several user interface changes (for example, the site logo changes, and you do not have access to the Sensors page).</i></div>

Fix Commands



Command	Description
<code>nessuscli fix</code>	Reset registration, show network interfaces, and list advanced settings that you have set.
<code>nessuscli fix [--secure] --list</code>	Using the <code>--secure</code> option acts on the encrypted preferences, which contain information about registration.
<code>nessuscli fix [--secure] --set <setting=value></code>	You can use <code>--list</code> , <code>--set</code> , <code>--get</code> , and <code>--delete</code> to modify or view preferences.
<code>nessuscli fix [--secure] --get <setting></code>	
<code>nessuscli fix [--secure] --delete <setting></code>	
<code>nessuscli fix --list-interfaces</code>	List the network adapters on this machine.
<code>nessuscli fix --set listen_address-s=<address></code>	Tell the server to only listen to connections on the address <code><address></code> that is an IP, not a machine name. This option is useful if you are running <code>nessusd</code> on a gateway and if you do not want people on the outside to connect to your <code>nessusd</code> .
<code>nessuscli fix --show</code>	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 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.
<code>nessuscli fix --reset</code>	This command deletes all your registration information and preferences, causing Nessus to run in a non-registered state. Tenable Nessus Manager retains the same linking key after resetting. Before running <code>nessuscli fix --reset</code> , verify running scans



Command	Description
	have completed, then stop the nessusd daemon or service, as described in Start or Stop Nessus .
<code>nessuscli fix --reset-all</code>	<p>This command resets Nessus to a fresh state, deleting all registration information, settings, data, and users.</p> <div data-bbox="548 485 1479 600" style="border: 1px solid red; padding: 5px;"><p>Caution: You cannot undo this action. Contact Tenable Support before performing a full reset.</p></div>
<code>nessuscli fix --set agent_update_channel=<value></code>	<p>(Tenable Nessus Manager-linked agents only)</p> <p>Sets the agent update plan to determine what version the agent automatically updates to.</p> <p>Values:</p> <ul style="list-style-type: none">• ga – Automatically updates to the latest Nessus 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. <div data-bbox="548 1556 1479 1791" style="border: 1px solid blue; padding: 5px;"><p>Note: For agents linked to Tenable Nessus Manager, you need to run the <code>agent_update_channel</code> command from the Tenable Nessus Manager <code>nessuscli</code> utility. For agents linked to Tenable Vulnerability Management, you need to run the <code>agent_update_channel</code> command from the <code>agent nessuscli</code> utility.</p></div>
<code>nessuscli fix --</code>	Retrieve your unique agent linking key.



Command	Description
<code>secure --get agent_linking_key</code>	<p>Note: You can only use this linking key to link an agent. You cannot use it to link a scanner or a child node.</p>
<code>nessuscli fix --secure --get child_node_linking_key</code>	<p>Retrieve your unique child node linking key.</p> <p>Note: You can only use this linking key to link a child node. You cannot use it to link an agent or a scanner.</p>
<code>nessuscli fix --secure --get scanner_linking_key</code>	<p>Retrieve your unique scanner linking key.</p> <p>Note: You can only use this linking key to link a scanner. You cannot use it to link an agent or a child node.</p>
<code>nessuscli fix --set niap_mode=enforcing</code>	<p>Enforces NIAP mode for Nessus. For more information about NIAP mode, see Configure Tenable Nessus for NIAP Compliance.</p>
<code>nessuscli fix --set niap_mode=non-enforcing</code>	<p>Disables NIAP mode for Nessus. For more information about NIAP mode, see Configure Tenable Nessus for NIAP Compliance.</p>
<code>nessuscli fix --set fips_mode=enforcing</code>	<p>Enforces the current validated FIPS module for Nessus communication and database encryption. The FIPS module does not affect scanning encryption.</p> <p>Note: Nessus also enforces the FIPS module when you enforce NIAP mode. For more information, see Configure Tenable Nessus for NIAP Compliance.</p>
<code>nessuscli fix --set fips_mode=non-enforcing</code>	<p>Disables the FIPS module for Nessus communication and database encryption.</p> <p>Note: Nessus also disables the FIPS module when you disable NIAP mode. For more information, see Configure Tenable Nessus for NIAP Compliance.</p>
<code>nessuscli fix --set path_to_java=<custom</code>	<p>Sets a custom file path to Java for PDF exports. If not set, Nessus uses the system path.</p>



Command	Description
<code>file path</code>	You must use an absolute file path that contains the Java binary. For example, if the Nessus installation is in <code>/usr/lib/jvm/java-17-openjdk-amd64</code> , the custom file path must be <code>/usr/lib/jvm/java-17-openjdk-amd64/bin</code> .
Certificate Commands	
<code>nessuscli mkcert-client</code>	Creates a certificate for the Nessus server.
<code>nessuscli mkcert [-q]</code>	Creates a certificate with default values. -q for quiet creation.
<code>nessuscli import-certs --serverkey=<server key path> --server-cert=<server certificate path> --cacert=<CA certificate path></code>	Validates the server key, server certificate, and CA certificate and checks that they match. Then, copies the files to the correct locations.
Software Update Commands	
<code>nessuscli update</code>	By default, this tool updates based on the software update options selected through the Nessus user interface. Note: This command only works for standalone Nessus scanners. The command does not work for scanners managed by Tenable Vulnerability Management or Tenable Security Center.
<code>nessuscli update --all</code>	Forces updates for all Nessus components. Note: This command only works for standalone Nessus scanners. The command does not work for scanners managed by Tenable Vulnerability Management or Tenable Security Center.



Command	Description
<pre>nessuscli update --plugins-only</pre>	<p>Forces updates for Nessus plugins only.</p> <div data-bbox="548 310 1479 464" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: This command only works for standalone Nessus scanners. The command does not work for scanners managed by Tenable Vulnerability Management or Tenable Security Center.</p></div>
<pre>nessuscli update <tar.gz filename></pre>	<p>Updates Nessus plugins by using a TAR file instead of getting the updates from the plugin feed. You obtain the TAR file when you Manage Tenable Nessus Offline - Download and Copy Plugins steps.</p>
<pre>nessuscli fix --set scanner_update_channel=<value></pre>	<p>(Tenable Nessus Professional and Tenable.io-managed scanners only)</p> <p>Sets the Tenable Nessus to determine what version Tenable Nessus automatically updates to.</p> <div data-bbox="548 957 1479 1152" style="border: 1px solid #0070C0; padding: 5px;"><p>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.</p></div> <p>Values:</p> <ul style="list-style-type: none">• 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



Command	Description
	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.	
<code>nessuscli manager download-core</code>	Downloads core component updates for remotely managed agents and scanners.
<code>nessuscli manager generate-plugins</code>	Generates plugins archives for remotely managed agents and scanners.
Managed Scanner Commands Used for linking, unlinking, and viewing the status of remote managed scanners.	
<code>nessuscli managed help</code>	Shows nessuscli-managed commands and syntax.
<code>nessuscli managed link --key=<key> --host=<host> --port=<port> [optional parameters]</code>	<p>Link an unregistered scanner to a manager.</p> <div style="border: 1px solid blue; padding: 5px;"><p>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).</p></div> <p>Optional Parameters:</p> <ul style="list-style-type: none">• <code>--name</code>: A name for the scanner.• <code>--ca-path</code>: A custom CA certificate to use to validate the manager's server certificate.• <code>--groups</code>: 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
	<p>For example: <code>--groups="Atlanta,Global Headquarters"</code></p> <div data-bbox="626 359 1479 474"><p>Note: The scanner group name is case-sensitive and must match exactly.</p></div> <ul style="list-style-type: none">• <code>--proxy-host</code>: The hostname or IP address of your proxy server.• <code>--proxy-port</code>: The port number of the proxy server.• <code>--proxy-username</code>: The name of a user account that has permissions to access and use the proxy server.• <code>--proxy-password</code>: The password of the user account that you specified as the username.• <code>--proxy-agent</code>: The user agent name, if your proxy requires a preset user agent.• <code>--aws-scanner</code>: Indicates that the Tenable Nessus scanner links as an AWS scanner. <div data-bbox="626 1178 1479 1293"><p>Note: The Tenable Nessus scanner must already be running on an AWS instance for this option to take effect.</p></div>
<code>nessuscli managed unlink</code>	Unlink a managed scanner from its manager.
<code>nessuscli managed status</code>	Identifies the status of the managed scanner.
Dump Command	
<code>nessuscli dump --plugins</code>	Adds a <code>plugins.xml</code> file in the <code>sbin</code> directory. For example, running the <code>/opt/nessus/sbin/nessuscli dump --plugins</code> on Linux adds a <code>plugins.xml</code> file to the <code>/opt/nessus/sbin/plugins</code> directory.



Command	Description
<p>Node Commands</p> <p>Used for viewing and changing node links in a cluster environment.</p>	
<pre>nessuscli node link --key=<key> -- host=<host> -- port=<port></pre>	<p>Links the child node to the parent node in a clustering environment.</p> <p>For more information on key, host, and port, see Link a Node.</p>
<pre>nessuscli node unlink</pre>	<p>Unlinks the child node from the parent node.</p>
<pre>nessuscli node status</pre>	<p>Shows whether the child node is linked to parent node and the number of agents that are linked.</p>



Nessuscli Agent

Use the Agent `nessuscli` utility to perform some Tenable Nessus 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
Linux	<code># /opt/nessus_agent/sbin/nessuscli <cmd> <arg1> <arg2></code>
Windows	<code>C:\Program Files\Tenable\Nessus Agent\nessuscli.exe <cmd> <arg1> <arg2></code>
macOS	<code># sudo /Library/NessusAgent/run/sbin/nessuscli <cmd> <arg1> <arg2></code>

Nessuscli Commands

Command	Description
Informational Commands	
<code># nessuscli help</code>	Displays a list of <code>nessuscli</code> commands.
<code># nessuscli -v</code>	Displays your current version of Tenable Nessus Agent.
Bug Reporting Commands	
<code># nessuscli bug-report-generator</code>	<p>Generates an archive of system diagnostics.</p> <p>If you run this command without arguments, the utility prompts you for values.</p> <p>Optional arguments:</p> <ul style="list-style-type: none"><code>--quiet</code> – Run the bug report generator without prompting user for feedback.



Command	Description
	<ul style="list-style-type: none">• <code>--scrub</code> – The bug report generator sanitizes the last two octets of the IPv4 address.• <code>--full</code> – The bug report generator collects extra data.
Image Preparation Commands	
<pre># nessuscli pre-prepare-image</pre>	<p>Performs pre-imaging cleanup, including the following:</p> <ul style="list-style-type: none">• Unlinks the agent, if linked.• Deletes any host tag on the agent. For example, the registry key on Windows or <code>tenable_tag</code> on Unix.• Deletes any UUID file on the agent. For example, <code>/opt/nessus/var/nessus/uuid</code> (or equivalent on MacOS/Windows).• Deletes <code>plugin dbs</code>.• Deletes <code>global db</code>.• Deletes <code>master.key</code>.• Deletes the backups directory. <p>Optional arguments:</p> <ul style="list-style-type: none">• <code>--json=<file></code> – Validates an auto-configuration <code>.json</code> file and places it in the appropriate directory.
Local Agent Commands	
Used to link, unlink, and display agent status	
<pre># nessuscli agent link --key=<key> --host=<host> --port=<port></pre>	<p>Using the Nessus Agent Linking Key, this command links the agent to the Tenable Nessus Manager or Tenable Vulnerability Management.</p> <p>Required arguments:</p> <ul style="list-style-type: none">• <code>--key</code> – The linking key that you retrieved from the manager.



Command	Description
	<ul style="list-style-type: none">• <code>--host</code> – The static IP address or hostname you set during the Tenable Nessus Manager installation. <div data-bbox="574 359 1479 636" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: Starting with Tenable Nessus Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using <code>sensor.cloud.tenable.com</code>. If agents are unable to connect to <code>sensor.cloud.tenable.com</code>, they use <code>cloud.tenable.com</code> instead. Agents with earlier versions continue to use the <code>cloud.tenable.com</code> domain.</p></div> <ul style="list-style-type: none">• <code>--port</code> – 8834 or your custom port. <p>Optional arguments:</p> <ul style="list-style-type: none">• <code>--auto-proxy</code> – (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.• <code>--name</code> – 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.• <code>--groups</code> – 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: "Atlanta,Global Headquarters" <div data-bbox="574 1570 1479 1686" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: The agent group name is case-sensitive and must match exactly.</p></div> <ul style="list-style-type: none">• <code>--ca-path</code> – A custom CA certificate to use to validate the manager's server certificate.



Command	Description
	<ul style="list-style-type: none">• <code>--offline-install</code> – When enabled (set to "yes"), installs Tenable Nessus Agent on the system, even if it is offline. Tenable Nessus 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.• <code>--network</code> – 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.• <code>--proxy-host</code> – The hostname or IP address of your proxy server.• <code>--proxy-port</code> – The port number of the proxy server.• <code>--proxy-password</code> – The password of the user account that you specified as the username.• <code>--proxy-username</code> – The name of a user account that has permissions to access and use the proxy server.• <code>--proxy-agent</code> – The user agent name, if your proxy requires a preset user agent.
<code># nessuscli agent unlink</code>	Unlinks agent from the Tenable Nessus Manager or Tenable Vulnerability Management.
<code># nessuscli scan-triggers --list</code>	Lists details about the agent's rule-based scans: <ul style="list-style-type: none">• Scan name• Status (for example, uploaded)• Time of last activity (shown next to the status)• Scan description



Command	Description
	<ul style="list-style-type: none">• Time of last policy modification• Time of last run• Scan triggers• Scan configuration template• Command to launch the scan (<code>nessuscli scan-triggers --start --UUID=<scan-uuid></code>)
<pre># nessuscli scan-triggers --start --UUID=<scan-uuid></pre>	<p>(Tenable Vulnerability Management-linked agents only)</p> <p>Manually executes a rule-based scan based on UUID.</p>
<pre># nessuscli agent status</pre>	<p>Displays the status of the agent, rule-based scanning information, jobs pending, and whether the agent is linked to the server.</p> <p>Optional arguments:</p> <ul style="list-style-type: none">• <code>--local</code> – (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.• <code>--remote</code> – (Default behavior) Fetches the job count from the manager and displays the status. <div data-bbox="574 1457 1479 1572" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: Tenable does not recommend running frequent status checks with the <code>--remote</code> option (for example, when using automation).</p></div> <ul style="list-style-type: none">• <code>--offline</code> – Provides the most recently cached agent status when it cannot connect to Tenable Nessus Manager or Tenable Vulnerability Management.• <code>--show-token</code> – Displays the agent's token that is used to identify and authenticate with its manager.



Command	Description
	<ul style="list-style-type: none">• <code>--show-uuid</code> – Displays the agent's Tenable UUID.
<pre># nessuscli plugins --info</pre>	<p>Lists details about the agent's full and inventory plugin sets:</p> <ul style="list-style-type: none">• 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 <p>Lists details and statistics about the agent's plugins, such as:</p> <ul style="list-style-type: none">• 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
<pre># nessuscli plugins --reset</pre>	<p>Deletes all plugins and plugin-related data off the disk. The agent is able to download plugins immediately after the deletion completes.</p> <div data-bbox="495 1493 1479 1570" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: This command only triggers if the agent has plugin data on its disk.</p></div>
<pre># install-relay -linking-key=<Tenable.ad relay linking key></pre>	<p>Installs a Tenable Identity Exposure Secure Relay on the agent.</p> <p>To retrieve the Tenable Identity Exposure relay linking key, see Secure Relay in the <i>Tenable.ad Administrator Guide</i>.</p>



Command	Description
Update Commands	
<pre># nessuscli agent update --file- e=<plugins_ set.tgz></pre>	<p>Manually installs a plugin set.</p>
<pre># nessuscli fix - -set agent_ update_ channel=<value></pre>	<p>(Tenable Vulnerability Management-linked agents only)</p> <p>Sets the agent update plan to determine what version the agent automatically updates to.</p> <p>Values:</p> <ul style="list-style-type: none">• 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 latest release. <div style="border: 1px solid blue; padding: 5px;"><p>Note: For agents linked to Tenable Vulnerability Management, you need to run the <code>agent_update_channel</code> command from the agent <code>nessuscli</code> utility. For agents linked to Tenable Nessus Manager, you need to run the <code>agent_update_channel</code> command from the Tenable Nessus Manager <code>nessuscli</code> utility.</p></div>
<pre># nessuscli fix - -set maximum_</pre>	<p>(Tenable Vulnerability Management-linked agents only)</p>



Command	Description
<code>scans_per_day-y=<value></code>	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 .
Fix Commands	
<code># nessuscli fix -list</code>	Displays a list of agent settings and their values.
<code>nessuscli fix --set <setting>=<value></code>	Set an agent setting to the specified value. For a list of agent settings, see Advanced Settings in the <i>Tenable Nessus Agent User Guide</i> .
<code># nessuscli fix -set update_hostname="<value>"</code>	Updates agent hostnames automatically in Tenable Vulnerability Management or Tenable Nessus Manager 7.1.1 or later. You can set the <code>update_hostname</code> parameter to <code>yes</code> or <code>no</code> . By default, this preference is disabled. Note: Restart the agent service for the change to take effect in Tenable Nessus Manager.
<code># nessuscli fix -set max_retries="<value>"</code>	Sets the maximum number of times an agent should retry in the event of a failure when executing the <code>agent link</code> , <code>agent status</code> , or <code>agent unlink</code> commands. The commands retry, the specified number of times, consecutively, sleeping increasing increments of time set by <code>retry_sleep_milliseconds</code> between attempts. The default value for <code>max_retries</code> is 0. For example, if you set <code>max_retries</code> to 4 and set <code>retry_sleep_milliseconds</code> 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. Note: This setting does not affect offline updates or the agent's normal 24 hour check-in after it is linked.



Command	Description
<pre># nessuscli fix - -set retry_sleep_ milliseconds=" <value>"</pre>	Sets the number of milliseconds that an agent sleeps for between retries in event of a failure when executing the agent <code>link</code> , <code>agent status</code> , or <code>agent unlink</code> commands. The default is 1500 milliseconds (1.5 seconds).
<pre># nessuscli fix - -set niap_mod- e=enforcing</pre>	Enforces NIAP mode for Nessus Agent. For more information about NIAP mode, see Configure Nessus Agent for NIAP Compliance .
<pre># nessuscli fix - -set niap_mod- e=non-enforcing</pre>	Disables NIAP mode for Nessus Agent. For more information about NIAP mode, see Configure Nessus Agent for NIAP Compliance .
<pre># nessuscli fix - -set fips_mod- e=enforcing</pre>	Enforces the current validated FIPS module for Nessus Agent communication and database encryption. The FIPS module does not affect scanning encryption. Note: Nessus Agent also enforces the FIPS module when you enforce NIAP mode. For more information, see Configure Nessus Agent for NIAP Compliance .
<pre># nessuscli fix - -set fips_mod- e=non-enforcing</pre>	Disables the FIPS module for Nessus Agent communication and database encryption. Note: Nessus Agent also disables the FIPS module when you disable NIAP mode. For more information, see Configure Nessus Agent for NIAP Compliance .
Fix Secure Settings	
<pre># nessuscli fix - -secure --set <setting>=<value></pre>	Set secure settings on the agent. Caution: Tenable does not recommend changing undocumented <code>--secure</code> settings as it may result in an unsupported configuration. For a list of supported secure settings, see Advanced Settings in the <i>Tenable Nessus Agent User Guide</i> .



Command	Description
<pre># nessuscli fix - -secure --get agent_linking_key</pre>	<p>(Nessus versions 10.4.0 and later only) Retrieve your unique agent linking key.</p> <div data-bbox="496 363 1479 478" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: You can only use this linking key to link an agent. You cannot use it to link a scanner or a child node.</p></div>
<p>Resource Control Commands</p>	
<pre># nessuscli fix - -set process_pri- ority="<value>" # nessuscli fix - -get process_pri- ority # nessuscli fix - -delete process_ priority</pre>	<p>Commands</p> <p>Set, get, or delete the <code>process_priority</code> setting.</p> <p>You can control the priority of the Nessus Agent relative to the priority of other tasks running on the system by using the <code>process_priority</code> preference.</p> <p>For valid values and more information on how the setting works, see Agent CPU Resource Control in the <i>Tenable Nessus Agent Deployment and User Guide</i> for <code><value></code> preference options</p>



Update Nessus Software (CLI)

When updating Nessus components, you can use the `nessuscli` update commands, also found in the [command-line](#) section.

Note: If you are working with Nessus offline, see [Manage Nessus Offline](#).

Note: You must run the following commands with administrator privileges.

Operating System	Command
Linux	<code># /opt/nessus/sbin/nessuscli <cmd> <arg1> <arg2></code>
Windows	<code>C:\Program Files\Tenable\Nessus <cmd> <arg1> <arg2></code>
macOS	<code># /Library/Nessus/run/sbin/nessuscli <cmd> <arg1> <arg2></code>
Software Update Commands	
<code>nessuscli update</code>	By default, this tool respects the software update options selected through the Nessus user interface.
<code>nessuscli update --all</code>	Forces updates for all Nessus components.
<code>nessuscli update --plugins-only</code>	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.

Before you begin:

- If you are using 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 Nessus marks the certificate as invalid. If there is no response, then 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 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	<code>/opt/nessus/var/nessus</code>
Windows	<code>C:\ProgramData\Tenable\Nessus\nessus</code>
macOS	<code>/Library/Nessus/run/var/nessus</code>

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 passwords	SHA-512 and the PBKDF2 function with a 512-bit key
Storing user and service accounts for scan credentials, as described in Credentials	AES-128
Scan Results	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 the Tenable product registration server	TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384
Communications between Tenable Nessus and the Tenable plugin update server	TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384



File and Process Allowlist

You need to allow Tenable Nessus to access third-party endpoint security products such as anti-virus applications and host-based intrusion and prevention systems.

Note: If your Windows installation uses a non-standard drive or folder structure, use the %PROGRAMFILES% and %PROGRAMDATA% environment variables.

The table following contains a list of Nessus folders, files, and processes that you should allow. For information about allowlisting Nessus Agent processes, see [File and Process Allowlist](#) in the *Nessus Agent User Guide*.

Note: In addition to the files 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

Files

C:\Program Files\Tenable\Nessus*

C:\Program Files (x86)\Tenable\Nessus*

C:\ProgramData\Tenable\Nessus*

Processes

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

Files

/opt/nessus/bin/*

/opt/nessus/bin/openssl

/opt/nessus/sbin/*

/opt/nessus_agent/lib/nessus/*

Processes

/opt/nessus/bin/nasl

/opt/nessus/sbin/nessusd

/opt/nessus/sbin/nessuscli

/opt/nessus/sbin/nessus-service

macOS

Files

/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



Manage Logs

Tenable Nessus has the following default log files:

- `nessusd.dump` – Nessus dump log file used for debugging output.
- `nessusd.messages` – Nessus scanner log.
- `www_server.log` – Nessus web server log.
- `backend.log` – Nessus backend log.
- `nessuscli.log` – Nessuscli log.

Default Log Locations

The following are the default log file locations for each operating system.

- Linux – `/opt/nessus/var/nessus/logs/<filename>`
- macOS – `/Library/Nessus/run/var/nessus/logs/<filename>`
- Windows – `C:\ProgramData\Tenable\Nessus\nessus\logs\<filename>`

You can customize log file locations when you [modify log settings](#).

Modify Log Settings

To modify log settings, use one of the following methods, depending on the log file:

- To modify log settings for `www_server.log`, `backend.log`, `nessusd.dump`, and custom logs, see [Modify log.json](#).
- [Modify advanced settings](#) – `nessusd.messages`

Modify log.json

You can configure log locations and rotation strategies for `www_server.log`, `nessusd.dump`, and `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.

Note: You cannot configure `nessusd.messages` settings using `log.json`. Configure those log settings using `logfile_rot` in the [advanced settings](#).



To modify log settings using log.json:

1. Using a text editor, open the log.json file, located in the corresponding directory:
 - **Linux** – /opt/nessus/var/nessus/log.json
 - **macOS** – /Library/Nessus/run/var/nessus/log.json
 - **Windows** – C:\ProgramData\Tenable\Nessus\nessus\log.json
2. For each log file, edit or create a reporters[x].reporter section, and add or modify the parameters described in [log.json Format](#).
3. Save the log.json file.
4. [Restart](#) the Tenable Nessus service.

The Tenable Nessus updates the log settings.

log.json Format

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	www_server.log: response backend.log: log, info, warn, error, trace	www_server.log: no backend.log: yes	Determines what log information the log includes. <ul style="list-style-type: none">• response – Web server activity logs <div style="border: 1px solid blue; padding: 5px; margin: 10px 0;">Note: response is the only valid tag for www_server.log.</div> <ul style="list-style-type: none">• info – Informational logs for a



			<p>specific task</p> <ul style="list-style-type: none">• 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
<code>type</code>	<code>file</code>	not recommended	Determines the type of the log file.
<code>rotation_strategy</code>	<code>size</code>	yes	<p>Determines whether the log archives files based on maximum rotation size or rotation time.</p> <p>Valid values:</p> <ul style="list-style-type: none">• size – Rotate the log based on size, as specified in <code>max_size</code>.• daily – Rotate the log based on time, as specified in <code>rotation_time</code>.



<code>rotation_time</code>	86400 (1 day)	yes	Rotation time in seconds. Only used if <code>rotation_strategy</code> is <code>daily</code> .
<code>max_size</code>	Tenable Nessus: 536870912 (512 MB) Agent: 10485760 (10 MB)	yes	Rotation size in bytes. Only used if <code>rotation_strategy</code> is <code>size</code> .
<code>max_files</code>	Tenable Nessus: 10 Agent: 2	yes	Maximum number of files allowed in the file rotation. The maximum number includes the main file, so 10 <code>max_files</code> is 1 main file and 9 backups. If you decrease this number, Tenable Nessus deletes the old logs.
<code>file</code>	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.
<code>context</code>	<code>true</code>	not recommended	Enables more context information for logs in



			the system format, such as <code>backend.log</code> .
format	www_server.log: combined backend.log: system	not recommended	Determines the format of the output. <ul style="list-style-type: none">• 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"
}
}
```

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"
}
}
```

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"  
    }  
]
```



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:

- [Nessus Environment Variables](#)
- [Deploy Tenable Nessus using JSON](#)



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.io, 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_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 text 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 `config.json` file format:

```
{
  "link": {
    "name": "sensor name",
    "host": "hostname or IP address",
    "port": 443,
    "key": "abcdefghijklmnopqrstuvwxyz",
    "ms_cert": "CA certificate for linking",
    "retry": 1,
    "proxy": {
      "proxy": "proxyhostname",
      "proxy_port": 443,
      "proxy_username": "proxyusername",
      "proxy_password": "proxypassword",
      "user_agent": "proxyagent",
    }
  }
}
```



```
        "proxy_auth": "NONE"
    }
},
"preferences": {
    "global.max_hosts": "500"
},
"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
<code>name</code>	(Optional) A name for the scanner.
<code>host</code>	The hostname or IP address of the manager you want to link to.
<code>port</code>	The port for the manager you want to link to. For Tenable Nessus Manager: 8834 or your custom port.
<code>key</code>	The linking key that you retrieved from the manager.
<code>ms_cert</code>	(Optional)



	A custom CA certificate to use to validate the manager's server certificate.
proxy	<p>(Optional)</p> <p>If you are using a proxy server, include the following:</p> <p>proxy: The hostname or IP address of your proxy server.</p> <p>proxy_port: The port number of the proxy server.</p> <p>proxy_username: The name of a user account that has permissions to access and use the proxy server.</p> <p>proxy_password: The password of the user account that you specified as the username.</p> <p>user_agent: The user agent name, if your proxy requires a preset user agent.</p> <p>proxy_auth: The authentication method to use for the proxy.</p>
aws_scanner	<p>(Optional)</p> <p>Set <code>aws_scanner</code> to true to link the Tenable Nessus scanner as an AWS scanner.</p> <div style="border: 1px solid #0070C0; padding: 5px;"><p>Note: The Tenable Nessus scanner must already be running on an AWS instance for the option to take effect.</p></div>

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 <code>password</code> 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 <code>disabled</code> , <code>basic</code> , <code>standard</code> , <code>administrator</code> , or <code>system_administrator</code> . For more information, see Users .
type	Set to <code>local</code> .



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

The process described in this section enables you to perform local security checks on Windows systems. You can only use Domain Administrator accounts to scan Domain Controllers.

Note: To run some local checks, Nessus requires that the host runs PowerShell 5.0 or newer.

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 a Domain Account for Authenticated Scanning

To create a domain account for remote host-based auditing of a Windows server, the server must first be a supported version of Windows and be part of a domain.

Create a Security Group called Nessus Local Access

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 Group Policy called Local Admin GPO

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

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 check boxes 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 Group policy management console, right-click the domain or the OU and select **Link an Existing GPO**.
2. Select the Tenable Nessus` Scan GPO.

Configure Windows

1. Under **Windows Firewall > Windows Firewall Settings**, enable **File and Printer Sharing**.
2. Using the `gpedit.msc` tool (via the Run prompt), invoke the 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.
3. (Windows 8 and earlier only) 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** and set it to either **Disabled** or **Not Configured**.
4. Enable the **Remote Registry** service (it is disabled by default). If the service is set to *manual* (rather than *enabled*), plugin IDs 42897 and 42898 only enable the registry during the scan.

Note: Enabling this option configures Nessus to attempt to start the remote registry service before starting the scan.



The Windows credentials provided in the Nessus scan policy must have administrative permissions to start the Remote Registry service on the host being scanned.

5. Open TCP ports **139** and **445** between Tenable Nessus and the target.
6. 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 <http://support.microsoft.com/kb/842715/en-us>.

- **C\$**

Caution: While not recommended, you can disable Windows User Account Control (UAC).

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.

What to do next:

- View the [prerequisites](#) for Windows credentialed checks.
- [Enable](#) Windows logins for local and remote audits.
- [Configure](#) a Nessus scan for Windows Logins.



Prerequisites

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.



Enable Windows Logins for Local and Remote Audits

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 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 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 bullets describe how to configure a domain or local account to use for Windows credentialed checks, depending on your needs.

- **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 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 cre-

entials 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**.

Configure Windows

Once you create an appropriate account for credentialed checks, there are several Windows configuration options that you must enable or disable before scanning (for more information, see [Credentialed Checks on Windows](#)):

- **(Local accounts only) User Account Control (UAC)**

Disable Windows User Account Control (UAC), or you must change a specific registry setting allow 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](#).

- **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**.

- Open any host firewalls to allow connections from 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**. You can enable it for a one-time audit, or leave it enabled permanently if you perform frequent audits.

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

Enable administrative shares (**IP\$**, **ADMIN\$**, **C\$**).

Note: Windows 10 disables **ADMIN\$** by default. For all other operating systems, the three administrative shares are enabled by default and can cause other issues if disabled. For more information, see <http://support.microsoft.com/kb/842715/en-us>.

Note: To troubleshoot missing administrative shares, see [the related Microsoft troubleshooting topic](#).



Configure a 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.

To configure a Nessus scan configuration for Windows logins:

1. In the scan settings, click the **Credentials** tab.

The Credentials menu opens.

2. In the Categories drop-down menu, select **Host**.
3. In the Host category, click **Windows**.

A Windows credentials pane appears.

4. Select an authentication method. Depending on the method, the remaining Windows settings change.
5. Depending on the authentication method, specify the SMB account username, password or hash, and domain.

To view the Windows credential setting descriptions, see [Windows](#).

6. Click **Save**. Tenable Nessus saves the new Windows credentials.



Credentialed Checks on Linux

The process described in this section enables you to perform local security checks on Linux based systems. The SSH daemon used in this example 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.

What to do next:

- View the [prerequisites](#) for Linux credentialed checks.
- [Enable](#) SSH local security checks.
- [Configure](#) Nessus for SSH host-based checks.



Prerequisites

Configuration Requirements for SSH

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 only accept certain types of encryption. 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 Nessus credential checks. It is not an in-depth tutorial on SSH, and assumes the reader has the prerequisite knowledge of Linux system commands.

Generating SSH Public and Private Keys

The first step is to generate a private/public key pair for the 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 dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/test/.ssh/id_dsa):
/home/test/Nessus/ssh_key
Enter passphrase (empty for no passphrase):
Enter 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 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 Nessus to use key-based authentication.

Nessus Windows users may wish to copy both keys to the main Nessus application directory on the system running Nessus (**C:\Program Files\Tenable\Nessus** by default), and then copy the public key to the target systems as needed. This makes it easier to manage the public and private key files.



Creating a User Account and Setting up the SSH Key

On every target system that you want to scan using local security checks, create a new user account dedicated to 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 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 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 System Housing the Public Key

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 “Creating a User Account and Setting up the SSH Key” above).

Test to make sure that the accounts and networks are configured correctly. Using the simple Linux command `id`, from the 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 Nessus user, the key exchange was successful.



Configure Nessus for SSH Host-Based Checks

If you have not already done so, secure copy the private and public key files to the system that you plan to use to access the Nessus scanner, as described in [Enable SSH Local Security Checks](#).

Nessus User Interface Steps

1. Click **New Scan** to create a new scan and select a template.
-or-
Click **My Scans** in the left navigation bar, choose an existing scan, then click the **Configure** button.
2. Click the **Credentials** tab.
3. Select **SSH**.
4. In the **Authentication method** drop-down box, select an authentication method.
5. Configure the remaining [settings](#).
6. Click the **Save** button.



Run Nessus as Non-Privileged User

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.

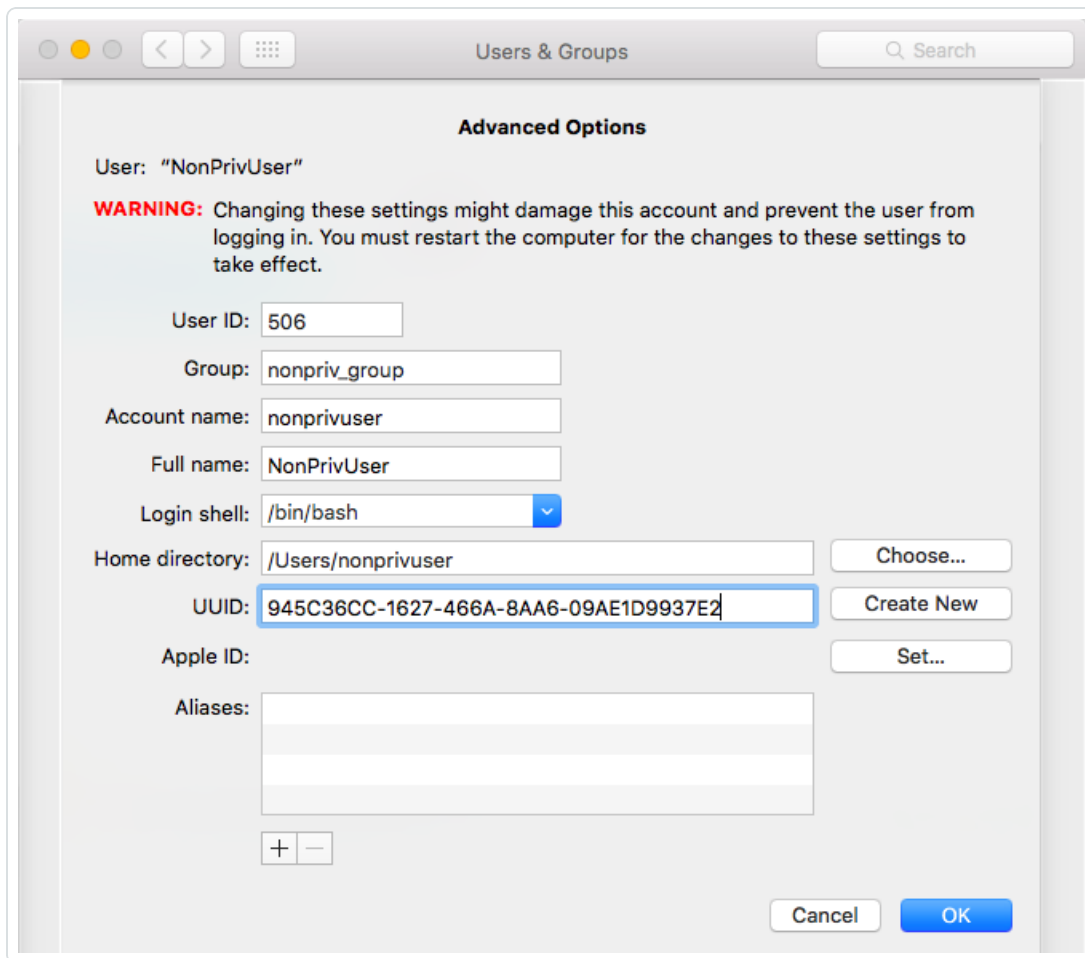
Steps

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.

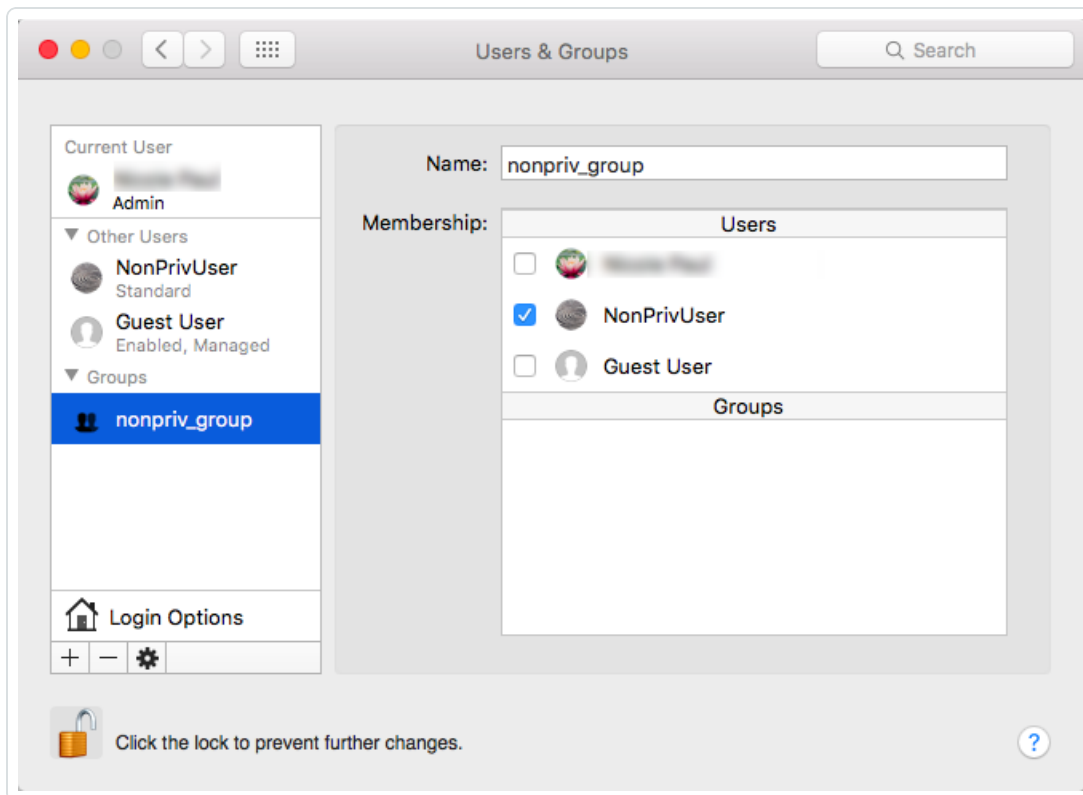
Use the following command to unload the Nessus service:

```
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.



- 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>
|
```

- 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
```

- 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 **sysctl.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
```

Run Nessus on FreeBSD 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.

Note: Unless otherwise noted, execute the following commands in a root login shell.

1. If you have not already done so, [Install](#) Nessus on FreeBSD.

```
pkg add Nessus-*.txz
```

2. Create a non-root account to run the Nessus service.

In this example, the user creates `nonprivuser` in the `nonprivgroup`.

```
# adduser
Username: nonprivuser
Full name: NonPrivUser
Uid (Leave empty for default):
Login group [nonprivuser]:
Login group is nonprivuser. Invite nonprivuser into other groups? []:
Login class [default]:
Shell (sh csh tcsh bash rbash nologin) [sh]:
Home directory [/home/nonprivuser]:
Home directory permissions (Leave empty for default):
```




```
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]:
Username : nonprivuser
Password : *****
Full Name : NonPrivUser
Uid : 1003
Class :
Groups : nonprivuser
Home : /home/nonprivuser
Home Mode :
Shell : /bin/sh
Locked : no
OK? (yes/no): yes
adduser: INFO: Successfully added (nonprivuser) to the user database.
Add another user? (yes/no): no
Goodbye!
```

3. Remove 'world' permissions on Nessus binaries in the `/sbin` directory.

```
chmod 750 /usr/local/nessus/sbin/*
```

4. Change ownership of `/opt/nessus` to the non-root user.

```
chown -R nonprivuser:nonprivuser /usr/local/nessus
```

5. Create a group to give the non-root user access to the `/dev/bpf` device and allow them to use raw sockets.

```
pw groupadd access_bpf
pw groupmod access_bpf -m nonprivuser
```



6. Confirm that `nonprivuser` appears in the group.

```
# pw groupshow access_bpf
access_bpf:*:1003:nonprivuser
```

7. Next, check your system limit values.

Using the `ulimit -a` command, verify that each parameter has, at minimum, the following values.

This example shows FreeBSD 10 values:

```
# ulimit -a
cpu time          (seconds, -t)    unlimited
file size        (512-blocks, -f) unlimited
data seg size    (kbytes, -d)     33554432
stack size       (kbytes, -s)     524288
core file size   (512-blocks, -c) unlimited
max memory size  (kbytes, -m)     unlimited
locked memory    (kbytes, -l)     unlimited
max user processes (-u)          6670
open files       (-n)          58329
virtual mem size (kbytes, -v)     unlimited
swap limit       (kbytes, -w)     unlimited
sbsize           (bytes, -b)      unlimited
pseudo-terminals (-p)          unlimited
```

8. If any of the values in Step 6. do not meet the minimum requirements, take the following steps to modify values.

Using a text editor, edit the `/etc/sysctl.conf` file.

Next, using the `service` command, restart the `sysctl` service:

```
service sysctl restart
```

Alternatively, you can reboot your system.

Verify the new, minimum required values by using the `ulimit -a` command again.



9. Next, using a text editor, modify the `/usr/local/etc/rc.d/nessusd` service script to remove and add the following lines:

Remove: `/usr/local/nessus/sbin/nessus-service -D -q`

Add: `chown root:access_bpf /dev/bpf`

Add: `chmod 660 /dev/bpf`

Add: `daemon -u nonprivuser /usr/local/nessus/sbin/nessus-service -D -q --no-root`

The resulting script should appear as follows:

```
nessusd_start() {
    echo 'Starting Nessus...'
    chown root:access_bpf /dev/bpf
    chmod 660 /dev/bpf
    daemon -u nonprivuser /usr/local/nessus/sbin/nessus-service -D -q --no-root
}
nessusd_stop() {
    test -f /usr/local/nessus/var/nessus/nessus-service.pid && kill `cat
/usr/local/nessus/var/nessus/nessus-service.pid` && echo 'Stopping Nessus...' &&
sleep 3
}
```



Upgrade Assistant

The following feature is not supported in Federal Risk and Authorization Manage Program (FedRAMP) environments. For more information, see the [FedRAMP Product Offering](#).

You can upgrade data from Tenable Nessus to Tenable Vulnerability Management via the **Upgrade Assistant** tool.

For more information, please refer to the Upgrade Assistant documentation: <https://docs.tenable.com/upgrade-assistant/nessus>