



Nessus 7.0.x User Guide

Last Updated: March 19, 2019

Table of Contents

Welcome to Nessus 7.0.x	13
Get Started with Nessus	16
Navigate Nessus	17
System Requirements	18
Hardware Requirements	19
Software Requirements	22
Licensing Requirements	26
Deployment Considerations	27
Host-Based Firewalls	28
IPv6 Support	29
Virtual Machines	30
Antivirus Software	31
Security Warnings	32
Install Nessus and Nessus Agents	33
Download Nessus	34
Install Nessus	36
Install Nessus on Linux	37
Install Nessus on Windows	38
Install Nessus on Mac OS X	40
Install Nessus Agents	42
Retrieve the Linking Key	43
Install a Nessus Agent on Linux	45

Install a Nessus Agent on Windows	49
Install a Nessus Agent on Mac OS X	53
Upgrade Nessus and Nessus Agents	56
Upgrade Nessus	57
Upgrade from Evaluation	58
Upgrade Nessus on Linux	59
Upgrade Nessus on Windows	60
Upgrade Nessus on Mac OS X	61
Upgrade a Nessus Agent	62
Configure Nessus	63
Install Nessus Home, Professional, or Manager	65
Link to Tenable.io	66
Link to Nessus Manager	67
Managed by Tenable.sc	69
Manage Activation Code	70
View Your Activation Code	71
Reset Activation Code	72
Update Activation Code	73
Transfer Activation Code	75
Manage Nessus Offline	77
Install Nessus Offline	79
Generate Challenge Code	82
Generate Your License	83
Download and Copy License File (nessus.license)	84

Register Your License with Nessus	85
Download and Copy Plugins	86
Install Plugins Manually	87
Update Nessus Software Manually	89
Remove Nessus and Nessus Agents	91
Nessus Removal	92
Uninstall Nessus on Linux	93
Uninstall Nessus on Windows	95
Uninstall Nessus on Mac OS X	96
Remove Nessus Agent	97
Uninstall a Nessus Agent on Linux	98
Uninstall a Nessus Agent on Windows	99
Uninstall a Nessus Agent on Mac OS X	100
Scans	101
Scan and Policy Templates	103
Agent Templates	111
Scan and Policy Settings	113
Basic Scan Settings	114
Discovery Scan Settings	118
Assessment Scan Settings	127
Report Scan Settings	141
Advanced Scan Settings	143
Credentials	146
Cloud Services	148

Database	151
Host	154
SNMPv3	155
SSH	156
Windows	164
Miscellaneous	172
Mobile	175
Patch Management	178
Plaintext Authentication	186
Compliance	189
SCAP Settings	191
Plugins	193
Special Use Templates	194
Manage Scans	197
Create a Scan	198
Create an Agent Scan	199
Modify Scan Settings	200
Configure an Audit Trail	201
Delete a Scan	202
Scan Results	203
Dashboard	204
Vulnerabilities	206
View Vulnerabilities	207
Filter Vulnerabilities	208

Modify a Vulnerability	214
Compare Scan Results	215
Scan Folders	216
Scan Folders	218
Manage Scan Folders	220
Policies	222
Create a Policy	224
Import a Policy	225
Modify Policy Settings	226
Delete a Policy	227
About Nessus Plugins	228
Create a Limited Plugin Policy	230
Plugin Rules	234
Create a Plugin Rule	235
Modify a Plugin Rule	236
Delete a Plugin Rule	237
Customized Reports	238
Customize Report Settings	239
Scanners	240
Link Nessus Scanner	241
Enable or Disable a Scanner	242
Remove a Scanner	243
Agents	244
Modify Agent Settings	246

Filter Agents	247
Unlink an Agent	249
Agent Status	251
Agent Groups	252
Create a New Agent Group	253
Modify an Agent Group	254
Delete an Agent Group	255
Blackout Windows	256
Create a Blackout Window	257
Modify a Blackout Window	258
Delete a Blackout Window	259
Settings Page	260
Set a Master Password	261
Update Nessus Software	262
Create a New Setting	265
Modify a Setting	266
Delete a Setting	267
About	268
Advanced Settings	270
LDAP Server	285
Configure an LDAP Server	286
Proxy Server	287
Configure a Proxy Server	288
Remote Link	289

SMTP Server	292
Configure an SMTP Server	293
Custom CA	294
Add a Custom CA	295
My Account	296
Users	297
Agent Settings	298
Accounts	300
Modify Your User Account	301
Generate an API Key	302
Create a User Account	303
Modify a User Account	304
Delete a User Account	305
Scans	306
Scan and Policy Templates	308
Scan and Policy Settings	316
Basic Scan Settings	317
Discovery Scan Settings	321
Assessment Scan Settings	330
Report Scan Settings	344
Advanced Scan Settings	346
Credentials	349
Cloud Services	351
Database	354

Host	357
SNMPv3	358
SSH	359
Windows	367
Miscellaneous	375
Mobile	378
Patch Management	381
Plaintext Authentication	389
Compliance	392
SCAP Settings	394
Plugins	396
Special Use Templates	397
Unofficial PCI ASV Validation Scan	400
Manage Scans	402
Create a Scan	403
Create an Agent Scan	404
Modify Scan Settings	405
Configure an Audit Trail	406
Compare Scan Results	407
Delete a Scan	408
Scan Folders	409
Manage Scan Folders	411
Policies	413
Create a Policy	415

Modify Policy Settings	416
Delete a Policy	417
About Nessus Plugins	418
Create a Limited Plugin Policy	420
Plugin Rules	424
Create a Plugin Rule	425
Modify a Plugin Rule	426
Delete a Plugin Rule	427
Customized Reports	428
Customize Report Settings	429
Scanners	430
Enable or Disable a Scanner	431
Remove a Scanner	432
Agents	433
Modify Agent Settings	435
Filter Agents	436
Unlink an Agent	438
Agent Groups	440
Create a New Agent Group	441
Modify an Agent Group	442
Delete an Agent Group	443
Blackout Windows	444
Create a Blackout Window	445
Modify a Blackout Window	446

Delete a Blackout Window	447
Additional Resources	448
Agent Software Footprint	449
Agent Host System Utilization	450
Amazon Web Services	451
Command Line Operations	452
Start or Stop Nessus	453
Start or Stop a Nessus Agent	455
Nessus-Service	457
Nessuscli	460
Nessuscli Agent	466
Update Nessus Software	470
Default Data Directories	471
Manage Logs Using log.json	472
Nessus Credentialated Checks	477
Credentialated Checks on Windows	479
Prerequisites	482
Enable Windows Logins for Local and Remote Audits	483
Configure Nessus for Windows Logins	486
Credentialated Checks on Linux	487
Prerequisites	488
Enable SSH Local Security Checks	489
Configure Nessus for SSH Host-Based Checks	492
Run Nessus as Non-Privileged User	493

Run Nessus on Linux with Systemd as a Non-Privileged User	494
Run Nessus on Linux with init.d Script as a Non-Privileged User	497
Run Nessus on Mac OS X as a Non-Privileged User	500
Run Nessus on FreeBSD as a Non-Privileged User	505
Scan Targets	509

Welcome to Nessus 7.0.x

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

Important: Upgrade your Nessus scanners by January 31st, 2019. For more information, see the [Nessus Service Bulletin](#).

Nessus Solutions

Tenable.io

Tenable.io is a subscription based license and is available at the [Tenable Store](#).

Tenable.io 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.io 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.io 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.io subscription includes:

- Unlimited scanning of your perimeter systems
- Web application audits
- Ability to prepare for security assessments against current PCI standards
- Up to 2 quarterly report submissions for PCI ASV validation through Tenable, Inc..
- 24/7 access to the Tenable, Inc. Support Portal for Nessus knowledge base and support ticket creation

[Tenable.io Product Page](#)

[Tenable.io User Manual](#)

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](#)

Nessus Agents

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

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 are missed by traditional scanning. Nessus Agents collect vulnerability, compliance, and system data, and report that information back to a manager for analysis. With Nessus Agents, you extend scan flexibility and coverage. You can scan hosts without using credentials, as well as offline assets and endpoints that intermittently connect to the internet. You can also run large-scale concurrent agent scans with little network impact.

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. 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, Nessus Agents identify vulnerabilities, policy violations, misconfigurations, and malware on the hosts where they are installed and report results back to the managing product. You can manage Nessus Agents with Nessus Manager or Tenable.io (including Tenable.io on-prem).

[Nessus Agents Product Page](#)

Nessus Manager

Note: Nessus Manager is no longer sold as of February 1, 2018. For existing customers, service will continue to be provided through the duration of your contract. For prospective customers, please consider [Tenable.io](#) for your vulnerability management needs.

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 mis-configuration 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.io. 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.

Get Started with Nessus

1. Ensure that your setup meets the minimum system requirements:
 - [Hardware Requirements](#)
 - [Software Requirements](#)
2. Obtain the proper [Activation Code for Nessus](#).
3. Follow the installation steps depending on your Nessus software and operating system:
 - Nessus
 - [Install Nessus on Linux](#)
 - [Install Nessus on Windows](#)
 - [Install Nessus on Mac OS X](#)
 - Nessus Agent
 - [Install a Nessus Agent on Linux](#)
 - [Install a Nessus Agent on Windows](#)
 - [Install a Nessus Agent on Mac OS X](#)
4. Perform the [initial configuration steps for Nessus](#) in the web front end.
5. Create a user account.
6. [Create a scan](#).

Navigate Nessus

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



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

System Requirements

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

- [Hardware Requirements](#)
- [Software Requirements](#)
- [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 being monitored, 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 additional disk space, memory, and processing power.

Nessus Scanners and Nessus Professional

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

Scenario	Minimum Recommended Hardware
Scanning up to 50,000 hosts per scan	CPU: 4 2GHz cores Memory: 4 GB RAM (8 GB RAM recommended) Disk space: 30 GB
Scanning more than 50,000 hosts per scan	CPU: 8 2GHz cores Memory: 8 GB RAM (16 GB RAM recommended) Disk space: 30 GB (Additional space may be needed for reporting)

Nessus Manager

The following table lists the hardware requirements for Nessus Manager.

Scenario	Minimum Recommended Hardware
Nessus Manager with 0-10,000 agents	CPU: 4 2GHz cores Memory: 16 GB RAM Disk space: 30 GB (Additional space may be needed for reporting)

Scenario	Minimum Recommended Hardware
Nessus Manager with 10,001-20,000 agents	<p>CPU: 8 2GHz cores</p> <p>Memory: 64 GB RAM</p> <p>Disk space: 30 GB (Additional space may be needed for reporting)</p> <p>Note: Engage with your Tenable representative for large deployments.</p>

Virtual Machines

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

Nessus Agents

Nessus Agents are designed to be lightweight and to use only minimal system resources. Generally, a Nessus Agent uses 40 MB of RAM (all pageable). A 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 Nessus Agent resource usage, see [Agent Software Footprint](#) and [Agent Host System Utilization](#).

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

Hardware	Minimum Requirement
Processor	1 Dual-core CPU
Processor Speed	< 1 Ghz
RAM	< 1 GB
Disk Space	< 1 GB
Disk Speed	15-50 IOPS

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

Software Requirements

Nessus supports Mac, Linux, and Windows operating systems.

Nessus Scanner, Nessus Manager, and Nessus Professional

See the following table to understand the software requirements for Nessus scanners, Nessus Professional, and Nessus Manager.

Operating System	Supported Versions
32-bit Linux	<ul style="list-style-type: none">Debian 7, Debian 8, and Debian 9 / Kali Linux 1, 2017.1, and RollingRed Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)SUSE 11 and 12 EnterpriseUbuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04
64-bit Linux	<ul style="list-style-type: none">Debian 7, 8, and 9 / Kali Linux 1, 2017.1, and RollingRed Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel)FreeBSD 10 and FreeBSD 11Fedora 24 and Fedora 25SUSE 11 and SUSE 12 EnterpriseUbuntu 12.04, 12.10, 13.04, 13.10, 14.04, 16.04, and 18.04
32-bit Windows	Windows 7, Windows 8, and Windows 10
64-bit Windows	<ul style="list-style-type: none">Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016Windows 7, Windows 8, and Windows 10

Operating System	Supported Versions
	<p>Tip: Windows Server 2008 R2's bundled version of Microsoft IE does not interface with a Java installation properly. This causes Nessus to not perform as expected in some situations: Microsoft's policy recommends not using MSIE on server operating systems.</p> <p>For increased performance and scan reliability when installing on a Windows platform, Tenable highly recommends that Nessus be installed on a server product from the Microsoft Windows family such as Windows Server 2008 R2.</p>

Nessus Agents

See the following table to understand the software requirements for Nessus agents.

Operating System	Supported Versions
32-bit Linux	<ul style="list-style-type: none"> Debian 6, Debian 7, Debian 8, and Debian 9 / Kali Linux 1, 2017.3 Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) SUSE 11 Enterprise Ubuntu 9.10, Ubuntu 10.04, Ubuntu 11.04, Ubuntu 11.10, Ubuntu 12.04, Ubuntu 12.10, Ubuntu 13.04, Ubuntu 13.10, Ubuntu 14.04, Ubuntu 16.04, and Ubuntu 17.10
64-bit Linux	<ul style="list-style-type: none"> Amazon Linux 2015.03, Amazon Linux 2015.09, Amazon Linux 2017.09, and Amazon Linux 2018.03 Debian 6, Debian 7, Debian 8, and Debian 9 / Kali Linux 1, 2017.3 Fedora 20, Fedora 21, Fedora 24, Fedora 25, Fedora 26, and Fedora 27 Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)

Operating System	Supported Versions
	<ul style="list-style-type: none"> Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) SUSE 11 and SUSE 12 Enterprise Ubuntu 9.10, Ubuntu 10.04, Ubuntu 11.04, Ubuntu 11.10, Ubuntu 12.04, Ubuntu 12.10, Ubuntu 13.04, Ubuntu 13.10, Ubuntu 14.04, Ubuntu 16.04, and Ubuntu 17.10
32-bit Windows	<ul style="list-style-type: none"> Windows Server 2008 Windows Server 7, Windows Server 8, and Windows Server 10
64-bit Windows	<ul style="list-style-type: none"> Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 Windows Server 7, Windows Server 8, and Windows Server 10
Mac OS X	Mac OS X 10.8 - 10.14

Supported Web Browsers

Nessus supports the following browsers:

- Google Chrome (50+)
- Apple Safari (10+)
- Mozilla Firefox (50+)
- Internet Explorer (11+)

Note: For Nessus 7.0 and later, you must enable Transport Layer Security (TLS) 1.2 in your browser.

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.

Licensing Requirements

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

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

Additionally, your activation code:

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

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

You may purchase a 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 Nessus for updates.

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

If you are using Tenable.sc to manage your Nessus scanners, the Activation Code and plugin updates are managed from Tenable.sc. You must start Nessus before it communicates with Tenable.sc, 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.sc), 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. Any time a vulnerability scan flows through a NAT device or application proxy of some sort, the check can be distorted 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 a scan is conducted through them. Nessus has a number of 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.sc 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:

- [Host-Based Firewalls](#)
- [IPv6 Support](#)
- [Virtual Machines](#)
- [Antivirus Software](#)
- [Security Warnings](#)

Host-Based Firewalls

Port 8834

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

Allow Connections

If your Nessus server is configured 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

Nessus can be configured to work with FirewallD. When Nessus is installed on RHEL 7, CentOS 7, and Fedora 20+ systems using firewalld, firewalld can be configured 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, at least one IPv6 interface must be configured 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 credentialled scans over IPv4). Both full and compressed IPv6 notation is supported when initiating scans.

Scanning IPv6 Global Unicast IP address ranges is not supported unless the IPs are entered separately (i.e., 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**.

Virtual Machines

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.

If your anti-virus software gives a warning, select **Allow** to let Nessus continue scanning.

If your anti-virus package has an option to add processes to an exception list, add **nessusd.exe** and **nessus-service.exe**.

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 web browser saying that the SSL certificate is invalid. You may either choose to temporarily accept the risk, 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 UI ([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 expected and normal behavior.

Bypassing SSL warnings

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

Browser	Instructions
Google Chrome	Select Advanced , and then Proceed to example.com (unsafe) .
Mozilla Firefox	Select I Understand the Risks , and then select Add Exception . Next select Get Certificate , and finally select Confirm Security Exception .
Microsoft Internet Explorer	Select Continue to this website (not recommended) .

Install Nessus and Nessus Agents

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

Nessus

- [Install Nessus on Mac OS X](#)
- [Install Nessus on Linux](#)
- [Install Nessus on Windows](#)

Nessus Agents

- [Install a Nessus Agent on Mac OS X](#)
- [Install a Nessus Agent on Linux](#)
- [Install a Nessus Agent on Windows](#)

Download Nessus

Nessus products are downloaded from the [Tenable Downloads Page](#).

When downloading Nessus from the [downloads page](#), 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** and **Nessus Professional** do not have different packages; your activation code determines which Nessus product will be installed.

Example Nessus package file names and descriptions

Nessus Packages	Package Descriptions
Nessus-<version number>-Win32.msi	Nessus <version number> for Windows 7, 8, and 10 - i386
Nessus-<version number>-x64.msi	Nessus <version number> for Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, and 10 - x86-64
Nessus-<version number>-debian6_amd64.deb	Nessus <version number> for Debian 6 and 7 / Kali Linux - AMD64
Nessus-<version number>.dmg	Nessus <version number> for Mac OS X 10.8, 10.9, and 10.10 - x86-64
Nessus-<version number>-es6.i386.rpm	Nessus <version number> for Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386
Nessus-<version number>-fc20.x86_64.rpm	Nessus <version number> for Fedora 20 and 21 - x86_64
Nessus-<version number>-suse10.x86_64.rpm	Nessus <version number> for SUSE 10.0 Enterprise - x86_64
Nessus-<version number>-ubuntu1110_amd64.deb	Nessus <version number> for Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 - AMD64

Example Nessus Agent package file names and descriptions

Nessus Agent Packages	Nessus Agent Package Descriptions
NessusAgent-<version number>-x64.msi	Nessus Agent <version number> for Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, and 10 - x86-64
NessusAgent-<version number>-amzn.x86_64.rpm	Nessus Agent <version number> for Amazon Linux 2015.03, 2015.09 - x86-64
NessusAgent-<version number>-debian6_i386.deb	Nessus Agent <version number> for Debian 6 and 7 / Kali Linux - i386
NessusAgent-<version number>.dmg	Nessus Agent <version number> for Mac OS X 10.8, 10.9, and 10.10 - x86-64
NessusAgent-<version number>-es6.x86_64.rpm	Nessus Agent <version number> for Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - x86_64
NessusAgent-<version number>-fc20.x86_64.rpm	Nessus Agent <version number> for Fedora 20 and 21 - x86_64
NessusAgent-<version number>-ubuntu1110_amd64.deb	Nessus Agent <version number> for Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 - AMD64

Install Nessus

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

- [Linux](#)
- [Windows](#)
- [Mac OS X](#)

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.

Download Nessus Package File

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

Use Commands to Install Nessus

From a command prompt, run the Nessus install command specific to your operating system.

Example Nessus Install Commands

Red Hat version 6

```
# rpm -ivh 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
```

Start the Nessus Daemon

From a command prompt, restart the nessusd daemon.

Example Nessus Daemon Start Commands

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

```
# service nessusd start
```

Debian/Kali and Ubuntu

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

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

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 will be displayed and a **Status** indication bar will illustrate the installation progress. The process may take several minutes.

If presented, Install WinPcap

As part of the Nessus installation process, WinPcap needs to be installed. If WinPcap was previously installed as part of another network application, the following steps will not appear, and you will continue with the installation of Nessus.

1. On the **Welcome to the WinPcap Setup Wizard** screen, select the **Next** button.
2. On the **WinPcap License Agreement screen**, read the terms of the license agreement, and then select the **I Agree** button to continue.
3. On the **WinPcap Installation options** screen, ensure that the **Automatically start the WinPcap driver at boot time** option is checked, and then select the **Install** button.
4. On the **Completing the WinPcap Setup Wizard** screen, select the **Finish** button.
The **Tenable Nessus InstallShield Wizard Completed** screen appears.
5. Select the **Finish** button.

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

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

Install Nessus on Mac OS X

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.

Download Nessus Package File

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

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 will be displayed 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 will be 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 will be displayed and a **Status** indication bar will illustrate the remaining installation progress. The process may take several minutes.

Summary

When the installation is complete, you will see the **The installation was successful** screen.

After the installation completes, select **Close**.

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

Install Nessus Agents

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

- [Linux](#)
- [Windows](#)
- [Mac OS X](#)

Once installed, Nessus Agents are linked to Nessus Manager or Tenable.io. Linked agents automatically download plugins from the manager upon connection; this process can take several minutes and is required before an agent can return scan results.

Retrieve the Linking Key

Before you begin the Nessus Agents installation process, you must retrieve the Nessus Agent Linking Key from Nessus Manager or Tenable.io.

Use this procedure to retrieve the linking key in Nessus Manager or Tenable.io.

To retrieve the linking key:

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. In the **Linked Agents** tab, click the **setup instructions** link.

The **Agent Setup Instructions** dialog box appears.

4. Record the **host**, **port**, and **key** values.

These values differ depending on whether you are linking to Tenable.io or Nessus Manager.

Option	Set To
Link a Nessus Agent to Nessus Manager	
Host	The static IP address or hostname you set during the Nessus Manager installation.
Port	8834 (customizable)
Key	The Linking Key specific to your instance of Nessus Manager. For example: 2d38345603b5b59a4526e39640655c3288a00324097a08f7a93e5480940d1cae
Link a Nessus Agent to Tenable.io	
Host	cloud.tenable.com
Port	443
Key	The Linking Key specific to your instance of Tenable.io. For example:

Option	Set To
	2d38415603b5b59a4526e39640655c3288a00324097a08f7a93e5480940d1cae

5. Click **Close**.

Install a Nessus Agent on Linux

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

Before You Begin

[Retrieve the Nessus Agents linking key.](#)

Download the Nessus Agent

On the [Nessus Agents Download Page](#), download the package specific to your operating system.

Example Nessus Agent Package Names

[PDF version](#)

Operating System	Example Package Name
Red Hat, CentOS, and Oracle Linux	NessusAgent-<version number>-es5.x86_64.rpm NessusAgent-<version number>-es6.i386.rpm NessusAgent-<version number>-es7.x86_64.rpm
Fedora	NessusAgent-<version number>-fc20.x86_64.rpm
Ubuntu	NessusAgent-<version number>-ubuntu1110_amd64.deb NessusAgent-<version number>-ubuntu1110_i386.deb NessusAgent-<version number>-ubuntu910_amd64.deb NessusAgent-<version number>-ubuntu910_i386.deb
Debian	NessusAgent-<version number>-debian6_amd64.deb NessusAgent-<version number>-debian6_i386.deb

Install Nessus Agent

Note: The following steps require root privileges.

Using the command line interface, install the Nessus Agent.

Example Linux Install Commands

Red Hat, CentOS, and Oracle Linux

```
# rpm -ivh NessusAgent-<version number>-es6.i386.rpm  
# rpm -ivh NessusAgent-<version number>-es5.x86_64.rpm
```

Fedora

```
# rpm -ivh NessusAgent-<version number>-fc20.x86_64.rpm
```

Ubuntu

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

Debian

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

You can install a full plugins set before linking for the purpose of reducing the bandwidth impact during a mass installation. This is accomplished via the `nessuscli agent update` command with the `--file` parameter specifying the location the plugins set. This must be done prior to [starting](#) the Nessus Agent. For example:

```
/opt/nessus_agent/sbin/nessuscli agent update --file=../plugins_set.tgz
```

The plugins set must be less than five days old. A stale plugins set older than five days will force a full plugins download to occur. You can download a recent plugins set from the [Nessus Agents download page](#).

Note: After installing a Nessus Agent, you must manually start the service using the command `/sbin/service nessusagent start`.

Link Agent to Nessus Manager

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

```
/opt/nessus_agent/sbin/nessuscli agent link  
--key=00abcd00000efgh11111i0k222lmpq3333st4455u66v777777w88xy9999zabc00
```

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

The supported arguments for this command are:

Argument	Required?	Value
key	yes	Use the values you from the manager.
host	yes	
port	yes	
name	no	Specify a name for your agent. If you do not specify a name for your agent, the name defaults to the name of the computer where you are installing the agent.
groups	no	Specify existing agent group or groups where you want to add the agent. If you do not specify an agent group during the install process, you can later add your linked agent to the group in Nessus Manager or Tenable.io.
offline-install	no	For Nessus Agents 7.0.3 or later, you can install the Nessus Agent on a system even if it is offline. Add the command line option <code>offline-install="yes"</code> to the command line input. The Nessus Agent will periodically attempt to link itself to either Tenable.io or Nessus Manager. If the agent cannot connect to the controller then it retries every hour, and if the agent can connect to the controller but the link fails then it retries every 24 hours.
cloud	no	Specify the <code>--cloud</code> argument to link to Tenable.io. The <code>--cloud</code> argument is a shortcut to specifying <code>--host=t=cloud.tenable.com --port=443</code> .

If the information that you provide is incorrect, a "Failed to link agent" error appears.

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

Verify a Linked Agent

To verify a linked agent in 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. Locate the new agent in the linked agents table.

Install a Nessus Agent on Windows

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

Note: This procedure describes deploying Nessus Agents via the command line. You can also deploy Nessus Agents with a standard Windows service such as Active Directory (AD), Systems Management Server (SMS), or other software delivery system for MSI packages. For more information on deploying via these methods, see the appropriate vendor's documentation.

Before You Begin

[Retrieve the Nessus Agents linking key.](#)

Deploy and Link via the Command Line

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

```
msiexec /i NessusAgent-<version number>-x64.msi NESSUS_GROUPS="Agent Group Name"  
NESSUS_SERVER="192.168.0.1:8834" NESSUS_  
KEY=00abcd00000efgh11111i0k2221mopq3333st4455u66v777777w88xy9999zabc00 /qn
```

For Nessus Agents 7.0.3 or later, you can install the Nessus Agent on a system even if it is offline. Add the command line option NESSUS_OFFLINE_INSTALL="yes" to the command line input. The Nessus Agent will periodically attempt to link itself to either Tenable.io or Nessus Manager. If the agent cannot connect to the controller then it retries every hour, and if the agent can connect to the controller but the link fails then it retries every 24 hours.

Additionally, you can install a full plugins set before linking for the purpose of reducing the bandwidth impact during a mass installation. Add the command line option NESSUS_PLUGINS_FILEPATH-H="C:\path\to\plugins_set.tgz" where *plugins_set.tgz* is a recent plugins set tarball less than five days old. A stale plugins set older than five days will force a full plugins download to occur. You can download a recent plugins set from the [Nessus Agents download page](#).

Note: The NESSUS_GROUPS parameter accepts group names. Quotations are necessary only when listing multiple groups, or one group with spaces in its name. For example:

- GroupName
- "Group Name"
- "Group, Another Group"

The following linking parameters are also available:

- NESSUS_NAME
- NESSUS_PROXY_AGENT
- NESSUS_PROXY_PASSWORD
- NESSUS_PROXY_SERVER
- NESSUS_PROXY_USERNAME
- NESSUS_CA_PATH
- NESSUS_PLUGINS_FILEPATH
- NESSUS_PROCESS_PRIORITY

Download Nessus Agent

On the [Nessus Agents Download Page](#), download the package specific to your operating system.

Example: Nessus Agent package file

NessusAgent-<version number>-Win32.msi

Windows Server 7, and 8 (32-bit)

Start Nessus Agent Installation

1. Navigate to the folder where you downloaded the Nessus Agent installer.
2. Next, double-click the file name to start the installation process. The **Welcome to the InstallShield Wizard for Nessus Agent** window appears.

Complete the Windows InstallShield Wizard

Caution: On Windows 7 x64 Enterprise, Windows 8 Enterprise, and Windows Server 2012, you may be required to perform a reboot to complete installation.

Note: For Nessus Agents 7.0 and later, if you want to include the system tray application in your installation, see the procedure described in [System Tray Application](#).

1. In the **Welcome to the InstallShield Wizard for Nessus Agent** window, click **Next** to continue.
2. In the **License Agreement** window, read the terms of the Tenable, Inc. Nessus software license and subscription agreement.
3. Click **I accept the terms of the license agreement**.
4. Click **Next**.
5. In the **Destination Folder** window, click **Next** to accept the default installation folder.
-or-
Click **Change** to browse and select a different folder where you want to install Nessus Agents.
6. In the **Configuration Options** window, type the **Agent Key** values:

Field	Required?	Value
Key	yes	Use the values you from the manager.
Server (host)	yes	
Groups	no	Specify existing agent group(s) where you want to add the agent. If you do not specify an agent group during the install process, you can later add your linked agent to an agent group.

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

7. Click **Next**.
8. In the **Ready to Install the Program** window, click **Install**.
9. If presented with a **User Account Control** message, click **Yes** to allow the Nessus Agent to install.
10. In the **InstallShield Wizard Complete** window, click **Finish**.

Note: If you attempt to clone an Agent and link it to Nessus Manager or Tenable.io, a 409 error may appear. This error appears because another machine has been linked with the same uuid value in the HKLM\Software\Tenable\TAG file. To resolve this issue, replace the value in the HKLM\Software\Tenable\TAG file with a valid UUIDv4 value.

Verify a Linked Agent

To verify a linked agent in 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. Locate the new agent in the linked agents table.

Install a Nessus Agent on Mac OS X

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

Before You Begin

[Retrieve the Nessus Agents linking key.](#)

Download Nessus Agent

From the [Nessus Agents Download Page](#), download the package specific to your operating system.

Example: Compressed Nessus Installer File

NessusAgent-<version number>.dmg

Install Nessus Agent

Note: The following steps require root privileges.

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

GUI Installation:

1. Double-click the Nessus agent .dmg (Mac OS X Disk Image) file.
2. Double-click Install Nessus Agent.pkg.
3. Complete the **Nessus Agent Install Wizard**.

Command Line Installation:

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

Note: The .NessusAgent.pkg file is normally invisible in macOS Finder.

2. Open Terminal.

-
3. At the command prompt, enter the following command:

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

You can install a full plugins set before linking for the purpose of reducing the bandwidth impact during a mass installation. This is accomplished via the `nessuscli agent update` command with the `--file` parameter specifying the location the plugins set. This must be done prior to [starting](#) the Nessus Agent. For example:

```
/opt/nessus_agent/sbin/nessuscli agent update --file=../plugins_set.tgz
```

The plugins set must be less than five days old. A stale plugins set older than five days will force a full plugins download to occur. You can download a recent plugins set from the [Nessus Agents download page](#).

Link Agent Using Command Line Interface

To link an agent on a Mac OS X:

1. Open Terminal.
2. At the command prompt, use the `nessuscli agent link` command.

For example:

```
# /Library/NessusAgent/run/sbin/nessuscli agent link
--key=00abcd00000efgh11111i0k222lmpq3333st4455u66v777777w88xy9999zabc00
--name=MyOSXAgent --groups=All --host=yourcompany.com --port=8834
```

The supported arguments for this command are:

Argument	Required?	Value
key	yes	Use the values you from the manager.
host	yes	
port	yes	
name	no	Specify a name for your agent. If you do not specify a name for

		your agent, the name defaults to the name of the computer where you are installing the agent.
groups	no	Specify existing agent group or groups where you want to add the agent. If you do not specify an agent group during the install process, you can later add your linked agent to the group in Nessus Manager or Tenable.io.
offline-install	no	<p>For Nessus Agents 7.0.3 or later, you can install the Nessus Agent on a system even if it is offline. Add the command line option <code>NESSUS_OFFLINE_INSTALL="yes"</code> to the command line input. The Nessus Agent will periodically attempt to link itself to either Tenable.io or Nessus Manager.</p> <p>If the agent cannot connect to the controller then it retries every hour, and if the agent can connect to the controller but the link fails then it retries every 24 hours.</p>
cloud	no	<p>Specify the <code>--cloud</code> argument to link to Tenable.io.</p> <p>The <code>--cloud</code> argument is a shortcut to specifying <code>--host-t=cloud.tenable.com --port=443</code>.</p>

Verify a Linked Agent

To verify a linked agent in 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. Locate the new agent in the linked agents table.

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](#)
 - [Upgrade Nessus on Mac OS X](#)
 - [Upgrade Nessus on Linux](#)
 - [Upgrade Nessus on Windows](#)
- [Upgrade a Nessus Agent](#)

Upgrade Nessus

This section includes information for upgrading Nessus Manager and Nessus Professional.

- [Upgrade from Evaluation](#)
- [Upgrade Nessus on Linux](#)
- [Upgrade Nessus on Windows](#)
- [Upgrade Nessus on Mac OS X](#)

Upgrade from Evaluation

If you used an evaluation version of Nessus and are now upgrading to a full-licensed version of Nessus, you simply need to 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.

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, CentOS, and Oracle Linux

```
# rpm -Uvh Nessus-<version number>-es6.i386.rpm
```

SUSE version 11

```
# rpm -Uvh Nessus-<version number>-suse11.i586.rpm
```

Fedora version 20

```
# rpm -Uvh Nessus-<version number>-fc20.x86_64.rpm
```

Ubuntu version 910

```
# dpkg -i Nessus-<version number>-ubuntu910_i386.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 to 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 will appear and a **Status** indication bar will display the upgrade progress.

6. On the **Tenable Nessus InstallShield Wizard Completed** screen, select the **Finish** button.
Nessus will load in your default browser, where you can log in.

Upgrade Nessus on Mac OS X

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

Upgrade a Nessus Agent

After you install Nessus Agents, Nessus Manager or Tenable.io updates the agents automatically.

In certain cases, such as airgapped or Internet restricted networks, you may want to download application updates manually from the Tenable Support Portal.

To download agent application updates:

1. Visit the [Tenable Downloads](#) page.

2. Click **Nessus Agents**.

The latest application update files for agents are available.

3. Click the application update file that you want to download.

The **License Agreement** window appears.

4. Click **I Agree**.

The download begins automatically.

Configure Nessus

Before You Begin

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

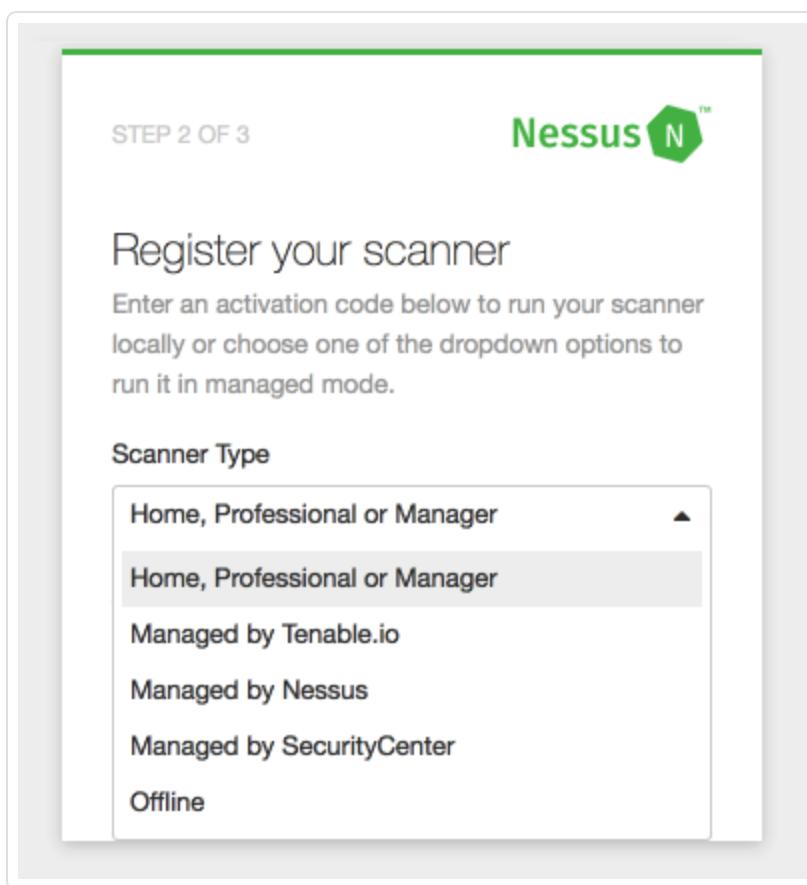
Refer to the [Security Warnings](#) section for steps necessary to bypass the SSL warnings.

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

Steps

1. On the **Create an account** window, enter a username and password for the Nessus System Administrator account.

Note: In Nessus Manager or Nessus Professional with legacy features, you can create additional Nessus System Administrator accounts after configuration.
2. Click the **Continue** button.
3. On the **Register your scanner** window, in the **Scanner Type** drop-down box, select the method by which you want to register Nessus:
 - [Nessus \(Home, Professional or Manager\)](#)
 - [Managed by Tenable.io](#)
 - [Managed by Nessus](#)
 - [Managed by Tenable.sc](#)
 - [Offline](#)



4. In the **Activation Code** box, type your activation code.

5. Click the **Continue** button.

You have successfully configured Nessus, and the Nessus web interface appears.

Install Nessus Home, Professional, or Manager

This option installs a stand-alone versions of Nessus Home, Nessus Professional, or Nessus Manager. During installation, you will be prompted to enter your Nessus [Activation Code](#); this [Activation Code](#) determines which product will be installed.

1. Select **Nessus (Home, Professional, or Manager)** from the **Registration** drop-down box.
2. Enter your **Activation Code**. The **Activation Code** is the code you obtained from the your license e-mail or from the [Tenable Downloads Page](#).
3. (Optional) Select the **Custom Settings** link to manually configure **Proxy** and **Plugin Feed** settings. Configuring **Custom Settings** allows you to override the default settings related to Nessus plugins.

Note: You may configure **Custom Host** settings only, **Plugin Feed** settings only, or both **Custom Host** and **Plugin Feed** settings.

- a. In the **Host** field, type the hostname or IP address of your proxy server.
 - b. In the **Port** field, type the Port Number of the proxy server.
 - c. In the **Username** field, type the name of a user account that has permissions to access and use the proxy server.
 - d. In the **Password**, type the password of the user account that you specified in the previous step.
 - e. In the **Plugin Feed** portion of the page, use the **Custom Host** field to enter the hostname or IP address of a custom plugin feed.
 - f. Select **Save** to commit your **Custom Settings**.
 - g. Finally, select the **Continue** button.
4. Nessus will finish the installation process; this may take several minutes.
 5. Using the System Administrator account you created, **Sign In** to Nessus.

Link to Tenable.io

During initial installation, you can install Nessus as a remote scanner linked to a Tenable.io. If you choose not to link the scanner during initial installation, you can [link your Nessus scanner later](#).

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

Before you begin

- Configure Nessus as described in [Configure Nessus](#).

To link Nessus to Tenable.io:

- On the **Register your scanner** screen, in the **Scanner Type** drop-down box, click **Link to Tenable.io**.
- In **Linking Key**, enter the linking key of your Tenable.io instance.
- (Optional) To configure more advanced settings, click **Settings**.

The **Advanced Settings** window appears.

- (Optional) Set **Proxy** settings.
 - (Optional) Set **Plugin Feed** settings.
 - (Optional) Set **Master Password** settings.
 - Click **Save**.
- Click **Continue**.

Link to Nessus Manager

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

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

Before you begin

- Configure Nessus as described in [Configure Nessus](#).

To link Nessus to Nessus Manager:

- On the **Register your scanner** screen, in the **Scanner Type** drop-down box, click **Link to Nessus Manager**.
- In the **Manager Host** box, type the host on which Nessus Manager is installed.
- In the **Manager Port** box, type 8834.
- In the **Linking Key** box, type the Linking Key that appears on the **Scanners** page in Nessus Manager.
- (Optional) Select the **Use Proxy** check box. If you select this check box, the following options appear:
 - In the **Host** box, type the host name or IP address of the proxy server.
 - In the **Port** box, type the port number of the proxy server.
 - In the **Username** box, type the username for an account that has permissions to access and use the proxy server.
 - In the **Password** box, type the password that corresponds to the user account that you specified in the previous step.
- If you want to use a custom plugin feed, click the **Advanced Settings** link.

The **Custom Host** box appears.

- In the **Custom Host** box, type the host name or IP address of a custom plugin feed.

-
- 8. Click **Save**.
 - 9. Click **Continue**.

Managed by Tenable.sc

During initial installation, you can install Nessus as a remote scanner linked to a Tenable.sc. If you choose not to link the scanner during initial installation, you can [link your Nessus scanner later](#).

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

Before you begin

- Configure Nessus as described in [Configure Nessus](#).

To link Nessus to Tenable.sc:

- On the **Register your scanner** screen, in the **Scanner Type** drop-down box, click **Managed by SecurityCenter**.
- Click **Continue**.

What to do next:

- Add the Nessus scanner to Tenable.sc as described in [Add a Nessus Scanner](#).

Manage Activation Code

To manage your activation code, use the following topics:

- [View Your Activation Code](#)
- [Reset Activation Code](#)
- [Update Activation Code](#)
- [Transfer Activation Code](#)

View Your Activation Code

View on the Support Portal

1. Navigate and log in to the [Tenable Support Portal](#).
2. In the **Main Menu** of the support portal, select the **Activation Codes**.
3. Next to your product name, select the  button to expand the product details.

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>
Mac OS X	<code># /Library/Nessus/run/sbin/nessuscli fetch --code-in-use</code>
Windows	<code>C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --code-in-use</code>

Reset Activation Code

In Nessus Manager and Nessus Professional legacy versions, if you uninstall and reinstall Nessus, you need to reset your activation code.

1. Navigate and log in to the [Tenable Support Portal](#).
2. In the **Main Menu** of the support portal, select **Activation Codes** .
3. Next to your product name, select the button to expand the product details.
4. Under the **Reset** column, select button.

Once reset, your activation code is available for use.

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

Update Activation Code

In the event that 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 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-xxxx-xxxx</code>
Mac OS X	<code># /Library/Nessus/run/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx-xxxx</code>
Windows	<code>C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register xxxx-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, you can use an activation code on multiple systems. This allows you to easily transfer a Nessus license from one system to another 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 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 web 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 **Nessus Home, 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-xxxx</code>
Mac OS X	<code># /Library/Nessus/run/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx-xxxx</code>
Windows	<code>C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register xxxx-xxxx-xxxx-xxxx-xxxx</code>

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

Manage Nessus Offline

To manage 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 follow the steps below:

1. [Generate Challenge Code](#).
2. [Generate Your License](#).
3. [Download and copy the license file \(nessus.license\)](#).

These instructions apply to Nessus 6.3 and newer and direct you to the following URL: <https://plugins.nessus.org/v2/offline.php>.

If you are using a version of Nessus 6.2 or earlier, you must use the information and instructions displayed at the following URL: <https://plugins.nessus.org/offline.php>.

4. [Register Your License with Nessus](#).
5. [Download and copy plugins to Nessus](#).
6. [Install Plugins Manually](#).
7. [Update Nessus Software Manually](#).

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, you will 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 the explanation purposes, we'll use 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 will be running 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 instructions below, we'll use computers **A** (offline Nessus server) and **B** (online computer) as examples.

1. During the [browser portion](#) of the Nessus installation, in the **Registration** drop-down, select **Offline**.
2. Once **Offline** is selected, the page displays a unique **Challenge Code**. In the example below, the challenge code is: **aaaaaaaa11b2222cc33d44e5f6666a777b8cc99999**.
This challenge code is used in the next step.
3. (Optional) Configure your Nessus setup to use Custom Settings.

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 that was displayed on the **Nessus Product Registration** screen.
Example Challenge Code: **aaaaaaaa11b2222cc33d44e5f6666a777b8cc99999**
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](#) displays 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 will download.

Tip: This custom URL is specific to your Nessus license and must be saved and used each time plugins need to be updated.

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

Use the directory specific to your operating system:

Platform	Command
Linux	# /opt/nessus/sbin/
FreeBSD	# /usr/local/nessus/sbin/
Mac OS X	# /Library/Nessus/run/sbin/
Windows	C:\Program Files\Tenable\Nessus

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 will finish 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. This identifier is called a challenge code.

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

Steps

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>
Mac OS X	<code># /Library/Nessus/run/sbin/nessuscli fetch --challenge</code>
Windows	<code>C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --challenge</code>

3. Copy the alphanumeric challenge code.

Example Challenge Code:

aaaaaaaa11b2222cc33d44e5f6666a777b8cc99999

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

Generate Your License

By default, when Nessus is installed, your license is hidden, and is automatically registered. This license is not viewable.

However, in the event that your Nessus Server is not connected to the internet (i.e., is offline) a license must be generated. This license is unique to your Nessus product and cannot be shared.

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, there is an embedded `nessus.license` file that includes the license text string displayed.

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.

Note: These instructions apply to Nessus 6.3 and newer and directs you to the following URL: <https://plugins.nessus.org/v2/offline.php>.

If you are using a version of Nessus 6.2 or earlier, you must use the information and instructions displayed on the following URL: <https://plugins.nessus.org/offline.php>.

1. While still using the computer with internet access (**B**), select the on-screen **nessus.license** link. The link will download 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
Mac OS X	# /Library/Nessus/run/etc/nessus
Windows	C:\ProgramData\Tenable\Nessus\conf

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

Register Your License with Nessus

In the event that you receive a new license and Activation Code, the license must be re-registered 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	# /opt/nessus/sbin/nessuscli fetch --register-offline /opt/nessus/etc/nessus/nessus.license
FreeBSD	# /usr/local/nessus/sbin/nessuscli fetch --register-offline /usr/local/nessus/etc/nessus/nessus.license
Mac OS X	# /Library/Nessus/run/sbin/nessuscli fetch --register-offline /Library/Nessus/run/etc/nessus/nessus.license
Windows	C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register-offline "C:\ProgramData\Tenable\Nessus\conf\nessus.license"

Download and Copy Plugins

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 must be used each time plugins need to be downloaded and updated again.

2. Next, select the on-screen custom URL link.

The link will download 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/
Mac OS X	# /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 plugins on an offline 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 Nessus user interface:

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 filename></code>
Mac OS X	<code># /Library/Nessus/run/sbin/nessuscli update <tar.gz filename></code>

Platform	Command
Windows	C:\Program Files\Tenable\Nessus>nessuscli.exe update <tar.gz <i>filename</i> >

Update Nessus Software Manually

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

1. Use the **Manual Software Update** feature in the Nessus user interface.

-or-

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>

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

Remove Nessus and Nessus Agents

This section includes information for removing Nessus and Nessus Agents.

- [Nessus Removal](#)

- [Uninstall Nessus on Mac OS X](#)
- [Uninstall Nessus on Linux](#)
- [Uninstall Nessus on Windows](#)

- [Remove Nessus Agent](#)

- [Uninstall a Nessus Agent on Mac OS X](#)
- [Uninstall a Nessus Agent on Linux](#)
- [Uninstall a Nessus Agent on Windows](#)

Nessus Removal

This section includes information for uninstalling and removing Nessus.

- [Uninstall Nessus on Linux](#)
- [Uninstall Nessus on Windows](#)
- [Uninstall Nessus on Mac OS X](#)

Uninstall Nessus on Linux

OPTIONAL: Export your Scans and Policies

1. Go to the folder(s) where your scans are stored.
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
```

Determine Nessus Package Name

From a command prompt, determine your package name.

Examples: Nessus Package Name Determination

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

```
# rpm -qa | grep Nessus
```

Debian/Kali and Ubuntu

```
# dpkg -l | grep Nessus
```

FreeBSD

```
# pkg_info | grep Nessus
```

Remove Nessus

1. Using the package name identified, use the remove command specific to your Linux-style operating system.

Examples: Nessus Remove Commands

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

```
# rpm -e <Package Name>
```

Debian/Kali and Ubuntu

```
# dpkg -r <package name>
```

FreeBSD

```
# pkg delete <package name>
```

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. 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 deletes all Nessus related files and folders.

Uninstall Nessus on Mac OS X

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 displays **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/PreferencePanes/Nessus Preferences.prefPane  
/Applications/Nessus
```

Disable the Nessus service

1. To prevent the Mac OS X 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 Agent

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

- [Uninstall a Nessus Agent on Linux](#)
- [Uninstall a Nessus Agent on Windows](#)
- [Uninstall a Nessus Agent on Mac OS X](#)

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 Nessus Agent on Linux:

1. From a command prompt, determine your package name.

Example Nessus Package Name Determination Commands

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

```
# rpm -qa | grep NessusAgent
```

Debian/Kali and Ubuntu

```
# dpkg -l | grep NessusAgent
```

FreeBSD

```
# pkg_info | grep NessusAgent
```

2. Using the package name identified, type the remove command specific to your Linux-style operating system.

Example Nessus Agent Remove Commands

Red Hat, CentOS, Oracle Linux, Fedora, SUSE

```
# rpm -e <Agent package name>
```

Debian/Kali and Ubuntu

```
# dpkg -r <Agent package name>
```

FreeBSD

```
# pkg delete <Agent package name>
```

Uninstall a Nessus Agent on Windows

Before you begin:

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

To uninstall Nessus Agent on Windows:

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 Nessus.

4. Click **Yes**.

Windows deletes all Nessus related files and folders.

Uninstall a Nessus Agent on Mac OS X

Before you begin:

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

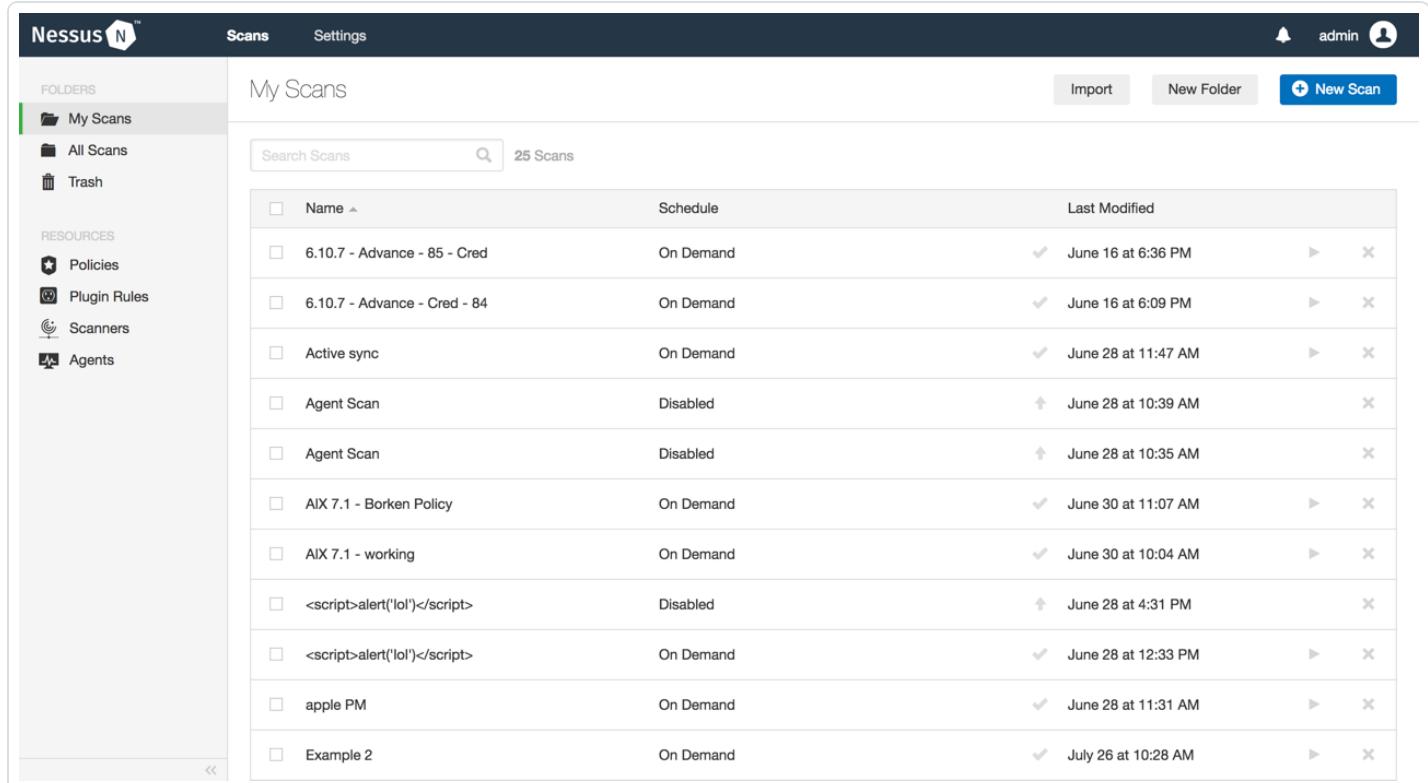
To uninstall Nessus Agent on Mac OS X:

1. Remove the Nessus directories. Using **Finder**, locate and delete the following items.
 - /Library/NessusAgent
 - /Library/LaunchDaemons/com.tenablesecurity.nessusagent.plist
 - /Library/PreferencePanes/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.

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 displays the **Folders** and **Resources** sections.



The screenshot shows the Nessus interface with the 'Scans' tab selected. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Scanners, Agents). The main area is titled 'My Scans' with a search bar and a count of 25 Scans. A table lists the scans with columns for Name, Schedule, and Last Modified. Each row has a checkbox, a preview icon, and edit/delete icons.

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

For more information, see the following sections:

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

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

Scan and Policy Templates

Templates facilitate the creation of **Scans** and **Policies**.

When you first create a **Scan** or **Policy**, the **Scan Templates** section or **Policy Templates** section appears, respectively. Templates are provided for scanners and agents. If you have created custom policies, they appear in the **User Defined** tab.

Tip: You can use the search box in the top navigation bar to filter templates in the section currently in view.

The templates that are available may vary. The Nessus interface provides brief explanations of each template in the product. This documentation includes a comprehensive explanation of the settings available for each template.

The following tables list the templates that are available in Nessus and the settings that are available for those templates.

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.

For information on agent templates, see [Agent Scan and Policy Templates](#).

Scanner Templates

Template	Description	Settings	Credentials	Compliance/SCAP
Advanced Scan	Scans without any recommendations.	All	All	All
Audit Cloud Infrastructure	Audits the configuration of third-party cloud services.	Basic: All Report: Output Advanced:	Cloud Services	AWS Microsoft Azure Rackspace Salesforce.com

Template	Description	Settings	Credentials	Compliance/SCAP
Badlock Detection	Performs remote and local checks for CVE-2016-2118 and CVE-2016-0128.	<p>Debug</p> <p><u>Basic:</u> General, Schedule, Notifications, Permissions</p> <p><u>Discovery:</u> All</p> <p><u>Assessment:</u> General, Windows, Malware</p> <p><u>Report:</u> All</p> <p><u>Advanced:</u> Debug Settings</p>	None	Unix Unix File Contents Windows Windows File Contents
Bash Shell-shock Detection	Performs remote and local checks for CVE-2014-6271 and CVE-2014-7169.	<p><u>Basic:</u> All</p> <p><u>Discovery:</u></p> <p>Scan Type</p> <p><u>Assessment:</u></p> <p>Web Applications</p> <p><u>Report:</u></p> <p>Output</p> <p><u>Advanced:</u> All</p>	<u>Database</u> <u>Host:</u> All <u>Miscellaneous</u> <u>Patch Management</u> <u>Plaintext</u> <u>Authentication</u>	None
Basic Network Scan	Performs a full system scan that is suit-	<p><u>Basic:</u> All</p> <p><u>Discovery:</u></p>	<u>Database</u> <u>Host:</u> SSH, Win-	None

Template	Description	Settings	Credentials	Compliance/SCAP
	able for any host. For example, you could use this template to perform an internal vulnerability scan on your organization's systems.	Scan Type <u>Assessment:</u> General, Brute Force, Web Applications, Windows <u>Report:</u> All <u>Advanced:</u> Scan Type	dows <u>Miscellaneous</u> <u>Patch Management</u> <u>Plaintext Authentication</u>	
Credentialed Patch Audit	Authenticates hosts and enumerates missing updates.	<u>Basic:</u> All <u>Discovery:</u> Scan Type <u>Assessment:</u> Brute Force, Windows, Malware <u>Report:</u> All <u>Advanced:</u> Scan Type	<u>Host:</u> SSH, Windows	None
DROWN Detection	Performs remote checks for CVE-2016-0800.	<u>Basic:</u> All <u>Discovery:</u> Scan Type <u>Report:</u> Output	None	None

Template	Description	Settings	Credentials	Compliance/SCAP
		<u>Advanced:</u> All		
Host Discovery	Performs a simple scan to discover live hosts and open ports.	<u>Basic:</u> All <u>Discovery:</u> Scan Type <u>Report:</u> Output <u>Advanced:</u> Performance Options	None	None
Intel AMT Security Bypass	Performs remote and local checks for CVE-2017-5689.	<u>Basic:</u> All <u>Discovery:</u> Scan Type <u>Report:</u> Output <u>Advanced:</u> All	<u>Host:</u> Windows	

Template	Description	Settings	Credentials	Compliance/SCAP
		<p>dows</p> <p>Report:</p> <p>All</p> <p>Advanced:</p> <p>Scan Type</p>		
Malware Scan	Scans for malware on Windows and Unix systems.	<p>Basic: All</p> <p>Discovery:</p> <p>Scan Type</p> <p>Assessment:</p> <p>Malware</p> <p>Report:</p> <p>Output</p> <p>Advanced:</p> <p>Scan Type</p>	<p>Host: SSH, Windows</p>	None
MDM Config Audit	Audits the configuration of mobile device managers.	<p>Basic: All</p> <p>Report:</p> <p>Output</p>	<p>Mobile</p>	Mobile Device Manager
Mobile Device Scan	Assesses mobile devices via Microsoft Exchange or an MDM.	<p>Basic: All</p> <p>Report: All</p> <p>Advanced:</p> <p>Debug</p>	<p>Miscellaneous</p> <p>Mobile</p>	None
Offline Config Audit	Audits the configuration of network devices.	<p>Basic: All</p> <p>Report: Output</p> <p>Advanced:</p>	None	Adtran AOS Bluecoat ProxySG Brocade Fabricos Check Point Gaia

Template	Description	Settings	Credentials	Compliance/SCAP
		Debug		Cisco IOS Dell Force10 FTOS Extreme ExtremeXOS Fireeye Fortigate Fortios HP Procurve Huawei VRP Juniper Junos Netapp Data Ontap Sonicwall Sonicos Watchguard
PCI Quarterly External Scan	Performs quarterly external scans as required by PCI. <div data-bbox="376 1142 670 1564" style="border: 1px solid #00AEEF; padding: 10px;"> Note: Because the nature of a PCI ASV scan is more paranoid and may lead to false positives, the scan data is not included in the aggregate Tenable.io data. This is by design. </div>	<u>Basic:</u> All <u>Discovery:</u> Host Discovery <u>Advanced:</u> Scan Type	<u>Plaintext Authentication</u> : HTTP	None
Policy Compliance Auditing	Audits system configurations against a known baseline.	<u>Basic:</u> All <u>Discovery:</u> Scan Type <u>Report:</u> Out-	<u>Database</u> <u>Host</u> <u>Host:</u> SSH, Win-	All

Template	Description	Settings	Credentials	Compliance/SCAP
		put Advanced: Scan Type	dows Miscellaneous Mobile	
SCAP and OVAL Auditing	Audits systems using SCAP and OVAL definitions.	Basic: All Discovery: Host Discovery Report: All Advanced: Scan Type	Host: SSH, Windows	SCAP Settings
Shadow Brokers Scan	Scans for vulnerabilities disclosed in the Shadow Brokers leaks.	Basic: All Discovery: Scan Type Report: Output Advanced: All	Host: SSH, Windows	None
Spectre and Meltdown	Performs remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.	Basic: All Discovery: Scan Type Report: Output Advanced: All	Host: SSH, Windows Miscellaneous Patch Management Plaintext Authentication	None
WannaCry	Scans for the Wan-	Basic: All	Host: Windows	None

Template	Description	Settings	Credentials	Compliance/SCAP
Ransomware	naCry ransomware.	<u>Discovery:</u> Scan Type <u>Report:</u> Out- put <u>Advanced:</u> All		
Web Application Tests	Scan for published and unknown web vulnerabilities.	<u>Basic:</u> All <u>Discovery:</u> Scan Type <u>Assessment:</u> General, Web Applications <u>Report:</u> All <u>Advanced:</u> All	<u>Plaintext</u> <u>Authentication</u> : HTTP	None

Agent Templates

You can use templates to create an agent scan or policy.

In both Nessus Manager and Tenable.io, default templates for agent scans appear in the **Agent** tab. The manager interface provides brief explanations of each default template.

Note: If you create custom policies for agent scans, those templates appear in the **User Defined** tab.

The table below briefly describes the settings for the default agent scan templates. You may also have access to [special templates](#).

For a comprehensive explanation of template settings, see the documentation for Nessus Manager or Tenable.io.

Template	Description	Settings	Compliance/SCAP
Advanced Agent Scan	Scans without any recommendations. Note: When you create an agent scan using the Advanced Agent Scan template, you must also select the plugins you want to use for the scan.	<u>Basic:</u> All <u>Discovery:</u> Port Scanning <u>Assessment:</u> General, Windows, Malware <u>Report:</u> All <u>Advanced:</u> Debug Settings	Unix Unix File Contents Windows Windows File Contents
Basic Agent Scan	Scans systems connected via Nessus Agents.	<u>Basic:</u> All <u>Discovery:</u> Port Scanning <u>Assessment:</u> General, Win-	None

Template	Description	Settings	Compliance/SCAP
		dows Report: All Advanced: Debug Set- tings	
Malware Scan	Scans for malware on systems connected via Nessus Agents.	Basic: All Discovery: Port Scan- ning Assessment: General, Mal- ware Report: All Advanced: Debug Set- tings	None
Policy Compliance Auditing	Audits systems connected via Nessus Agents.	Basic: All Discovery: Port Scan- ning Report: Out- put Advanced: Debug Set- tings	Unix Unix File Contents Windows Windows File Con- tents

Scan and Policy Settings

Scan or Policy **Settings** are organized into collections of configuration items, specifically **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** settings. Each of these collections are subdivided into further sections. For example, the **Basic** settings include the **General**, **Schedule**, **Notifications**, and **Permissions** sections. Additionally, the sections may contain groups of related configuration items. For example, the **Host Discovery** section contains the **General Settings**, **Ping Methods**, **Fragile Devices**, **Wake-on-LAN**, and **Network Type** groups.

The following sections of the documentation are organized to reflect the interface. For example, if you wanted to find information about the **General** section (3 in the previous image) of the **Basic** settings (2 in the previous image) that appears when you select the **Settings** tab (1 in the previous image), you should locate the table labeled [General in the Basic topic](#). The tables include subheadings to reflect groups of related configuration items that appear in a particular section.

The following settings exist for each policy, though available configuration items may vary based on the selected template:

- [Basic](#)
- [Discovery](#)
- [Assessment](#)
- [Report](#)
- [Advanced](#)

Basic Scan Settings

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

Note: Configuration items that are required by a particular scan or policy are indicated in the 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 or policy. This value is displayed on the Nessus interface.
Description	None	(Optional) Specifies a description of the scan or policy.
Folder	My Scans	Specifies the folder where the scan appears after being saved.
Dashboard	Disabled	(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	Varies	(Nessus Manager only) Specifies the scanner that performs the scan. The default scanner varies based on the organization and user.
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 hostname[ip] syntax (e.g., www.example.com [192.168.1.1]).</p>
Upload Targets	None	<p>Uploads a text file that specifies targets. 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 <p>Note: Unicode/UTF-8 encoding is not supported.</p>

Schedule

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

Setting	Default Value	Description
Frequency	Once	Specifies how often the scan is launched.

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

Notifications

Setting	Default Value	Description

Email Recipient(s)	None	Specifies zero or more email addresses, separated by commas, that are alerted when a scan completes and the results are available.
Attach Report	Off	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	Specifies the report type (CSV, Nessus, or PDF) that you want to attach to the email.
Max Attachment Size	25	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. 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.

Permission	Description
No Access	Groups and users set to No Access cannot interact with the scan in any way. When you create a scan or policy, 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.

Discovery Scan Settings

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

Note: Configuration items that are required by a particular scan or policy are indicated in the Nessus interface.

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

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

The following tables list by section all available settings. When you select any template other than Advanced Network Scan, the [**Scan Type**](#) setting also appears.

Scan Type

The **Scan Type** setting appears for all templates that have **Discovery** settings, except Advanced Network Scan. The options that are available for the **Scan Type** setting vary from template to template. The following table describes the options that are available per template. If a template is not listed in the table, no **Discovery** settings are available for that template.

The Nessus user interface provides descriptions of each option.

Note: When **Custom** is selected, the following sections appear: [**Host Discovery**](#), [**Port Scanning**](#), and [**Service Discovery**](#).

Template	Available Options
Badlock Detection	Four options are available: <ul style="list-style-type: none">• Quick• Normal (default)• Thorough• Custom
Bash Shellshock Detection	
DROWN Detection	

Basic Network Scan	Three options are available:
Basic Web App Scan	<ul style="list-style-type: none"> • Port scan (common ports) (default) • Port scan (all ports) • Custom
Credentialed Patch Audit	
Internal PCI Network Scan	
Web Application Tests	
Host Discovery	Five options are available:
	<ul style="list-style-type: none"> • Host enumeration (default) • OS Identification • Port scan (common ports) • Port scan (all ports) • Custom
Malware Scan	Three options are available:
	<ul style="list-style-type: none"> • Host enumeration (default) • Host enumeration (include fragile hosts) • Custom
Policy Compliance Auditing	Two options are available:
	<ul style="list-style-type: none"> • Default (default) • Custom
SCAP and OVAL Auditing	Two options are available:
	<ul style="list-style-type: none"> • Host enumeration (default) • Custom

Host Discovery

By default, some settings in the **Host Discovery** section are enabled. 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](#)
- [Network Type](#)

Setting	Default Value	Description
Ping the remote host	On	<p>This option enables Nessus to ping remote hosts on multiple ports to determine if they are alive. When set to On, General Settings and Ping Methods appear.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> Note: To scan VMware guest systems, Ping the remote host must be set to Off. </div>
General Settings		
Use Fast Network Discovery	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. Fast network discovery bypasses those additional tests.
Ping Methods		
ARP	Enabled	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.
TCP	Enabled	Ping a host using TCP.
Destination ports (TCP)	Built-In	Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that are checked via TCP ping.
ICMP	Enabled	Ping a host using the Internet Control Message Protocol (ICMP).
Assume ICMP unreachable from the gateway means the host is down	Disabled	Assume ICMP unreachable from the gateway means the host is down. When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When this option is enabled, when Nessus receives an ICMP Unreachable message, it considers the targeted host dead. This is to help speed up discovery on some

		<p>networks.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <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	Specifies the number of attempts to retry pinging the remote host.
UDP	Disabled	<p>Ping a host using the User Datagram Protocol (UDP).</p> <p>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	When enabled, Nessus scans network printers.
Scan Novell Netware hosts	Disabled	When enabled, Nessus scans Novell NetWare hosts.
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.
Network Type		
Network Type	Mixed	Specifies if you are using publicly routable IPs, private non-internet

	(use RFC 1918)	<p>routable IPs, or a mix of these.</p> <p>This setting has three options:</p> <ul style="list-style-type: none"> • Mixed (use RFC 1918) • Private LAN • Public WAN (internet) <p>The default value, Mixed, should be selected if you are using RFC 1918 addresses and have multiple routers within your network.</p>
--	----------------	--

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	If a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), Nessus considers it closed.
Port Scan Range	Default	<p>Two keywords can be typed into the Port scan range box.</p> <ul style="list-style-type: none"> • <i>default</i> instructs Nessus to scan approximately 4,790 commonly used ports. The list of ports can be found in the <code>nessus-services</code> file. • <i>all</i> instructs Nessus to scan all 65,536 ports, including port 0.

Setting	Default Value	Description
<p>Additionally, you can type a custom range of ports by using a comma-delimited list of ports or port ranges. For example, 21,23,25,80,110 or 1-1024,8080,9000-9200. If you wanted to scan all ports excluding port 0, you would type 1-65535.</p> <p>The custom range specified for a port scan is applied to the protocols you have selected in the Network Port Scanners 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 T:1-1024,U:300-500.</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, 1-1024,T:1024-65535,U:1025.</p>		
Local Port Enumerators		
SSH (net-stat)	Enabled	<p>This option 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 (net-stat)	Enabled	<p>A WMI-based scan uses netstat to determine open ports.</p> <p>Note: If enabled, any custom range typed in the Port Scan Range box is ignored.</p> <p>If any port enumerator (netstat or SNMP) is successful, the port range becomes <i>all</i>. Nessus still treats unscanned ports as closed if the Consider unscanned ports as closed check box is selected.</p>
SNMP	Enabled	<p>When enabled, if the appropriate credentials are provided by the user, Nessus can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the</p>

Setting	Default Value	Description
		version of the returned SNMP string. This information is necessary for these audits.
Only run network port scanners if local port enumeration failed	Enabled	Rely on local port enumeration first before relying on network port scans.
Verify open TCP ports found by local port enumerators	Disabled	If a local port enumerator (e.g., WMI or netstat) finds a port, Nessus also verifies that it is open remotely. This helps determine if some form of access control is being used (e.g., TCP wrappers, firewall).
Network Port Scanners		
TCP	Disabled	On some platforms (e.g., Windows and Mac OS X), enabling this scanner causes Nessus to use the SYN scanner to avoid serious performance issues native to those operating systems.
Override automatic firewall detection	Disabled	<p>When enabled, this setting overrides automatic firewall detection. 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. <p>This description also applies to the Override automatic firewall detection setting that is available following SYN.</p>

Setting	Default Value	Description
SYN	Enabled	Use the Nessus SYN scanner to identify open TCP ports on the target hosts. SYN scans are generally considered to be less intrusive than TCP scans depending on the security monitoring device, such as a firewall or Intrusion Detection System (IDS). The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines the port state based on a reply or lack of reply.
UDP	Disabled	<p>This option engages Nessus built-in 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	<p>Attempts to map each open port with the service that is running on that port.</p> <p>Caution: In some rare cases, probing might disrupt some services and cause unforeseen side effects.</p>
Search for	On	Controls how Nessus will test SSL-based services.

Setting	Default Value	Description
SSL based services		<p>Caution: Testing for SSL capability on all ports may be disruptive for the tested host.</p>
Search for SSL/TLS Services (enabled)		
Search for SSL/TLS on	Known SSL/TLS ports	<p>This setting has two options:</p> <ul style="list-style-type: none"> • Known SSL/TLS ports • All ports
Identify certificates expiring within x days	60	Identifies SSL and TLS certificates that are within the specified number of days of expiring.
Enumerate all SSL ciphers	True	When enabled, Nessus 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, Nessus checks that none of the identified certificates have been revoked.

Assessment Scan Settings

The **Assessment** scan settings are used for configuring 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.

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

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

Scan Type

The **Scan Type** setting contains options that vary from template to template.

The Nessus interface provides descriptions of each option. The **Custom** option displays different **Assessment** settings depending on the selected template.

Template	Available Options
Basic Network Scan	Four options are available: <ul style="list-style-type: none">• Scan for known web vulnerabilities• Scan for all web vulnerabilities (quick)• Scan for all web vulnerabilities (complex)• Custom
Basic Web App Scan	
Internal PCI Network Scan	

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, Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to Show potential false alarms then 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 Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. Not enabling Override normal accuracy is a middle ground between these two settings.
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 in some cases. 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 (e.g., a few hours ago). This can be configured 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 being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.
From address	The test messages sent to the SMTP server(s) 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 cause the account to be locked out 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		

Hydra options only appear when Hydra is installed on the same computer as the scanner or agent executing the scan.

Always enable Hydra (slow)	Disabled	Enables Hydra whenever the scan is performed.
Logins file		A file that contains user names 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 log on attempt.
Try empty passwords	Enabled	If enabled, Hydra tries user names without using a password.
Try login as password	Enabled	If enabled, Hydra tries a user name 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, only the user names specified in the logins file are used for the scan. Otherwise, additional user names discovered by other plugins are added to the logins file and used 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	Can be set to <i>Local accounts</i> , <i>Domain Accounts</i> , or <i>Either</i> .
Interpret passwords as NTLM hashes	Disabled	If enabled, Hydra interprets passwords as NTLM hashes.
Cisco login password		This password is used to log in to a Cisco system before brute forcing enable passwords. If no password is provided 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 that is protected by HTTP basic or digest authentication. If a web page is not provided 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 slave. 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.

Setting	Default Value	Description
Modbus/TCP Coil Access		Modbus uses a function code of 1 to read coils in a Modbus slave. 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.
End at Register	16	The register at which to stop scanning.
ICCP/COTP TSAP Addressing Weakness		The ICCP/COTP TSAP Addressing menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values.
Start COTP TSAP	8	Specifies the starting TSAP value to try.
Stop COTP TSAP	8	Specifies the ending TSAP value to try. All values between the Start and Stop values are tried.

Web Applications

By default, web applications are not scanned. When you first access the **Web Application** section, the **Scan Web Applications** setting appears and is set to **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 the	Disabled	This option enables Nessus to take screenshots to

Setting	Default Value	Description
cloud to take screen-shots of public web servers		<p>better demonstrate some findings. This includes some services (e.g., VNC, RDP) as well as configuration specific options (e.g., web server directory indexing). The feature only works for internet-facing hosts, as the screenshots are generated on a managed server and sent to the Nessus scanner.</p> <p>Screen shots are not exported with a Nessus scan report.</p>
Use a custom User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	Specifies which type of web browser Nessus impersonates while scanning.
Web Crawler		
Start crawling from	/	The URL of the first page that is tested. If multiple pages are required, use a colon delimiter to separate them (e.g., /:/php4:/base).
Excluded pages (regex)	/server_privileges\ .php <> log out	<p>Specifies portions of the web site to exclude from being crawled. For example, to exclude the /manual directory and all Perl CGI, set this field to: (^/manual) <> (\.pl(\?.*)?\$.).</p> <p>Nessus supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).</p>
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 selected, Nessus follows dynamic links and may exceed the parameters set above.

Setting	Default Value	Description
Application Test Settings		
Enable generic web application tests	Disabled	Enables the options listed below.
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.
Try all HTTP methods	Disabled	This option instructs Nessus to also use POST requests for enhanced web form testing. By default, the web application tests only use GET requests, unless this option is enabled. 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

Setting	Default Value	Description
Test more than one parameter at a time per form	Disabled	<p>other web servers using this option.</p> <p>This setting manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, 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, Nessus would attempt <code>/test.php?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 discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for <code>/test.php?a=a=XSS&b=3&c=3&d=3</code> when the first value of each variable is 1. • Test random combinations of three or

Setting	Default Value	Description
		<p>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.</p> <ul style="list-style-type: none"> • 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	<p>This setting determines when a new flaw is targeted. This applies at the script level. Finding an XSS flaw does not disable searching for SQL injection or header injection, but unless otherwise specified, there is at most one report for each type on a given port. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported if they were caught by the same attack.</p> <p>This setting has three options:</p> <ul style="list-style-type: none"> • Stop after one flaw is found per web server (fastest): As soon as a flaw is found on a web server by a script, 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 (e.g., XSS), Nessus switches to the next parameter of the

Setting	Default Value	Description
		<p>same CGI, the next known CGI, or to the next port or server.</p> <ul style="list-style-type: none"> • Look for all flaws (slowest): Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.
URL for Remote File Inclusion	http://rfi.nessus.org/rfi.txt	During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to use for tests. By default, 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](#)
- [Enumerate Domain Users](#)
- [Enumerate Local Users](#)

Setting	Default Value	Description
General Settings		
Request information about the SMB Domain	Enabled	If enabled, domain users are queried instead of local users.

Enumerate Domain Users		
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		
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 Whitelist 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 Whitelist 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>

Provide your own list of known bad MD5 hashes	None	Additional known bad MD5 hashes can be uploaded 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 any matches are found when scanning a target, the description appears in the scan results. Hash-delimited comments (e.g., #) can also be used in addition to the comma-delimited ones.
Provide your own list of known good MD5 hashes	None	Additional known good MD5 hashes can be uploaded 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 any matches are found when scanning a target, and a description was provided for the hash, the description appears in the scan results. Standard hash-delimited comments (e.g., #) can optionally be used in addition to the comma-delimited ones.
Hosts file whitelist	None	Nessus checks system hosts files for signs of a compromise (e.g., 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 to be ignored by Nessus during a scan. Include one IP and one hostname (formatted identically to your hosts file on the target) per line in a regular text file.
Yara Rules		
Yara Rules File	None	A .yar file containing the YARA rules to be applied in the scan. You can only upload one file per scan, so include all rules in a single file. For more information, see yara.readthedocs.io .
File System Scanning		
Scan file system	Off	Turning on this option allows you to scan system directories and files on host computers. <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> Caution: Enabling this setting in scans targeting 10 or more hosts could result in performance degradation. </div>
Scan %Systemroot%	Off	Enables file system scanning to scan %Systemroot%.

Scan %ProgramFiles%	Off	Enables file system scanning to scan %ProgramFiles%.
Scan %ProgramFiles(x86)%	Off	Enables file system scanning to scan %ProgramFiles(x86)%.
Scan %ProgramData%	Off	Enables file system scanning to scan %ProgramData%.
Scan User Profiles	Off	Enables file system scanning to scan user profiles.
Custom Filescan Directories	None	A custom file that lists directories to be scanned by malware file scanning. List each directory on one line.

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>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.
Show missing patches that have been superseded	Enabled	If enabled, includes superseded patch information in the scan report.
Hide results from plugins initiated as a dependency	Enabled	If enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disable this setting.
Output		
Allow users to edit scan 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.

Setting	Default Value	Description
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.

Advanced Scan Settings

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

The Advanced settings include the following sections:

- [**General Settings**](#)
- [**Performance**](#)
- [**Debug Settings**](#)

Scan Type

The **Scan Type** setting appears for the following templates:

- Basic Network Scan
- Basic Web App Scan
- Credentialed Patch Audit
- Internal PCI Network Scan
- Malware Scan
- PCI Quarterly External Scan
- Policy Compliance Auditing
- SCAP and OVAL Auditing

All templates that include the **Scan Type** setting have the same options:

- **Default**
- **Scan low bandwidth links**
- **Custom**

The Nessus interface provides descriptions of each option.

Note: When **Custom** is selected, the **General** section appears. The **General** section includes the settings that appear on the following table.

The following table includes the default values for the Advanced Network Scan template. Depending on the template you select, certain 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, 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 in a random order	Disabled	By default, Nessus scans a list of IP addresses in sequential order. When enabled, Nessus scans the list of hosts in a random order across the entire target IP space. This is typically useful in helping to distribute the network traffic during large scans.
Performance		
Slow down the scan when network congestion is detected	Disabled	This enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity. If detected, Nessus throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Nessus automatically attempts to use the available space within the network pipe again.
Network timeout (in seconds)	5	Specifies the time that Nessus 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 Nessus scanner will perform against a single host at one time.

Setting	Default Value	Description
Max simultaneous hosts per scan	80	Specifies the maximum number of hosts that a Nessus scanner will scan at the same time.
Max number of concurrent TCP sessions per host	none	<p>Specifies the maximum number of established TCP sessions for a 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. E.g., if this option is set to 15, the SYN scanner sends 150 packets per second at most.</p>
Max number of concurrent TCP sessions per scan	none	This setting limits the maximum number of established TCP sessions for the entire scan, regardless of the number of hosts being scanned.
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.

Credentials

When you configure a scan or policy's **Credentials**, the Nessus scanner can be granted local access to scan the target system without requiring an agent. This can facilitate scanning of a very large network to determine local exposures or compliance violations. As noted, some steps of policy creation may be optional. Once created, the policy is saved with recommended settings.

Nessus leverages the ability to log into remote Linux hosts via Secure Shell (SSH); and with Windows hosts, Nessus leverages a variety of Microsoft authentication technologies. Note that 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.

Note: By default, when creating credentialed scans or policies, hosts are identified and marked with a **Tenable Asset Identifier (TAI)**. This globally unique identifier is written to the host's registry or file system and subsequent scans can retrieve and use the TAI.

This option is enabled (by default) or disabled in the [Advanced > General Settings](#) of a scan or policy's configuration settings: **Create unique identifier on hosts scanned using credentials**

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.

The following types of credentials are managed 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 is dependent on the privileges granted to the user account. The more privileges the scanner has via the login account (e.g., 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.

Cloud Services

Nessus supports Amazon Web Services (AWS), Microsoft Azure, Rackspace, and Salesforce.com.

AWS

Users can select Amazon AWS from the Credentials menu and enter credentials for compliance auditing an account in AWS.

Option	Description
AWS Access Key ID	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>In order 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• ap-northeast-1• ap-northeast-2• ap-southeast-1

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

Option	Description
Username	Username required to log in
Password	Password associated with the username
Client Id	Microsoft Azure Client Id
Subscription IDs	List subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions will be audited.

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

Nessus supports database authentication using PostgreSQL, DB2, MySQL SQL Server, Oracle, and MongoDB.

Database

Nessus supports two authentication methods for database credentials: Password or CyberArk (Nessus Manager only).

Password

Option	Description
Username	The username for the database.
Password	The password for the supplied username.
Database Type	Nessus supports Oracle, SQL Server, MySQL, DB2, Informix/DRDA, and PostgreSQL.

CyberArk

In Nessus Manager, you have the option of using CyberArk to manage your credentials. CyberArk is a popular enterprise password vault that helps you manage privileged credentials to use in a scan.

Option	Description
Username	The target system's username.
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.
CyberArk AIM Service URL	The URL of the AIM service. By default, this field uses /AIMWebService/v1.1/AIM.asmx.

Option	Description
Central Credential Provider Username	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Central Credential Provider Password	If the CyberArk Central Credential Provider is configured 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 Private Key Passphrase	(Optional) The passphrase for the private key, if required.
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.
CyberArk Account Details Name	The unique name of the credential you want to retrieve from CyberArk.
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, select this option. Refer to the custom_CA.inc documentation for how to use self-signed certificates.
Database Type	Nessus supports Oracle, SQL Server, MySQL, DB2, Informix/DRDA, and Post-

Option	Description
	greSQL.

MongoDB

Option	Description
Username	The username for the database.
Password	The password for the supplied username.
Database	Name of the database to audit.
Port	Port the database listens on.

Host

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.

These credentials are used to obtain local information from remote systems, including network devices, for patch auditing or compliance checks.

There is a field for entering the SNMPv3 user name for the account that will perform 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.

Option	Description
Username	The username for a SNMPv3 based account.
Port	Direct Nessus to scan a different port if SNMP is running on a port other than 161.
Security level	Select the security level for SNMP: authentication, privacy, or both.
Authentication algorithm	Select MD5 or SHA1 based on which algorithm the remote service supports.
Authentication password	The password for the username specified.
Privacy algorithm	The encryption algorithm to use for SNMP traffic.
Privacy password	A password used to protect encrypted SNMP communication.

SSH

On Linux systems and supported network devices, Nessus uses Secure Shell (SSH) protocol version 2 based programs (e.g., OpenSSH, Solaris SSH, etc.) for host-based checks.

This mechanism encrypts the data in transit to protect it from being viewed by sniffer programs. Nessus supports five types of authentication methods for use with SSH: username and password, public/private keys, digital certificates, and Kerberos.

Users can select SSH settings from the **Credentials** menu and enter credentials for scanning Linux systems.

These credentials are used to obtain local information from remote Linux systems for patch auditing or compliance checks.

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

Global Credential Settings

There are four settings for SSH credentials that apply to all SSH Authentication methods.

Option	Default Value	Description
known_hosts file	none	If an SSH known_hosts file is available and provided as part of the Global Credential Settings of the scan policy in the known_hosts file field, Nessus will only attempt to log into hosts in this file. This can ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log into a system that may not be under your control.
Preferred port	22	This option can be set 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 will impersonate while scanning.
Attempt least	Cleared	Enables or disables dynamic privilege escalation. When enabled,

Option	Default Value	Description
privilege (experimental)		<p>Nessus attempts to run the scan with an account with lesser privileges, even if the Elevate privileges with option is enabled. If a command fails, Nessus will escalate privileges. Plugins 102095 and 102094 report which plugins ran with or without escalated privileges.</p> <p>Note: Enabling this option may increase scan run time by up to 30%.</p>

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, the public key is used to encrypt data and the private key is used 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. Formats from other SSH applications, including PuTTY and SSH Communications Security, must be converted to OpenSSH public key format.

The most effective credentialled 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 has been 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 only accept certain types of encryption. Check your SSH server to ensure the correct algorithm is supported.

Nessus encrypts all passwords stored in policies. However, the use of SSH keys for authentication rather than SSH passwords is recommended. This helps ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log in to a system that may not be under your control.

Note: For supported network devices, Nessus will only support the network device's username and password for SSH connections.

If an account other than root must be used for privilege escalation, it can be specified 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 or DSA Open SSH key file of the user.
Private key passphrase	Passphrase of the Private Key.
Elevate privileges with	Allows for increasing privileges once authenticated.

Certificate

Option	Description
Username	Username of the account which is being used for authentication on the host system.
User Certificate	RSA or DSA Open SSH certificate file of the user.
Private Key	RSA or DSA Open SSH key file 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
Username	The target system's username.
CyberArk AIM Service URL	The URL of the AIM service. By default, this field uses /AIMWeb-service/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 the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Central Credential Provider Password	If the CyberArk Central Credential Provider is configured 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 Private Key Passphrase	(Optional) The passphrase for the private key, if required.
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.

Option	Description
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 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 a user is granted a TGT, it can be used 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. Note that 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	This option can be set 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. Note that if you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.
Realm	The Realm is the authentication domain, usually noted as the domain name of the target (e.g., example.com).
Elevate privileges with	Allows for increasing privileges once authenticated.

If Kerberos is used, sshd must be configured with Kerberos support to verify the ticket with the KDC. Reverse DNS lookups must be properly configured 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.

Thycotic Secret Server Authentication

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 that the secret is stored as on the Thycotic server. It is referred to as the “Secret Name” on the Thycotic server.
Thycotic Secret Server URL (required)	This is used to set the transfer method, target , and target directory for the scanner. The value can be found in Admin > Configuration > Application Settings > Secret Server URL on the Thycotic server. For example consider the following address https://pw.mydomain.com/SecretServer/ . We will parse this to know that https defines it is a ssl connection, pw.mydomain.com is the target address, /SecretServer/ is the root directory.
Thycotic Login Name (required)	The username to authenticate to the Thycotic server.
Thycotic Password (required)	The password associated with the Thycotic Login Name.
Thycotic Organization (required)	This value is used in cloud instances of Thycotic to define which organization your query should hit.
Thycotic Domain (optional)	This is an optional value set if the domain value is set 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.

BeyondTrust

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.
<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>	
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 will be requested.
Use privilege escalation	If enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, it will use it for the scan.

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. Additionally, Nessus supports several different types of authentication methods for Windows-based systems: CyberArk, Kerberos, LM Hash, NTLM Hash, and Thycotic Secret Server.

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. Note that 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 a variety of 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 field is optional and Nessus will be able to log on with domain credentials without this field. 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 onto the local server, the username of Administrator is used with the password of that account. To log onto the domain, the Administrator username would also be used, but with the domain password and the name of the domain.

When multiple SMB accounts are configured, Nessus will try to log in with the supplied credentials sequentially. Once Nessus is able to authenticate with a set of credentials, it will check 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 a variety of security checks for Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 that are more accurate if a domain account is provided. Nessus does attempt to try several checks in most cases 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, Inc. blog post [Dynamic Remote Registry Auditing - Now you see it, now you don't!](#)

Credentialed scans on Windows systems require that a full administrator level account be used. 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 will 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.

Global Credential Settings

Option	Default	Description
Never send credentials in the clear	Enabled	For security reasons, Windows credentials are not sent in the clear by default.
Do not use NTLMv1 authentication	Enabled	If this option is disabled, then it is theoretically possible to trick Nessus into attempting to log into a Windows server with domain credentials via the NTLM version 1 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	Disabled	This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be run-

Option	Default	Description
Registry service during the scan		ning in order for Nessus to execute some Windows local check plugins.
Enable administrative shares during the scan	Disabled	This option will allow Nessus to access certain registry entries that can be read with administrator privileges.

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
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 the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Central Credential Provider Password	If the CyberArk Central Credential Provider is configured 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	The file that contains the PEM certificate used to communicate with the Cyber-

Option	Description
Certificate	Ark host.
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.
PolicyId	The PolicyID assigned to the credentials you would like to retrieve from the CyberArk Central Credential Provider.
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.
CyberArk Account Details Name	The unique name of the credential you want to retrieve from CyberArk.

Kerberos

Option	Default	Description
Password	none	Like with other credentials methods, this is the user password on the target system. This is a required field.
Key Distribution Center	none	This host supplies the session tickets for the user. This is a required field.

Option	Default	Description
(KDC)		
KDC Port	88	This option can be set to direct Nessus to connect to the KDC if it is running on a port other than 88.
KDC Transport	TCP	Note that 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 field.

LM Hash

Option	Description
Username	The target system's username.
Hash	Hash being utilized.
Domain	The Windows domain of the specified user's name.

NTLM Hash

Option	Description
Username	The target system's username.
Hash	Hash being utilized.
Domain	The Windows domain of the specified user's name.

Thycotic Secret Server

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	(Required) The value you want Nessus to use when setting the transfer method,

Secret Server URL	<p>target, and target directory for the scanner. Find the value on the Thycotic server, in Admin > Configuration > Application Settings > Secret Server URL.</p> <p>For example, if you type <code>https://pw.mydomain.com/SecretServer</code>, Nessus determines it is an SSL connection, that <code>pw.mydomain.com</code> is the target address, and that <code>/SecretServer</code> is the root directory.</p>
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 Nessus query should target.
Thycotic Domain	The domain, if set for the Thycotic server.
Private Key	If enabled, Nessus uses key-based authentication for SSH connections instead of password authentication.
Verify SSL Certificate	If enabled, Nessus verifies the SSL Certificate on the Thycotic server. For more information about using self-signed certificates, see Custom SSL Certificates .

BeyondTrust

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> <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>
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 will be requested.
Use privilege escalation	If enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, it will use it for the scan.

Miscellaneous

This section includes information and settings for credentials in the **Miscellaneous** pages.

ADSI

ADSI requires the domain controller information, domain, and domain admin and password.

ADSI allows Nessus to query an ActiveSync server to determine if any Android or iOS-based devices are connected. Using the credentials and server information, Nessus authenticates to the domain controller (not the Exchange server) to directly query it for device information. This feature does not require any ports be specified in the scan policy. These settings are required for mobile device scanning.

Option	Description
Domain Controller	Name of the domain controller for ActiveSync
Domain	Name of the Windows domain for ActiveSync
Domain Admin	Domain admin's username
Domain Password	Domain admin's password

Nessus supports obtaining the mobile information from Exchange Server 2010 and 2013 only; Nessus cannot retrieve information from Exchange Server 2007.

IBM iSeries

IBM iSeries only requires an iSeries username and password.

Palo Alto Networks PAN-OS

Palo Alto Networks PAN-OS requires a PAN-OS username and password, management port number, and you can enable HTTPS and verify the SSL certificate.

Red Hat Enterprise Virtualization (RHEV)

RHEV requires username, password, and network port. Additionally, you can provide verification for the SSL certificate.

Option	Description
Username	Username to login to the RHEV server. This is a required field.

Option	Description
Password	Username to the password to login to the RHEV server. This is a required field.
Port	Port to connect to the RHEV server.
Verify SSL Certificate	Verify that the SSL certificate for the RHEV server is valid.

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. Additionally, you have the option of not enabling SSL certificate verification:

Option	Description
Username	Username to login to the ESXi server. This is a required field.
Password	Username to the password to login to the ESXi server. This is a required field.
Do not verify SSL Certificate	Do not verify that the SSL certificate for the ESXi server is valid.

VMware vCenter SOAP API

VMware vCenter SOAP API allows you to access vCenter. This requires a username, password, vCenter hostname, and vCenter port.

Additionally, you can require HTTPS and SSL certificate verification.

Credential	Description
vCenter Host	Name of the vCenter host. This is a required field.
vCenter Port	Port to access the vCenter host.
Username	Username to login to the vCenter server. This is a required field.
Password	Username to the password to login to the vCenter server. This is a required field.

Credential	Description
HTTPS	Connect to the vCenter via SSL.
Verify SSL Certificate	Verify that the SSL certificate for the ESXi server is valid.

X.509

For X.509, you will need to supply the client certificate, client private key, its corresponding passphrase, and the trusted Certificate Authority's (CA) digital certificate.

Mobile

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 if 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 if 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 if 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 (required)	The Billing ID provided for MaaS360
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

MobileIron

Option	Description
VSP Admin Portal URL	The server URL Nessus uses to authenticate to the MobileIron administrator portal.
Port	(Optional) The port Nessus uses to authenticate to MobileIron (typically, port

	443).
Username	The username for the account you want Nessus to use to authenticate to MobileIron.
Password	The password for the account you want Nessus to use to authenticate to MobileIron.
HTTPS	(Optional) When enabled, Nessus uses an encrypted connection to authenticate to MobileIron.
Verify SSL Certificate	When enabled, Nessus verifies that the SSL Certificate on the server is signed by a trusted CA.

Patch Management

Nessus Manager can leverage credentials for the Red Hat Network Satellite, IBM BigFix, Dell KACE 1000, WSUS, and SCCM patch management systems to perform patch auditing on systems for which credentials may not be available to the Nessus scanner.

Options for these patch management systems can be found under **Credentials** in their respective drop-down boxes: Symantec Altiris, IBM BigFix, Red Hat Satellite Server, Microsoft SCCM, Dell KACE K1000, and Microsoft WSUS.

IT administrators are expected to manage the patch monitoring software and install any agents required by the patch management system on their systems.

Scanning with Multiple Patch Managers

If you provide multiple sets of credentials to Nessus for patch management tools, Nessus uses all of them. Available credentials are:

- Credentials supplied to directly authenticate to the target
- Dell KACE 1000
- IBM BigFix
- Microsoft System Center Configuration Manager (SCCM)
- Microsoft Windows Server Update Services (WSUS)
- Red Hat Network Satellite Server
- Symantec Altiris

If you provide credentials for a host, as well as one or more patch management systems, 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 Mac OS X systems. Nessus and Tenable.sc have the ability to query KACE K1000 to verify whether or not patches are installed on systems managed by KACE K1000 and display the patch information through the Nessus or Tenable.sc user interface.

- 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 Nessus is able to connect to the target system, it performs checks on that system and ignores KACE K1000 output.
- The data returned to Nessus by KACE K1000 is only as current as the most recent data that the KACE K1000 has obtained from its managed hosts.

KACE K1000 scanning uses four Nessus plugins.

- `kace_k1000_get_computer_info.nbin` (Plugin ID 76867)
- `kace_k1000_get_missing_updates.nbin` (Plugin ID 76868)
- `kace_k1000_init_info.nbin` (Plugin ID 76866)
- `kace_k1000_report.nbin` (Plugin ID 76869)

You must provide credentials for the Dell KACE K1000 system for K1000 scanning to work properly.

Under the **Credentials** tab, select **Patch Management**, then select **Dell KACE K1000**.

Option	Default	Description
Server	none	KACE K1000 IP address or system name. This is a required field.
Database Port	3306	Port the K1000 database is running on (typically TCP 3306).
Organization Database Name	ORG1	The name of the organization component for the KACE K1000 database. This component will begin with the letters ORG and end with a number that corresponds with the K1000 database username.
Database Username	none	Username required to log into the K1000 database. R1 is the default if no user is defined. The username will begin with the letter R. This username will end in the same number that represents the number of the organization to scan. This is a required field
K1000 Database Password	none	Password required to authenticate the K1000 Database Username. This is a required field.

IBM BigFix

IBM BigFix is available from IBM to manage the distribution of updates and hotfixes for desktop systems. Nessus and Tenable.sc have the ability to query IBM BigFix to verify whether or not patches are installed on systems managed by IBM BigFix and display the patch information.

- If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore IBM BigFix output.
- The data returned to Nessus by TEM is only as current as the most recent data that the IBM BigFix server has obtained from its managed hosts.

IBM BigFix scanning uses five Nessus plugins:

- Patch Management: Tivoli Endpoint Manager Compute Info Initialization (Plugin ID 62559)
- Patch Management: Missing updates from Tivoli Endpoint Manager (Plugin ID 62560)
- Patch Management: IBM Tivoli Endpoint Manager Server Settings (Plugin ID 62558)
- Patch Management: Tivoli Endpoint Manager Report (Plugin ID 62561)
- Patch Management: Tivoli Endpoint Manager Get Installed Packages (Plugin ID 65703)

Credentials for the IBM BigFix server must be provided for IBM BigFix scanning to work properly.

Option	Default	Description
Web Reports Server	None	Name of IBM BigFix Web Reports Server
Web Reports Port	none	Port that the IBM BigFix Web Reports Server listens
Web Reports Username	none	Web Reports administrative username
Web Reports Password	none	Web Reports administrative username's password
HTTPS	Enabled	If the Web Reports service is using SSL
Verify SSL certificate	Enabled	Verify that the SSL certificate is valid

Package reporting is supported by RPM-based and Debian-based distributions that IBM 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 IBM BigFix officially supports them, there is no support available.

For local check plugins to trigger, only RHEL, CentOS, Scientific Linux, Oracle Linux, Debian, and Ubuntu are supported. The plugin Patch Management: Tivoli Endpoint Manager Get Installed Packages must be enabled.

In order to use these auditing features, you must make changes to the IBM BigFix server. You must import a custom analysis into IBM BigFix so that detailed package information is retrieved and made

available to Nessus. Before beginning, save the following text to a file on the IBM BigFix system, and name it with a .bes extension.

```
<?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 Nessus 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>Fri, 01 Feb 2013 15:54:09 +0000</Value>
        </MIMEField>
        <Domain>BESC</Domain>
        <Property Name="Packages - With Versions (Tenable)" ID="1"><![CDATA[if
(exists true whose (if true then (exists debianpackage) else false)) then unique
values of (name of it & "|" & version of it as string & "|" & "deb" & "|" &
architecture of it & "|" & architecture of operating system) of packages whose
(exists version of it) of debianpackages else if (exists true whose (if true then
(exists rpm) else false)) then unique values of (name of it & "|" & version of it as
string & "|" & "rpm" & "|" & architecture of it & "|" & architecture of operating
system) of packages of rpm else "<unsupported>" ]]></Property>
    </Analysis>
</BES>
```

Microsoft System Center Configuration Manager (SCCM)

Microsoft System Center Configuration Manager (SCCM) is available to manage large groups of Windows-based systems. Nessus has the ability to query the SCCM service to verify whether or not patches are installed on systems managed by SCCM and display the patch information through the Nessus or Tenable.sc web interface.

- If the credentialed check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore SCCM output.

- The data returned by SCCM is only as current as the most recent data that the SCCM server has obtained from its managed hosts.
- Nessus connects to the server that is running the SCCM site (e.g., credentials must be valid for the SCCM service, meaning an admin account in SCCM with the privileges to query all the data in the SCCM MMC). This server may also run the SQL database, or the database as well as the SCCM repository can be on separate servers. When leveraging this audit, Nessus must connect to the SCCM Server, not the SQL or SCCM server if they are on a separate box.

Nessus SCCM patch management plugins support SCCM 2007 and SCCM 2012.

SCCM scanning is performed using four Nessus plugins.

- Patch Management: SCCM Server Settings (Plugin ID 57029)
- Patch Management: Missing updates from SCCM(Plugin ID 57030)
- Patch Management: SCCM Computer Info Initialization(Plugin ID 73636)
- Patch Management: SCCM Report(Plugin ID 58186)

Credentials for the SCCM system must be provided for SCCM scanning to work properly. Under the Credentials tab, select Patch Management and then Microsoft SCCM.

Credential	Description
Server	SCCM IP address or system name
Domain	The domain the SCCM server is a part of
Username	SCCM admin username
Password	SCCM admin password

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. Nessus and Tenable.sc have the ability to query WSUS to verify whether or not patches are installed on systems managed by WSUS and display the patch information through the Nessus or Tenable.sc web interface.

- If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore WSUS output.

- The data returned to Nessus by WSUS is only as current as the most recent data that the WSUS server has obtained from its managed hosts.

WSUS scanning is performed using three Nessus plugins.

- Patch Management: WSUS Server Settings (Plugin ID 57031)
- Patch Management: Missing updates from WSUS (Plugin ID 57032)
- Patch Management: WSUS Report (Plugin ID 58133)

Credentials for the WSUS system must be provided for WSUS scanning to work properly. Under the Credentials tab, select Patch Management and then Microsoft WSUS.

Credential	Default	Description
Server	None	WSUS IP address or system name
Port	8530	Port WSUS is running on (typically TCP 80 or 443)
Username	none	WSUS admin username
Password	none	WSUS admin password
HTTPS	Enabled	If the WSUS service is using SSL
Verify SSL certificate	Enabled	Verify that the SSL certificate is valid

Red Hat Satellite Server

Red Hat Satellite is a systems management platform for Linux-based systems. Nessus has the ability to 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, Inc., the RHN Satellite plugin will also work with Spacewalk Server, the Open Source Upstream Version of Red Hat Satellite. Spacewalk has the capability of managing distributions based on Red Hat (RHEL, CentOS, Fedora) and SUSE. Tenable supports the Satellite server for Red Hat Enterprise Linux.

- If the credential check sees a system, but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore RHN Satellite output.
- The data returned to Nessus by RHN Satellite is only as current as the most recent data that the Satellite server has obtained from its managed hosts.

Satellite scanning is performed using five Nessus plugins:

- Patch Management: Patch Schedule From Red Hat Satellite Server (Plugin ID 84236)
- Patch Management: Red Hat Satellite Server Get Installed Packages (Plugin ID 84235)
- Patch Management: Red Hat Satellite Server Get Managed Servers (Plugin ID 84234)
- Patch Management: Red Hat Satellite Server Get System Information (Plugin ID 84237)
- Patch Management: Red Hat Satellite Server Settings (Plugin ID 84238)

If the RHN Satellite server is version 6, three additional Nessus plugins are used:

- Patch Management: Red Hat Satellite Server Get Installed Packages (Plugin ID 84231)
- Patch Management: Red Hat Satellite 6 Settings (Plugin ID 84232)
- Patch Management: Red Hat Satellite 6 Report (Plugin ID 84233)

Red Hat Satellite 6 Server

Credential	Default	Description
Satellite server	none	RHN Satellite IP address or system name
Port	443	Port Satellite is running on (typically TCP 80 or 443)
Username	none	Red Hat Satellite username
Password	none	Red Hat Satellite password
HTTPS	Enabled	If the Red Hat Satellite service is using SSL
Verify SSL Certificate	Enabled	Verify that the SSL certificate is valid

Symantec Altiris

Altiris is available from Symantec to manage the distribution of updates and hotfixes for Linux, Windows, and Mac OS X systems. Nessus and Tenable.sc have 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 Nessus or Tenable.sc web interface.

- If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore Altiris output.

- The data returned to Nessus by Altiris is only as current as the most recent data that the Altiris has obtained from its managed hosts.
- Nessus connects to the Microsoft SQL server that is running on the Altiris host (e.g., credentials must be valid for the MSSQL database, meaning a database account with the privileges to query all the data in the Altiris MSSQL database). The database server may be run on a separate host from the Altiris deployment. When leveraging this audit, Nessus must connect to the MSSQL database, not the Altiris server if they are on a separate box.

Altiris scanning is performed using four Nessus plugins.

- `symantec_altiris_get_computer_info.nbin` (Plugin ID 78013)
- `symantec_altiris_get_missing_updates.nbin` (Plugin ID 78012)
- `symantec_altiris_init_info.nbin` (Plugin ID 78011)
- `symantec_altiris_report.nbin` (Plugin ID 78014)

Credentials for the Altiris Microsoft SQL (MSSQL) database must be provided for Altiris scanning to work properly. Under the Credentials tab, select Patch Management and then Symantec Altiris.

Credential	Default	Description
Server	none	Altiris IP address or system name. This is a required field.
Database Port	5690	Port the Altiris database is running on (Typically TCP 5690)
Database Name	Symantec_CMDB	The name of the MSSQL database that manages Altiris patch information.
Database User-name	None	Username required to log into the Altiris MSSQL database. This is a required field.
Database Pass-word	none	Password required to authenticate the Altiris MSSQL database. This is a required field.
Use Windows Authentication	Disabled	Denotes whether or not to use NTLMSSP for compatibility with older Windows Servers, otherwise it will use Kerberos

To ensure Nessus can properly utilize Altiris to pull patch management information, it must be configured to do so.

Plaintext Authentication

Caution: Using plaintext credentials is not recommended. Use encrypted authentication methods when possible.

If a secure method of performing credential 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, SNMPv1/v2c, and telnet/rsh/rexec.

By supplying credentials, Nessus may have the ability to do more extensive checks to determine vulnerabilities. HTTP credentials supplied will be used 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 (e.g., Authentication failed!).
Use authenticated regex on HTTP headers	Disabled	Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to better determine authentication state.

Option	Default	Description
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, e.g., /login.html.
Login submission page	The action parameter for the form method. For example, the login form for <form method="POST" name="auth_form" action="/login.php"> would be /login.php.
Login parameters	Specify the authentication parameters (e.g., login=%USER%&password=%PASS%). If the keywords %USER% and %PASS% are used, they will be substituted with values supplied on the Login configurations drop-down box. This field can be used to provide more than two parameters if required (e.g., a group name or some other piece of information is required for the authentication process).
Check authentication on	The absolute path of a protected web page that requires authentication, to better assist Nessus in determining authentication status, e.g., /admin.html.

Option	Description
page	
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 (e.g., web browser, web proxy, etc.) with the HTTP cookies import settings. A cookie file can be uploaded so that Nessus uses the cookies when attempting to access a web application. The cookie file must be in Netscape format.

telnet/rsh/rexec

The telnet/rsh/rexec authentication section is also username and password, but there are additional 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. Up to 4 SNMP community strings can be configured.

Compliance

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.

The advantage of using Nessus to perform vulnerability scans and compliance audits is that all of this data can be obtained at one time. Knowing how a server is configured, how it is patched and what vulnerabilities are present can help 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.

Audit Capability	Required Credentials
Adtran AOS	SSH
Amazon AWS	Amazon AWS
Blue Coat ProxySG	SSH
Brocade FabricOS	SSH
Check Point GAiA	SSH
Cisco IOS	SSH
Citrix XenServer	SSH
Database	Database credentials
Dell Force10 FTOS	SSH
Extreme ExtremeXOS	SSH
FireEye	SSH
Fortigate FortiOS	SSH
HP ProCurve	SSH

Huawei	SSH
IBM iSeries	IBM iSeries
Juniper Junos	SSH
Microsoft Azure	Microsoft Azure
Mobile Device Manager	AirWatch/Apple Profile Manager/MobileironÂ
MongoDB	MongoDB
NetApp Data ONTAP	SSH
Palo Alto Networks PAN-OS	PAN-OS
Rackspace	Rackspace
RHEV	RHEV
Salesforce.com	Salesforce SOAP API
SonicWALL SonicOS	SSH
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

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 settings for each option are described in the following table.

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	<p>(SCAP Version 1.2 only) The Data Stream ID that you copied from the SCAP XML file.</p> <p>Example:</p> <div style="border: 1px solid #ccc; padding: 10px;"><pre><data-stream id="scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip"></pre></div>
SCAP Benchmark ID	None	<p>The Benchmark ID that you copied from the SCAP XML file.</p> <p>Example:</p> <div style="border: 1px solid #ccc; padding: 10px;"><pre><xccdf:Benchmark id="xccdf_gov.nist_benchmark_USGCB-Windows-7"></pre></div>
SCAP Profile ID	None	<p>The Profile ID that you copied from the SCAP XML file.</p> <p>Example:</p>

		<xccdf:Profile id="xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1">
OVAL Result Type	Full results w/ system characteristics	<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 enables you to select security checks by **Plugin Family** or individual plugins checks.

Clicking on the **Plugin Family** allows you to enable (**green**) or disable (**gray**) the entire family. Selecting a family displays the list of its plugins. Individual plugins can be enabled or disabled to create very specific scans.

A family with some plugins disabled is **blue** and displays **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** displays the plugin output that would be seen in a report.

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

When a scan or policy is created and saved, it records all of the plugins that are initially selected. When new plugins are received via a plugin update, they are automatically enabled if the family they are associated with is enabled. If the family has been disabled or partially enabled, new plugins in that family are also automatically disabled.

Caution: The **Denial of Service** family contains some plugins that could cause outages on a network if the Safe Checks option is not enabled, in addition to some useful checks that will not cause any harm. The **Denial of Service** family can be used in conjunction with Safe Checks to ensure that any potentially dangerous plugins are not run. However, it is recommended that the **Denial of Service** family not be used on a production network unless scheduled during a maintenance window and with staff ready to respond to any issues.

Special Use Templates

Note: For more information about performing custom audits with Nessus, see the [Custom Auditing video](#).

Compliance

Nessus compliance auditing can be configured using one or more of the following **Scanner** and **Agent** templates.

- Audit Cloud Infrastructure
- MDM Config Audit
- Offline Config Audit
- SCAP and OVAL Auditing
- Policy Compliance Auditing

Mobile Device

With Nessus Manager, the Nessus Mobile Devices plugin family provides the ability to obtain information from devices registered in a Mobile Device Manager (MDM) and from Active Directory servers that contain information from Microsoft Exchange Servers.

- To query for information, the Nessus scanner must be able to reach the Mobile Device Management servers. You must ensure no screening devices block traffic to these systems from the Nessus scanner. In addition, Nessus must be given administrative credentials (e.g., domain administrator) to the Active Directory servers.
- To scan for mobile devices, Nessus must be configured with authentication information for the management server and the mobile plugins. Since Nessus authenticates directly to the management servers, a scan policy does not need to be configured to scan specific hosts.
- For ActiveSync scans that access data from Microsoft Exchange servers, Nessus will retrieve information from phones that have been updated in the last 365 days.

Payment Card Industry (PCI)

Tenable offers two **Payment Card Industry Data Security Standard (PCI DSS)** templates: one for testing internal systems (11.2.1) and one for Internet facing systems (11.2.2). Also, these scan templates

may also be used to complete scans after significant changes to your network, as required by PCI DSS 11.2.3.

Template	Product	Description
PCI Quarterly External Scan	Tenable.io Only	<p>The PCI Quarterly External Scan template is only available in Tenable.io. Using this template, Tenable.io tests for all PCI DSS external scanning requirements, including web applications.</p> <p>The scan results obtained using the PCI Quarterly External Scan template may be submitted to Tenable, Inc. (an Approved Scanning Vendor) for PCI validation.</p> <p>Refer to the Scan Results section for details on creating, reviewing, and submitting PCI scan results.</p>
PCI Quarterly External Scan (Unofficial)	Nessus Manager	For Nessus Manager and Nessus Professional versions, Tenable provides the PCI Quarterly External Scan (Unofficial) template.
	Nessus Professional	<p>This template can be used to simulate an external scan (PCI DSS 11.2.2) to meet PCI DSS quarterly scanning requirements. However, the scan results from the Unofficial template cannot be submitted to Tenable, Inc. for PCI Validation.</p> <p>The PCI Quarterly External Scan (Unofficial) Template performs the identical scanning functions as the Tenable.io version of this template.</p>
PCI Quarterly External Scan (Unofficial)	Nessus Manager	The Internal PCI Network Scan template can be used to meet PCI DSS Internal scanning requirement (11.2.1).
	Nessus Professional	

SCAP and OVAL

The National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) is a set of policies for managing vulnerabilities and policy compliance in government agencies. It relies on multiple open standards and policies, including OVAL, CVE, CVSS, CPE, and FDCC policies.

- SCAP compliance auditing requires sending an executable to the remote host.
- Systems running security software (e.g., McAfee Host Intrusion Prevention), may block or quarantine the executable required for auditing. For those systems, an exception must be made for the 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.

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](#)

Create a 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 scan template that you want to use.

4. Configure the scan's [settings](#).

5. If you want to launch the scan later, click the **Save** button.

The scan is saved.

-or-

If you want to launch the scan immediately, click the  button, and then click **Launch**.

The scan is saved and launched.

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. If you want to launch the scan later, click the **Save** button.

Tenable.io saves the scan.

-or-

If you want to launch the scan immediately, click the  button, then click **Launch**.

Tenable.io saves and launches the scan.

Modify Scan Settings

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. 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.

The settings are saved.

Configure an Audit Trail

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. (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, which displays the results that match the criteria that you entered in one or both boxes.

Delete a Scan

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. 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 permanently delete the scan, 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 permanently delete, click the  button.

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

6. Click the **Delete** button.

The scan is deleted.

Tip: On the **Trash** page, in the upper right corner, click the **Empty Trash** button to permanently delete all scans in 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.

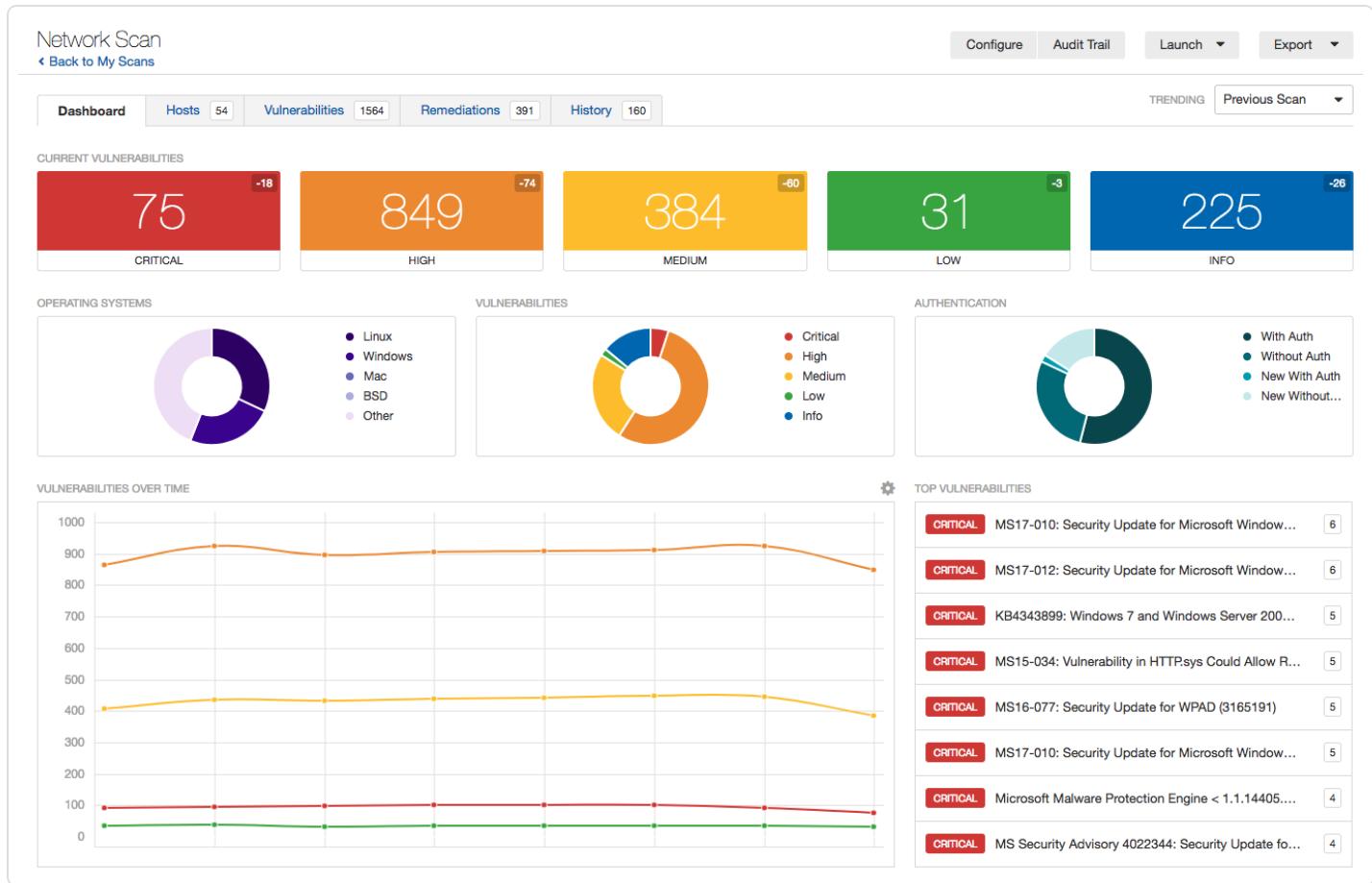
You can view scan results in one of several views:

Page	Description
Dashboard	In Nessus Manager, the default scan results page displays the Dashboard view.
Hosts	The Hosts page displays all scanned targets. If the scan is configured for compliance scanning, the button allows you to navigate between the Compliance and Vulnerability results.
Vulnerabilities	List of identified vulnerabilities, sorted by severity.
Compliance	If the scan includes compliance checks, this list displays counts and details sorted by vulnerability severity.
Remediations	If the scan's results include Remediation information, this list displays all remediation details, sorted by the number of vulnerabilities.
Notes	The Notes page displays additional information about the scan and the scan's results.
History	The History displays a listing of scans: Start Time , End Time , and the Scan Statuses .

Dashboard

In Nessus Manager, you can configure a scan to display the scan's results in an interactive dashboard view.

Based on the type of scan performed and the type of data collected, the dashboard displays key values and trending indicators.



Dashboard View

Based on the type of scan performed and the type of data collected, the dashboard displays key values and a trending indicator.

Dashboard Details

Name	Description

Current Vul-nerabilities	The number of vulnerabilities identified by the scan, by severity.
Operating Sys-tem Com-parison	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. At least 2 scans must be completed for this chart to appear.
Top Hosts	Top 8 hosts that had the highest number of vulnerabilities found in the scan.
Top Vul-nerabilities	Top 8 vulnerabilities based on severity.

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

Severity	Plugin Name	Plugin Family	Count	Host Details
INFO	Common Network Enumeration (CPE)	General	1	IP: DNS: 00:00:00:00:2f:af
INFO	Device Type	General	1	MAC: OS: Microsoft Windows 10 Service Pack 2
INFO	Ethernet Card Manufacturer Detection	Mac	1	Model: Intel PRO/100 MT Desktop Systems
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	Start: Today at 01:23 AM End: Today at 01:23 AM
INFO	ICMP Timeouting Request Remote Date Disclosure	General	1	Request Type: ICMP Response Type: ICMP
INFO	Microsoft Windows SMB Log-in Possible	Windows	1	
INFO	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Windows	1	
INFO	Microsoft Windows SMB NULL Session Authentication	Windows	1	
INFO	Microsoft Windows SMB Registry - Nessus Cannot Access the Windows Registry	Windows	1	
INFO	Microsoft Windows SMB Service Detection	Windows	2	
INFO	Microsoft Windows XP Unencrypted Installation Detection	Windows	1	
INFO	MS18-067 Microsoft Windows Server Crafted RPC Request Handling Remote Code Execution (55864) (unauthenticated check)	Windows	1	
INFO	MS19-005 Microsoft Windows SMB Vulnerabilities Remote Code Execution (55868) (unauthenticated check)	Windows	1	
INFO	Nessus Scan Information	Settings	1	
INFO	Nessus STIX scanner	Port scanners	3	
INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1	

Details of a single host's plugin scan result

Description: The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

Solution: Apply the following registry changes per the referenced Technet articles:
Set:
- HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Lsa\Restriction\maxLogins
- HKEY_LOCAL_MACHINE\CurrentControlSet\Services\lanmanserver\parameters\restrictNullSessionSuccess=1
Remove BROWSE from:
- HKEY_LOCAL_MACHINE\CurrentControlSet\Services\lanmanserver\parameters\allowSessionPipes
Restart once the registry changes are complete.

See Also:
<http://support.microsoft.com/kb/187878/>
<http://support.microsoft.com/kb/184282/>
[http://technet.microsoft.com/en-us/library/cc789986\(ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc789986(ws.10).aspx)

Output:
It was possible to bind to the 'lbcnneer' pipe.

Reference Information:
CVE: CVE-1999-0518, CVE-1999-0520, CVE-2002-1117
CVSS Base Score: 3.0
CVSS Vector: CVSS2#AV:N/AC:L/C/N/C/N/A/N
CVSS Temporal Score: CVSS3#E/D/U/R/C/D
CVSS Temporal Vector: 4.3

For information on managing vulnerabilities, see:

- [View Vulnerabilities](#)
- [Filter Vulnerabilities](#)
- [Modify a Vulnerability](#)

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.

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:

- Click a specific host to view vulnerabilities found on that host.
- Click the **Vulnerabilities** tab to view all vulnerabilities.

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, displaying plugin information and output for each instance on a host.

Filter Vulnerabilities

You can search or use filters to view specific scan results. You can filter results based on different vulnerability attributes, and you can create detailed and customized scan result views by using multiple filters.

To search for vulnerabilities:

1. Do one of the following:
 - In scan results, 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 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.

The **Filter** window appears.
3. 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**, 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.

5. Click **Apply**.

Your filter is applied and the table displays vulnerabilities that match your filters.

To remove filters:

1. Click **Filter** next to the search box.

The **Filter** window appears.

2. To remove a single filter, click **X** next to the filter entry.
3. To remove all filters, click **Clear Filters**.

The filters are removed from the vulnerabilities displayed 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 (e.g., 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 (e.g., 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 (e.g., 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 (e.g., 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 (e.g., 5).</p> <p>This filter can be used 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 will be flagged 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 (e.g., 3.3).
CVSS Temporal Vector	Filter results based on if a CVSS v2.0 temporal vector is equal to, is not equal to, contains, or does not contain a given string (e.g., 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 (e.g., 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 (e.g., 5).</p> <p>This filter can be used 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 will be flagged 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 (e.g., 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 (e.g., 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 (e.g., 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 (e.g., 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 (e.g., 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 (e.g., 192.168 or lab).
IAVA	Filter results based on if an IAVA reference is equal to, is not equal to, contains, or does not contain a given string (e.g., 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 (e.g., 2012-A-0008).
IAVM Severity	Filter results based on the IAVM severity level (e.g., 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 (e.g., 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 (e.g., 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 (e.g., 12/01/2011).
Plugin Description	Filter results if Plugin Description contains, or does not contain a given string (e.g., remote).
Plugin Family	Filter results if Plugin Name is equal to or is not equal to one of the designated Nessus plugin families. The possible matches are provided 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 (e.g., 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 (e.g., 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 (e.g., windows).
Plugin Output	Filter results if Plugin Description is equal to, is not equal to, contains, or does not contain a given string (e.g., 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 (e.g., 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 (e.g., 80).
Protocol	Filter results if a protocol is equal to or is not equal to a given string (e.g., http).
Risk Factor	Filter results based on the risk factor of the vulnerability (e.g., 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 (e.g., 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 (e.g., seclists.org).
Solution	Filter results if the plugin solution contains or does not contain a given string (e.g., upgrade).
Synopsis	Filter results if the plugin synopsis contains or does not contain a given string (e.g., PHP).
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 (e.g., 01/01/2012). <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> Note: Pressing the button next to the date will bring up a calendar interface for easier date selection. </div>

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, it cannot be recovered and you accept its associated risks.

6. (Optional) Select **Apply this rule to all future scans**.

If you select this option, Nessus modifies this vulnerability for all future scans. Nessus does not modify vulnerabilities found in past scans.

7. Click **Save**.

The vulnerability updates with your setting.

Compare Scan Results

You can compare two scan results to see differences between them. The comparison shows what is new since the baseline (i.e., the primary result selected), not a differential of the two results. You cannot compare imported scans or more than two scans.

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 new vulnerabilities are found, or how two scans may not be targeting the same hosts.

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 a scan baseline for the comparison, then click **Continue**.

The scan result differences are displayed.

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 cannot be removed:

- My Scans
- All Scans
- Trash

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 displays 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 displays scans that you have deleted. In the **Trash** folder, you can permanently remove scans from your Nessus instance, or restore the scans to a selected folder. If you delete a folder that contains scans, all scans in that folder are moved to the **Trash** folder. Scans stored in the **Trash** folder are automatically deleted after 30 days.

My Scans

[Import](#)[New Folder](#)[!\[\]\(d6c8ae51752fdcd93110a0e7e996b424_img.jpg\) New Scan](#)

Total Records: 2



<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		

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 cannot be removed:

- My Scans
- All Scans
- Trash

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 displays 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 displays scans that you have deleted. In the **Trash** folder, you can permanently remove scans from your Nessus instance, or restore the scans to a selected folder. If you delete a folder that contains scans, all scans in that folder are moved to the **Trash** folder. Scans stored in the **Trash** folder are automatically deleted after 30 days.

My Scans

[Import](#)[New Folder](#)[!\[\]\(43996c3e78376a0bef83304b845ca0d8_img.jpg\) 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

These procedures can be performed by a standard user or administrator.

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.

The folder is created and appears 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.

The folder is deleted. If the folder contained scans, those scans are moved to the **Trash** folder.

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 the [Scan and Policy Templates](#) topic.

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 (e.g., 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.

The policy is saved.

Import a Policy

You can import a scan or policy that was [exported](#) as a Nessus report (.nessus file) 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 select window appears.

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

Note: You can import only .nessus file types as a policy.

Nessus imports the file as a policy.

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

Modify Policy Settings

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. 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.

The settings are saved.

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  button.

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

4. Click the **Delete** button.

The policy is deleted.

About Nessus Plugins

As information about new vulnerabilities are discovered and released into the general public domain, Tenable, Inc. research staff designs programs to enable Nessus to detect them.

These programs are named *plugins*, and are written in the Nessus proprietary scripting language, called *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.

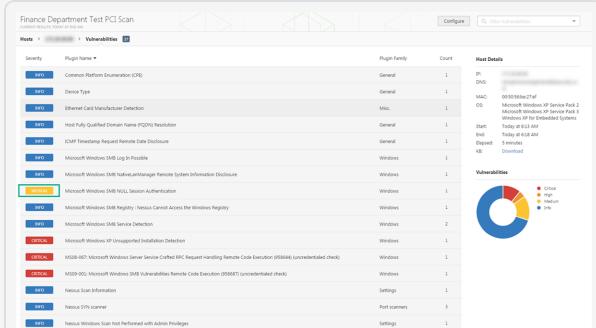
Nessus supports the Common Vulnerability Scoring System (CVSS) and supports both v2 and v3 values simultaneously. If both CVSS2 and CVSS3 attributes are present, both scores are calculated. However in determining the Risk Factor attribute, currently the CVSS2 scores take precedence.

Plugins also are utilized to obtain configuration information from authenticated hosts to leverage 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](#).

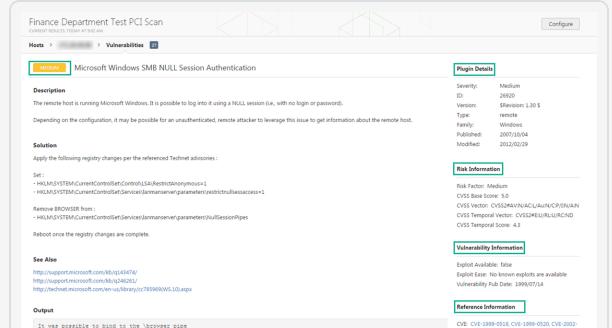
Example Plugin Information

List of a single host's scan results by plugin severity and plugin name



Severity	Plugin Name	Count
Critical	Common Platform Enumeration (CPE)	1
High	Ethernet Card Manufacturer Selection	1
Medium	Host Fully Qualified Domain Name (FQDN) Resolution	1
Low	ICMP Veneering Request Remote Denial of Service Disclosure	1
Critical	Microsoft Windows SMB Log In Possible	1
Medium	Microsoft Windows SMB NetshareManager Remote System Information Disclosure	1
Critical	Microsoft Windows SMB NULL Session Authentication	1
Medium	Microsoft Windows SMB Registry - Service Cannot Access the Windows Registry	1
Low	Microsoft Windows SMB Service Detection	1
Critical	Microsoft Windows XP Unsigned Installation Detection	1
Critical	MISB-001 Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (95864) (unauthenticated check)	1
Critical	MISB-002 Microsoft Windows SMB Vulnerabilities Remote Code Execution (95867) (unauthenticated check)	1
Medium	Nessus Scale Information	1
Low	Nessus SIDS scanner	1
Low	Nessus Windows Scan Test Performed with Admin Privileges	1

Details of a single host's plugin scan result



Plugin Details

Severity	Medium
Plugin ID	001
Version	Shivam: 1.0.0
Type	remote
Family	Vulnerabilities
Published	2012/10/04
Modified	2012/02/02

Risk Information

Risk Factor	Medium
CVSS Base Score	6.8
CVSS Temporal Vector	CVSS:3.0/EU/UR/RC/ND
CVSS Temporal Score	4.3

Vulnerability Information

Exploit Available	No
Exploit Ease	No known exploits are available
Vulnerability Pub Date	1999/07/14

Reference Information

CVE	CVE-1999-0518, CVE-1999-0520, CVE-2002-1117
CVSS	CVSS:2.0/AV/N/AC/N/C/P/IN/N/A
CVSS Temporal Vector	CVSS:2.0/EU/UR/RC/ND
CVSS Temporal Score	4.3

How do I get Nessus Plugins?

By default, plugins are set for automatic updates and Nessus 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 manually download plugins. 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.

Tip: Plugins are obtained from port 443 of plugins.nessus.org, plugins-customers.nessus.org, or plugins-us.nessus.org.

How do I update Nessus Plugins?

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

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

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, all of the plugin families are enabled.

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.

All the plugin families are disabled.

New Policy / Advanced Scan

[Back to Policy Templates](#)

Disable All | Enable All

Show Enabled | Show All

Settings	Credentials	Compliance	Plugins
No plugin family selected.			
STATUS	PLUGIN FAMILY	TOTAL	STATUS
DISABLED	AIX Local Security Checks	11384	
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

7. Click the plugin family that you want to include.

The list of plugins appears in the left navigation bar.

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	
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.

Each plugin is enabled.

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	
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 **Search Plugin Families** box in the upper right corner.

- Click the **Save** button.

The policy is saved.

Plugin Rules

Plugin Rules allow you to hide or change the severity of any given plugin. In addition, rules can be limited to a specific host or specific time frame. From this page you can view, create, edit, and delete your rules.

The **Plugin Rules** option provides a facility to create a set of rules that dictate the behavior of certain plugins related to any scan performed. A rule can be based on the **Host** (or all hosts), **Plugin ID**, an optional **Expiration Date**, and manipulation of **Severity**.

This allows you to re-prioritize the severity of plugin results to better account for your organization's security posture and response plan.

Example Plugin Rule

Host: 192.168.0.6

Plugin ID: 79877

Expiration Date: 12/31/2016

Severity: Low

This rule is created for 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 12/31/2016. After 12/31/2016, the results of plugin ID 79877 will return 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.

The plugin rule is saved.

Modify a Plugin Rule

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 **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.

The settings are saved.

Delete a Plugin Rule

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 **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.

The plugin rule is deleted.

Customized Reports

On the **Customized Reports** page in Nessus Professional, you can customize the title and logo that appear on each report.

Customized Reports

You can add a custom name or logo for use when exporting HTML or PDF files from your scan results. Images must be in JPEG, GIF or PNG format with a max file size of 10MB and should not contain transparency.

Custom Name

Custom Logo

Customize Report Settings

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

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

The **My Scans** page appears.

2. In the left navigation bar, click **Customized Reports**.

3. In the **Custom Name** box, type the name that you want to appear on the report.

4. To upload a custom logo, click the **Upload** button.

A window appears in which you can select a file to upload.

5. Click the **Save** button.

Your custom title and logo appear on all future reports.

Scanners

By default, Tenable.io is configured with a regional, specific cloud scanner. In addition to using the default cloud scanner, users can also link Nessus scanners, NNM scanners, and Nessus Agents to Tenable.io.

Once linked to Tenable.io, use the Tenable.io key to add remote scanners to **Scanner Groups**. You can also manage and select remote scanners when configuring scans.

The **Linked Scanners** page displays scanner names, types, and permissions.

The **Scanners** page displays the Linking Key and a list of remote scanners. You can click on a linked scanner to view details about that scanner.

Scanners are identified by scanner type and indicate if the scanner has **Shared** permissions.

Remote scanners can be linked to Nessus Manager with the Linking Key or valid account credentials. Once linked, scanners can be managed locally and selected when configuring scans.

Scanners

Remote [scanners](#) can be linked to Nessus using the provided key. Once linked, they can be managed locally and selected when configuring scans. From this page you can view the current status of your scanners and drilldown to control all running scans.

Linking Key: [REDACTED](#)

<input type="checkbox"/>	Name	Status	Scans	Version	Linked On	Last Modified	Edit	Delete
<input type="checkbox"/>	centos7x64nh	Offline	0	N/A	July 24 at 8:10 PM	July 24 at 8:10 PM	Edit	Delete
<input checked="" type="checkbox"/>	Local Scanner	Online	0	6.11.0	June 16 at 4:35 PM	July 25 at 12:54 PM	Edit	Delete

Link Nessus Scanner

To link your Nessus scanner during initial installation, see [Configure Nessus](#).

If you choose not to link the scanner during initial installation, you can link Nessus scanner later. You can link a Nessus scanner to a manager such as Nessus Manager, Tenable.io, or Industrial Security 1.2 or later.

To link a 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.io: **Scans > Scanners**
 - Nessus Manager: **Scans > Scanners**
 - Industrial Security: **Sensor > Sensor Configuration**
2. In Nessus, in the top navigation bar, click **Settings**.
3. In the left navigation bar, click **Remote Link**.
4. Fill out the linking settings for your manager as described in [Remote Link](#).
5. Click **Save**.

Enable or Disable a Scanner

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

Enable a Scanner

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

The **My Scans** page appears.

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

3. In the scanners table, in the row for the scanner that you want to enable, hover over the  button.

 becomes .

4. Click the  button.

The scanner is enabled.

Disable a Scanner

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

The **My Scans** page appears.

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

3. In the scanners table, in the row for the scanner that you want to disable, hover over the  button.

 becomes .

4. Click the  button.

The scanner is disabled.

Remove a Scanner

This procedure can be performed by an administrator.

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

The **My Scans** page appears.

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

3. In the scanners table, in the row for the scanner that you want to remove, click the  button.

The scanner is removed.

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.

The **Agents** page displays the Linking Key and a list of linked agents. You can click on a linked agent to view details about that agent. There are four tabs available on the **Agents** page: **Linked Agents**, **Agent Groups**, **Blackout Windows**, and **Agent Settings**.

Once linked, an agent must be added to a group for use when configuring scans. Linked agents will automatically download plugins from the manager upon connection. Agents are automatically unlinked after a period of inactivity.

Note: Agents can take several minutes to download plugins, but it is required before an agent returns scan results.

Agents

Linked Agents Agent Groups Blackout Windows Agent Settings

 Agents can be linked to Nessus using the following [setup instructions](#). Once linked, they will automatically download all necessary plugins. This process takes several minutes and is required before an agent will return results.

Linking Key: 

<input type="checkbox"/>	Name	Status	IP Address	Platform	Groups	Version	Last Plugin Update	Last Scanned
<input type="checkbox"/>	<script>alert('lol...')	Offline	[REDACTED]	Linux (debian6-...)	qa-agent	6.11.0	August 3	June 28
<input type="checkbox"/>	centos7-6101-d...	Offline	[REDACTED]	Linux (es7-x86-...)	qa-agent	6.11.0	August 3	June 28
<input type="checkbox"/>	centos7-6102-d...	Offline	[REDACTED]	Linux (es7-x86-...)	qa-agent	6.11.0	August 3	June 28
<input type="checkbox"/>	centos7-6103-d...	Offline	[REDACTED]	Linux (es7-x86-...)	qa-agent	6.11.0	August 3	June 28
<input type="checkbox"/>	centos7-6104-d...	Offline	[REDACTED]	Linux (es7-x86-...)	qa-agent	6.11.0	August 3	June 28
<input type="checkbox"/>	centos7-6105-d...	Offline	[REDACTED]	Linux (es7-x86-...)	qa-agent	6.11.0	August 3	June 28

Agent Groups

Agent groups are used to organize and manage the agents linked to your scanner. Each agent can be added to any number of groups and scans can be configured 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.

Modify Agent Settings

Use this procedure to modify agent settings in Nessus Manager.

To modify agent settings:

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. Click the **Agent Settings** tab.

4. Modify the [settings](#) as necessary.

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

Filter Agents

Use this procedure to filter agents in Nessus Manager.

To filter agents in the agents table:

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. Above the agents table, click the **Filter** button.

The **Filter** window appears.

4. Configure the options as necessary. Depending on the parameter you select, different options appear:

Parameter	Operator	Expression
IP Address	is equal to is not equal to contains does not contain	In the text box, type the IPv4 or IPv6 addresses on which you want to filter.
Last Connection Last Plugin Update Last Scanned	earlier than later than on not on	In the text box, type the date on which you want to filter.
Member of Group	is equal to is not equal to	From the drop-down list, select from your existing agent groups.

Parameter	Operator	Expression
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.
Version	is equal to is not equal to contains does not contain	In the text box, type the version you want to filter.

5. Click **Apply**.

The manager filters the list of agents to include only those that match your configured options.

Unlink an Agent

When you 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](#).

Use this procedure to unlink an agent in Nessus Manager.

To unlink a single agent:

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. For Nessus 7.1.1 and later: In the agents table, in the row for the agent that you want to unlink, click the  button.

-or-

For Nessus 7.1.0 and earlier: In the agents table, in the row for the agent that you want to unlink, click the  button.

A dialog box appears, confirming your selection to unlink the agent.

4. Click the **Unlink** button.

The manager unlinks the agent.

To unlink multiple agents:

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. In the agents table, click the check box in each row for each agent you want to unlink.

4. In the upper-right corner, click **Unlink**.

A dialog box appears, confirming your selection to unlink the agent.

5. Click the **Unlink** button.

The manager unlinks the agents.

Agent Status

Nessus Agents can be in one of the following states:

Status	Description
Online	The host that contains the Nessus Agent is currently connected and in communication with Nessus Manager.
Offline	The host that contains the Nessus Agent is currently powered down or not connected to a network.
Initializing	The Nessus Agent is in the process of checking in with Nessus Manager.
Unlinked	<p>The agent is in an unlinked state.</p> <p>Agents with this status are only present if Track unlinked agents is enabled.</p> <p>Note: Agents that are automatically unlinked via the Unlink inactive agents after X days setting can automatically relink to Nessus Manager if they come back online. Agents that are manually unlinked must be manually relinked.</p>

Agent Groups

You can use agent groups to organize and manage the agents linked to your Nessus Manager. You can add an agent to more than one group, and configure scans to use these groups as targets. 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.sc. 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 must be imported into Tenable.sc. The .nessus file size affects hard drive space and bandwidth.

To manage agent groups, use the following procedures:

- [Create a New 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 Nessus Manager.

To create a new agent group:

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. Click the **Agent Groups** tab.

4. In the upper right corner, click the **New Group** button.

The **New Agent Group** window appears.

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

6. Click **Add**.

The new agent group appears in the table.

Modify an Agent Group

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

To modify an agent group:

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. Click the **Agent Groups** tab.

4. In the row for the agent group that you want to modify, click the  button.

The **Edit Agent Group** window appears.

5. Modify the name of the agent group as needed.

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

Delete an Agent Group

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

To delete an agent group:

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. Click the **Agent Groups** tab.

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

A dialog box appears, prompting you to confirm your deletion.

5. Click **Delete**.

Blackout Windows

Blackout windows apply to all linked agents and prevent the agents from receiving and applying software updates during scheduled windows. Agents still receive plugin updates and continue performing scheduled scans during these windows.

To manage blackout windows, use the following procedures:

- [Create a Blackout Window](#)
- [Modify a Blackout Window](#)
- [Delete a Blackout Window](#)

Create a Blackout Window

Blackout windows will apply to all linked agents and will prevent the agents from receiving and applying software updates during scheduled windows. Agents will still receive plugin updates and continue performing scheduled scans during these windows.

To create a blackout window for linked agents:

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. Click the **Blackout Windows** tab.

4. In the upper-right corner, click the **New Window** button.

The **New Blackout Window** page appears.

5. Configure the options as necessary.

6. Click **Save**.

The blackout window goes into effect and appears on the **Blackout Windows** tab.

Modify a Blackout Window

Use this procedure to manage a blackout window for agent scanning in Nessus Manager.

To modify a blackout window:

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. Click the **Blackout Windows** tab.

4. In the blackout window table, click the blackout window you want to modify.

The **Blackout Windows / <Name>** window appears, where **<Name>** is the name of the selected blackout window.

5. Modify the options as necessary.

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

Delete a Blackout Window

Use this procedure to delete a blackout window for agent scanning in Nessus Manager.

To delete a blackout window for agent scanning:

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. Click the **Blackout Windows** tab.

4. In the blackout window table, in the row for the blackout window that you want to delete, click the delete button (✖).

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

5. Click **Delete** to confirm the deletion.

Settings Page

The **Settings** page contains the following sections:

- [About](#)
- [Advanced](#)
- [Proxy Server](#)
- [Remote Link](#)
- [SMTP Server](#)
- [Custom CA](#)
- [My Account](#)
- [Users](#)

Tip: For instructions on performing the actions available on the **System Settings** page, see the related [How To](#) section of this guide.

The screenshot shows the Nessus Settings page with the 'About' section selected. The left sidebar has 'SETTINGS' and 'ACCOUNTS' sections. The 'About' section is active, showing the 'Overview' tab. The main content area displays Nessus Manager details and plugin information.

Nessus Manager		Plugins	
Version	6.11.0 (#969) WINDOWS	Last Updated	Today at 6:15 AM ⓘ
Activation Code	██	Plugin Set	201708040615
Expiration	February 27, 2018		
Licensed Hosts	10000		
Licensed Scanners	1 of 100		
Licensed Agents	14 of 10000		

Set a Master Password

If you set a master password, Nessus encrypts all policies and credentials contained in the policy, and prompts you for the password as needed.

Caution: If you lose your master password, it cannot be recovered by an administrator or Tenable, Inc. Support.

1. In Nessus, in the top navigation bar, click **Settings**.
- The **About** page appears.
2. Click the **Master Password** tab.
3. In the **New Password** box, type your desired password.
4. Click the **Save** button.

The master password is saved.

Update Nessus Software

Update to Nessus Pro v7

Note: The **Update to Pro 7** tab appears only if you have already upgraded to Nessus Professional v7 from a legacy version of Nessus.

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

The **About** page appears.

2. Click the **Update to Pro 7** tab.
3. Click the **Update to Nessus Pro v7** button.

The **What's new in Nessus Professional v7** dialog box appears.

What's new in Nessus Professional v7

You can remain on your current version of Nessus until Dec 31, 2018.
After this date, you will be required to update to version 7.x

Easily transferable license
No more waiting to transfer your license between laptops and users

Emailed scan reports
Reports can be emailed as an attachment upon completion.

Customized reports
Add your own company name and logo to Nessus reports for more personalization.

Nessus Professional v7 will not provide scanning capabilities via API and will not allow you to create more users.

I agree to the [Nessus Software License and Subscription Agreement](#)

[Update to Nessus Professional 7](#)

[Remind me later](#)

4. Select the **I agree to the Nessus Software License and Subscription Agreement** check box.

5. Click the **Update to Nessus Professional v7** button.

Your Nessus Professional instance is updated to the Nessus Professional v7 feature set.

Revert from Nessus Pro v7

Note: The **Revert from Pro 7** tab appears only if you have already upgraded to Nessus Professional v7 from a legacy version of Nessus.

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

The **About** page appears.

2. Click the **Revert from Pro 7** tab.

3. Click the **Restore Nessus Professional Legacy** button.

The legacy Nessus Professional features are restored.

Configure Automatic Updates

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

The **About** page appears.

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

3. In the **Automatic Updates** section, select one of the following options:

- **Update all components:** Updates the Nessus engine and downloads the latest plugin set.
- **Update plugins:** Downloads the latest plugin set.

4. Depending on how specifically you want to define the update interval,

In the **Update Frequency** box, select the interval at which you want Nessus to update (**Daily**, **Weekly**, or **Monthly**).

-or-

In the **Update Frequency** section, click the button.

A box appears where you can type the number of hours you want to define as the interval.

5. In the **Update Server** box, type the server from which you want Nessus to download plugins.

6. Click the **Save** button.

Nessus downloads any available updates automatically per your settings.

Download Updates Manually

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

The **About** page appears.

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

3. In the **Automatic Updates** section, click **Disabled**.

4. In the **Update Server** box, type the server from which you want Nessus to download plugins.

5. Click the **Save** button.

Nessus downloads any available updates.

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.

The setting is saved.

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  button.

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

4. Click **Delete**.

The setting is deleted.

About

The **About** page displays an overview of Nessus licensing and plugin information. When you access the product settings, the **About** page appears by default. Basic users cannot view the **Software Update** or **Master Password** tabs. Standard users can only view the product version and basic information about the current plugin set.

The screenshot shows two side-by-side "About" pages. The left page is for "Nessus Professional" and the right page is for "Nessus Manager". Both pages have a header with tabs: Overview, Revert from Pro 7, Software Update, and Master Password. The "Overview" tab is selected. Below the tabs, there are sections for "Nessus Professional Version 7" and "Nessus Manager". Each section includes fields for Version, Licensed Hosts, Last Updated, Expiration, Plugin Set, and Activation Code. The "Nessus Manager" page also includes sections for Plugins, Licensed Scanners, and Licensed Agents.

Note: The **Revert from Pro 7** or **Update to Pro 7** tab appears only if you have upgraded to Nessus Professional v7 from a legacy version of Nessus Professional.

Value	Description
Nessus Professional	
Version	The version of your Nessus instance.
Licensed Hosts	The number of hosts you can scan, depending on your license.
Last Updated	The date on which the plugin set was last refreshed.
Expiration	The date on which your license expires.
Plugin Set	The ID of the current plugin set.
Activation Code	The activation code for your instance of Nessus.
Nessus Manager	
Version	The version of your Nessus instance.
Licensed Hosts	The number of hosts you can scan, depending on your license.

Value	Description
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 expires.
Plugin Set	The ID of the current plugin set.
Activation Code	The activation code for your instance of Nessus.

Advanced Settings

The **Advanced Settings** page allows you to manually configure Nessus. You can configure advanced settings from the Nessus user interface, or from the command line interface. Nessus validates your input values to ensure only valid configurations are allowed.

Advanced Settings are grouped into the following categories:

- [User Interface](#)
- [Scanning](#)
- [Logging](#)
- [Performance](#)
- [Security](#)
- [Agents and Scanners](#)
- [Miscellaneous](#)
- [Custom](#)

Details

- Advanced settings apply globally across your Nessus instance.
- To configure advanced settings, you must use a Nessus administrator user account.
- Not all advanced settings are automatically populated in the Nessus interface.
- Changes may take several minutes to take effect.
- Some settings require restarting Nessus for the change to apply.
- Custom policy settings supersede the global advanced settings.

User Interface

Setting	Identifier	Description	Default	Valid Values
Allow Post-	allow_post_	Allows a user to make edits to	yes	yes or no

Setting	Identifier	Description	Default	Valid Values
Scan Editing	scan_editing	scan results after the scan is complete.		
Disable Nessus Web Server	disable_xmlrpc	Disables the new XMLRPC (Web Server) interface.	no	yes or no
Disable UI	disable_ui	Disables the user interface on managed scanners.	no	yes or no
Maximum Concurrent Web Users	global.max_web_users	Maximum web users who can connect simultaneously.	1024	Integers. If set to 0, no limit is enforced.
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	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

Scanning

Setting	Identifier	Description	Default	Valid Values
Attached Report Maximum Size	attached_report_maximum_size	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. Nessus does not support report attachments larger than 50 MB.	25	Integers 0-50

Setting	Identifier	Description	Default	Valid Values
Auto Enable Plugin Dependencies	auto_enable_dependencies	Automatically activates the plugins that are depended on. If disabled, not all plugins may run despite being selected in a scan policy.	yes	yes or no
CGI Paths for Web Scans	cgi_path	A colon-delimited list of CGI paths to use for web server scans.	/cgi-bin:/scripts	String
Log Verbose Scan Details	log_verbosity	Logs every detail of the attack. Helpful for debugging issues with the scan, but this may be disk intensive.	no	yes or no
Maximum Ports in Scan Reports	report.max_ports	The maximum number of allowable ports. If there are more ports in the scan results than this value, the excess will be discarded. This limit helps guard against fake targets that may have thousands of reported ports, but can also result in valid results being deleted from the scan results database, so you may want to increase the default if this is a problem.	1024	Integers
Nessus Rules File Location	rules	<p>Location of the Nessus rules file (nessusd.rules). The following are the defaults for each operating system:</p> <p>Linux: /opt/nessus/etc/nessus/nessusd.rules</p> <p>Mac OS X: /Library/Nessus/run/var/nessus/conf/nessusd.rules</p> <p>Windows: C:\ProgramData\Tenable\Nessus\conf\nessusd.rules</p>	Nessus config directory for your operating system	String

Setting	Identifier	Description	Default	Valid Values
		able\Nessus\nessus\conf\nessusd.rules		
Non-Simultaneous Ports	non_simult_ports	Specifies ports against which two plugins cannot not be 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 it is terminated.	0	Integers 0-10080
PCAP Snapshot Length	pcap.snaplen	The snapshot size used for packet capture; the maximum size of a captured network packet. Typically, this value is automatically set based on the scanner's NIC. However, depending on your network configuration, packets may be truncated, 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 packets being truncated.	0	Integers 0-262144
Port Range	port_range	Range of the ports the port scanners scans.	default	default, all, a comma-separated list of ports and/- or port ranges.

Setting	Identifier	Description	Default	Valid Values
Reverse DNS Lookups	reverse_lookup	When enabled, targets are identified by their fully qualified domain name (FQDN) in the scan report. When disabled, the report identifies the target by hostname or IP address.	no	yes or no
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, the list of plugin dependencies and their output are not included in the report. A plugin may be selected 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 this option is set, Nessus does not scan a network incrementally (10.0.0.1, then 10.0.0.2, then 10.0.0.3, and so on) but attempts to slice the workload throughout the whole network (e.g., it scans 10.0.0.1, then 10.0.0.127, then 10.0.0.2, then 10.0.0.128, and so on).	no	yes or no

Logging

Setting	Identifier	Description	Default	Valid Values
Log Additional	log_details	When enabled, scan logs includes the user name, scan name, and current plugin name in addition to the base information.	no	yes or no

Setting	Identifier	Description	Default	Valid Values
Scan Details				
Nessus Dump File Location	dump-file	<p>Location of a dump file for debugging output if generated.</p> <p>The following are the defaults for each operating system:</p> <ul style="list-style-type: none"> Linux: /opt/nessus/var/nessus/logs/nessusd.dump Mac OS X: /Library/Nessus/run/var/nessus/logs/nessusd.dump Windows: C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.dump 	<i>Nessus log directory for your operating system</i>	String
Nessus Dump File Log Level	nasl_log_type	The type of NASL engine output in nessusd.dump.	normal	normal, none, trace, or full.
Nessus Scanner Log Location	logfile	<p>Location where the Nessus log file is stored.</p> <p>The following are the defaults for each operating system:</p> <ul style="list-style-type: none"> Linux: /opt/nessus/var/nessus/logs/nessusd.messages Mac OS X: /Library/Nes- 	<i>Nessus log directory for your</i>	String

Setting	Identifier	Description	Default	Valid Values
		sus/run/var/nessus/logs/nessusd.messages Windows: C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.messages	operating system	
Use Milliseconds in Logs	log-file-msec	When enabled, log timestamps are in milliseconds. When disabled, log timestamps are in seconds.	no	yes or no

Performance

Setting	Identifier	Description	Default	Valid Values
Global Max Hosts Concurrently Scanned	global.max_hosts	Maximum number of hosts that can be scanned simultaneously across all scans.	2150	Integers
Global Max TCP Sessions	global.max_simult_tcp_sessions	Maximum number of simultaneous TCP sessions across all scans.	50	Integers 0 - 2000. If set to 0, no limit is enforced.
Max Concurrent Checks Per Host	max_checks	Maximum number of simultaneous plugins that can run concurrently on each host.	5	Integers. If set to 0, no limit is enforced.
Max Concurrent Hosts	max_hosts	Maximum number of hosts checked at one time during	5	Integers. If set to 0,

Setting	Identifier	Description	Default	Valid Values
Per Scan		a scan.		no limit is enforced.
Max Concurrent Scans	global.max_scans	Maximum number of simultaneous scans that can be run by the scanner.	0	0-1000 If set to 0, no limit is enforced.
Max TCP Sessions Per Host	host.max_simult_tcp_sessions	Maximum number of simultaneous TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner sends, which is 10 times the number of TCP sessions. E.g., if this option is set to 15, the SYN scanner sends 150 packets per second at most.	0	Integers. If set to 0, no limit is enforced.
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 being scanned.	0	Integers 0-2000. If set to 0, no limit is enforced.
Optimize Tests	optimize_test	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	optimization_level	Determines the type of check that is performed before a plugin runs.	None	open_ports or required_

Setting	Identifier	Description	Default	Valid Values
		If this setting is set to open_ports, then Nessus checks that required ports are open; if they are not, the plugin does not run. If this setting is set to required_keys, then Nessus performs the open port check, and also checks that required keys (KB entries) exist, ignoring the excluded key check.		keys
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 impact.	low	low or high
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
Scan Check Read Timeout	checks_read_timeout	Read timeout for the sockets of the tests.	5	Integers 0-1000

Setting	Identifier	Description	Default	Valid Values
Stop Scan on Host Disconnect	stop_scan_on_disconnect	When enabled, Nessus stops scanning a host that seems to have been disconnected during the scan.	no	yes or no
Stop Scan on Host Hang	stop_scan_on_hang	When enabled, Nessus stops scanning a scan that seems to be hung.	no	yes or no
Throttle Scan on CPU Overload	throttle_scan	When enabled, Nessus throttles scan when the CPU is overloaded.	yes	yes or no
Webserver Thread Pool Size	www_thread_pool_size	Thread pool size for the webserver/backend.	100	Integers 0-500

Security

Setting	Identifier	Description	Default	Valid Values
Cipher Files on Disk	cipher_files_on_disk	Encipher files that Nessus writes.	yes	yes or no
Max Concurrent Sessions Per User	max_sessions_per_user	Maximum concurrent sessions per user	0	Integers 0-2000. If set to 0, no limit is enforced.
SSL Cipher List	ssl_cipher_list	Cipher list to use for Nessus backend connections. Nessus only supports strong SSL ciphers when connecting to	strong	noexp, strong, and edh.

Setting	Identifier	Description	Default	Valid Values
		port 8834.		
SSL Mode	ssl_mode	Minimum supported version of TLS.	tls_1_0	compat, ssl_3_0, tls_1_1, and tls_1_2.

Agents & Scanners

Note: The following settings are only available in Nessus Manager.

Setting	Identifier	Description	Default	Valid Values
Agent Software Updates	agent_software_update	Controls whether agent updates are allowed to be downloaded.	yes	yes or no
Agents Progress	agents_progress_viewable	When a scan gathers information from agents, Nessus Manager does not show detailed agents information if the number of agents exceeds this setting. Instead, a message indicates that results are being gathered and will be viewable when the scan is complete.	100	Integers. If set to 0, this defaults to 100.

Setting	Identifier	Description	Default	Valid Values
Automatic Hostname Update	update_hostname	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
Concurrent Agent Software Updates	cloud.manage.download_max	The maximum concurrent agent update downloads.	10	Integers
Track Unique Agents	track_unique_agents	When enabled, Nessus Manager checks if MAC addresses of agents trying to link match MAC addresses of currently linked agents with the same hostname, platform, and distro. Nessus Manager deletes duplicates that it finds.	no	yes or no

Miscellaneous

Setting	Identifier	Description	Default	Valid Values
Automatic Update Delay	auto_update_delay	Number of hours that Nessus waits between automatic updates.	24	Integers > 0
Automatic Updates	auto_update	Automatically updates plugins. If enabled and Nessus is registered, 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.	yes	yes or no
Automatically Update Nessus	auto_update_ui	Automatically download and apply Nessus updates.	yes	yes or no
Initial Sleep Time	ms_agent_sleep	(Nessus Manager only) Sleep time between managed scanner and agent requests. This can be overridden by Nessus Manager or Tenable.io.	30	Integers 5-3300
Max HTTP Client Requests	max_http_client_requests	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, no debug port is established.	None	String in one of the following formats: <i>port</i> or <i>localhost</i> : <i>port</i> or <i>ip</i> : <i>port</i>
Nessus	config_	Location of the configuration file that contains	Nessus	String

Setting	Identifier	Description	Default	Valid Values
Preferences Database	file	<p>the engine preference settings.</p> <p>The following are the defaults for each operating system:</p> <ul style="list-style-type: none"> Linux: /opt/nessus/etc/nessus/nessusd.db Mac OS X: /Library/Nessus/run/etc/nessus/conf/nessusd.db Windows: C:\ProgramData\Tenable\Nessus\conf\nessusd.db 	<i>database directory for your operating system</i>	
Non-User Scan Result Cleanup Threshold	report_cleanupthreshold_days	The age threshold (in days) for removing old system-user scan reports.	30	Integers > 0
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 (e.g., 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 crash information is automatically sent to Tenable, Inc.. to identify problems. No personal or system-identifying information is sent to Tenable, Inc.	yes	yes or no
Scan Source IP(s)	source_ip	Source IPs to use when running on a multi-homed host. If multiple IPs are provided, Nessus will cycle through them whenever it performs a	None	IP address or comma-

Setting	Identifier	Description	Default	Valid Values
		new connection.		separated list of IP addresses.

Custom

Not all advanced settings are populated in the Nessus user interface, but some settings can be set in the command line interface.

The following table lists available advanced settings that are not listed by default in the Nessus user interface but can still be configured.

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).
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 are scanned in parallel). Adjust this setting based on the sensitivity of the remote device to large numbers of SYN packets.	65536	Integers
login_banner	A text banner displays 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

LDAP Server

In Nessus Manager, the **LDAP Server** page displays 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

Port

Username

Password

Base DN

Show advanced settings

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.

4. Click the **Save** button.

The LDAP server is saved.

Proxy Server

The **Proxy Server** page displays options that allow 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.

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="text"/>
Auth Method	AUTO DETECT <input type="button" value="▼"/>
User-Agent	<input type="text"/>

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.

4. Click the **Save** button.

The proxy server is saved.

Remote Link

The **Remote Link** page displays options that allow you to link your Nessus scanner to a licensed Nessus Manager or Tenable.io.

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

Save **Cancel**

Option	Set To
Link Nessus to Nessus Manager	
Link to	Nessus Manager
Scanner Name	The name you want to use for this Nessus scanner.
Manager Host	The static IP address or hostname of the Nessus Manager instance you want to link to.
Manager Port	Your Nessus Manager port, or the default 8834.

Option	Set To
Linking Key	The key specific to your instance of 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 host name 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 Nessus to Tenable.io	
Link to	Tenable.io
Scanner Name	cloud.tenable.com
Linking Key	The key specific to your instance of Tenable.io. 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 host name 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 Nessus to Industrial Security	
Link to	Nessus Manager

Option	Set To
Scanner Name	The name you want to use for this Nessus scanner in Industrial Security.
Manager Host	The IP address of your Industrial Security instance.
Manager Port	Your Industrial Security port, or the default 443.
Linking Key	<p>The key specific to your instance of Industrial Security. It will look something like the following string:</p> <pre>2d38435603c5b59a4526d39640655c3288b00324097a08f7a93e5480940d1cae</pre>
Use Proxy	<p>Select or deselect the check box depending on your proxy settings. If you select Use Proxy, you must also configure:</p> <ul style="list-style-type: none"> • Host — the host name or IP address of the proxy server. • Port — the port number of the proxy server. • Username — the username for an account that has permissions to access and use the proxy server. • Password — the password associated with the username you provided.

SMTP Server

The **SMTP Server** page displays options that allow you to configure a Simple Mail Transfer Protocol (SMTP) server. When you configure an SMTP server, Nessus emails scan results to the list of recipients that you specify.

Note: To configure an SMTP server for Nessus, you must have an HTML compatible email client.

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	<input type="text"/>
Port	<input type="text"/>
From (sender email)	<input type="text"/>
Encryption	<input type="button" value="No Encryption"/>
Hostname (for email links)	<input type="text"/> Example: localhost:8834
Auth Method	<input type="button" value="NONE"/>

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.

4. Click the **Save** button.

The SMTP server is saved.

Custom CA

The **Custom CA** page displays a text box that you can use to upload a custom certificate authority (CA) in Nessus. For instructions on how to create a custom CA, see the [Create a New Custom CA and Server Certificate](#) topic.

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-----
MIIEczCCAlugAwIBAgIBADANBgkqhkiG9w0BAQQFAD..AkGA1UEBhMCR0Ix
EzARBgNVBAgTC1NbWUtU3RhdGUxFDASBgNVBAcTC0..0EgTHRkMTcwNQYD
VQQLEY5DbGFzcyAxIFB1YmxpYyBQcmIyXJ5IENlcn..XRpb24gQXV0aG9y
aXR5MRQwEgYDVQDEwtCZXN0IENBIEx0ZDAeFw0wMD..TuwMTzaFw0wMTAy
MDQxOTUwMTzaMIGHMQswCQYDVQQGEwJHQjETMBEGa1..29tZs1TdGF0ZTEU
MBIGA1UEChMLQmVzdCBDQSBMdgQxNzA1BgNVBAstLk..DEgUHVibG1jIFBy
aWlhcnkgQ2YdGlmawNhdGlvbiBdXRob3JpdHkxFD..AMTC0Jlc3QgQ0Eg
THRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg..Tz2mr7SzIAmfQyu
vBjN9OijjRazXBZ1Bjp5CE/Wm/Rx500PRK+Lh9x5eJ..ANBE0sTK0ZsDGM
ak2mlg7orI3dy3VHqIxFTz0Ta1d+NAjwnLe4nOb7//.k05ShhBrJGBKKxb
8n104o/5p8HAsZPdzbfMIyNjzBM2o5y5A13wiLitE..fyYkQzaxCw0Awz1
kVHiIyCuaFw5j1pSzkv6sv+4IDMbT/XpCo8LewTa..sh+etLD6FttTjYbb
rvZ8RQM1tlKdoMHg2qxraAV++HNBYmNWs0duEdjUbJ..X19TtnS4o1Ckj7P
Oflj1QIDAQABo4HnMhkMB0GA1UdDgQWBBQ8urMCRL..5akIp9NJHJw5TCB
tAYDVR0jBIGsMIGpgBQ8urMCRLYYMHUKU5akIp9NJH..aSBijCBhzELMAkG
A1UEBhMCR0IxExARBgNVBAgTC1NbWUtU3RhdGUxFD..AoTC0Jlc3QgQ0Eg
THRkMTcwNQYDVQDLEy5DbGFzcyAxIFB1YmxpYyBQcm..ENlcnRpZmljYXRp
b24gQXV0aG9yaXR5MRQwEgYDVQDEwtCZXN0IENBIE..DAMBgNVHRMEBTAD
AQH/MA0GCSqGSIb3DQEBAUAA4IBAQCluYBcsSncwA..DCsQer772C2ucpX
xQUE/C0pWnm6gDkwd5D0DSMDJRqV/wecZ4wC6B73f5..bLhGYHaXJeSD6Kr
It8una2gY4l20//on88r5IWJlm1loA8e4FR2yrBHX..adsGeFKkyNrwGi/
7vQMFxdGsRrXNGRgnX+vWDZ3/zWI0joDtCkNnqEpVn..HoX
-----END CERTIFICATE-----
```

Save **Cancel**

Add a Custom CA

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, type your custom CA.

Note: See the instructions on [how to create a custom CA](#).

4. Click the **Save** button.

The custom CA is saved.

My Account

The **Account Settings** page displays settings for the current authenticated user.

Note: Once created, a username cannot be changed.

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:

- API Keys are only presented upon initial generation. Store API keys in a safe location.
- API Keys cannot be retrieved by Nessus. If you lose your API Key, you must generate a new API Key.
- Regenerating an API Key will immediately deauthorize any applications currently using the key.

Users

The **User Profile** page displays a table of all Nessus user accounts. This documentation refers to that table as the *users table*. Each row of the users table includes the user name, 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.io. You can change the role of a user account at any time, as well as disable the account. The following table describes the roles that can be assigned to users:

Name	Description
Basic	Basic user roles can read scan results. Note: This role is not available in Nessus Professional.
Standard	Standard users can create scans, policies, and user asset lists.
Administrator	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. Note: This role is not available in Nessus Professional.
System Administrator	System Administrators have the same privileges as Administrators, but can also manage and modify system configuration settings.
Disabled	Disabled user accounts cannot be used to log in to Nessus.

Agent Settings

The **Agent Settings** page allows you to manually configure options for inactive agents and blackout windows configured on the Blackout Windows tab. For more information on creating, modifying, and deleting blackout windows, see [Blackout Windows](#).

The following table describes the available options.

Option	Description
Manage Agents	
Track unlinked agents	<p>When this setting is enabled, agents that are unlinked are preserved in the manager along with the corresponding agent data.</p> <p>Note: This option can also be set using the nessuscli utility.</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> <p>Requires that Track unlinked agents is enabled.</p>
Override Blackout Windows (Nessus 8.3 and earlier)	
Exclude all agents from software updates	<p>If enabled, this option overrides scheduled blackout windows. It prevents agents from receiving software updates at any time.</p> <p>Agents will still receive plugin updates and continue to perform scheduled scans.</p>
Blackout Windows (Nessus 8.4 and later)	
Enforce a permanent blackout window schedule	<p>When enabled, a permanent blackout window schedule is enforced and any rules below are applied.</p> <p>Note: Any scheduled blackout windows will be overridden by the permanent blackout window.</p>
Prevent software updates	When enabled, agents do not receive software updates during scheduled blackout windows.
Prevent plugin updates	When enabled, agents do not receive plugin updates during scheduled blackout windows.

Option	Description
Prevent agent scans	When enabled, the system does not run agent scans during scheduled blackout windows.

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](#)

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 the account is created.

4. Click **Save**.

Your account settings are saved.

Generate an API Key

Caution: Generating a new API key will replace any existing keys and deauthorize any linked applications.

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.

Create a User Account

This procedure can be performed by an administrator in Nessus Manager or Nessus Professional with legacy features. Multiple users are not available in Nessus Professional 7.0 and later.

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 the account is created.

5. Click **Save**.

The user account is saved.

Modify a User Account

This procedure can be performed by an administrator in Nessus Manager or Nessus Professional with legacy features. Multiple users are not available in Nessus Professional 7.0 and later.

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 the account is created.

5. Click **Save**.

Your account settings are saved.

Delete a User Account

This procedure can be performed by an administrator in Nessus Manager.

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  button.

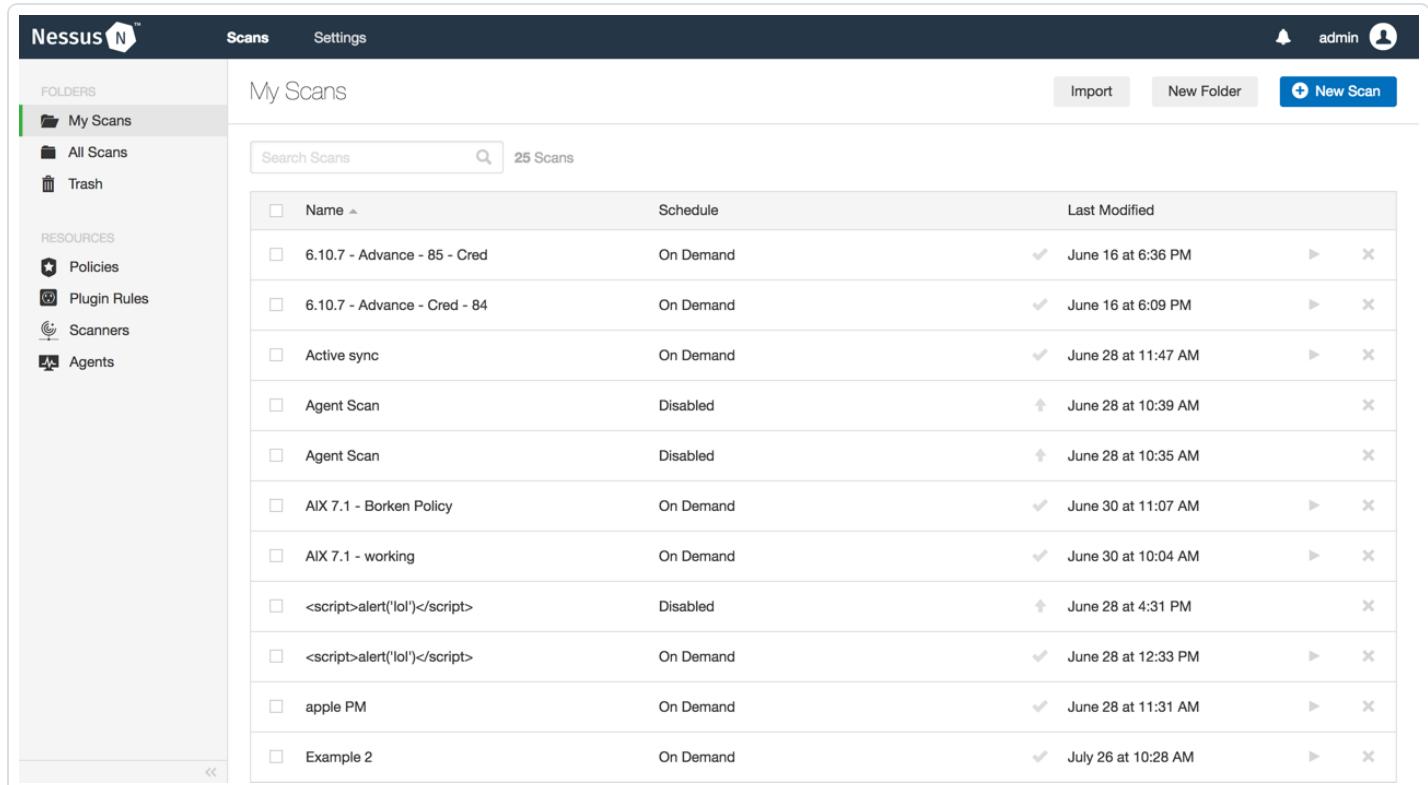
A dialog box appears, confirming your selection to delete the user.

4. Click **Delete**.

The user is deleted.

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 displays the **Folders** and **Resources** sections.



The screenshot shows the Nessus interface with the 'Scans' tab selected. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Scanners, Agents). The main area is titled 'My Scans' with a search bar and a count of 25 Scans. A table lists the scans with columns for Name, Schedule, and Last Modified. Each row has a checkbox, a preview icon, and edit/delete icons.

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

For more information, see the following sections:

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

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

Scan and Policy Templates

Templates facilitate the creation of **Scans** and **Policies**.

When you first create a **Scan** or **Policy**, the **Scan Templates** section or **Policy Templates** section appears, respectively. Templates are provided for scanners and agents. If you have created custom policies, they appear in the **User Defined** tab.

Tip: You can use the search box in the top navigation bar to filter templates in the section currently in view.

The templates that are available may vary. The Nessus interface provides brief explanations of each template in the product. This documentation includes a comprehensive explanation of the settings available for each template.

The following tables list the templates that are available in Nessus and the settings that are available for those templates.

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.

For information on agent templates, see [Agent Scan and Policy Templates](#).

Scanner Templates

Template	Description	Settings	Credentials	Compliance/SCAP
Advanced Scan	Scans without any recommendations.	All	All	All
Audit Cloud Infrastructure	Audits the configuration of third-party cloud services.	Basic: All Report: Output Advanced:	Cloud Services	AWS Microsoft Azure Rackspace Salesforce.com

Template	Description	Settings	Credentials	Compliance/SCAP
Badlock Detection	Performs remote and local checks for CVE-2016-2118 and CVE-2016-0128.	<p>Debug</p> <p><u>Basic:</u> General, Schedule, Notifications, Permissions</p> <p><u>Discovery:</u> All</p> <p><u>Assessment:</u> General, Windows, Malware</p> <p><u>Report:</u> All</p> <p><u>Advanced:</u> Debug Settings</p>	None	Unix Unix File Contents Windows Windows File Contents
Bash Shell-shock Detection	Performs remote and local checks for CVE-2014-6271 and CVE-2014-7169.	<p><u>Basic:</u> All</p> <p><u>Discovery:</u> Host: All</p> <p>Scan Type</p> <p><u>Assessment:</u> Web Applications</p> <p><u>Report:</u> Plaintext</p> <p>Output</p> <p><u>Advanced:</u> All</p>	<u>Database</u> <u>Host</u> : All <u>Miscellaneous</u> <u>Patch Management</u> <u>Authentication</u>	None
Basic Network Scan	Performs a full system scan that is suit-	<p><u>Basic:</u> All</p> <p><u>Discovery:</u></p>	<u>Database</u> <u>Host:</u> SSH, Win-	None

Template	Description	Settings	Credentials	Compliance/SCAP
	able for any host. For example, you could use this template to perform an internal vulnerability scan on your organization's systems.	<p>Scan Type</p> <p><u>Assessment:</u> General, Brute Force, Web Applications, Windows</p> <p><u>Report:</u> All</p> <p><u>Advanced:</u> Scan Type</p>	<p>dows</p> <p><u>Miscellaneous</u></p> <p><u>Patch Management</u></p> <p><u>Plaintext Authentication</u></p>	
Credentialated Patch Audit	Authenticates hosts and enumerates missing updates.	<p><u>Basic:</u> All</p> <p><u>Discovery:</u> Scan Type</p> <p><u>Assessment:</u> Brute Force, Windows, Malware</p> <p><u>Report:</u> All</p> <p><u>Advanced:</u> Scan Type</p>	<p><u>Host:</u> SSH, Windows</p>	None
DROWN Detection	Performs remote checks for CVE-2016-0800.	<p><u>Basic:</u> All</p> <p><u>Discovery:</u> Scan Type</p> <p><u>Report:</u> Output</p>	None	None

Template	Description	Settings	Credentials	Compliance/SCAP
		<u>Advanced:</u> All		
Host Discovery	Performs a simple scan to discover live hosts and open ports.	<u>Basic:</u> All <u>Discovery:</u> Scan Type <u>Report:</u> Output <u>Advanced:</u> Performance Options	None	None
Intel AMT Security Bypass	Performs remote and local checks for CVE-2017-5689.	<u>Basic:</u> All <u>Discovery:</u> Scan Type <u>Report:</u> Output <u>Advanced:</u> All	<u>Host:</u> Windows	

Template	Description	Settings	Credentials	Compliance/SCAP
		<p>dows</p> <p><u>Report:</u></p> <p>All</p> <p><u>Advanced:</u></p> <p>Scan Type</p>		
Malware Scan	Scans for malware on Windows and Unix systems.	<p><u>Basic:</u> All</p> <p><u>Discovery:</u></p> <p>Scan Type</p> <p><u>Assessment:</u></p> <p>Malware</p> <p><u>Report:</u></p> <p>Output</p> <p><u>Advanced:</u></p> <p>Scan Type</p>	<p><u>Host:</u> SSH, Win-dows</p>	None
MDM Config Audit	Audits the configuration of mobile device managers.	<p><u>Basic:</u> All</p> <p><u>Report:</u></p> <p>Output</p>	<u>Mobile</u>	Mobile Device Manager
Mobile Device Scan	Assesses mobile devices via Microsoft Exchange or an MDM.	<p><u>Basic:</u> All</p> <p><u>Report:</u> All</p> <p><u>Advanced:</u></p> <p>Debug</p>	<p><u>Miscellaneous</u></p> <p><u>Mobile</u></p>	None
Offline Config Audit	Audits the configuration of network devices.	<p><u>Basic:</u> All</p> <p><u>Report:</u> Out-put</p> <p><u>Advanced:</u></p>	None	Adtran AOS Bluecoat ProxySG Brocade Fabricos Check Point Gaia

Template	Description	Settings	Credentials	Compliance/SCAP
		Debug		Cisco IOS Dell Force10 FTOS Extreme ExtremeXOS Fireeye Fortigate Fortios HP Procurve Huawei VRP Juniper Junos Netapp Data Ontap Sonicwall Sonicos Watchguard
PCI Quarterly External Scan	Performs quarterly external scans as required by PCI. <div data-bbox="376 1142 670 1564" style="border: 1px solid #00AEEF; padding: 10px;"> Note: Because the nature of a PCI ASV scan is more paranoid and may lead to false positives, the scan data is not included in the aggregate Tenable.io data. This is by design. </div>	<u>Basic:</u> All <u>Discovery:</u> Host Discovery <u>Advanced:</u> Scan Type	<u>Plaintext Authentication</u> : HTTP	None
Policy Compliance Auditing	Audits system configurations against a known baseline.	<u>Basic:</u> All <u>Discovery:</u> Scan Type <u>Report:</u> Out-	<u>Database</u> <u>Host</u> <u>Host:</u> SSH, Win-	All

Template	Description	Settings	Credentials	Compliance/SCAP
		put Advanced: Scan Type	dows Miscellaneous Mobile	
SCAP and OVAL Auditing	Audits systems using SCAP and OVAL definitions.	Basic: All Discovery: Host Discovery Report: All Advanced: Scan Type	Host: SSH, Windows	SCAP Settings
Shadow Brokers Scan	Scans for vulnerabilities disclosed in the Shadow Brokers leaks.	Basic: All Discovery: Scan Type Report: Output Advanced: All	Host: SSH, Windows	None
Spectre and Meltdown	Performs remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.	Basic: All Discovery: Scan Type Report: Output Advanced: All	Host: SSH, Windows Miscellaneous Patch Management Plaintext Authentication	None
WannaCry	Scans for the Wan-	Basic: All	Host: Windows	None

Template	Description	Settings	Credentials	Compliance/SCAP
Ransomware	naCry ransomware.	<u>Discovery:</u> Scan Type <u>Report:</u> Out- put <u>Advanced:</u> All		
Web Application Tests	Scan for published and unknown web vulnerabilities.	<u>Basic:</u> All <u>Discovery:</u> Scan Type <u>Assessment:</u> General, Web Applications <u>Report:</u> All <u>Advanced:</u> All	<u>Plaintext</u> <u>Authentication</u> : HTTP	None

Scan and Policy Settings

Scan or Policy **Settings** are organized into collections of configuration items, specifically **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** settings. Each of these collections are subdivided into further sections. For example, the **Basic** settings include the **General**, **Schedule**, **Notifications**, and **Permissions** sections. Additionally, the sections may contain groups of related configuration items. For example, the **Host Discovery** section contains the **General Settings**, **Ping Methods**, **Fragile Devices**, **Wake-on-LAN**, and **Network Type** groups.

The following sections of the documentation are organized to reflect the interface. For example, if you wanted to find information about the **General** section (3 in the previous image) of the **Basic** settings (2 in the previous image) that appears when you select the **Settings** tab (1 in the previous image), you should locate the table labeled [General in the Basic topic](#). The tables include subheadings to reflect groups of related configuration items that appear in a particular section.

The following settings exist for each policy, though available configuration items may vary based on the selected template:

- [Basic](#)
- [Discovery](#)
- [Assessment](#)
- [Report](#)
- [Advanced](#)

Basic Scan Settings

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

Note: Configuration items that are required by a particular scan or policy are indicated in the 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 or policy. This value is displayed on the Nessus interface.
Description	None	(Optional) Specifies a description of the scan or policy.
Folder	My Scans	Specifies the folder where the scan appears after being saved.
Dashboard	Disabled	(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	Varies	(Nessus Manager only) Specifies the scanner that performs the scan. The default scanner varies based on the organization and user.
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 hostname[ip] syntax (e.g., www.example.com [192.168.1.1]).</p>
Upload Targets	None	<p>Uploads a text file that specifies targets. 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 <p>Note: Unicode/UTF-8 encoding is not supported.</p>

Schedule

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

Setting	Default Value	Description
Frequency	Once	Specifies how often the scan is launched.

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

Notifications

Setting	Default Value	Description

Email Recipient(s)	None	Specifies zero or more email addresses, separated by commas, that are alerted when a scan completes and the results are available.
Attach Report	Off	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	Specifies the report type (CSV, Nessus, or PDF) that you want to attach to the email.
Max Attachment Size	25	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. 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.

Permission	Description
No Access	Groups and users set to No Access cannot interact with the scan in any way. When you create a scan or policy, 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.

Discovery Scan Settings

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

Note: Configuration items that are required by a particular scan or policy are indicated in the Nessus interface.

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

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

The following tables list by section all available settings. When you select any template other than Advanced Network Scan, the [**Scan Type**](#) setting also appears.

Scan Type

The **Scan Type** setting appears for all templates that have **Discovery** settings, except Advanced Network Scan. The options that are available for the **Scan Type** setting vary from template to template. The following table describes the options that are available per template. If a template is not listed in the table, no **Discovery** settings are available for that template.

The Nessus user interface provides descriptions of each option.

Note: When **Custom** is selected, the following sections appear: [**Host Discovery**](#), [**Port Scanning**](#), and [**Service Discovery**](#).

Template	Available Options
Badlock Detection	Four options are available: <ul style="list-style-type: none">• Quick• Normal (default)• Thorough• Custom
Bash Shellshock Detection	
DROWN Detection	

Basic Network Scan	Three options are available:
Basic Web App Scan	<ul style="list-style-type: none"> • Port scan (common ports) (default) • Port scan (all ports) • Custom
Credentialed Patch Audit	
Internal PCI Network Scan	
Web Application Tests	
Host Discovery	Five options are available:
	<ul style="list-style-type: none"> • Host enumeration (default) • OS Identification • Port scan (common ports) • Port scan (all ports) • Custom
Malware Scan	Three options are available:
	<ul style="list-style-type: none"> • Host enumeration (default) • Host enumeration (include fragile hosts) • Custom
Policy Compliance Auditing	Two options are available:
	<ul style="list-style-type: none"> • Default (default) • Custom
SCAP and OVAL Auditing	Two options are available:
	<ul style="list-style-type: none"> • Host enumeration (default) • Custom

Host Discovery

By default, some settings in the **Host Discovery** section are enabled. 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](#)
- [Network Type](#)

Setting	Default Value	Description
Ping the remote host	On	<p>This option enables Nessus to ping remote hosts on multiple ports to determine if they are alive. When set to On, General Settings and Ping Methods appear.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> Note: To scan VMware guest systems, Ping the remote host must be set to Off. </div>
General Settings		
Use Fast Network Discovery	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. Fast network discovery bypasses those additional tests.
Ping Methods		
ARP	Enabled	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.
TCP	Enabled	Ping a host using TCP.
Destination ports (TCP)	Built-In	Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that are checked via TCP ping.
ICMP	Enabled	Ping a host using the Internet Control Message Protocol (ICMP).
Assume ICMP unreachable from the gateway means the host is down	Disabled	Assume ICMP unreachable from the gateway means the host is down. When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When this option is enabled, when Nessus receives an ICMP Unreachable message, it considers the targeted host dead. This is to help speed up discovery on some

		<p>networks.</p> <div style="border: 1px solid #0070C0; 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	Specifies the number of attempts to retry pinging the remote host.
UDP	Disabled	<p>Ping a host using the User Datagram Protocol (UDP).</p> <p>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	When enabled, Nessus scans network printers.
Scan Novell Netware hosts	Disabled	When enabled, Nessus scans Novell NetWare hosts.
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.
Network Type		
Network Type	Mixed	Specifies if you are using publicly routable IPs, private non-internet

	(use RFC 1918)	<p>routable IPs, or a mix of these.</p> <p>This setting has three options:</p> <ul style="list-style-type: none"> • Mixed (use RFC 1918) • Private LAN • Public WAN (internet) <p>The default value, Mixed, should be selected if you are using RFC 1918 addresses and have multiple routers within your network.</p>
--	----------------	--

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	If a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), Nessus considers it closed.
Port Scan Range	Default	<p>Two keywords can be typed into the Port scan range box.</p> <ul style="list-style-type: none"> • <i>default</i> instructs Nessus to scan approximately 4,790 commonly used ports. The list of ports can be found in the <code>nessus-services</code> file. • <i>all</i> instructs Nessus to scan all 65,536 ports, including port 0.

Setting	Default Value	Description
		<p>Additionally, you can type a custom range of ports by using a comma-delimited list of ports or port ranges. For example, 21,23,25,80,110 or 1-1024,8080,9000-9200. If you wanted to scan all ports excluding port 0, you would type 1-65535.</p> <p>The custom range specified for a port scan is applied to the protocols you have selected in the Network Port Scanners 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 T:1-1024,U:300-500.</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, 1-1024,T:1024-65535,U:1025.</p>
Local Port Enumerators		
SSH (net-stat)	Enabled	<p>This option 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 (net-stat)	Enabled	<p>A WMI-based scan uses netstat to determine open ports.</p> <p>Note: If enabled, any custom range typed in the Port Scan Range box is ignored.</p> <p>If any port enumerator (netstat or SNMP) is successful, the port range becomes <i>all</i>. Nessus still treats unscanned ports as closed if the Consider unscanned ports as closed check box is selected.</p>
SNMP	Enabled	<p>When enabled, if the appropriate credentials are provided by the user, Nessus can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the</p>

Setting	Default Value	Description
		version of the returned SNMP string. This information is necessary for these audits.
Only run network port scanners if local port enumeration failed	Enabled	Rely on local port enumeration first before relying on network port scans.
Verify open TCP ports found by local port enumerators	Disabled	If a local port enumerator (e.g., WMI or netstat) finds a port, Nessus also verifies that it is open remotely. This helps determine if some form of access control is being used (e.g., TCP wrappers, firewall).
Network Port Scanners		
TCP	Disabled	On some platforms (e.g., Windows and Mac OS X), enabling this scanner causes Nessus to use the SYN scanner to avoid serious performance issues native to those operating systems.
Override automatic firewall detection	Disabled	<p>When enabled, this setting overrides automatic firewall detection. 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. <p>This description also applies to the Override automatic firewall detection setting that is available following SYN.</p>

Setting	Default Value	Description
SYN	Enabled	Use the Nessus SYN scanner to identify open TCP ports on the target hosts. SYN scans are generally considered to be less intrusive than TCP scans depending on the security monitoring device, such as a firewall or Intrusion Detection System (IDS). The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines the port state based on a reply or lack of reply.
UDP	Disabled	<p>This option engages Nessus built-in 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	<p>Attempts to map each open port with the service that is running on that port.</p> <p>Caution: In some rare cases, probing might disrupt some services and cause unforeseen side effects.</p>
Search for	On	Controls how Nessus will test SSL-based services.

Setting	Default Value	Description
SSL based services		<p>Caution: Testing for SSL capability on all ports may be disruptive for the tested host.</p>
Search for SSL/TLS Services (enabled)		
Search for SSL/TLS on	Known SSL/TLS ports	<p>This setting has two options:</p> <ul style="list-style-type: none"> • Known SSL/TLS ports • All ports
Identify certificates expiring within x days	60	Identifies SSL and TLS certificates that are within the specified number of days of expiring.
Enumerate all SSL ciphers	True	When enabled, Nessus 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, Nessus checks that none of the identified certificates have been revoked.

Assessment Scan Settings

The **Assessment** scan settings are used for configuring 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.

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

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

Scan Type

The **Scan Type** setting contains options that vary from template to template.

The Nessus interface provides descriptions of each option. The **Custom** option displays different **Assessment** settings depending on the selected template.

Template	Available Options
Basic Network Scan	Four options are available: <ul style="list-style-type: none">• Scan for known web vulnerabilities• Scan for all web vulnerabilities (quick)• Scan for all web vulnerabilities (complex)• Custom
Basic Web App Scan	
Internal PCI Network Scan	

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, Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to Show potential false alarms then 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 Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. Not enabling Override normal accuracy is a middle ground between these two settings.
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 in some cases. 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 (e.g., a few hours ago). This can be configured 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 being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.
From address	The test messages sent to the SMTP server(s) 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 cause the account to be locked out 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		

Hydra options only appear when Hydra is installed on the same computer as the scanner or agent executing the scan.

Always enable Hydra (slow)	Disabled	Enables Hydra whenever the scan is performed.
Logins file		A file that contains user names 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 log on attempt.
Try empty passwords	Enabled	If enabled, Hydra tries user names without using a password.
Try login as password	Enabled	If enabled, Hydra tries a user name 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, only the user names specified in the logins file are used for the scan. Otherwise, additional user names discovered by other plugins are added to the logins file and used 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	Can be set to <i>Local accounts</i> , <i>Domain Accounts</i> , or <i>Either</i> .
Interpret passwords as NTLM hashes	Disabled	If enabled, Hydra interprets passwords as NTLM hashes.
Cisco login password		This password is used to log in to a Cisco system before brute forcing enable passwords. If no password is provided 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 that is protected by HTTP basic or digest authentication. If a web page is not provided 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 slave. 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.

Setting	Default Value	Description
Modbus/TCP Coil Access		Modbus uses a function code of 1 to read coils in a Modbus slave. 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.
End at Register	16	The register at which to stop scanning.
ICCP/COTP TSAP Addressing Weakness		The ICCP/COTP TSAP Addressing menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values.
Start COTP TSAP	8	Specifies the starting TSAP value to try.
Stop COTP TSAP	8	Specifies the ending TSAP value to try. All values between the Start and Stop values are tried.

Web Applications

By default, web applications are not scanned. When you first access the **Web Application** section, the **Scan Web Applications** setting appears and is set to **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 the	Disabled	This option enables Nessus to take screenshots to

Setting	Default Value	Description
cloud to take screen-shots of public web servers		<p>better demonstrate some findings. This includes some services (e.g., VNC, RDP) as well as configuration specific options (e.g., web server directory indexing). The feature only works for internet-facing hosts, as the screenshots are generated on a managed server and sent to the Nessus scanner.</p> <p>Screen shots are not exported with a Nessus scan report.</p>
Use a custom User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	Specifies which type of web browser Nessus impersonates while scanning.
Web Crawler		
Start crawling from	/	The URL of the first page that is tested. If multiple pages are required, use a colon delimiter to separate them (e.g., /:/php4:/base).
Excluded pages (regex)	/server_privileges\ .php <> log out	<p>Specifies portions of the web site to exclude from being crawled. For example, to exclude the /manual directory and all Perl CGI, set this field to: (^/manual) <> (\.pl(\?.*)?\$\$).</p> <p>Nessus supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).</p>
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 selected, Nessus follows dynamic links and may exceed the parameters set above.

Setting	Default Value	Description
Application Test Settings		
Enable generic web application tests	Disabled	Enables the options listed below.
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.
Try all HTTP methods	Disabled	This option instructs Nessus to also use POST requests for enhanced web form testing. By default, the web application tests only use GET requests, unless this option is enabled. 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

Setting	Default Value	Description
Test more than one parameter at a time per form	Disabled	<p>other web servers using this option.</p> <p>This setting manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, 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, Nessus would attempt <code>/test.php?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 discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for <code>/test.php?a=a=XSS&b=3&c=3&d=3</code> when the first value of each variable is 1. • Test random combinations of three or

Setting	Default Value	Description
		<p>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.</p> <ul style="list-style-type: none"> • 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	<p>This setting determines when a new flaw is targeted. This applies at the script level. Finding an XSS flaw does not disable searching for SQL injection or header injection, but unless otherwise specified, there is at most one report for each type on a given port. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported if they were caught by the same attack.</p> <p>This setting has three options:</p> <ul style="list-style-type: none"> • Stop after one flaw is found per web server (fastest): As soon as a flaw is found on a web server by a script, 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 (e.g., XSS), Nessus switches to the next parameter of the

Setting	Default Value	Description
		<p>same CGI, the next known CGI, or to the next port or server.</p> <ul style="list-style-type: none"> • Look for all flaws (slowest): Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.
URL for Remote File Inclusion	http://rfi.nessus.org/rfi.txt	During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to use for tests. By default, 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](#)
- [Enumerate Domain Users](#)
- [Enumerate Local Users](#)

Setting	Default Value	Description
General Settings		
Request information about the SMB Domain	Enabled	If enabled, domain users are queried instead of local users.

Enumerate Domain Users		
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		
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 Whitelist 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 Whitelist 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>

Provide your own list of known bad MD5 hashes	None	Additional known bad MD5 hashes can be uploaded 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 any matches are found when scanning a target, the description appears in the scan results. Hash-delimited comments (e.g., #) can also be used in addition to the comma-delimited ones.
Provide your own list of known good MD5 hashes	None	Additional known good MD5 hashes can be uploaded 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 any matches are found when scanning a target, and a description was provided for the hash, the description appears in the scan results. Standard hash-delimited comments (e.g., #) can optionally be used in addition to the comma-delimited ones.
Hosts file whitelist	None	Nessus checks system hosts files for signs of a compromise (e.g., 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 to be ignored by Nessus during a scan. Include one IP and one hostname (formatted identically to your hosts file on the target) per line in a regular text file.
Yara Rules		
Yara Rules File	None	A .yar file containing the YARA rules to be applied in the scan. You can only upload one file per scan, so include all rules in a single file. For more information, see yara.readthedocs.io .
File System Scanning		
Scan file system	Off	Turning on this option allows you to scan system directories and files on host computers. <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> Caution: Enabling this setting in scans targeting 10 or more hosts could result in performance degradation. </div>
Scan %Systemroot%	Off	Enables file system scanning to scan %Systemroot%.

Scan %ProgramFiles%	Off	Enables file system scanning to scan %ProgramFiles%.
Scan %ProgramFiles(x86)%	Off	Enables file system scanning to scan %ProgramFiles(x86)%.
Scan %ProgramData%	Off	Enables file system scanning to scan %ProgramData%.
Scan User Profiles	Off	Enables file system scanning to scan user profiles.
Custom Filescan Directories	None	A custom file that lists directories to be scanned by malware file scanning. List each directory on one line.

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>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.
Show missing patches that have been superseded	Enabled	If enabled, includes superseded patch information in the scan report.
Hide results from plugins initiated as a dependency	Enabled	If enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disable this setting.
Output		
Allow users to edit scan 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.

Setting	Default Value	Description
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.

Advanced Scan Settings

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

The Advanced settings include the following sections:

- [General Settings](#)
- [Performance](#)
- [Debug Settings](#)

Scan Type

The **Scan Type** setting appears for the following templates:

- Basic Network Scan
- Basic Web App Scan
- Credentialed Patch Audit
- Internal PCI Network Scan
- Malware Scan
- PCI Quarterly External Scan
- Policy Compliance Auditing
- SCAP and OVAL Auditing

All templates that include the **Scan Type** setting have the same options:

- **Default**
- **Scan low bandwidth links**
- **Custom**

The Nessus interface provides descriptions of each option.

Note: When **Custom** is selected, the **General** section appears. The **General** section includes the settings that appear on the following table.

The following table includes the default values for the Advanced Network Scan template. Depending on the template you select, certain 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, 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 in a random order	Disabled	By default, Nessus scans a list of IP addresses in sequential order. When enabled, Nessus scans the list of hosts in a random order across the entire target IP space. This is typically useful in helping to distribute the network traffic during large scans.
Performance		
Slow down the scan when network congestion is detected	Disabled	This enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity. If detected, Nessus throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Nessus automatically attempts to use the available space within the network pipe again.
Network timeout (in seconds)	5	Specifies the time that Nessus 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 Nessus scanner will perform against a single host at one time.

Setting	Default Value	Description
Max simultaneous hosts per scan	80	Specifies the maximum number of hosts that a Nessus scanner will scan at the same time.
Max number of concurrent TCP sessions per host	none	<p>Specifies the maximum number of established TCP sessions for a 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. E.g., if this option is set to 15, the SYN scanner sends 150 packets per second at most.</p>
Max number of concurrent TCP sessions per scan	none	This setting limits the maximum number of established TCP sessions for the entire scan, regardless of the number of hosts being scanned.
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.

Credentials

When you configure a scan or policy's **Credentials**, the Nessus scanner can be granted local access to scan the target system without requiring an agent. This can facilitate scanning of a very large network to determine local exposures or compliance violations. As noted, some steps of policy creation may be optional. Once created, the policy is saved with recommended settings.

Nessus leverages the ability to log into remote Linux hosts via Secure Shell (SSH); and with Windows hosts, Nessus leverages a variety of Microsoft authentication technologies. Note that 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.

Note: By default, when creating credentialed scans or policies, hosts are identified and marked with a **Tenable Asset Identifier (TAI)**. This globally unique identifier is written to the host's registry or file system and subsequent scans can retrieve and use the TAI.

This option is enabled (by default) or disabled in the [Advanced > General Settings](#) of a scan or policy's configuration settings: **Create unique identifier on hosts scanned using credentials**

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.

The following types of credentials are managed 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 is dependent on the privileges granted to the user account. The more privileges the scanner has via the login account (e.g., 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.

Cloud Services

Nessus supports Amazon Web Services (AWS), Microsoft Azure, Rackspace, and Salesforce.com.

AWS

Users can select Amazon AWS from the Credentials menu and enter credentials for compliance auditing an account in AWS.

Option	Description
AWS Access Key ID	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>In order 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• ap-northeast-1• ap-northeast-2• ap-southeast-1

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

Option	Description
Username	Username required to log in
Password	Password associated with the username
Client Id	Microsoft Azure Client Id
Subscription IDs	List subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions will be audited.

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

Nessus supports database authentication using PostgreSQL, DB2, MySQL SQL Server, Oracle, and MongoDB.

Database

Nessus supports two authentication methods for database credentials: Password or CyberArk (Nessus Manager only).

Password

Option	Description
Username	The username for the database.
Password	The password for the supplied username.
Database Type	Nessus supports Oracle, SQL Server, MySQL, DB2, Informix/DRDA, and PostgreSQL.

CyberArk

In Nessus Manager, you have the option of using CyberArk to manage your credentials. CyberArk is a popular enterprise password vault that helps you manage privileged credentials to use in a scan.

Option	Description
Username	The target system's username.
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.
CyberArk AIM Service URL	The URL of the AIM service. By default, this field uses /AIMWebService/v1.1/AIM.asmx.

Option	Description
Central Credential Provider Username	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Central Credential Provider Password	If the CyberArk Central Credential Provider is configured 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 Private Key Passphrase	(Optional) The passphrase for the private key, if required.
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.
CyberArk Account Details Name	The unique name of the credential you want to retrieve from CyberArk.
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, select this option. Refer to the custom_CA.inc documentation for how to use self-signed certificates.
Database Type	Nessus supports Oracle, SQL Server, MySQL, DB2, Informix/DRDA, and Post-

Option	Description
	greSQL.

MongoDB

Option	Description
Username	The username for the database.
Password	The password for the supplied username.
Database	Name of the database to audit.
Port	Port the database listens on.

Host

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.

These credentials are used to obtain local information from remote systems, including network devices, for patch auditing or compliance checks.

There is a field for entering the SNMPv3 user name for the account that will perform 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.

Option	Description
Username	The username for a SNMPv3 based account.
Port	Direct Nessus to scan a different port if SNMP is running on a port other than 161.
Security level	Select the security level for SNMP: authentication, privacy, or both.
Authentication algorithm	Select MD5 or SHA1 based on which algorithm the remote service supports.
Authentication password	The password for the username specified.
Privacy algorithm	The encryption algorithm to use for SNMP traffic.
Privacy password	A password used to protect encrypted SNMP communication.

SSH

On Linux systems and supported network devices, Nessus uses Secure Shell (SSH) protocol version 2 based programs (e.g., OpenSSH, Solaris SSH, etc.) for host-based checks.

This mechanism encrypts the data in transit to protect it from being viewed by sniffer programs. Nessus supports five types of authentication methods for use with SSH: username and password, public/private keys, digital certificates, and Kerberos.

Users can select SSH settings from the **Credentials** menu and enter credentials for scanning Linux systems.

These credentials are used to obtain local information from remote Linux systems for patch auditing or compliance checks.

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

Global Credential Settings

There are four settings for SSH credentials that apply to all SSH Authentication methods.

Option	Default Value	Description
known_hosts file	none	If an SSH known_hosts file is available and provided as part of the Global Credential Settings of the scan policy in the known_hosts file field, Nessus will only attempt to log into hosts in this file. This can ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log into a system that may not be under your control.
Preferred port	22	This option can be set 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 will impersonate while scanning.
Attempt least	Cleared	Enables or disables dynamic privilege escalation. When enabled,

Option	Default Value	Description
privilege (experimental)		<p>Nessus attempts to run the scan with an account with lesser privileges, even if the Elevate privileges with option is enabled. If a command fails, Nessus will escalate privileges. Plugins 102095 and 102094 report which plugins ran with or without escalated privileges.</p> <p>Note: Enabling this option may increase scan run time by up to 30%.</p>

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, the public key is used to encrypt data and the private key is used 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. Formats from other SSH applications, including PuTTY and SSH Communications Security, must be converted to OpenSSH public key format.

The most effective credentialled 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 has been 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 only accept certain types of encryption. Check your SSH server to ensure the correct algorithm is supported.

Nessus encrypts all passwords stored in policies. However, the use of SSH keys for authentication rather than SSH passwords is recommended. This helps ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log in to a system that may not be under your control.

Note: For supported network devices, Nessus will only support the network device's username and password for SSH connections.

If an account other than root must be used for privilege escalation, it can be specified 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 or DSA Open SSH key file of the user.
Private key passphrase	Passphrase of the Private Key.
Elevate privileges with	Allows for increasing privileges once authenticated.

Certificate

Option	Description
Username	Username of the account which is being used for authentication on the host system.
User Certificate	RSA or DSA Open SSH certificate file of the user.
Private Key	RSA or DSA Open SSH key file 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
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 the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Central Credential Provider Password	If the CyberArk Central Credential Provider is configured 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 Private Key Passphrase	(Optional) The passphrase for the private key, if required.
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.

Option	Description
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 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 a user is granted a TGT, it can be used 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. Note that 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	This option can be set 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. Note that if you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.
Realm	The Realm is the authentication domain, usually noted as the domain name of the target (e.g., example.com).
Elevate privileges with	Allows for increasing privileges once authenticated.

If Kerberos is used, sshd must be configured with Kerberos support to verify the ticket with the KDC. Reverse DNS lookups must be properly configured 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.

Thycotic Secret Server Authentication

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 that the secret is stored as on the Thycotic server. It is referred to as the “Secret Name” on the Thycotic server.
Thycotic Secret Server URL (required)	This is used to set the transfer method, target , and target directory for the scanner. The value can be found in Admin > Configuration > Application Settings > Secret Server URL on the Thycotic server. For example consider the following address https://pw.mydomain.com/SecretServer/ . We will parse this to know that https defines it is a ssl connection, pw.mydomain.com is the target address, /SecretServer/ is the root directory.
Thycotic Login Name (required)	The username to authenticate to the Thycotic server.
Thycotic Password (required)	The password associated with the Thycotic Login Name.
Thycotic Organization (required)	This value is used in cloud instances of Thycotic to define which organization your query should hit.
Thycotic Domain (optional)	This is an optional value set if the domain value is set 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.

BeyondTrust

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.
<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>	
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 will be requested.
Use privilege escalation	If enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, it will use it for the scan.

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. Additionally, Nessus supports several different types of authentication methods for Windows-based systems: CyberArk, Kerberos, LM Hash, NTLM Hash, and Thycotic Secret Server.

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. Note that 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 a variety of 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 field is optional and Nessus will be able to log on with domain credentials without this field. 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 onto the local server, the username of Administrator is used with the password of that account. To log onto the domain, the Administrator username would also be used, but with the domain password and the name of the domain.

When multiple SMB accounts are configured, Nessus will try to log in with the supplied credentials sequentially. Once Nessus is able to authenticate with a set of credentials, it will check 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 a variety of security checks for Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 that are more accurate if a domain account is provided. Nessus does attempt to try several checks in most cases 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, Inc. blog post [Dynamic Remote Registry Auditing - Now you see it, now you don't!](#)

Credentialed scans on Windows systems require that a full administrator level account be used. 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 will 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.

Global Credential Settings

Option	Default	Description
Never send credentials in the clear	Enabled	For security reasons, Windows credentials are not sent in the clear by default.
Do not use NTLMv1 authentication	Enabled	If this option is disabled, then it is theoretically possible to trick Nessus into attempting to log into a Windows server with domain credentials via the NTLM version 1 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	Disabled	This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be run-

Option	Default	Description
Registry service during the scan		ning in order for Nessus to execute some Windows local check plugins.
Enable administrative shares during the scan	Disabled	This option will allow Nessus to access certain registry entries that can be read with administrator privileges.

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
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 the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Central Credential Provider Password	If the CyberArk Central Credential Provider is configured 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	The file that contains the PEM certificate used to communicate with the Cyber-

Option	Description
Certificate	Ark host.
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.
PolicyId	The PolicyID assigned to the credentials you would like to retrieve from the CyberArk Central Credential Provider.
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.
CyberArk Account Details Name	The unique name of the credential you want to retrieve from CyberArk.

Kerberos

Option	Default	Description
Password	none	Like with other credentials methods, this is the user password on the target system. This is a required field.
Key Distribution Center	none	This host supplies the session tickets for the user. This is a required field.

Option	Default	Description
(KDC)		
KDC Port	88	This option can be set to direct Nessus to connect to the KDC if it is running on a port other than 88.
KDC Transport	TCP	Note that 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 field.

LM Hash

Option	Description
Username	The target system's username.
Hash	Hash being utilized.
Domain	The Windows domain of the specified user's name.

NTLM Hash

Option	Description
Username	The target system's username.
Hash	Hash being utilized.
Domain	The Windows domain of the specified user's name.

Thycotic Secret Server

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	(Required) The value you want Nessus to use when setting the transfer method,

Secret Server URL	<p>target, and target directory for the scanner. Find the value on the Thycotic server, in Admin > Configuration > Application Settings > Secret Server URL.</p> <p>For example, if you type <code>https://pw.mydomain.com/SecretServer</code>, Nessus determines it is an SSL connection, that <code>pw.mydomain.com</code> is the target address, and that <code>/SecretServer</code> is the root directory.</p>
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 Nessus query should target.
Thycotic Domain	The domain, if set for the Thycotic server.
Private Key	If enabled, Nessus uses key-based authentication for SSH connections instead of password authentication.
Verify SSL Certificate	If enabled, Nessus verifies the SSL Certificate on the Thycotic server. For more information about using self-signed certificates, see Custom SSL Certificates .

BeyondTrust

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> <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>
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 will be requested.
Use privilege escalation	If enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, it will use it for the scan.

Miscellaneous

This section includes information and settings for credentials in the **Miscellaneous** pages.

ADSI

ADSI requires the domain controller information, domain, and domain admin and password.

ADSI allows Nessus to query an ActiveSync server to determine if any Android or iOS-based devices are connected. Using the credentials and server information, Nessus authenticates to the domain controller (not the Exchange server) to directly query it for device information. This feature does not require any ports be specified in the scan policy. These settings are required for mobile device scanning.

Option	Description
Domain Controller	Name of the domain controller for ActiveSync
Domain	Name of the Windows domain for ActiveSync
Domain Admin	Domain admin's username
Domain Password	Domain admin's password

Nessus supports obtaining the mobile information from Exchange Server 2010 and 2013 only; Nessus cannot retrieve information from Exchange Server 2007.

IBM iSeries

IBM iSeries only requires an iSeries username and password.

Palo Alto Networks PAN-OS

Palo Alto Networks PAN-OS requires a PAN-OS username and password, management port number, and you can enable HTTPS and verify the SSL certificate.

Red Hat Enterprise Virtualization (RHEV)

RHEV requires username, password, and network port. Additionally, you can provide verification for the SSL certificate.

Option	Description
Username	Username to login to the RHEV server. This is a required field.

Option	Description
Password	Username to the password to login to the RHEV server. This is a required field.
Port	Port to connect to the RHEV server.
Verify SSL Certificate	Verify that the SSL certificate for the RHEV server is valid.

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. Additionally, you have the option of not enabling SSL certificate verification:

Option	Description
Username	Username to login to the ESXi server. This is a required field.
Password	Username to the password to login to the ESXi server. This is a required field.
Do not verify SSL Certificate	Do not verify that the SSL certificate for the ESXi server is valid.

VMware vCenter SOAP API

VMware vCenter SOAP API allows you to access vCenter. This requires a username, password, vCenter hostname, and vCenter port.

Additionally, you can require HTTPS and SSL certificate verification.

Credential	Description
vCenter Host	Name of the vCenter host. This is a required field.
vCenter Port	Port to access the vCenter host.
Username	Username to login to the vCenter server. This is a required field.
Password	Username to the password to login to the vCenter server. This is a required field.

Credential	Description
HTTPS	Connect to the vCenter via SSL.
Verify SSL Certificate	Verify that the SSL certificate for the ESXi server is valid.

X.509

For X.509, you will need to supply the client certificate, client private key, its corresponding passphrase, and the trusted Certificate Authority's (CA) digital certificate.

Mobile

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 if 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 if 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 if 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 (required)	The Billing ID provided for MaaS360
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

MobileIron

Option	Description
VSP Admin Portal URL	The server URL Nessus uses to authenticate to the MobileIron administrator portal.
Port	(Optional) The port Nessus uses to authenticate to MobileIron (typically, port

	443).
Username	The username for the account you want Nessus to use to authenticate to MobileIron.
Password	The password for the account you want Nessus to use to authenticate to MobileIron.
HTTPS	(Optional) When enabled, Nessus uses an encrypted connection to authenticate to MobileIron.
Verify SSL Certificate	When enabled, Nessus verifies that the SSL Certificate on the server is signed by a trusted CA.

Patch Management

Nessus Manager can leverage credentials for the Red Hat Network Satellite, IBM BigFix, Dell KACE 1000, WSUS, and SCCM patch management systems to perform patch auditing on systems for which credentials may not be available to the Nessus scanner.

Options for these patch management systems can be found under **Credentials** in their respective drop-down boxes: Symantec Altiris, IBM BigFix, Red Hat Satellite Server, Microsoft SCCM, Dell KACE K1000, and Microsoft WSUS.

IT administrators are expected to manage the patch monitoring software and install any agents required by the patch management system on their systems.

Scanning with Multiple Patch Managers

If you provide multiple sets of credentials to Nessus for patch management tools, Nessus uses all of them. Available credentials are:

- Credentials supplied to directly authenticate to the target
- Dell KACE 1000
- IBM BigFix
- Microsoft System Center Configuration Manager (SCCM)
- Microsoft Windows Server Update Services (WSUS)
- Red Hat Network Satellite Server
- Symantec Altiris

If you provide credentials for a host, as well as one or more patch management systems, 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 Mac OS X systems. Nessus and Tenable.sc have the ability to query KACE K1000 to verify whether or not patches are installed on systems managed by KACE K1000 and display the patch information through the Nessus or Tenable.sc user interface.

- 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 Nessus is able to connect to the target system, it performs checks on that system and ignores KACE K1000 output.
- The data returned to Nessus by KACE K1000 is only as current as the most recent data that the KACE K1000 has obtained from its managed hosts.

KACE K1000 scanning uses four Nessus plugins.

- `kace_k1000_get_computer_info.nbin` (Plugin ID 76867)
- `kace_k1000_get_missing_updates.nbin` (Plugin ID 76868)
- `kace_k1000_init_info.nbin` (Plugin ID 76866)
- `kace_k1000_report.nbin` (Plugin ID 76869)

You must provide credentials for the Dell KACE K1000 system for K1000 scanning to work properly.

Under the **Credentials** tab, select **Patch Management**, then select **Dell KACE K1000**.

Option	Default	Description
Server	none	KACE K1000 IP address or system name. This is a required field.
Database Port	3306	Port the K1000 database is running on (typically TCP 3306).
Organization Database Name	ORG1	The name of the organization component for the KACE K1000 database. This component will begin with the letters ORG and end with a number that corresponds with the K1000 database username.
Database Username	none	Username required to log into the K1000 database. R1 is the default if no user is defined. The username will begin with the letter R. This username will end in the same number that represents the number of the organization to scan. This is a required field
K1000 Database Password	none	Password required to authenticate the K1000 Database Username. This is a required field.

IBM BigFix

IBM BigFix is available from IBM to manage the distribution of updates and hotfixes for desktop systems. Nessus and Tenable.sc have the ability to query IBM BigFix to verify whether or not patches are installed on systems managed by IBM BigFix and display the patch information.

- If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore IBM BigFix output.
- The data returned to Nessus by TEM is only as current as the most recent data that the IBM BigFix server has obtained from its managed hosts.

IBM BigFix scanning uses five Nessus plugins:

- Patch Management: Tivoli Endpoint Manager Compute Info Initialization (Plugin ID 62559)
- Patch Management: Missing updates from Tivoli Endpoint Manager (Plugin ID 62560)
- Patch Management: IBM Tivoli Endpoint Manager Server Settings (Plugin ID 62558)
- Patch Management: Tivoli Endpoint Manager Report (Plugin ID 62561)
- Patch Management: Tivoli Endpoint Manager Get Installed Packages (Plugin ID 65703)

Credentials for the IBM BigFix server must be provided for IBM BigFix scanning to work properly.

Option	Default	Description
Web Reports Server	None	Name of IBM BigFix Web Reports Server
Web Reports Port	none	Port that the IBM BigFix Web Reports Server listens
Web Reports Username	none	Web Reports administrative username
Web Reports Password	none	Web Reports administrative username's password
HTTPS	Enabled	If the Web Reports service is using SSL
Verify SSL certificate	Enabled	Verify that the SSL certificate is valid

Package reporting is supported by RPM-based and Debian-based distributions that IBM 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 IBM BigFix officially supports them, there is no support available.

For local check plugins to trigger, only RHEL, CentOS, Scientific Linux, Oracle Linux, Debian, and Ubuntu are supported. The plugin Patch Management: Tivoli Endpoint Manager Get Installed Packages must be enabled.

In order to use these auditing features, you must make changes to the IBM BigFix server. You must import a custom analysis into IBM BigFix so that detailed package information is retrieved and made

available to Nessus. Before beginning, save the following text to a file on the IBM BigFix system, and name it with a .bes extension.

```
<?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 Nessus 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>Fri, 01 Feb 2013 15:54:09 +0000</Value>
        </MIMEField>
        <Domain>BESC</Domain>
        <Property Name="Packages - With Versions (Tenable)" ID="1"><![CDATA[if
(exists true whose (if true then (exists debianpackage) else false)) then unique
values of (name of it & "|" & version of it as string & "|" & "deb" & "|" &
architecture of it & "|" & architecture of operating system) of packages whose
(exists version of it) of debianpackages else if (exists true whose (if true then
(exists rpm) else false)) then unique values of (name of it & "|" & version of it as
string & "|" & "rpm" & "|" & architecture of it & "|" & architecture of operating
system) of packages of rpm else "<unsupported>" ]]></Property>
    </Analysis>
</BES>
```

Microsoft System Center Configuration Manager (SCCM)

Microsoft System Center Configuration Manager (SCCM) is available to manage large groups of Windows-based systems. Nessus has the ability to query the SCCM service to verify whether or not patches are installed on systems managed by SCCM and display the patch information through the Nessus or Tenable.sc web interface.

- If the credentialed check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore SCCM output.

- The data returned by SCCM is only as current as the most recent data that the SCCM server has obtained from its managed hosts.
- Nessus connects to the server that is running the SCCM site (e.g., credentials must be valid for the SCCM service, meaning an admin account in SCCM with the privileges to query all the data in the SCCM MMC). This server may also run the SQL database, or the database as well as the SCCM repository can be on separate servers. When leveraging this audit, Nessus must connect to the SCCM Server, not the SQL or SCCM server if they are on a separate box.

Nessus SCCM patch management plugins support SCCM 2007 and SCCM 2012.

SCCM scanning is performed using four Nessus plugins.

- Patch Management: SCCM Server Settings (Plugin ID 57029)
- Patch Management: Missing updates from SCCM(Plugin ID 57030)
- Patch Management: SCCM Computer Info Initialization(Plugin ID 73636)
- Patch Management: SCCM Report(Plugin ID 58186)

Credentials for the SCCM system must be provided for SCCM scanning to work properly. Under the Credentials tab, select Patch Management and then Microsoft SCCM.

Credential	Description
Server	SCCM IP address or system name
Domain	The domain the SCCM server is a part of
Username	SCCM admin username
Password	SCCM admin password

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. Nessus and Tenable.sc have the ability to query WSUS to verify whether or not patches are installed on systems managed by WSUS and display the patch information through the Nessus or Tenable.sc web interface.

- If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore WSUS output.

- The data returned to Nessus by WSUS is only as current as the most recent data that the WSUS server has obtained from its managed hosts.

WSUS scanning is performed using three Nessus plugins.

- Patch Management: WSUS Server Settings (Plugin ID 57031)
- Patch Management: Missing updates from WSUS (Plugin ID 57032)
- Patch Management: WSUS Report (Plugin ID 58133)

Credentials for the WSUS system must be provided for WSUS scanning to work properly. Under the Credentials tab, select Patch Management and then Microsoft WSUS.

Credential	Default	Description
Server	None	WSUS IP address or system name
Port	8530	Port WSUS is running on (typically TCP 80 or 443)
Username	none	WSUS admin username
Password	none	WSUS admin password
HTTPS	Enabled	If the WSUS service is using SSL
Verify SSL certificate	Enabled	Verify that the SSL certificate is valid

Red Hat Satellite Server

Red Hat Satellite is a systems management platform for Linux-based systems. Nessus has the ability to 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, Inc., the RHN Satellite plugin will also work with Spacewalk Server, the Open Source Upstream Version of Red Hat Satellite. Spacewalk has the capability of managing distributions based on Red Hat (RHEL, CentOS, Fedora) and SUSE. Tenable supports the Satellite server for Red Hat Enterprise Linux.

- If the credential check sees a system, but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore RHN Satellite output.
- The data returned to Nessus by RHN Satellite is only as current as the most recent data that the Satellite server has obtained from its managed hosts.

Satellite scanning is performed using five Nessus plugins:

- Patch Management: Patch Schedule From Red Hat Satellite Server (Plugin ID 84236)
- Patch Management: Red Hat Satellite Server Get Installed Packages (Plugin ID 84235)
- Patch Management: Red Hat Satellite Server Get Managed Servers (Plugin ID 84234)
- Patch Management: Red Hat Satellite Server Get System Information (Plugin ID 84237)
- Patch Management: Red Hat Satellite Server Settings (Plugin ID 84238)

If the RHN Satellite server is version 6, three additional Nessus plugins are used:

- Patch Management: Red Hat Satellite Server Get Installed Packages (Plugin ID 84231)
- Patch Management: Red Hat Satellite 6 Settings (Plugin ID 84232)
- Patch Management: Red Hat Satellite 6 Report (Plugin ID 84233)

Red Hat Satellite 6 Server

Credential	Default	Description
Satellite server	none	RHN Satellite IP address or system name
Port	443	Port Satellite is running on (typically TCP 80 or 443)
Username	none	Red Hat Satellite username
Password	none	Red Hat Satellite password
HTTPS	Enabled	If the Red Hat Satellite service is using SSL
Verify SSL Certificate	Enabled	Verify that the SSL certificate is valid

Symantec Altiris

Altiris is available from Symantec to manage the distribution of updates and hotfixes for Linux, Windows, and Mac OS X systems. Nessus and Tenable.sc have 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 Nessus or Tenable.sc web interface.

- If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore Altiris output.

- The data returned to Nessus by Altiris is only as current as the most recent data that the Altiris has obtained from its managed hosts.
- Nessus connects to the Microsoft SQL server that is running on the Altiris host (e.g., credentials must be valid for the MSSQL database, meaning a database account with the privileges to query all the data in the Altiris MSSQL database). The database server may be run on a separate host from the Altiris deployment. When leveraging this audit, Nessus must connect to the MSSQL database, not the Altiris server if they are on a separate box.

Altiris scanning is performed using four Nessus plugins.

- `symantec_altiris_get_computer_info.nbin` (Plugin ID 78013)
- `symantec_altiris_get_missing_updates.nbin` (Plugin ID 78012)
- `symantec_altiris_init_info.nbin` (Plugin ID 78011)
- `symantec_altiris_report.nbin` (Plugin ID 78014)

Credentials for the Altiris Microsoft SQL (MSSQL) database must be provided for Altiris scanning to work properly. Under the Credentials tab, select Patch Management and then Symantec Altiris.

Credential	Default	Description
Server	none	Altiris IP address or system name. This is a required field.
Database Port	5690	Port the Altiris database is running on (Typically TCP 5690)
Database Name	Symantec_CMDB	The name of the MSSQL database that manages Altiris patch information.
Database User-name	None	Username required to log into the Altiris MSSQL database. This is a required field.
Database Pass-word	none	Password required to authenticate the Altiris MSSQL database. This is a required field.
Use Windows Authentication	Disabled	Denotes whether or not to use NTLMSSP for compatibility with older Windows Servers, otherwise it will use Kerberos

To ensure Nessus can properly utilize Altiris to pull patch management information, it must be configured to do so.

Plaintext Authentication

Caution: Using plaintext credentials is not recommended. Use encrypted authentication methods when possible.

If a secure method of performing credential 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, SNMPv1/v2c, and telnet/rsh/rexec.

By supplying credentials, Nessus may have the ability to do more extensive checks to determine vulnerabilities. HTTP credentials supplied will be used 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 (e.g., Authentication failed!).
Use authenticated regex on HTTP headers	Disabled	Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to better determine authentication state.

Option	Default	Description
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, e.g., /login.html.
Login submission page	The action parameter for the form method. For example, the login form for <form method="POST" name="auth_form" action="/login.php"> would be /login.php.
Login parameters	Specify the authentication parameters (e.g., login=%USER%&password=%PASS%). If the keywords %USER% and %PASS% are used, they will be substituted with values supplied on the Login configurations drop-down box. This field can be used to provide more than two parameters if required (e.g., a group name or some other piece of information is required for the authentication process).
Check authentication on	The absolute path of a protected web page that requires authentication, to better assist Nessus in determining authentication status, e.g., /admin.html.

Option	Description
page	
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 (e.g., web browser, web proxy, etc.) with the HTTP cookies import settings. A cookie file can be uploaded so that Nessus uses the cookies when attempting to access a web application. The cookie file must be in Netscape format.

telnet/rsh/rexec

The telnet/rsh/rexec authentication section is also username and password, but there are additional 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. Up to 4 SNMP community strings can be configured.

Compliance

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.

The advantage of using Nessus to perform vulnerability scans and compliance audits is that all of this data can be obtained at one time. Knowing how a server is configured, how it is patched and what vulnerabilities are present can help 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.

Audit Capability	Required Credentials
Adtran AOS	SSH
Amazon AWS	Amazon AWS
Blue Coat ProxySG	SSH
Brocade FabricOS	SSH
Check Point GAiA	SSH
Cisco IOS	SSH
Citrix XenServer	SSH
Database	Database credentials
Dell Force10 FTOS	SSH
Extreme ExtremeXOS	SSH
FireEye	SSH
Fortigate FortiOS	SSH
HP ProCurve	SSH

Huawei	SSH
IBM iSeries	IBM iSeries
Juniper Junos	SSH
Microsoft Azure	Microsoft Azure
Mobile Device Manager	AirWatch/Apple Profile Manager/MobileironÂ
MongoDB	MongoDB
NetApp Data ONTAP	SSH
Palo Alto Networks PAN-OS	PAN-OS
Rackspace	Rackspace
RHEV	RHEV
Salesforce.com	Salesforce SOAP API
SonicWALL SonicOS	SSH
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

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 settings for each option are described in the following table.

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	<p>(SCAP Version 1.2 only) The Data Stream ID that you copied from the SCAP XML file.</p> <p>Example:</p> <div style="border: 1px solid #ccc; padding: 10px;"><pre><data-stream id="scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip"></pre></div>
SCAP Benchmark ID	None	<p>The Benchmark ID that you copied from the SCAP XML file.</p> <p>Example:</p> <div style="border: 1px solid #ccc; padding: 10px;"><pre><xccdf:Benchmark id="xccdf_gov.nist_benchmark_USGCB-Windows-7"></pre></div>
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 enables you to select security checks by **Plugin Family** or individual plugins checks.

Clicking on the **Plugin Family** allows you to enable (**green**) or disable (**gray**) the entire family. Selecting a family displays the list of its plugins. Individual plugins can be enabled or disabled to create very specific scans.

A family with some plugins disabled is **blue** and displays **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** displays the plugin output that would be seen in a report.

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

When a scan or policy is created and saved, it records all of the plugins that are initially selected. When new plugins are received via a plugin update, they are automatically enabled if the family they are associated with is enabled. If the family has been disabled or partially enabled, new plugins in that family are also automatically disabled.

Caution: The **Denial of Service** family contains some plugins that could cause outages on a network if the Safe Checks option is not enabled, in addition to some useful checks that will not cause any harm. The **Denial of Service** family can be used in conjunction with Safe Checks to ensure that any potentially dangerous plugins are not run. However, it is recommended that the **Denial of Service** family not be used on a production network unless scheduled during a maintenance window and with staff ready to respond to any issues.

Special Use Templates

Note: For more information about performing custom audits with Nessus, see the [Custom Auditing video](#).

Compliance

Nessus compliance auditing can be configured using one or more of the following **Scanner** and **Agent** templates.

- Audit Cloud Infrastructure
- MDM Config Audit
- Offline Config Audit
- SCAP and OVAL Auditing
- Policy Compliance Auditing

Mobile Device

With Nessus Manager, the Nessus Mobile Devices plugin family provides the ability to obtain information from devices registered in a Mobile Device Manager (MDM) and from Active Directory servers that contain information from Microsoft Exchange Servers.

- To query for information, the Nessus scanner must be able to reach the Mobile Device Management servers. You must ensure no screening devices block traffic to these systems from the Nessus scanner. In addition, Nessus must be given administrative credentials (e.g., domain administrator) to the Active Directory servers.
- To scan for mobile devices, Nessus must be configured with authentication information for the management server and the mobile plugins. Since Nessus authenticates directly to the management servers, a scan policy does not need to be configured to scan specific hosts.
- For ActiveSync scans that access data from Microsoft Exchange servers, Nessus will retrieve information from phones that have been updated in the last 365 days.

Payment Card Industry (PCI)

Tenable offers two **Payment Card Industry Data Security Standard (PCI DSS)** templates: one for testing internal systems (11.2.1) and one for Internet facing systems (11.2.2). Also, these scan templates

may also be used to complete scans after significant changes to your network, as required by PCI DSS 11.2.3.

Template	Product	Description
PCI Quarterly External Scan	Tenable.io Only	<p>The PCI Quarterly External Scan template is only available in Tenable.io. Using this template, Tenable.io tests for all PCI DSS external scanning requirements, including web applications.</p> <p>The scan results obtained using the PCI Quarterly External Scan template may be submitted to Tenable, Inc. (an Approved Scanning Vendor) for PCI validation.</p> <p>Refer to the Scan Results section for details on creating, reviewing, and submitting PCI scan results.</p>
PCI Quarterly External Scan (Unofficial)	Nessus Manager	For Nessus Manager and Nessus Professional versions, Tenable provides the PCI Quarterly External Scan (Unofficial) template.
	Nessus Professional	<p>This template can be used to simulate an external scan (PCI DSS 11.2.2) to meet PCI DSS quarterly scanning requirements. However, the scan results from the Unofficial template cannot be submitted to Tenable, Inc. for PCI Validation.</p> <p>The PCI Quarterly External Scan (Unofficial) Template performs the identical scanning functions as the Tenable.io version of this template.</p>
PCI Quarterly External Scan (Unofficial)	Nessus Manager	The Internal PCI Network Scan template can be used to meet PCI DSS Internal scanning requirement (11.2.1).
	Nessus Professional	

SCAP and OVAL

The National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) is a set of policies for managing vulnerabilities and policy compliance in government agencies. It relies on multiple open standards and policies, including OVAL, CVE, CVSS, CPE, and FDCC policies.

- SCAP compliance auditing requires sending an executable to the remote host.
- Systems running security software (e.g., McAfee Host Intrusion Prevention), may block or quarantine the executable required for auditing. For those systems, an exception must be made for the 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.

Unofficial PCI ASV Validation Scan

Approved Scanning Vendors (ASVs) are organizations that validate adherence to certain Data Security Standards (DSS) requirements by performing vulnerability scans of internet facing environments of merchants and service providers.

Tenable, Inc. is a Payment Card Industry (PCI) ASV, and is certified to validate vulnerability scans of internet-facing systems for adherence to certain aspects of the PCI DSS and Tenable.io is a validated ASV solution.

Nessus Professional and Nessus Manager features two PCI related scan templates: Internal PCI Network Scan and Unofficial PCI Quarterly External Scan.

Internal PCI Network Scan

This template creates scans that may be used to satisfy internal (PCI DSS 11.2.1) scanning requirements for ongoing vulnerability management programs that satisfy PCI compliance requirements. These scans may be used for ongoing vulnerability management and to perform rescans until passing or clean results are achieved. Credentials can optionally be provided to enumerate missing patches and silent-side vulnerabilities.

Note: while the PCI DSS requires you to provide evidence of passing or "clean" scans on at least a quarterly basis, you are also required to perform scans after any significant changes to your network (PCI DSS 11.2.3).

Unofficial PCI Quarterly External Scan

The Unofficial PCI Quarterly External Scan template creates a scan that **simulates** an external scan (PCI DSS 11.2.2) performed by Tenable.io to meet PCI DSS quarterly scanning requirements. Although the results **may not be submitted for validation**, they may be used to see what "official" Tenable.io results might look like. Users that have external PCI scanning requirements should use this template in Tenable.io, which allows scanning unlimited times before submitting results to Tenable, Inc. for validation (Tenable.io is a validated ASV solution).

For more information on performing and submitting an official PCI Quarterly External Scan, see the [Tenable.io User Guide](#).

Submit Scan Results

Only Tenable.io customers have the option to submit their PCI scan results to Tenable, Inc. for PCI ASV validation.

When submitted, scan results are uploaded and the scan results can be reviewed from a PCI DSS perspective.

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](#)

Create a 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 scan template that you want to use.

4. Configure the scan's [settings](#).

5. If you want to launch the scan later, click the **Save** button.

The scan is saved.

-or-

If you want to launch the scan immediately, click the  button, and then click **Launch**.

The scan is saved and launched.

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. If you want to launch the scan later, click the **Save** button.

Tenable.io saves the scan.

-or-

If you want to launch the scan immediately, click the  button, then click **Launch**.

Tenable.io saves and launches the scan.

Modify Scan Settings

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. 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.

The settings are saved.

Configure an Audit Trail

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. (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, which displays the results that match the criteria that you entered in one or both boxes.

Compare Scan Results

You can compare two scan results to see differences between them. The comparison shows what is new since the baseline (i.e., the primary result selected), not a differential of the two results. You cannot compare imported scans or more than two scans.

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 new vulnerabilities are found, or how two scans may not be targeting the same hosts.

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 a scan baseline for the comparison, then click **Continue**.

The scan result differences are displayed.

Delete a Scan

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. 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 permanently delete the scan, 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 permanently delete, click the  button.

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

6. Click the **Delete** button.

The scan is deleted.

Tip: On the **Trash** page, in the upper right corner, click the **Empty Trash** button to permanently delete all scans in the **Trash** folder.

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 cannot be removed:

- My Scans
- All Scans
- Trash

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 displays 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 displays scans that you have deleted. In the **Trash** folder, you can permanently remove scans from your Nessus instance, or restore the scans to a selected folder. If you delete a folder that contains scans, all scans in that folder are moved to the **Trash** folder. Scans stored in the **Trash** folder are automatically deleted after 30 days.

My Scans

[Import](#)[New Folder](#)[!\[\]\(63397692ebc30b483e262b17faf660bb_img.jpg\) 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

These procedures can be performed by a standard user or administrator.

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.

The folder is created and appears 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.

The folder is deleted. If the folder contained scans, those scans are moved to the **Trash** folder.

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 the [Scan and Policy Templates](#) topic.

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	▼ X
<input type="checkbox"/> Internal PCI Network Scan Policy	Internal PCI Network Scan	Today at 10:36 AM	▼ X

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 (e.g., 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.

The policy is saved.

Modify Policy Settings

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. 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.

The settings are saved.

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  button.

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

4. Click the **Delete** button.

The policy is deleted.

About Nessus Plugins

As information about new vulnerabilities are discovered and released into the general public domain, Tenable, Inc. research staff designs programs to enable Nessus to detect them.

These programs are named *plugins*, and are written in the Nessus proprietary scripting language, called *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.

Nessus supports the Common Vulnerability Scoring System (CVSS) and supports both v2 and v3 values simultaneously. If both CVSS2 and CVSS3 attributes are present, both scores are calculated. However in determining the Risk Factor attribute, currently the CVSS2 scores take precedence.

Plugins also are utilized to obtain configuration information from authenticated hosts to leverage 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

Severity	Plugin Name	Count
Critical	Common Platform Enumeration (CPE)	1
High	Ethernet Card Manufacturer Selection	1
Medium	Host Fully Qualified Domain Name (FQDN) Resolution	1
Low	ICMP Veneerizing Request Remote Denial of Service	1
Critical	Microsoft Windows SMB Log In Possible	1
Medium	Microsoft Windows SMB Null Session Authentication Disclosure	1
Critical	Microsoft Windows SMB Registry - Remote Control Across the Windows Registry	1
Medium	Microsoft Windows SMB Service Detection	1
Low	Microsoft Windows XP Unsigned Installation Detection	1
Critical	MS16-047 Microsoft Windows Server Service Conflict RPC Request Handling Remote Code Execution (958644) (unauthenticated check)	1
Critical	MS19-002 Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (unauthenticated check)	1
Medium	Nessus Scan Information	1
Low	Nessus SHM scanner	1
Informational	Nessus Windows Scan Test Performed with Admin Privileges	1

Host Details

Vulnerabilities

Details of a single host's plugin scan result

How do I get Nessus Plugins?

By default, plugins are set for automatic updates and Nessus 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 manually download plugins. 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.

Tip: Plugins are obtained from port 443 of plugins.nessus.org, plugins-customers.nessus.org, or plugins-us.nessus.org.

How do I update Nessus Plugins?

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

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

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, all of the plugin families are enabled.

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.

All the plugin families are disabled.

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
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

7. Click the plugin family that you want to include.

The list of plugins appears in the left navigation bar.

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	
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.

Each plugin is enabled.

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
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 **Search Plugin Families** box in the upper right corner.

- Click the **Save** button.

The policy is saved.

Plugin Rules

Plugin Rules allow you to hide or change the severity of any given plugin. In addition, rules can be limited to a specific host or specific time frame. From this page you can view, create, edit, and delete your rules.

The **Plugin Rules** option provides a facility to create a set of rules that dictate the behavior of certain plugins related to any scan performed. A rule can be based on the **Host** (or all hosts), **Plugin ID**, an optional **Expiration Date**, and manipulation of **Severity**.

This allows you to re-prioritize the severity of plugin results to better account for your organization's security posture and response plan.

Example Plugin Rule

Host: 192.168.0.6

Plugin ID: 79877

Expiration Date: 12/31/2016

Severity: Low

This rule is created for 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 12/31/2016. After 12/31/2016, the results of plugin ID 79877 will return 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.

The plugin rule is saved.

Modify a Plugin Rule

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 **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.

The settings are saved.

Delete a Plugin Rule

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 **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.

The plugin rule is deleted.

Customized Reports

On the **Customized Reports** page in Nessus Professional, you can customize the title and logo that appear on each report.

Customized Reports

You can add a custom name or logo for use when exporting HTML or PDF files from your scan results. Images must be in JPEG, GIF or PNG format with a max file size of 10MB and should not contain transparency.

Custom Name

Custom Logo

Customize Report Settings

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

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

The **My Scans** page appears.

2. In the left navigation bar, click **Customized Reports**.

3. In the **Custom Name** box, type the name that you want to appear on the report.

4. To upload a custom logo, click the **Upload** button.

A window appears in which you can select a file to upload.

5. Click the **Save** button.

Your custom title and logo appear on all future reports.

Scanners

By default, Tenable.io is configured with a regional, specific cloud scanner. In addition to using the default cloud scanner, users can also link Nessus scanners, NNM scanners, and Nessus Agents to Tenable.io.

Once linked to Tenable.io, use the Tenable.io key to add remote scanners to **Scanner Groups**. You can also manage and select remote scanners when configuring scans.

The **Linked Scanners** page displays scanner names, types, and permissions.

The **Scanners** page displays the Linking Key and a list of remote scanners. You can click on a linked scanner to view details about that scanner.

Scanners are identified by scanner type and indicate if the scanner has **Shared** permissions.

Remote scanners can be linked to Nessus Manager with the Linking Key or valid account credentials. Once linked, scanners can be managed locally and selected when configuring scans.

Scanners

Remote [scanners](#) can be linked to Nessus using the provided key. Once linked, they can be managed locally and selected when configuring scans. From this page you can view the current status of your scanners and drilldown to control all running scans.

Linking Key: [REDACTED](#)

<input type="checkbox"/>	Name	Status	Scans	Version	Linked On	Last Modified	Edit	Delete
<input type="checkbox"/>	centos7x64nh	Offline	0	N/A	July 24 at 8:10 PM	July 24 at 8:10 PM	Edit	Delete
<input checked="" type="checkbox"/>	Local Scanner	Online	0	6.11.0	June 16 at 4:35 PM	July 25 at 12:54 PM	Edit	Delete

Enable or Disable a Scanner

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

Enable a Scanner

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

The **My Scans** page appears.

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

3. In the scanners table, in the row for the scanner that you want to enable, hover over the  button.

 becomes .

4. Click the  button.

The scanner is enabled.

Disable a Scanner

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

The **My Scans** page appears.

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

3. In the scanners table, in the row for the scanner that you want to disable, hover over the  button.

 becomes .

4. Click the  button.

The scanner is disabled.

Remove a Scanner

This procedure can be performed by an administrator.

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

The **My Scans** page appears.

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

3. In the scanners table, in the row for the scanner that you want to remove, click the  button.

The scanner is removed.

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.

The **Agents** page displays the Linking Key and a list of linked agents. You can click on a linked agent to view details about that agent. There are four tabs available on the **Agents** page: **Linked Agents**, **Agent Groups**, **Blackout Windows**, and **Agent Settings**.

Once linked, an agent must be added to a group for use when configuring scans. Linked agents will automatically download plugins from the manager upon connection. Agents are automatically unlinked after a period of inactivity.

Note: Agents can take several minutes to download plugins, but it is required before an agent returns scan results.

Agents

Linked Agents **Agent Groups** **Blackout Windows** **Agent Settings**



Aagents can be linked to Nessus using the following [setup instructions](#). Once linked, they will automatically download all necessary plugins. This process takes several minutes and is required before an agent will return results.

Linking Key: [REDACTED]

Filter	Search Agents		14 Agents				
Name	Status	IP Address	Platform	Groups	Version	Last Plugin Update	Last Scanned
<script>alert('lol...')	Offline	[REDACTED]	Linux (debian6-...)	qa-agent	6.11.0	August 3	June 28
centos7-6101-d...	Offline	[REDACTED]	Linux (es7-x86-...)	qa-agent	6.11.0	August 3	June 28
centos7-6102-d...	Offline	[REDACTED]	Linux (es7-x86-...)	qa-agent	6.11.0	August 3	June 28
centos7-6103-d...	Offline	[REDACTED]	Linux (es7-x86-...)	qa-agent	6.11.0	August 3	June 28
centos7-6104-d...	Offline	[REDACTED]	Linux (es7-x86-...)	qa-agent	6.11.0	August 3	June 28
centos7-6105-d...	Offline	[REDACTED]	Linux (es7-x86-...)	qa-agent	6.11.0	August 3	June 28

Agent Groups

Agent groups are used to organize and manage the agents linked to your scanner. Each agent can be added to any number of groups and scans can be configured 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.

Modify Agent Settings

Use this procedure to modify agent settings in Nessus Manager.

To modify agent settings:

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. Click the **Agent Settings** tab.

4. Modify the [settings](#) as necessary.

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

Filter Agents

Use this procedure to filter agents in Nessus Manager.

To filter agents in the agents table:

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. Above the agents table, click the **Filter** button.

The **Filter** window appears.

4. Configure the options as necessary. Depending on the parameter you select, different options appear:

Parameter	Operator	Expression
IP Address	is equal to is not equal to contains does not contain	In the text box, type the IPv4 or IPv6 addresses on which you want to filter.
Last Connection Last Plugin Update Last Scanned	earlier than later than on not on	In the text box, type the date on which you want to filter.
Member of Group	is equal to is not equal to	From the drop-down list, select from your existing agent groups.

Parameter	Operator	Expression
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.
Version	is equal to is not equal to contains does not contain	In the text box, type the version you want to filter.

5. Click **Apply**.

The manager filters the list of agents to include only those that match your configured options.

Unlink an Agent

When you 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](#).

Use this procedure to unlink an agent in Nessus Manager.

To unlink a single agent:

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. For Nessus 7.1.1 and later: In the agents table, in the row for the agent that you want to unlink, click the  button.

-or-

For Nessus 7.1.0 and earlier: In the agents table, in the row for the agent that you want to unlink, click the  button.

A dialog box appears, confirming your selection to unlink the agent.

4. Click the **Unlink** button.

The manager unlinks the agent.

To unlink multiple agents:

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. In the agents table, click the check box in each row for each agent you want to unlink.

4. In the upper-right corner, click **Unlink**.

A dialog box appears, confirming your selection to unlink the agent.

5. Click the **Unlink** button.

The manager unlinks the agents.

Agent Groups

You can use agent groups to organize and manage the agents linked to your Nessus Manager. You can add an agent to more than one group, and configure scans to use these groups as targets. 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.sc. 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 must be imported into Tenable.sc. The .nessus file size affects hard drive space and bandwidth.

To manage agent groups, use the following procedures:

- [Create a New 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 Nessus Manager.

To create a new agent group:

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. Click the **Agent Groups** tab.

4. In the upper right corner, click the **New Group** button.

The **New Agent Group** window appears.

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

6. Click **Add**.

The new agent group appears in the table.

Modify an Agent Group

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

To modify an agent group:

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. Click the **Agent Groups** tab.

4. In the row for the agent group that you want to modify, click the  button.

The **Edit Agent Group** window appears.

5. Modify the name of the agent group as needed.

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

Delete an Agent Group

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

To delete an agent group:

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. Click the **Agent Groups** tab.

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

A dialog box appears, prompting you to confirm your deletion.

5. Click **Delete**.

Blackout Windows

Blackout windows apply to all linked agents and prevent the agents from receiving and applying software updates during scheduled windows. Agents still receive plugin updates and continue performing scheduled scans during these windows.

To manage blackout windows, use the following procedures:

- [Create a Blackout Window](#)
- [Modify a Blackout Window](#)
- [Delete a Blackout Window](#)

Create a Blackout Window

Blackout windows will apply to all linked agents and will prevent the agents from receiving and applying software updates during scheduled windows. Agents will still receive plugin updates and continue performing scheduled scans during these windows.

To create a blackout window for linked agents:

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. Click the **Blackout Windows** tab.

4. In the upper-right corner, click the **New Window** button.

The **New Blackout Window** page appears.

5. Configure the options as necessary.

6. Click **Save**.

The blackout window goes into effect and appears on the **Blackout Windows** tab.

Modify a Blackout Window

Use this procedure to manage a blackout window for agent scanning in Nessus Manager.

To modify a blackout window:

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. Click the **Blackout Windows** tab.

4. In the blackout window table, click the blackout window you want to modify.

The **Blackout Windows / <Name>** window appears, where **<Name>** is the name of the selected blackout window.

5. Modify the options as necessary.

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

Delete a Blackout Window

Use this procedure to delete a blackout window for agent scanning in Nessus Manager.

To delete a blackout window for agent scanning:

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. Click the **Blackout Windows** tab.

4. In the blackout window table, in the row for the blackout window that you want to delete, click the delete button (✖).

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

5. Click **Delete** to confirm the deletion.

Additional Resources

This section contains the following resources:

- [About Nessus Plugins](#)
- [About Scan Targets](#)
- [Amazon Web Services](#)
- [Command Line Operations](#)
- [Create a Limited Plugin Policy](#)
- [Manage SSL Certificates](#)
- [Default Data Directories](#)
- [Manage Logs Using log.json](#)
- [Nessus Credentialized Checks](#)
- [Offline Update Page Details](#)
- [PCI ASV Validation Scan](#)
- [Run Nessus as Non-Privileged User](#)
- [Scan Targets](#)
- [System Tray Application](#)

Agent Software Footprint

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

Agent Footprint on Disk	Total Software Footprint on Disk	RAM Usage While Not Scanning	Average RAM Usage While Scanning/Peak	Network Bandwidth Usage
6.6 MB	800 MB including plugin updates	<10%	45 MB RAM	~1.5 MB/day* Expected to be much higher in normal conditions.

*Assuming only one scan a day with no plugin updates. Used nethogs program to collect network usage (sent/received) of nessusd. After a single scan that detected 66 vulnerabilities on the agent host, 0.855 MB was sent and received (breakdown: .771 MB sent, .084 MB received). After two total scans, 1.551 MB was sent and 0.204 MB was received. Set to > 1 MB day as the polling for jobs adds up (~0.008 MB per poll).

Agent Host System Utilization

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

Generally, a Nessus Agent uses 40 MB of RAM (all pageable). A Nessus Agent uses almost no CPU while idle, but is designed to use up to 100% of CPU when available during jobs.

To measure network utilization when uploading results, Tenable monitored Agent uploads intoTenable.io over a 7 day period. Of over 36,000 uploads observed:

- The average size was 1.6 MB.
- The largest size was 37 MB.
- 90% of uploads were 2.2 MB or less.
- 99% of uploads were 5 MB or less.
- Nessus Agent consumes 40 MB of RAM when dormant.
- The Watchdog service consumes 3 MB.
- Plugins consume approximately 300 MB of disk space (varies based on operating system).
- Scan results from Nessus Agents to Nessus Manager and Tenable.io range between 2-3 MB.
- Check-in frequency starts at 30 seconds and is adjusted by Nessus Manager orTenable.io based on the management system load (number of agents).

Amazon Web Services

For information on integrating Nessus with Amazon Web Services, see the [Nessus \(BYOL\) on Amazon Web Services Quick Start Guide](#).

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 data is recorded and is accepted when you press the **Enter** key.

The following topics are included in this section:

- [Start or Stop Nessus](#)
- [Start or Stop Nessus Agent](#)
- [Nessus-Service](#)
- [Nessuscli](#)
- [Nessuscli Agent](#)
- [Update Nessus Software](#)

Start or Stop Nessus

The following represent best practices for starting and stopping Nessus.

Mac OS X

1. Navigate to **System Preferences**.
2. Click the  button.
3. Click the  button.
4. Type your username and password.
5. To stop the Nessus service, click the **Stop Nessus** button.

-or-

To start the Nessus service, click the **Start Nessus** button.

Start or Stop	Mac OS X Command Line Operation
Start	<pre># launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist</pre>
Stop	<pre># launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist</pre>

Windows

1. Navigate to **Services**.
2. In the **Name** column, click **Tenable Nessus**.
3. To stop the **Nessus** service, right-click **Tenable Nessus**, and then click **Stop**.

-or-

To restart the Nessus service, right-click **Tenable Nessus**, and then click **Start**.

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

Linux

Use the following commands:

Start or Stop	Linux Command Line Operation
RedHat, CentOS, and Oracle Linux	
Start	# /sbin/service nessusd start
Stop	# /sbin/service nessusd stop
SUSE	
Start	# /etc/rc.d/nessusd start
Stop	# /etc/rc.d/nessusd stop
FreeBSD	
Start	# service nessusd start
Stop	# service nessusd stop
Debian, Kali, and Ubuntu	
Start	# /etc/init.d/nessusd start
Stop	# /etc/init.d/nessusd stop

Start or Stop a Nessus Agent

The following represent best practices for starting and stopping a Nessus Agent on a host.

Mac OS X

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	Mac OS X Command Line Operation
Start	<pre># launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nessusagent.plist</pre>
Stop	<pre># launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusagent.plist</pre>

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	<code># service nessusagent start</code>
Stop	<code># service nessusagent stop</code>
Debian, Kali, and Ubuntu	
Start	<code># /etc/init.d/nessusagent start</code>
Stop	<code># /etc/init.d/nessusagent stop</code>

Nessus-Service

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

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

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

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

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

Nessus-Service Syntax

Operating System	Command
Linux	<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>
Mac OS X	<code># /Library/Nessus/run/sbin/nessus-service [-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
```

FreeBSD

```
# /usr/local/nessus/sbin/nessus-service -q -D
```

Nessusd Commands

Option	Description
-c <config-file>	When starting the nessusd server, this option is used to specify the server-side nessusd configuration file to use. It allows for the use of an alternate configuration file instead of the standard db.
-a <address>	When starting the nessusd server, this option is used to tell the server to only listen to connections on the address <address> that is an IP, not a machine name. This option is useful if you are running nessusd on a gateway and if you do not want people on the outside to connect to your nessusd.
-S <ip [,ip2,...]>	When starting the nessusd server, force the source IP of the connections established by Nessus during scanning to <ip>. This option is only useful if you have a multihomed machine with multiple public IP addresses that you would like to use instead of the default one. For this setup to work, the host running nessusd must have multiple NICs with these IP addresses set.
-D	When starting the nessusd server, this option forces the server to run in the background (daemon mode).
-v	Display the version number and exit.
-l	Display a list of those third-party software licenses.
-h	Show a summary of the commands and exit.
--ipv4-only	Only listen on IPv4 socket.
--ipv6-only	Only listen on IPv6 socket.
-q	Operate in "quiet" mode, suppressing all messages to stdout.
-R	Force a re-processing of the plugins.
-t	Check the time stamp of each plugin when starting up to only compile newly updated plugins.
-K	Set a master password for the scanner. If a master password is set, Nessus encrypts all policies and credentials contained in the policy. When a password is set, the Nessus UI prompts you for the password.

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

Nessuscli

Some Nessus functions can be administered through a command line interface 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: All commands must be run by a user with administrative privileges.

Nessuscli Syntax

Operating System	Command
Linux	# /opt/nessus/sbin/nessuscli <arg1> <arg2>
Mac OS X	# /Library/Nessus/run/sbin/nessuscli <arg1> <arg2>
Windows	C:\Program Files\Tenable\Nessus or C:\ProgramData\Tenable\Nessus

Nessuscli Commands

Command	Description
Help Commands	
nessuscli help	Displays a list of Nessus commands. The help output may vary, depending on your Nessus license.
nessuscli [cmd] help	Displays additional help for specific commands identified in the nessuscli help output.
Bug Reporting Commands	
The bug reporting commands create an archive that can be sent to Tenable, Inc. to help diagnose issues. By default, the script runs in interactive mode.	

Command	Description
nessuscli bug-report-generator	<p>Generates an archive of system diagnostics.</p> <p>Running this command without arguments prompts for values.</p> <ul style="list-style-type: none"> --quiet: run the bug report generator without prompting user for feedback. --scrub: when in quiet mode, bug report generator sanitizes the last two octets of the IPv4 address. --full: when in quiet mode, bug report generator collects extra data.
User Commands	
nessuscli rmuser <username>	Allows you to remove a Nessus user.
nessuscli chpasswd <username>	Allows you to change a user's password. You are prompted to enter the Nessus user's name. Passwords are not echoed on the screen.
nessuscli adduser <username>	<p>Allows you to add a Nessus user account.</p> <p>You are prompted for a username, password, and opted to allow the user to have an administrator type account. Additionally, you are prompted to add Users Rules for this new user account.</p>
nessuscli lsuser	Displays a list of Nessus users.
Fetch Commands	
Manage Nessus registration and fetch updates	
nessuscli fetch --register <Activation Code>	<p>Uses your Activation Code to register Nessus online.</p> <p>Example:</p> <pre># /opt/nessus/sbin/nessuscli fetch --register XXXX-XXXX-XXXX-XXXX</pre>
nessuscli fetch --	Uses your Activation Code to register Nessus online, but does

Command	Description
<code>register-only <Activation Code></code>	<p>not automatically download plugin or core updates.</p> <p>Example:</p> <pre># /opt/nessus/sbin/nessuscli fetch --register-only xxxx-xxxx-xxxx-xxxx</pre>
<code>nessuscli fetch --register-offline nessus.license</code>	<p>Registers Nessus 6.3 and newer with the nessus.license file obtained from https://plugins.nessus.org/v2/offline.php.</p> <p>Note: If you are using a version of Nessus 6.2 or earlier, you must use the information and instructions displayed on https://plugins.nessus.org/offline.php. In Nessus 6.2 and earlier, the license is contained in the fc.file.</p>
<code>nessuscli fetch --check</code>	<p>Displays whether Nessus is properly registered and is able to receive updates.</p>
<code>nessuscli fetch --code-in-use</code>	<p>Displays the Nessus Activation Code being used by Nessus.</p>
<code>nessuscli fetch --challenge</code>	<p>Displays the challenge code needed to use when performing an offline registration.</p> <p>Example challenge code: aaaaaa11b2222c-c33d44e5f6666a777b8cc99999</p>
<code>nessuscli fetch --security-center</code>	<p>Prepares Nessus to be connected to Security Center.</p>
Fix Commands	

Command	Description
<code>nessuscli fix</code>	Reset registration, display network interfaces, and manage advanced settings.
<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 <name=value></code>	<code>--list</code> , <code>--set</code> , <code>--get</code> , and <code>--delete</code> can be used to modify or view preferences.
<code>nessuscli fix [--secure] --get <name></code>	
<code>nessuscli fix [--secure] --delete <name></code>	
<code>nessuscli fix --list-interfaces</code>	List the network adapters on this machine.
<code>nessuscli fix --reset</code>	<p>This command deletes all your registration information and preferences, causing Nessus to run in a non-registered state. Nessus Manager retains the same linking key after resetting.</p> <p>Before running <code>nessuscli fix --reset</code>, verify running scans have completed, then stop the <code>nessusd</code> daemon or service.</p> <p>Windows: <code>net stop "Tenable Nessus"</code></p> <p>Linux: <code>service nessusd stop</code></p>
<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="628 1425 1493 1531" style="border: 1px solid orange; padding: 10px;"> <p>Caution: Contact Tenable support before performing a full reset. This action cannot be undone.</p> </div>
Certificate Commands	
<code>nessuscli mkcert-client</code>	Creates a certificate for the Nessus server.
<code>nessuscli mkcert [-q]</code>	Quietly creates a certificate with default values.
Software Update Commands	

Command	Description
<code>nessuscli update</code>	By default, this tool respects the software update options selected through the Nessus UI.
<code>nessuscli update --all</code>	Forces updates for all Nessus components.
<code>nessuscli update --plugins-only</code>	Forces updates for Nessus plugins only.
<code>nessuscli update <tar.gz filename></code>	Updates Nessus plugins by using a TAR file instead of getting the updates from the plugin feed. The TAR file is obtained when you Manage Nessus Offline - Download and Copy Plugins steps.
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>	Displays nessuscli managed commands and syntax.
<code>nessuscli managed link --key=<key> --host=<host> --port=<port> [optional parameters]</code>	<p>Link a managed scanner to the Nessus Manager.</p> <p>Additional Parameters</p> <ul style="list-style-type: none"> --name=<name> --ca-path=<ca_file_name> --proxy-host=<host> --proxy-port=<port> --proxy-username=<username> --proxy-password=<password> --proxy-agent=<agent>

Command	Description
nessuscli managed unlink	Unlink a managed scanner to the Nessus Manager.
nessuscli managed status	Identifies the status of the managed scanner.

Nessuscli Agent

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

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

Nessuscli Agent Syntax

Operating System	Command
Linux	<code># /opt/nessus_agent/sbin/nessuscli agent <arg1> <arg2></code>
Mac OS X	<code># /Library/NessusAgent/run/sbin/nessuscli <arg1> <arg2></code>
Windows	<code>C:\Program Files\Tenable\Nessus Agent</code> or <code>C:\ProgramData\Tenable\Nessus Agent</code> Run cmd.exe as administrator

Nessuscli Agent Commands

Command	Description
Help Commands	
<code># nessuscli agent help</code>	Displays a list of Nessus Agent commands.
Bug Reporting Commands	
<code># nessuscli bug-report-generator</code>	Generates an archive of system diagnostics. If you run this command without arguments, the utility prompts you for values. Optional arguments: <code>--quiet</code> : Run the bug report generator without prompting user for

Command	Description
	<p>feedback.</p> <p>--scrub: When in quiet mode, the bug report generator sanitizes the last two octets of the IPv4 address.</p> <p>--full: When in quiet mode, the bug report generator collects extra data.</p>
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 Nessus Manager or Tenable.io.</p> <p>Required arguments:</p> <ul style="list-style-type: none"> --key=<key> --host=<host> --port=<port> <p>Optional arguments:</p> <ul style="list-style-type: none"> --name=<name> --groups=<group1,group2,...> --ca-path=<ca_file_name> --offline-install --proxy-host=<host> --proxy-port=<port> --proxy-username=<username> --proxy-password=<password> --proxy-agent=<agent> <p>Tenable.io arguments:</p>

Command	Description
	--cloud
# nessuscli agent unlink	Unlinks agent from the Nessus Manager or Tenable.io.
# nessuscli agent update	<p>Used to manually install a plugins set.</p> <p>Required arguments:</p> <p>--file=<plugins_set.tgz></p>
# nessuscli agent status	<p>Displays the status of the agent, jobs pending, and if the agent is linked or not linked to server.</p> <p>Optional arguments:</p> <ul style="list-style-type: none"> --local: Provides the status, current jobs count, and jobs pending. This option prevents the agent from contacting the management software that it is linked with to fetch the status. Instead, it displays the last known information from its most recent sync. --remote: Fetches the job count from the manager and displays the status. --offline: Provides the most recently cached agent status when it cannot connect to Nessus Manager or Tenable.io.
Fix Commands	
# nessuscli fix --set update_hostname=<value>"	<p>Updates agent hostnames automatically in Tenable.io or Nessus Manager 7.1.1 or later.</p> <p>The update_hostname parameter can be set to yes or no. By default, this preference is disabled.</p> <div data-bbox="514 1552 1493 1657" style="border: 1px solid #0070C0; padding: 10px; background-color: #F0FFF0;"> <p>Note: Restart the agent service for the change to take effect in Nessus Manager.</p> </div>
# nessuscli fix --set track_unique_agents=<value>"	Tracks unique agent assets by MAC address to prevent duplicates and outdated agents from appearing in Nessus Manager if a system is reinstalled.

Command	Description
	The <code>track_unique_agent</code> parameter is available in Nessus 7.1.1 and can be set to yes or no. By default, this preference is enabled.
# nessuscli fix --set max_retries-s=<value>"	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> , and <code>agent unlink</code> commands.
nessuscli fix --secure --list	Displays a list of agent settings and their values.
Resource Control Commands	
# nessuscli fix --set process_priority=<value> # nessuscli fix --get process_priority	<p>Optional arguments:</p> <ul style="list-style-type: none"> --set --get --delete <p>Note: See Agent CPU Resource Control in the <i>Nessus Agent Deployment and User Guide</i> for <value> preference options</p>

Update Nessus Software

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](#).

Operating System	Command
Linux	# /opt/nessus/sbin/nessuscli <arg1> <arg2>
Mac OS X	# /Library/Nessus/run/sbin/nessuscli <arg1> <arg2>
Windows Commands must <i>Run as administrator</i>	C:\Program Files\Tenable\Nessus or C:\ProgramData\Tenable\Nessus
Software Update Commands	
nessuscli update	By default, this tool respects the software update options selected through the Nessus UI.
nessuscli update --all	Forces updates for all Nessus components.
nessuscli update --plugins-only	Forces updates for Nessus plugins only.

Default Data Directories

The default 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>
Mac OS X	<code>/Library/Nessus/run/var/nessus</code>

Manage Logs Using log.json

You can configure the size and location of log data by editing the `log.json` file.

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

- **Linux:** `/opt/nessus/var/nessus/log.json`
- **Mac OS X:** `/Library/Nessus/run/var/nessus/log.json`
- **Windows:** `C:\ProgramData\Tenable\Nessus\nessus\log.json`

2. For each `reporters[x].reporter`, add or modify the following parameters.

Parameter	Default value	Description
<code>rotation_strategy</code>	<code>size</code>	Determines whether the log archives files based on rotation time or maximum rotation size. If you set the rotation strategy to <code>daily</code> , the log rotates based on <code>rotation_time</code> . If you set the rotation strategy to <code>size</code> , the log rotates based on <code>max_size</code> .
<code>rotation_time</code>	<code>86400 (1 day)</code>	Rotation time in seconds. Used if <code>rotation_strategy</code> is <code>daily</code> .
<code>max_size</code>	<code>Scanner: 536870912 (512 MB)</code> <code>Agent: 10485760 (10 MB)</code>	Rotation size in bytes. Used if <code>rotation_strategy</code> is <code>size</code> .
<code>max_files</code>	<code>Scanner: 100</code> <code>Agent: 2</code>	Maximum number of files allowed in the file rotation. The maximum number includes the main file, so 100 <code>max_files</code> is 1 main file and 99 backups. If you decrease this number, old logs will be deleted.
<code>file</code>	Depends on operating system and	The location of the log file.

	log file	<p>The following are the default paths for each operating system:</p> <p>Linux: /opt/nessus/var/nessus/logs/<filename></p> <p>Mac: /Library/Nessus/run/var/nessus/logs/<filename></p> <p>Windows: C:\ProgramData\Tenable\Nessus\nessus\logs\<filename></p>
--	----------	--

3. Save the log.json file.
4. Restart the [Nessus service](#).

The log settings are updated.

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",
        "error"
      ]
    }
  ]
}
```

```

        "warn",
        "error",
        "trace"
    ],
    "reporter": {
        "type": "file",
        "file": "/opt/nessus/var/nessus/logs/backend.log"
    },
    "context": true,
    "format": "system"
}
]
}

}

```

Mac OS X 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 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"
}
]
```

Nessus Credentialated Checks

In addition to remote scanning, Nessus can be used to scan for local exposures. For information about configuring credentialated checks, see [Credentialated Checks on Windows](#) and [Credentialated 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 may not be detected from an external scan.

In a typical network vulnerability assessment, a remote scan is performed 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 displayed, which may be inconclusive or incorrect. By using secured credentials, the Nessus scanner can be granted local access to scan the target system without requiring an agent. This can facilitate scanning of a very 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 credentialated 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

Credentialated scans can perform any operation that a local user can perform. The level of scanning is dependent on the privileges granted to the user account that Nessus is configured 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, an account with “root” privileges is required.

Credentialed scans on Windows systems require that an administrator level account be used. Several bulletins and software updates by Microsoft have made reading the registry to determine software patch level unreliable without administrator privileges. 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. On Windows XP Pro, this file access will only work with a local administrator account if the “Network access: Sharing and security model for local accounts” policy is changed to “Classic – local users authenticate as themselves”.

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. Only Domain Administrator accounts can be used to scan Domain Controllers.

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 Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, Windows 7, Windows 8, or Windows 10 and must 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 will use to perform Nessus Windows Authenticated Scans to the 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.

Nessus uses Server Message Block (SMB) and Windows Management Instrumentation (WMI). You must ensure Windows Firewall allows access to the system.

Allow WMI on Windows Vista, 7, 8, 10, 2008, 2008 R2, 2012, 2012 R2, and 2016 Windows Firewall

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 Nessus Scan GPO.

Configure Windows 2008, Vista, 7, 8, and 10

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. 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 ensure it is set to either **Disabled** or **Not Configured**.
4. The **Remote Registry** service must be enabled (it is disabled by default). It can be enabled manually for continuing audits, either by an administrator or by Nessus. Using plugin IDs 42897 and 42898, Nessus can enable the service just for the duration of the scan.

Note: Enabling this option configures Nessus to attempt to start the remote registry service prior to 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.

Caution: While not recommended, Windows User Account Control (UAC) can be disabled.

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.

This key must be created 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 UAC is disabled, then EnableLUA must be set to 0 in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System as well.

Prerequisites

A very 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 will assign 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 about Windows credentials is that the account used to perform the checks should have privileges to access all required files and registry entries, which in many cases means administrative privileges. If Nessus is not provided the credentials for an administrative account, at best it can be used to perform registry checks for the patches. While this is still a valid method to determine if a patch is installed, 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, then it will actually check the version of the dynamic-link library (.dll) on the remote host, which is considerably more accurate.

Configure a Local Account

To configure a stand-alone Windows server with credentials to be used that is not part of a domain, simply create a unique account as the administrator.

Make sure that the configuration of this account is not set with a typical default of **Guest only: local users authenticate as guest**. Instead, switch this to **Classic: local users authenticate as themselves**.

Configuring a Domain Account for Local Audits

To create a domain account for remote host-based auditing of a Windows server, the server must first be Windows 2000 Server, Windows XP Pro, or Windows 2008 Server and be part of a domain.

To configure the server to allow logins from a domain account, use the **Classic** security model. To do this, follow these 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 authen-**

ticate as themselves.

6. Click **OK**.

This will cause users local to 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, will authenticate as a guest and will likely not have enough credentials to perform a remote audit.

Configuring Windows XP

When performing authenticated scans against Windows XP systems, there are several configuration options that must be enabled:

- The WMI service must be enabled on the target.
- The Remote Registry service must be enabled on the target.
- File & Printer Sharing must be enabled in the target's network configuration.
- Ports 139 and 445 must be open between the Nessus scanner and the target.
- An SMB account must be used that has local administrator rights on the target.

You may be required to change the Windows local security policies or they could block access or inherent permissions. A common policy that will affect credentialed scans is found under:

Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options > Network access: Sharing and security model for local accounts.

If this local security policy is set to something other than **Classic - local users authenticate as themselves**, a compliance scan will not run successfully.

Configuring Windows Server, Vista, 7, 8, and 10.

When performing authenticated scans against Windows systems, there are several configuration options that must be enabled:

- Under **Windows Firewall > Windows Firewall Settings**, enable **File and Printer Sharing**.
- 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**. This option must be set to either **Disabled** or **Not Configured**.
- Windows User Account Control (UAC) must be disabled, or a specific registry setting must be changed to allow Nessus audits. 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 DWORD named **LocalAccountTokenFilterPolicy** and set its value to “1”. This key must be created 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](#).
- The Remote Registry service must be enabled (it is disabled by default). It can be enabled for a one-time audit, or left enabled permanently if frequent audits are performed.

Configure Nessus for Windows Logins

Nessus User Interface

In the Scan Credential Settings section, select Windows. Specify the SMB account name, password and optional domain, then select **Submit**. The new scan policy will be added to the list of managed scan policies.

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.

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 have the ability to run any command on the system. On Linux systems, this is known as 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, it is strongly recommended that SSH keys be used instead of credentials when possible.

Configuration Requirements for Kerberos

If Kerberos is used, sshd must be configured with Kerberos support to verify the ticket with the KDC. Reverse DNS lookups must be properly configured for this to work. The Kerberos interaction method must be **gssapi-with-mic**.

Enable SSH Local Security Checks

This section is intended to provide a high-level procedure for enabling SSH between the systems involved in the Nessus credential checks. It is not intended to be an in-depth tutorial on SSH. It is assumed 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. This key pair can be generated from any of your Linux systems, using any user account. However, it is important that the keys be owned by the defined Nessus user.

To generate the key pair, use `ssh-keygen` and save the key in a safe place. In the following example the keys are generated on a Red Hat ES 3 installation.

```
# 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 (i.e., do not set any passphrase). If a passphrase is specified, it must be specified in **Policies > Credentials > SSH settings** in order 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 to be scanned 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 will call the user nessus, but you can use any name.

Once the account is created for the user, make sure that the account has no valid password set. On Linux systems, new user accounts are locked by default, unless an initial password was explicitly set. If you are using an account where a password had been set, 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 will be `/home/nessus/.ssh`. An example for Linux systems is provided below:

```
# 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 a user account that has been locked may not be used to execute commands (e.g., cron jobs). Non-login accounts are used only to execute commands and 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 the user account is created, 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 will be scanned for host checks as shown below. 192.1.1.44 is an example remote system that will be tested with the host-based checks.

```
# 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 Nessus is installed using the secure ftp command, **sftp**. Note that the file on the target system must be named `authorized_keys`.

Return to the System Housing the Public Key

Set the permissions on both the `/home/nessus/.ssh` directory, as well as 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 will be tested 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, securely copy the private and public key files to the system that you will 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 6.7 and later has the ability to 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

- For use with Nessus 6.7 or later.
- 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. If you have not already, [install Nessus](#).
2. Create a non-root account to run the Nessus service.

```
sudo useradd -r 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: `cap_net_admin` is used to put interface in promiscuous mode.
`cap_net_raw` is used to create raw sockets for packet forgery.
`cap_sys_resource` is used 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 additional 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. Remove and add the following lines to the `/usr/lib/systemd/system/nessusd.service` script:

- **Remove:** `ExecStart=/opt/nessus/sbin/nessus-service -q`
- **Add:** `ExecStart=/opt/nessus/sbin/nessus-service -q --no-root`
- **Add:** `User=nonprivuser`

The resulting script should appear as follows:

```
[Service]  
Type=simple  
PIDFile=/opt/nessus/var/nessus/nessus-service.pid  
ExecStart=/opt/nessus/sbin/nessus-service -q --no-root  
Restart=on-abort  
ExecReload=/usr/bin/pkill nessusd  
EnvironmentFile=-/etc/sysconfig/nessusd  
User=nonprivuser  
  
[Install]  
WantedBy=multi-user.target
```

7. Reload and start `nessusd`.

In this step, Nessus restarts as root, but `systemd` starts it as `nonprivuser`.

```
sudo systemctl daemon-reload  
sudo service nessusd start
```

Run Nessus on Linux with init.d Script as a Non-Privileged User

Limitations

These steps are for use with Nessus 6.7 or later.

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 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:

cap_net_admin is used to put the interface in promiscuous mode.

cap_net_raw is used to create raw sockets for packet forgery.

cap_sys_resource is used 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 additional 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 --pid-  
file --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 non-privuser:nonprivuser /opt/nessus` command to regain ownership of directories created at runtime.

Run Nessus on Mac OS X as a Non-Privileged User

Limitations

- For use with Nessus 6.7 or later.
- 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.

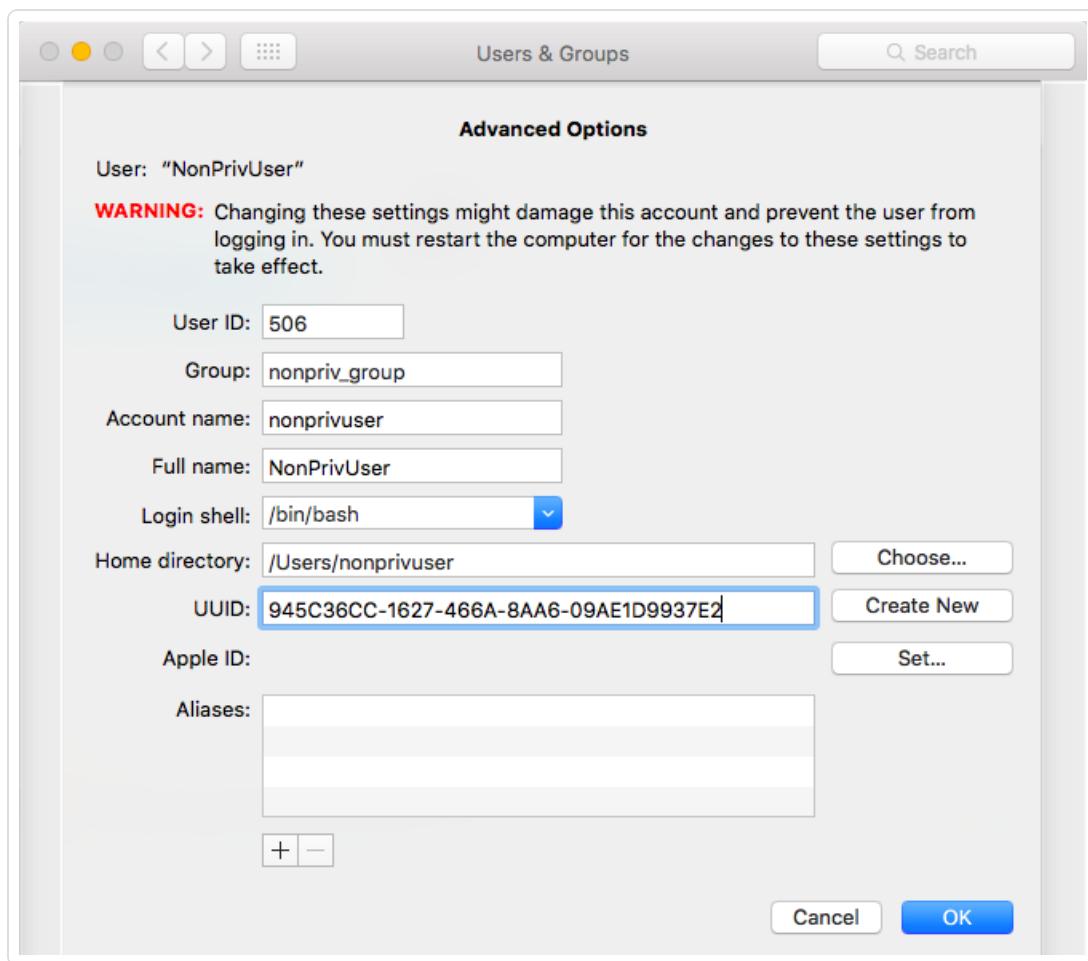
Steps

1. If you have not already done so, [Install](#) Nessus on MacOSX.
2. Since the Nessus service is running as root, it needs to be unloaded.

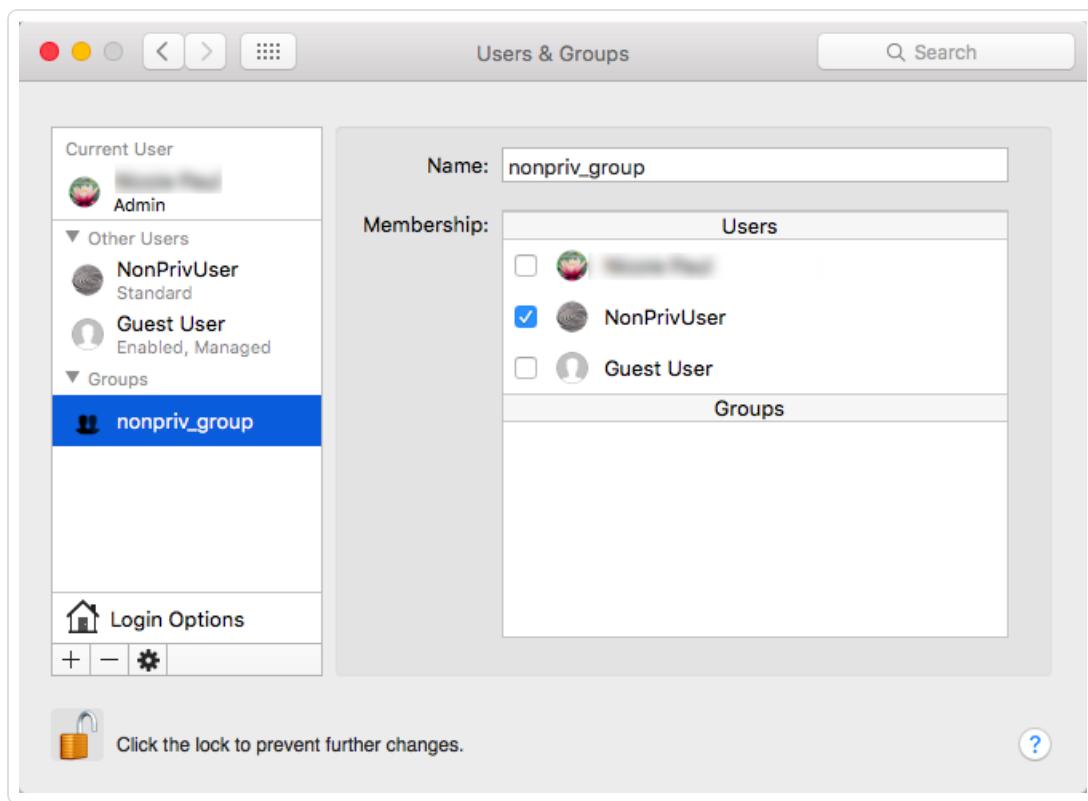
Use the following command to unload the Nessus service:

```
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**. This user will be configured 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, as well as 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 will need to create a launch daemon giving the "nonpriv" user, or a group that it is a part of, read/write permissions to all /dev/bpf*.

9. For Step 8. changes to take effect, reboot your system.

10. Using a text editor, modify the Nessus

/Library/LaunchDaemons/com.tenablesecurity.nessusd.plist file and add the following lines. **Do not modify any of the existing lines.**

```
<string>--no-root</string>
<key>UserName</key>
<string>nonprivuser</string>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Disabled</key>
    <true/>
    <key>Label</key>
    <string>com.tenablesecurity.nessusd</string>
    <key>ProgramArguments</key>
    <array>
        <string>/Library/Nessus/run/sbin/nessus-service</string>
        <string>-q</string>
        <string>--no-root</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
    <key>UserName</key>
    <string>nonprivuser</string>
</dict>
</plist>
|
```

11. Using **sysctl**, verify the following parameters have the minimum values:

```
$ sysctl debug.bpf_maxdevices
debug.bpf_maxdevices: 16384
$ sysctl kern.maxfiles
kern.maxfiles: 12288
$ sysctl kern.maxfilesperproc
kern.maxfilesperproc: 12288
$ sysctl kern.maxproc
kern.maxproc: 1064
$ sysctl kern.maxprocperuid
kern.maxprocperuid: 1064
```

12. If any of the values in Step 9. do not meet the minimum requirements, take the following steps to modify values.

Create a file called **/etc/sysctl.conf**.

Using the 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 any of the values in Step 11. are not set to the default OSX values above, take the following steps to modify values.

Using the 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

- For use with Nessus 6.7 or later.
- 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 which will run the Nessus service.

In this example, nonprivuser is created 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 nonprivuser was added to 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 displays 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
}
```

Scan Targets

Hostname targets that look like either a link6 target (start with the text "link6") or like one of the two IPv6 range forms can be forced to be processed as a hostname by putting single quotes around the target.

The following table explains target types, examples, and a short explanation of what happens when that target type is scanned.

Target Description	Example	Explanation
A single IPv4 address	192.168.0.1	The single IPv4 address is scanned
A single IPv6 address	2001:db8::2120:17ff:fe56:333b	The single IPv6 address is scanned
A single link local IPv6 address with a scope identifier	fe80:0:0:0:216:cbff:fe92:88d0%eth0	The single IPv6 address is scanned. Note that usage of interfaces names instead of interface indexes for the scope identifier is not support on Windows platforms
An IPv4 range	192.168.0.1-192.168.0.255	All IPv4 addresses between the start address and end address including both addresses.
An IPv4 address with one or more octets replaced with numeric ranges	192.168.0-1.3-5	The example will expand to all combinations of the values given in the octet ranges: 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.168.1.3, 192.168.1.4 and 192.168.1.5
An IPv4 subnet with CIDR notation	192.168.0.0/24	All addresses within the specified subnet are scanned. The address given is not the start address. Specifying any address within the subnet with the same CIDR will scan the same set of hosts.

Target Description	Example	Explanation
An IPv4 subnet with netmask notation	192.168.0.0/255.255.255.128	All addresses within the specified subnet are scanned. The address is not a start address. Specifying any address within the subnet with the same netmask will scan the same hosts
A host resolvable to either an IPv4 or an IPv6 address	www.yourdomain.com	The single host is scanned. 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	The hostname is resolved to an IPv4 address and then treated 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	The hostname is resolved to an IPv4 address and then treated like any other IPv4 address with netmask notation
The text 'link6' optionally followed by an IPv6 scope identifier	link6 or link6%16	Multicast ICMPv6 echo requests are sent out on the interface specified by the scope identifier to the ff02::1 address. All hosts that respond to the request are scanned. If no IPv6 scope identifier is given the requests are sent out on all interfaces. Note that usage of interfaces names for the scope identifier is not supported on Windows platforms
Some text with either a	www.tenable.com[10.0.1.1] or	The virtual server is targeted at the specific IP address within the brackets, and that host is scanned.

Target Description	Example	Explanation
single IPv4 or IPv6 address within square brackets	www.nessus.org[2001:db8::abcd]	