



Nessus 6.10 User Guide

Last Updated: May 31, 2017



Table of Contents

Nessus 6.10 User Guide	1
Welcome to Nessus	10
Nessus Workflow	13
About Nessus Plugins	14
System Requirements	16
Hardware Requirements	17
Software Requirements	18
Licensing Requirements	21
Download Nessus	22
Deployment Considerations	24
Host Based Firewalls	25
IPv6 Support	26
Virtual Machines	27
Anti-virus Software	28
Security Warnings	29
Install Nessus and Nessus Agents	30
Install Nessus	31
Install Nessus on Linux	32
Install Nessus on Windows	33
Install Nessus on Mac OS X	35
Nessus Agent Install	37
Install a Nessus Agent on Linux	38

Install a Nessus Agent on Windows	42
Install a Nessus Agent on Mac OS X	46
Upgrade Nessus and Nessus Agents	49
Nessus Upgrade	50
Upgrade from Evaluation	51
Linux Upgrade	52
Windows Upgrade	53
Mac Upgrade	54
Upgrade a Nessus Agent	55
Configure Nessus	56
Nessus (Home, Professional, or Manager)	58
Link to Nessus Manager	59
Link to Tenable.io	62
Managed by SecurityCenter	64
Install Nessus Offline	65
Register Nessus Offline	70
Generate Challenge Code	72
Generate Your License	73
Download and Copy License File (nessus.license)	74
Register Your License with Nessus	75
Download and Copy Plugins	76
Install Plugins Manually	77
Update Nessus Plugins using tar.gz	78
Remove Nessus and Nessus Agents	79



Nessus Removal	80
Uninstall Nessus on Linux	81
Uninstall Nessus on Windows	83
Uninstall Nessus on Mac OS X	84
Nessus Agent Removal	85
Uninstall a Nessus Agent on Linux	87
Uninstall a Nessus Agent on Windows	89
Uninstall a Nessus Agent on Mac OS X	90
Nessus Features	91
Navigating Nessus	92
Scans Page	93
Scan Folders	95
Scan Statuses	97
Scan Results	98
Dashboards	102
Scan Results Pages	105
Report Filters	106
Report Screenshots	110
Compare Report Results (Diff)	111
Knowledge Base	112
Exported Results	113
Policies Page	114
Templates	116
Settings	125

Basic Settings	126
Discovery Settings	130
Assessment Settings	139
Report Settings	152
Advanced Settings	154
Credentials	157
Cloud Services	159
Database	161
Host	162
Miscellaneous	176
Mobile	179
Patch Management	182
Plaintext Authentication	190
Compliance	193
Plugins	195
Special Use Templates	196
User Profile Page	199
Settings Page	201
Scanners	202
Scanners / Local / Overview (Manager)	206
Nessus Agents	207
Agent Groups	209
User and Group Accounts	210
Communication	211

Advanced Settings	213
Manage Nessus	226
Manage Scans	227
Create a Scan	228
Create an Agent Scan	230
Create a Scan Folder	236
Manage Scans	237
Manage Agent Groups	240
Policies	243
Create a Policy	244
Create a Limited Plugin Policy	247
Manage Policies	251
User Profile	253
Account Settings	254
API Keys	256
Change Password	257
Plugin Rules	258
Manage the Settings Page	259
System Settings	260
Scanners / Local / Software Update	261
Nessus UI Software Update Page	262
Update Nessus Version	264
Update Plugins	265
Update Activation Code	266



Update Nessus Software	268
Manage Scanners	269
Nessus Professional	270
Nessus Manager	273
Scanners / Local / Overview (Manager)	274
Scanners / Local / Permissions	275
Scanners / Remote / Linked	276
Scanners / Agents / Linked	277
Manage Nessus Agents	281
Update the custom_CA.inc File	283
Manage Accounts	284
Manage Communications	287
LDAP Server	288
SMTP Server	290
Proxy Server	291
CleanCisco ISE	292
Manage Advanced Settings	293
Additional Resources	294
Amazon Web Services	295
Command Line Operations	296
Start or Stop Nessus	297
Nessus-Service	299
Nessuscli	302
Nessuscli Agent	307

Update Nessus Software	310
Custom SSL Certificates	311
SSL Client Certificate Authentication	313
Create a New Custom CA and Server Certificate	314
Upload a Custom CA Certificate	316
Create Nessus SSL Certificates for Login	317
Enable Connections with Smart Card or CAC Card	320
Connect with Certificate or Card Enabled Browser	321
Enable SSH Local Security Checks	323
Manage Activation Code	327
View Your Activation Code	328
Reset Activation Code	329
Update Activation Code	330
Manage Nessus License and Registration	332
More Nessus Resources	333
Nessus Credentialed Checks	334
Credentialed Checks on Windows	336
Prerequisites	340
Enable Windows Logins for Local and Remote Audits	341
Configure Nessus for Windows Logins	344
Credentialed Checks on Unix	345
Prerequisites	346
Enable SSH Local Security Checks	347
Configure Nessus for SSH Host-Based Checks	350



Offline Update Page Details	353
Unofficial PCI ASV Validation Scan	355
Run Nessus as Non-Privileged User	357
Run Nessus on Linux with Systemd as a Non-Privileged User	358
Run Nessus on Linux with init.d Script as a Non-Privileged User	361
Run Nessus on MAC OSX as a Non-Privileged User	363
Run Nessus on FreeBSD as a non-privileged User	368
Scan Targets	372

Welcome to Nessus

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 Network Security.
- 24/7 access to the Tenable Network Security Support Portal for Nessus knowledgebase 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 Network Security'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.

Why Use Nessus Agents?

- Supported by all major operating systems
- The performance overhead of agents is minimal, and because agents rely on local host resources, they can potentially reduce your overall network scanning overhead
- Eliminate the need to manage credentials for vulnerability scanning
- Can be deployed using most software management systems
- Automatically updated, so maintenance is minimal
- Designed to be highly secure, leveraging encryption to protect your data
- Scanning of laptops or other transient devices that are not always connected to the local network

[Nessus Agents Product Page](#)

Nessus Manager

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.

Tip: If you are new to Nessus, see the [Nessus Workflow](#).

Nessus Workflow

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](#).

About Nessus Plugins

As information about new vulnerabilities are discovered and released into the general public domain, Tenable Network Security's 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.

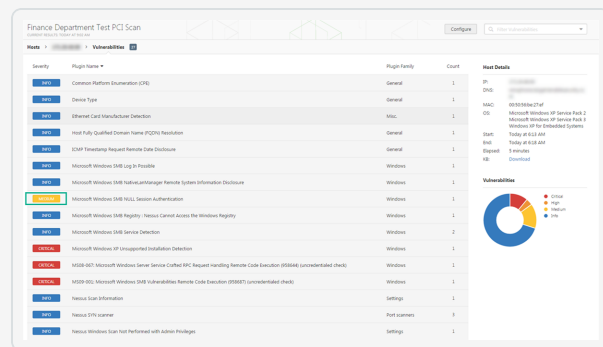
Nessus supports the Common Vulnerability Scoring System (CVSS) and supports both v2 and v3 values simultaneously. If both CVSS2 and CVSS3 attributes are present, both scores will get calculated. However in determining the Risk Factor attribute, currently the CVSS2 scores take precedence.

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](#).

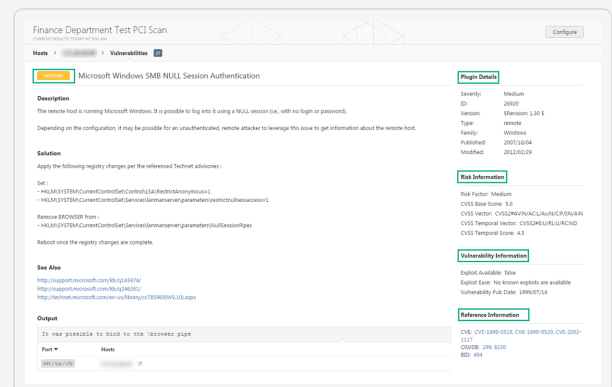
Example Plugin Information

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



Severity	Plugin Name	Plugin Family	Count
High	Common Platform Enumeration (CPE)	General	1
High	Device Type	General	1
High	External Card Infrastructure Detection	Win	1
High	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
High	ICMP Timestamp Request Remote Date Disclosure	General	1
High	Microsoft Windows SMB Log In Possible	Windows	1
High	Microsoft Windows SMB NetEnum/Enum Remote System Information Disclosure	Windows	1
High	Microsoft Windows SMB NULL Session Authentication	Windows	1
High	Microsoft Windows SMB Registry - NetEnum/Enum Remote System Registry	Windows	1
High	Microsoft Windows SMB Service Detection	Windows	2
High	Microsoft Windows XP Unauthenticated Installation Detection	Windows	1
High	MSB-001 Microsoft Windows Server Service Control (SC) Request Handling Remote Code Execution (RCE) (Unauthenticated Check)	Windows	1
High	MSB-002 Microsoft Windows SMB Vulnerability Remote Code Execution (RCE) (Unauthenticated Check)	Windows	1
High	Nessus Scan Information	Settings	1
High	Nessus VPN Scanner	Port Scanners	1
High	Nessus Windows Scan Test Performed with Admin Privileges	Settings	1

Details of a single host's plugin scan result



Microsoft Windows SMB NULL Session Authentication

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 advisory:
Set:
- HKEY_LOCAL_MACHINE\CurrentControlSet\Control\LSA\RestrictAnonymous\1
- HKEY_LOCAL_MACHINE\CurrentControlSet\Services\LanmanServer\parameters\restrictnullsessions=1
Remove BROWSE from:
- HKEY_LOCAL_MACHINE\CurrentControlSet\Services\LanmanServer\parameters\shell\classes\reg
Restart once the registry changes are complete.

See Also:
http://support.microsoft.com/kb/944742
http://support.microsoft.com/kb/944742
http://technet.microsoft.com/en-us/library/cc739900/WS.LS.aspx

Output:
[X] Was possible to bind to the 'browser' pipe

Plugin Details:
Severity: Medium
ID: 28920
Version: 3.10.1
Type: Remote
Family: Windows
Published: 2007/08/04
Updated: 2012/02/29

Bad Information:
Risk Factor: Medium
CVSS Vector: CVE:28920:AV:N/AC:L/AU:N/C:R/N/A/N
CVSS Temporal Vector: CVE:28920:AV:N/AC:L/AU:N/C:R/N/A/N
CVSS Temporal Score: 4.3

Vulnerability Information:
Exploit Available: Yes
Exploit Code: No known exploits are available
Vulnerability Pub Date: 1999/07/14

Reference Information:
CVE: CVE-1999-0533, CVE-1999-0532, CVE-2002-1337
OSVDB: 289, 8230
BD: 494

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 UI.

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.

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.

Nessus Hardware Requirements

Scenario	Minimum Recommended Hardware
Nessus managing up to 50,000 hosts	CPU: 1 dual-core 2 GHz CPU Memory: 2 GB RAM (4 GB RAM recommended) Disk space: 30 GB
Nessus managing more than 50,000 hosts	CPU: 1 dual-core 2 GHz CPU (2 dual-core recommended) Memory: 2 GB RAM (8 GB RAM recommended) Disk space: 30 GB (Additional space may be needed for reporting)

Suggested Nessus Manager Hardware Requirements

Scenario	Minimum Recommended Hardware
Nessus Manager managing 30,000 agents	CPU: Multiple cores, but prioritize the number of GHz over the number of cores. Memory: 64 GB RAM

Virtual Machines

Nessus can be installed on a Virtual Machine that meets the same requirements specified. 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.

Software Requirements

Nessus supports Mac, Linux, and Windows operating systems.

Nessus Manager and Nessus Professional

Operating System	Supported Versions
Linux	<ul style="list-style-type: none">• Debian 6, 7, and 8 / Kali Linux 1, 2, and Rolling - i386• Debian 6, 7, and 8 / Kali Linux 1, 2, and Rolling - AMD64• Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - i386• Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - x86_64• Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386• Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - x86_64• Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) - x86_64• FreeBSD 10 - AMD64• Fedora 20 and 21 - x86_64• SUSE 10.0 Enterprise - x86_64• SUSE 11 Enterprise - i586• SUSE 11 Enterprise - x86_64• Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - i386• Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - AMD64
Windows	<ul style="list-style-type: none">• Windows 7, 8, and 10 - i386• Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 - x86-64



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, it is highly recommended that Nessus be installed on a server product from the Microsoft Windows family such as Windows Server 2008 R2.</p>
Mac OS X	Mac OS X 10.8, 10.9, 10.10, 10.11, and 10.12 - x86-64

Nessus Agents

Operating System	Supported Versions
Linux	<ul style="list-style-type: none">• Debian 6, 7, and 8 - i386• Debian 6, 7, and 8 - AMD64• Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - i386• Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - x86_64• Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386• Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - x86_64• Red Hat ES 7 / CentOS 7 / Oracle Linux 7 - x86_64• Fedora 20 and 21 - x86_64• Ubuntu 10.04 - i386• Ubuntu 10.04 - AMD64• Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 - i386• Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 - AMD64



Operating System	Supported Versions
Windows	<ul style="list-style-type: none">Windows 7, 8, and 10 - i386Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 - x86-64
Mac OS X	Mac OS X 10.8, 10.9, 10.10, 10.11, and 10.12 - x86-64

Browsers

The following browsers are supported for Nessus.

- Google Chrome (50+)
- Apple Safari (9+)
- Mozilla Firefox (45+)
- Internet Explorer (9+)

PDF Reports

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

Oracle Java or **OpenJDK** must be installed **prior** to the installation of Nessus.

Note: If **Oracle Java** or **OpenJDK** is installed **after** the Nessus installation, Nessus must be reinstalled for the PDF report generation to function.

Licensing Requirements

Nessus is available to operate either as a subscription or managed by SecurityCenter. 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.

It is recommended that you obtain the Activation Code before starting the installation process, as that information will be required before you can authenticate to the Nessus GUI interface.

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](#).

You may purchase a Nessus subscription through Tenable Network Security's 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 Network Security. This code will be used when configuring your copy of Nessus for updates.

If you are using SecurityCenter to manage your Nessus scanners, the Activation Code and plugin updates are managed from SecurityCenter. Nessus needs to be started to be able to communicate with SecurityCenter, which it will normally 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 SecurityCenter), enter "SecurityCenter" (case sensitive) without quotes into the Activation Code box.

Please refer to the following link for the most current information on obtaining an Activation Code:

<http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code>

Download Nessus

Nessus products are downloaded from the [Tenable Support Portal](#).

When downloading Nessus from the [Tenable Support Portal](#), 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>-ber.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
NNessusAgent-<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

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.

This section contains the following deployment considerations:

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

Host Based Firewalls

Port 8834

The Nessus UI 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 credentialed 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.

Anti-virus 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 Installation

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

Nessus Agent Installation

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

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

Download Nessus Manager.

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
```

The remaining Nessus installation steps will be performed in your web browser. [Configure Nessus](#)

Install Nessus on Windows

Download Nessus Manager

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 Network Security Nessus** screen appears. Select **Next** to continue.
2. On the **License Agreement** screen, read the terms of the Tenable Network Security Nessus software license and subscription agreement.
3. Select the **I accept the terms of the license agreement** radio button, 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 Network Security 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. Next, on the **Completing the WinPcap Setup Wizard** screen, select the **Finish** button.
 5. Finally, the **Tenable Nessus InstallShield Wizard Completed** screen appears. 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. [Configure Nessus](#).

Install Nessus on Mac OS X

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 Network Security Nessus Server Install

When the installation begins, the **Install Tenable Network Security Nessus Server** screen will be displayed and provides an interactive navigation menu.

Introduction

The **Welcome to the Tenable Network Security 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 Network Security** 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 Network Security 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 installation was successful.** screen.

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

The remaining Nessus installation steps will be performed in your web browser.

[Configure Nessus](#)

Nessus Agent Install

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**.

- **Nessus Agents** are **not** available for use with **Nessus Professional**.
- **Nessus Agents** can only be installed **after** the installation of **Nessus Manager**, but can be linked to Tenable.io without future setup in Tenable.io.
- **Nessus Agents** are downloaded from the [Nessus Agents Download Page](#).
- Before you start the **Agent** installation process, you will first retrieve the **Nessus Agent Linking Key** from within the **Nessus Manager** or **Tenable.io** interface.
- Linked agents will automatically download plugins from the manager upon connection; this process can take several minutes and is required before an agent will return scan results.

Install a Nessus Agent on Linux


Retrieve Agent Linking Key from within Nessus

1. Log in to Nessus.
2. Select the  button.
3. On the **Scanners / Agents / Linked** page, select **Agent > Linked** and read the on-screen message.


Agents can be linked to this manager using the provided key with the following setup instructions. Once linked, they must be added to a **group** for use when configuring scans.

Also, linked agents will automatically download plugins from the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.

Scanners / Agents / Linked

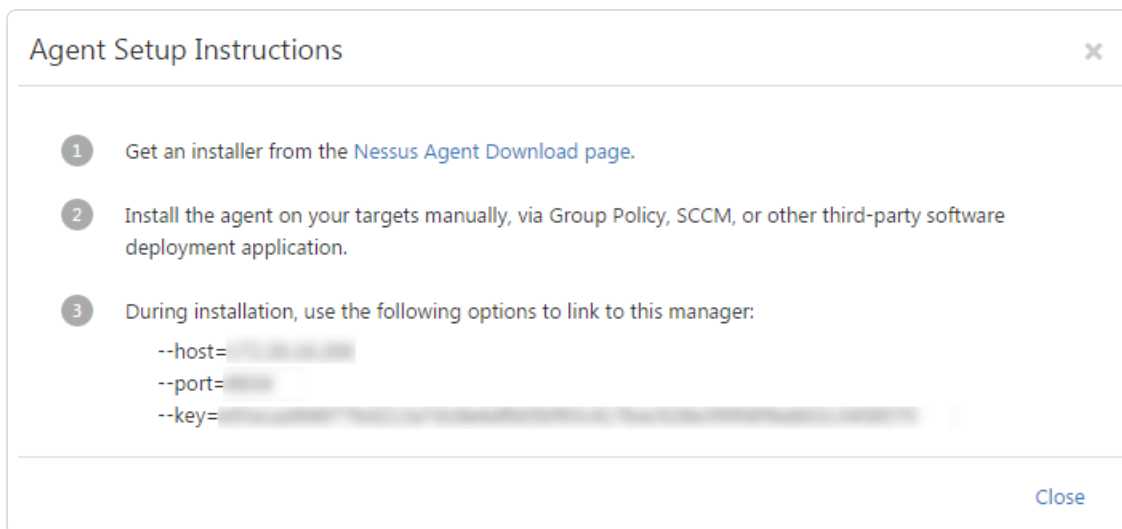


Agents can be linked to this manager using the provided key with the following [setup instructions](#). Once linked, they must be added to a [group](#) for use when configuring scans. Also, linked agents will automatically download plugins from the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.

Linking Key: 

4. Select the **setup instructions** link.

The **Agent Setup Instructions** window appears.



5. Record the **host**, **port**, and **key** values. These values will be used during the installation of the Nessus Agent.
6. Select the **Close** button.

Download the Nessus Agent

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

Example Nessus Agent Package Names

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

Note: The following steps require root privileges.

Install Nessus Agent

Using the command line interface, install the Nessus Agent.

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

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
```

Link Agent to Nessus Manager

During this step, you will need the **Agent Key** values obtained from the Nessus UI:

Agent Key Values

Required Values

- Key

Agent Key Values

- Host
- Port

Optional Values

- Name (A name for your Agent)
- Groups (Existing Agent Group(s) that you want your Agent to be a member of)


If you do not specify an Agent Group during the install process, you can later add your linked Agent to an Agent Group within the Nessus UI.

At the command prompt, use the following command as an example to construct the **nessuscli agent link** string.

```
/opt/nessus_agent/sbin/nessuscli agent link  
--key=00abcd0000efgh11111i0k222lmopq3333st4455u66v77777w88xy9999zabc00  
--name=MyOSXAgent --groups="All" --host=yourcompany.com --port=8834
```

Note: If you attempt to clone an Agent and link it to Nessus Manager, a 409 error may appear. This is 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 Linked Agent.

1. In Nessus, select the  button.
2. View Agents on the **Scanners / Agents / Linked** page.

Note: If information provided in your command string is incorrect, a **Failed to link agent** error will be displayed.

Install a Nessus Agent on Windows

Before You Begin

Nessus Agents can be deployed with a standard Windows service such as Active Directory (AD), Systems Management Server (SMS), or other software delivery system for MSI packages.

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

Nessus Agents can be deployed and linked using 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-  
Y=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00 /qn
```


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

- 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

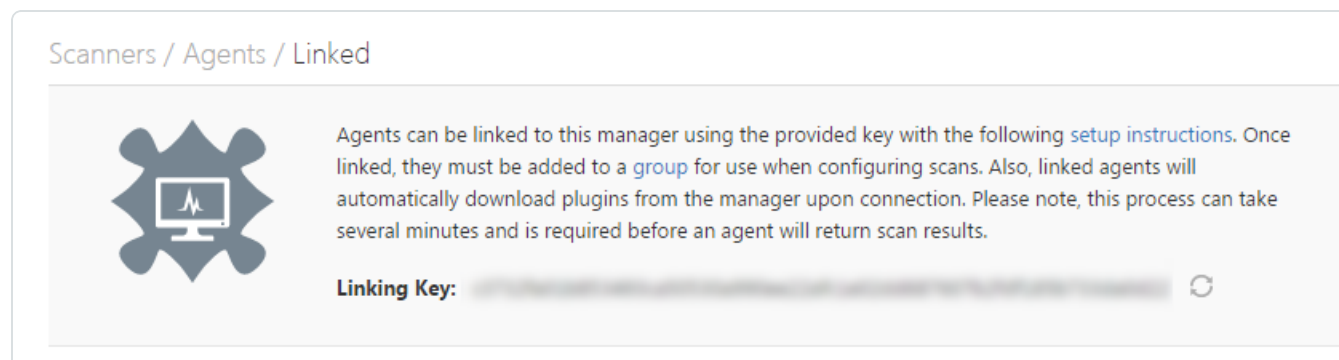
Retrieve Agent Linking Key from within Nessus

1. Log in to Nessus.
2. Select the  button.

3. On the **Scanners / Agents / Linked** page, select **Agent > Linked** and read the on-screen message.

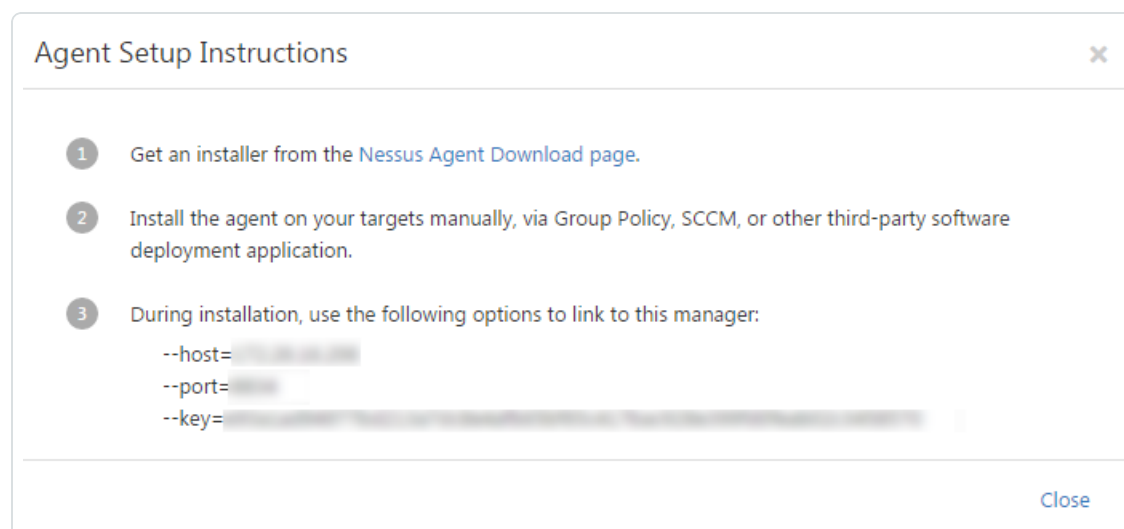
Agents can be linked to this manager using the provided key with the following **setup instructions**. Once linked, they must be added to a **group** for use when configuring scans.

Also, linked agents will automatically download plugins from the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.



4. Select the **setup instructions** link.

The **Agent Setup Instructions** window appears.



5. Record the **host**, **port**, and **key** values. These values will be used during the installation of the Nessus Agent.
6. Select the **Close** button.

Download Nessus Agent

From the [Nessus Agents Download Page](#), download the Nessus Agent 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.

Complete the Windows InstallShield Wizard

1. First, the **Welcome to the InstallShield Wizard for Nessus Agent** dialog box will appear. Select **Next** to continue.
2. From the **License Agreement** window, read the terms of the Tenable Network Security Nessus software license and subscription agreement.
3. Select the **I accept the terms of the license agreement** radio button, 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 in a different folder.

Note: During the next step, you will need the **Agent Key** values: **Key**, **Server (host)**, and **Groups**.

5. On the **Configuration Options** screen, enter the **Agent Key** values: **Key**, **Server (host)**, and **Groups**, and then select **Next**.

Agent Key Values

Required Values

- Key
- Server (host)

Agent Key Values

Optional Value

- Groups (Existing Agent Group(s) that you want your Agent to be a member of)


If you do not specify an Agent Group during the install process, you can later add your linked Agent to an Agent Group within the Nessus UI.

Note: Your Agent Name will be the computer name where the agent is installed.

6. On the **Ready to Install the Program** screen, select **Install**.
7. If presented with a **User Account Control** message, select **Yes** to allow the Nessus Agent to be installed.
8. When the **InstallShield Wizard Complete** screen appears, select **Finish**.


Note: If you attempt to clone an Agent and link it to Nessus Manager, a 409 error may appear. This is 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 Linked Agent

1. In **Nessus**, select the  button .
2. View the linked agents on the **Scanners / Agents / Linked** page.

Install a Nessus Agent on Mac OS X


Retrieve Agent Linking Key

1. Log in to Nessus.
2. Select the  button.
3. On the **Scanners / Agents / Linked** page, select **Agent > Linked** and read the on-screen message.


Agents can be linked to this manager using the provided key with the following **setup instructions**. Once linked, they must be added to a **group** for use when configuring scans.

Also, linked agents will automatically download plugins from the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.

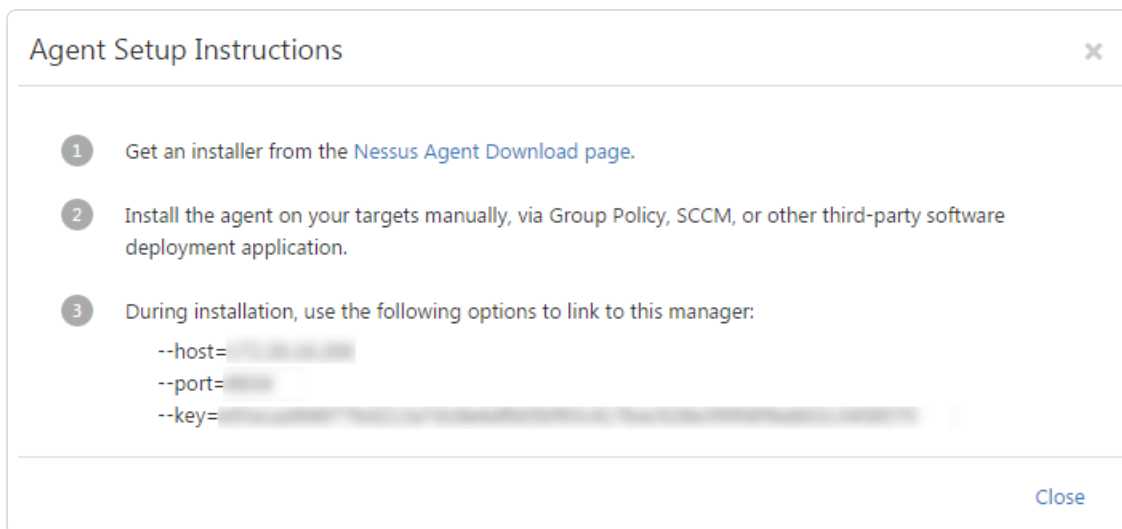
Scanners / Agents / Linked



Agents can be linked to this manager using the provided key with the following [setup instructions](#). Once linked, they must be added to a [group](#) for use when configuring scans. Also, linked agents will automatically download plugins from the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.

Linking Key: 

4. In the first sentence of the Scanners / Agents / Linked window, select the **setup instructions** link.



5. Record the **host**, **port**, and **key** values. These values will be used during the installation of the Nessus Agent.
6. Select the **Close** button.

Download Nessus Agent

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

Example: Compressed Nessus Installer File

NessusAgent-<version number>.dmg

Note: The following steps require root privileges.

Install Nessus Agent

1. Double-click the Nessus **.dmg** (Mac OSX Disk Image) file.
2. Double-click **Nessus.pkg**.
3. Complete the **Nessus Agent InstallShield Wizard**.

Note: Next, you will use the command line interface (Terminal) to link your Nessus Agent to Nessus Manager or Tenable.io.

Link Agent Using Command Line Interface

You will need the **Agent Key** values obtained from the Nessus UI (Step 1): **host**, **port**, and **key**.

Agent Key Values

Required Values

- Key
- Host
- Port

Optional Values

- Name (A name for your Agent)
- Groups (Existing Agent Group(s) that you want your Agent to be a member of)


If you do not specify an Agent Group during the install process, you can later add your linked Agent to an Agent Group within the Nessus UI.

1. Open Terminal.
2. At the command prompt, use the following command as an example to construct your link-specific string.

Example Mac Agent Link Command:

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

Verify Linked Agent

1. In **Nessus**, select the  button.
2. View linked Agents on the **Scanners / Agents / Linked** page.

This completes the process of installing a Nessus Agent on Mac OSX.

Upgrade Nessus and Nessus Agents

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

- [Nessus Upgrade](#)
 - [Upgrade from Evaluation](#)
 - [Mac Upgrade](#)
 - [Linux Upgrade](#)
 - [Windows Upgrade](#)
- [Upgrade a Nessus Agent](#)

Nessus Upgrade


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

- [Upgrade from Evaluation](#)
- [Linux Upgrade](#)
- [Windows Upgrade](#)
- [Mac Upgrade](#)

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 add your full-version **Activation Code** on the **Settings** page of the Nessus UI.

Use a New Activation Code

1. Select the  button next to the **Activation Code**.
2. Select the **Registration** type.
3. Enter the new **Activation Code**.
4. Select **Save**.

Nessus will download and install the Nessus engine and the latest Nessus plugins.

Once the download process is complete, Nessus will restart, and then prompt you to log in to Nessus again.

Linux Upgrade

Download Nessus

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

Use Commands to Upgrade Nessus

From a command prompt, run the Nessus upgrade command.

Example Nessus Upgrade Commands

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.

Examples: Nessus Daemon Start Commands

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.

Windows Upgrade

Download Nessus

From the [Tenable Support Portal](#), download the latest, full-license version of Nessus. The download package is specific the Nessus build version, your platform, your platform version, and your CPU.

Example Nessus Installer Files

Nessus-<version number>-Win32.msi

Nessus-<version number>-x64.msi

Start Nessus Installation

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

Complete the Windows InstallShield Wizard

1. At the **Welcome to the InstallShield Wizard for Tenable Network Security Nessus** screen, select **Next**.
2. On the **License Agreement** screen, read the terms of the Tenable Network Security Nessus software license and subscription agreement.
3. Select the **I accept the terms of the license agreement** radio button, 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 Network Security 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.

Mac Upgrade

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

Upgrade a Nessus Agent

Once installed, Nessus Agents are updated automatically by Nessus Manager or Tenable.io. If your Nessus Manager instance is running offline, you can download application updates for agents from the Tenable Support Portal.

Steps: Download Agent Application Updates

1. Log in to the [Tenable Support Portal](#).
2. Click **Downloads**.
3. Click **Nessus and Nessus Manager**.

In the **Nessus Agent** section, the latest application update files for agents are available.

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

The download begins automatically.

Configure Nessus

Begin Browser Portion of the Nessus Setup

1. On the **Welcome to Nessus** page, select the link at the end of the **Please connect via SSL** statement. You will be redirected and you will continue with the remaining installation steps.

Caution: When accessing Nessus via a web browser, you will encounter a message related to a security certificate issue: a connection privacy problem, an untrusted site, an unsecure connection, or similar security related message. 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.

2. Accept, then disable privacy settings.
3. On the **Welcome to Nessus** page, select the **Continue** button.

Create Nessus System Administrator Account

1. On the **Initial Account Setup** page, in the **Username** field, type the username that will be used for this Nessus System Administrator's account.

Note: After setup, you can create additional Nessus System Administrator accounts.


2. Next, in the **Password** field, type the password that will be used for this Nessus System Administrator's account.
3. In the **Confirm Password** field, re-enter the Nessus System Administrator account's password.
4. Finally, select the **Continue** button.

Select Nessus Registration

- [Nessus \(Home, Professional, or Manager\)](#)
- [Link to Nessus Manager](#)
- [Link to Tenable.io](#)

- [Managed by SecurityCenter](#)
- [Install Nessus Offline](#)

Product Registration



As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. [Registering this scanner](#) will grant you access to download these plugins.

Registration

Activation Code

[Continue](#) [Back](#)

Nessus (Home, Professional or Manager) ▲

Nessus (Home, Professional or Manager)

Link to Nessus Manager

Link to Tenable Cloud

Managed by SecurityCenter

Offline

[Advanced Settings](#)

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.
2. Enter your **Activation Code**. The **Activation Code** is the code you obtained from the your license e-mail or from the [Tenable Support Portal](#).
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 host name 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 host name 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 Nessus Manager

This option installs Nessus as a Remote (Secondary) Scanner, linked to a Nessus Manager install.

During installation, you will be prompted to enter the Nessus **Manager Host**, Nessus **Manager Port**, and Nessus Manager **Linking Key**.

Tip: In Nessus Manager, the **Linking Key** is displayed on the **Scanners / Remote / Linked** page.

Scanners / Remote / Linked



Remote scanners can be linked to this manager using the provided key. Once linked, they can be managed locally and selected when configuring scans.

Linking Key: 

1. Select **Link to Nessus Manager** from the Registration drop-down.
2. Next, enter the Nessus **Manager Host**, **Manager Port** (Nessus is installed on Port 8834 by default), and the Nessus Manger **Linking Key**.

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 host name 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 host name 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

This option installs Nessus as a remote scanner, linked to Tenable.io.

During installation, you will be prompted to enter Tenable.io **Linking Key**.

Tip: In Tenable.io, the **Linking Key** is displayed on the **Scanners > Linked Scanners** page.

Scanners

Linked Scanners

Scanner Groups




Remote scanners (Nessus or PVS) can be linked to Tenable Cloud using the provided key. Once linked, they can be managed locally and selected when configuring scans.

Linking Key:

[Redacted Linking Key] 

1. Select **Link to Tenable.io** from the **Registration** drop-down.
2. Next, enter the Tenable.io **Linking Key**.


Product Registration



As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. [Registering this scanner](#) will grant you access to download these plugins.

Registration Link to Tenable Cloud


Linking Key

Use Proxy  ☐

[Continue](#) [Back](#) [Advanced Settings](#)

Nessus will finish the installation process; this may take several minutes.

3. Using the System Administrator account you created, **Sign In** to Nessus.



Note: Although you will not be prompted to enter this information, Tenable.io settings are as follows:

Host: cloud.tenable.com

Port: 443

Managed by SecurityCenter

This option is used when installing Nessus, which will be managed by SecurityCenter.

Install Nessus Offline

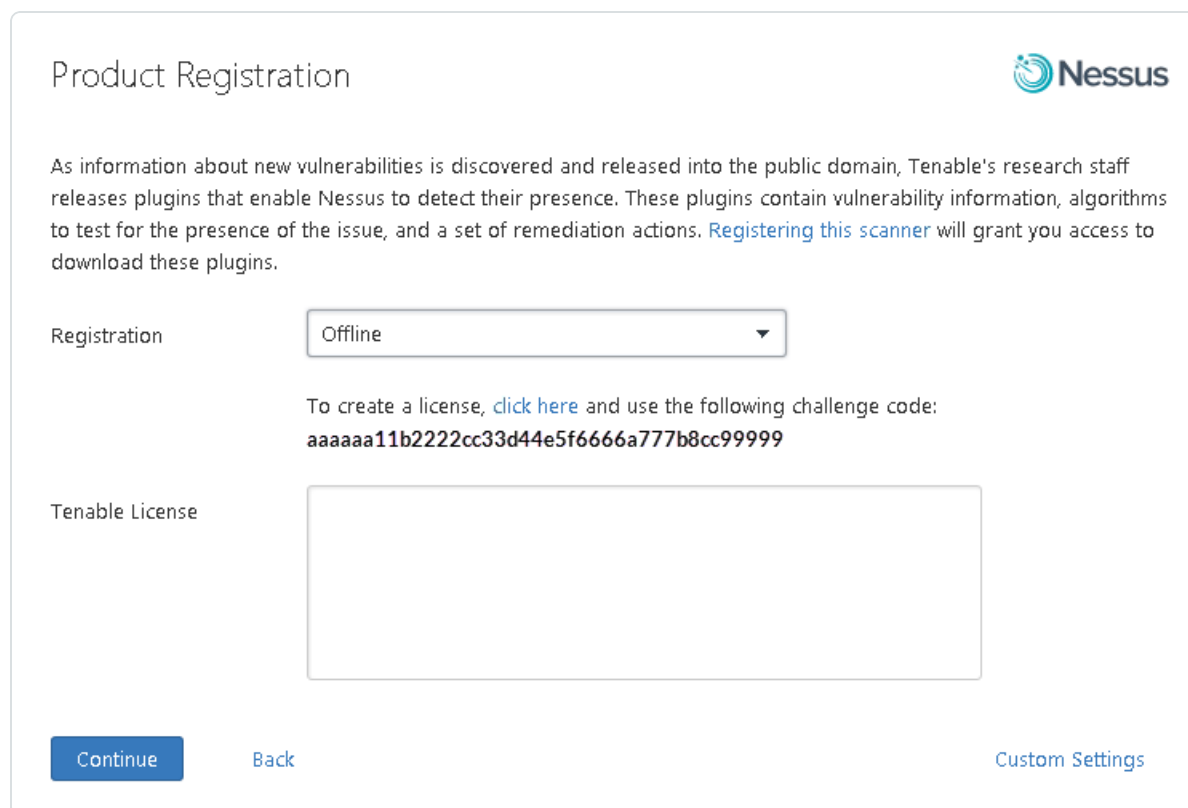
A Nessus **Offline** registration is suitable for computers that will be running Nessus, but are not connected to the Internet. To ensure that Nessus has the most up-to-date plugins, Nessus servers not connected to the Internet must perform these specific steps to register Nessus.

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 [Configure Nessus](#), 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: **aaaaaa11b2222cc33d44e5f6666a777b8cc99999**.

This challenge code is used in the next step.



The screenshot shows the 'Product Registration' page for Nessus. At the top right is the Nessus logo. Below the title, there is a paragraph explaining that new vulnerabilities are discovered and released into the public domain, and that Tenable's research staff releases plugins to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. A link 'Registering this scanner' is provided, stating it will grant access to download these plugins.

Below the paragraph, there is a 'Registration' label and a dropdown menu with 'Offline' selected. Below this, there is a text prompt: 'To create a license, [click here](#) and use the following challenge code: **aaaaaa11b2222cc33d44e5f6666a777b8cc99999**'. Below the challenge code is a 'Tenable License' label and a large empty text box for pasting the license.

At the bottom, there are three buttons: 'Continue' (blue), 'Back' (light blue), and 'Custom Settings' (light blue).

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](#).

Generate a license for Nessus 6.3 and newer.

To generate a license for an older version of Nessus click [here](#).

Type 'nessuscli fetch --challenge' on your nessusd server and type in the result :

Enter your activation code :

Submit

2. In the top field, enter the challenge code that was displayed on the **Nessus Product Registration** screen.

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**.

The [Offline Update Page Details](#) 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 Network Security LICENSE----- and ends with -----END Tenable Network Security 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 license text-string displayed.

<https://plugins.nessus.org/v2/nessus.php>

```
-----BEGIN TENABLE LICENSE-----
```

[Illegible license text]

```
-----END TENABLE LICENSE-----
```

You may also install the license using Nessus command line tools:

- nessus.license

1. While still using the computer with Internet access **(B)**, select the on-screen, custom URL link. The link will download a compressed TAR file.

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


- 67 -

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 Network Security LICENSE-----** and ends with **-----END Tenable Network Security 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 Network Security LICENSE-----** and ends with **-----END Tenable Network Security LICENSE-----**.

Product Registration



As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. [Registering this scanner](#) will grant you access to download these plugins.

Registration

Offline

To create a license, [click here](#) and use the following challenge code:

Tenable License

```

-----BEGIN TENABLE LICENSE-----
-----END TENABLE LICENSE-----

```

Continue

Back

Custom Settings

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.

Register Nessus Offline

When your Nessus server is not connected to the Internet, you must perform certain operations offline. This may include installing Nessus offline, updating Nessus with a new license, or downloading and installing Nessus plugins.

There are 3 distinct scenarios to consider when managing Nessus offline and each of these scenarios require the use of 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

You are performing a new install of Nessus, but for security purposes, the server is not connected to the Internet. In this scenario, you will perform the complete steps to [install Nessus while offline](#). During this process, Nessus plugins are downloaded and installed on the offline Nessus server.

Scenario 2: Update Nessus Licensing

You have an existing Nessus server that is offline, your license changes, and you must update Nessus with the new license / activation code. In this case, you will perform the following operations:

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 on the following URL: <https://plugins.nessus.org/offline.php>.

4. [Register Your License with Nessus](#)
5. [Download and copy plugins to Nessus](#)
6. [Update Nessus Plugins using tar.gz](#)

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. [Update Nessus Plugins using tar.gz](#)

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	

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	# /opt/nessus/sbin/nessuscli fetch --challenge
FreeBSD	# /usr/local/nessus/sbin/nessuscli fetch --challenge
Mac OS X	# /Library/Nessus/run/sbin/nessuscli fetch --challenge
Windows	C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --challenge

3. Copy the alphanumeric challenge code.
Example Challenge Code:
aaaaaa11b2222cc33d44e5f6666a777b8cc99999
4. Use the copied challenge code to [Generate Your License](#).

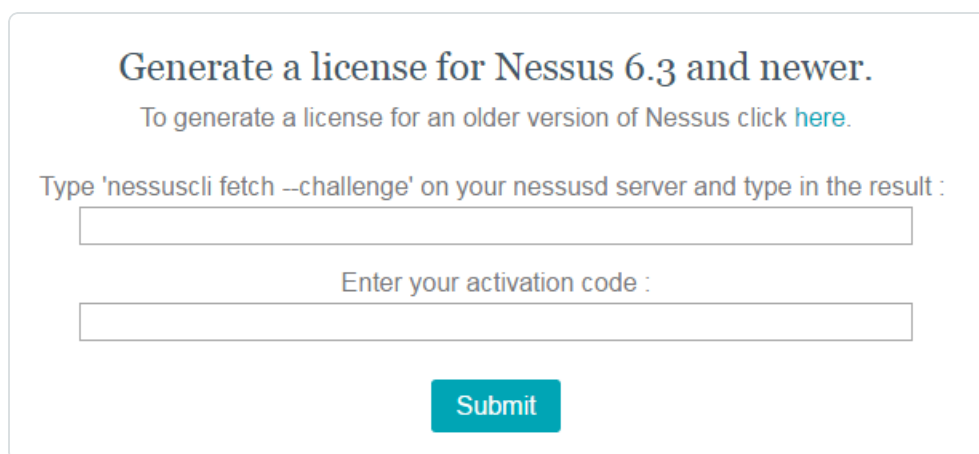
Generate Your License

By default, when 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 (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](#).

A screenshot of a web form titled "Generate a license for Nessus 6.3 and newer." Below the title is a link: "To generate a license for an older version of Nessus click [here](#)." The form contains two text input fields. The first field is preceded by the instruction "Type 'nessuscli fetch --challenge' on your nessusd server and type in the result :". The second field is preceded by the instruction "Enter your activation code :". Below the second field is a teal "Submit" button.

Generate a license for Nessus 6.3 and newer.

To generate a license for an older version of Nessus click [here](#).

Type 'nessuscli fetch --challenge' on your nessusd server and type in the result :

Enter your activation code :

Submit

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:\Program Files\Tenable\Nessus\nessus.license"

Download and Copy Plugins

After submitting the required information on the [Offline Update Page Details](#), you will 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	Command
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

If you used the steps to [Download and Copy Plugins](#) offline, your next step is to update Nessus plugins using the compressed TAR file.

Once you have copied the plugins file, there are two ways to update Nessus using the compressed TAR file.

1. Use the **Manual Software Update** feature in the Nessus user interface.
2. Use the command line interface and the **nessuscli update** command.

Option 1: Manual Software Update via the UI

1. On the **offline** system running Nessus (A), select the  button.
2. From the side-bar menu, select **Software Update**.
3. Next, select the **Manual Software Update** button.
4. On the **Manual Software Update** dialog box, select **Upload your own plugin archive**, and then select **Continue**.
5. Navigate to the directory where you downloaded the compressed TAR file.
6. Select the compressed TAR file and then select **Open**.
Nessus updates with the uploaded plugins.

Option 2: Update via the Command Line

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	# /opt/nessus/sbin/nessuscli update <tar.gz filename>
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>

Update Nessus Plugins using tar.gz

On the **offline** system running Nessus (A), there are two ways to update Nessus using the [downloaded, compressed TAR file](#):

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 UI

1. On the **offline** system running Nessus (A), select the  button.
2. From the side-bar menu, select **Software Update**.
3. Next, select the **Manual Software Update** button.
4. On the **Manual Software Update** dialog box, select **Upload your own plugin archive**, and then select **Continue**.
5. Navigate to the directory where you downloaded the compressed TAR file.
6. Select the compressed TAR file and then select **Open**.

Option 2: Update via the Command Line

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	# /opt/nessus/sbin/nessuscli update <tar.gz filename>
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](#)
- [Nessus Agent Removal](#)
 - [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 file 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

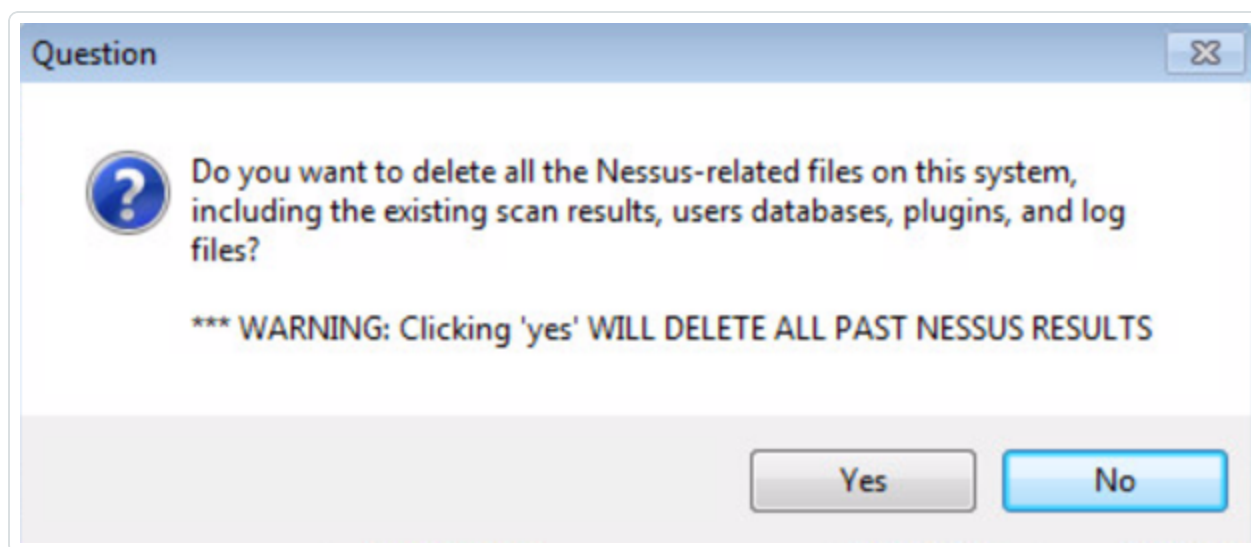
```
# rm -rf /usr/local/nessus/bin
```

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

Uninstall Nessus on Windows

Use Windows to Uninstall Nessus

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



4. Select **Yes** to continue, otherwise select **No**.

Next, Windows will remove all Nessus related files and folders.

This completes the process of uninstalling **Nessus Professional** or **Nessus Manager** on the **Windows** operating system.

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/PreferencePanels/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.


Nessus Agent Removal

Regardless of your operating system, you can remove linked **Nessus Agents** from within the Nessus UI. However this will not remove Nessus Agent files and folders on the computer where the Agent was installed.


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

Remove Linked Agents


Scanners / Agents / Linked




Agents can be linked to this manager using the provided key with the following [setup instructions](#). Once linked, they must be added to a [group](#) for use when configuring scans. Also, linked agents will automatically download plugins from the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.

Linking Key: 0c80f7839725f252a87f281f1f8f16140d4d06796393814a3495ca91c6d02577 

<input type="checkbox"/>	Name ▼	Status	IP Address	Platform	Groups	Version	Last Plugin Update	Last Scanned	
<input type="checkbox"/>	centos5-agent-6...	● Online	192.168.1.10	Linux (es5-x86-64)	All	6.10.4	06:15 AM	11:14 AM	✕
<input type="checkbox"/>	centos6-agent-6...	● Online	192.168.1.11	Linux (es6-x86-64)	All	6.10.4	06:15 AM	11:14 AM	✕
<input type="checkbox"/>	centos6-agent-6...	● Online	192.168.1.12	Linux (es6-x86-64)	All	6.8.1	06:15 AM	11:14 AM	✕
<input type="checkbox"/>	centos7-agent-6...	● Online	192.168.1.13	Linux (es7-x86-64)	All	6.10.4	06:15 AM	11:14 AM	✕
<input type="checkbox"/>	centos7-agent-6...	● Online	192.168.1.14	Linux (es7-x86-64)	All	6.10.4	06:15 AM	11:14 AM	✕
<input type="checkbox"/>	centos7-agent3-...	● Online	192.168.1.15	Linux (es7-x86-64)	All	6.7.0	06:15 AM	11:14 AM	✕
<input type="checkbox"/>	debian7-agent-6...	● Online	192.168.1.16	Linux (debian6-x...	All	6.10.4	06:15 AM	11:14 AM	✕
<input type="checkbox"/>	debian7-agent-6...	● Online	192.168.1.17	Linux (debian6-x...	All	6.9.1	06:15 AM	11:14 AM	✕
<input type="checkbox"/>	ubuntu14-agent-...	● Online	192.168.1.18	Linux (ubuntu11...	All	6.10.4	06:15 AM	11:14 AM	✕
<input type="checkbox"/>	ubuntu14-agent-...	● Online	192.168.1.19	Linux (ubuntu11...	All	6.9.2	06:15 AM	11:14 AM	✕

1. In Nessus, select the  button
2. Navigate to the **Scanners / Agents / Linked** page.

-
- 
3. Select the X button next to the agent that you would like to delete.
 4. On the **Remove Agent** screen, select the **Remove** button, otherwise, select **Cancel**.

Tip: To remove (delete) multiple agents at once, use the check boxes, and then select the REMOVE button.

If you are using a **Mac** or **Linux** operating system, you can also unlink your agent from the command line.

After unlinking your agent from the command line, the agent will automatically be removed from the **Scanners / Agents / Linked** page in Nessus.

Uninstall a Nessus Agent on Linux

OPTIONAL: Unlink Nessus Agent

1. From the command line, type the following command.

```
nessuscli agent unlink
```

2. If prompted, provide the administrator password.

Remove Nessus Agent

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

Examples: Nessus Package Name Determination

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.

Examples: 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



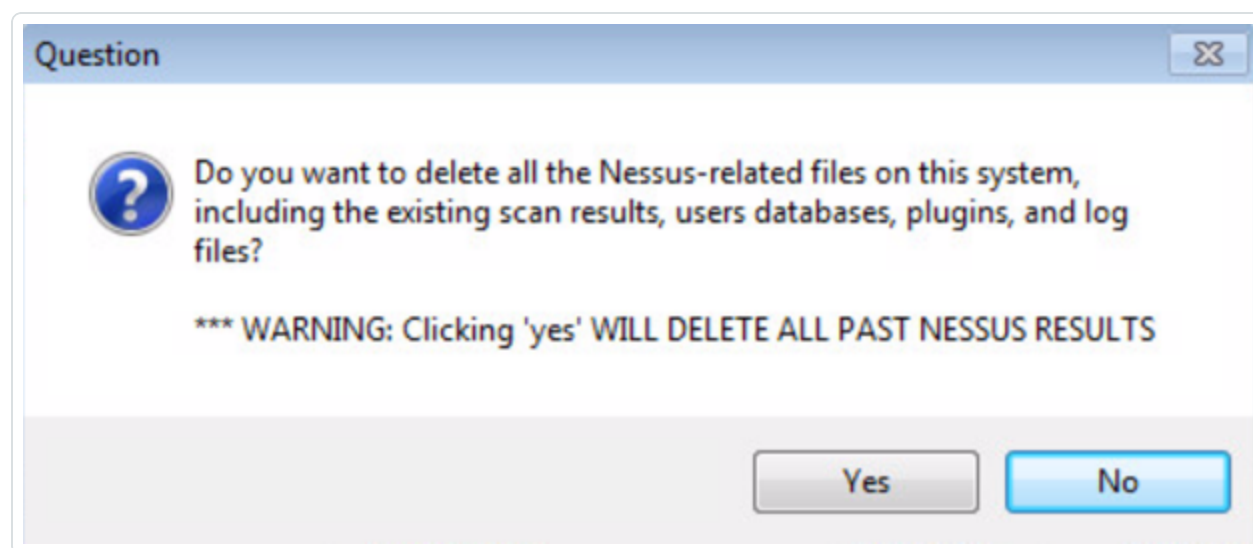
```
# pkg delete <Agent Package Name>
```

Uninstall a Nessus Agent on Windows

Remove Tenable Network Security Nessus Agent Product

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

At the start of the uninstall process, a warning message is displayed.



4. Select **Yes** to continue, otherwise select **No**.

Next, Windows will remove all related Nessus files and folders.

This completes the process of uninstalling the Nessus Agent on the Windows operating system

Uninstall a Nessus Agent on Mac OS X

Unlink Agent

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

```
# /Library/NessusAgent/run/sbin/nessuscli agent unlink
```

2. If prompted, provide the administrator password.

Remove Nessus directories, sub-directories, and files

Using **Finder**, locate and delete the following items.

- /Library/NessusAgent
- /Library/LaunchDaemons/com.tenablesecurity.nessusagent.plist
- /Library/PreferencePanes/Nessus Agent Preferences.prefPane

Disable the Nessus Agent service

This step prevents the system from attempting to start the agent service.

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

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

2. If prompted, provide the administrator password.

Nessus Features





This section describes the following features in the Nessus web interface:

- [Navigating Nessus](#)
- [Scans](#)
- [Policies](#)
- [User Profile](#)
- [Settings](#)
- Templates

Navigating Nessus

The **Nessus** top navigation menu provides you with links to common Nessus actions.



Item	Description
Nessus logo	When clicked, the Nessus logo links to the home page. The home page will always be the Scans / My Scans page.
Scans	The Scans item directs you to your Scans / My Scans page, which lists scans you have created.
Policies	The Policies item directs you to your Policies / All Policies page, which lists policies you have created.
Username	<p>The logged-in user's name is displayed.</p> <p>When clicked, the down arrow displays links to the User Profile, Help & Support (the Tenable Support Portal), What's New features, and allows you to Sign Out.</p>
	<p>The  button links you to the Nessus Setting pages: Scanners, Accounts, Communication, and Advanced.</p> <p>Visibility of and access to general settings and options are determined based on the User Type assigned to the logged-in user's Nessus Account.</p>
	When clicked, the  button displays messages related to Nessus operations.

[TopNavAdvancedSearchBarBellUsernameLeftNav](#)

Scans Page

The default Nessus landing page is the **My Scans** section of the **Scans** page.

Name	Schedule	Last Modified	Actions
My Windows Malware Scan	Monthly on day 1 at 23:00	09:43 AM	▶ ■
My Scheduled Basic Scan	Once on September 1 at 09:30	09:43 AM	■
My Daily Scan	Daily at 01:00	09:28 AM	▶ ✕
My New DNS Scan	On Demand	09:24 AM	▶ ✕
My Basic Network Scan	On Demand	09:24 AM	▶ ✕
My Host Discovery Scan	On Demand	09:18 AM	▶ ✕


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

When logging into Nessus for the first time, the **Scans / My Scans** page will be empty and will remain empty until a **New Scan** is created.

The **All Scans** displays all Scans within all folders.

This page displays the following elements:

- **New Scan** button
- Scan Folders
- Scan Trash
- **All Scans** Link
- Scan Names
- Scan Schedules
- Last Modified Dates

-
- 
- Scan Status
 - Scan Controls

Scan Folders

- Upon install, the Nessus interface displays 3 scan system folders, which cannot be deleted: **My Scans**, **Trash**, and **All Scans**.
- **Scan / All Scans** displays all scans in all folders.
- When a scan is created, the default folder selected is **My Scans**.
- During the creation of a scan, only existing folders can be selected; scan folders cannot be created during a scan.
- From the left navigation, hovering over a scan folder's name allows you to **Rename** or **Delete** it.
- Deleting a scan folder with scans in it, moves the scans to the **Trash** folder.
- Scans in **Trash** folder no longer perform; however, the scan has not been deleted.
- From the **Trash** folder, scans can be deleted, moved to another folder, or moved to a **New Folder**.
- Scans stored in the **Trash** folder will be automatically deleted after 30 days.

After a scan is created, and based on permissions, when a scan is selected from the Scans page, the **More** button appears and the following additional options for the selected scan become available:

- **Configure**
- **Copy to**
- **Launch**
- **Mark Unread**
- **Move to**

Scans2Policies

admin

Upload

Search Scans

More

Configure

Copy to

Launch

Mark Unread

Move to

Scans / My Scans

<input type="checkbox"/> Name	Schedule	Last Modified
<input checked="" type="checkbox"/> My Basic Network Scan	On Demand	✓ 09:24 AM
<input type="checkbox"/> My Daily Scan	Daily at 01:00	✓ 09:28 AM
<input type="checkbox"/> My Host Discovery Scan	On Demand	⊘ 09:18 AM
<input type="checkbox"/> My New DNS Scan	On Demand	⊘ 09:24 AM
<input type="checkbox"/> My Scheduled Basic Scan	Once on September 1 at 09:30	🔄 09:33 AM
<input type="checkbox"/> My Windows Malware Scan	Monthly on day 1 at 23:00	⚠ 09:33 AM

Scan Statuses

Status	Description
✓ Completed	This scan has finished running and is now complete.
⚡ Aborted	This scan has been aborted. This status indicates the Nessus service was stopped during a scan.
↑ Imported	This scan has been imported; it was not run using this scanner.
📅 Pending	This is a scheduled scan or a scan that has been created but has not run yet.
🔄 Running	This scan is currently running and has not yet completed.
🔄 Resuming	This scan is resuming from a stopped state.
⌛ Canceling	This scan is in the process of being canceled.
⌛ Canceled	This scan has been canceled.
⏸ Pausing	This scan is in the process of being paused.
⏸ Paused	This scan has been paused.
🔌 Stopping	This scan is in the process of being stopped.
🔌 Stopped	This scan is in a stopped state.

Scan Results

Nessus features rich, flexible, customizable reporting tools.

Using color-coded indicators along with corresponding values, you can quickly assess your scan's data to help you understand your organization's health and vulnerabilities.

Navigating Scan Results

Scan reports and dashboard pages are reviewed using common interactive features.

You can:

- Hover over menu, page, or dashboard elements.
- Drill into data by clicking on line items or page elements.
- Use ascending ▲ and descending ▼ sorting controls.
- Navigate between pages using forward > or back < controls.

View Scan Results

The screenshot shows the Nessus Scans dashboard. At the top, there's a navigation bar with 'Scans' (2) and 'Policies'. The user is logged in as 'admin'. Below the navigation bar, there's a 'More' dropdown menu open, showing options: 'Configure', 'Copy to', 'Launch', 'Mark Unread', and 'Move to'. The main content area is titled 'Scans / My Scans' and contains a table of scans. The table has columns for 'Name', 'Schedule', and 'Last Modified'. The scans listed are: 'My Basic Network Scan' (On Demand, 09:24 AM), 'My Daily Scan' (Daily at 01:00, 09:28 AM), 'My Host Discovery Scan' (On Demand, 09:18 AM), 'My New DNS Scan' (On Demand, 09:24 AM), 'My Scheduled Basic Scan' (Once on September 1 at 09:30, 09:33 AM), and 'My Windows Malware Scan' (Monthly on day 1 at 23:00, 09:33 AM). Each row has a checkbox, a status icon, and a 'Last Modified' timestamp.

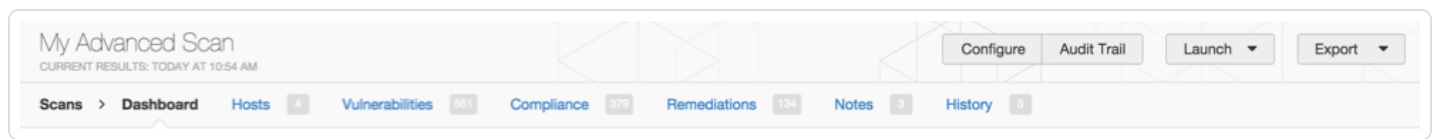
Name	Schedule	Last Modified
<input checked="" type="checkbox"/> My Basic Network Scan	On Demand	✓ 09:24 AM
<input type="checkbox"/> My Daily Scan	Daily at 01:00	✓ 09:28 AM
<input type="checkbox"/> My Host Discovery Scan	On Demand	⊘ 09:18 AM
<input type="checkbox"/> My New DNS Scan	On Demand	⊘ 09:24 AM
<input type="checkbox"/> My Scheduled Basic Scan	Once on September 1 at 09:30	🔄 09:33 AM
<input type="checkbox"/> My Windows Malware Scan	Monthly on day 1 at 23:00	⏸ 09:33 AM

1. Navigate to the **Scans / All Scans** page.
2. Select the name of the of scan.

OR

1. Navigate to the **Scans / All Scans** page.
2. Place a check box next to the name of the scan.
3. Use the **More** drop-down menu, and then select **Configure**.

Based on permissions and the scan's actions, you can **Configure** the scan, search the scan's **Audit Trail**, **Launch** the scan, or **Export** the scan's results.



Option	Description
Configure	Navigates you back to the scan's configuration settings.
Audit Trail	Displays the audit trail dialogue.
Launch	Display two choices to launch a scan: Default and Custom. <ul style="list-style-type: none"> • Default: This option uses the scan's pre-configured settings. • Custom: This options allows for Customer Scan Targets.
Export	Allows you to export the scan's result in one of four formats: Nessus (.nessus), HTML, CSV, or Nessus DB (.db). Nessus DB format is an encrypted, proprietary format, which exports all scan data. A password must be created, and then used when importing the .nessus file type.

Dashboard

When a scan is configured with **Dashboard > Enabled**, the scan's results page defaults to the inter-active dashboard view.

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

Settings / Basic / General

Name

My Basic Network Scan

Description

Folder

My Scans

Dashboard

Enabled

Scanner

Enabled

Disabled

Targets

192.168.0.1 - 192.168.0.99

Upload Targets

[Add File](#)

Save

Cancel

Dashboard Details

Name	Description
Current Vulnerabilities	The number of vulnerabilities identified.
Operating System Comparison	The percentage of operating systems identified.
Vulnerability Comparison	The percentage of all vulnerabilities, identified by severity.
Host Count	The percentage of hosts scanned by credentialed and non-credentialed author-



Comparison	ization types: without authorization, new (scan) without authorization, with authorization, and new (scan) with authorization.
Top Vul- nerabilities	Top 8 vulnerabilities based on severity.

Dashboards

When a scan is configured with **Dashboard Enabled**, the scan's results page defaults to the interactive dashboard view.

Settings / Basic / General

Name

My Basic Network Scan

Description

Folder

My Scans

Dashboard

Enabled

Scanner

Enabled

Disabled

Targets

192.168.0.1 - 192.168.0.99

Upload Targets

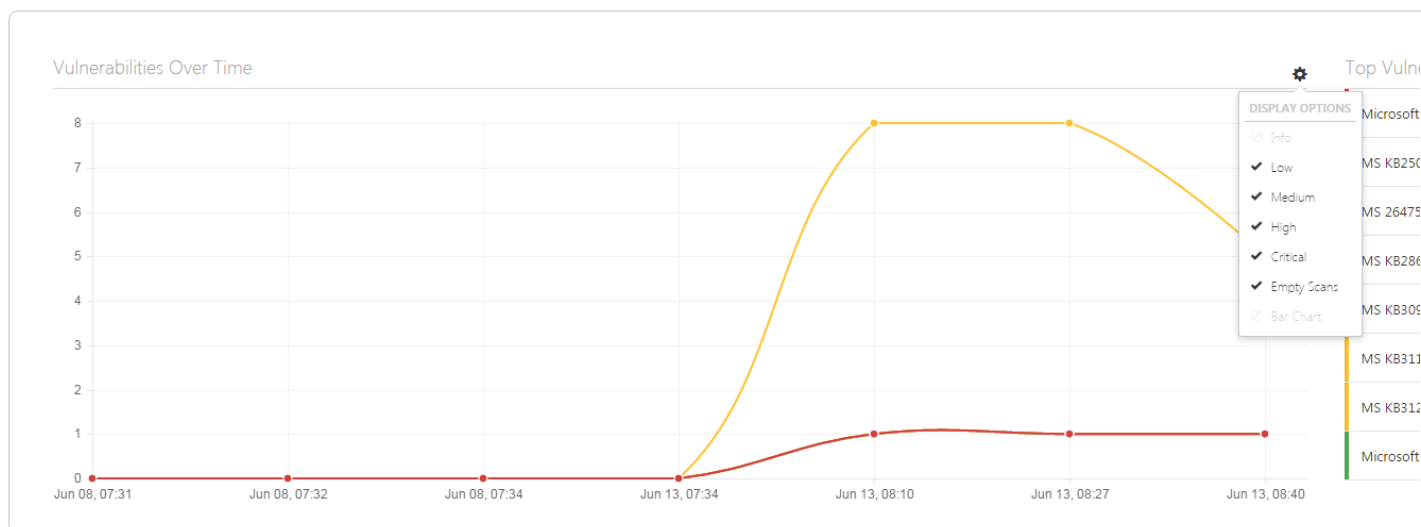
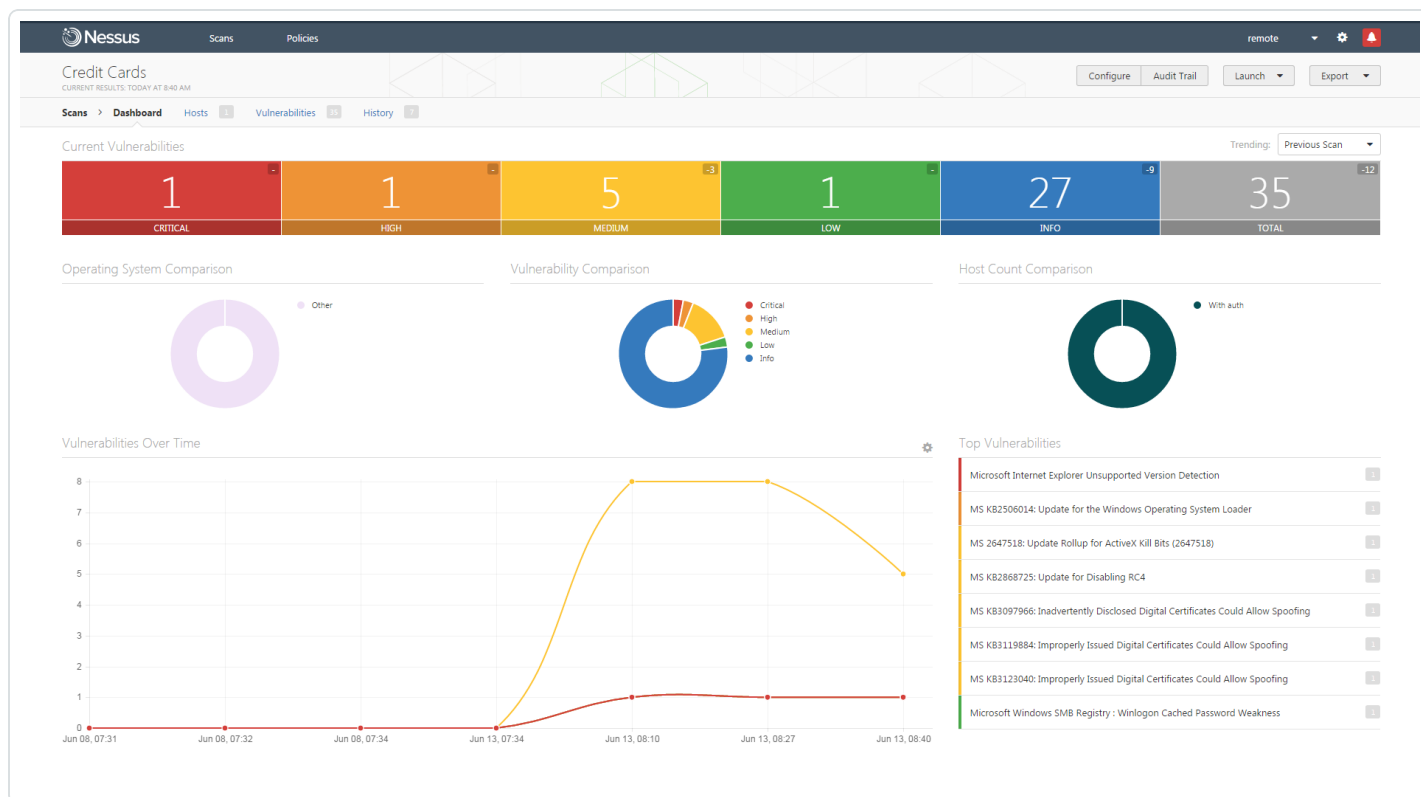
Add File

Save

Cancel

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 Vulnerabilities	The number of vulnerabilities identified by the scan, by severity.




Operating System Comparison	The percentage of operating systems identified by the scan.
Vulnerability Comparison	The percentage of all vulnerabilities by the scan, identified by severity.
Host Count Comparison	The percentage of hosts scanned by credentialed and non-credentialed authorization types: without authorization, new (scan) without authorization, with authorization, and new (scan) with authorization.
Vulnerabilities Over Time	Vulnerabilities found over a period of time. Note: At least 2 scans must be completed for this chart to be displayed.
Top Hosts	Top 8 hosts that had the highest number of vulnerabilities found in the scan.
Top Vulnerabilities	Top 8 vulnerabilities based on severity.

Scan Results Pages

When you select a scan's name from the Scans page, you will be redirected to its results pages.

The following table lists examples of each possible scan results page:

Page	Description
Dashboard	If configured, 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 plugin 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 .

Report Filters

Nessus offers a flexible system of filters to assist in displaying specific report results. Filters can be used to display results based on any aspect of the vulnerability findings. When multiple filters are used, more detailed and customized report views can be created.

The first filter type is a simple text string entered into the **Filter Vulnerabilities** box on the upper right. As you type, Nessus will immediately begin to filter the results based on your text and what it matches in the titles of the findings. The second filter type is more comprehensive and allows you to specify more details. To create this type of filter, begin by clicking on the down arrow on the right side of the Filter Vulnerabilities box. Filters can be created from any report tab. Multiple filters can be created with logic that allows for complex filtering.

A filter is created by selecting the plugin attribute, a filter argument, and a value to filter on. When selecting multiple filters, specify the keyword **Any** or **All** accordingly. If **All** is selected, then only results that match all filters will be displayed:

Option	Description
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 Description	Filter results if Plugin Description contains, or does not contain a given string (e.g., remote).
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 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 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 Type	Filter results if Plugin Type is equal to or is not equal to one of the two types of plugins: local or remote.
Solution	Filter results if the plugin Solution contains or does not contain a given string (e.g., upgrade).
Synopsis	Filter results if the plugin Solution contains or does not contain a given string (e.g., PHP).



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).
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).
CWE	Filter results based on Common Weakness Enumeration (CWE ²) if a CVSS vector is equal to, is not equal to, contains, or does not contain a CWE reference number (e.g., 200).
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).
CVSS Base Score	<p>Filter results based on if a CVSS 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 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 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 vector is equal to, is not equal to, contains, or does not contain a given string (e.g., AV:N).
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). Note: Pressing the button next to the date will bring up a calendar interface for easier date selection.
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 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 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).
CVE	Filter results based on if a CVE reference is equal to, is not equal to, contains, or does not contain a given string (e.g., 2011-0123).
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).
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).
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).
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).
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).
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).
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.
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).
IAVT	Filter results based on if an IAVT reference is equal to, is not equal to, contains, or does not contain a given string (e.g., 2012-A-0008).
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).



Risk Factor	Filter results based on the risk factor of the vulnerability (e.g., Low, Medium, High, Critical).
Exploits Available	Filter results based on the vulnerability having a known public exploit.
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.
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.
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.
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.
Elliot Exploit Framework	Filter results based on if the presence of an exploit in the Elliot exploit framework is equal to or is not equal to true or false.
Elliot Exploit Name	Filter results based on if an Elliot exploit is equal to, is not equal to, contains, or does not contain a given string (e.g., Typo3 FD).
ExploitHub	Filter results based on if the presence of an exploit on the ExploitHub web site is equal to or is not equal to true or false.

Report Screenshots

Nessus also has the ability to take screenshots during a vulnerability scan and include them in a report.

For example, if Nessus discovers VNC running without a password to restrict access, a screenshot will be taken to show the session and included in the report.

You must enable this feature in the **General** section of a scan policy, in **Scan Web Applications**.

Compare Report Results (Diff)

With Nessus, you can compare two scan reports against each other to display any differences. The ability to show scan differentials helps to point out how a given system or network has changed over time. This helps in 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.

Adv with Cred

CURRENT RESULTS: DECEMBER 2 AT 5:23 PM

Diff

Delete

Launch

Scans > Dashboard Hosts 3 Vulnerabilities 401 Remediations 54 History 2

☐ Start Time ▲

End Time

Status

✓ **Current** December 2 at 5:14 PM

December 2 at 5:23 PM

✓ Completed

✓ December 2 at 3:10 PM

December 2 at 3:18 PM

✓ Completed

Scan Details

Name: Adv with Cred

Status: Completed

Policy: Advanced Policy With Cred

Scanner: Local Scanner

Folder: My Scans

Start: December 2 at 5:14 PM

End: December 2 at 5:23 PM

Elapsed: 9 minutes

Targets: [show all](#)

Vulnerabilities

Critical

High

Medium

Low

Info

Knowledge Base

A Knowledge Base (KB) is saved with every scan performed. This is an ASCII text file containing a log of information relevant to the scan performed and results found. A KB is often useful during cases where you need support from Tenable Network Security, as it allows Customer Support staff to understand exactly what Nessus did, and what information was found. You can download a KB from the **Host Details** section.

Only scans performed on the host will have an associated KB.

Exported Results

Once a scan is finished running, Nessus scan results can be exported.

Using the **Export** button, you can export the scan's results in one of four formats:

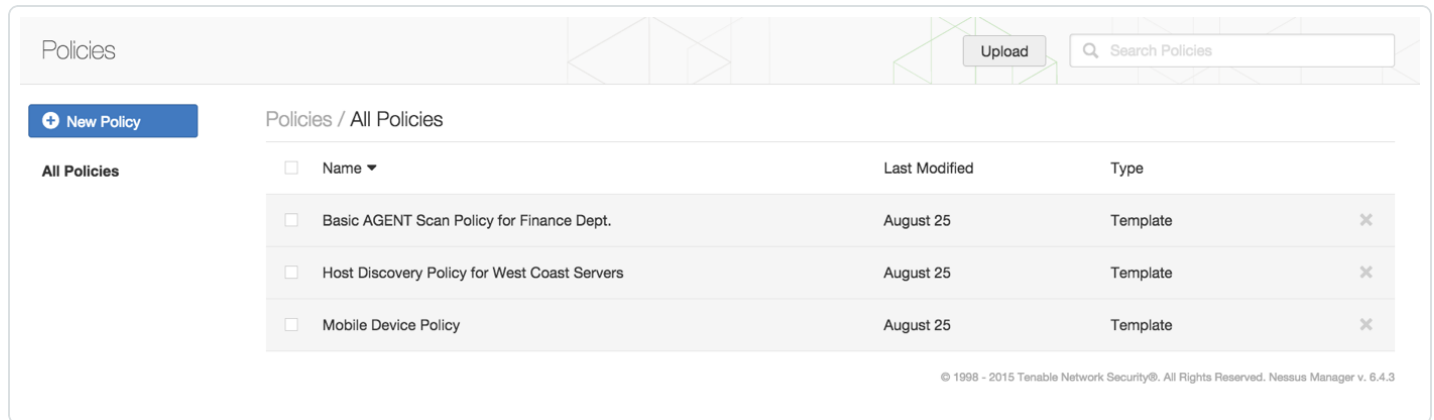
- Nessus (.nessus)
- HTML
- CSV
- Nessus DB (.db)

Nessus DB format is an encrypted, proprietary format, which exports all scan data. A password must be created, and then used when importing the `.nessus` file type.

Note: If the Nessus server time zone is changed after Nessus is installed and running, the time displayed on HTML and PDF reports will show the accurate time of day for the (new) changed time zone, but the time zone **label** will reflect the previous label of the previous time zone. To resolve this issue, restart the Nessus service.

Policies Page

The **Policies** page displays your created policies.



Policies

Upload

Search Policies

New Policy

Policies / All Policies

All Policies

<input type="checkbox"/> Name ▼	Last Modified	Type
<input type="checkbox"/> Basic AGENT Scan Policy for Finance Dept.	August 25	Template
<input type="checkbox"/> Host Discovery Policy for West Coast Servers	August 25	Template
<input type="checkbox"/> Mobile Device Policy	August 25	Template

© 1998 - 2015 Tenable Network Security®. All Rights Reserved. Nessus Manager v. 6.4.3

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

The following items are available on the **Policies** page:


















- 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, Linux 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.

When creating a Policy, in the Policy Library, **Nessus** organizes policies into three categories: **Scanner Templates**, **Agent Templates**, and **User-created** policies.






Scan Library

All Templates Scanner Agent User



Scanner Templates

 Advanced Scan Configure a scan without using any recommendations.	 Audit Cloud Infrastructure Audit the configuration of third-party cloud services.	 Badlock Detection Remote and local checks for CVE-2016-2118 and CVE-2016-0128.	 Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and CVE-2014-7169.	 Basic Network Scan A full system scan suitable for any host.
 Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	 DROWN Detection Remote checks for CVE-2016-0800.	 Host Discovery A simple scan to discover live hosts and open ports.	 Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan.	 Malware Scan Scan for malware on Windows and Unix systems.
 MDM Config Audit Audit the configuration of mobile device managers.	 Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.	 Offline Config Audit Audit the configuration of network devices.	 PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI.	 Policy Compliance Auditing Audit system configurations against a known baseline.
 SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.	 Web Application Tests Scan for published and unknown web vulnerabilities.			

Agent Templates

 Advanced Agent Scan Configure an agent scan without using any recommendations.	 Basic Agent Scan Scan systems connected via Nessus Agents.	 Malware Scan Scan for malware on systems connected via Nessus Agents.	 Policy Compliance Auditing Audit systems connected via Nessus Agents.	 SCAP and OVAL Agent Auditing Audit systems using SCAP and OVAL definitions.
---	---	--	---	--

User Created Policies

 East Coast Finance Scan A user created policy.	 West Coast Agent Scan A user created policy.
---	---

Templates

Templates are used to 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 on 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 that are available for each template](#). Additionally, the following tables list the templates that are available in Nessus and the settings available for those templates.

Scanner Templates

Template	Description	Settings	Credentials	Compliance/SCAP
Advanced Network Scan	Scans without any recommendations.	All	All	All
Audit Cloud Infrastructure	Audits the configuration of third-party cloud services.	All Basic Settings Report: Output	Cloud Services	AWS Microsoft Azure Rackspace Salesforce.com
Badlock Detection	Performs remote and local checks for CVE-2016-2118 and CVE-2016-0128.	Basic: General , Permissions Discovery: Port Scanning Assessment: General , Win-	None	Unix Unix File Contents Windows Windows File Contents

Template	Description	Settings	Credentials	Compliance/SCAP
		dows, Malware All Report groups Advanced: Debug Settings		
Bash Shellshock Detection	Performs remote and local checks for CVE-2014-6271 and CVE-2014-7169.	All Basic Settings Discovery: Scan Type Assessment: Web Applications Report: Output All Advanced Settings	Database Host Miscellaneous Patch Management Plaintext Authentication	None
Basic Network Scan	Performs a full system scan that is suitable for any host. For example, you could use this template to perform an internal vulnerability scan on your organization's systems.	All Basic Settings Discovery: Scan Type Assessment: General , Brute Force , Web Applications , Windows	Database Host Miscellaneous Patch Management Plaintext Authentication	None



Template	Description	Settings	Credentials	Compliance/SCAP
		All Report groups Advanced: Scan Type		
Basic Web App Scan	Scans web apps with a Nessus scanner.	All Basic Settings Discovery: Scan Type Assessment: General, Web Applications All Report groups Advanced: Scan Type	HTTP	None
Credentialed Patch Audit	Authenticates hosts and enumerates missing updates.	All Basic Settings Discovery: Scan Type Assessment: Brute Force, Windows, Malware All Report groups Advanced: Scan Type	SSH Windows	None
DROWN	Performs remote	All Basic Set-	None	None



Template	Description	Settings	Credentials	Compliance/SCAP
Detection	checks for CVE-2016-0800.	tings Discovery: Scan Type Report: Out-put Advanced: General , Per-formance , Debug		
Host Dis-covery	Performs a simple scan to discover live hosts and open ports.	All Basic Set-tings Discovery: Scan Type Report: Out-put	None	None
Internal PCI Network Scan	Performs an internal PCI DSS (11.2.1) vulnerability scan.	All Basic Set-tings Discovery: Scan Type Assessment: General , Brute Force , Web Applic-ations , Win-dows All Report groups Advanced:	SSH Windows Patch Man-agement	None

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



Template	Description	Settings	Credentials	Compliance/SCAP
				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.	All Basic Settings Discovery: Host Discovery Advanced: Scan Type	None	None
Policy Compliance Auditing	Audits system configurations against a known baseline.	All Basic Settings Discovery: Scan Type Report: Output Advanced: Scan Type	Database SSH Windows Miscellaneous Mobile	All
SCAP and	Audits systems using	All Basic Set-	SSH	Linux (SCAP)

Template	Description	Settings	Credentials	Compliance/SCAP
OVAL Auditing	SCAP and OVAL definitions.	tings Discovery: Host Discovery All Report groups Advanced: Scan Type	Windows	Linux (OVAL) Windows (SCAP) Windows (OVAL)

Agent Templates

Template	Description	Settings	Credentials	Compliance/SCAP
Advanced Agent Scan <div> 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. </div>	Scans without any recommendations.	All Basic Settings Discovery: Port Scanning Assessment: General , Windows , Malware All Report groups Advanced: Debug	None	Unix Unix File Contents Windows Windows File Contents
Basic Agent Scan	Scans systems connected via Nessus Agents.	All Basic Settings Discovery: Port Scanning	None	None



Template	Description	Settings	Credentials	Compliance/SCAP
		ning Assessment: General, Windows All Report groups Advanced: Debug		
Malware Scan	Scans for malware on systems connected via Nessus Agents.	All Basic Settings Discovery: Port Scanning Assessment: General, Malware All Report groups Advanced: Debug	None	None
Policy Compliance Auditing	Audits systems connected via Nessus Agents.	All Basic Settings Discovery: Port Scanning Report: Output Advanced:	None	Unix Unix File Contents Windows Windows File Contents



Template	Description	Settings	Credentials	Compliance/SCAP
		Debug		

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 Settings

The **Basic** 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 ,by section, all available **Basic** settings.

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	Specifies a description of the scan or policy.
Scan Results	Show in dashboard	Specifies whether the results of the scan should appear in dashboards or be kept private. When set to Keep private , results can only be viewed by accessing the scan directly.
Folder	My Scans	Specifies the folder where the scan appears after being saved.
Scanner	Varies	Specifies the scanner that performs the scan. The default scanner varies based on the organization and user.

Asset Lists	None	You can select or add a new target group to which the scan applies. Assets in the target group are used as scan targets.
Targets	None	Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets. Targets can be specified using a number of different formats .
Upload Targets	None	Uploads a text file that specifies targets. The targets file must be formatted in the following manner: <ul style="list-style-type: none"> • The file must be ASCII format. • Only one target per line. • No extra spaces should appear at the end of a line. • No extra lines should appear following the last target. <div> Note: Unicode/UTF-8 encoding is not supported. </div>

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.



		<ul style="list-style-type: none">• 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 10/31/2016 at 9:12 AM, the default starting date and time is set to 10/31/2016 and 09:30.</p>
Timezone	Zulu	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 <i>Weekly</i> 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 <i>Monthly</i> for Frequency .
Summary	N/A	Provides a summary of the schedule for your scan based on the values you have specified for the available settings.

Notifications

Setting	Default Value	Description
Email Recipient (s)	None	Specifies zero or more email addresses that are alerted when a scan completes and the results are available.
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 Settings

The **Discovery** 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 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 Bash Shellshock Detection DROWN Detection	Four options are available: <ul style="list-style-type: none">• Quick• Normal (default)• Thorough• Custom



Basic Network Scan Basic Web App Scan Credentialed Patch Audit Internal PCI Network Scan	Three options are available: <ul style="list-style-type: none">• Port scan (common ports) (default)• Port scan (all ports)• Custom
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 Tenable.io to ping remote hosts on multiple ports to determine if they are alive. When set to <i>On</i>, General Settings and Ping Methods appear.</p> <div> <p>Note: To scan VMware guest systems, Ping the remote host must be set to Off.</p> </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



		networks. Note: Some firewalls and packet filters use this same behavior for hosts that are up, but connected to a port or protocol that is filtered. With this option enabled, this leads to the scan considering the host is down when it is indeed up.
Maximum number of Retries	2	Specifies the number of attempts to retry pinging the remote host.
UDP	Disabled	Ping a host using the User Datagram Protocol (UDP). UDP is a stateless protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.
Scan Network Printers	Disabled	Instructs Nessus to scan network printers.
Scan Novell Netware hosts	Disabled	Instructs Nessus to scan Novell NetWare hosts.
Wake-on-LAN		
List of MAC Addresses	None	The Wake-on-LAN (WOL) menu controls which hosts to send WOL magic packets to before performing a scan. Hosts that you want to start prior to scanning are provided by uploading a text file that lists one MAC address per line. For example: <div>33:24:4C:03:CC:C7 FF:5C:2C:71:57:79</div>
Boot time wait (in minutes)	5 minutes	The amount of time to wait for hosts to start before performing the scan.
Network Type		
Network Type	Mixed (use RFC 1918)	Specifies if you are using publicly routable IPs, private non-Internet routable IPs, or a mix of these. This setting has three options:



		<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. <p>Additionally, you can type a custom range of ports by using a comma-delimited list of ports or port ranges. For example, <code>21, 23, 25, 80, 110</code> or <code>1-1024, 8080, 9000-9200</code>. If you</p>

Setting	Default Value	Description
		<p>wanted to scan all ports excluding port 0, you would type <code>1-65535</code>.</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 <code>T: 1-1024, U: 300-500</code>.</p> <p>You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate protocol. For example, <code>1-1024, T: 1024-65535, U: 1025</code>.</p>
Local Port Enumerators		
SSH (netstat)	Enabled	<p>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 Unix-based systems and requires authentication credentials.</p>
WMI (netstat)	Enabled	<p>A WMI-based scan uses netstat to determine open ports.</p> <div> <p>Note: If enabled, any custom range typed in the Port Scan Range box is ignored.</p> </div> <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 version of the returned SNMP string. This information is necessary for these audits.</p>

Setting	Default Value	Description
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>
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

Setting	Default Value	Description
		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> <div> Caution: In some rare cases, probing might disrupt some services and cause unforeseen side effects. </div>
Search for SSL based ser-	On	Controls how Nessus will test SSL-based services.

Setting	Default Value	Description
vices		<div> Caution: Testing for SSL capability on all ports may be disruptive for the tested host. </div>
Search for SSL/TLS Services (enabled)		
Search for SSL/TLS on	Known SSL/TLS ports	This setting has two options: <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 Settings

The **Assessment** 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 will be reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of Avoid potential false alarms will cause 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	Nessus attempts to send spam through each SMTP device to the address listed in this	

party domain	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 will interpret 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 web-site		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.
End at Register	16	The register at which to stop scanning.
ICCP/COTP TSAP		The ICCP/COTP TSAP Addressing menu determines a Connection Oriented

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.
Addressing Weakness		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 cloud to take screenshots of public web-	Disabled	This option enables Nessus to take screenshots to 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



Setting	Default Value	Description
servers		Internet-facing hosts, as the screenshots are generated on a managed server and sent to the Nessus scanner. Screenshots are not exported with a Nessus scan report.
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	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(\?.*)?\$). Nessus supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).
Maximum pages to crawl	1000	The maximum number of pages to crawl.
Maximum depth to crawl	6	Limit the number of links Nessus follows for each start page.
Follow dynamic pages	Disabled	If selected, Nessus follows dynamic links and may exceed the parameters set above.
Application Test Settings		
Enable gen-	Disabled	Enables the options listed below.



Setting	Default Value	Description
eric web application testss		
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 injecton test may look like /target.cgi?a='&b=2. With HTTP Parameter Pollution (HPP) enabled, the request may look like /target.cgi?a='&a=1&b=2.
Test embedded web servers	Disabled	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.

Setting	Default Value	Description
Test more than one parameter at a time per form	Disabled	<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=XSS&b=3&c=3&d=3</code> when the first value of each variable is 1. • Test random combinations of three or more parameters (slower): This form of testing randomly checks a combination of three or more parameters. This is more thorough



Setting	Default Value	Description
		<p>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 same CGI, the next known CGI, or to the next port or server.



Setting	Default Value	Description
		<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 Network Security 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		
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	None	Additional known good MD5 hashes can be uploaded via a text file that



your own list of known good MD5 hashes		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 hostnames that will be ignored by Nessus during a scan. Include one hostname per line in a regular text file
File System Scanning		
Scan file system	Off	

Report Settings

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

- [Processing](#)
- [Output](#)

Setting	Default Value	Description
Processing		
Override normal verbosity	Disabled	This setting has two options: <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 Settings

The **Advanced** 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 selected, 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 will scan 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.
Create unique identifier on hosts scanned using credentials	Enabled	Creates a unique identifier for credentialed 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 will throttle 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.
Use Linux ker-	Disabled	This enables Nessus to use the Linux kernel to detect when it is send-



Setting	Default Value	Description
nel congestion detection		ing too many packets and the network pipe is approaching capacity. If detected, Nessus will throttle 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 will wait for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish 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.
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 will eventually send (e.g., if this option is set to 15, the SYN scanner will send 1500 packets per second at most).</p>
Max number of concurrent TCP sessions per scan	none	<p>This setting limits the maximum number of established TCP sessions for the entire scan, regardless of the number of hosts being scanned.</p> <p>For scanners installed on any Windows host, this value must be set to 19 or less to get accurate results.</p>
Debug Settings		
Enable plugin debugging	Disabled	Attaches available debug logs from plugins to the vulnerability output of this scan

Credentials

By using 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 will be saved with recommended settings.

Nessus leverages the ability to log into remote Unix 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. By configuring credentials, it 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. For example,

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
- 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 will open 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 IDS	The AWS access key ID string.
AWS Secret Key	AWS secret key that provides the authentication for AWS Access Key ID.

AWS Global Settings

Option	Default	Description
Regions to access	Rest of the World	<p>In order for Nessus to audit an Amazon AWS account, you must define the regions you want to scan. Per Amazon policy, you will need different credentials to audit account configuration for the China region than you will for the Rest of the World. Choosing the Rest of the World will open the following choices:</p> <ul style="list-style-type: none">• us-east-1• us-west-1• us-west-2• eu-west-1• ap-northeast-1• ap-southeast-1• ap-southeast-2• sa-east-1• us-gov-west-1
HTTPS	Enabled	Use HTTPS to access Amazon 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
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

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.

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 Unix 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.

- [Public Key](#)
- [Certificate](#)
- [CyberArk Vault](#)
- [Kerberos](#)
- [Password](#)
- [Thycotic Secret Server](#)

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

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

Note: Non-privileged users with local access on Unix 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 three 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 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

Option	Default Value	Description
		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.

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 credentialed scans are when the supplied credentials have root privileges. Since many sites do not permit a remote login as root, Nessus can invoke `su`, `sudo`, `su+sudo`, `dzdo`, `.k5login`, or `pbrun` with a separate password for an account that 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 Vault

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Nessus can get credentials from CyberArk to use in a scan.



Option	Description
Username	The target system's username.
Domain	This is an optional field if the above username is part of a domain.
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.
Central Credential Provider Port	The port the CyberArk Central Credential Provider is listening on.
Vault Username (optional)	If the CyberArk Central Credential Provider is configured to use basic authentication you can fill in this field for authentication.
Vault Password (optional)	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.
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 the custom_CA.inc documentation for how to use self-signed certificates.

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 Unix-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 Trans-	The KDC uses TCP by default in Unix implementations. For UDP, change this option.



Option	Description
port	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 connectionpw.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 to 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.

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](#)
- [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 Network Security 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 the Do not use NTLMv1 authentication 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 Registry service during the scan	Disabled	This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running 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 Vault

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Nessus can get credentials from CyberArk to use in a scan.



Option	Description
Username	The target system's username.
Domain	This is an optional field if the above username is part of a domain.
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.
Central Credential Provider Port	The port the CyberArk Central Credential Provider is listening on.
Vault Username (optional)	If the CyberArk Central Credential Provider is configured to use basic authentication you can fill in this field for authentication.
Vault Password (optional)	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.
Appld	The Appld that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.
PolicyId	The PolicyID assigned to the credentials you would like to retrieve from the CyberArk Central Credential Provider.
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.

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 (KDC)	none	This host supplies the session tickets for the user. This is a required field.
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	The username that is used to authenticate via ssh to the system.



(required)	
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 to 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.

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 (required)	The server URL to authenticate with MobileIron
Port	Set to use a different port to authenticate



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.

Patch Management

Nessus Manager can leverage credentials for the Red Hat Network Satellite, IBM TEM, 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 menus: Symantec Altiris, IBM Tivoli Endpoint Manager (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 multiple sets of credentials are supplied to Nessus for patch management tools, Nessus will use all of them. Available credentials are:

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

If credentials are provided for a host, as well as a patch management system, or multiple patch management systems, Nessus will compare the findings between all methods and report on conflicts or provide a satisfied finding. Using the Patch Management Windows Auditing Conflicts plugins, the patch data differences (conflicts) between the host and a patch management system will be highlighted.

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 SecurityCenter 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 SecurityCenter GUI.

- 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 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 is performed using 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)

Credentials for the Dell KACE K1000 system must be provided for K1000 scanning to work properly. Under the Credentials tab, select Patch Management and then 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 Tivoli Endpoint Manager (TEM)

Tivoli Endpoint Manager (TEM) is available from IBM to manage the distribution of updates and hot-fixes for desktop systems. Nessus and SecurityCenter have the ability to query TEM to verify whether or not patches are installed on systems managed by TEM 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 TEM output.
- The data returned to Nessus by TEM is only as current as the most recent data that the TEM server has obtained from its managed hosts.

TEM scanning is performed using 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 Tivoli Endpoint Manager server must be provided for TEM scanning to work properly.

Option	Default	Description
Web Reports Server	None	Name of IBM TEM Web Reports Server
Web Reports Port	none	Port that the IBM TEM 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 TEM 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 officially supported by TEM, 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, changes must be made to the IBM TEM server. A custom Analysis must be imported into TEM so that detailed package information will be retrieved and made available to Nessus. This process is outlined below. Before beginning, the following text must be saved to a file on the TEM system, and named 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 SecurityCenter GUI.

- 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 SecurityCenter 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 SecurityCenter GUI.

- 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 Network Security, 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	
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 SecurityCenter 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 SecurityCenter GUI.

- 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 Username	None	Username required to log into the Altiris MSSQL database. This is a required field.
Database Password	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 credentialed checks is not available, users can force Nessus to try to perform checks over unsecure protocols; use the Plaintext Authentication options.

This menu allows the Nessus scanner to use credentials when testing HTTP, NNTP, FTP, POP2, POP3, IMAP, IPMI, 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-n=%USER%&password=%PASS%). If the keywords %USER% and %PASS% are used, they will be substituted with values supplied on the Login configurations drop-down menu. 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 into 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/Mobileiron
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

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 will display the list of its plugins. Individual plugins can be enabled or disabled to create very specific scans.

A family with some plugins disabled will turn **blue** and display **Mixed** to indicate only some plugins are enabled. Clicking on the plugin family will load the complete list of plugins, and allow for granular selection based on your scanning preferences.

Selecting a specific **Plugin Name** will display the plugin output that will be displayed as 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 will automatically be enabled if the family they are associated with is enabled. If the family has been disabled or partially enabled, new plugins in that family will automatically be disabled as well.

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

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 Network Security (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 Nessus Professional	<p>For Nessus Manager and Nessus Professional versions, Tenable provides the PCI Quarterly External Scan (Unofficial) template.</p> <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 Network Security 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 Nessus Professional	<p>The Internal PCI Network Scan template can be used to meet PCI DSS Internal scanning requirement (11.2.1).</p>

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.

User Profile Page

The **User Profile** page includes the following sections:

- Account Settings
- Change Password
- Plugin Rules
- API Keys

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


Account Settings

The **Account Settings** section displays settings for the current authenticated user. Usernames cannot be changed. Based on your Nessus product, the following information appears in this section:

Version	Settings
Tenable.io	Username (email address) Full Name Email User Type
Nessus Manager	Username Full Name Email User Type
Nessus Professional	Username User Type

Change Password

The **Change Password** section allows you to change your password. Users with administrative privileges can change other user passwords.

To change another user's password, log in to Nessus as a user with administrative privileges, and select the  button, and then navigate to the **Users** section of the **Accounts** page.

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** section 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 reprioritize the severity of plugin results to better account for your organization's security posture and response plan.

API Keys

API Keys consist of an Access Key and a Secret Key, and are used to authenticate with the **Nessus REST API** (version 6.4 or greater) and passed with requests using the "X-ApiKeys" HTTP header.

Select the **Generate** button to create an **Access Key** and a **Secret Key**.

Note:

- API Keys are only presented upon initial generation. Please store API Keys in a safe location, as they cannot be retrieved later.
- API Keys cannot be retrieved by Nessus. If lost, an API Key must be regenerated.
- Regenerating an API Key will immediately deauthorize any applications currently using the key.

Settings Page

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

- [Scanners](#)
- [User and Group Accounts](#)
- [Communication](#)
- [Advanced Settings](#)

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 web interface. The top navigation bar includes the Nessus logo, 'Scans', 'Policies', and a user profile 'admin' with a dropdown arrow, a settings gear icon, and a notification bell icon. Below the navigation bar, the 'Settings' page is displayed with tabs for 'Scanners', 'Accounts', 'Communication', and 'Advanced'. The 'Scanners' tab is active, showing a sub-section 'Scanners / Local / Overview'. On the left, there is a sidebar menu with categories: 'LOCAL' (Overview, Permissions, Software Update), 'REMOTE' (Linked), 'AGENTS' (Linked, Groups, Blackout Windows), and 'GLOBAL' (Custom CA). The main content area displays two tables. The first table, titled 'Nessus Manager', shows system information: Version 6.10.5 (#794) with a refresh icon, Licensed Hosts 3000, Licensed Scanners 0 of 1000, and Licensed Agents 11 of 1000. The second table, titled 'Plugins', shows: Last Updated April 07, 2017 with a refresh icon, Expiration January 01, 2020, Plugin Set 201704071215, and Activation Code [REDACTED] with an edit icon.

Nessus Manager		Plugins	
Version	6.10.5 (#794)	Last Updated	April 07, 2017
Licensed Hosts	3000	Expiration	January 01, 2020
Licensed Scanners	0 of 1000	Plugin Set	201704071215
Licensed Agents	11 of 1000	Activation Code	[REDACTED]

Scanners

Scanners are displayed on the **Settings** page and displays the left navigation menu that includes links to settings specific to **Scanners**.

Based on product version, the **Scanners** page navigation includes **Overview**, **Link** (Nessus Professional only), **Software Update**, and in **Nessus Manager**, linked **Remote** and **Agents** scanners.

The screenshot shows the 'Settings' page with the 'Scanners' tab selected. The left sidebar contains a navigation menu with 'Overview' selected under the 'LOCAL' section. The main content area is titled 'Scanners / Local / Overview' and displays information for the 'Nessus Manager' and 'Plugins'.

Nessus Manager		Plugins	
Version	6.7.0	Last Updated	May 16, 2016
Licensed Hosts	256	Expiration	June 13, 2016
Licensed Scanners	0 of 10	Plugin Set	201605162130
Licensed Agents	1 of 10	Activation Code	[Redacted]

Scans	Start Time	Last Modified	Owner	Status
Advanced Compliance Scan	May 15	07:05 AM	remote	Paused
Finance Department Basic Network Scan	May 15	07:05 AM	remote	Paused

Scanners / Local / Overview

Purpose: The Scanners / Local / Overview page displays the **Overview** for your **Local** Nessus Scanner and its Nessus plugins, including the following information:

- Your Nessus product name and version.
- Your number of licensed hosts.
- Your number of licensed Scanners.
- Your number of licensed Agents (Nessus Manager and Tenable.io only).
- Your plugin last update.
- Your plugin expiration date.
- The plugin set identifier.
- Your Nessus Activation Code.

The button next to the **Activation Code** allows you to update your **Activation Code** as needed.

Nessus Manager		Plugins	
Version	6.7.0	Last Updated	May 16, 2016
Licensed Hosts	256	Expiration	June 13, 2016
Licensed Scanners	0 of 10	Plugin Set	201605162130
Licensed Agents	1 of 10	Activation Code	

Scans ▼	Start Time	Last Modified	Owner	Status
Advanced Compliance Scan	May 15	07:05 AM	remote	Paused
Finance Department Basic Network Scan	May 15	07:05 AM	remote	Paused

Setting	Description	Product Version(s)	User Type(s)
Local			
Overview	The overview page gives detailed information about the product version and plugins.	Nessus Manager Nessus Professional	All user account roles except Basic
Permissions	Users or groups are added to the permission page for the following permissions: <ul style="list-style-type: none"> No Access: Any users or groups specified cannot view, use, or manage the scanners. Can Use: Users or groups specified can view and use the scanner, but cannot make any changes. Can Manage: Users or groups specified can make changes to the scanner's settings. 	Nessus Manager Nessus Professional	System Administrator
Link	Enabling this option allows this local scanner to be linked to Nessus Manager or to Tenable.io. <div> Tip: When linking to Tenable.io, use the following settings: </div>	Nessus Professional	System Administrator

Setting	Description	Product Version(s)	User Type(s)
	<ul style="list-style-type: none"> • Manager Host: cloud.tenable.com • Manager Port: 443 • Linking Key: Cloud Linking Key <p>In Tenable.io, the Linking Key is displayed on the Scanners > Linked Scanners page.</p> <p>Note: Nessus Professional can be linked to another Nessus Manager or Tenable.io instance only once.</p>		
Software Update	<p>Software updates can be configured for updating all Nessus components, Nessus plugins only, or disabled altogether.</p> <p>Options include Update Frequency and you have the ability to configure a custom Plugin Feed host.</p> <p>This page also allows you to perform a Manual Software Update using the downloaded, compressed TAR file obtained when you Register Nessus Offline and Download and Copy Plugins.</p>	Nessus Manager Nessus Professional	System Administrator
Remote			
Linked	Remote scanners can be linked to this manager through the provided key or valid account credentials. Once linked, they can be managed locally and selected when configuring scans.	Nessus Manager	System Administrator Administrator
Agents			
Linked	Agents can be linked to this manager using the provided key with the following setup instruc-	Nessus Manager	System Administrator



Setting	Description	Product Version(s)	User Type(s)
	<p>tions. Once linked, they must be added to a group for use when configuring scans. Also, linked agents will automatically download plugins from the manager upon connection.</p> <div>Note: this process can take several minutes and is required before an agent will return scan results.</div>		
Groups	<p>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. From this view, you can manage your agent groups.</p>	Nessus Manager	System Administrator

Scanners / Local / Overview (Manager)

Nessus Manager Overview page displays the **Overview** for your **Local** Nessus Scanner and its Nessus plugins:

- Your Nessus product name and version.
- Your number of licensed hosts.
- Your number of licensed scanners.
- Your number of licensed agents.
- Your plugin last update.
- Your plugin expiration date.
- The plugin set identifier.
- Your Nessus Activation Code.

From the Overview Page, you can:

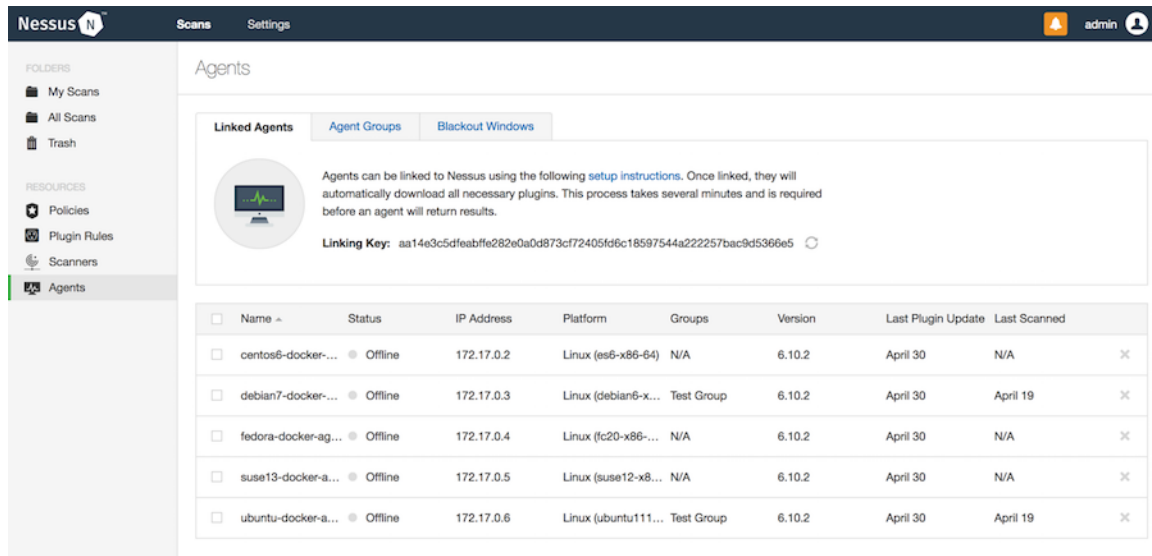
- [Update Nessus Version](#)
- [Update Plugins](#)
- [Update Activation Code](#)

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

Nessus Agents

Nessus Agents can be connected to Tenable.io or Nessus Manager. Agents increase scan flexibility by making it easy to scan assets without host credentials or assets that are offline. In addition, you can use agents to conduct large-scale concurrent scans with little network impact.

In the **Scanners** section of the **Settings** page, in the **Agents** section, you can view details about your linked agents, add or remove agents from Agent Groups, and manage Blackout Windows.



The screenshot shows the Nessus interface with the 'Agents' section selected. The 'Linked Agents' tab is active, displaying a list of agents. A 'Linking Key' is shown as a long alphanumeric string. The table below lists the agents:

<input type="checkbox"/>	Name ^	Status	IP Address	Platform	Groups	Version	Last Plugin Update	Last Scanned	
<input type="checkbox"/>	centos6-docker-...	Offline	172.17.0.2	Linux (es6-x86-64)	N/A	6.10.2	April 30	N/A	✕
<input type="checkbox"/>	debian7-docker-...	Offline	172.17.0.3	Linux (debian6-x...	Test Group	6.10.2	April 30	April 19	✕
<input type="checkbox"/>	fedora-docker-ag...	Offline	172.17.0.4	Linux (fc20-x86-...	N/A	6.10.2	April 30	N/A	✕
<input type="checkbox"/>	suse13-docker-a...	Offline	172.17.0.5	Linux (suse12-x8...	N/A	6.10.2	April 30	N/A	✕
<input type="checkbox"/>	ubuntu-docker-a...	Offline	172.17.0.6	Linux (ubuntu111...	Test Group	6.10.2	April 30	April 19	✕

[List of Linked Agents](#)[Agent Group Management](#)[Blackout Windows](#)

This table displays your linked agents. Click any row in the table to view more details about the agent.

Click [here](#) to add or remove agents from Agent Groups.

Click [here](#) to manage Blackout Windows.

In the **Blackout Windows** section, you can block automatic updates from occurring at specific times.

Scanners / Agents / Linked



Agents can be linked to this manager using the provided key with the following [setup instructions](#). Once linked, they must be added to a [group](#) for use when configuring scans. Also, linked agents will automatically download plugins from the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.

Linking Key: 0c80f7839725f252a87f281f1f8f16140d4d06796393814a3495ca91c6d02577

<input type="checkbox"/>	Name ▼	Status	IP Address	Platform	Groups	Version	Last Plugin Update	Last Scanned	
<input type="checkbox"/>	centos5-agent-6...	● Online	192.168.1.1	Linux (es5-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos6-agent-6...	● Online	192.168.1.2	Linux (es6-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos6-agent-6...	● Online	192.168.1.3	Linux (es6-x86-64)	All	6.8.1	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos7-agent-6...	● Online	192.168.1.4	Linux (es7-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos7-agent-6...	● Online	192.168.1.5	Linux (es7-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos7-agent3-...	● Online	192.168.1.6	Linux (es7-x86-64)	All	6.7.0	06:15 AM	11:14 AM	×
<input type="checkbox"/>	debian7-agent-6...	● Online	192.168.1.7	Linux (debian6-x...	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	debian7-agent-6...	● Online	192.168.1.8	Linux (debian6-x...	All	6.9.1	06:15 AM	11:14 AM	×
<input type="checkbox"/>	ubuntu14-agent-...	● Online	192.168.1.9	Linux (ubuntu11...	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	ubuntu14-agent-...	● Online	192.168.1.10	Linux (ubuntu11...	All	6.9.2	06:15 AM	11:14 AM	×

For instructions about installing agents, see [Nessus Agent Install](#).

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.

On the **Scanners / Agents / Linked** page, you can create a new group.


Once a new group has been created, you can:

- Manage its agents.
- Set permissions for the agent group.
- Rename the agent group.

During the installation of Nessus Agents, you had the option of adding your agent to an existing agent group.

Scanners / Agents / Groups

New Group



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. From this view, you can manage your agent groups.

☐ Name ▼

☐ Targets ×

☐ Windows Agents ×

If you did not create any agent groups prior to installing the Nessus Agent, or you opted to not add your agent to an existing group, you can create agent groups in the Nessus UI.

User and Group Accounts

Setting Name	Description	Product Version(s)	User Type(s)
Users	Individual Nessus accounts to be used for assigning permissions.	Tenable.io Nessus Professional Nessus Manager	All User Types
Groups	Collections of users created for shared permissions.	Tenable.io Nessus Manager	System Administrator

Settings

ScannersAccountsCommunicationAdvanced

ACCOUNTS

UsersGroups

Accounts / Users

+ New User

<input type="checkbox"/> Name ▾	Last Login	Type
<input type="checkbox"/> Adam	N/A	Administrator
<input type="checkbox"/> Basya	N/A	Basic
<input checked="" type="checkbox"/> remote	04:52 PM	System Administrator
<input type="checkbox"/> Stan	N/A	Standard
<input type="checkbox"/> Sylvia	N/A	System Administrator

Settings

ScannersAccountsCommunicationAdvanced

ACCOUNTS

UsersGroups

Accounts / Groups

+ New Group

<input type="checkbox"/> Name ▾	Members
<input type="checkbox"/> Finance Department	3
<input type="checkbox"/> IT Security Group	3

Communication

The **Communications** page allows you to configure Nessus to communicate with network servers and connector services.

Nessus Scans Policies Sylvia [Settings Icon] [Notification Icon]

Settings

Scanners Accounts **Communication** Advanced


NETWORK

- LDAP Server
- Proxy Server
- SMTP Server

CONNECTORS

- Cisco ISE

Communication / Network / 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, Nessus administrators can add users straight from their directory and these users can authenticate using their directory credentials.

General Settings

Host

Port

Username

Password

Base DN

Advanced Settings

Show advanced settings ☐

Setting Name	Description	Product Version(s)	User Type(s)
NETWORK			
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, Nessus administrators can add users straight from their directory and these	Tenable.io Nessus Manager	System Administrator

Setting Name	Description	Product Version(s)	User Type(s)
	<p>users can authenticate using their directory credentials.</p> <div> Tip: Nessus auto-negotiates encryption, therefore there are no encryption options in the Nessus interface. </div>		
Proxy Server	Proxy servers are used to forward HTTP requests. If your organization requires one, Nessus uses these settings to perform plugin updates and communicate with remote scanners. There are five fields that control proxy settings, but only the host and port are required. Username, password, and user-agent are available if needed.	Tenable.io Nessus Manager Nessus Professional	System Administrator
SMTP Server	Simple Mail Transfer Protocol (SMTP) is an industry standard for sending and receiving email. Once configured for SMTP, Nessus will email scan results to the list of recipients specified in a scan's "Email Notifications" configuration. These results can be customized through filters and require an HTML compatible email client.	Tenable.io Nessus Manager Nessus Professional	System Administrator
CONNECTORS			
Cisco ISE	Cisco Identity Services Engine (ISE) is a security policy management and control platform that simplifies access control and security compliance for wired, wireless, and VPN connectivity. Cisco ISE is primarily used to provide secure access, support BYOD initiatives, and enforce usage policies. Nessus only supports Cisco ISE version 1.2 or greater.	Nessus Manager	System Administrator

Advanced Settings

The **Advanced** page allows you to manually configure the Nessus daemon.

Settings

Scanners

Accounts

Communication

Advanced

Search Settings

Advanced Settings

New Setting

Setting ▼	Value	
<input type="checkbox"/> allow_post_scan_editing	yes	×
<input type="checkbox"/> auto_enable_dependencies	yes	×
<input type="checkbox"/> auto_update	yes	×
<input type="checkbox"/> auto_update_delay	24	×

- Advanced Settings are global settings.
- To configure Advanced Settings, you must use a Nessus System Administrator user account.
- When modified, changes go into effect a few minutes after the setting is saved.
- `global.max_hosts`, `max_hosts`, and `max_checks` settings can have a particularly great impact on the ability to perform scans.
- Custom policy settings supersede the global Advanced Settings.

Note: When an Advanced Setting is added or an existing setting is modified, you are prompted to either **Discard** or **Save** the setting.

Setting	Default	Description
allow_post_scan_editing	Yes	Allows a user to make edits to scan results after the scan is complete.
auto_enable_dependencies	Yes	Automatically activates the plu-



Setting	Default	Description
		gins that are depended on. If disabled, not all plugins may run despite being selected in a scan policy.
auto_update	Yes	Automatically updates plugins. If enabled and Nessus is registered, fetch the newest plugins from plugins.nessus.org automatically. Disable if the scanner is on an isolated network that is not able to reach the Internet.
auto_update_delay	24	Number of hours to wait between two updates. Four (4) hours is the minimum allowed interval.
cgi_path	/cgi-bin:/scripts	A colon-delimited list of CGI paths.
checks_read_timeout	5	Read timeout for the sockets



Setting	Default	Description
		of the tests.
disable_ui	No	Disables the user interface on managed scanners.
disable_ntp	Yes	Disables the old NTP legacy protocol.
disable_xmlrpc	No	Disables the new XMLRPC (Web Server) interface.
dumpfile	C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.dump	Location of a dump file for debugging output if generated.
global.max_hosts	2150	Maximum number of simultaneous checks against each host tested.
global.max_scans	0	<p>If set to non-zero, this defines the maximum number of scans that may take place in parallel.</p> <p>If this option is not used, no limit is enforced.</p>



Setting	Default	Description
global.max_simult_tcp_sessions	50	<p>Maximum number of simultaneous TCP sessions between all scans.</p> <p>If this option is not used, no limit is enforced.</p>
global.max_web_users	1024	<p>If set to non-zero, this defines the maximum of (web) users who can connect in parallel.</p> <p>If this option is not used, no limit is enforced.</p>
listen_address	0.0.0.0	<p>IPv4 address to listen for incoming connections.</p> <p>If set to 127.0.0.1, this restricts access to local connections only.</p>
log_whole_attack	No	<p>Logs every detail of the attack.</p> <p>Helpful for debugging issues with the scan, but this may be disk</p>



Setting	Default	Description
		intensive.
logfile	C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.messages	Location where the Nessus log file is stored.
login_banner	None	A text banner that appears before the initial login the Flash or HTML5 client.
max_hosts	5	Maximum number of hosts checked at one time during a scan.
max_checks	5	Maximum number of simultaneous checks against each host tested.
nasl_log_type	Normal	Direct the type of NASL engine output in nessusd.dump.
nasl_no_signature_check	No	Determines if Nessus considers all NASL scripts as being signed. Selecting "yes" is unsafe and not recommended.



Setting	Default	Description
nessus_syn_scanner.global_throughput.max	65536	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.
nessus_udp_scanner.max_run_time	31536000	Used to specify the maximum run time, in seconds, for the UDP port scanner. If the setting is not present, a default value of 365 days (31536000 seconds) is used instead.
non_simult_ports	139, 445, 3389	Specifies ports against which two plugins cannot not be run simultaneously.

Setting	Default	Description
optimize_test	Yes	Optimizes the test procedure. Changing this to “no” causes scans to take longer and typically generate more false positives.
plugin_upload	Yes	Designates if admin users may upload plugins.
plugins_timeout	320	Maximum lifetime of a plugin’s activity (in seconds).
port_range	Default	Range of the ports the port scanners scans. Can use keywords “default” or “all”, as well as a comma delimited list of ports or ranges of ports.
purge_plugin_db	No	Determines if Nessus purges the plugin database at each update. This directs Nessus to



Setting	Default	Description
		remove, re-download, and re-build the plugin database for each update. Choosing yes causes each update to be considerably slower.
qdb_mem_usage	Low	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, settings this to “low” uses considerably less memory, but at the price of a moderate performance impact.
reduce_connections_on_	No	Reduces the number of TCP



Setting	Default	Description
congestion		sessions in parallel when the network appears to be congested.
report_crashes	Yes	<p>Anonymously reports crashes to Tenable Network Security.</p> <p>When set to yes, Nessus crash information is sent to Tenable Network Security to identify problems. Personal nor system-identifying information is sent to Tenable Network Security.</p>
remote_listen_port	None	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

Setting	Default	Description
		port). By adding this setting, you can link your managed scanners and agents a different port (Example: 9000) instead of the defined in xmlrpc_listen_port (default 8834).
rules	C:\ProgramData\Tenable\Nessus\conf\nessusd.rules	Location of the Nessus Rules file (nessusd.rules).
safe_checks	Yes	Safe checks rely on banner grabbing rather than active testing for a vulnerability.
silent_dependencies	Yes	If 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,



Setting	Default	Description
		Nessus runs those plugin dependencies, but does not include their output in the report. Setting this option to no causes both the selected plugin and any plugin dependencies to all appear in the report.
slice_network_addresses	No	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).
ssl_cipher_list	Strong	Nessus only supports 'strong' SSL ciphers

Setting	Default	Description
		when connecting to port 8834.
ssl_mode	tls_1_2	<p>Minimum supported version of TLS.</p> <p>If not present or if removed, Nessus will use TLS 1.0 (tls_1_0).</p>
stop_scan_on_disconnect	No	Stops scanning a host that seems to have been disconnected during the scan.
stop_scan_on_hang	No	Stops a scan that seems to be hung.
throttle_scan	Yes	Throttles scan when CPU is overloaded.
user_max_login_attempt	None	<p>The number of possible invalid login attempts before a user is locked out.</p> <div> <p>Note: A user with administrative privileges must edit the locked</p> </div>



Setting	Default	Description
		<div>account to unlock the user.</div>
www_logfile	C:\ProgramData\Tenable\Nessus\nessus\logs\www_server.log	Location where the Nessus Web Server (user interface) log is stored.
xmlrpc_idle_session_timeout	30	XMLRPC Idle Session Timeout in minutes. Value defaults to 30 minutes. If the value is set to zero (0), the default value of 30 minutes applies. There is no maximum limit for this value.
xmlrpc_listen_port	8834	Port for the Nessus Web Server to listen on (new XMLRPC protocol).

Manage Nessus

This section includes instructions and procedures for common Nessus usage.

- [Manage Nessus License and Registration](#)
- [Manage Activation Code](#)
- [User Profile](#)
- [System Settings](#)
- [Manage Scanners](#)
- [Manage Accounts](#)
- [Manage Communications](#)
- [Manage Advanced Settings](#)
- [Manage Scans](#)
- [Policies](#)
- [Manage Nessus Agents](#)
- [Custom SSL Certificates](#)
- [Enable SSH Local Security Checks](#)
- [Credentialed Checks on Windows](#)

Manage Scans

This section includes information and steps to perform common tasks associated with managing Nessus Scans.

For information, see the following links:

- [Create a Scan](#)
- [Create an Agent Scan](#)
- [Create a Scan Folder](#)
- [Manage Scans](#)
- [Manage Agent Groups](#)

Tip: For more information about the **Scans** page, see the related [Features](#) section of this guide.

Create a Scan

All Scan and Policy Templates share **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** settings, as well as **Credentials** options.

Advanced Scan templates include **Compliance** and **Plugins** options.

Note: Tenable offers a Nessus scanner AMI in the AWS Marketplace for use with Tenable.io that is preauthorized to scan your AWS instances. There is no need to ask AWS for permission. When you launch a Nessus preauthorized scanner, it appears as a scanner in your instance of Tenable.io. When you select that scanner in a scan configuration, the Targets subsection appears on the Settings page in the Basic section. In the Targets subsection, you can select the AWS instances you want to scan. See the How-To guide for preauthorized scanners, available on the [Tenable AWS integrations page](#). Note that this is available only for Tenable.io.

Create a Basic Network Scan

1. On the **Scans / My Scans** page, select the **New Scan** button.

The **Scan Library** appears.

2. Select the **Basic Network Scan** template.
3. Configure the scan settings using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.
4. Select **Credentials**.
5. In the **Credentials** list, select the applicable credentials required to perform the scan. Multiple credentials can be added.
6. Select **Save** or **Launch**.
 - Select the **Save** button to save the scan without launching. The scan is set to **On Demand**, and can be launched from the **Scans / MyScans** page.
 - Select the **Save ▼** arrow to display the **Launch** option. If you select **Launch**, the scan will be saved and launch immediately.

Create an Advanced Scan

1. On the **Scans / My Scans** page, select the **New Scan** button.

The **Scan Library** appears.

2. Select the **Advanced Scan** template.
3. Configure the scan settings using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.
4. Select **Credentials**.
5. In the **Credentials** list, select the applicable credentials required to perform the scan. Multiple credentials can be added and configured.
6. If applicable, select **Compliance**.
7. In the **Compliance Checks** list, select compliance checks applicable to perform the scan. Multiple compliance checks can be added and configured.
8. If applicable, select **Plugins**.

The enabled plugins appear.

9. Select **Save** or **Launch**.
 - Select the **Save** button to save the scan without launching. The scan is set to **On Demand**, and can be launched from the **Scans / MyScans** page.
 - Select the **Save ▼** arrow to display the **Launch** option. If you select **Launch**, the scan will be saved and launch immediately.

Create a PCI Quarterly External Scan (Unofficial)

1. Navigate to the **Scans / My Scans** page.
2. Select the **New Scan** button.
3. Select the **PCI Quarterly External Scan (Unofficial)** template.
4. Enter a **Name** and **Description**.
5. Next, if applicable, configure settings: **Basic**, **Discovery**, and **Advanced**.

Tip: In Nessus Professional and Nessus Manager, the scan results from the PCI Quarterly External Scan (Unofficial) may **not** be submitted to Tenable Network Security for PCI AVS Validation. This feature is available only in Tenable.io.

Tip: For scanning agents, see [Manage Nessus Agents](#).

Create an Agent Scan

Note: Before an Agent can be used in a scan, the Agent must be added to at least one [Agent Group](#).

Create a Basic Agent Scan

1. On the **Scans / My Scans** page, select the **New Scan** button.

The **Scan Library** appears.

Scan Library

Search Library

All Templates

Scanner

Agent

User

Scanner Templates

Advanced Scan
Configure a scan without using any recommendations.

Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan
A full system scan suitable for any host.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

DROWN Detection
Remote checks for CVE-2016-0800.

Host Discovery
A simple scan to discover live hosts and open ports.

Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan
Scan for malware on Windows and Unix systems.

MDM Config Audit
Audit the configuration of mobile device managers.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit
Audit the configuration of network devices.

PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing
Audit system configurations against a known baseline.

SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.

Web Application Tests
Scan for published and unknown web vulnerabilities.

Agent Templates

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

Basic Agent Scan
Scan systems connected via Nessus Agents.

Malware Scan
Scan for malware on systems connected via Nessus Agents.

Policy Compliance Auditing
Audit systems connected via Nessus Agents.

SCAP and OVAL Agent Auditing
Audit systems using SCAP and OVAL definitions.

User Created Policies

East Coast Finance Scan
A user created policy.

West Coast Agent Scan
A user created policy.

2. Select the **Agent** tab.
3. Select the **Basic Agent Scan** template.

Agent Templates



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



Basic Agent Scan
Scan systems connected via Nessus Agents.



Malware Scan
Scan for malware on systems connected via Nessus Agents.



Policy Compliance Auditing
Audit systems connected via Nessus Agents.



SCAP and OVAL Agent Auditing
Audit systems using SCAP and OVAL definitions.

4. Next, enter your Agent Scan details.

Name	Required
Folder	The folder where this Agent Scan is stored. The default selection is My Scans .
Dashboard	If you select Enabled , the scan results are included in dashboards .
Agent Groups	Required Use the drop-down to select one or more Agent Groups .
Scan Window	Use the Scan Window drop-down to select an interval of time. To be included and visible in vulnerability reports, Nessus Agents must report within this time-frame. Predefined values: <ul style="list-style-type: none"> • 15 minutes • 30 minutes • 1 hour • 6 hours • 12 hours • 1 day

New Scan / Basic Agent Scan

Scan Library > Settings

BASIC ✓

General

Schedule

Notifications

Permissions

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Settings / Basic / General

Name: IT Department Basic Agent Scan

Description:

Folder: My Scans

Dashboard: Enabled

Agent Groups: IT Dept Agent Group

Scan Window: 1 hour

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

Save Cancel

5. OPTIONAL: Configure the scan's **Settings: Basic, Discovery, Assessment, Report,** and **Advanced** links.

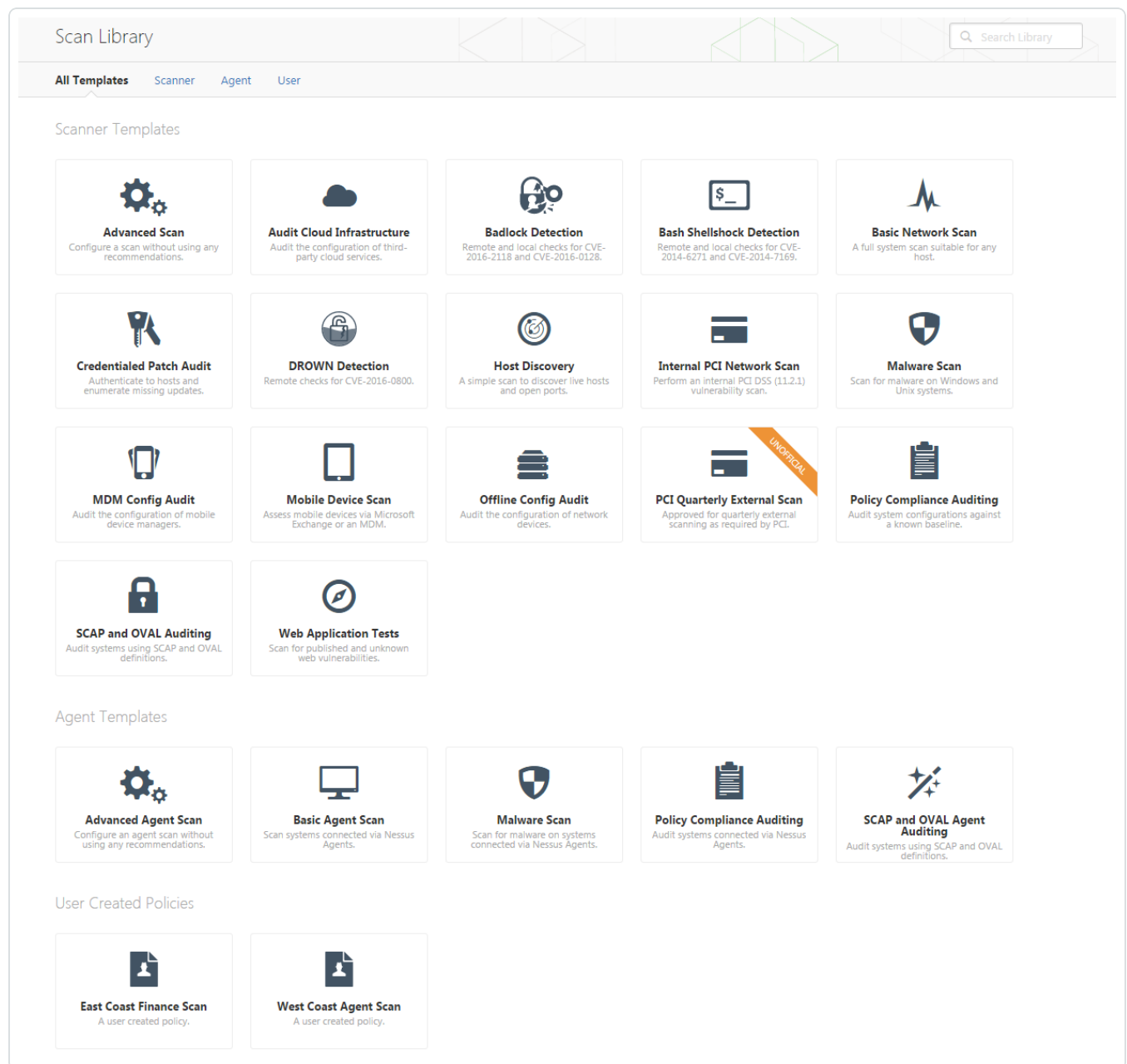
6. Select **Save** or **Launch**.

- Select the **Save** button to save the scan without launching. The scan is set to **On Demand**, and can be launched from the **Scans / MyScans** page.
- Select the **Save ▼** arrow to display the **Launch** option. If you select **Launch**, the scan will be saved and launch immediately.

Create an Advanced Agent Scan

1. On the **Scans / My Scans** page, select the **New Scan** button.

The **Scan Library** appears.



2. Select the **Advanced Agent Scan** template.
3. Configure the scan's **Settings** using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.
4. Select **Credentials**.
5. If applicable, select **Compliance**.



6. From the **Compliance Checks** list, select compliance checks applicable to perform the scan. Multiple compliance checks can be added and configured.
7. If applicable, select **Plugins**; enabled plugins are displayed.
8. Select **Save** or **Launch**.
 - Select the **Save** button to save the scan without launching. The scan is set to **On Demand**, and can be launched from the **Scans / MyScans** page.
 - Select the **Save ▼** arrow to display the **Launch** option. If you select **Launch**, the scan will be saved and launch immediately.

Create a Scan Folder

1. From the **Scans / My Scans** page, select **New Folder**.
2. Provide a **Name** for your new folder. The name must be 20 characters or fewer.

Manage Scans

View all scans on the [Scans / All Scans](#) page.

The screenshot shows the Tenable Scans interface. At the top, there's a navigation bar with 'Scans' (2) and 'Policies'. The user is logged in as 'admin'. A 'More' dropdown menu is open, showing options: 'Configure', 'Copy to', 'Launch', 'Mark Unread', and 'Move to'. Below the menu, there's a table of scans. The table has columns for 'Name', 'Schedule', and 'Last Modified'. The scans listed are: 'My Basic Network Scan' (On Demand, 09:24 AM), 'My Daily Scan' (Daily at 01:00, 09:28 AM), 'My Host Discovery Scan' (On Demand, 09:18 AM), 'My New DNS Scan' (On Demand, 09:24 AM), 'My Scheduled Basic Scan' (Once on September 1 at 09:30, 09:33 AM), and 'My Windows Malware Scan' (Monthly on day 1 at 23:00, 09:33 AM). Each scan row has a checkbox, a status icon, and a 'More' button.

Name	Schedule	Last Modified
<input checked="" type="checkbox"/> My Basic Network Scan	On Demand	✓ 09:24 AM
<input type="checkbox"/> My Daily Scan	Daily at 01:00	✓ 09:28 AM
<input type="checkbox"/> My Host Discovery Scan	On Demand	⊘ 09:18 AM
<input type="checkbox"/> My New DNS Scan	On Demand	⊘ 09:24 AM
<input type="checkbox"/> My Scheduled Basic Scan	Once on September 1 at 09:30	🔄 09:33 AM
<input type="checkbox"/> My Windows Malware Scan	Monthly on day 1 at 23:00	⚠ 09:33 AM

When a scan is selected from the list of scans, the **More** button appears and additional options for the selected scan become available.

Select **Configure** to display the scan results and modify scan settings.

Scans 2 Policies

admin

More

Configure

Copy to

Launch

Mark Unread

Move to

Upload

Search Scans

Scans / My Scans

<input type="checkbox"/> Name	Schedule	Last Modified
<input checked="" type="checkbox"/> My Basic Network Scan	On Demand	✓ 09:24 AM
<input type="checkbox"/> My Daily Scan	Daily at 01:00	✓ 09:28 AM
<input type="checkbox"/> My Host Discovery Scan	On Demand	⊘ 09:18 AM
<input type="checkbox"/> My New DNS Scan	On Demand	⊘ 09:24 AM
<input type="checkbox"/> My Scheduled Basic Scan	Once on September 1 at 09:30	🔄 09:33 AM
<input type="checkbox"/> My Windows Malware Scan	Monthly on day 1 at 23:00	⏸ 09:33 AM

Upload a Scan

Scans results can be exported and then imported using the **Upload** button. Valid file formats are **.(dot)-nessus** and **.db**. Uploaded scans are imported into the **Scan / My Scans** folder.

After a scan is imported, you can view its [Scan Results](#). By default, imported scans do not have the [Dashboard Enabled](#) feature turned on.

Tip: Scans results can be imported from other Nessus Manager scans, even from other Nessus installs.

Upload Scan Options

Option	Description
.nessus	<p>An XML-based format and the de-facto standard in Nessus 4.2 and later. This format uses an expanded set of XML tags to make extracting and parsing information more granular. This report does not allow chapter selection.</p> <p>If the policy is exported and saved to a .nessus file, the passwords are stripped.</p> <p>When importing a .nessus file format, you will need to re-apply your passwords to the credentials being used.</p>



Nessus DB	An encrypted database format used in Nessus 5.2 and later that contains all the information in a scan, including the audit trails and results. When exporting to this format, you are prompted for a password to encrypt the results of the scan.
-----------	---

Configure a Scan

The **Configure** option allows you to manage scan settings and schedules.

Disable a Scheduled Scan

If the scan that you have selected is configured with a schedule, the **More** menu allows you to disable the scan's schedule.

Copy a Scan

Based on permissions, you have the ability to **Copy** existing scans.

1. Select the scan to be copied.
2. From the **More** drop-down menu, select **Copy to**.
3. Copy the scan to an existing folder or select **New Folder** to create a new folder to store the copied scan.
4. Type a new **Scan Name** and choose whether or not to **Include scans history**.

Imported scans cannot be copied; they can be moved.

Move a Scan

Similar to copying a scan, the **Move to** option allows you to move a selected scan to a different folder, to the **Trash** folder, or allows you to create a **New Folder** to move the scan to.

Manage Agent Groups

On the **Scanners / Agents / Linked** page, you can create a new agent group.

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.


Once a new group has been created, you can:

- Add agents to the group.
- Manage its agents.
- Set permissions for the agent group.
- Rename the agent group.

During the installation of Nessus Agents, you had the option of adding your agent to an existing agent group.

If you did not have any agent groups created prior to the Nessus Agent's install, or you opted to not add your agent to an existing group, you can create agent groups in the Nessus UI.

Create an Agent Group

1. In Nessus, select the settings  button.
2. Select the link for **Scanners / Agents / Groups**.
3. Select the **New Group** button.
4. In the **Name** field, name your agent group.
5. Select **Save** to continue.

The new **Agent Group** page appears.

AVAILABLE AGENTS 4	Use All	MEMBER AGENTS 0
NENG-A1-Win7Ultx32	+	No member agents
NENG-A3-Win2k8R2Entx64	+	
NENG-A5-Win2k12x64	+	
NENG-NP-WIN7	+	

Add an Agent to a Group

1. Go to the **Scanners / Agents / Groups** page.
2. Select the name of the agent group to which you want to add Agents.
3. From the **Available Agents** list, select the + button.

The agent moves from the **Available Agents** column to the **Member Agents** column.

AGENT GROUP	Scanners / Agents / Groups / My Nessus Agent Group		
	Manage Agents	AVAILABLE AGENTS 2	Use All
	Permissions		MEMBER AGENTS 2
	Settings		Remove All
		NENG-A3-Win2k8R2Entx64	NENG-A1-Win7Ultx32
		NENG-A5-Win2k12x64	NENG-NP-WIN7

Add Permissions to an Agent Group

1. Go to the **Scanners / Agents / Groups** page.
2. Select the name of the agent group to which you want to add permissions.
3. Select the **Permissions** link.

Note: Only existing Nessus users or groups can be added to permissions for the agent group(s).

On this page, you have the following options:

-
- Set permissions for the **Default** Nessus group.
 - Add individual Nessus users and set specific permissions for that user.
 - Add Nessus **User Groups** and set specific permissions for that group.

Agent groups have two permission options: **Can Use** or **No Access**.

Change the Name of an Agent Group

1. Go to the **Scanners / Agents / Groups** page.
2. Select the name of the agent group .
3. Select the **Settings** link.
4. In the **Name** field, rename your group.
5. Select **Save**.

Policies

This section includes information and steps to perform common tasks associated with managing Nessus Policies.

- [Create a Policy](#)
- [Create a Limited Plugin Policy](#)
- [Manage Policies](#)

Tip: For more information about the **Policies** page, see the related [Features](#) section of this guide.

Create a Policy

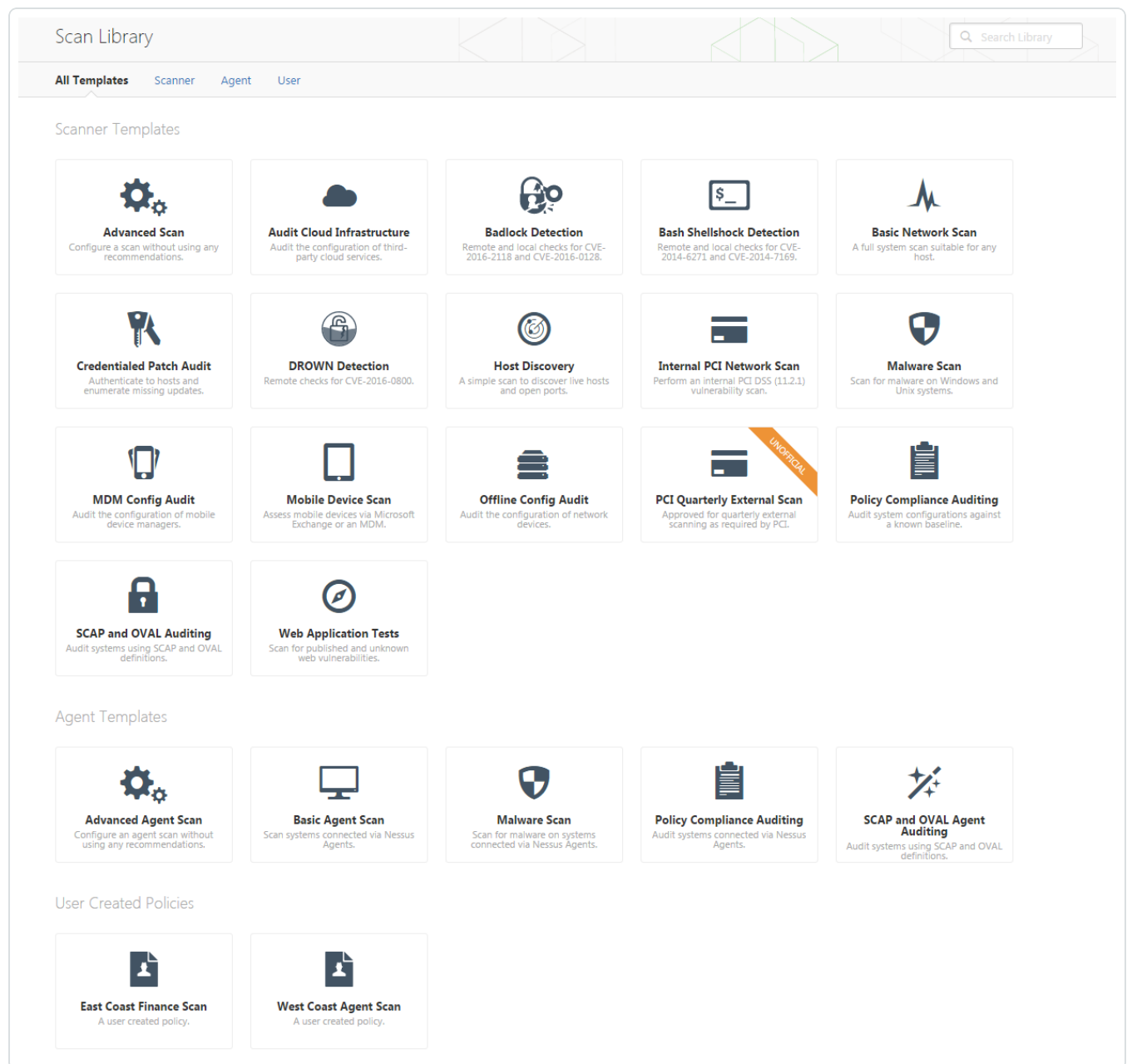
On the **Policies** page, you can create a **New Policy**, or manage your policies.

Tip: Creating a new Policy involves the same steps as creating a new Scan: Use the **New Policy** button, select a template, and configure your policy's settings.

Create a Basic Scan Policy

1. On the **Policies** page, select **New Policy**

The **Template Library** appears.



2. Select the **Basic Network Scan** template.
3. Configure the scan's **Settings** using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.
4. Select **Credentials**.
5. From the **Credentials** list, select applicable credentials required to perform the scan. Multiple credentials can be added and configured.

This policy is ready to be used when creating new **Basic Network Scans**.

Create an Advanced Scan Policy

1. On the **Policies** page, select **New Policy**.

The **Policy Library** appears.

2. Select the **Advanced Scan** template.
 3. Configure the scan's **Settings** using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.
 4. Select **Credentials**.
 5. From the **Credentials** list, select applicable credentials required to perform the scan. Multiple credentials can be added and configured.
 6. If applicable, select **Compliance**.
 7. From the **Compliance Checks** list, select compliance checks applicable to perform the scan. Multiple compliance checks can be added and configured.
 8. If applicable, select **Plugins**; enabled plugins are displayed.
- If Agents are linked to Nessus, you also can create Agent policies.

Create a Limited Plugin Policy

Steps

1. On the **Policies** page, select **New Policy**.

The **Policy Library** appears.

2. Select the **Advanced Scan** template.
3. Configure the scan's **Settings** using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.
4. Select **Credentials**.
5. From the **Credentials** list, select applicable credentials required to perform the scan. Multiple credentials can be added and configured.
6. If applicable, select **Compliance**.
7. From the **Compliance Checks** list, select compliance checks applicable to perform the scan. Multiple compliance checks can be added and configured.
8. Select **Plugins**.

By default, all plugins are **Enabled**.

New Policy / Advanced Scan

Policy Library > Settings Credentials Compliance **Plugins**

Show Enabled | Show All

Status	Plugin Family	Total
ENABLED	ADX Local Security Checks	11254
ENABLED	Amazon Linux Local Security Checks	712
ENABLED	Backdoors	108
ENABLED	CentOS Local Security Checks	2183
ENABLED	CGI abuses	3458
ENABLED	CGI abuses : XSS	626
ENABLED	CISCO	717

Save Cancel

Status	Plugin Name	Plugin ID
No plugin family selected.		

9. Select the **Disable All** button.

New Policy / Advanced Scan

Policy Library > Settings Credentials Compliance **Plugins**

Disable All Enable All Filter Plugin Families

Show Enabled | Show All

Status	Plugin Family	Total	Status	Plugin Name	Plugin ID
DISABLED	ADX Local Security Checks	11254	No plugin family selected.		
DISABLED	Amazon Linux Local Security Checks	712			
DISABLED	Backdoors	108			
DISABLED	CentOS Local Security Checks	2183			
DISABLED	CGI abuses	3458			
DISABLED	CGI abuses : XSS	626			
DISABLED	CISCO	717			

Save Cancel

10. In the plugins list, select the **Plugin Family** name you want to enable.

New Policy / Advanced Scan

Policy Library > Settings Credentials Compliance **Plugins**

Disable All Enable All Filter Plugin Families

Show Enabled | Show All

Status	Plugin Family	Total	Status	Plugin Name	Plugin ID
DISABLED	ADX Local Security Checks	11254	No plugin family selected.		
DISABLED	Amazon Linux Local Security Checks	712			
DISABLED	Backdoors	108			
DISABLED	CentOS Local Security Checks	2183			
DISABLED	CGI abuses	3458			
DISABLED	CGI abuses : XSS	626			
DISABLED	CISCO	717			

Save Cancel

After you select the **Plugin Family** name, all associated plugins appear as **Disabled** in the right column.

New Policy / Advanced Scan

Policy Library > Settings Credentials Compliance **Plugins**

Disable All Enable All Filter Plugin Families

Show Enabled | Show All

Status	Plugin Family	Total
DISABLED	ADX Local Security Checks	11254
DISABLED	Amazon Linux Local Security Checks	712
DISABLED	Backdoors	108
DISABLED	CentOS Local Security Checks	2183
DISABLED	CGI abuses	3458
DISABLED	CGI abuses : XSS	626
DISABLED	CISCO	717

Save Cancel

Status	Plugin Name	Plugin ID
DISABLED	Amazon Linux AMI : 389-ds-base (ALAS-2013-184)	69743
DISABLED	Amazon Linux AMI : 389-ds-base (ALAS-2013-223)	70227
DISABLED	Amazon Linux AMI : 389-ds-base (ALAS-2013-255)	71395
DISABLED	Amazon Linux AMI : 389-ds-base (ALAS-2014-311)	73230
DISABLED	Amazon Linux AMI : 389-ds-base (ALAS-2014-396)	78339
DISABLED	Amazon Linux AMI : 389-ds-base (ALAS-2015-501)	82508
DISABLED	Amazon Linux AMI : 389-ds-base (ALAS-2015-538)	83977

11. Next, from the right column, select the **Disabled** button next to each **Plugin Name** that you wish to include in your policy.
- In the right column, each plugin switches from **Disabled** to **Enabled** and the **Plugin Family** in the left column now shows **Mixed**.
- To commit your changes, select the **Save** button.

New Policy / Advanced Scan

Policy Library > Settings Credentials Compliance **Plugins**

Disable All Enable All Filter Plugin Families

Show Enabled | Show All

Status	Plugin Family	Total
DISABLED	ADX Local Security Checks	11254
MIXED	Amazon Linux Local Security Checks	712
DISABLED	Backdoors	108
DISABLED	CentOS Local Security Checks	2183
DISABLED	CGI abuses	3458
DISABLED	CGI abuses : XSS	626
DISABLED	CISCO	717

Save Cancel

Status	Plugin Name	Plugin ID
DISABLED	Amazon Linux AMI : 389-ds-base (ALAS-2013-184)	69743
DISABLED	Amazon Linux AMI : 389-ds-base (ALAS-2013-223)	70227
DISABLED	Amazon Linux AMI : 389-ds-base (ALAS-2013-255)	71395
ENABLED	Amazon Linux AMI : 389-ds-base (ALAS-2014-311)	73230
ENABLED	Amazon Linux AMI : 389-ds-base (ALAS-2014-396)	78339
ENABLED	Amazon Linux AMI : 389-ds-base (ALAS-2015-501)	82508
ENABLED	Amazon Linux AMI : 389-ds-base (ALAS-2015-538)	83977

12. Optional: Use the top menu, select the **Filter Plugin Families** search box to search for, find, and apply specific plugins.
- When finished, select the **Apply** button.
- From the results list, select the **Enable** button and then select the **Save** button.

New Policy / Advanced Scan

Policy Library > Settings Credentials Compliance Plugins

Disable AllEnable AllFilter Plugin Families

MatchAllof the following:

Bugtraq IDis equal toNUMBER

ApplyCancelClear Filters

Status	Plugin Family	Total
DISABLED	AIX Local Security Checks	11254
DISABLED	Amazon Linux Local Security Checks	712
DISABLED	Backdoors	108
DISABLED	CentOS Local Security Checks	2183
DISABLED	CGI abuses	3458
DISABLED	CGI abuses : XSS	626
DISABLED	CISCO	717

StatusPlugin Name

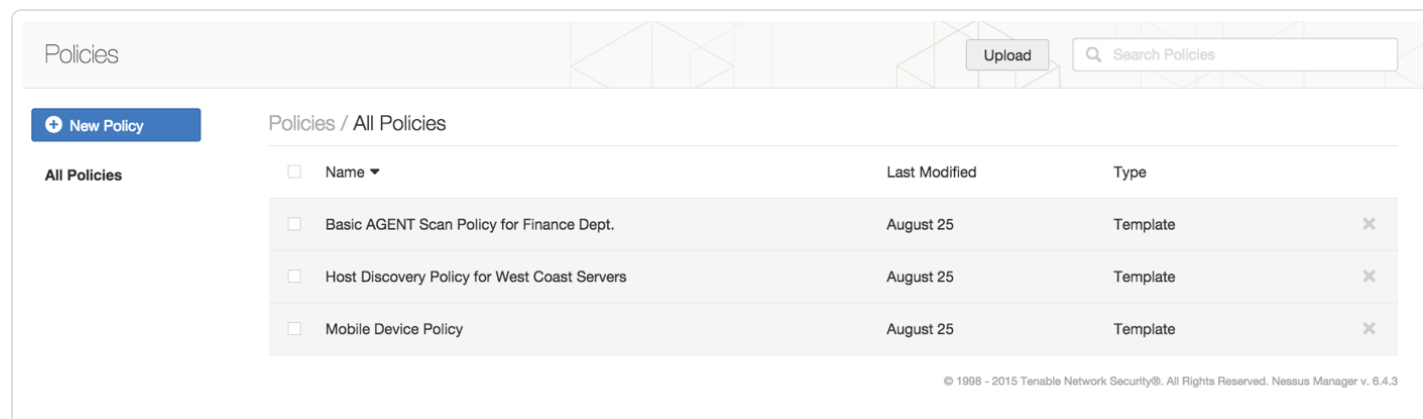
No plugin family

SaveCancel

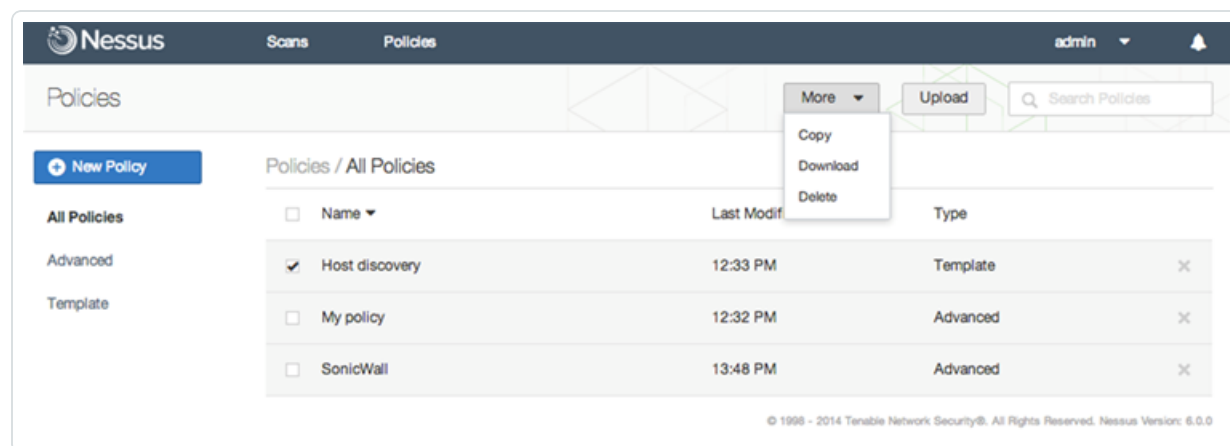
13. Optional: Add more plugins to your custom policy, clicking the **Save** button after enabling plu-
gins.

Manage Policies

The **Policies** page display your existing policies.



When you select a policy from the list of existing policies (placing a check in the box besides its name), the **More** button will appear.



Upload a Policy

The **Upload** button allows you to upload a previous policy. Using the native file browser box, select the policy from your local system and select **Open**.

Download a Policy

Select **Download** to open the browser's download dialog box. From here, you can open the policy in an external program (e.g., text editor) or save the policy to the directory of your choice. Depending on the browser, the policy may be downloaded automatically.



Note: Passwords and .audit files contained in a policy will not be exported.

Copy a Policy

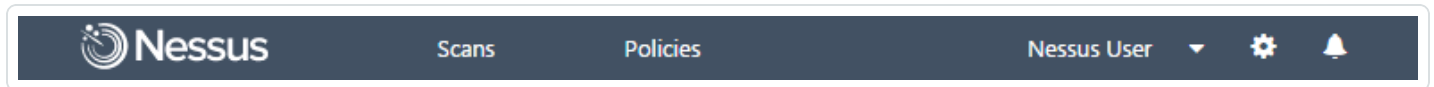
To copy a policy, select the policy, select **More**, and select **Copy**.

Delete a Policy

To delete a policy, select the policy, select **X** or **More**, and select **Delete**.

User Profile

To access the **User Profile** page, on the top navigation menu, select the drop down arrow next to your user name, and select **User Profile**.



Your **User Profile** includes the following pages:

- [Account Settings](#)
- [API Keys](#)
- [Change Password](#)
- [Plugin Rules](#)

Tip: For more information about the **User Profile** page, see the related [Features](#) section of this guide.

Account Settings

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

Note: Once created, a username cannot be changed.

User Profile

◀ Back

Account Settings

Change Password

Plugin Rules

API Keys

User Profile / Account Settings

Username

Sylvia

Full Name

Email

User Type

System Administrator

Save

Cancel

Based on your Nessus product, the following information appears.

Version	Settings
Tenable.io	Username (e-mail address of the user) Full Name Email User Type
Nessus Manager	Username Full Name Email User Type
Nessus Pro-	User Name

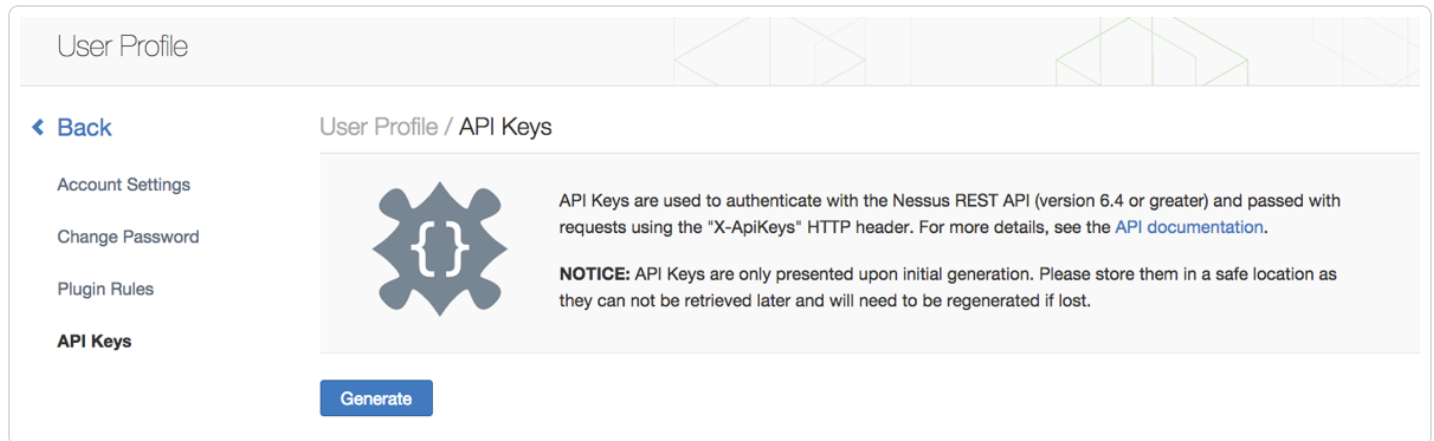


Professional	<div>User Type</div> <div>Note: Nessus Professional user accounts do not have an associated email address. Nessus Professional has only two user types: System Administrator and Standard.</div>
--------------	---

API Keys

API Keys (an Access Key and a Secret Key) are used to authenticate with the **Nessus REST API** (version 6.4 or greater) and passed with requests using the "X-ApiKeys" HTTP header.

The **User Profile / API Keys** page allows you to generate API keys.




Select the **Generate** button to create an **Access Key** and a **Secret Key**.

Note:

- API Keys are only presented upon initial generation. Please store API Keys in a safe location, as they cannot be retrieved later.
- API Keys cannot be retrieved by Nessus. If lost, the API Keys must be regenerated.
- Regenerating the API Keys immediately unauthorizes any applications currently utilizing the key.

Change Password

The **Change Password** section allows you to change your password. Users with administrative privileges can change other user passwords.

To change another user's password, log in to Nessus as a user with administrative privileges, select the  button, and navigate to the **Users** section of the **Accounts** page.

Plugin Rules

Create a new Plugin Rule

1. On the **User Profile/ Plugin Rules** page, select the **New Rule** button.
2. Enter values for the Host, Plugin ID, Expiration Date (Optional), and the Severity that you would like the plugin to adopt.
3. Select the **Save** button.

New Plugin Rule Example

Host: 192.168.0.6

Plugin ID: 9877

Expiration Date: 12/31/2016

Severity: Critical

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.

Update a Plugin Rule

1. On the **User Profile/ Plugin Rules** page, select the Plugin Rule(s) that you want to update.
2. On the **Edit Rule** page, update the **Host, Plugin ID, Expiration Date, or Severity** values.
3. Select the **Save** button.

Delete a Plugin Rule

1. On the **User Profile/ Plugin Rules** page, select the check box(es) for the Plugin Rule(s) that you want to delete.
2. Select the **Delete** button.
3. On the **Delete Rule** confirmation screen, select **Delete**.


Manage the Settings Page

This section contains the following tasks available on the **Settings** page.

- [System Settings](#)
- [Manage Scanners](#)
- [Manage Accounts](#)
- [Manage Communications](#)
- [Manage Advanced Settings](#)

Tip: For more information about the **Settings** page, see the related [Features](#) section of this guide.

System Settings

From the Nessus home page, the  button links you to the Nessus system **Settings**: [Scanners](#), [Accounts](#), [Communication](#), and [Advanced](#).

If **Remote** scanners are linked to this Nessus Manager, a list of their scans are listed.

Settings

ScannersAccountsCommunicationAdvanced

LOCAL

OverviewPermissionsSoftware Update

REMOTE

Linked

AGENTS

Linked

Groups

Scanners / Local / Overview

Nessus Manager

Version6.7.0

Licensed Hosts256

Licensed Scanners0 of 10

Licensed Agents1 of 10

Plugins

Last UpdatedMay 16, 2016

ExpirationJune 13, 2016

Plugin Set201605162130

Activation Code

Scans

Advanced Compliance Scan

Finance Department Basic Network Scan

Start Time

May 15

May 15

Last Modified

07:05 AM

07:05 AM

Owner

remote

remote

Status

Paused

Paused

Scanners / Local / Software Update

On the **Scanners / Local / Software** page, you can configure how and when you want to install Nessus updates.

There are two parts of a Nessus update: Component Updates and Plugin Updates.

When an update becomes available, you can opt to use the **Manual Software Update** or opt to use **Automatic Updates**.

To view the [Software Update page](#), select the  button.

- [Update Nessus Version](#)
- [Update Plugins](#)
- [Update Activation Code](#)

Nessus UI Software Update Page

Actions related to Nessus components and the latest plugins for Nessus are performed by using the **Software Update** page or via the [Update Nessus Software](#).

To access the **Software Update** page, use the  button.

Manual Software Update

At the top of the **Software Update** page, you can opt to use the **Manual Software Update** button.

When you select this method of software update, Nessus performs a one-time update.

Manual Software Update Options

- Update all components
- Update plugins (only)

Note: If you select the **Update plugins** option, the scanner receives plugin updates, but does not receive feature or operational updates for the Nessus UI or the Nessus engine. Selecting this option prevents new features and functionality from being displayed and or and becoming operational.

- Upload your own plugin archive

A plugin archive is a compressed TAR file that is created and downloaded when you [Register Nessus Offline](#) and [Download and Copy Plugins](#). For more information, see [Install Plugins Manually](#).


Tip: **Manual Software Update** can be used in conjunction with **Automatic Updates**.

Automatic Updates

- Update all components
- Update plugins
- Disabled

Update Frequency

-
- Daily
 - Weekly
 - Monthly

Select the  button next to **Update Frequency** interval to customize the update frequency by any number of hours.


Plugin Feed

You can opt to provide a specific **Plugin Feed** host. For example, if plugins must be updated from a site residing in the U.S., you can specify “plugins-us.nessus.org”.

Note: If you are using Nessus offline, see the [Register Nessus Offline](#) section.

Update Nessus Version


Steps

1. On the **Scanners / Local / Overview** page next to the **Version** number, select the  button.
2. On the **Software Update** screen, the following warning message appears:

Updating this scanner requires a restart and will abort all running scans. Are you sure you want to continue?
3. Select **Continue**.

Once the download process is complete, Nessus restarts, and then prompts you to log in again.

Update Plugins

1. On the **Scanners / Local / Overview** page next to the **Last Updated** date, select the  button.
2. Select **Continue** to proceed.

Nessus updates with the latest Nessus plugins.

Update Activation Code



In the event that you receive a new license corresponding Activation Code, your activation code must be re-registered with Nessus.

You can update Nessus with the new activation code using either of the following methods:

- Update the Nessus Activation Code in the UI.
- Update the Nessus Activation Code via Command Line.

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

Update Nessus in the UI

1. In Nessus, select the  button ([System Settings](#) page).
2. Select the  button next to the Activation Code.
3. On the **Update Activation** screen, select your **Registration** type.
4. Enter the new Activation Code.
5. Select **Save**.

Next, Nessus downloads and installs the Nessus engine and the latest Nessus plugins.

Once the download process is complete, Nessus restarts, and then prompts you to log in again.

Nessus updates with the new licensing information.

Update Nessus via Command Line

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

Platform	Command
Linux	# /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx
FreeBSD	# /usr/local/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx



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

Next, Nessus downloads and installs the Nessus engine and the latest Nessus plugins.

Once the download process is complete, Nessus restarts, and then prompts you to log in again.

Nessus updates with the new licensing information.

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 [Register Nessus Offline](#).

Operating System	Command
Linux	# /opt/nessus/sbin/nessuscli <arg1> <arg2>
Mac OSX	# /Library/Nessus/run/sbin/nessuscli <arg1> <arg2>
Windows	C:\Program Files\Tenable\Nessus or C:\ProgramData\Tenable\Nessus
Commands must <i>Run as administrator</i>	
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.

Manage Scanners

The **Settings / Scanners** page allows you to view and manage your **Local** scanner, your [Remote](#) scanners, and your [Agents](#).

Nessus Professional, Nessus Manager, and Nessus Agents feature slightly different Scanner settings:

- [Nessus Professional](#)
- [Nessus Manager](#)
- [Nessus Agents](#)

Nessus Professional

The settings landing page displays the Overview for your local Nessus Scanner and its Nessus plugins:

- Your Nessus product name and version
- Your plugin last update
- Your plugin expiration date
- The plugin set identifier
- Your Nessus Activation Code

From the Overview Page, you can:

- [Update Nessus Version](#)
- [Update Plugins](#)
- [Update Activation Code](#)


If you are working with Nessus offline, see [Register Nessus Offline](#)

Link Scanner to Nessus Manager or Tenable.io

The **Local / Link** page is a **Nessus Professional** only feature. This page allows you to link your Nessus Professional Scanner to Nessus Manager or to Tenable.io.

1. On the **Local / Link** page, use the toggle to create a linked scanner.


Scanners / Local / Link



Enabling this option allows the local scanner to be linked to 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.

☐

Scanners / Local / Link



Enabling this option allows the local scanner to be linked to 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.

☒

Scanner Name

Manager Host

Manager Port

Linking Key

Use Proxy

☐

Save

Cancel

2. Create a unique **Scanner Name**.
3. Enter the **Manager Host**, **Manager Port**, and **Linking Key** obtained from Nessus Manager or Tenable.io.

Option	Description
Scanner Name	Unique Scanner Name. This name will appear in Nessus Manager or Tenable.io's linked scanners.
Manager Host	The hostname or IP address of Nessus Manager. If connecting to Tenable.io, use cloud.tenable.com as the Manager Host.
Manager Port	The port number to connect to Nessus Manager (8834). If connecting to Tenable.io, use port 443.
Linking Key	The Nessus Manager or Tenable.io Linking Key . <div> <p>Tip: In Nessus Manager, the Linking Key is displayed on the Scanners / Remote / Linked page.</p> <p>In Tenable.io, the Linking Key is displayed on the Scanners > Linked Scanners page.</p> </div>

Option	Description
Use Proxy	OPTIONAL: If communication must be directed through a proxy, select this option. Once selected, the scanner uses the Proxy Server information provided on the Communication / Network / Proxy Server page.

Nessus Manager

In Nessus Manager, the **Scanners** pages include:

- [Scanners / Local / Overview](#)
- [Scanners / Local / Permissions](#)
- [Scanners / Local / Software Update](#)
- [Scanners / Remote / Linked](#)
- [Scanners / Agents / Linked](#)

Scanners / Local / Overview (Manager)

Nessus Manager Overview page displays the **Overview** for your **Local** Nessus Scanner and its Nessus plugins:

- Your Nessus product name and version.
- Your number of licensed hosts.
- Your number of licensed scanners.
- Your number of licensed agents.
- Your plugin last update.
- Your plugin expiration date.
- The plugin set identifier.
- Your Nessus Activation Code.

From the Overview Page, you can:

- [Update Nessus Version](#)
- [Update Plugins](#)
- [Update Activation Code](#)

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

Scanners / Local / Permissions


In **Nessus Manager**, you can control the permissions of the local scanner by adding users or group, or by setting the default group's settings.

- **No Access:** Any users or groups specified cannot view, cannot use, or cannot manage the Scanners.
- **Can Use:** Users or groups specified here can view and use the scanner; they are not able to make any changes.
- **Can Manage:** Users or groups specified here can make changes to the Scanner's settings.


Scanners / Remote / Linked





Remote scanners can be linked to this Nessus Manager by using the Linking Key displayed. Once linked, Remote scanners can be selected when configuring scans.


Scanners / Remote / Linked



Remote scanners can be linked to this manager using the provided key. Once linked, they can be managed locally and selected when configuring scans.

Linking Key: [Redacted] 

Name ▼	Status	Scans	Owner		
<input type="checkbox"/> My_Remote_Scanner_1	● Offline	0	R system		
<input type="checkbox"/> My_Remote_Scanner_2	● Offline	0	R system		

Tip: You can regenerate the Linking Key by clicking the  button to the right of the key. Regenerating the key does not disable any secondary scanners that are already registered.

From the scanners list, you can use the **Disable / Enable** button or the **Remove** button to connect, disconnect, or remove your linked scanner(s).

To manage your remote linked scanner's settings, open the remote scanner from the scanner's list.

The **Overview** page displays details for your **Remote / Linked** scanner.


On the **Permissions** page, you can configure the permissions of the users or groups who **Can use**, **Can manage**, or have **No access** this remote scanner.

Scanners / Agents / Linked


After you have performed a [Nessus Agent Install](#), you can view and manage your Nessus Agents in the Nessus UI.

In Nessus Manager, select the  button.

Scanners / Agents / Linked



Agents can be linked to this manager using the provided key with the following [setup instructions](#). Once linked, they must be added to a [group](#) for use when configuring scans. Also, linked agents will automatically download plugins from the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.

Linking Key: 0c80f7839725f252a87f281f1f8f16140d4d06796393814a3495ca91c6d02577 

<input type="checkbox"/>	Name ▼	Status	IP Address	Platform	Groups	Version	Last Plugin Update	Last Scanned	
<input type="checkbox"/>	centos5-agent-6...	● Online	192.168.1.1	Linux (es5-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos6-agent-6...	● Online	192.168.1.2	Linux (es6-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos6-agent-6...	● Online	192.168.1.3	Linux (es6-x86-64)	All	6.8.1	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos7-agent-6...	● Online	192.168.1.4	Linux (es7-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos7-agent-6...	● Online	192.168.1.5	Linux (es7-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos7-agent3-...	● Online	192.168.1.6	Linux (es7-x86-64)	All	6.7.0	06:15 AM	11:14 AM	×
<input type="checkbox"/>	debian7-agent-6...	● Online	192.168.1.7	Linux (debian6-x...	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	debian7-agent-6...	● Online	192.168.1.8	Linux (debian6-x...	All	6.9.1	06:15 AM	11:14 AM	×
<input type="checkbox"/>	ubuntu14-agent-...	● Online	192.168.1.9	Linux (ubuntu11...	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	ubuntu14-agent-...	● Online	192.168.1.10	Linux (ubuntu11...	All	6.9.2	06:15 AM	11:14 AM	×

Delete Agents

On the **Scanners / Agents / Linked** page, you can delete agents.

To delete multiple agents at once, select the check boxes that correspond to the agents you want to delete, and then select the **Remove** button at the top of the page.

Scanners / Agents / Groups

Once linked to Nessus Manager, Nessus Agents can be managed by adding or removing them from **Nessus Agent Groups**.

On the **Scanners / Agents / Linked** page, you can create a new agent group.

Once a new group has been created, you can:


- Manage its Agents
- Set Permissions for the Agent Group
- Rename the Agent Group

During the installation of Nessus Agents, you had the option of adding your agent to an existing Agent Group.

If you did not have any Agent Groups created prior to the Nessus Agent's install, or you opted to not add your agent to an existing group, you can create **Agent Groups** in the Nessus UI.

Scanners / Agents / Groups

New Group



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. From this view, you can manage your agent groups.

☐ Name ▼

☐ Targets ×

☐ Windows Agents ×

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.

Steps

Create an Agent Group

1. In Nessus, select the  button.

2. Select **Scanners / Agents / Groups**.
3. Select the **New Group** button.
4. In the **Name** field, name your Agent Group.
5. Select **Save** to continue.

Your new **Agent Group** page appears.

Scanners / Agents / Groups / My Nessus Agent Group		
AVAILABLE AGENTS 4	Use All	MEMBER AGENTS 0
NENG-A1-Win7Ultx32	+	No member agents
NENG-A3-Win2k8R2Entx64	+	
NENG-A5-Win2k12x64	+	
NENG-NP-WIN7	+	

Once created, you can manage agent groups from the **Scanners / Agents / Groups** page.

To access agent group settings, select the agent group from the list.

Add an Agent to a Group

1. Go to the **Scanners / Agents / Groups** page.
2. Select the name of the **Agent Group** to which you want to add agents.
3. From the **Available Agents** list, select the + button.

The agent moves from the **Available Agents** column to the **Member Agents** column.

AGENT GROUP Manage Agents Permissions Settings	Scanners / Agents / Groups / My Nessus Agent Group		
	AVAILABLE AGENTS 2	Use All	MEMBER AGENTS 2 Remove All
	NENG-A3-Win2k8R2Entx64	+	NENG-A1-Win7Ultx32 ✕
	NENG-A5-Win2k12x64	+	NENG-NP-WIN7 ✕

Add Permissions to an Agent Group

-
1. Go to the **Scanners / Agents / Groups** page.
 2. Select the name of the **Agent Group** to which you want to add permissions.
 3. Select the **Permissions** link.

Note: Only existing Nessus users or groups can be added to the permissions for the Agent Group(s).

On this page, you have the following options:

- Set permissions for the **Default** Nessus group.
- Add individual Nessus users and set specific permissions for that user.
- Add Nessus **User Groups** and set specific permissions for that group.

Agent Groups have two permission options: **Can Use** or **No Access**.

Change the name of the Agent Group


1. Go to the **Scanners / Agents / Groups** page.
2. Select the **Agent Group** name that you want to change.
3. Select **Settings**.
4. In the **Name** field, rename your group.
5. Select **Save**.

Manage Nessus Agents


Once installed, **Nessus Agents** are viewed and managed in the Nessus Manager or Tenable.io interface.

Note: Before an Agent can be used in a scan, the Agent must be added to at least one agent group. For more information, see [Manage Agent Groups](#) and [Create an Agent Scan](#).


View your Linked Agents

1. In Nessus, select the  button.
2. From the **Scanners** overview page, select **Agents > Linked**.

Scanners / Agents / Linked





Agents can be linked to this manager using the provided key with the following [setup instructions](#). Once linked, they must be added to a [group](#) for use when configuring scans. Also, linked agents will automatically download plugins from the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.

Linking Key: 0c80f7839725f252a87f281f1f8f16140d4d06796393814a3495ca91c6d02577 

<input type="checkbox"/>	Name ▼	Status	IP Address	Platform	Groups	Version	Last Plugin Update	Last Scanned	
<input type="checkbox"/>	centos5-agent-6...	● Online	192.168.1.10	Linux (es5-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos6-agent-6...	● Online	192.168.1.11	Linux (es6-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos6-agent-6...	● Online	192.168.1.12	Linux (es6-x86-64)	All	6.8.1	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos7-agent-6...	● Online	192.168.1.13	Linux (es7-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos7-agent-6...	● Online	192.168.1.14	Linux (es7-x86-64)	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	centos7-agent3-...	● Online	192.168.1.15	Linux (es7-x86-64)	All	6.7.0	06:15 AM	11:14 AM	×
<input type="checkbox"/>	debian7-agent-6...	● Online	192.168.1.16	Linux (debian6-x...	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	debian7-agent-6...	● Online	192.168.1.17	Linux (debian6-x...	All	6.9.1	06:15 AM	11:14 AM	×
<input type="checkbox"/>	ubuntu14-agent-...	● Online	192.168.1.18	Linux (ubuntu11...	All	6.10.4	06:15 AM	11:14 AM	×
<input type="checkbox"/>	ubuntu14-agent-...	● Online	192.168.1.19	Linux (ubuntu11...	All	6.9.2	06:15 AM	11:14 AM	×

Create a Blackout Window

-
- 
1. In Nessus, select the  button.
 2. From the **Scanners** overview page, select **Agents > Blackout Windows**.
 3. In the upper right corner, click **New Blackout Window**.
 4. Adjust the settings as necessary, and click **Save**.

Remove a Linked Agent

To remove a linked Agent, you can select the **x** or you can use the check-boxes to select and remove multiple linked Agents.

Once linked to Nessus, Nessus Agents can be managed by adding or removing them in Nessus Agent Groups.

Update the custom_CA.inc File

Before You Begin

These steps describe how to update the custom_CA.inc file with your custom CAs (Certificate Authority) in Nessus.

Steps

1. In Nessus, in the upper right corner, click the  button.


The **Settings** page appears.

2. In the **Scanners** section of the **Settings** page, in the **Global** section, click **Custom CA**.
3. In the **Certificate** box, paste the contents of the custom_CA.inc file.
4. Click **Save**.

The custom_CA.inc file is updated.

Manage Accounts

You can create and manage **Users** and **Groups** on the **Accounts** page.

1. On the Nessus home page, select the  button.
2. Select **Accounts**.

The following table describes settings and options in Nessus Manager, Tenable.io, and Nessus Professional.

Setting Name	Description	Product Version(s)	User Type(s)
Users	Users are individual Nessus accounts to be used for assigning permissions.	Tenable.io Nessus Manager Nessus Professional	All User Types
Groups	Group are collections of users created for shared permissions.	Tenable.io Nessus Manager	System Administrator


Nessus Manager also has the ability to manage users using a configured LDAP Server.

Tenable.io: You must define the username as the registered email address within the **Tenable.io** service.

Note: Once an account is created, the account **Username** cannot be changed. If you need to change an account's username, you must create a New User account with a new username.

Steps

Create a User Account


1. From the Nessus home page, select the  button.
2. Select **Accounts**.



3. Select the **New User** button.
4. Enter a **Username**.
5. Enter the user's **Full Name**.
6. Enter the user's **Email** address.
7. Create a user **Password**.
8. Retype the user's **Password**.
9. Select a **User Role**.
10. Select **Save**.

User Role	Description
Basic	Basic user roles can only read scan results. <div>Note: This role is not available in Nessus Professional.</div>
Standard	Standard user roles can create scans, create policies, create schedules, and create reports. They cannot modify any user accounts, user groups, scanners, or system configuration settings.
Administrator	Administrator user roles have the same privileges as the Standard role, but can also manage users, manage user groups, and manage scanners. <div>Note: This role is not available in Nessus Professional.</div>
System Administrator	System Administrator user roles have the same privileges as the Administrator role and can manage and modify system configuration settings.

Create Groups

1. From the Nessus home page, select the  button.
2. Select **Accounts**.
3. Select **Groups**.
4. Select the **New Group** button.

-
- 
5. Enter a **Name** for the **Group**.

The next page allows you to **Add Users** to the group you created.

Add Users to the Group

1. Select the **Add User** button.
2. Use the drop-down menu to select a user to be added to the group.
3. If necessary, add additional users to the group.
4. When done, select the **Save** button.

Tip: Once you create users and groups, you can manage them on the **Accounts / Users** or **Accounts / Groups** pages.

Manage Communications

The **Settings / Communications** page allows you to configure Nessus to communicate with network servers and connector services.

Note: Nessus Professional includes only the **Proxy Server** and **SMTP Server** communication options.

- [LDAP Server](#)
- [SMTP Server](#)
- [Proxy Server](#)
- [CleanCisco ISE](#)

The screenshot shows the Nessus web interface. The top navigation bar includes the Nessus logo, 'Scans', 'Policies', a user profile 'Sylvia', and settings/notification icons. The 'Settings' page is active, with sub-tabs for 'Scanners', 'Accounts', 'Communication', and 'Advanced'. The 'Communication' tab is selected, showing a left sidebar with 'NETWORK' (LDAP Server, Proxy Server, SMTP Server) and 'CONNECTORS' (Cisco ISE). The main content area is titled 'Communication / Network / LDAP Server' and features an LDAP icon and a descriptive paragraph. Below this, the 'General Settings' section contains input fields for 'Host', 'Port', 'Username', 'Password', and 'Base DN' (pre-filled with 'cn=users,dc=example,dc=com'), along with a 'Test Authentication' button. The 'Advanced Settings' section has a 'Show advanced settings' checkbox. At the bottom are 'Save' and 'Cancel' buttons.

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, Nessus administrators can add users straight from their directory and these users can authenticate using their directory credentials.

General Settings

Host

Port

Username

Password

Base DN

Advanced Settings

Show advanced settings ☐

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, Nessus administrators can add users straight from their directory and these users can authenticate using their directory credentials.

Nessus auto-negotiates encryption, therefore there are no encryption options in the Nessus interface.

Allowable Characters

- Upper and lower case alphabetical characters (A – Z and a-z)
- Numerical characters (0 – 9)
- Period (.)
- Underscore (_)
- Dash (-)
- Plus (+)
- Ampersand (&)


If Nessus encounters characters or symbols other than specified, a 400 error will occur.

General Settings

- Host
- Port
- Username
- Password
- Base DN

Advanced Settings

- Username Attribute
- Email Attribute

-
- 
- Name Attribute
 - CA (PEM Format)

SMTP Server

Simple Mail Transfer Protocol (SMTP) is an industry standard for sending and receiving email. Once configured for SMTP, Nessus emails scan results 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.

General Settings

- Host
- Port
- From (sender email)
- Encryption
- Hostname (for email links)
- Auth Method

Proxy Server

Proxy servers are used to forward HTTP requests. If your organization requires one, Nessus uses these settings to perform plugin updates and communicate with remote scanners.

General Settings

- Host (required)
- Port (required)
- Username (optional)
- Password (optional)
- Auth Method
 - Auto Detect (Default)
 - None
 - Basic
 - Digest
 - NTLM
- User-Agent (optional)

If the proxy you are using filters specific HTTP user agents, a custom user-agent string can be supplied.

CleanCisco ISE

Cisco Identity Services Engine (ISE) is a security policy management and control platform that simplifies access control and security compliance for wired, wireless, and VPN connectivity.

Cisco ISE is primarily used to provide secure access, support BYOD initiatives, and enforce usage policies. Nessus only supports Cisco ISE version 1.2 or greater.

General Settings

- Host (required)
- Port (required)
- Username (required)
- Password (required)

Permissions

- Add users or groups

You may add Nessus users and Nessus groups to the Cisco ISE connector and set permissions as **No Access**, **Can view**, or **Can quarantine**. By default, permissions are set at **No Access**.

Manage Advanced Settings

Nessus Manager and **Nessus Professional** features **Advanced Settings**. These customizable settings provide granular control of Nessus operations.

Caution: Advanced Settings are helpful in specific situations, but changing settings is not required for routine use. Modifying Advanced Settings may involve risk, so please use them with caution. If you are unsure about modifying any setting, please contact Tenable Network Security Support support@tenable.com.

- Advanced Settings are global settings.
- To configure **Advanced Settings**, you must use a Nessus **System Administrator** user account.
- When modified, changes go into effect a few minutes after the setting is saved.
- `global.max_hosts`, `max_hosts`, and `max_checks` settings can have a particularly great impact on Nessus' ability to perform scans.
- Custom policy settings supersede the global Advanced Settings.

Note: When an Advanced Setting is added or an existing setting is modified, you are prompted to either **Discard** or **Save** the setting.

Modify Advanced Value

1. From the **Advanced Settings** page, select the name of the value.
2. Type a new **Value**
3. Select **Save**.

Tip: Changes go into effect a few minutes after the setting is saved.

Additional Resources

This section contains the following resources:

- [Run Nessus as Non-Privileged User](#)
- [Manage Nessus License and Registration](#)
- [Manage Activation Code](#)
- [Command Line Operations](#)
- [Custom SSL Certificates](#)
- [Enable SSH Local Security Checks](#)
- [Nessus Credentialed Checks](#)
- [Unofficial PCI ASV Validation Scan](#)
- [Scan Targets](#)
- [Offline Update Page Details](#)
- [More Nessus Resources](#)

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 hit the **Enter** key.



The following topics are included in this section:

- [Start or Stop Nessus](#)
- [Nessus-Service](#)
- [Nessuscli](#)
- [Nessuscli Agent](#)
- [Update Nessus Software](#)

Start or Stop Nessus

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

Mac OS X

1. Navigate to **System Preferences**.
2. Select the  button.
3. Select the  button.
4. Enter your username and password.
5. To stop the Nessus service, select the **Stop Nessus** button.

-or-

To start the Nessus service, select the **Start Nessus** button.

Start or Stop	Mac OS X Command Line Operation
Start	<code># launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist</code>
Stop	<code># launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist</code>

Windows

1. Navigate to **Services**.
2. In the **Name** column, select **Tenable Nessus**.
3. To stop the **Nessus** service, right-click **Tenable Nessus**, and then select **Stop**.

-or-

To restart the Nessus service, right-click **Tenable Nessus**, and then select **Start**.



Start or Stop	Windows Command Line Operation
Start	<code>C:\Windows\system32>net start "Tenable Nessus"</code>
Stop	<code>C:\Windows\system32>net stop "Tenable Nessus"</code>

Linux

Start or Stop	Linux Command Line Operation
RedHat, CentOS, and Oracle Linux	
Start	<code># /sbin/service nessusd start</code>
Stop	<code># /sbin/service nessusd stop</code>
SUSE	
Start	<code># /etc/rc.d/nessusd start</code>
Stop	<code># /etc/rc.d/nessusd stop</code>
FreeBSD	
Start	<code># service nessusd start</code>
Stop	<code># service nessusd stop</code>
Debian, Kali, and Ubuntu	
Start	<code># /etc/init.d/nessusd start</code>
Stop	<code># /etc/init.d/nessusd 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	# /opt/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]
FreeBSD	# /usr/local/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]
Mac OS X	# /Library/Nessus/run/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]

Suppress Command Output Examples

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

Linux

```
# /opt/nessus/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 multi-homed machine with multiple public IP addresses that you would like to use instead of the default one. For this setup to work, the host running nessusd must have multiple NICs with 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 timestamp 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 Network Security 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 Network Security to help diagnose issues. By default, the script runs in interactive mode.	
nessuscli bug-report-gen-	Generates an archive of system diagnostics.



Command	Description
erator	Running this command without arguments prompts for values. --quiet: run the bug report generator without prompting user for feedback. --scrub: when in quiet mode, bug report generator sanitizes the last two octets of the IPv4 address. --full: when in quiet mode, bug report generator collects extra data.
User Commands	
nessuscli rmuser [user-name]	Allows you to remove a Nessus user.
nessuscli chpasswd [user-name]	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 [user-name]	Allows you to add a Nessus user account. 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.
nessuscli lsuser	Displays a list of Nessus users.
Fetch Commands	
Manage Nessus registration and fetch updates	
nessuscli fetch --register <Activation Code>	Uses your Activation Code to register Nessus online. Example # /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx
nessuscli fetch --register-offline nessus.license	Registers Nessus 6.3 and newer with the nessus.license file obtained from https://plugins.nessus.org/v2/offline.php . 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.



Command	Description
<code>nessuscli fetch --check</code>	Displays whether Nessus is properly registered and is able to receive updates.
<code>nessuscli fetch --code-in-use</code>	Displays the Nessus Activation Code being used by Nessus.
<code>nessuscli fetch --challenge</code>	Displays the Challenge code needed to use when performing an off-line registration. Example Challenge Code: aaaaaa11b2222c-c33d44e5f6666a777b8cc99999
<code>nessuscli fetch --security-center</code>	Prepares Nessus to be connected to Security Center.
Fix Commands	
<code>nessuscli fix</code>	Reset registration, display network interfaces, and manage advanced settings.
<code>nessuscli fix [--secure] --list</code>	Using the --secure option acts on the encrypted preferences, which contain information about registration. --list, --set, --get, and --delete can be used to modify or view preferences.
<code>nessuscli fix [--secure] --set <name=value></code>	
<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>	This command deletes all your registration information and preferences, causing Nessus to run in a non-registered state. Before running <code>nessuscli fix --reset</code> , verify running scans have completed, then stop the <code>nessusd</code> daemon or service. Windows: <code>net stop "Tenable Nessus"</code> Linux: <code>service nessusd stop</code>



Command	Description
Certificate Commands	
nessuscli mkcert-client	Creates a certificate for the Nessus server.
nessuscli mkcert [-q]	Quietly creates a certificate with default values.
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.
nessuscli update <tar.gz filename>	Updates Nessus plugins by using a TAR file instead of getting the updates from the plugin feed. The TAR file is obtained when you Register Nessus Offline - Download and Copy Plugins steps.
Manager Commands	
Used for generating plugin updates for your managed scanners and agents connected to a manager.	
nessuscli manager download-core	Downloads core component updates for remotely managed agents and scanners.
nessuscli manager generate-plugins	Generates plugins archives for remotely managed agents and scanners.
Managed Scanner Commands	
Used for linking, unlinking and viewing the status of remote managed scanners.	
nessuscli managed help	Displays nessuscli managed commands and syntax.
nessuscli managed link --key=<key> --host=<host> --port=<port> [optional parameters]	Link a managed scanner to the Nessus Manager. Additional Parameters --name=<name> --ca-path=<ca_file_name> --proxy-host=<host>



Command	Description
	<code>--proxy-port=<port></code> <code>--proxy-username=<username></code> <code>--proxy-password=<password></code> <code>--proxy-agent=<agent></code>
<code>nessuscli managed unlink</code>	Unlink a managed scanner to the Nessus Manager.
<code>nessuscli managed status</code>	Identifies the status of the managed scanner.

Nessuscli Agent

Some Nessus Agent functions can be performed and administered through a command line interface using the **nessuscli agent** utility.

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

Nessuscli Agent Syntax

Operating System	Command
Linux	# /opt/nessus_agent/sbin/nessuscli agent <arg1> <arg2>
Mac OS X	# /Library/NessusAgent/run/sbin/nessuscli <arg1> <arg2>
Windows	C:\Program Files\Tenable\Nessus Agent or C:\ProgramData\Tenable\Nessus Agent Run cmd.exe as administrator

Nessuscli Agent Commands

Command	Description
Help Commands	
# nessuscli agent help	Displays a list of Nessus Agent commands
Bug Reporting Commands	
# nessuscli bug-report-generator	Generates an archive of system diagnostics. Running this command without arguments prompts for values. --quiet: run the bug report generator without prompting user for feedback..



Command	Description
	<p>--scrub: when in quiet mode, bug report generator sanitizes the last two octets of the IPv4 address</p> <p>--full: when in quiet mode, bug report generator collects extra data..</p>
Local Agent Commands	
Used to link, unlink, and display agent status	
<pre># nessuscli agent link --key=<key> [--name=<name>] [- -groups=<group1,group2,...>] [--ca-path=<ca_file_ name>] --host=<host> --port=<port></pre>	<p>Using the key obtained from within Nessus Manager, this command links the agent to the Nessus Manager.</p> <p>Optional Parameters</p> <p>--name=<name></p> <p>--groups=<group1,group2,...></p> <p>--ca-path=<ca_file_name></p> <p>--proxy-host=<host></p> <p>--proxy-port=<port></p> <p>--proxy-username=<username></p> <p>--proxy-password=<password></p> <p>--proxy-agent=<agent></p>
<pre># nessuscli agent unlink</pre>	Unlinks agent from the Nessus Manager.
<pre># nessuscli agent status</pre>	<p>Displays the status of the agent: jobs pending and if the agent linked or not linked to server.</p> <p>Example Status</p> <p>Agent linked 3 jobs pending</p> <p>Agent not linked to a server</p>



Command	Description
	Agent is linked to 192.168.0.1:8834 1 jobs pending

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 [Register Nessus Offline](#).

Operating System	Command
Linux	# /opt/nessus/sbin/nessuscli <arg1> <arg2>
Mac OSX	# /Library/Nessus/run/sbin/nessuscli <arg1> <arg2>
Windows	C:\Program Files\Tenable\Nessus or C:\ProgramData\Tenable\Nessus
Commands must <i>Run as administrator</i>	
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.

Custom SSL Certificates

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

To avoid browser warnings, a custom SSL certificate specific to your organization can be used. During the installation, Nessus creates two files that make up the certificate: `servercert.pem` and `serverkey.pem`. These files must be replaced with certificate files generated by your organization or a trusted Certificate Authority (CA).

Before replacing the certificate files, stop the Nessus server. Replace the two files and re-start the Nessus server. Subsequent connections to the scanner should not display an error if the certificate was generated by a trusted CA.

You can configure Nessus for custom SSL certificates using the following steps:

- [SSL Client Certificate Authentication](#)
- [Create a New Custom CA and Server Certificate](#)
- [Create Nessus SSL Certificates for Login](#)
- [Enable Connections with Smart Card or CAC Card](#)
- [Connect with Certificate or Card Enabled Browser](#)

Location of Certificate Files

Operating System	Directory
Linux	<code>/opt/nessus/com/nessus/CA/servercert.pem</code> <code>/opt/nessus/var/nessus/CA/serverkey.pem</code>
FreeBSD	<code>/usr/local/nessus/com/nessus/CA/servercert.pem</code> <code>/usr/local/nessus/var/nessus/CA/serverkey.pem</code>
Windows Vista and later	<code>C:\ProgramData\Tenable\Nessus\nessus\CA\servercert.pem</code> <code>C:\ProgramData\Tenable\Nessus\nessus\CA\serverkey.pem</code>
Mac OS X	<code>/Library/Nessus/run/com/nessus/CA/servercert.pem</code>



Operating System	Directory
	<code>/Library/Nessus/run/var/nessus/CA/serverkey.pem</code>
<p>You can also use the <code>/getcert</code> switch to install the root CA in your browser, which will remove the warning.</p> <p><code>https://[IP address]:8834/getcert</code></p>	

Note: To set up an intermediate certificate chain, a file named `serverchain.pem` must be placed in the same directory as the `servercert.pem` file. This file contains the 1-n intermediate certificates (concatenated public certificates) necessary to construct the full certificate chain from the Nessus server to its ultimate root certificate (one trusted by the user's browser).

SSL Client Certificate Authentication

Nessus supports use of SSL client certificate authentication. This allows use of SSL client certificates, smart cards, and CAC authentication when the browser is configured for this method.

Nessus allows for password-based or SSL Certificate authentication methods for user accounts. When creating a user for SSL certificate authentication, the `nessuscli mkcert-client` utility is used through the command line on the Nessus server.

Create a New Custom CA and Server Certificate

To allow SSL certificate authentication in Nessus, you must configure the Nessus web server with a server certificate and CA (Certificate Authority).

This allows the web server to trust certificates created by the Certificate Authority (CA) for authentication purposes. Generated files related to certificates must be owned by root:root, and have the correct permissions by default.

Note: You must re-link any connected Nessus Agents or managed Scanners after loading new certificates.

Steps

1. Create a new custom CA and server certificate for the Nessus server using the **nessuscli mkcert** command at the command line. This will place the certificates in their correct directories.

When prompted for the hostname, enter the DNS name or IP address of the server in the browser such as `https://hostname:8834/` or `https://ipaddress:8834/`. The default certificate uses the hostname.

2. If you want to use a CA certificate instead of the Nessus generated one, make a copy of the self-signed CA certificate using the appropriate command for your OS:

Linux

```
# cp /opt/nessus/com/nessus/CA/cacert.pem /opt/nessus/com/nessus/CA/ORIGcacert.pem
```

Windows Vista and later

```
C:\> copy \ProgramData\Tenable\Nessus\nessus\CA\cacert.pem  
C:\ProgramData\Tenable\Nessus\nessus\CA\ORIGcacert.pem
```

3. If the certificates to be used for authentication are created by a CA other than the Nessus server, the CA certificate must be installed on the Nessus server.

Linux

Copy the organization's CA certificate to `/opt/nessus/com/nessus/CA/cacert.pem`

Windows 7 and later

Copy the organization's CA certificate to `C:\ProgramData\Tenable\Nessus\nessus\CA\cacert.pem`

4. Configure the Nessus server for certificate authentication. Once certificate authentication is enabled, log in using a username and password is disabled.

Caution: Connecting Agents, Remote Scanners, or Managed Scanners using the `force_pubkey_auth` option is not supported.

Linux

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

Windows

```
C:\> \program files\Tenable\Nessus\nessuscli fix --set force_pubkey_auth=yes
```

5. Once the CA is in place and the `force_pubkey_auth` setting is enabled, restart the Nessus services with the `service nessusd restart` command.

Note: Any linked Agents will still have an old certificate (`ms_cert`) and communication will fail to the Nessus Manager. Relink the Agent using the following commands:

```
nessuscli agent unlink
```

```
nessuscli agent link --host=<host> --port=<port> --key=<key> --groups<-group1,group2>
```

After Nessus has been configured with the proper CA certificate(s), you can log in to Nessus using SSL client certificates, Smart Cards, and CACs.

Upload a Custom CA Certificate

These steps describe how to upload a custom CA (Certificate Authority) certificate to the Nessus web server through the command line.

Steps

1. [Create one or more custom CA and server certificates.](#)
2. Back up the original Nessus CA and server certificates and keys:

```
cp /opt/nessus/com/nessus/CA/cacert.pem  
/opt/nessus/com/nessus/CA/cacert.pem.orig  
cp /opt/nessus/var/nessus/CA/cakey.pem /opt/nessus/var/nessus/CA/cakey.pem.orig  
cp /opt/nessus/com/nessus/CA/servercert.pem  
/opt/nessus/com/nessus/CA/servercert.pem.orig  
cp /opt/nessus/var/nessus/CA/serverkey.pem  
/opt/nessus/var/nessus/CA/serverkey.pem.orig
```

3. Replace the original certificates with the new custom certificates:

```
cp customCA.pem /opt/nessus/com/nessus/CA/cacert.pem  
cp customCA.key /opt/nessus/var/nessus/CA/cakey.pem  
cp servercert.pem /opt/nessus/com/nessus/CA/servercert.pem  
cp server.key /opt/nessus/var/nessus/CA/serverkey.pem
```

4. Restart Nessus:

```
service nessusd restart
```

Note: Any linked agent has an old certificate in its configuration, (ms_cert) and upon restart, communication fails to the manager. You can remedy this by relinking the agent to the controller:

```
nessuscli agent unlink  
nessuscli agent link --host=<host> --port=<port> --key=<key> --groups<group1,group2>
```

You can also load the cacert.pem file into the custom_CA.inc file in the Agents plugin directory:

```
scp customCA.pem root@agentip:/opt/nessus_agent/lib/nessus/custom_CA.inc
```

Create Nessus SSL Certificates for Login

To log in to a Nessus server with SSL certificates, the certificates must be created with the proper utility. For this process, the `nessuscli mkcert-client` command line utility is used on the system. The six questions asked are to set defaults for the creation of users during the current session. These include certificate lifetime, country, state, location, organization, and organizational unit. The defaults for these options may be changed during the actual user creation if desired. The user(s) will then be created one at a time as prompted. At the end of the process the certificates are copied appropriately and are used to log in to the Nessus server.

1. On the Nessus server, run the `nessuscli mkcert-client` command.

Linux:

```
# /opt/nessus/sbin/nessuscli mkcert-client
```

Windows (Run as a local Administrator user):

```
C:\> \Program Files\Tenable\Nessus\nessuscli mkcert-client
```

2. Fill in the fields as prompted. The process is identical on a Linux or Windows server.

mkcert-client Output

```

-----
This script will now ask you for information to create SSL client certificates.
Nessus username for user: sylvester
Do you want to add sylvester to the Nessus server
as soon as their certificate is created? (y/n) [y]: y
Should this user be an administrator? (y/n) [n]: y
User rules
-----
nessusd has a rules system which allows you to restrict the hosts
that sylvester has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the Nessus Command Line Reference for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)

Login      : sylvester
Password   : *****
Client certificate life time in days [365]:
Two letter country code [US]:
State or province name [NY]:
City [New York]:
Organization [Nessus Users United]:
Organizational unit [nessus-users]:
Email [none@none.com]:

--- Confirmation ---
Username: sylvester <This user will be a new administrator>
Client certificate life time in days: 365
Country: US
State or province: NY
City: New York
Organization: Nessus Users United
Organizational unit: nessus-users
Email: none@none.com
Is this ok? (y/n) [n]: y

Congratulations. Your client certificate was properly created.

The following files were created :
  Nessus Client :
    Certificate = C:\ProgramData\Tenable\Nessus\nessus\tmp\cert_sylvester.pem
    Private key = C:\ProgramData\Tenable\Nessus\nessus\tmp\key_sylvester.pem

The user sylvester was successfully created.
Create another cert? (y/n) [y]: _

```

Tip: The client certificates will be placed in the temporary directory in Nessus:

Linux: /opt/nessus/var/nessus/tmp/

Mac OSX: /Library/Nessus/run/var/nessus/tmp/

Windows: C:\programdata\tenable\nessus\tmp

Tip: Windows installations of Nessus do not come with “man” pages (local manual instructions). Consult the Tenable Network Security Support Portal for additional details on commonly used Nessus executables.

3. Two files are created in the temporary directory. In the example demonstrated in the above image, `cert_sylvester.pem` and `key_sylvester.pem` were created. These two files must be combined and exported into a format that may be imported into the web browser such as `.pfx`. This may be accomplished with the openssl program and the following command:

```
#  
#openssl pkcs12 -export -out combined_sylvester.pfx -inkey key_sylvester.pem -  
in cert_sylvester.pem -chain -CAfile /opt/nessus/com/nessus/CA/cacert.pem -  
passout 'pass:password' -name 'Nessus User Certificate for: sylvester'
```

The resulting file `combined_sylvester.pfx` will be created in the directory from which the command is launched. This file must then be imported into the web browser's personal certificate store.

Enable Connections with Smart Card or CAC Card

Once the CAcert has been created for the smart card, CAC, or similar device, you must create corresponding Nessus users. During this process, the users created must match the CN used on the card that the user will use to connect.

1. On the Nessus server, run the `nessus-mkcert-client` command.

Linux

```
# /opt/nessus/sbin/nessuscli mkcert-client
```

Windows (Run as a local Administrator user):

```
C:\> \Program Files\Tenable\Nessus\nessuscli.exe mkcert-client
```

2. Fill in the fields as prompted. The process is identical on a Linux or Windows server. The user name must match the CN supplied by the certificate on the card.

Tip: Client certificates are created in a randomized temporary directory appropriate to the system. The temporary directory will be identified on the line beginning with "Your client certificates are in". For the use of card authentication, these certificates are not needed and may be deleted.

Once created, a user with the proper card may access the Nessus server and authenticate automatically once their PIN or similar secret is provided.

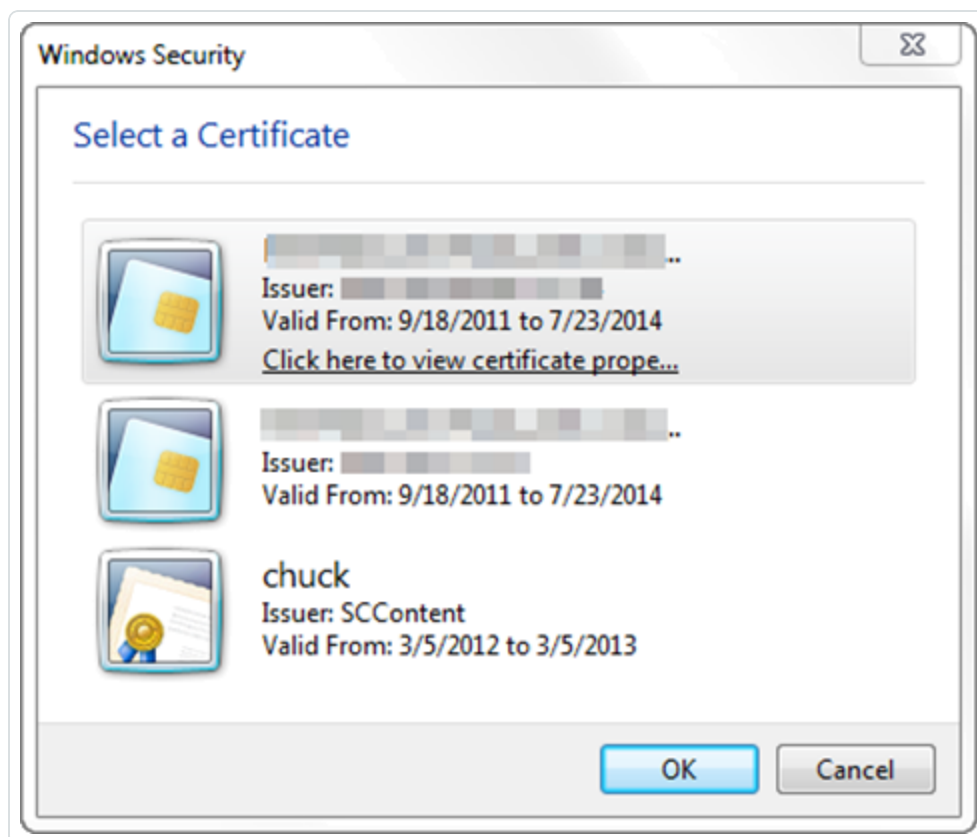
Connect with Certificate or Card Enabled Browser

The following information is provided with the understanding that your browser is configured for SSL certificate authentication. This includes the proper trust of the CA by the web browser. Please refer to your browser's help files or other documentation to configure this feature.

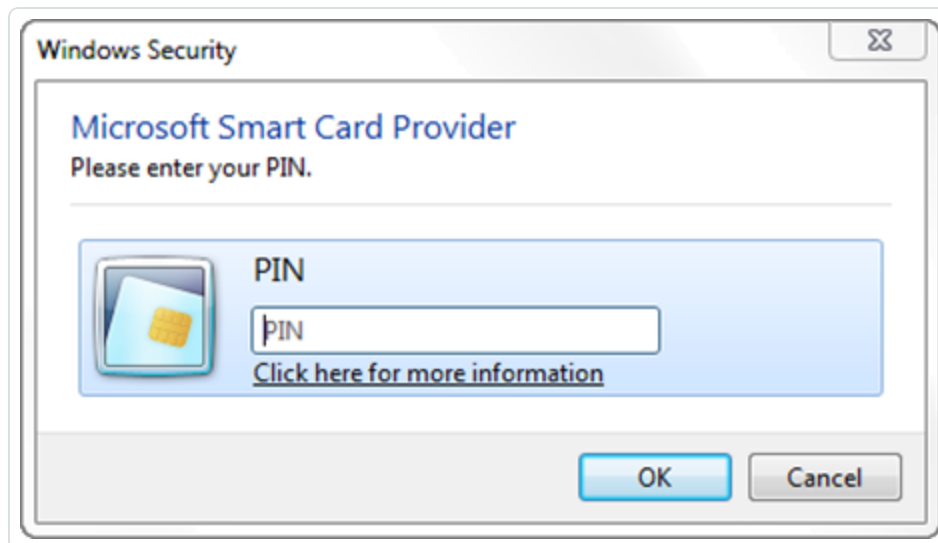
The process for certificate login begins when a user connects to Nessus.

Steps

1. Launch a browser and navigate to the Nessus server.
2. The browser will present a list of available certificate identities to select from:



3. Once a certificate has been selected, a prompt for the PIN or password for the certificate is presented (if required) to access your certificate. When the PIN or password is successfully entered, the certificate will be available for the current session with Nessus.



4. Upon navigating to the Nessus web interface, the user may briefly see the username and password screen followed by an automatic login as the designated user. The Nessus user interface may be used normally.

Note: If you log out of the session, you will be presented with the standard Nessus login screen. If you wish to log in again with the same certificate, refresh your browser. If you need to use a different certificate, you must restart your browser session.

Enable SSH Local Security Checks

Before You Begin

This section applies to Linux and Network Devices

This section is intended to provide a high-level procedure for enabling SSH between the systems involved in the Nessus credentialed 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.

Generate 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 hit the Return key twice (i.e., do not set any passphrase). If a passphrase is specified, it must be specified in the Policies → Credentials → SSH settings options 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.

Create 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.

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`.

Note: Do not use the **no-pty** option in your **authorized_keys** file for SSH authentication. This can impact the SSH credentialed scans.

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.

Enable SSH Local Security Checks on Network Devices

In addition to using SSH for local security checks, Nessus also supports local security checks on various network devices. Those network devices currently include Cisco IOS devices, F5 networks devices, Huawei devices, Junos devices, and Palo Alto Networks devices.



Network devices that support SSH require both a username and password. Currently, Nessus does not support any other forms of authentication to network devices.

See your appropriate network device manual for configuring SSH support.

Manage Activation Code

From time to time, you may have cause to manage your Activation Code.

The following topics include instructions to:

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

If you are using Nessus offline, see [Register Nessus Offline](#).

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

If you uninstall, and then you reinstall Nessus, you will 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 **X** 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 corresponding Activation Code, your activation code must be re-registered with Nessus.

You can update Nessus with the new activation code using either of the following methods:

- Update the Nessus Activation Code in the UI.
- Update the Nessus Activation Code via Command Line.

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

Update Nessus in the UI

1. In Nessus, select the  button ([System Settings](#) page).
2. Select the  button next to the Activation Code.
3. On the **Update Activation** screen, select your **Registration** type.
4. Enter the new Activation Code.
5. Select **Save**.

Next, Nessus downloads and installs the Nessus engine and the latest Nessus plugins.

Once the download process is complete, Nessus restarts, and then prompts you to log in again.

Nessus updates with the new licensing information.

Update Nessus via Command Line

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

Platform	Command
Linux	# /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx
FreeBSD	# /usr/local/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx



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

Next, Nessus downloads and installs the Nessus engine and the latest Nessus plugins.

Once the download process is complete, Nessus restarts, and then prompts you to log in again.

Nessus updates with the new licensing information.



Manage Nessus License and Registration

If your license changes, Nessus must be updated.

If your Nessus server has connectivity to the Internet, you will be able to follow the [Update Activation Code](#) steps.

If for security purposes your installation of Nessus does not have connectivity to the Internet, see [Register Nessus Offline](#).

More Nessus Resources

[Product Pages](#)

[Nessus Product Page](#)

[Nessus Product Feature Comparisons](#)

[Tenable Plugins Home Page](#)

[Tenable Support Portal](#)

[Nessus FAQs](#)

Nessus Credentialed Checks

In addition to remote scanning, Nessus can be used to scan for local exposures.

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 onsite 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 credentialed scan can quickly determine which systems are out of date on patch installation. This is especially important when a new vulnerability is made public and executive management wants a quick answer regarding the impact to the organization.

Another major concern for organizations is to determine compliance with site policy, industry standards (such as the Center for Internet Security (CIS) benchmarks) or legislation (such as Sarbanes-Oxley, Gramm-Leach-Bliley or HIPAA). Organizations that accept credit card information must demonstrate compliance with the Payment Card Industry (PCI) standards. There have been quite a few well-publicized cases where the credit card information for millions of customers was breached. This represents a significant financial loss to the banks responsible for covering the payments and heavy fines or loss of credit card acceptance capabilities by the breached merchant or processor.

Access Level

Credentialed scans can perform any operation that a local user can perform. The level of scanning is dependant on the privileges granted to the user account that Nessus is configured to use.

Non-privileged users with local access on Unix 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 Unix 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.

Note: 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, Windows 7, Windows 8, or Windows 10 and must be part of a domain.

Create a Security Group called Nessus Local Access

1. Log onto a Domain Controller and open **Active Directory Users and Computers**.
2. Create a security group by selecting **Action** → **New** → **Group**.
3. Name the group **Nessus Local Access**. Make sure it has a **Scope** of **Global** and a **Type** of **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 pane 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 SMB (Server Message Block) and WMI (Windows Management Instrumentation) for this we need to make sure that the Windows Firewall will allow access to the system.

Allow WMI on Windows Vista, 7, 8, 10, 2008, 2008R2 and 2012 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 list.
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 so as 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, File and Printer Sharing must be enabled.
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, and in many cases this 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, you should 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-**

authenticate as themselves.

6. Select **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, 2010, 2008, Vista, and 7

When performing authenticated scans against Windows 2008 systems, there are several configuration options that must be enabled:

- Under **Windows Firewall** -> **Windows Firewall Settings**, **File and Printer Sharing** must be enabled.
- Using the gpedit.msc tool (via the "Run.." prompt), enable the **Group Policy Object Editor**. Navigate to **Local Computer Policy** > **Administrative Templates** > **Network** > **Network Con-**

nections > 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 Web 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.

Nessus Unix Command Line

Using .nessus Files

Nessus has the ability to save configured scan policies, network targets and reports as a **.nessus** file. The **Nessus Web Interface** section describes the steps to create a **.nessus** file that contains SMB credentials.

Using .nessusrc Files

If you are manually building a **.nessusrc** file, there are three entries that allow for the configuration of the username, password and optional domain as shown below:

```
Login configurations[entry]:SMB account : =  
Login configurations[password]:SMB password : =  
Login configurations[entry]:SMB domain (optional) : =
```

Credentialed Checks on Unix

The process described in this section enables you to perform local security checks on Unix 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.

To enable local security checks, there are two basic methods that can be used:

1. Use of a SSH private/public key pair
2. User credentials and `sudo` access or credentials for `su` access

Prerequisites

Configuration Requirements for SSH

Nessus 4.x 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 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.

User Privileges

For maximum effectiveness, the SSH user must have the ability to run any command on the system. On Unix 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 Unix 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 Unix 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 pass phrase or hit the “Return” key twice (i.e., do not set any passphrase). If a pass phrase is specified, it must be specified in the Policies -> Credentials -> SSH settings options 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 Unix command “**id**”, from the Nessus scanner, run the following command:

```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

If it successfully returns information about the Nessus user, the key exchange was successful.

Configure Nessus for SSH Host-Based Checks

If you have not already done so, secure copy the private and public key files to the system that you will use to access the Nessus scanner.

Nessus Web Interface Steps

In the Scan Credential Settings section, select SSH.

- If an SSH **known_hosts** file is available and provided as part of the scan policy in the **known_hosts file** box, 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 login to a system that may not be under your control.
- In the **Username** box, enter the name of the account that is dedicated to Nessus on each of the scan target systems.
- If you are using a password for SSH, enter it in the **Password** box.
- In the **Private Key** box, locate the private key file on your local system.
- If you are using a passphrase for the SSH key (optional), enter it in the **Private key passphrase** box.
- Nessus and SecurityCenter users can additionally use “su” or “sudo” in the **Elevate privileges with** box and a separate password.

The most effective credentialed scans are those when the supplied credentials have “root” privileges. Since many sites do not permit a remote login as root, Nessus users can invoke “su” or “sudo” with a separate password for an account that has been set up to have “su” or “sudo” privileges.

Nessus Unix Command Line

Nessus support for host-based checks is available in Nessus 2.2.0 and later and requires that SSL support be compiled in. Run the “`nessusd -d`” command to verify that you have the correct version and SSL libraries as follows:

```
# nessusd -d
This is Nessus 4.0.0. [build T987] for Linux 2.6.18-53.1.6.el5
compiled with gcc version 4.1.2 20070626 (Red Hat 4.1.2-14)
Current setup :
```

```
flavor : (undefined)
nasl : 4.0.0
libnessus : 4.0.0
SSL support : enabled
SSL is used for client / server communication
Running as euid : 0
Magic hash: (undefined)#
```

Using .nessus Files

Nessus has the ability to save configured scan policies, network targets and reports as a **.nessus** file. The **Nessus Web Interface Steps** section describes the steps to create a **.nessus** file that contains SSH credentials.

Using .nessusrc Files

If you are manually creating **.nessusrc** files, there are several parameters that can be configured to specify SSH authentication. An example of an unpopulated listing is shown below:

```
Use SSH to perform local security checks[entry]:SSH user name : =
Use SSH to perform local security checks[file]:SSH public key to use : =
Use SSH to perform local security checks[file]:SSH private key to use : =
Use SSH to perform local security checks[password]:Passphrase for SSH key
: =
SSH settings[entry]:SSH user name : =
SSH settings[password]:SSH password (unsafe!) : =
SSH settings[file]:SSH public key to use : = no
SSH settings[file]:SSH private key to use : =
SSH settings[password]:Passphrase for SSH key : =
```

If you are using Kerberos, you must configure a Nessus scanner to authenticate to a KDC by entering the following information in the scanner **.nessusrc** file:

```
Kerberos KDC port : 88
Kerberos KDC Transport : udp
Kerberos Realm (SSH Only) : myrealm
Kerberos Key Distribution Center (KDC): 192.168.20.66
```



The default KDC port is “88” and the default transport protocol is “udp”. The other value for transport is “tcp”. Last, the Kerberos Realm name and IP address of the KDC are required.

Note: You must already have a Kerberos environment established to use this method of authentication.

Offline Update Page Details

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

Based the steps you are using to [Register Nessus Offline](#), the resulting web page displayed 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 Network Security LICENSE----- and ends with -----END Tenable Network Security 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 license text-string displayed.

<https://plugins.nessus.org/v2/nessus.php>

```
-----BEGIN TENABLE LICENSE-----
[Illegible License Text]
-----END TENABLE LICENSE-----
```

You may also install the license using Nessus command line tools:

- nessus.license

Unofficial PCI ASV Validation Scan

Approved Scanning Vendors (ASVs) are organizations that validate adherence to certain DSS requirements by performing vulnerability scans of Internet facing environments of merchants and service providers.

Tenable Network Security is a PCI Approved Scanning Vendor (ASV), and is certified to validate vulnerability scans of Internet-facing systems for adherence to certain aspects of the PCI Data Security Standards (PCI DSS) and Tenable.io is a validated Approved Scanning Vendor (ASV) solution.

Nessus Professional and Nessus Manager features 2 PCI related scan templates:

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 client-side vulnerabilities.

Note: while the PCI DSS requires you to provide evidence of passing or "clean" scans on at least a quarterly basis, you 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 Network Security 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 Network Security for PCI ASV validation.



When submitted, scan results are uploaded and the scan results can be reviewed from a PCI DSS perspective.

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, perform a Nessus [Linux Install](#).
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_pr/sbin/nessus-service -q`
- **Add:** `ExecStart=/opt/nessus_pr/sbin/nessus-service -q --no-root`
- **Add:** `User=nonprivuser`


The resulting script should appear as follows:

```
[Service]
Type=simple
PIDFile=/opt/nessus_pr/var/nessus/nessus-service.pid
ExecStart=/opt/nessus_pr/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, perform a Nessus [Linux Install](#).
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. Remove and add the following lines to the **/etc/init.d/nessusd** script:

Remove: `/opt/nessus/sbin/nessus-service -q -D`

Add: `daemon --user=nonprivuser /opt/nessus/sbin/nessus-service -q -D --no-root`

The resulting script should appear as follows:

```
start() {
    KIND="$NESSUS_NAME"
    echo -n $"Starting $NESSUS_NAME : "
    daemon --user=nonprivuser /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
```

Run Nessus on MAC OSX 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.

The screenshot shows the 'Users & Groups' window in macOS, specifically the 'Advanced Options' tab for a user named 'NonPrivUser'. The window has a title bar with standard macOS window controls and a search field. The 'User' field is set to 'NonPrivUser'. A red warning message states: 'WARNING: Changing these settings might damage this account and prevent the user from logging in. You must restart the computer for the changes to these settings to take effect.' The 'User ID' is 506, 'Group' is nonpriv_group, 'Account name' is nonprivuser, 'Full name' is NonPrivUser, and 'Login shell' is /bin/bash. The 'Home directory' is /Users/nonprivuser, with a 'Choose...' button. The 'UUID' is 945C36CC-1627-466A-8AA6-09AE1D9937E2, with a 'Create New' button. The 'Apple ID' field is empty, with a 'Set...' button. There is an 'Aliases' field with a list box and a '+' button. At the bottom right are 'Cancel' and 'OK' buttons.

Users & Groups

Search

Advanced Options

User: "NonPrivUser"

WARNING: Changing these settings might damage this account and prevent the user from logging in. You must restart the computer for the changes to these settings to take effect.

User ID: 506

Group: nonpriv_group

Account name: nonprivuser

Full name: NonPrivUser

Login shell: /bin/bash

Home directory: /Users/nonprivuser Choose...

UUID: 945C36CC-1627-466A-8AA6-09AE1D9937E2 Create New

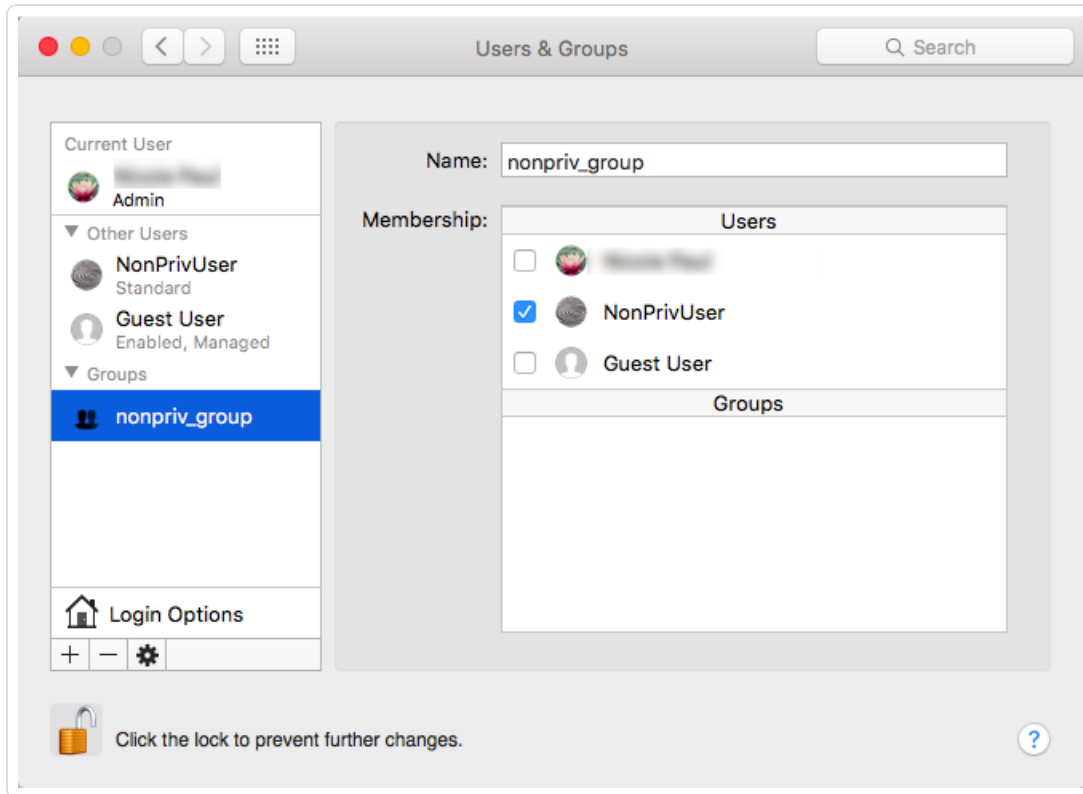
Apple ID: Set...

Aliases:

+ -

Cancel OK

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.

- Using a text editor, modify the Nessus `/Library/LaunchDaemons/com.tenablesecurity.nessusd.plist` file and add the following lines. Do not modify any of the existing lines.

```
<string>--no-root</string>
<key>UserName</key>
<string>nonprivuser</string>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Disabled</key>
  <true/>
  <key>Label</key>
  <string>com.tenablesecurity.nessusd</string>
  <key>ProgramArguments</key>
  <array>
    <string>/Library/Nessus/run/sbin/nessus-service</string>
    <string>-q</string>
    <string>--no-root</string>
  </array>
  <key>RunAtLoad</key>
  <true/>
  <key>UserName</key>
  <string>nonprivuser</string>
</dict>
</plist>
|
```

- Using `sysctl`, verify the following parameters have the minimum values:

```
$ sysctl debug.bpf_maxdevices
debug.bpf_maxdevices: 16384
$ sysctl kern.maxfiles
kern.maxfiles: 12288
$ sysctl kern.maxfilesperproc
kern.maxfilesperproc: 12288
$ sysctl kern.maxproc
kern.maxproc: 1064
$ sysctl kern.maxprocperuid
kern.maxprocperuid: 1064
```

-
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 **systctl.conf** file with the correct values found in Step 9.

Example:

```
$ cat /etc/sysctl.conf
kern.maxfilesperproc=12288
kern.maxproc=1064
kern.maxprocperuid=1064
```

13. Next, using the **launchctl limit** command, verify your OS default values.

Example: MacOSX 10.10 and 10.11 values.

```
$ launchctl limit
cpu            unlimited      unlimited
filesize       unlimited      unlimited
data           unlimited      unlimited
stack          8388608        67104768
core           0              unlimited
rss            unlimited      unlimited
memlock        unlimited      unlimited
maxproc        709         1064
maxfiles       256         unlimited
```

14. If 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 the 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 host-name 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]	