tenable network security

Nessus User Guide

Last Updated: 3/4/2016

Table of Contents

About Nessus Products

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 & compliance personnel, IT administrators, network admins and security analysts. These collaborative features reduce the time and cost of security scanning and compliance auditing by streamlining scanning, malware and misconfiguration discovery, and remediation.

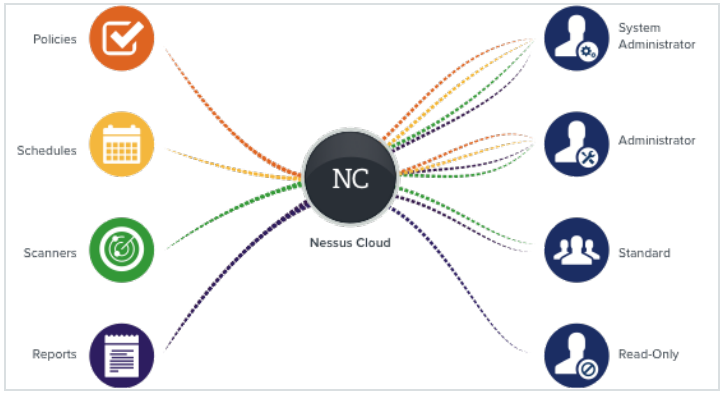
Nessus Manager protects physical, virtual, mobile and cloud environments. Nessus Manager is available for on-premises deployment or from the cloud, as Nessus® Cloud, hosted by Tenable. Nessus Manager supports the widest range of systems, devices and assets, and with both agent-less and Nessus Agent deployment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

Nessus Cloud

Nessus Cloud is a subscription based license and is available at the Tenable Store.

The subscription includes:

- One user account per subscription
- 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, Inc.
- 24/7 access to the Tenable Support Portal for Nessus knowledgebase and support ticket creation



Nessus® Cloud is Tenable's hosted, cloud-based vulnerability management solution that combines the powerful detection, scanning and auditing features of Nessus with multi-user support enabling extensive collaborative capabilities of scanners and resources.

In addition, Nessus Cloud is Tenable's Approved Scanning Vendor (ASV) solution for validating adherence to certain PCI DSS requirements for performing vulnerability scans of Internet facing systems.

Nessus Cloud 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, Nessus Cloud 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, Nessus Cloud 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.

Nessus Cloud Product Page

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's expert vulnerability research team, Nessus sets the standard for vulnerability scanning speed and accuracy.

Nessus Professional Product Page

Nessus Plugins

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

Plugins also are utilized to obtain configuration information from authenticated hosts to leverage for configuration audit purposes against security best practices.

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 download plugins. For more details, see the Command Line section of this guide.

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

Optionally, during the **Product Registration** portion of the Browser Portion of the Nessus install, you can choose the **Custom Settings** link and provide a hostname or IP address to a server which hosts your custom plugin feed.

How do I update Nessus Plugins?

By default, Nessus checks for updated components and plugins every 24 hours. Additionally, you can manually update from the Settings Page in the UI.

You can also use the nessuscli update command update plugins. For more details, see the Command Line section of this guide.

Tenable Plugins Home Page

Nessus Agents

Nessus Agents, available with Nessus Cloud 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 User Guide

Last Updated: 3/4/2016

This guide includes information to prepare you for installing, configuring, and using Nessus Manager®, Nessus Professional® and Nessus Agents®.

Please email any comments and suggestions to support@tenable.com.

Getting Started

This section provides information about you Nessus license, your system requirements, and how to download Nessus products.

Summary

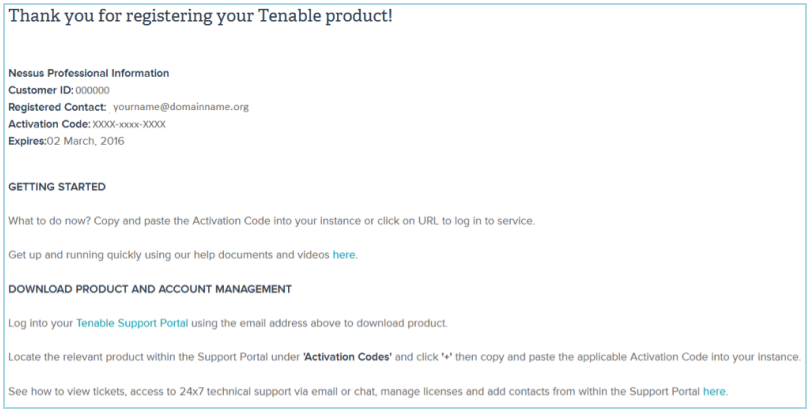
This section contains information about your **Nessus Manager** or **Nessus Professional** product registration and license.

Product Registration

Upon registration of your **Nessus** product, you received an e-email with details of your registration and instructions.

This e-mail includes your:

- Product Name
- Customer ID
- Registered Contact
- Alpha-numeric Activation Code
- Expiration Date



Thank you for registering your Tenable product!

Nessus Professional Information
Customer ID: 000000
Registered Contact: yourname@domainname.org
Activation Code: XXXX-xxxx-XXXX
Expires:02 March, 2016

GETTING STARTED

What to do now? Copy and paste the Activation Code into your instance or click on URL to log in to service.

Get up and running quickly using our help documents and videos here.

DOWNLOAD PRODUCT AND ACCOUNT MANAGEMENT

Log into your Tenable Support Portal using the email address above to download product.

Locate the relevant product within the Support Portal under **'Activation Codes'** and click **'+'** then copy and paste the applicable Activation Code into your instance.

See how to view tickets, access to 24x7 technical support via email or chat, manage licenses and add contacts from within the Support Portal here.

Activation Code

Your activation code is unique and specific to your Nessus product license.

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.

Additionally, your activation code...

- is a **one-time** code. If you uninstall and then re-install Nessus, you will need reset your activation code.
- must used with the Nessus installation within 24 hours.
- cannot be shared between scanners.
- is not case sensitive.
- is used to obtain the latest vulnerability checks when performing a **plugin** update.
- must be used to receive new plugins, otherwise you will be unable to start the Nessus server.

View Activation Code

From the Tenable Support Portal, you can view your registered **Activation Code(s).**

1. Navigate and log in to the Tenable Support Portal.
2. In the **Main Menu** of the support portal, click the **Activation Codes** link.
3. Next to your product name, click the ☒ button to expand the product details.

> You can also view your current **Activation Code** by using the Command Line: `nessuscli fetch --code-in-use`.

Reset Activation Code

If you uninstall, then 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, click the **Activation Codes** link.
3. Next to your product name, click the ☒ button to expand the product details.
4. Under the **Reset** column, click **X** button.

Once reset, your activation code is available for use.

Update Nessus License

If your Nessus license changes, Nessus must be updated accordingly.

If your Nessus server has connectivity to the internet, you will be able to perform an Online update within the Nessus user interface.

If for security purposes, your installation of Nessus does not have connectivity to the internet, you must perform an Offline update.

Online Update

1. In Nessus, navigate to the Settings page.
2. Click the pencil icon  next to the **Activation Code**.
3. Select your **Registration** type.

4. Enter the new **Activation Code**.
5. Click **Save**.

Next, 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 again.

At this point, Nessus is updated with the new licensing information.

Offline Update

If the system running Nessus is configured without Internet access, you can use the following steps on a computer with Internet access.

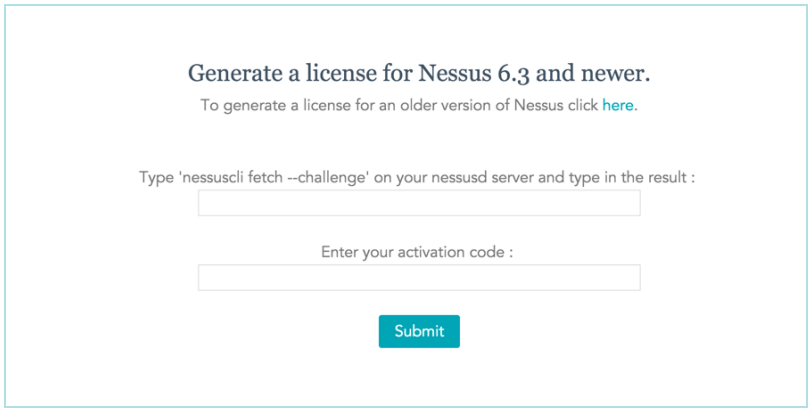
On the Nessus system running Nessus, using the command line, this process generates a **Challenge code**.

On another system with Internet access, this challenge code is entered into the Nessus Offline Registration Page.

Step 1. Obtain a Challenge code

1. On the system running Nessus, open a command prompt.
2. Use the nessuscli fetch --challenge command specific to your operating system.
3. Copy the alpha-numeric "challenge" string; you will use this in the next steps.

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



Step 2. Generate the License

1. On a system with Internet access, navigate to the Nessus Offline Registration Page.
2. Where prompted, type in the challenge code that was generated using the nessuscli fetch --challenge command.
3. Next, where prompted, enter your Nessus activation code.
4. Click **Submit**.

This process produces a URL that gives you direct access to Nessus plugins and creates the **nessus.license** file, which will be used on the Nesuss system.

5. Copy the **nessus.license** file to the appropriate directory of the server running Nessus.

Platform	Directory
Linux	# /opt/nessus/etc/nessus/
FreeBSD	# /usr/local/nessus/etc/nessus
Mac OS X	# /Library/Nessus/run/etc/nessus
Windows	C:\Program Files\Tenable\Nessus\conf
The URL generated is **customized** for Nessus. **Save this URL**; it will be used every time you update your Plugins.	

Step 3. Perform Registration using --register-offline Command

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

Platform	Command
Linux	# /opt/nessus/bin/nessuscli fetch --register-offline /opt/nessus/etc/nessus/nessus.license
FreeBSD	# /usr/local/nessus/bin/nessuscli fetch --register-offline /usr/local/nessus/etc/nessus/nessus.license
Mac OS X	# /Library/Nessus/run/bin/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\conf\nessus.license"

Step 4. Obtain Latest Plugins

1. On a system with Internet access, open a browser and enter your custom URL.
2. Obtain the TAR file (e.g., all-2.0.tar.gz).
3. Copy the .tar.gz file to the system running Nessus.
4. On the system running Nessus, open a command prompt.
5. 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>

System Requirements

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

Hardware Requirements

Smaller Networks	Larger Networks
Processor: Intel Dual-core **Processor Speed**: 2 GHz **RAM**: 2GB (4GB recommended) **Disk Space:** 30GB	**Processor:** Intel Dual-core (2 Dual-core recommended) **Processor Speed**: 2 GHz **RAM**: 2GB (8GB recommended) **Disk Space:** 30GB (Additional space allocations should be considered for reporting.)

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 Nessus' vulnerability checks, host enumeration, and operating system identification will be negatively affected.

Operating Systems

Nessus supports Mac, Unix, and Windows operating systems.

Nessus Operating Systems

Mac OSX

- Mac OSX 10.8-10.11 (x86-64)

Unix

- Debian 6 and 7 / Kali Linux 1.x (i386 and x86-64)
- Fedora 20 and 21 (i386 and x86-64)
- FreeBSD 10 (x86-64)
- Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 and x86-64)
- Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (i386 and x86-64) [Server, Desktop, Workstation]
- Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (x86-64) [Server, Desktop, Workstation]

- SUSE 10 (x86-64) and 11 (i386 and x86-64)
- Ubuntu 10.04 (9.10 package), 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 (i386 and x86-64)

Windows Operating Systems

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Microsoft Server 2012 R2 (x86-64)
- Windows 7 and 8 (i386 and x86-64)

Windows Server 2008 R2's bundled version of Microsoft IE does not interface with a Java installation properly. This causes Nessus not to perform as expected in some situations: Microsoft's policy recommends not using MSIE on server operating systems.

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.

Nessus Agent Operating Systems

- Fedora 20 and 21 (x86-64)
- Debian 6 and 7 (i386 and x86-64)

- Mac OSX 10.8-10.11 (x86-64)
- Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 and x86-64)
- Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (i386 and x86-64) [Server, Desktop, Workstation]
- Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (x86-64) [Server, Desktop, Workstation]
- Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2 (x86-64)
- Windows 7 and 8 (i386 and x86-64)
- Ubuntu 10.04, 12.04, and 14.04 (i386 and x86-64)

Browsers

When using the Nessus user interface, the following browsers are supported.

- Google Chrome (24+)
- Apple Safari (6+)
- Mozilla Firefox (20+)
- Internet Explorer (9+)

PDF Reporting

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

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

For details on installing Oracle Java, visit the Oracle Java website.

If **Oracle Java** is installed **after** the Nessus installation, Nessus will need to be reinstalled for the PDF report generation to function properly.

Product Download

Nessus products are downloaded from the Tenable Support Portal.

When downloading Nessus from the Tenable Support Portal, make sure that 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 and 8 - i386
Nessus-<version number>-x64.msi	Nessus <version number> for Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, and 8 - x86-64

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

Example Nessus Agent package file names and descriptions

Nessus Agent Packages	Nessus Agent Package Descriptions
NessusAgent-<version number>-x64.msi	Nessus Agent <version number> for Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, and 8 - x86-64

Nessus Agent Packages	Nessus Agent Package Descriptions
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

Install, Upgrade, Uninstall

This section includes information about installing, upgrading, and removing Nessus and Nessus Agents, on all supported operating systems.

Before you install Nessus

The section prepares you for a successful installation of Nessus.

To install and perform command-line operations, Nessus requires system root or Administrator permissions.

Deployment

When deploying Nessus, knowledge of routing, filters, and firewall policies is often helpful. It is recommended that Nessus be deployed so that it has good IP connectivity to the networks it is scanning. 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.

Host Based Firewalls

If your Nessus server is configured on a host with a "personal" firewall such as ZoneAlarm, Windows firewall, or any other firewall software, it is required that connections be allowed from the Nessus client's IP address from where the user is browsing.

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

IPv6 Support

Nessus supports scanning of IPv6 based resources. Many operating systems and devices are shipping 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 does support Link-local ranges with the **link6** directive as the scan target or local link with **eth0**.

Virtual Machines

If your virtual machine is using Network Address Translation (NAT) to reach the network, many of Nessus' vulnerability checks, host enumeration, and operating system identification will be 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, click on **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**, and 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 will be displayed.

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 will encounter when accessing the Nessus UI (https://[server IP]:8834).

Example Security Warning

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

This is expected and normal behavior, because Nessus is providing a self-signed SSL certificate.

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	Click on **Advanced**, and then **Proceed to example.com (unsafe)**.
Mozilla Firefox	Click on **I Understand the Risks**, and then click on **Add Exception**. Next click on **Get Certificate**, and finally click **Confirm Security Exception**.
Microsoft Internet Explorer	Click on **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 Cloud

Because **Nessus Cloud** is a subscription based product, there are no installation steps to perform.

Nessus Cloud Log-in

1. Open a web browser.
2. Type https://cloud.tenable.com
3. Enter your **Username** and **Password**, and then click the **Sign In** button.

Reset Password

1. From the **Nessus Cloud** log in page, click **Forgot your password?**
2. At the @ prompt, type the **Email Address** associated with your **Nessus Cloud** user account.
3. At the prompt, type the answer to the security question displayed, and then click the **Send** button.

> Shortly, you will receive an email, which includes a link to reset your password.

4. When you receive the email, click the link provided and complete the reset password instructions.

Nessus Installation

This section details instructions for installing Nessus Manager and Nessus Professional on Mac, Unix, and Windows operating systems.

There are two parts to the installation process: the operating system specific portion, followed by the OS agnostic browser portion, which completes the installation.

Mac Install

Step 1. Download Nessus package file

For details, refer to the Product Download topic.

Step 2. Extract the Nessus files

Double-click the Nessus-6.4.0.dmg file.

Step 3. Start Nessus Installation

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

Step 4. Complete the Tenable Nessus Server Install

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

Introduction

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

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

License

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

Installation Type

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

- Click the **Change Install Location** button.
- Click 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, click the **Install** button.

Next, the **Installing Tenable 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, click **Close**.

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

Unix Install

Step 1. Download Nessus Manager.

For details, refer to the Product Download topic.

Step 2. 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-6.4.0-es6.x86_64.rpm
```

Debian version 6

```
# dpkg -i Nessus-6.4.0-debian6_amd64.deb
```

FreeBSD version 10

```
# pkg add Nessus-6.4.0-fbsd10-amd64.txz
```

Step 3. 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. Browser Portion

Windows Install

Step 1. Download Nessus Manager

For details, refer to the Product Download topic.

Step 2. Start Nessus Installation

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

Step 3. Complete the Windows InstallShield Wizard

1. First, the **Welcome to the InstallShield Wizard for Tenable Nessus** screen will be displayed. Click **Next** to continue.
2. On the **License Agreement** screen, read the terms of the Tenable Network Security, Inc. Nessus Software License and Subscription Agreement.
3. Click the **I accept the terms of the license agreement** radio button, and then click the **Next** button.
4. On the **Destination Folder** screen, click the **Next** button to accept the default installation folder. Otherwise, click the **Change** button to install Nessus to a different folder.
5. On the **Ready to Install the Program** screen, click the **Install** button.

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

Step 4. 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 be displayed, and you will continue with the installation of Nessus.

1. On the **Welcome to the WinPcap Setup Wizard** screen, click the **Next** button.
2. On the **WinPcap License Agreement screen**, read the terms of the license agreement, and then click 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 click the **Install** button.
4. Next, on the **Completing the WinPcap Setup Wizard** screen, click the **Finish** button.
5. Finally, the **Tenable Nessus InstallShield Wizard Completed** screen will be displayed. Click the **Finish** button.

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

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

Installation Browser Portion

Step 1. Begin Browser Portion of the Nessus Setup

1. On the **Welcome to Nessus** page, click 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.

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 is providing a self-signed SSL certificate.

2. Accept, then Disable Privacy Settings

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

3. On the **Welcome to Nessus 6** page, click the **Continue** button.

Step 2. 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.

   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, click the **Continue** button.

Step 3. Register your Nessus Product

At this point of the installation process, you will identify which type of registration you are performing.

1. Using the **Registration** drop-down menu, select your registration type.

Registration Type	Description
Nessus (Home, Professional, or Manager)	This option installs Nessus Home, Nessus Professional, or Nessus Manager. During installation, you will be prompted to enter your Nessus Activation Code; this activation code determines which one of these product will be installed.
Nessus Scanner	This option installs Nessus as a remote scanner. During installation, you will be prompted to enter the Nessus Manager's Link Key.
Managed by Security Center	This option is used when installing Nessus, which will be managed by Security Center.
Offline	This option is used when you are performing an Offline installation and registration of Nessus.

2. In the **Activation Code** field, type in the alpha-numeric code that you obtained from the Tenable Support Portal.
3. OPTIONAL: Click 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.

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

4. In the **Host** field, type the host name or IP address of your proxy server.
5. In the **Port** field, type the Port Number of the proxy server.
6. In the **Username** field, type the name of a user account that has permissions to access and use the proxy server.
7. In the **Password**, type the password of the user account that you specified in the previous step.
8. 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.
9. Click **Save** to commit your **Custom Settings**.
10. Finally, click the **Continue** button.

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

Step 4. Login to Nessus

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

Unix-based operating sytems may attempt to connect to the Nessus server with a relative host name which is not in DNS (e.g., http://mybox:8834/). If the host name is not in DNS or not in the /etc/hosts file, you must connect to the Nessus server using an IP address or a valid DNS name.

This completes the installation process.

Nessus Agent Install

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

Once installed**, Nessus Agents** are linked to **Nessus Manager** or **Nessus Cloud**. **Nessus**

- **Nessus Agents** are **not** available for use with **Nessus Professional**.
- **Nessus Agents** can only be installed **after** the installation of **Nessus Manager** or the configuration of **Nessus Clou**d.
- **Nessus Agents** are downloaded from the Nessus Agents Download Page, installed, and then linked to a Nessus Manager.
- Before you start the **Agent** installation process, you will first retrieve the **Nessus Agent Key** from within the **Nessus Manager** or **Nessus Cloud** interface.
- During the **Nessus Agent** install process, you will be required to enter the **Nessus Agent Key**.
- 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.

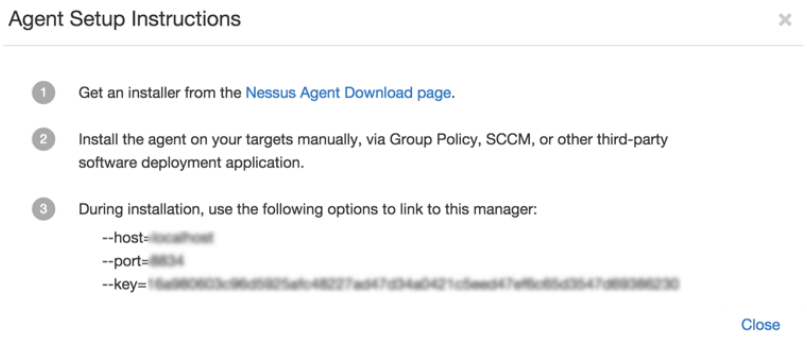
Mac Agent Install

Step 1. Retrieve Agent Key from within Nessus

1. Log-in to the Nessus UI.
2. Click the gear icon .
3. On the **Scanners / Agents / Linked** page, click **Agent** > **Linked**.

Linked Agent 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.



Step 2. Click the setup instructions link that appears within the on-screen message.

1. Record the **host**, **port**, and **key** values. These values will be used during the installation of the **Agent**.
2. Click the **Close** button.

Step 3. Download Nessus Agent

From the Nessus Agents Download Page, download the **Nessus Agent** specific to your operating system.

Example: Compressed Nessus Installer File

NessusAgent-<version number>.dmg

Step 4. Install Nessus Agent

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

Next, you will use the command line interface (Terminal) to link your **Nessus Agent** to **Nessus Manager** or Nessus Cloud.

Step 5. Link Agent using Command Line Interface

During this step, 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

Agent Key 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=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00
--name="MyOSXAgent" --groups="All" --host=yourcompany.com --port=8834
```

Step 6. Verify that your Agent is linked.

1. In **Nessus**, click the gear icon .
2. View linked Agents on the **Scanners / Agents / Linked** page.

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

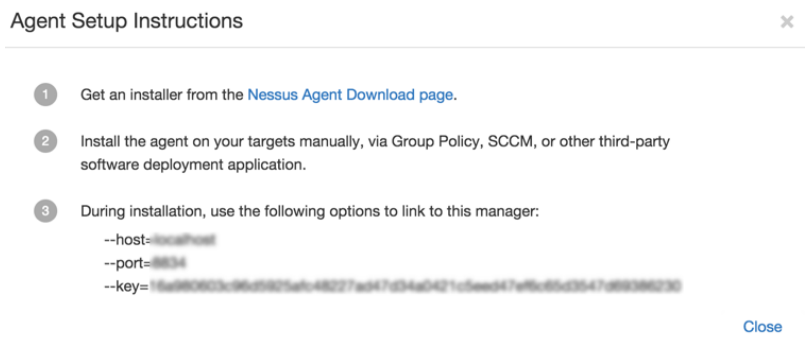
Unix Agent Install

Step 1. Retrieve Agent Key from within Nessus

1. Log-in to the Nessus UI.
2. Click the gear icon .
3. On the **Scanners / Agents / Linked** page, click **Agent** > **Linked**.

Linked Agent 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.



Step 2. Click the setup instructions link that appears within the on-screen message.

1. Record the **host**, **port**, and **key** values. These values will be used during the installation of the **Agent**.
2. Click the **Close** button.

Step 3. Download 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>-es5.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

Step 4. Link Agent using Command Line Interface

This step requires root privileges.

During this step, 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)

Agent Key Values

--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.

In the command line interface, use the correct package-manager command to install the Nessus Agent.

Example Unix 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
```

During this step, you will need the **Agent Key** values: **host**, **port**, and **key**.

3. At the command prompt, use the following command as an example to construct your specific string.

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**

Agent Key Values
within the Nessus UI.

Example Unix Agent Link Command

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

4. Verify that your Agent is displayed in Nessus Manager or Nessus Cloud.
5. In Nessus, click the gear icon .
6. View Agents on the **Scanners / Agents / Linked** page.

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

This completes the process of installing a **Nessus Agent** on the **Unix** operating system.

Windows Agent Install

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.

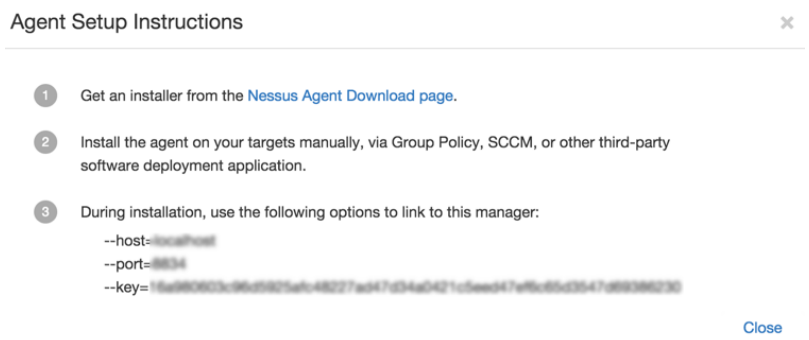
On Windows 7 x64 Enterprise, Windows 8 Enterprise, and Windows Server 2012, you may be required to perform a reboot to complete installation .

Step 1. Retrieve Agent Key from within Nessus

1. Log-in to the Nessus UI.
2. Click the gear icon .
3. On the **Scanners / Agents / Linked** page, click **Agent** > **Linked**.

   Linked Agent 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.



Step 2. Click the setup instructions link that appears within the on-screen message.

1. Record the **host**, **port**, and **key** values. These values will be used during the installation of the **Agent**.
2. Click the **Close** button.

Step 3. 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)

Step 4. Start Nessus Installation

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

Step 5. Complete the Windows InstallShield Wizard

1. First, the **Welcome to the InstallShield Wizard for Nessus Agent** screen will be displayed. Click **Next** to continue.
2. On the **License Agreement** screen, read the terms of the **Tenable Network Security, Inc. Nessus Software License and Subscription Agreement**.
3. Click the **I accept the terms of the license agreement** radio button, and then click the **Next** button.
4. On the **Destination Folder** screen, click the **Next** button to accept the default installation folder. Otherwise, click the **Change** button to install Nessus to a different folder.

During this 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 click **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.

Unlike Mac and Unix installs, you will not have the option to **Name** your agent. Your agent's name will be the computer name where the agent is installed.

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

Step 6. Verify that your Agent is linked

1. In **Nessus**, click the gear icon .
2. View the linked agents on the **Scanners / Agents / Linked** page.

Nessus Agents can be deployed and linked using the command line interface.

Example:

> msiexec /i NessusAgent-<version number>-Win32.msi NESSUS_GROUPS="Agent Group Name" NESSUS_SERVER="192.168.0.1:8834" NESSUS_KEY=00abcd00000efgh11111i0k222lmopq3333st4455u66v777777w88xy9999zabc00 /qn

This completes the process of installing a **Nessus Agent** on the **Windows** operating system.

Upgrade Nessus and Nessus Agents

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

Nessus Upgrade

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

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. Click the pencil icon next to the **Activation Code**.
2. Select the **Registration** type.
3. Enter the new **Activation Code**.
4. Click **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.

Mac Upgrade

The process of upgrading Nessus on a Mac is the same process as a new Mac Install.

Unix: Upgrade

Step 1. Download Nessus Manager

From the Tenable Support Portal, download the latest, full-license version of Nessus Manager.

Step 2. 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-6.4.0-es6.i386.rpm
```

SUSE version 11

```
# rpm -Uvh Nessus-6.4.0-suse11.i586.rpm
```

Fedora version 20

```
# rpm -Uvh Nessus-6.4.0-fc20.x86_64.rpm
```

Ubuntu version 910

```
# dpkg -i Nessus-6.4.0-ubuntu910_i386.deb
```

Step 3. 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 **Unix** operating system.

Windows: Upgrade

Step 1. Download Nessus Manager

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

Examples: Nessus Installer Files

```
Nessus-6.4.0-Win32.msi
```

```
Nessus-6.4.0-x64.msi
```

Step 2. Start Nessus Installation

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

Step 3. Complete the Windows InstallShield Wizard

1. At the **Welcome to the InstallShield Wizard for Tenable Nessus** screen, click **Next**.
2. On the **License Agreement** screen, read the terms of the Tenable Network Security, Inc. Nessus Software License and Subscription Agreement.
3. Click the **I accept the terms of the license agreement** radio button, and then click the **Next** button.

4. On the **Destination Folder** screen, click the **Next** button to accept the default installation folder. Otherwise, click the **Change** button to install Nessus to a different folder.
5. On the **Ready to Install the Program** screen, click the **Install** button.

The **Installing Tenable Nessus** screen will be displayed and a **Status** indication bar will illustrate the upgrade progress.

On the **Tenable Nessus InstallShield Wizard Completed** screen click the **Finish** button.

After the **InstallShield Wizard** completes, the **Welcome to Nessus** page will load in your default browser; you can now log in to Nessus.

This completes the **Nessus** upgrade process on a **Windows** operating system.

Nessus Agents: Upgrade

Once installed, **Nessus Agents** are automatically updated by Nessus Manager or **Nessus Cloud**; there is no action required.

Remove Nessus and Nessus Agents

This section includes information for removing Nessus and Nessus Agents.

Nessus Removal

This section includes information for uninstalling and removing Nessus.

Mac Uninstall

Step 1. Stop Nessus

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

The **Status** becomes red and displays **Stopped**

5. Finally, exit the **Nessus.Preferences** screen.

Step 2. Remove the following Nessus directories, subdirectories, or files

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

Step 3. 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.

Unix: Uninstall

Step 1. OPTIONAL: Export your Scans and Policies

1. Go to the folder(s) where your Scans are stored.
2. Double-click on the Scan to view its Dashboard.
3. In the upper right corner, select the Export button, and then choose the Nessus .db file option.

Step 2. 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
```

Step 3. Determine Nessus Package Name

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 Nessus
   ```

   Debian/Kali and Ubuntu

   ```
   # dpkg -l | grep -i nessus
   ```

   FreeBSD

   ```
   # pkg_info   | grep -i nessus
   ```

Step 4. Remove Nessus

1. Using the package name identified, use the remove command specific to your Unix-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 Unix-style operating system, remove remaining files that were not part of the original installation.

Examples: Nessus Remove Command

Linux

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

FreeBSD

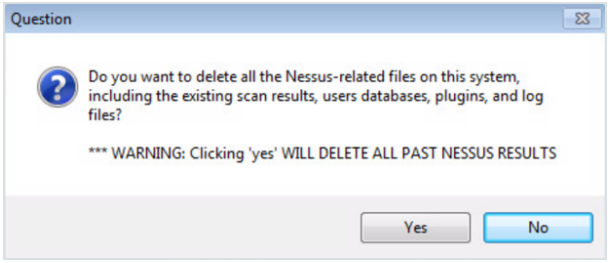
```
# rm -rf /usr/local/nessus/bin
```

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

Windows: Uninstall

Step 1. 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, click the **Uninstall** option.



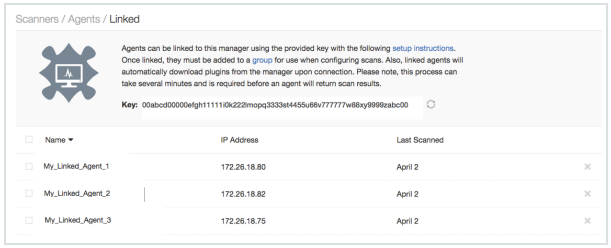
4. Click **Yes** to continue, otherwise click **No**.

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.

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.



1. In Nessus, click the gear icon .
2. Navigate to the **Scanners / Agents / Linked** page.
3. Click the X button next to the agent that you would like to delete.
4. On the **Remove Agent** screen, click the **Remove** button, otherwise, click **Cancel**.

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

If you are using a **Mac** or **Unix** 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.

Mac Agent Removal

Step 1. 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.

Step 2. Remove Nessus directories, sub-directories, and files

1. Using **Finder**, located and deleted the following items.

```
/Library/Nessus Agent
/Library/LaunchDaemons/com.tenablesecurity.nessusagent.plist
/Library/PreferencePanes/Nessus Agent Preferences.prefPane
/Applications/Nessus Agent
```

2. (Optional) To permanently delete these files and folders, empty the Mac's **Trash**.

Step 3. Disable the Nessus Agent service

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

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

2. If prompted, provide the administrator password.

This final step prevents Mac OS X from trying to start the now non-existent service.

This completes the process of uninstalling a **Nessus Agent** on the **Mac OS X** operating system.

Unix Agent Removal

OPTIONAL Step 1. Unlink Nessus Agent

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

```
nessuscli agent unlink
```

2. If prompted, provide the administrator password.

Step 2. 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 -i nessusagent
```

FreeBSD

```
# pkg_info | grep -i nessusagent
```

2. Using the package name identified, type the remove command specific to your Unix-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>
```

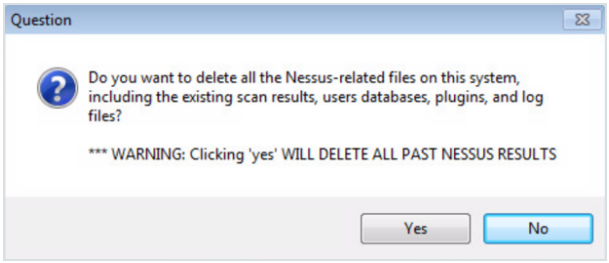
This completes the process of removing the **Nessus Agent** on the **Unix** operating systems.

Windows Agent Removal

Step 1. Remove Tenable 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, click the **Uninstall** option.

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



4. Click **Yes** to continue, otherwise click **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

Nessus Features

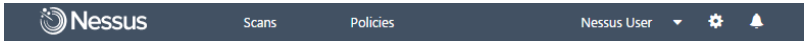
This section includes information about Nessus features, including Nessus Agents, which are available for use with Nessus Manager.

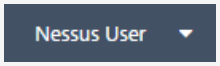
Unless otherwise noted, features apply to Nessus Manager and Nessus Professional.

Interface

Home Page

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



Item	Description
	When clicked, the **Nessus** logo links to the home page. The home page will always be your **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.
	The logged-in user's name is displayed. 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**.
	The gear icon  links you to the Nessus **Setting** pages: **Scanners**, **Accounts**, **Communication**, and **Advanced**. 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.

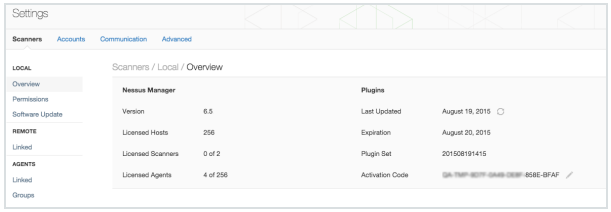
	When clicked, the bell icon  displays messages related to Nessus operations.

Nessus System Settings Page

When the gear icon is clicked, the Settings page is displayed.

The **Settings** page displays a top navigation menu that includes links to settings specific to **Scanners**, **Accounts**, **Communication**, and **Advanced** options, and the landing page displays the **Overview** for your **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** (Nessus Manager and Nessus Cloud only)
- Your **Plugin** last update
- Your **Plugin** expiration date
- The **Plugin** set identifier
- Your **Nessus Activation Code**



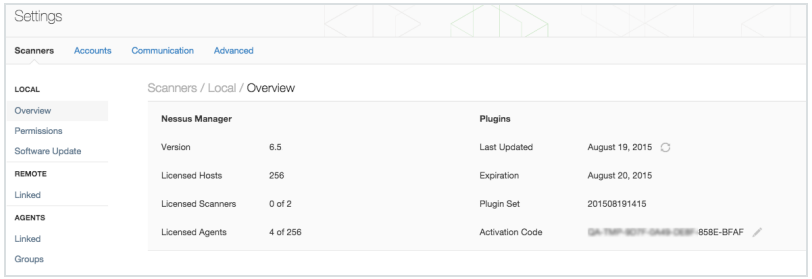
The pencil icon next to the **Activation Code** allows you to update your **Activation Code** as needed.

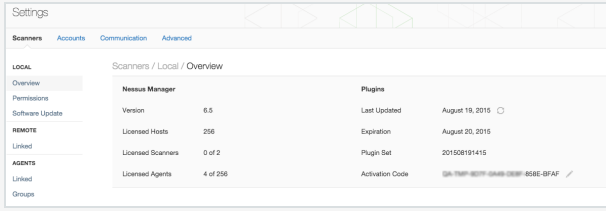
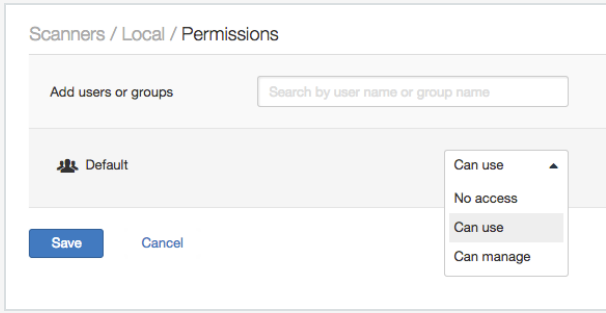
The **Scanners** default landing page displays the Nessus scanner's version and plugin information and software updates. In **Nessus Professional**, the navigation menu include **Overview**, **Link**, and **Software Update**.

In **Nessus Manager**, the navigation features also include **Remote** scanners and **Agents**.

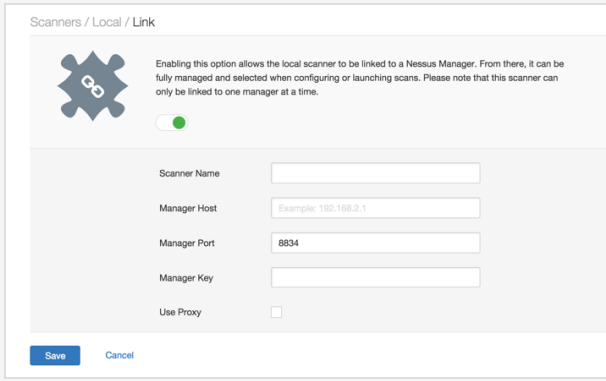
Scanners

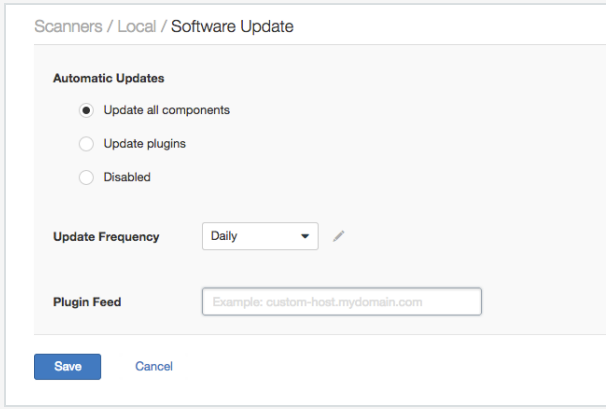
Based on product version, the **Scanners** navigation includes **Overview**, **Link** (Nessus Professional), **Software Update**, and in **Nessus Manager**, the navigation also includes **Remote** scanners and **Agents**.

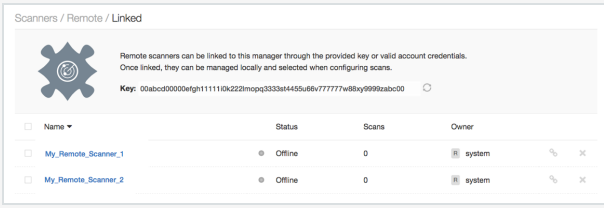


Setting Name	Description	Product Version(s)	User Type(s)	Image
LOCAL				
Overview	The overview page gives detailed information about the product version and plugins.	• Nessus Cloud • Nessus Manager • Nessus Professional	All User Types except Read Only	
Permissions	Users or groups are added to the permission page for no access, the ability to use, or the ability to manage the scanner. • No Access	• Nessus Manager • Nessus Professional	System Administrator	

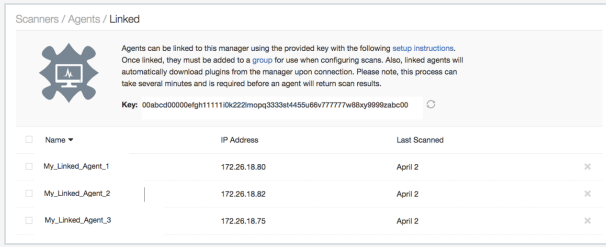
Setting Name	Description	Product Version(s)	User Type(s)	Image
	Any users or groups specified cannot view, use, or manage the Scanners. • Can Use Users or groups specified here can view and use the scanner; they will not be able to make any changes. • Can Manage Users or			

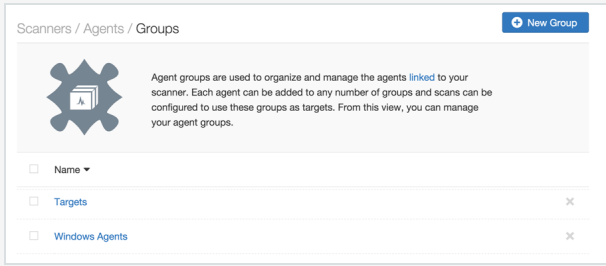
Setting Name	Description	Product Version(s)	User Type(s)	Image
	groups specified here can make changes to the Scanner's settings.			
Link	Enabling this option allows the local scanner to be linked to a Nessus Manager. From there, it can be fully managed and selected when configuring or launching scans.	• Nessus Professional	System Administrator	

Setting Name	Description	Product Version(s)	User Type(s)	Image
	Please note that this scanner can only be linked to one manager at a time.			
Software Update	Software updates can be configured for updating all components, plugins only, or disabled. The page also allows a custom host to be added for the plugin feed.	• Nessus Manager • Nessus Professional	System Administrator	
REMOTE				

Setting Name	Description	Product Version(s)	User Type(s)	Image
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 Cloud • Nessus Manager	System Administrator and Administrator	

AGENTS

Setting Name	Description	Product Version(s)	User Type(s)	Image
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	• Nessus Cloud • Nessus Manager	System Administrator	

Setting Name	Description	Product Version(s)	User Type(s)	Image
	the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.			
Groups	Agent groups are used to organize and manage the agents linked to your scanner. Each agent can be added to any	• Nessus Cloud • Nessus Manager	System Administrator	

Setting Name	Description	Product Version(s)	User Type(s)	Image
	number of groups and scans can be configured to use these groups as targets. From this view, you can manage your agent groups.			

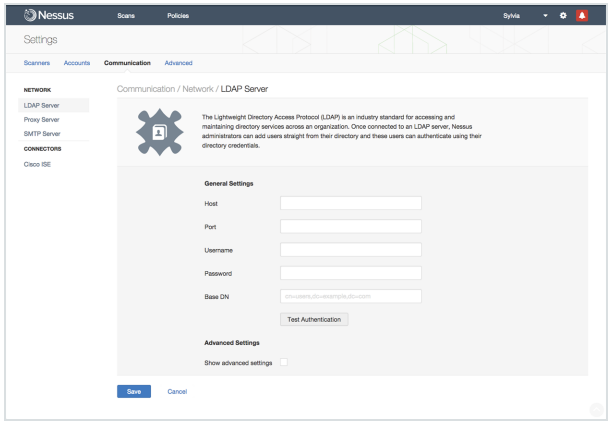
Accounts

Setting Name	Description	Product Version(s)	User Type(s)
Users	Individual Nessus accounts to be used for assigning permissions.	• Nessus Cloud • Nessus Manager • Nessus Professional	All User Types

Groups	Collections of users created for shared permissions.	• Nessus Cloud • Nessus Manager	System Administrator

Communication

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



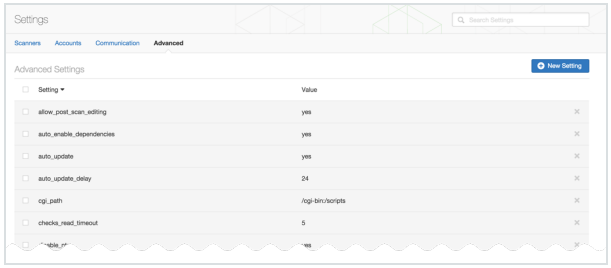
Setting Name	Description	Product Version(s)	User Type(s)
NETWORK			
LDAP	The Lightweight Directory Access Protocol (LDAP) is an industry standard for	• Nessus	System

Setting Name	Description	Product Version(s)	User Type(s)
Server	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.	Cloud • Nessus Manager • Nessus Professional	Administrator
Proxy Server	Proxy servers are used to forward HTTP requests. If your organization requires one, Nessus will use these settings to perform plugin updates and communicate with remote scanners. 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	• Nessus Cloud • 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 custom tailored through filters and require an HTML compatible email client.	• Nessus Cloud • Nessus Manager • Nessus	System Administrator

Setting Name	Description	Product Version(s)	User Type(s)
		Professional	
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 Only

Advanced Settings

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



- 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.

Setting Name	Description	Default
allow_post_scan_editing	Allows a user to make edits to scan results after the scan completes.	yes
auto_enable_dependencies	Automatically activate the plugins that are depended on. If disabled, not all plugins may run despite being selected in a scan policy.	yes
auto_update	Automatic plugin updates. 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.	yes
auto_update_	Number of hours to wait between two updates.	24

delay	Four (4) hours is the minimum allowed interval.	
cgi_path	During the testing of web servers, use this colon delimited list of CGI paths.	/cgi-bin:/scripts
checks_read_timeout	Read timeout for the sockets of the tests.	5
disable_ui	Disables the user interface on managed scanners.	no
disable_ntp	Disable the old NTP legacy protocol.	yes
disable_xmlrpc	Disable the new XMLRPC (Web Server) interface.	no
dumpfile	Location of a dump file for debugging output if generated.	C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.dump
global.max_hosts	Maximum number of simultaneous checks against each host tested.	2150
global.max_scans	If set to non-zero, this defines the maximum number of scans that may take place in parallel. Note: If this option is not used, no limit is enforced.	0
global.max_	Maximum number of simultaneous TCP sessions	50

simult_tcp_sessions	between all scans. Note: If this option is not used, no limit is enforced.	
global.max_web_users	If set to non-zero, this defines the maximum of (web) users who can connect in parallel. Note: If this option is not used, no limit is enforced.	1024
listen_address	IPv4 address to listen for incoming connections. If set to 127.0.0.1, this will restrict access to local connections only.	0.0.0.0
log_whole_attack	Log every detail of the attack? Helpful for debugging issues with the scan, but this may be disk intensive.	no
logfile	Location where the Nessus log file is stored.	C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.messages
max_hosts	Maximum number of hosts checked at one time during a scan.	5
max_checks	Maximum number of simultaneous checks against each host tested.	5
nasl_log_type	Direct the type of NASL engine output in nessusd.dump.	normal

nasl_no_ signature_ check	Determines if Nessus will consider all NASL scripts as being signed. Selecting “yes” is unsafe and not recommended.	no
nessus_udp_ scanner.max_ run_time	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.	31536000
non_simult_ ports	Specifies ports against which two plugins cannot not be run simultaneously.	139, 445, 3389
optimize_test	Optimize the test procedure. Changing this to “no” will cause scans to take longer and typically generate more false positives.	yes
plugin_upload	Designate if admin users may upload plugins.	yes
plugins_ timeout	Maximum lifetime of a plugin’s activity (in seconds).	320
port_range	Range of the ports the port scanners will scan. Can use keywords “default” or “all”, as well as a comma	default

	delimited list of ports or ranges of ports.	
purge_plugin_db	Determines if Nessus will purge the plugin database at each update. This directs Nessus to remove, re-download, and re-build the plugin database for each update. Choosing yes will cause each update to be considerably slower.	no
qdb_mem_usage	Directs Nessus to use more or less memory when idle. If Nessus is running on a dedicated server, setting this to “high” will use more memory to increase performance. If Nessus is running on a shared machine, settings this to “low” will use considerably less memory, but at the price of a moderate performance impact.	low
reduce_connections_on_congestion	Reduce the number of TCP sessions in parallel when the network appears to be congested.	no
report_crashes	Anonymously report crashes to Tenable.	yes When set to yes, Nessus crash information is sent to Tenable

		to identify problems. Personal nor system-identifying information is sent to Tenable.
rules	Location of the Nessus Rules file (nessusd.rules).	C:\ProgramData\Tenable\Nessus\conf\nessusd.rules
safe_checks	Safe checks rely on banner grabbing rather than active testing for a vulnerability.	yes
silent_ dependencies	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, Nessus will run those plugin dependencies, but will not include their output in the report. Setting this option to no will cause both the selected plugin, and any plugin dependencies to all appear in the report.	yes
slice_ network_ addresses	If this option is set, Nessus will not scan a network incrementally (10.0.0.1, then 10.0.0.2, then 10.0.0.3, and so on) but will attempt to slice the workload throughout the whole network (e.g., it will scan 10.0.0.1, then 10.0.0.127, then 10.0.0.2,	no

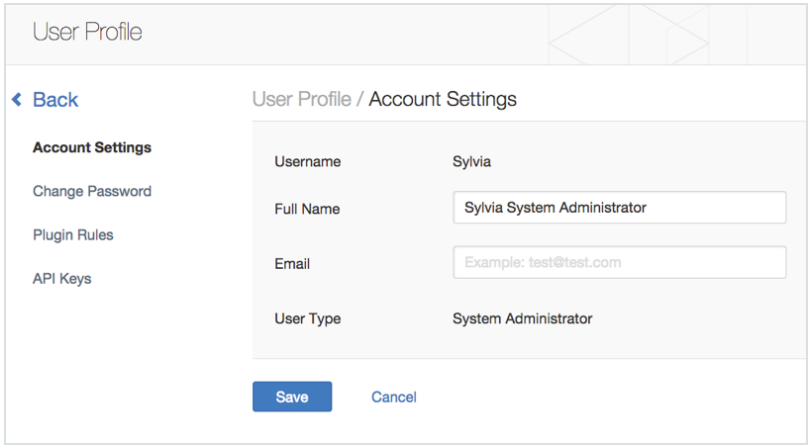
	then 10.0.0.128, and so on).	
ssl_cipher_list	Nessus only supports 'strong' SSL ciphers when connecting to port 8834.	strong
stop_scan_on_disconnect	Stop scanning a host that seems to have been disconnected during the scan.	no
stop_scan_on_hang	Stop a scan that seems to be hung.	no
throttle_scan	Throttle scan when CPU is overloaded.	yes
www_logfile	Location where the Nessus Web Server (user interface) log is stored.	C:\ProgramData\Tenable\Nessus\nessus\logs\www_server.log
xmlrpc_idle_session_timeout	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 will still apply. There is no maximum limit for this value.	30
xmlrpc_listen_port	Port for the Nessus Web Server to listen to (new XMLRPC protocol).	8834

User Profile

This section includes information about the currently-logged-in user's profile and profile settings.

User Profile / Account Settings

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



Based on your Nessus product, the following information is displayed.

Version	Settings
Nessus Cloud	Username (e-mail address) Full Name Email

	User Type Nessus Cloud accounts use the email address of the user for logins.
Nessus Manager	Username Full Name Email User Type
Nessus Professional	User Name User Type Nessus Professional user accounts do not have an associated email address. Nessus Professional has only two user types: System Administrator and Standard.

Change Password

The **User Profile / Change Password** page allows you to change the password.

The current user has the ability to change their own password, while administrators have the ability to change their own password and other user's passwords.

To change another user's password, the administrator selects the gear icon and navigates to the **Accounts / Users** 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.

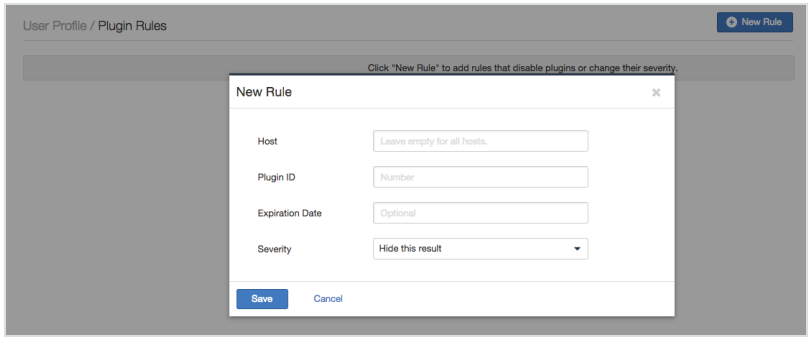
The **Plugin Rules** option provides a facility to create a set of rules that dictate the behavior of certain plugins related to any scan performed. A rule can be based on the **Host** (or all hosts), **Plugin ID**, an optional **Expiration Date**, and manipulation of **Severity**.

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

New Plugin Rule Example

This rule has been created for IP address 192.168.0.6. Once saved, this rule changes the results 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.

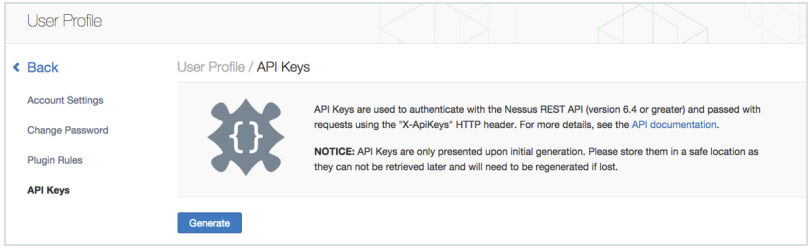
Click **New Rule** to add rules that disable plugins or change their severity.



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.



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

API Keys Warnings

- 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 will immediately un-authorize any applications currently utilizing the key.

Template Library

Nessus templates are used to facilitate the creation of **Scans** and **Policies**.

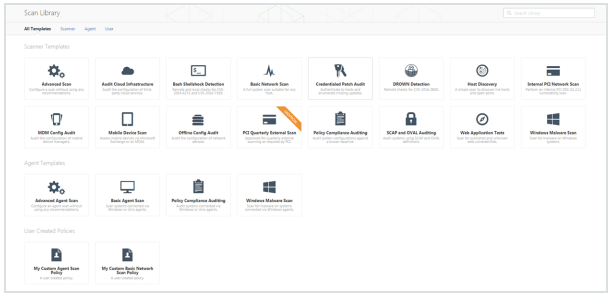
A **Scan** is the act of Nessus assessing a host for vulnerabilities, based on defined rules.

A **Policy** is a set of rules that defines what a scan does.

When a new Scan or a new Policy is created, the **Template Library** is displayed; each library contains **Scanner Templates**, and **Agent Templates**.

- **Policy Templates** and **Scanner Templates** share many settings and configuration options.
- **Scanner Templates** include settings regarding **Folder** location, **Dashboard** options, identification of **Scanners** and **Targets**, **Schedules**, and **Email Notifications**.

- **Policy Templates**do not include settings regarding **Folder** location, **Dashboard** options, identification of **Scanners** and **Targets**, **Schedules**, and **Email Notifications**.
- **Agent Templates**do not include **Credentials** options.



While the templates in each library are named identically, actual **Vulnerability Scanning** is performed by the creation and usage of a **Scan**, and the creation and usage of a **Policy** defines the rules by which those scans operate.

Contents of the Template Library changes as vulnerabilities are discovered.

Scanner Templates Names and Descriptions

Scanner Template Name	Scanner Template Description
Advanced Scan	Scan template for users who want total control of their scan or policy configuration.
Audit Cloud Infrastructure	Compliance specific template used for auditing the configuration of third-party cloud services.

Scanner Template Name	Scanner Template Description
Bash Shellshock Detection	Remote and credentialed checks for the Bash Shellshock vulnerability.
Basic Network Scan	For users scanning internal or external hosts.
Credentialed Patch Audit	Log in to systems and enumerate missing software updates.
DROWN Detection	Remote checks for CVE-2016-0800.
Host Discovery	Identifies live hosts and open ports.
Internal PCI Network Scan	For companies required to run an internal scan to meet Payment Card Industry Data Security Standards (PCI DSS) internal scanning requirements (11.2.1). In addition, Nessus Cloud is Tenable's Approved Scanning Vendor (ASV) solution for adherence to PCI DSS 11.2.2 external scanning requirements by performing vulnerability scans of Internet facing environments.
MDM Config Audit	Compliance specific template used for auditing the configuration of Mobile Device Managers (MDM).
Mobile Device Scan	For users of Apple Profile Manager, ADSI, MobileIron, or Good MDM.
Offline Config Audit	Compliance specific template used to upload and audit the config file of a network device.

Scanner Template Name	Scanner Template Description
PCI Quarterly External Scan	An approved policy for quarterly external scanning required by PCI. This is offered on Nessus Cloud only.
Policy Compliance Auditing	Compliance specific template used to audit system configurations against a known baseline provided by the user.
SCAP and OVAL Compliance Auditing	Compliance specific template used to audit systems using Security Content Automation Protocol (SCAP) and OVAL definitions.
Web Application Tests	For users performing generic web application scans.
Windows Malware Scan	For users searching for malware on Windows systems.

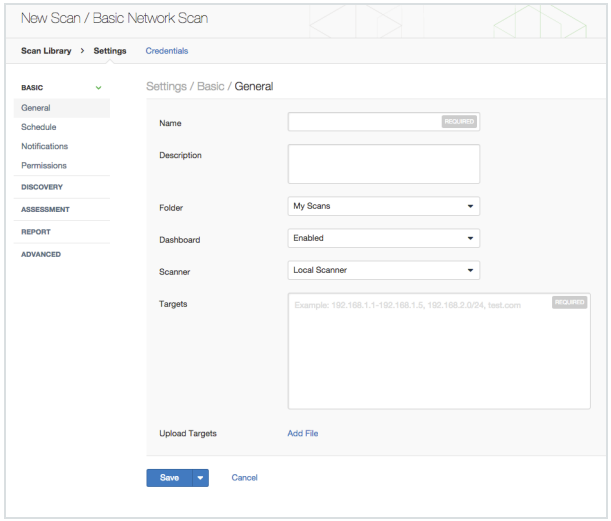
Scan Template Settings

When creating a **new Scan or a new Policy**, you'll notice that both share the following template settings:

- **Basic**
- **Discovery**
- **Assessment**
- **Report**

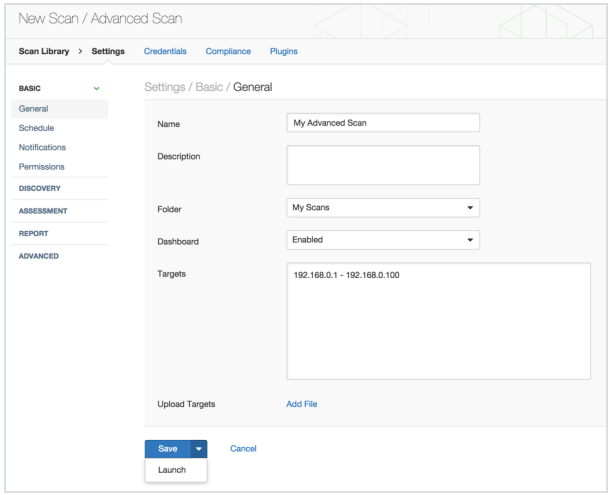
- **Advanced**
- **Credentials**

Basic Network Scan Template



Advanced Scan Template

Using the **Advanced Scan** template allows for total customization of your scan or policy settings.



Settings / Basic

Settings / Basic / General

Setting	Description
Name	Sets the name that will be displayed in the Nessus user interface to identify the scan.
Description	Optional field for a more detailed description of the scan.
Folder	The Nessus user interface folder to store the scan results.
Dashboard	Enable or disable scan dashboards. Dashboards are enabled for all new scans by default. However, they are disabled on existing or imported scans unless you enable them.

Targets	Valid Formats • A single IP address (e.g., 192.168.0.1) • An IP range (e.g., 192.168.0.1-192.168.0.255 or 192.168.0[4-10]) • A subnet with CIDR notation (e.g., 192.168.0.0/24) • A resolvable host (e.g., www.yourdomain.com) • A resolvable host with subnet (www.yourdomain.com/255.255.255.0) • A resolvable host with CIDR notation (www.yourdomain.com/24) • A single IPv6 address (e.g., link6%eth0, 2001:db8::2120:17ff:fe57:333b, fe80:0000:0000:0000:0216:cbff:fe92:88d0%eth0)
Upload Targets	A text file that includes targeted hosts. The host file must be formatted as ASCII text with one host per line and no extra spaces or lines. Unicode/UTF-8 encoding is not supported.

Settings / Basic / Schedule

Setting	Description
Launch	Sets Scan's launch interval

	• Once Schedule the scan at a specific time. • Daily Schedule the scan to occur on a daily basis, at a specific time or to repeat up to every 20 days. • Weekly Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks. • Monthly Schedule the scan to occur every month, by time and day or week of month, for up to 20 months. • Yearly Schedule the scan to occur every year, by time and day, for up to 20 years.
Starts On	Sets a fixed date and time for the initial launch to occur.
Time Zone	Sets the time zone for the launch's time settings.
Summary	Provides complete details about your scan's schedule configuration.

Settings / Basic / Notifications

Setting	Description
A SMTP Server is required and must be configured.	
Email Recipient(s)	Email addresses of users or distribution groups to receive Nessus notifications.
Result Filters	Defines the type of information to be emailed.

Settings / Basic / Permissions

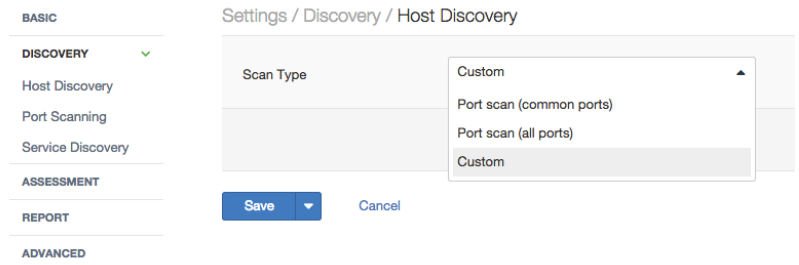
This option is only available in Nessus Manager; **Nessus Professional does not include these settings**.

Setting	Description
No Access	Only the user who created the policy can view, use, or edit the policy
Can View	Other users can view the scan results. They will not be able to control or configure the scan.
Can Control	Other users can control the scan (launch, pause, and stop) and view the scan results. They will not be able to configure the scan.
Can Configure	Other users can control the scan and configure the scan settings. They cannot delete the scan.

Settings / Discovery

The **Discovery** page controls options related to discovery and port scanning, including port ranges and methods.

Setting	Description
Scan Type	• Port scan (common ports) • Port scan (all ports) • Custom When **Custom** is selected, additional options become available: **Host Discovery**, **Port Scanning**, and **Service Discovery**.



Settings / Discovery / Host Discovery

Setting	Description
Ping the remote host	This option enables Nessus to ping remote hosts on multiple ports to determine if they are alive. When selected, this will enable other pinging options. To scan VMware guest systems, Ping the remote host must disabled.
General Settings	
Test the local Nessus host	If **Ping the remote host** is enabled, this option is enabled by default for this policy. This option allows you to include or exclude the local Nessus host from the scan. This is used when the Nessus host falls within the target network range for the scan.
Fast network discovery	If **Ping the remote host** is enabled, you will be able to see this option. By default, this option is not enabled. When Nessus pings a remote IP and receives a reply, it performs extra checks to make sure that it is not a transparent proxy or a load balancer that would return noise but no result (some devices answer to every port 1-65535 even when there is no service behind the device). Such checks can take some time, especially if the remote host is firewalled. If the fast network discovery option is enabled, Nessus will not perform these checks.

Ping Methods	
ARP	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.
TCP	Ping a host using TCP.
Destination ports (TCP)	Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that will be checked via TCP ping. If you are not sure of the ports, leave this setting to the default of built-in.
ICMP	Ping a host using the Internet Control Message Protocol (ICMP). 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 will consider the targeted host dead. This is to help speed up discovery on some networks. Note that some firewalls and packet filters use this same behavior for hosts that are up but are connecting to a port or protocol that is filtered. With this option enabled, this will lead to the scan considering the host is down when it is indeed up.

	Number of Retries (ICMP) allows you to specify the number of attempts to try to ping the remote host. The default is two attempts.
UDP	Ping a host using the User Datagram Protocol (UDP). UDP is a stateless protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.
Fragile devices	The Fragile Devices menu offers two options that instruct the Nessus scanner not to scan hosts that have a history of being fragile, or prone to crashing when receiving unexpected input. Use **Scan Network Printers** or **Scan Novell Netware hosts** to instruct Nessus to scan those particular devices. It is recommended that scanning of these devices be performed in a manner that allows IT staff to monitor the systems for issues.
Wake-on-LAN	The Wake-on-LAN (WOL) menu controls which hosts to send WOL magic packets to before performing a scan and how long to wait (in minutes) for the systems to boot. The list of MAC addresses for WOL is entered using an uploaded text file with one host MAC address

	per line. **Example WOL File Contents** 00:11:22:33:44:55 aa:bb:cc:dd:ee:ff
Network Type	Allows you to specify if you are using publicly routable IPs, private non-Internet routable IPs or a mix of these. Select Mixed if you are using RFC 1918 addresses and have multiple routers within your network.

Settings / Discovery / Port Scanning

Port scanning options define how the port scanner will behave and which ports to scan.

Setting	Description
Ports	
Consider Unscanned	If a port is not scanned with a selected port scanner (e.g., out of the range specified), Nessus will consider it closed.

Setting	Description
Ports as Closed	
Port Scan Range	• Keyword default instructs Nessus to scan approximately 4,790 common ports. The list of ports can be found in the nessus-services file. • Keyword all instructs Nessus instructs Nessus to scan all 65,536 ports, including port 0. • Keyword Custom List allows Nessus to use a custom range of ports by using a comma-delimited list of ports or port ranges. **Example: 21,23,25,80,110 or 1-1024,8080,9000-9200.** **Specifying 1-65535 will scan all ports.** You may also 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 specify T:1-1024,U:300-500. You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate protocol ("1-1024,T:1024-65535,U:1025"). If you are scanning a single protocol, select only that port scanner and specify the ports normally.

Setting	Description
	The range specified for a port scan will be applied to both TCP and UDP scans.
Local Port Enumerators	
SSH (netstat)	This option uses netstat to check for open ports from the local machine. It relies on the netstat command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.
WMI (netstat)	A WMI based scan uses netstat to determine open ports, thus ignoring any port ranges specified. If any port enumerator (netstat or SNMP) is successful, the port range becomes all. However, Nessus will still honor the consider unscanned ports as closed option if selected.
SNMP	If the settings are provided by the user (under Credentials), this will allow Nessus to 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.
Only run network port scanners if	Rely on local port enumeration first before relying on network port scans.

Setting	Description
local port enumeration failed	
Verify open TCP ports found by local port enumerators	If a local port enumerator (e.g., WMI or netstat) finds a port, Nessus will also verify 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	On some platforms (e.g., Windows and Mac OS X), selecting this scanner will cause Nessus to use the SYN scanner to avoid serious performance issues native to those operating systems.
SYN	Use Nessus' built-in SYN scanner to identify open TCP ports on the targets. SYN scans are a popular method for conducting port scans and generally considered to be a bit less intrusive than TCP scans, depending on the security monitoring device such as a firewall or Intrusion Detection System (IDS). The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines port state based on a reply, or lack of reply.

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

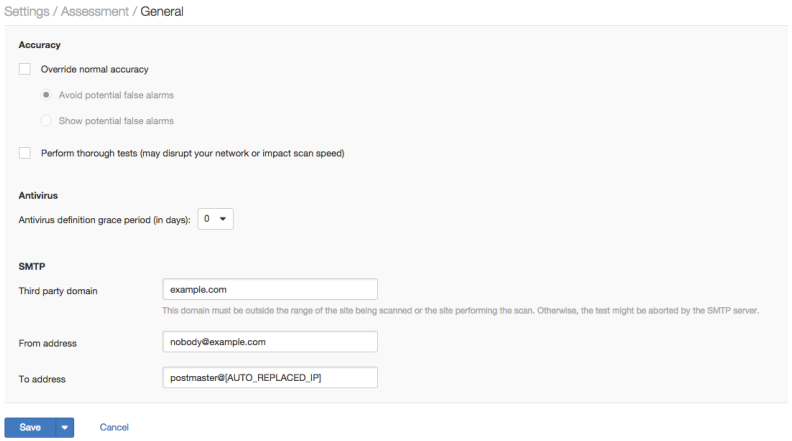
Settings / Discovery / Service Discovery

The Service Discovery page defines options that attempt to map each open port with the service that is running on that port.

There is a possibility that probing may disrupt servers or cause unforeseen side effects.

Setting	Description
General Settings	
Probe all ports to find services	Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.
Search for SSL based services	The Search for SSL based services controls how Nessus will test SSL based services. If toggled, choose between Known SSL ports (e.g., 443) and All ports. Testing for SSL capability on all ports may be disruptive for the tested host.
Search for SSL/TLS Services (enabled)	
Enumerate all SSL ciphers	When Nessus performs an SSL scan, it tries to determine the SSL ciphers used by the remote server by attempting to establish a connection with each different documented SSL cipher, regardless of what the server says is available.
Enable CRL checking (connects to Internet)	Direct Nessus to check SSL certificates against known Certificate Revocation Lists (CRL).

Settings / Assessment



Settings / Assessment / General

Option	Default	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	Disabled	Causes various plugins to work harder. For example, when looking through SMB file shares,

thorough tests (may disrupt your network or impact scan speed)		a plugin can analyze 3 directory levels deep instead of 1. This could cause much more network traffic and analysis in some cases. Note that by being more thorough, the scan will be 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 will consider signatures out of date regardless of how long ago an update was available (e.g., a few hours ago). This can be configured to allow for up to 7 days before reporting them out of date.
SMTP		
Third party domain	Nessus will attempt to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.	
From	The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this	

address	field.
To address	Nessus will attempt 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.

Settings / Assessment / Brute Force

Option	Default	Description
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.
Test default Oracle accounts (slow)	Disabled	Test for known default accounts in Oracle software.

Settings / Assessment / SCADA

Option	Description
Modbus/TCP	The Modbus/TCP Coil Access options are available for commercial users. This drop-down menu item is

Option	Description
Coil Access	dynamically generated by the SCADA plugins available with the commercial version of Nessus. 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. The defaults for this are 0 for the Start reg and 16 for the End reg.
ICCP/COTP TSAP Addressing Weakness	The ICCP/COTP TSAP Addressing menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values. The start and stop values are set to 8 by default.

Settings / Assessment / Web Applications

Option	Default	Description
General		
Use the cloud to take	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

Option	Default	Description
screenshots of public webservers		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 will impersonate while scanning.
Web Crawler		
Start crawling from	/	The URL of the first page that will be 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	Enable exclusion of portions of the web site 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

Option	Default	Description
		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 will follow for each start page.
Follow dynamic pages	Disabled	If selected, Nessus will follow dynamic links and may exceed the parameters set above.
Application Test Settings		
Enable generic web application testss	Disabled	Enables the options listed below.

Option	Default	Description
Abort web application tests if HTTP login fails	Disabled	If Nessus cannot login to the target via HTTP, then do not run any web application tests.
Try all HTTP methods	Disabled	This option will instruct Nessus to also use POST requests for enhanced web form testing. By default, the web application tests will 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 will test each script/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 supplying the same variable with valid content as well. For example, a normal SQL injection test may look like /target.cgi?a='&b=2. With HTTP Parameter Pollution (HPP) enabled, the request may look like /target.cgi?a='&a=1&b=2.

Option	Default	Description
Test embedded web servers	Disabled	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.
Test more than one parameter at a time per form	Disabled	This option 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 /test.php?arg1=XSS&b=1&c=1 where b and c allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This drop-down has four options: **Test random pairs of parameters** – This form of testing will randomly check 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

Option	Default	Description
		efficient than the one value test. While testing multiple parameters, it will test an attack string, variations for a single variable and then use the first value for all other variables. For example, Nessus would attempt /test.php?a=XSS&b=1&c=1&d=1 and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for /test.php?a=XSS&b=3&c=3&d=3 when the first value of each variable is 1. **Test random combinations of three or more parameters (slower)** – This form of testing will randomly check a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Note that increasing the amount of combinations by three or more increases the web application test time. **Test all combinations of parameters (slowest)** – This method of testing will do a fully exhaustive test of 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	Disabled	This option determines when a new flaw is targeted. This applies at the script level;

Option	Default	Description
after first flaw is found per web page		finding an XSS flaw will not disable searching for SQL injection or header injection, but you will have at most one report for each type on a given port, unless thorough tests is set. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported sometimes, if they were caught by the same attack. The drop-down has four options: **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, or the next known CGI, or to the next port/server. **Look for all flaws (slowest)** – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.
URL for	http://rfi.nessus.org/rfi.txt	During Remote File Inclusion (RFI) testing, this option specifies a file on a remote host to

Option	Default	Description
Remote File Inclusion		use for tests. By default, Nessus will use a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended 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 web site. Scanning the local network for web sites with small applications will typically complete in under an hour, however web sites with large applications may require a higher value.

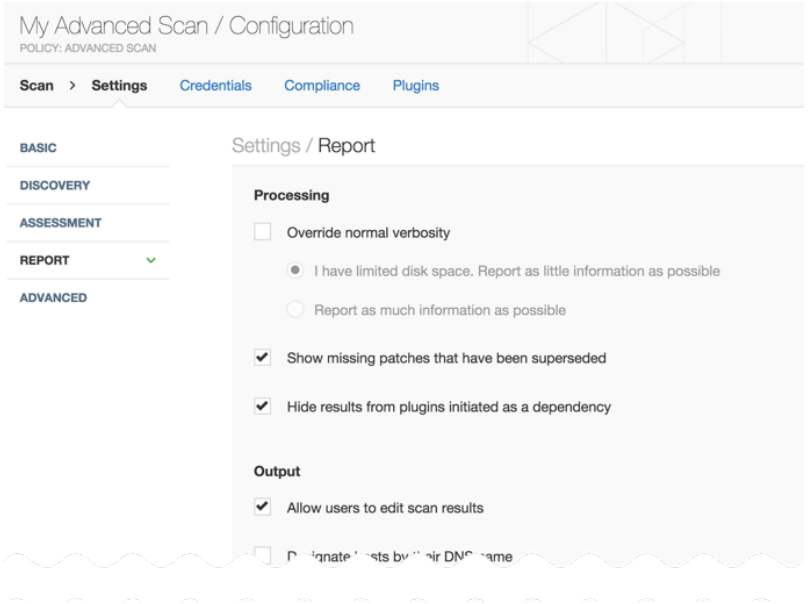
Settings / Assessment / Windows

Option	Description
General Setting	
Request information about the SMB Domain	If the option **Request information about the domain** is set, then domain users will be queried instead of local users.
Enumerate Domain Users	

Start UID	1000
End UID	1200
Enumerate Local User	
Start UID	1000
End UID	1200
Malware Files	
Provide your own list of known bad MD5 hashes	Additional known bad MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target and a description was provided for the hash the description will show up in the scan results. Standard hash-delimited comments (e.g., #) can optionally be used in addition to the comma-delimited ones.
Provide your own list of known good MD5 hashes	Additional known good MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, and a description was provided for the hash, the description will show up in the scan results. Standard hash-delimited comments (e.g., #) can optionally be used in addition to the comma-delimited ones.
Hosts file whitelist	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
Malware Settings	
Disable DNS Resolution	Checking this option will prevent Nessus from using the cloud to compare scan findings against known malware.

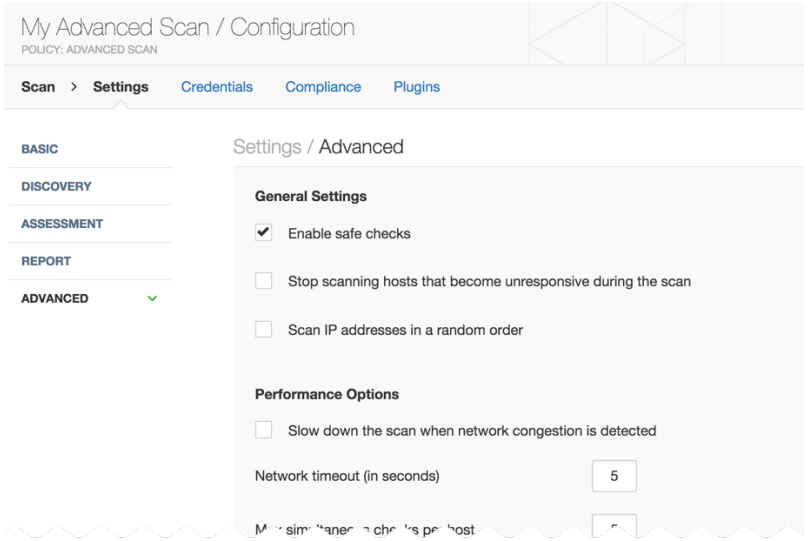
Settings / Report



Option	Default	Description
Processing		
Override normal verbosity	Disabled	"I have limited disk space. Report as little information as possible will provide less information about plugin activity in the report to minimize impact on disk space. "Report as much information as possible will provide more information about plugin activity in the report.
Show missing patches that have been superseded	Enabled	This option allows you to configure Nessus to include or remove superseded patch information in the scan report. This option is off by default, except for policies created using the Internal PCI Network Scan template in the Policy Library.
Hide results from plugins initiated as a dependency	Enabled	If this option is checked, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, uncheck the box.
Output		
Allow users to edit scan results	Enabled	This feature allows users to delete items from the report when checked. When performing a scan for regulatory compliance or other types of audits, uncheck this to show that the scan was not tampered with.

Option	Default	Description
Designate hosts by their DNS name	Disabled	Use the host name rather than IP address for report output.
Display hosts that respond to ping	Disabled	Select this option to specifically report on the ability to successfully ping a remote host.
Display unreachable hosts	Disabled	If this option is selected, hosts that did not reply to the ping request will be included in the security report as dead hosts. Do not enable this option for large IP blocks.

Scan Setting / Advanced



Option	Default	Description
General Settings		
Enable Safe Checks	Enabled	Enable Safe Checks disables all plugins that may have an adverse effect on the remote host.
Stop scanning hosts that become	Disabled	If checked, Nessus will stop 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 (e.g., IDS) has begun to block traffic to a server. Continuing scans on these machines will send unnecessary traffic across the network

Option	Default	Description
unresponsive during the scan		and delay the scan.
Scan IP addresses in a random order	Disabled	By default, Nessus scans a list of IP addresses in sequential order. If checked, Nessus will scan the list of hosts in a random order. This is typically useful in helping to distribute the network traffic directed at a particular subnet during large scans. Before July 2013, this option worked on a per-subnet basis. This feature has since been enhanced to randomize across the entire target IP space.
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 will automatically attempt to use the available space within the network pipe again.
Network timeout (in	5	Set to five seconds by default. This is 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

Option	Default	Description
seconds)		may wish to set this to a higher number of seconds.
Max simultaneous checks per host	5	This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time.
Max simultaneous hosts per scan	5	This setting limits the maximum number of hosts that a Nessus scanner will scan at the same time.
Max number of concurrent TCP sessions per host	none	This setting limits the maximum number of established TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner will eventually send (e.g., if this option is set to 15, the SYN scanner will send 1500 packets per second at most).
Max number of concurrent TCP sessions	none	This setting limits the maximum number of established TCP sessions for the entire scan, regardless of the number of hosts being scanned. For Nessus scanners installed on Windows XP, Vista, 7, and 8 hosts, this value must be set to

Option	Default	Description
per scan		19 or less to get accurate results.
Debug Settings		
Log scan details to server	Disabled	Logs the start and finish time for each plugin used during a scan to nessusd.messages.
Enable plugin debugging	Disabled	Attaches available debug logs from plugins to the vulnerability output of this scan

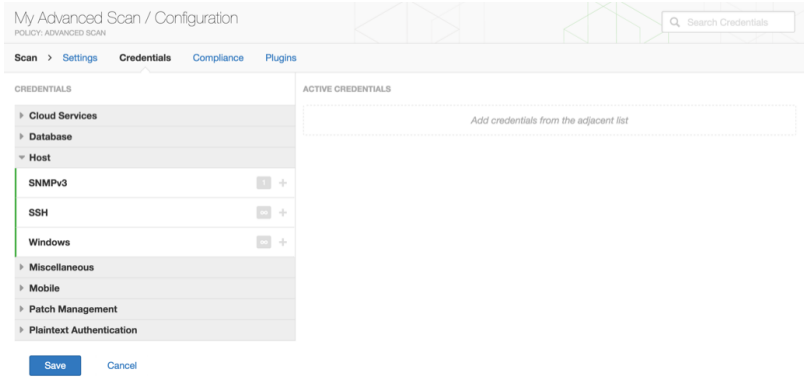
Scan Credentials Settings

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.

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, 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.



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 policy:

- Database, which includes MongoDB, Oracle, MySQL, DB2, PostgreSQL, and SQL Server
- Cloud Services, which includes Amazon Web Services (AWS), Microsoft Azure, Rackspace, and Salesforce.com
- Host, which includes Windows logins, SSH, and SNMPv3

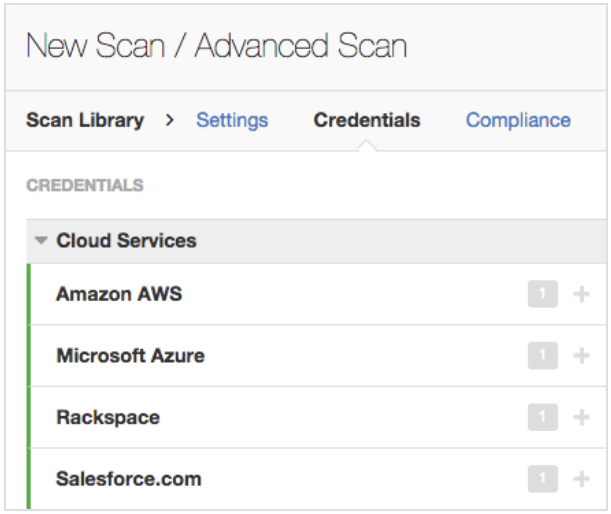
- Mobile Device Management
- Patch Management servers
- VMware, Red Hat Enterprise Virtualization (RHEV), IBM iSeries, Palo Alto Networks PAN-OS, and directory services (ADSI and X.509)
- Plaintext authentication mechanism including FTP, HTTP, POP3, and other services

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 that Nessus is configured to use. The more privileges the scanner has via the login account (e.g., root or administrator access), the more thorough the scan results.

Nessus will open several concurrent authenticated connections to carry out credentialed auditing to ensure it is done in a timely fashion. Ensure that the host being audited does not have a strict account lockout policy based on concurrent sessions.

Cloud Services

Nessus supports Amazon AWS, Microsoft Azure, Rackspace, and Saleforce.com.



Amazon 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.

Amazon AWS Global Settings

Option	Default	Description
Regions to access	Rest of the World	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: • 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	Enabled	Verify the validity of the SSL digital certificate.

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.

Option	Description
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 three forms of host authentication: SNMPv3, Secure Shell (SSH), and Windows.

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

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.

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 Global Settings for SSH credentials that apply to all SSH Authentication methods.

Option	Default	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 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.

Authentication Options

Option	Description
Authentication method	Nessus supports five types of authentication methods for use with SSH. Options • Public Key • Certificate • CyberArk Vault

Option	Description
	• Kerberos • Password
Username	Username of the account that is being used for authentication on the host system.
Private Key	RSA or DSA Open SSH key file of the user. Only RSA and DSA OpenSSH keys are supported
Private key passphrase	Passphrase of the Private Key.
Elevate privileges with	Allows for increasing privileges once authenticated. Options • .k5login • Cisco • dzdo • pbrun • su

Option	Description
	• su+sudo • sudo

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.

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.

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.

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 of the Private Key.

Option	Description
passphrase	
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.

Option	Description
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 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 that 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 Transport	The KDC uses TCP by default in Unix implementations. For UDP, change this option. Note that if you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.
Realm	The Realm is the authentication domain, usually noted as the domain name of the target (e.g., example.com).
Elevate	Allows for increasing privileges once authenticated.

Option	Description
privileges with	

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.

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.

Windows

The Windows credentials menu item has settings to provide Nessus with information such as SMB account name, password, and domain name. Nessus supports several different types of authentication methods for Windows-based systems:

- 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 2008, Windows 2008 R2, Windows 2012, and Windows 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.

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. For more information, you can read the Tenable blog post titled Dynamic Remote Registry Auditing - Now you see it, now you don't!. This service must be started for a Nessus credentialed scan to fully audit a system using credentials.

http://www.tenable.com/blog/real-time-situational-awareness-never-say-i-don-t-know

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	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

Option	Default	Description
authentication		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.

Authentication Methods

Option	Description
Windows Authentication Methods	Options: Password, CyberArk, Kerberos, LM Hash, and NTLM Hash
Username	The target system's username.
Password	Password of the username specified.
Domain	The Windows domain of the specified user's name.

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	The CyberArk Central Credential Provider IP/DNS address.

Option	Description
Host	
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.
Valut 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.

Option	Description
PolicyId	The PolicyID assigned to the credentials you would like to retrieve from the CyberArk Central Credential Provider.
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to 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

Option	Default	Description
		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.

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	Name of the domain controller for

Option	Description
Controller	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.

RHEV (Red Hat Enterprise Virtualization)

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.
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.

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

Credential	Description
Certificate	

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.

Patch Management

Nessus Manager and Nessus Cloud 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.

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.

Option	Default	Description
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 fiel
K1000 Database Password	none	Password required to authenticate the K1000 Database Username. This is a required field.

IBM Tivoli Endpoint Manager (BigFix)

Tivoli Endpoint Manager (TEM) is available from IBM to manage the distribution of updates and hotfixes 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

Option	Default	Description
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 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

Credential	Description
Domain	The domain the SCCM server is a part of
Username	SCCM admin username
Password	SCCM admin password

Microsoft 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, 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 57066)
- Patch Management: Red Hat Satellite Server Get Installed Packages (Plugin ID 57065)
- Patch Management: Red Hat Satellite Server Get Managed Servers (57064)
- Patch Management: Red Hat Satellite Server Get System Information (Plugin ID 57067)
- Patch Management: Red Hat Satellite Server Settings (Plugin ID 57063)

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_	The name of the MSSQL database that manages Altiris patch information.

Credential	Default	Description
	CMDB	
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.

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
- IBM TEM
- Microsoft WSUS

- Microsoft SCCM
- Red Hat Network Satellite
- Dell KACE 1000
- 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.

Plaintext Authentication

> Using cleartext 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, by configuring the Plaintext Authentication drop-down menu item.

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 here will be used for Basic and Digest authentication only.

Credentials for FTP, IPMI, NNTP, POP2, and POP3 are username and password only.

FTP

Username and Password are the only required credentials.

IPMI

Username and Password are the only required credentials.

NNTP

Username and Password are the only required credentials.

POP2

Username and Password are the only required credentials.

POP3

Username and Password are the only required credentials.

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.
Use authenticated regex on HTTP headers	Disabled	The regex searches are case sensitive by default. This instructs Nessus to ignore case.

Authentication methods

Automatic authentication

Username and Password Required

Basic/Digest authentication

Username and Password Required

HTTP Login Form

The HTTP login page settings provide control over where authenticated testing of a custom web-based application begins.

Option	Description
Username	Login user's name.
Password	Password of the user specified.
Login page	The absolute path to the login page of the application, e.g., /login.html.
Login submission page	The action parameter for the form method. For example, the login form for <form method="POST" name="auth_form" action="/login.php"> would be /login.php.
Login parameters	Specify the authentication parameters (e.g., login=%USER%&password=%PASS%). If the keywords %USER% and %PASS% are used, they will be substituted with values supplied on the Login configurations drop-down

Option	Description
	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 page	The absolute path of a protected web page that requires authentication, to better assist Nessus in determining authentication status, e.g., /admin.html.
Regex to verify successful authentication	A regex pattern to look for on the login page. Simply receiving a 200 response code is not always sufficient to determine session state. Nessus can attempt to match a given string such as Authentication successful!

HTTP cookies import

To facilitate web application testing, Nessus can import HTTP cookies from another piece of software (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.

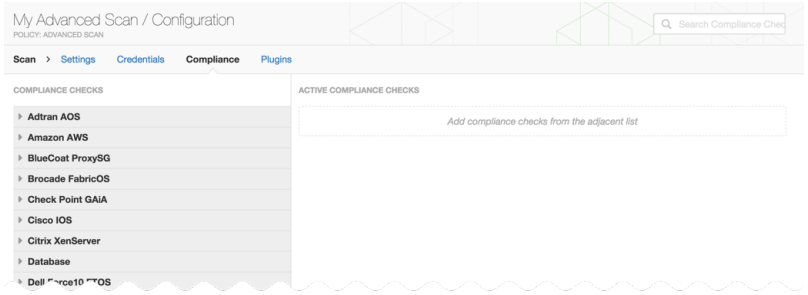
telnet/rsh/rexec

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.

Scan Compliance Settings



Compliance Policy	Required Credentials	Description
Adtran AOS	SSH	An option that allows a system or policy file to be specified to test Adtran AOS based devices against compliance standards.
Amazon AWS	SSH	An option that allows a system to be specified to test the AWS account configuration against compliance standards.
Blue Coat	SSH	An option that allows a system to be specified to test Blue Coat ProxySG devices

Compliance Policy	Required Credentials	Description
ProxySG		against compliance standards.
Brocade FabricOS		An option that allows a system or policy file to be specified to test Brocade FabricOS based devices against compliance standards.
Check Point GAiA	SSH	An option that allows a system to be specified to test Check Point GAiA based devices against compliance standards.
Cisco IOS	SSH	An option that allows a device or policy file to be specified to test Cisco IOS based devices against compliance standards. + In addition to being able to upload your own .audit files, there are also DISA STIG and other best practices files available.
Citrix XenServer	SSH	A commercial option that allows a system to be specified to test Citrix XenServers against compliance standards
Database	Database credentials	An option that allows a policy file to be specified to test databases such as DB2, SQL Server, MySQL, and Oracle against compliance standards.
Dell Force10 FTOS	SSH	An option that allows a system or policy file to be specified to test Dell Force10 FTOS based devices against compliance standards.
Extreme	SSH	An option that allows a system or policy file to be specified to test Extreme

Compliance Policy	Required Credentials	Description
ExtremeXOS		ExtremeXOS based devices against compliance standards.
FireEye	SSH	An option that allows a system or policy file to be specified to test FireEye devices against compliance standards.
Fortigate FortiOS	SSH	An option that allows a system or policy file to be specified to test Fortigate FortiOS based devices against compliance standards.
HP ProCurve	SSH	An option that allows a system or policy file to be specified to test HP ProCurve devices against compliance standards.
Huawei	SSH	An option that allows a device or policy file to be specified to test Huawei VRP based devices against compliance standards.
IBM iSeries	IBM iSeries	An option that allows a policy file to be specified to test IBM iSeries systems against compliance standards.
Juniper Junos	SSH	An option that allows a device or policy file to be specified to test Juniper Junos devices against compliance standards.
MongoDB	MongoDB	An option that allows a system or policy file to be specified to test MongoDB systems against compliance standards.

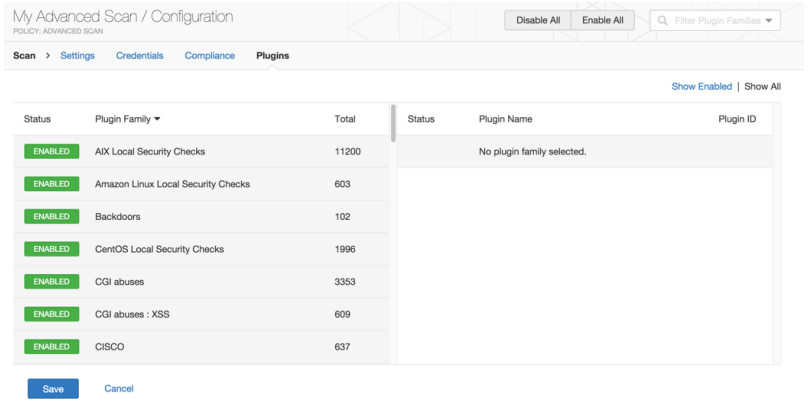
Compliance Policy	Required Credentials	Description
NetApp Data ONTAP	SSH	An option that allows a system or policy file to be specified to test NetApp Data ONTAP devices against compliance standards.
Palo Alto Networks PAN-OS	PAN-OS	An option that allows a system to be specified to test Palo Alto Networks PAN-OS devices against compliance standards.
RHEV	RHEV	An option that allows a system to be specified to test Red Hat Enterprise Virtualization devices against compliance standards.
Salesforce.com	Salesforce SOAP API	An option that allows a system to be specified to test Salesforce applications against compliance standards.
SonicWALL SonicOS	SSH	An option that allows a system or policy file to be specified to test SonicWALL SonicOS devices against compliance standards.
Unix	SSH	An option that allows a policy file to be specified to test Unix systems against compliance standards.
Unix File Contents	SSH	The Unix File Contents Compliance Checks menu allows users to upload Windows-based audit files that search a system for a specific type of content (e.g., source code errors, credit cards, Social Security numbers) to help determine compliance with

Compliance Policy	Required Credentials	Description
		corporat
VMware vCenter/vSphere	VMware ESX SOAP API or VMware vCenter SOAP API	An option that allows a system to be specified to test VMware devices against compliance standards.
Windows	Windows	An option that allows a policy file to be specified to test Windows systems against compliance standards.
Windows File Contents	Windows	The Windows File Contents Compliance Checks menu allows users to upload Windows-based audit files that search a system for a specific type of content (e.g., credit cards, Social Security numbers) to help determine compliance with corporate regulations or third-party standards

Scan Plugins Settings

The **Advanced Scan** templates include **Plugin** options.

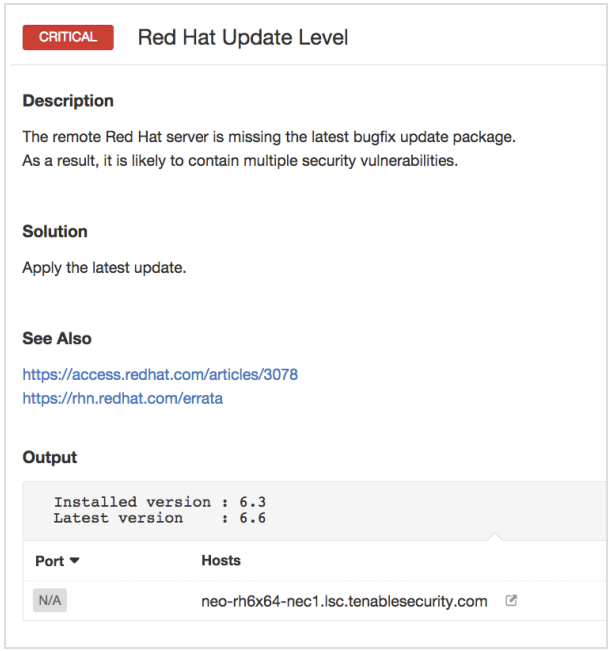
The **Plugins** menu enables you to select security checks by Plugin Family or individual checks.



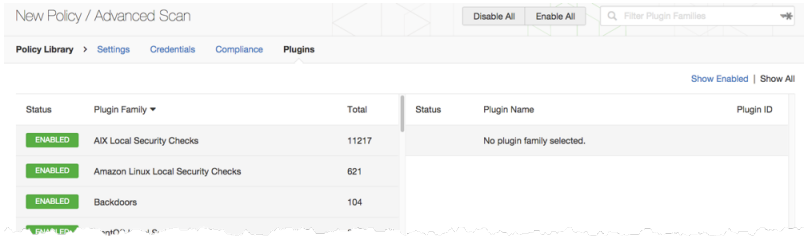
Clicking on the plugin family allows you to enable (green) or disable (grey) the entire family. Selecting a family will display the list of its plugins. Individual plugins can be enabled or disabled to create very specific scan policies.

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.

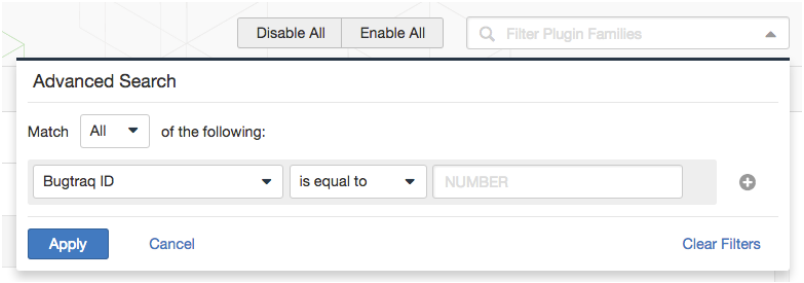
Selecting a specific plugin will display the plugin output that will be displayed as seen in a report. The synopsis and description will provide more details of the vulnerability being examined. Scrolling down in your browser will also show solution information, additional references if available, risk information; exploit information, and any vulnerability database or informational cross-references.



At the top of the plugin family page, you can create filters to build a list of plugins to include in the policy, as well as disable or enable all plugins. Filters allow granular control over plugin selection. Multiple filters can be set in a single policy.



To create a filter, click the Filter Plugin Families drop-down arrow.



Each filter created provides several options for refining a search. The filter criteria can be based on Any, where any one criteria will return matches, or All, where every filter criteria must be present. For example, if we want a policy that only includes plugins that have an exploit or can be exploited without a scripted exploit, we create two filters and select Any for the criteria.

> To use filters to create a policy, it is recommended you start by disabling all plugins. Using plugin filters, narrow down the plugins you want to be in your policy. Once completed, select each plugin family and click Enable Plugins.

When a 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.

The Denial of Service family contains some plugins that could cause outages on a network if the Safe Checks option is not enabled, but does contain 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.

Agent Templates

Agent Template Name	Agent Template Description
Advanced Agent Scan	Allows you to create and manually configure a customized **Agent Scan**.
Basic Agent Scan	Scans systems connected to Windows or Unix agents.
Policy Compliance Auditing	Used for auditing systems connected via Windows or Unix agents.
Windows Malware Scan	Scans for malware on systems connected via Windows agents.

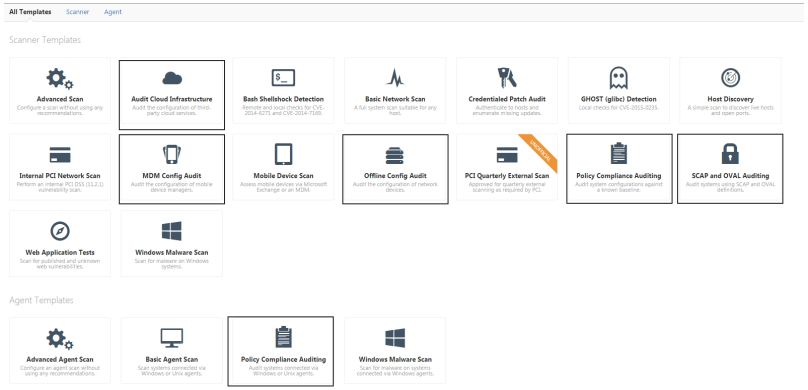
Special Use Templates

Compliance

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

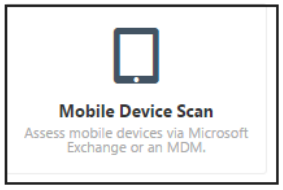
- Audit Cloud Infrastructure
- MDM Config Audit
- Offline Config Audit

- SCAP and OVAL Auditing
- Policy Compliance Auditing



Mobile Device

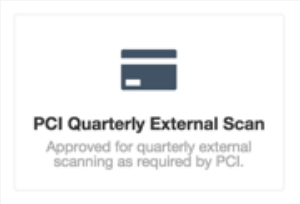
With Nessus Manager, the Nessus Mobile Devices plugin family provides the ability to obtain information from devices registered in a Mobile Device Manager (MDM) and from Active Directory servers that contain information from Microsoft Exchange Servers.

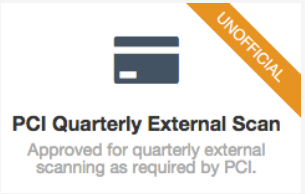
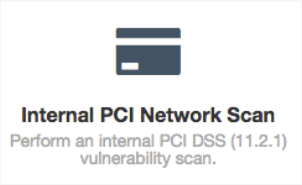


- To query for information, the Nessus scanner must be able to reach the Mobile Device Management servers. You must ensure no screening devices block traffic to these systems from the Nessus scanner. In addition, Nessus must be given administrative credentials (e.g., domain administrator) to the Active 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.

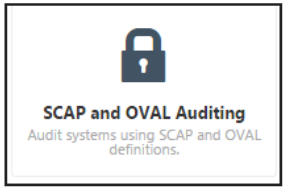
Payment Card Industry (PCI)

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
	Nessus Cloud Only	The PCI Quarterly External Scan template is only available in **Nessus Cloud**. Using this template, **Nessus Cloud** tests for all PCI DSS external scanning requirements, including web applications. The scan results obtained using the **PCI Quarterly External Scan** template may be submitted to Tenable (an Approved Scanning Vendor)for PCI

		validation. Refer to the Scan Results section for details on creating, reviewing, and submitting PCI scan results.
	**Nessus Manager** **Nessus Professional**	For Nessus Manager and Nessus Professional versions, Tenable provides the **PCI Quarterly External Scan (Unofficial)** template. 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 for PCI Validation. The PCI Quarterly External Scan (Unofficial) Template performs the identical scanning functions as the **Nessus Cloud** version of this template.
	**Nessus Manager** **Nessus Professional**	The **Internal PCI Network Scan** template can be used to meet **PCI DSS** Internal scanning requirement (11.2.1).

SCAP and OVAL

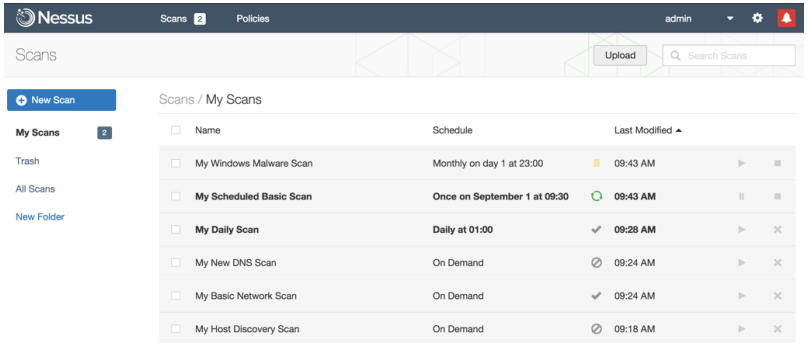


The National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) is a set of policies for managing vulnerabilities and policy compliance in government agencies. It relies on multiple open standards and policies, including OVAL, CVE, CVSS, CPE, and FDCC policies.

- 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.

Scans Page

The **Nessus** home screen will always display your **Scans / My Scans** page.



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

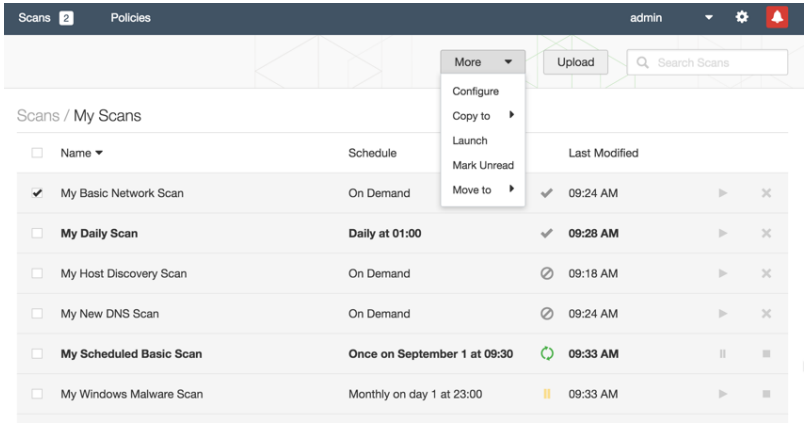
Scan Folders

- 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 will appear and additional options for the selected scan becomes available.

- Configure
- Copy to

- Launch
- Mark Unread
- Move to



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 Reports

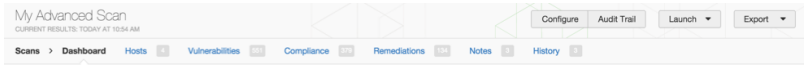
This section includes information about Nessus Reports:

- Report navigation
- Report pages
- Dashboards

- Report filters
- Report screenshots
- Scan knowledgebase
- Comparing reports

Report Navigation

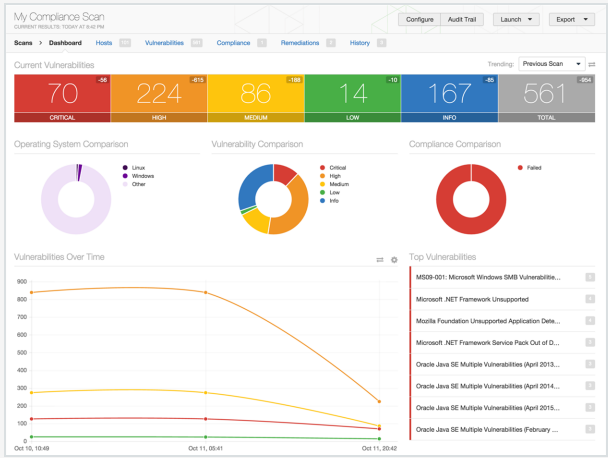
Based on permissions and the scan's actions, you can **Configure** the scan, search the scan's **Audit Trail**, **Launch** the scan, or **Export** the scan's results.

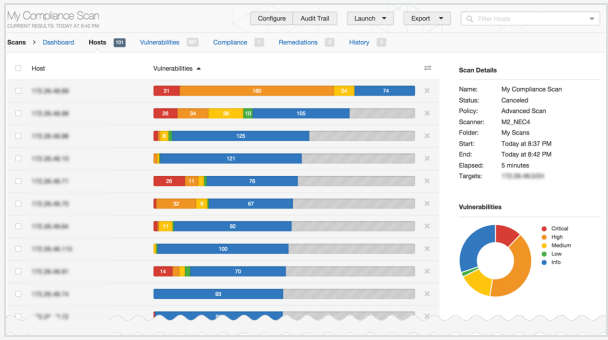
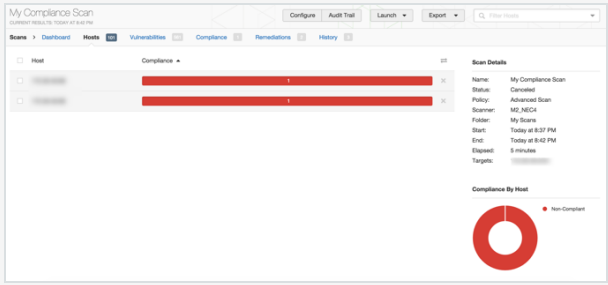


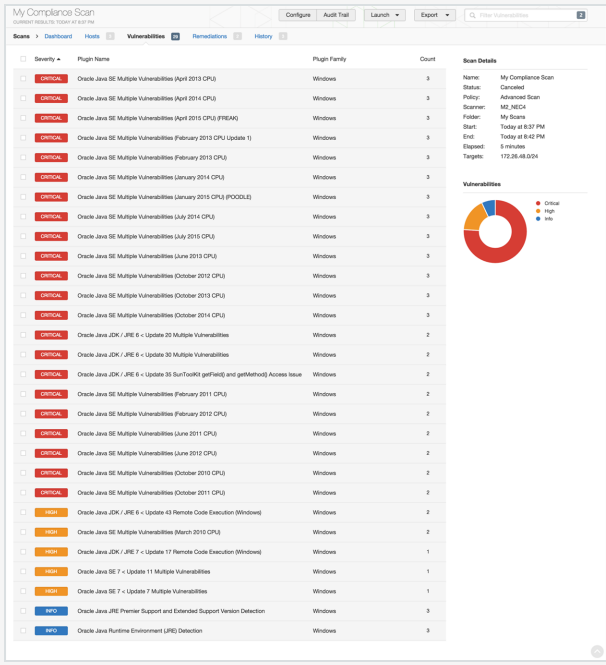
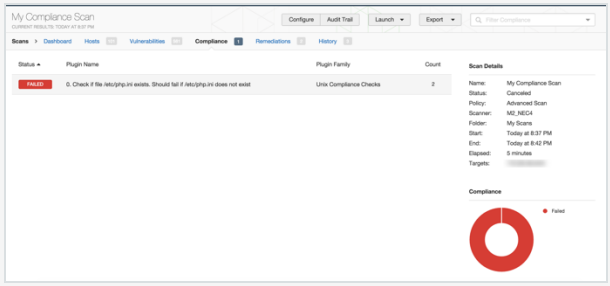
Option	Description
Configure	Navigates you back to the scan's configuration settings.
Audit Trail	Displays the audit trail dialogue.
Launch	Display two choices to launch a scan: Default and Custom. • Default: This option uses the scan's pre-configured settings. • Custom: This options allows for **Customer Scan Targets**.

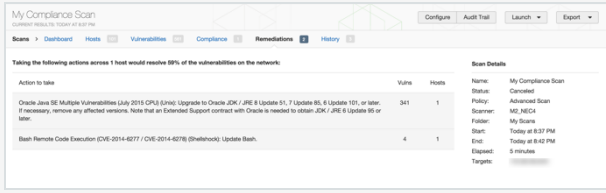
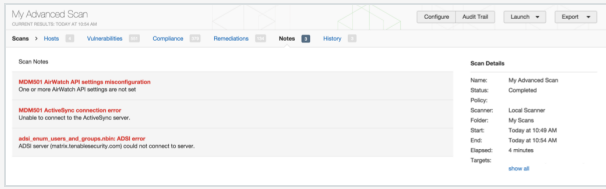
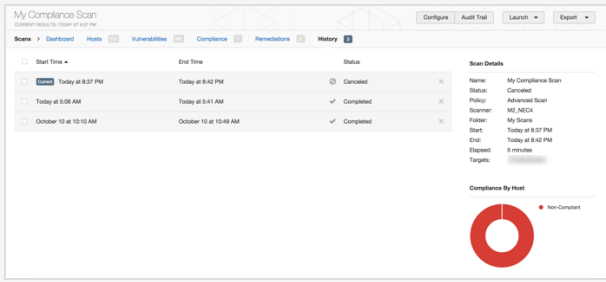
Export	Allows you to export the scan's result in one of four formats: Nessus (.nessus), HTML, CSV, or Nessus DB. Nessus DB format is an encrypted, proprietary format, which exports **all** scan data.

Report Pages

Page	Description	Example
Dashboard	If configured, the default scan results page displays the Dashboard view.	 When visible, the exchange icon ⇄ allows you to navigate between compliance and

		vulnerability results.
Hosts	The **Hosts** page displays all scanned targets. If the scan is configured for compliance scanning, the exchange icon ⇄ allows you to navigate between the **compliance** and **vulnerability** results.	 

Vulnerabilities		
Compliance		

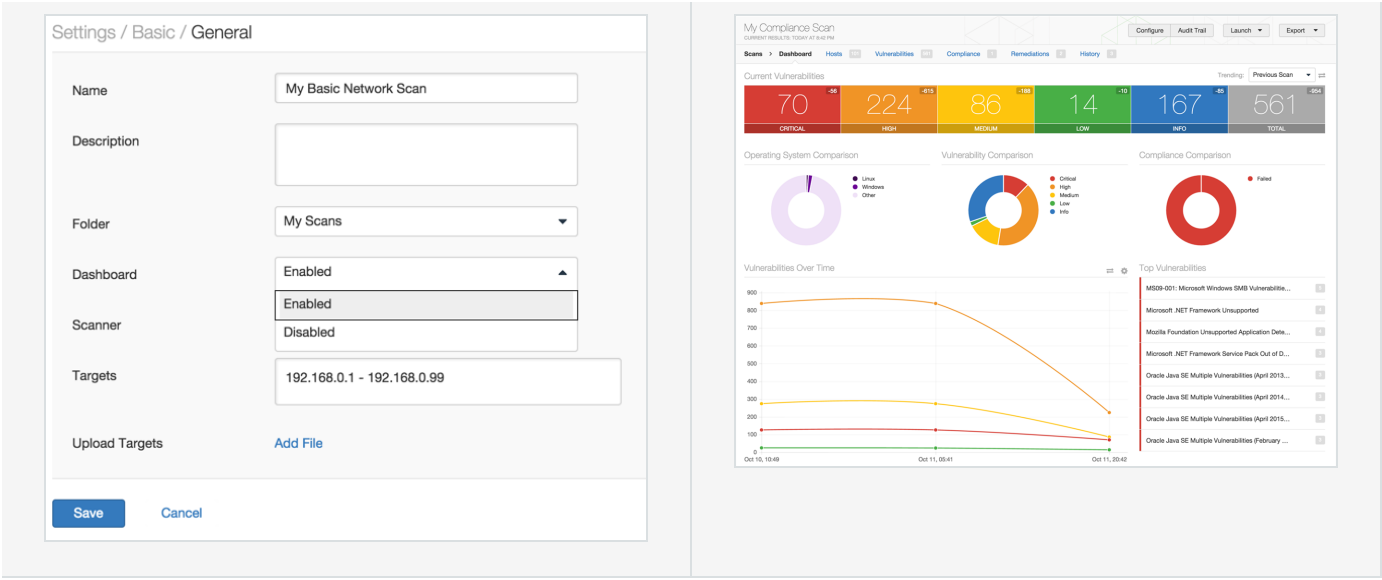
Remediations		
Notes	The **Notes** page displays additional information about the scan and the scan's results.	
History	The **History** displays a listing of scans: **Start Time**, **End Time**, and the **Scan Statuses**.	

Dashboards

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

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

The **Dashboard** view can be **Disabled** and **Enabled** at will



Dashboard Details

Name	Description
Current Vulnerabilities	The number of vulnerabilities identified.
Operating System	The percentage of operating systems identified.

Comparison	
Vulnerability Comparison	The percentage of all vulnerabilities, identified by severity.
Host Count Comparison	The percentage of hosts scanned by credentialed and non-credentialed authorization types: without authorization, new (scans) without authorization, with authorization, and new (scan) with authorization.
Top Hosts	
Top Vulnerabilities	Top 8 vulnerabilities based on severity.

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[a]) 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	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) 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.
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 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	Filter results based on if the presence of an exploit in the CANVAS exploit framework is equal to or is not

Exploit Framework	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

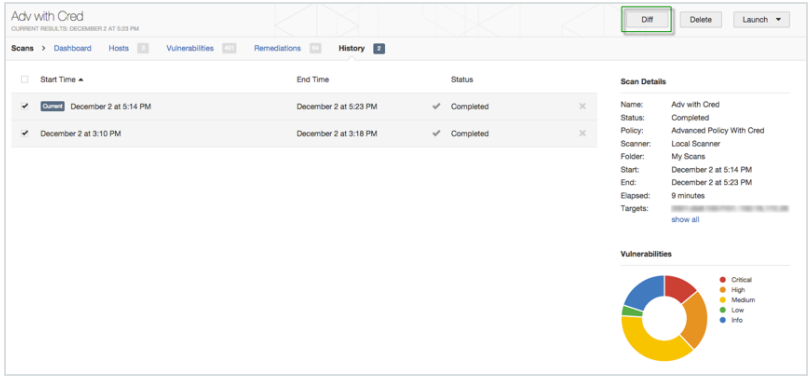
Nessus also has the ability to take screenshots during a vulnerability scan and include them in a report.

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.

This feature must be enabled in the Scan Web Applications section of a scan policy, under General.

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.



Knowledge Base

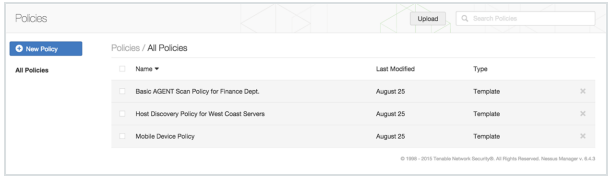
A **Knowledge Base (KB)** is saved with every scan performed. This is an ASCII text file containing a log of information relevant to the scan performed and results found. A KB is often useful during cases where you need support from Tenable, as it allows Support staff to understand exactly what Nessus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

To download a KB, select a report and then a specific host. To the right of the host name or IP there is link titled Host Details. Click on this and one of the host details is KB with a Download link:

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

Policies Page

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

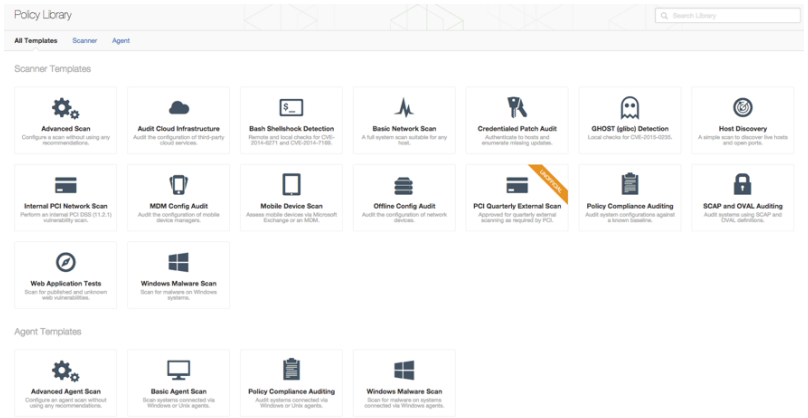


A Nessus policy is a set of configuration options related to performing a **Vulnerability Scan**.

- Parameters that control technical aspects of the scan such as timeouts, number of hosts, type of port scanner, and more.
- Credentials for local scans (e.g., Windows, SSH), authenticated Oracle database scans, HTTP, FTP, POP, IMAP, or Kerberos based authentication.

- Granular family or plugin-based scan specifications.
- Database compliance policy checks, report verbosity, service detection scan settings, Unix compliance checks, and more.
- Offline configuration audits for network devices, allowing safe checking of network devices without needing to scan the device directly.
- Windows malware scans which compare the MD5 checksums of files, both known good and malicious files.

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

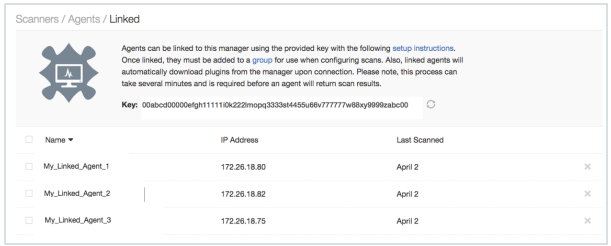


Note: User-created policies are those policies that are created from the default templates.

Nessus Agents

Nessus Agents Nessus Agents, available with Nessus Cloud 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.

Once installed, your **Nessus Agents** are viewed in the Nessus UI.



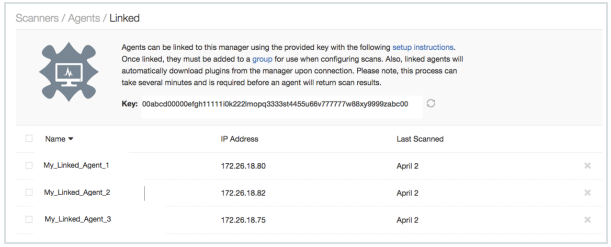
1. In Nessus, click the gear icon .
2. From the **Scanners** overview page, click the **Agents > Linked** item.

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

Nessus Agents

Nessus Agents Nessus Agents, available with Nessus Cloud 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.

Once installed, your **Nessus Agents** are viewed in the Nessus UI.



1. In Nessus, click the gear icon .
2. From the **Scanners** overview page, click the **Agents > Linked** item.

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

Agent Groups

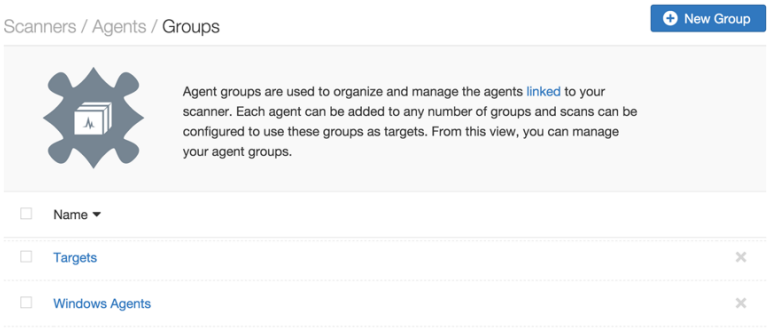
Agent groups are used to organize and manage the agents linked to your scanner. Each agent can be added to any number of groups and scans can be configured to use these groups as targets.

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.



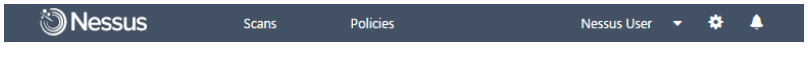
If you did not have any **Agent Groups** created prior to the Nessus Agent's install, or you opted to not add your agent to an existing group, you can create **Agent Groups** in the Nessus UI.

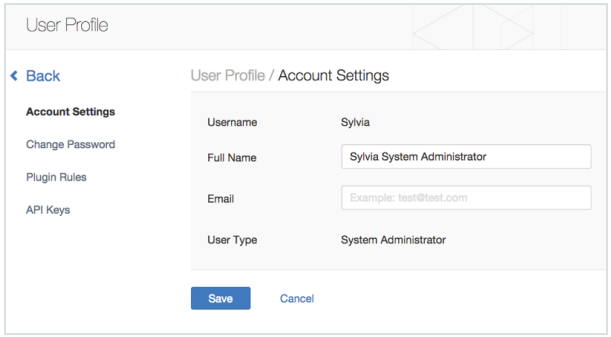
How To Summary

This section includes instructions and procedures for common Nessus functions.

Manage Your User Profile

From the Nessus top navigation menu, select the drop down arrow next to your user name.

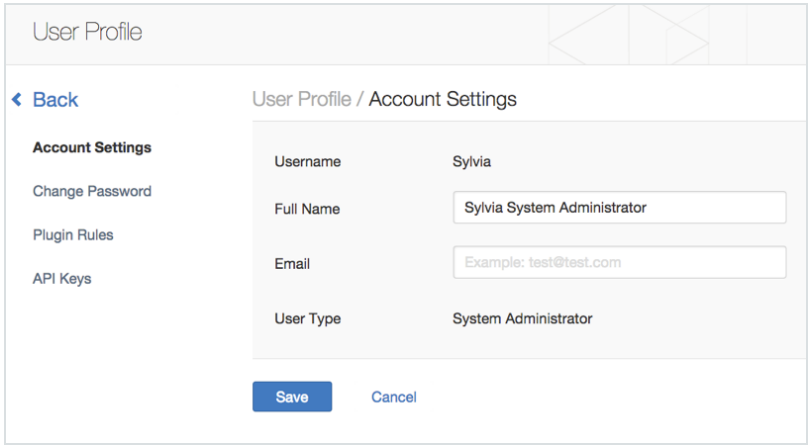




Once created, a username cannot be changed.

User Profile / Account Settings

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



Based on your Nessus product, the following information is displayed.

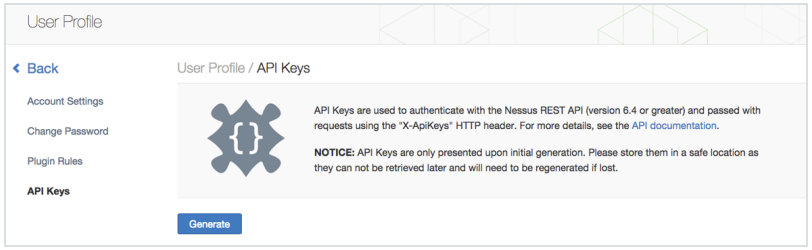
Version	Settings
Nessus Cloud	Username (e-mail address) Full Name Email User Type Nessus Cloud accounts use the email address of the user for logins.
Nessus	Username

Manager	Full Name Email User Type
Nessus Professional	User Name User Type Nessus Professional user accounts do not have an associated email address. Nessus Professional has only two user types: System Administrator and Standard.

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.



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

API Keys Warnings

- 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 will immediately un-authorize any applications currently utilizing the key.

Change Password

The **User Profile / Change Password** page allows you to change the password.

The current user has the ability to change their own password, while administrators have the ability to change their own password and other user's passwords.

To change another user's password, the administrator selects the gear icon and navigates to the **Accounts / Users** 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.

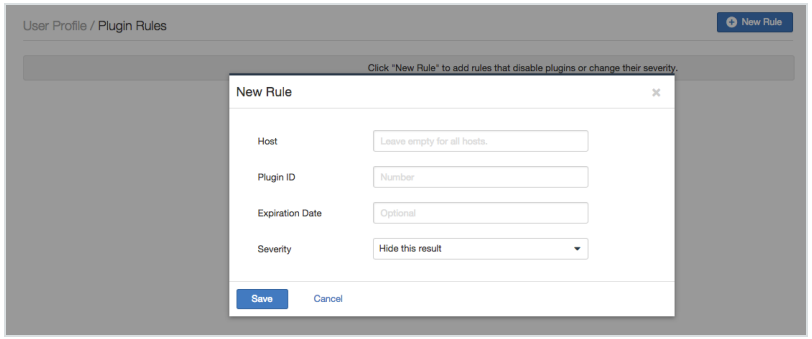
The **Plugin Rules** option provides a facility to create a set of rules that dictate the behavior of certain plugins related to any scan performed. A rule can be based on the **Host** (or all hosts), **Plugin ID**, an optional **Expiration Date**, and manipulation of **Severity**.

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

New Plugin Rule Example

This rule has been created for IP address 192.168.0.6. Once saved, this rule changes the results 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.

Click **New Rule** to add rules that disable plugins or change their severity.



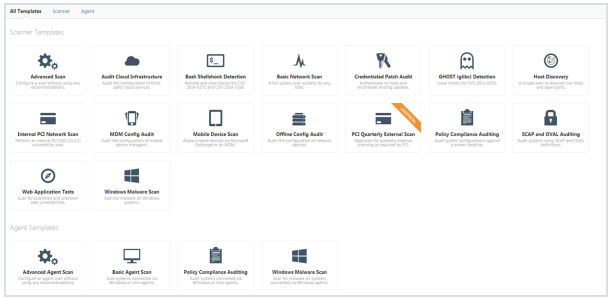
How To Scans

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

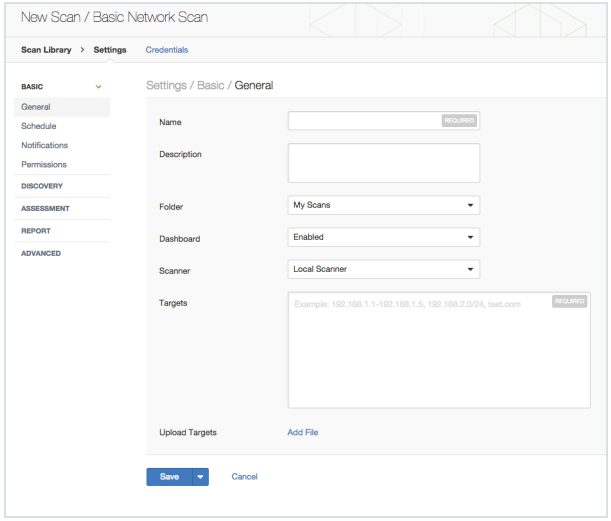
Create a Scan

Create a Basic Scan

1. From the **Scans / My Scans** page, use the **New Scan** button to create a new scan; you will be redirected to the **Scan Library**.



2. Select a template.
3. Configure the scan's **Settings** using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.



4. Next, click **Credentials**.
5. From the **Credentials** list, select applicable credentials required to perform the scan. Multiple credentials can be added.
6. When done, you have the option to **Save** the scan or **Launch** the scan.

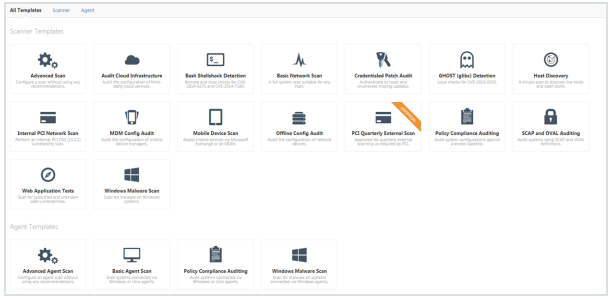
- Clicking the **Save** button will save the scan, but the scan will not launch; it will be set to **On Demand** and it can be launched from the **Scans / MyScans** page.
- Clicking the **Save** ▼ arrow will allow you to select **Launch**; the scan will be saved and will launch immediately.

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

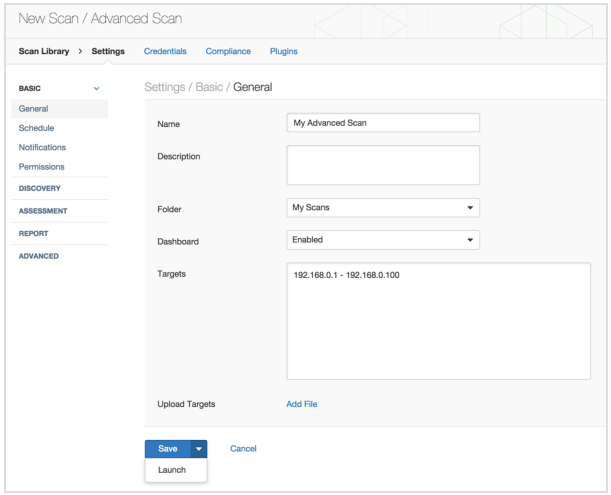
Advanced Scan templates include **Compliance** and **Plugins** options.

Create an Advanced Scan

1. From the **Scans / My Scans** page, use the **New Scan** button to create a new scan; you will be redirected to the **Scan Library**.



2. Select the **Advanced Scan** template.
3. Configure the scan's **Settings** using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.



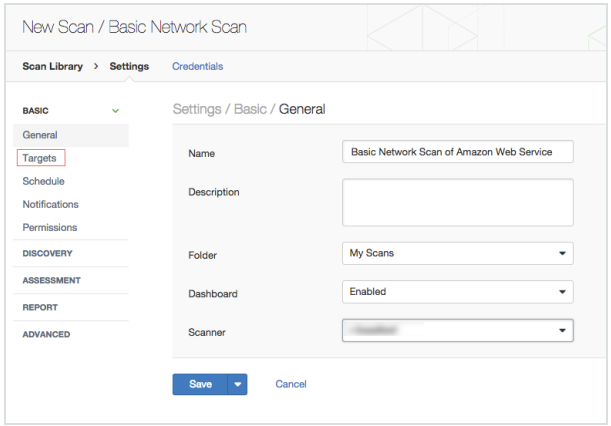
4. Click **Credentials**.
5. From the **Credentials** list, select applicable credentials required to perform the scan. Multiple credentials can be added and configured.
6. If applicable, click **Compliance**.
7. From the **Compliance Checks** list, select compliance checks applicable to perform the scan. Multiple compliance checks can be added and configured.
8. If applicable, click **Plugins**; enabled **Plugins** are displayed.
9. When done, you have the option to **Save** the scan or **Launch** the scan.

- Clicking the **Save** button will save the scan, but the scan will not launch; it will be set to **On Demand** and it can be launched from the **Scans / MyScans** page.
- Clicking the **Save** ▼ arrow will allow you to select **Launch**; the scan will be saved and will launch immediately.

Create a Basic Scan

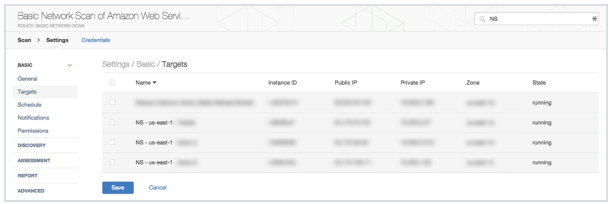
1. From the **Scans / My Scans** page, use the **New Scan** button to create a new scan; you will be redirected to the **Scan Library**.
2. Select a Scanner Template.

   When you create a scan that performs its scan on an **AWS** remote scanner, the **Targets** link appears on the **Basic** menu.



The **Targets** menu option in only displayed if the remote scanner selected is a **AWS** remote scanner.

3. Configure the scan's **Targets** using the **Basic / Targets** menu item.



4. Click the check box for each target that will be scanned.

5. Next, configure the rest of scan's **Settings** using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.
6. If credentials are required, from the **Credentials** list, select applicable credentials required to perform the scan; multiple credentials can be added.
7. When done, you have the option to **Save** the scan or **Launch** the scan.

- Clicking the **Save** button will save the scan, but the scan will not launch; it will be set to **On Demand** and it can be launched from the Scans / MyScans page.
- Clicking the **Save** ▼ arrow will allow you to select Launch; the scan will be saved and will launch immediately.

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.

Create a PCI Quarterly External Scan (Unofficial)

1. Navigate to the **Scans / My Scans** page.
2. Click 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**.

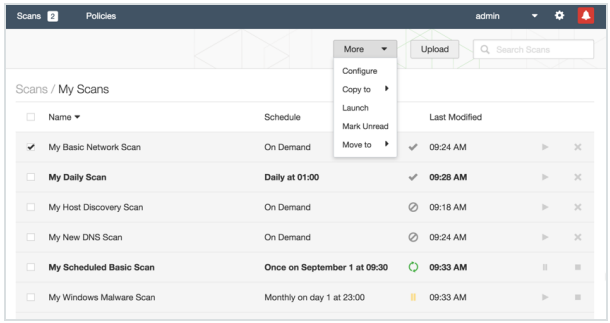
The scan results from the PCI Quarterly External Scan (Unofficial) may not be submitted to Tenable for PCI AVS Validation.

Create a Scan Folder

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

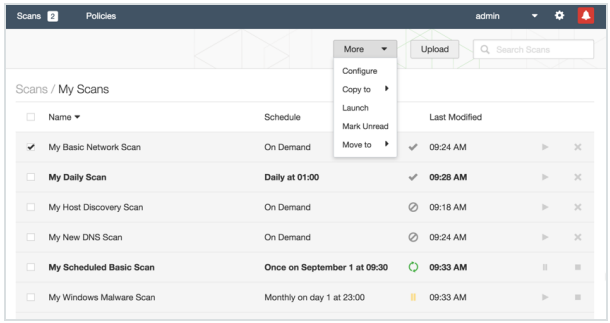
Manage Scans

View all scans on the **Scans / All Scans** page.



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

Configure displays the scan's results and allows you to modify the original scan settings.



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.

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

Upload Scan Options

Option	Description
.nessus	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. If the policy is exported and saved to a .nessus file, the passwords will be stripped. When importing a .nessus file format, you will need to re-apply your passwords to the credentials being used.
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 will be prompted for a password to encrypt the results of the scan.

Configure a Scan

The **Configure** option allows you manage scans, including their schedules and settings, and you have the ability to update them as needed.

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** 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.

How To Policies

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

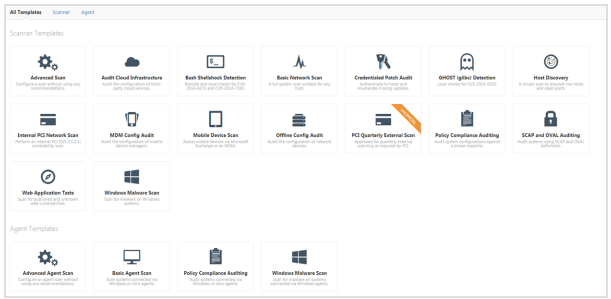
Create a Policy

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

> 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. From the **Policies** page, click **New Policy**; you will be redirected to the **Template Library**.



2. Select the **Basic Network Scan** template.
3. Configure the scan's **Settings** using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.
4. Click **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**.

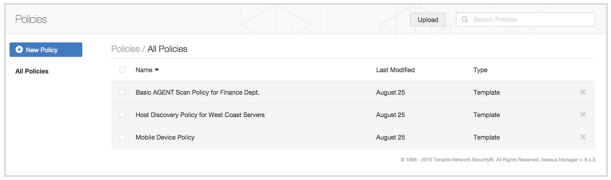
Create Advanced Scan Policy

1. From the **Policies** page, click the **New Policy**; you will be redirected to the **Policy Library**.
2. Select the **Advanced Scan** template.
3. Configure the scan's **Settings** using the **Basic**, **Discovery**, **Assessment**, **Report**, and **Advanced** links.
4. Click **Credentials**.
5. From the **Credentials** list, select applicable credentials required to perform the scan. Multiple credentials can be added and configured.
6. If applicable, click **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, click **Plugins**; enabled **Plugins** are displayed.

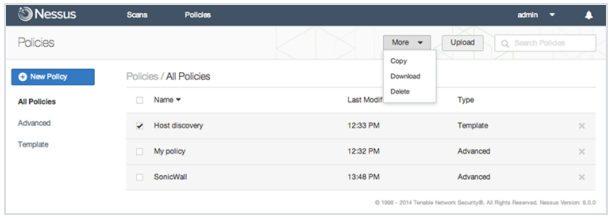
If Agents are linked to Nessus, you also can create Agent policies.

Manage Policies

Your policies are displayed on the **Policies** page.



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 previously policy. Using the native file browser box, select the policy from your local system and click on Open.

Download a Policy

Clicking on Download will open the browser's download dialog box allows you to 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.

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

Copy a Policy

To copy a policy, select a policy, then click the More button and choose Copy.

Delete a Policy

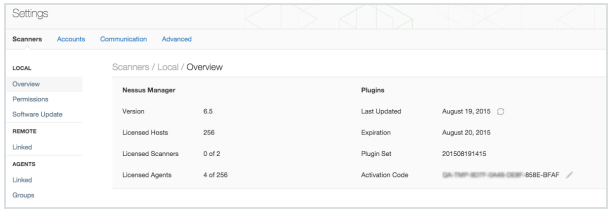
To delete a policy, select a policy, then click the X icon or use the More button, **Delete** option.

Deleting a policy is permanent; there is no folder from which the policy can be recovered.

System Settings

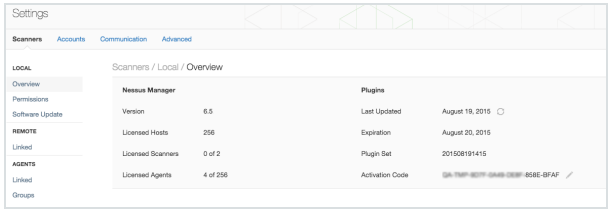
From the Nessus home page, the gear icon links you to the Nessus system **Setting** pages: **Scanners**, **Accounts**, **Communication**, and **Advanced**.

From here, you can manage Nessus system settings.



Manage Scanners

The **Settings / Scanners** page allows you to manage your local and remote scanners, as well as your Agents.



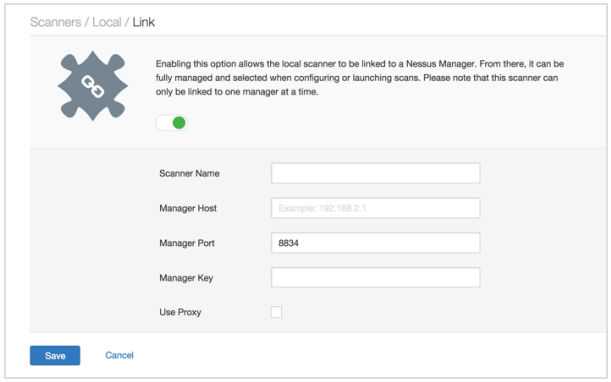
Scanners / Local

On the **Local / Overview** page, you can update Nessus components and plugins using the update icon.

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

Scanners / Local / Link

The **Local/Link** page is a **Nessus Professional** only feature.



Create a Linked a Scanner

1. On the **Local / Link** page, use the toggle to create a linked scanner.
2. Assign the scanner a unique name.
3. Enter the alpha-numeric key generated from the Nessus Manager.
4. Enter the Nessus Manager IP address and primary scanner port.
5. If applicable, select the **Use Proxy** check-box.

The **Manager Key** is the alpha-numeric key obtained from the **Remote/Linked** page in Nessus Manager.

A Proxy Server must be configured to use the **Use Proxy** option.

Option	Description

Scanner Name	Unique identifier for this Nessus scanner for the Nessus Manager
Manager Host	IP address of the Nessus Manager
Manager Port	Port number to connect to the Nessus Manager
Manager Key	Nessus Manager Key.
Use Proxy	If communication must be directed through a proxy, select this option. Once selected, the scanner will use the Proxy Server information provided on the **Communication / Network / Proxy Server** page.

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, use, or manage the Scanners.
- Can Use

  Users or groups specified here can view and use the scanner; they will not be able to make any changes.

- Can Manage

  Users or groups specified here can make changes to the Scanner's settings.

Scanners / Local / Software Update

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

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

> Note that if "Update plugins" is selected, the scanner will not receive automatic updates for the Nessus UI or engine. This can prevent new features and functionality from being displayed and operational.

Manual Software Update

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

This option allow you to update Nessus all components, plugins, or a plugin archive.

When this method of software update is selected, updated are performed once.

> Invoking a **Manual Software Update** can be used in conjunction with **Automatic Updates**.

Automatic Updates

- Update all components
- Update plugins
- Disabled

Update Frequency

- Daily
- Weekly
- Monthly

The pencil icon next to the selected **Update Frequency** interval allows you customize the update frequency into 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”.

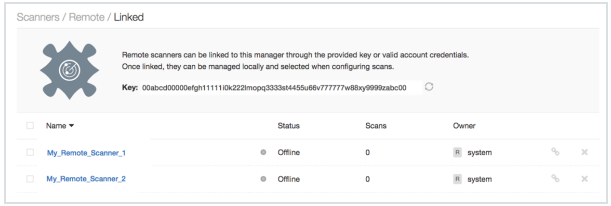
Manage Remote Scanners

Scanners / Remote / Linked

Remote scanners can be linked to this manager by using the **Key** displayed on the **Remote / Linked** page, or by using valid account credentials.

This key is only used for the initial linking of the Nessus Manager and a Nessus scanner.

Once linked, remote scanners can be managed locally and selected when configuring scans.



> If there is ever concern over the shared secret becoming compromised, you can regenerate the key at any time by clicking the icon to the right of the key.
>
> Regenerating the key will not disable any secondary scanners that are already registered. Once the secondary scanner has established communications with the primary scanner, it will display on this interface under Remote scanners menu under the Linked menu.

From the scanners list, you can use the **Disable / Disable** icon or **Remove** icon to connect, disconnect, or delete 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.

Nessus scanners are configured with default settings when they are first registered to the Nessus Manager.

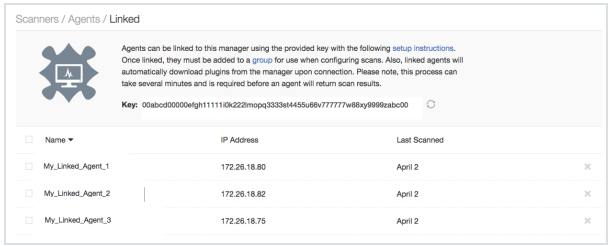
Manage Nessus Agents

After you have performed a Nessus Agent Install, your Nessus Agents are viewed and managed in the Nessus UI.

In Nessus Manager, click the gear icon .

Scanners / Agents / Linked

View your linked agents on **Agents / Linked** page.



Delete Agents

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

To delete multiple agents at once, use the checkboxes, and them click 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**.

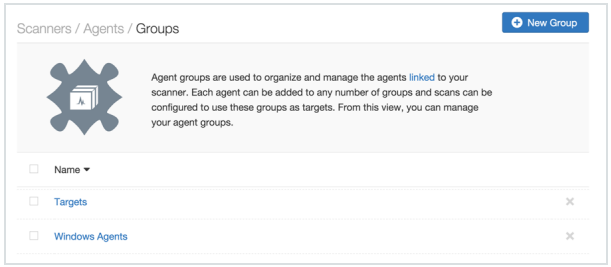
On the **Scanners / Agents / Linked** page, you can create a new agent group.

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.

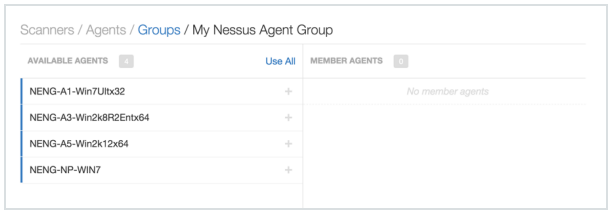


Agent groups are used to organize and manage the agents linked to your scanner. Each agent can be added to any number of groups and scans can be configured to use these groups as targets.

Create an Agent Group

1. In Nessus, click the gear icon .
2. Next, click on the link for **Scanners / Agents / Groups**.
3. Click the **New Group** button.
4. In the **Name** field, name your Agent Group.
5. Click **Save** to continue.

Your new **Agent Group** page is displayed.



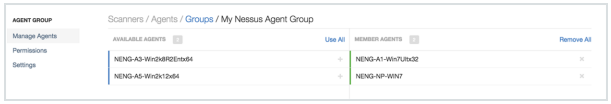
Once created, agent groups can be managed from the **Scanners / Agents / Groups** page.

To display 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. Click the name of the **Agent Group** that you will be adding Agents to.
3. From the **Available Agents** list, click the + button.

The agent will move from the **Available Agents** column to the **Member Agents** column.



Add Permissions to an Agent Group

1. Go to the **Scanners / Agents / Groups** page.
2. Click the name of the **Agent Group** that you will be adding permissions to.
3. Click the **Permissions** link.

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. Click the name of the **Agent Group** that for which you want to change the name.
3. Click the **Settings** link.
4. In the **Name** field, rename your group.
5. Click **Save**.

Manage User Accounts

Users and **Groups** are created and managed from the **Accounts** page.

1. From the Nessus home page, click the gear icon .
2. Next, click **Accounts**.

The following table describes settings and options visible in **Nessus Manager**, **Nessus Cloud**, and **Nessus Professional**.

Setting Name	Description	Product Version(s)	User Type(s)
Users	Individual Nessus accounts to be used for assigning permissions.	• Nessus Cloud • Nessus	All User Types

Setting Name	Description	Product Version(s)	User Type(s)
		Manager • Nessus Professional	
Groups	Collections of users created for shared permissions.	• Nessus Cloud • Nessus Manager	System Administrator

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

Nessus Cloud: You must define the username as the registered email address within the **Nessus Cloud** service.

> **Warning:** Once a username is created, it cannot be changed.

If you need to change a user's username, you must create a new a new user with the appropriate login name.

Create Users

1. From the Nessus home page, click the gear icon .
2. Next, click **Accounts**.
3. Click 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. Click **Save**.

User Role	Description
Read Only	Users can only read scan results. Not available in Nessus Professional
Standard	Users can create scans, policies, schedules, and reports. They cannot change any user, user groups, scanner, or system configurations.
Administrator	Users have the same privileges as the **Standard** role, but can also manage users, manage user groups, and manage scanners. Not available in Nessus Professional
System	Users have the same privileges as the **Administrator** role and can also configure the system.

Administrator	

Create Groups

1. From the Nessus home page, click the gear icon .
2. Next, click **Accounts**.
3. Click **Groups**.
4. Click the **New Group** button.
5. Enter a **Name** for the **Group**.

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

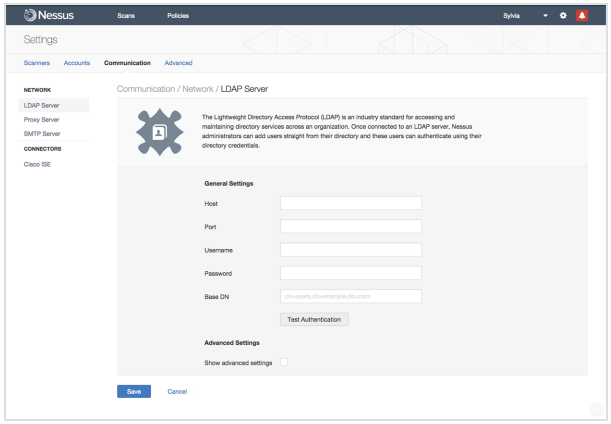
Add Users to the Group

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

Once created, users ange groups can be managed from the **Accounts / Users** or **Accounts / Groups** page, then selecting the object to be mangaged, modified, or deleted.

Manage Communications

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



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

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 will email 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 will use these settings to perform plugin updates and communicate with remote scanners.

General Settings

- Host (required)
- Port (required)
- Username (optional)
- Password (optional)
- User-Agent (optional)

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

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.

General Settings

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

Permissions

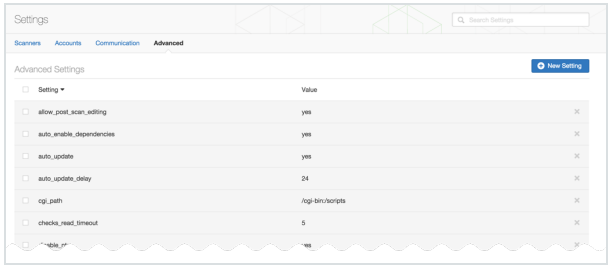
- Add users or groups

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.

- 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.



Modify Advanced Value

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

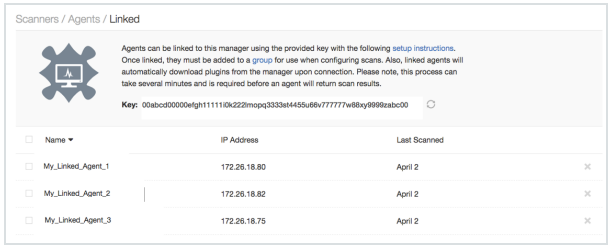
Changes go into effect a few minutes after the setting is saved.

Manage Nessus Agents

Once installed, your **Nessus Agents** are viewed in the Nessus UI.

View your Linked Agents

1. In Nessus, click the gear icon .
2. From the **Scanners** overview page, click the **Agents > Linked** item.



From this page, you can only remove Linked Agents.

Remove a Linked Agent

To remove a linked Agent, you can click 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**.

Manage Agent Groups

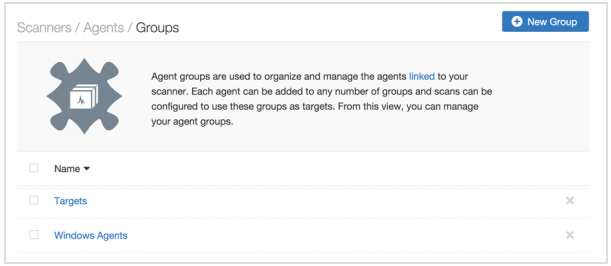
On the **Scanners / Agents / Linked** page, you can create a new Agent Group.

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.

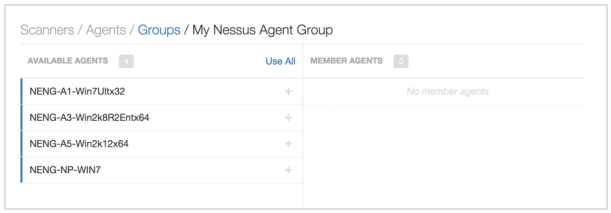


> Agent groups are used to organize and manage the agents linked to your scanner. Each agent can be added to any number of groups and scans can be configured to use these groups as targets.

Create an Agent Group

1. In Nessus, click the gear icon .
2. Next, click on the link for **Scanners / Agents / Groups**.
3. Click the **New Group** button.
4. In the **Name** field, name your Agent Group.
5. Click **Save** to continue.

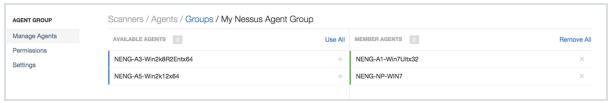
Your new **Agent Group** page is displayed.



Add an Agent to a Group

1. Go to the **Scanners / Agents / Groups** page.
2. Click the name of the **Agent Group** that you will be adding Agents to.
3. From the **Available Agents** list, click the + button.

The agent will move from the **Available Agents** column to the **Member Agents** column.



Add Permissions to an Agent Group

1. Go to the **Scanners / Agents / Groups** page.
2. Click the name of the **Agent Group** that you will be adding permissions to.
3. Click the **Permissions** link.

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 a Agent Group

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

Navigating 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.

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

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.

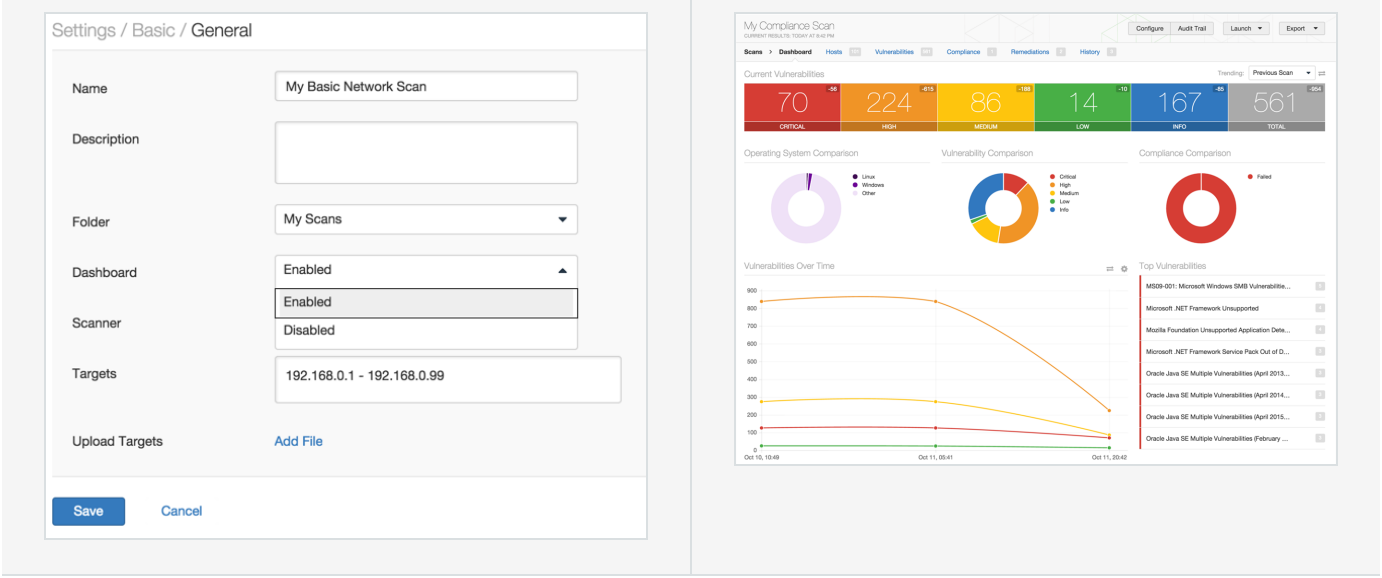
Option	Description
Configure	Navigates you back to the scan's configuration settings.
Audit Trail	Displays the audit trail dialogue.
Launch	Display two choices to launch a scan: Default and Custom. • Default: This option uses the scan's pre-configured settings. • Custom: This options allows for **Customer Scan Targets**.
Export	Allows you to export the scan's result in one of four formats: Nessus (.nessus), HTML, CSV, or Nessus DB.

	Nessus DB format is an encrypted, proprietary format, which exports **all** scan data.

Dashboard

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

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



Dashboard 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 Comparison	The percentage of hosts scanned by credentialed and non-credentialed authorization types: without authorization, new (scans) without authorization, with authorization, and new (scan) with authorization.
Top Vulnerabilities	Top 8 vulnerabilities based on severity.

PCI ASV Validation

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, Inc. 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 Nessus Cloud is a validated Approved Scanning Vendor (ASV) solution.

Create a PCI Quarterly External Scan

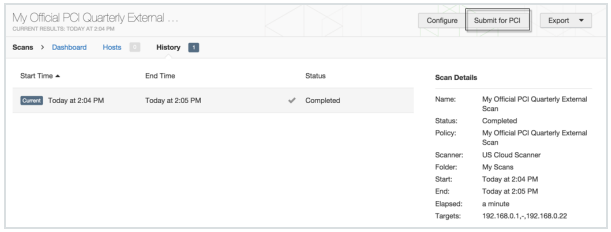
1. Login to Nessus Cloud.
2. Navigate to the Scans / My Scans page.
3. Click the New Scan button.
4. Select the PCI Quarterly External Scan template.
5. Enter a Name and Description.
6. Next, if applicable, configure settings: Basic, Discovery, and Advanced.

Creating a PCI Quarterly External Scan policy will allow you to create scans based on your policy; the policy will appear in the template library in the User Created Policies area.

Submit Scan Results

Nessus Cloud 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.



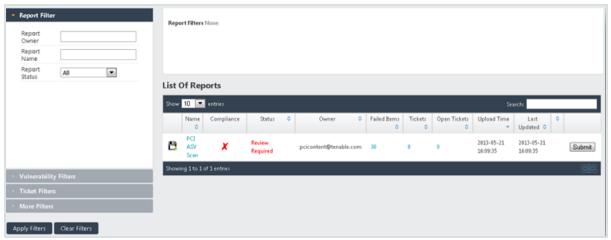
1. From the Scans / My Scans page, click your PCI DSS ASV scan.
2. Click Submit for PCI.
3. On the Submit for PCI Validation screen, click the Continue button.

- PCI-DSS ASV scans older than three months cannot be submitted for review. No Submit for PCI button will appear for those scans.
- Any policies created with the PCI Quarterly External Scan policy template cannot be edited further to ensure the required testing is performed.
- Customers are allowed up to two quarterly report submissions for PCI ASV validation through Tenable Network Security, Inc.

PCI Validation Portal

https://pci.tenable.com/

Once a customer logs into the PCI Validation user section, they are presented with a list of reports that have been submitted by their unique Nessus Cloud login. The Report Filter allows reports to be filtered by Owner, Name, and Status.

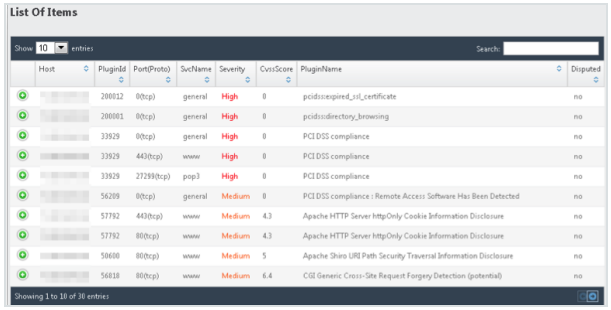


Results

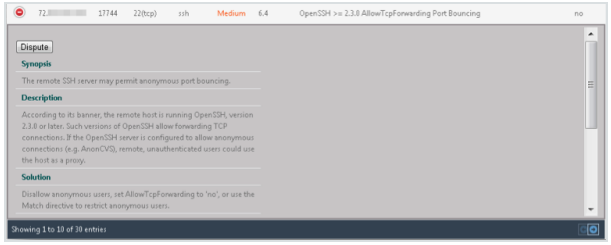
To pass a PCI DSS ASV assessment, all items (except for denial of service (DoS) vulnerabilities) listed as Critical, High, or Medium (or with a CVSS score of 4.0 or higher) must either be remediated or disputed by the customer, and all disputed items must either be resolved, accepted as exceptions, accepted as false positives, or mitigated through the use of compensating controls. All items listed as Critical, High, or Medium in the Nessus Cloud can be viewed in detail, and all items carry an option to dispute the item in question.

Clicking the name of the scan in the List of Reports allows the user to view a list of hosts and the number of vulnerabilities found on each host, sorted by severity.

Nessus Cloud customers are responsible for reviewing all of their Failed Items before submitting a scan report to Tenable Network Security. Selecting the Failed Items in the List of Reports allows you to jump directly to the items that may affect your PCI ASV Validation compliance status.



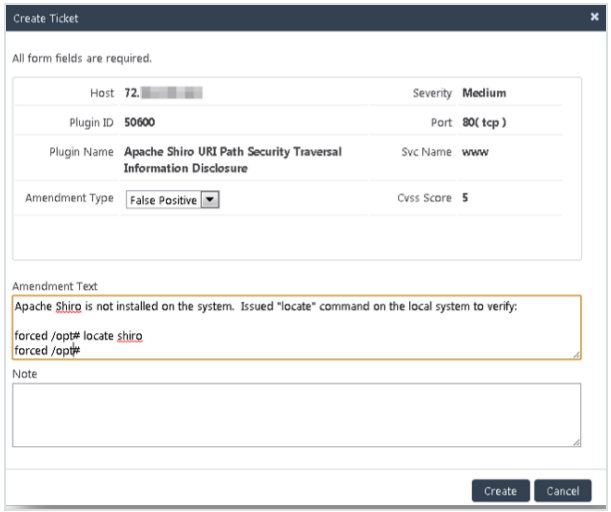
Use the green + button under the far left column to expand an individual entry for additional vulnerability details.



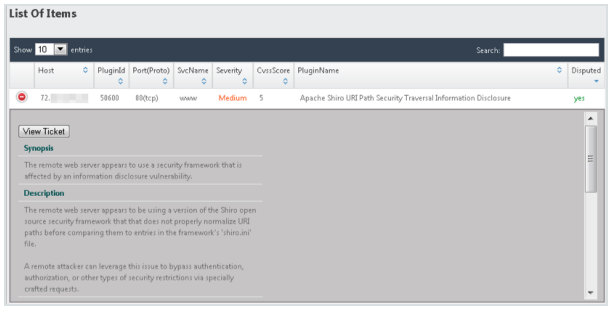
As shown above, a Dispute button is displayed for each individual item, which allows the customer to enter additional details about vulnerability remediation, or dispute what they believe may be a false positive generated by the initial scan.

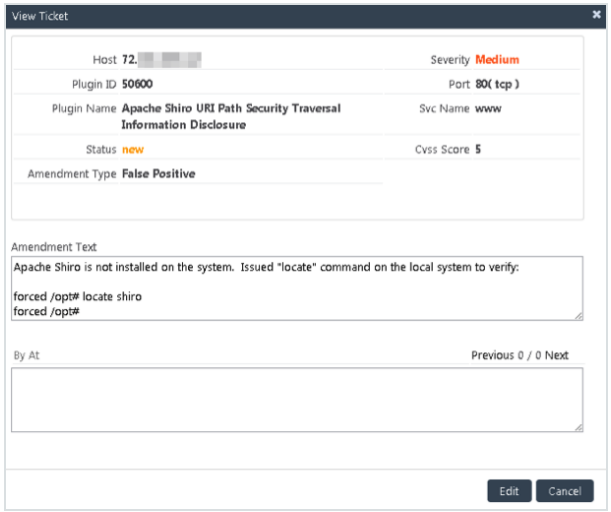
Disputes

When an item is disputed, a ticket is created that allows for the selection of an amendment type, the addition of text to the amendment, and any other notes that the customer may want to add prior to submission for review by Tenable Network Security.

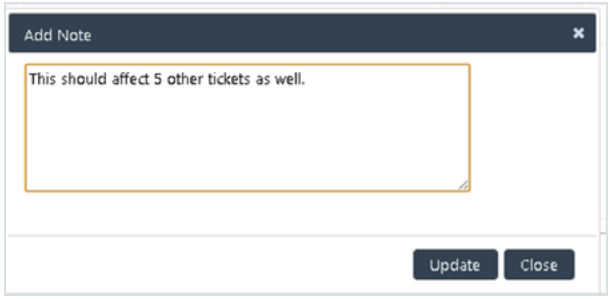


Once a ticket for a particular item has been created, the customer can view it by selecting the item in question and then selecting View Ticket.





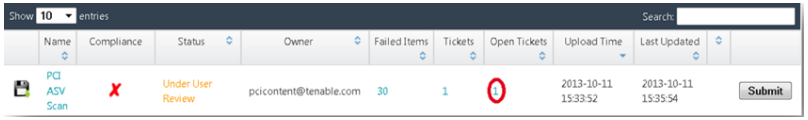
Additional comments can be added by clicking the Edit button, then Add Note, and saving the note into the ticket by clicking Update.



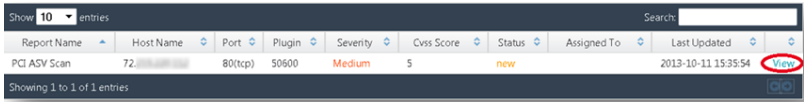
Plugin 33929, PCI DSS Compliance, is an administrative plugin that links to the results of other plugins. If a report shows that a host is not PCI DSS compliant, resolving all failed items will then allow plugin 33929 to resolve and be replaced with plugin 33930, PCI DSS Compliance: Passed. In cases of disputes or exceptions, if all failed report items are successfully disputed or given exceptions, an exception can then be given for plugin 33929 based on the remediation of all other report issues.

Attachments as Evidence for a Dispute

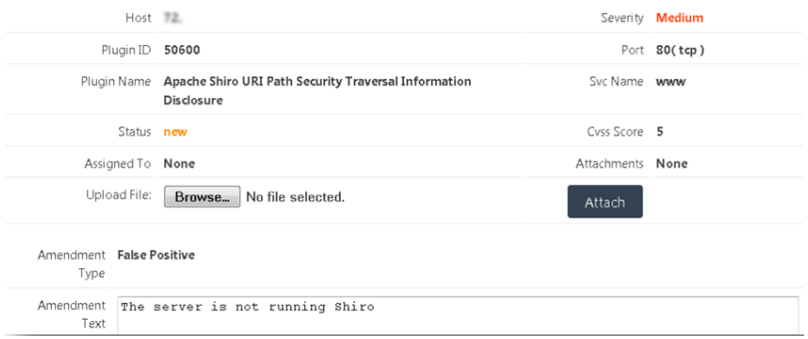
Once a ticket is created, it is possible to submit supporting evidence as an attachment. After creating a ticket, click the number listed under Open Tickets to display all open tickets.



In the List of Tickets screen, click View.

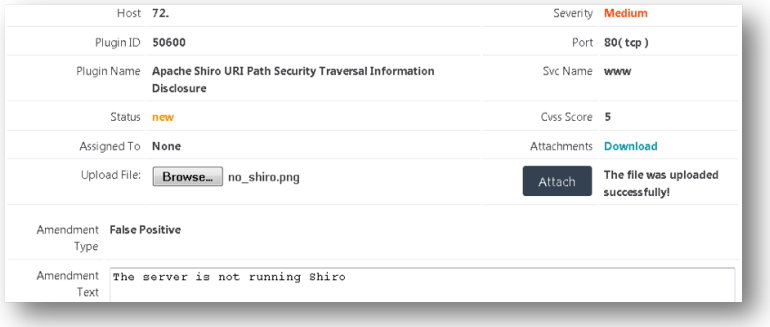


When the screen for the open ticket is displayed, options for Upload File and Attach are displayed:



Click Browse... to navigate to and select the evidence file (screenshot, Word document, PDF, etc.) to be uploaded.

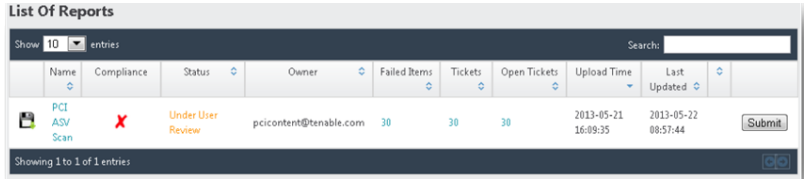
Next, click Attach to attach the file to the ticket. When completed, the screen will display a message that the file was uploaded successfully.



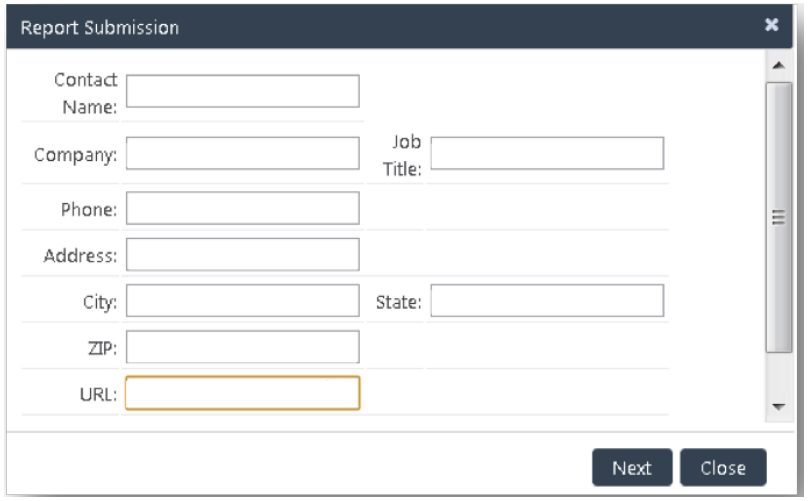
Clicking the Download link next to Attachments will show the names of all files attached to the ticket.

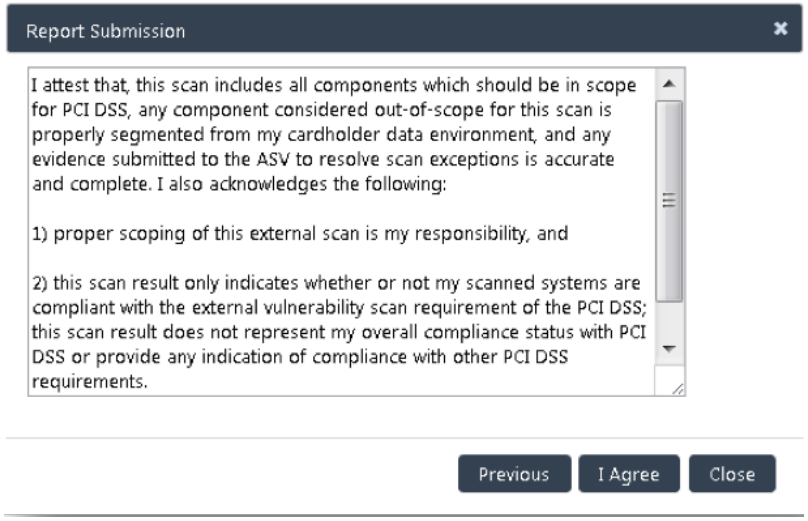
Submitting a Scan Report for Tenable Review

When tickets have been created for all outstanding report items under user review, the report can then be sent to Tenable Network Security for ASV review.

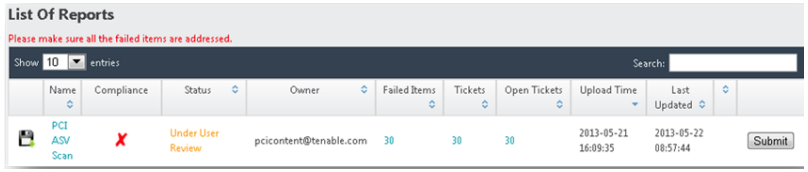


Before a report can be submitted for review, the customer must fill in contact information and agree to an attestation that includes mandatory text as described in the ASV Program Guide.

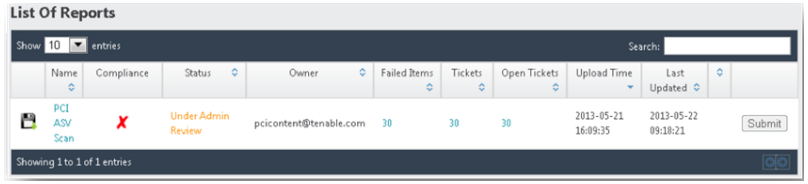




If a customer neglects to address any outstanding item for a particular scan before the report is submitted for ASV review, they will be prompted to make sure that a ticket has been created for each item. Any report with outstanding items that have not been addressed by the customer cannot be submitted to Tenable Network Security for review.

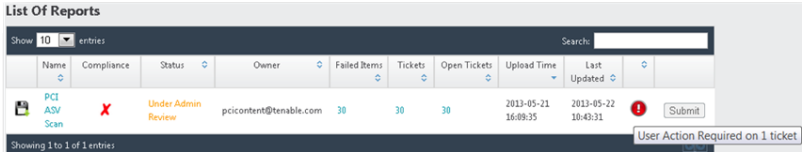


When a report is finally submitted to Tenable Network Security for review, the status of the report changes from Under User Review to Under Admin Review and the Submit option is removed (grayed out) to prevent the submission of duplicate items or reports.



> The Withdraw function within an open ticket is only available once a report has been submitted for review by Tenable's Nessus Cloud. Be careful when using the Withdraw function; withdrawing a ticket will cause the item in question to be flagged as unresolved due to having inconclusive evidence, and the report as a whole will be deemed as non-compliant.

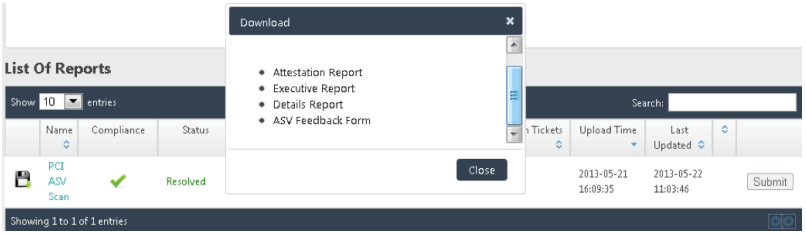
If a Tenable Network Security staff member requests more information or if any other user action is required by the customer for a ticket, an indicator will appear in the customer's List of Reports as shown below.



The ticket can then be amended by the user and resubmitted to Tenable Network Security for further review.

PCI ASV Report Formats

Once a scan report has earned compliance status by Tenable's Nessus Cloud, customers have the option of viewing reports in Attestation Report, Executive Report, or Detailed Report formats. An ASV Feedback Form is also provided to the Nessus Cloud customer. These options are available through the Download icon listed next to each report.



The Attestation Report, Executive Report, and Details Report are only available to the customer in PDF format and cannot be edited.

Scan Customer Information		Approved Scanning Vendor Information	
Company:	Tenable Network Security	Company:	Tenable Network Security
Contact:	John Smith	Contact:	
Title:	PCI Analyst	Title:	Software Engineer
Telephone:	(410) 872-0555	Telephone:	4108720555
Email:	pcicontent@tenable.com	Email:	@tenable.com
Business Address:	7063 Columbia Gateway Drive	Business Address:	7063 Columbia Gateway Drive, Suite 100
City:	Columbia	City:	Columbia
State:	MD	State:	MD
ZIP:	21046	ZIP:	21046
URL:	http://www.tenable.com	URL:	www.tenable.com

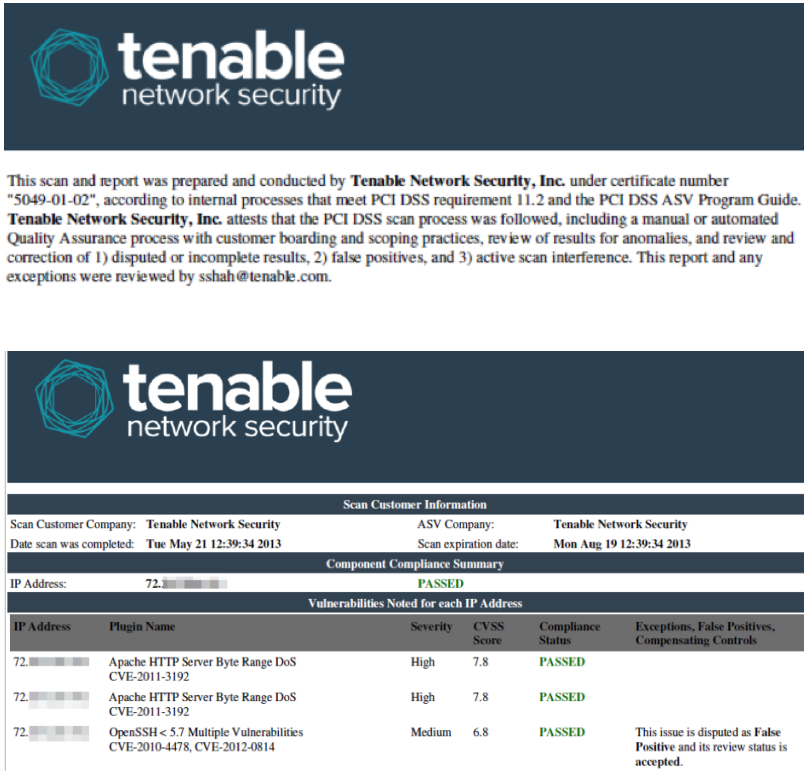
Scan Status

- Compliance Status: **PASSED**
- Number of unique components scanned: **1**
- Number of identified failing vulnerabilities: **30**
- Number of components* found by ASV but not scanned because scan customer confirmed components were out of scope: **0**
- Date scan completed: **Tue May 21 12:39:34 2013**
- Scan expiration date (90 days from date scan completed): **Mon Aug 19 12:39:34 2013**

Scan Customer Attestation

Tenable Network Security attests on **2013-05-22 09:18:21** that this scan includes all components* which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements

ASV Attestation



tenable network security

This scan and report was prepared and conducted by **Tenable Network Security, Inc.** under certificate number "5049-01-02", according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. **Tenable Network Security, Inc.** attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by sshah@tenable.com.

tenable network security

Scan Customer Information

Scan Customer Company:	**Tenable Network Security**	ASV Company:	**Tenable Network Security**
Date scan was completed:	**Tue May 21 12:39:34 2013**	Scan expiration date:	**Mon Aug 19 12:39:34 2013**

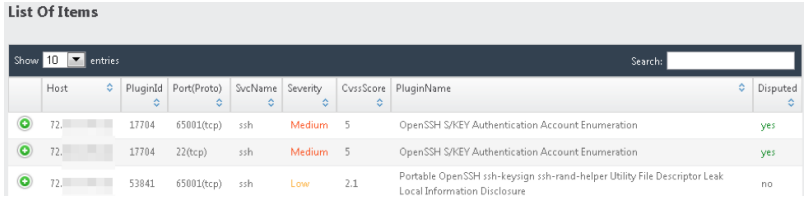
Component Compliance Summary

IP Address:	**72.**
	PASSED

Vulnerabilities Noted for each IP Address

IP Address	Plugin Name	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, Compensating Controls
72.	Apache HTTP Server Byte Range DoS CVE-2011-3192	High	7.8	PASSED	
72.	Apache HTTP Server Byte Range DoS CVE-2011-3192	High	7.8	PASSED	
72.	OpenSSH < 5.7 Multiple Vulnerabilities CVE-2010-4478, CVE-2012-0814	Medium	6.8	PASSED	This issue is disputed as **False Positive** and its review status is **accepted**.

When a report name and then host name is selected within the web-based interface, a list of items pertaining to the selected report is displayed.


List Of Items

Show 10 entries Search:

	Host	PluginId	Port(Proto)	SvcName	Severity	CvssScore	PluginName	Disputed
	72.	17704	65001(tcp)	ssh	Medium	5	OpenSSH S/KEY Authentication Account Enumeration	yes
	72.	17704	22(tcp)	ssh	Medium	5	OpenSSH S/KEY Authentication Account Enumeration	yes
	72.	53841	65001(tcp)	ssh	Low	2.1	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure	no

Custom SSL Certificates

Usage

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.

Location of Certificate Files

Operating System	Directory
Linux	/opt/nessus/com/nessus/CA/servercert.pem

	/opt/nessus/var/nessus/CA/serverkey.pem
FreeBSD	/usr/local/nessus/com/nessus/CA/servercert.pem /usr/local/nessus/var/nessus/CA/serverkey.pem
Windows Vista and later	C:\ProgramData\Tenable\Nessus\nessus\CA\servercert.pem C:\ProgramData\Tenable\Nessus\nessus\CA\serverkey.pem
Mac OS X	/Library/Nessus/run/com/nessus/CA/servercert.pem /Library/Nessus/run/var/nessus/CA/serverkey.pem
You can also use the /getcert switch to install the root CA in your browser, which will remove the warning. https://[IP address]:8834/getcert	

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.

Configure Nessus for Certificates

The first step to allow SSL certificate authentication is to configure the Nessus web server with a server certificate and CA.

This process 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.

Create a new custom CA and server certificate

1. (Optional) 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 a CA certificate is to be used instead of the Nessus generated one, make a copy of the self-signed CA certificate using the appropriate command for your OS:

   Linux/Unix

   ```
   # 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/Unix

```
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, login using a username and password is disabled.

Linux/Unix

```
# /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.

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

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/Unix:

   ```
   # /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/Unix or Windows server.

   mkcert-client Output

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
```

Windows installations of Nessus do not come with “man” pages (local manual instructions). Consult the Tenable 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 for the smart card, CAC, or similar device has been put in place, corresponding users must be created to match within Nessus. During this process, the users created must match the CN used on the card with which the user will use to connect.

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

   Linux/Unix

   ```
   # /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/Unix or Windows server. The user name must match the CN supplied by the certificate on the card.

> 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.

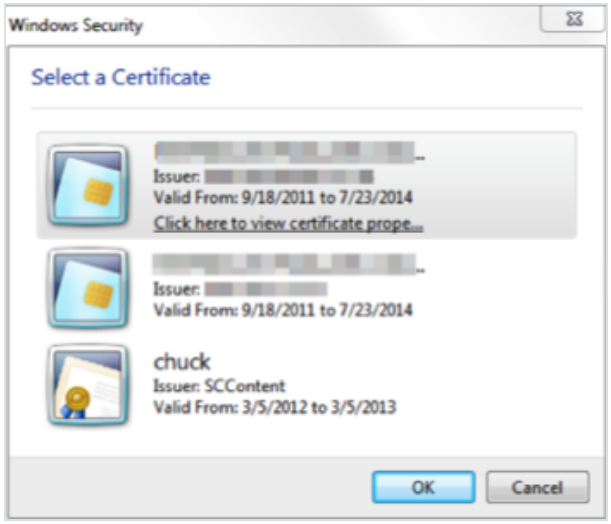
Once created, a user with the proper card may access the Nessus server and authenticate automatically once their PIN or similar secret is provided.

Connect with Certificate or Card Enabled Browser

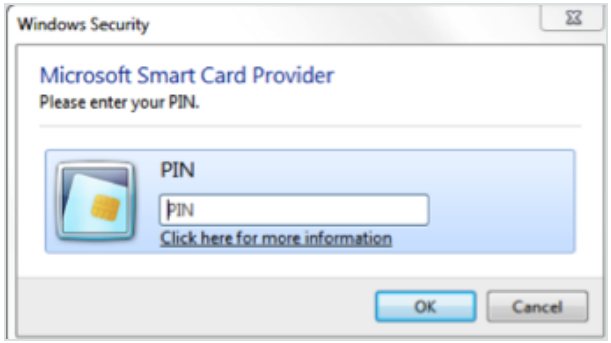
The following information is provided with the understanding that your browser is configured for SSL certificate authentication. This includes the proper trust of the CA by the web browser. Please refer to your browser's help files or other documentation to configure this feature.

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

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.

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

This section applies to Unix 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 Unix 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.

his 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 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.

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 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.

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.

Credentialed Checks on Windows

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 an 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.

To configure the server to allow logins from a domain account, the Classic security model should be invoked.

1. Open Group Policy by clicking on start, click Run, type gpedit.msc and then click OK.
2. Select Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options.
3. From the list of policies open Network access: Sharing and security model for local accounts.
4. In this dialog, select Classic – local users authenticate as themselves and click OK to save this.

This will cause users local to the domain to authenticate as themselves, even though they are actually not really physically local on the particular server. Without doing this, all remote users, even real users in the domain, will actually authenticate as a Guest and will likely not have enough credentials to perform a remote audit.

> The gpedit.msc tool is not available on some version such as Windows 7 Home, which is not supported by Tenable.

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, and Windows 8 and be part of a domain.

Create a Security Group called Nessus Local Access

1. Log onto a Domain Controller, open Active Directory Users and Computers.
2. Create a security Group from Menu select 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 on 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 type Nessus Local Access and then click Check Names.
5. Click OK twice to close the dialog box.
6. Click Add under This group is a member of:

7. Add the Administrators Group.
8. Click 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, 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. Click on Next.
6. Select the Checkboxes for:

   Windows Management Instrumentation (ASync-In)

   Windows Management Instrumentation (WMI-In)

   Windows Management Instrumentation (DCOM-In)

7. Click on Next
8. Click on Finish

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 on the domain or the OU and select Link an Existing GPO
2. Select the Nessus Scan GPO

Configure Windows 2008, Vista, and 7

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.

Enabling this option grants Nessus permission to enable and disable the Remote Registry service—even if you have explicitly set it to 'Disabled'.

Windows User Account Control (UAC) can be disabled alternatively, but that is not recommended. 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.

Additional Resources

This section includes additional resources for Nessus, Nessus Agents and Tenable Support.

Scan Targets Explained

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 with a start and end address	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	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, 192.168.0.4 and 192.168.0.5

Target Description	Example	Explanation
octets replaced with numeric ranges		
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.
An IPv4 subnet with netmask notation	192.168.0.0/255.255.255.128	All addresses within the specified subnet are scanned. The address is not a start address. Specifying any address within the subnet with the same netmask will scan the same hosts
A host resolvable to either an IPv4 or an IPv6 address	www.yourdomain.com	The single host is scanned. If the hostname resolves to multiple addresses the address to scan is the first IPv4 address or if it did not resolve to an IPv4 address, the first IPv6 address.

Target Description	Example	Explanation
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

Target Description	Example	Explanation
Some text with either a single IPv4 or IPv6 address within square brackets	"Test Host 1[10.0.1.1]" or "Test Host 2[2001:db8::abcd]	The IPv4 or IPv6 address within the brackets is scanned like a normal single target

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.

Command Line Operations

This section includes command line operations for Nessus and Nessus Agents.

During command line operations, prompts for sensitive information, such as a password, do not show characters as you type. However, the data is being recorded and will be accepted when you hit the **Enter** key.

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.

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 will make the server run in the background (daemon mode).
-v	Display the version number and exit.

Option	Description
-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 will encrypt all policies and credentials contained in the policy. When a password is set, the Nessus UI will prompt you for the password. If your master password is set and then lost, it cannot be recovered by your administrator nor Tenable Support.

The # killall nessusd command is used to halt Nessus; Nessus will immediately stop all services and stop all in-process scans.

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.

nessuscli is available on all Nessus 6.x supported platforms.

nessuscli Syntax

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 Run cmd.exe as adminstrator.

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 to help diagnose issues. By default, the script will run in interactive mode.	
nessuscli bug-report-generator	Generates an archive of system diagnostics Running this command without arguments will prompt for values. --quiet: run the bug report generator without prompting user for feedback --scrub: when in quiet mode, bug report generator will sanitize the last two octets of the IPv4 address --full: when in quiet mode, bug report generator will collect extra data

Command	Description
USER COMMANDS	
nessuscli rmuser [username]	Allows you to remove a Nessus user.
nessuscli chpasswd [username]	Allows you to change a user's password. You will be prompted to enter the Nessus user's name. Passwords will not be echoed on the screen.
nessuscli adduser [username]	Allows you to add a Nessus user account. You will be prompted for a username, password, and opted to allow the user to have an administrator type account. Additionally, you will be 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 <serial>	Uses your Activation Code to register Nessus online. Example # /opt/nessus/sbin/nessuscli fetch --register xxxx-xxxx-xxxx-xxxx

Command	Description
nessuscli fetch --register-offline [<file.rc>]	Registers Nessus with an rc.file obtained fromhttps://plugins.nessus.org/v2/offline.php
nessuscli fetch --check	Displays whether Nessus is properly registered and is able to receive updates
nessuscli fetch --code-in-use	Displays the Nessus Activation Code being used
nessuscli fetch --challenge	Displays the Challenge code needed to use the Nessus offline registration
nessuscli fetch --security-center	Prepares Nessus to be connected to Security Center
FIX COMMANDS	
nessuscli fix	Reset registration, display network interfaces, and manage advanced settings. Using the --secure option will act on the encrypted preferences, which contain information about registration --list, --set, --get, and --delete can be used to modify or view preferences.
nessuscli fix [--secure] --list	
nessuscli fix [--secure] --set <name=value>	

Command	Description
nessuscli fix [--secure] --get <name>	
nessuscli fix [--secure] --delete <name>	
nessuscli fix --list-interfaces	List the network adapters on this machine
nessuscli fix --reset	This command will delete all your registration information and preferences, causing Nessus to be put into a non-registered state Before running nessuscli fix --reset, verify running scans have completed, then stop the nessusd daemon or service. Windows (Must be run as Administrator) net stop "Tenable Nessus" Linux service nessusd stop
CERTIFICATE COMMANDS	

Command	Description
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 will respect 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 <plugin archive>	Supplying a plugin archive will cause Nessus to be updated from the archive instead of the feed.
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.	

Command	Description
nessuscli managed help	Displays nessuscli manged 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> --proxy-port=<port> --proxy-username=<username> --proxy-password=<password> --proxy-agent=<agent>
nessuscli managed unlink	Unlink a managed scanner to the Nessus Manager.
nessuscli managed status	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.

nessuscli agent Syntax

Operating System	Command
Linux	# /opt/nessus_agent/sbin/nessuscli agent <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	
# /opt/nessus_agent/sbin/nessuscli agent help	Displays a list of Nessus Agent commands
nessuscli agent help	Displays additional help for specific commands identified in the nessuscli agent help output.
BUG REPORTING COMMANDS	

Command	Description
nessuscli agent bug-report-generator	Generates an archive of system diagnostics Running this command without arguments will prompt for values. --quiet: run the bug report generator without prompting user for feedback --scrub: when in quiet mode, bug report generator will sanitize the last two octets of the IPv4 address --full: when in quiet mode, bug report generator will collect extra data
LOCAL AGENT COMMANDS Used to link, unlink, and display agent status	
# nessuscli agent link --key=<key> [--name=<name>] [--groups=<group1,group2,...>] [--ca-path=<ca_file_name>] [host] [proxy]	Using the key obtained from within Nessus Manager, this command links the agent to the Nessus Manager.
# nessuscli agent unlink	Unlinks agent from the Nessus Manager

Command	Description
# nessuscli agent status	Displays the status of the agent: jobs pending and if the agent linked or not linked to server. **Example Status** Agent linked 3 jobs pending Agent not linked to a server Agent is linked to 192.168.0.1:8834 1 jobs pending

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. Click the Nessus  icon.
3. Click the lock  icon.
4. Enter your username and password.
5. To stop the Nessus service, click the Stop Nessus button.
6. To start the Nessus service, click the Start Nessus button.

Mac OS X Command Line

Start	Stop
# launchctl load –w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist	# launchctl unload –w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist

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 click Stop.
4. To restart the Nessus service, right-click Tenable Nessus, and then click Start.

Windows Command Line

Start	Stop
C:\Windows\system32>net start “Tenable Nessus”	C:\Windows\system32>net stop “Tenable Nessus”

Linux

Linux Command Line

Start	Stop
Red Hat, CentOS and Oracle Linux	
# /sbin/service nessusd start	# /sbin/service nessusd stop
SUSE	
# /etc/rc.d/nessusd start	# /etc/rc.d/nessusd stop
FreeBSD	
# service nessusd start	# service nessusd stop
Debian/Kali and Ubuntu	

Start	Stop
# /etc/init.d/nessusd start	# /etc/init.d/nessusd stop

Additional Resources

Product Pages

Nessus Product Page

Nessus Product Feature Comparisons

Tenable Plugins Home Page

Tenable Support Portal

Nessus FAQs

More Documentation

Title/Link	Description
Nessus 6.4 Installation and Configuration Guide	The installation, operation, and configuration of Nessus Professional, Nessus Manager, Nessus Agents, and Nessus Cloud. (Last Updated June 30, 2015.)

Nessus 6.4 User Guide	Describes how to configure and operate the Nessus User Interface for Nessus Professional, Nessus Manager, Nessus Agents, and Nessus Cloud. (Last Updated June 30, 2015.)
Nessus 6.4 Command Line Reference	Describes the command line tools of Tenable Network Security's Nessus 6.4 vulnerability scanner. (Last Updated June 30, 2015.)
Nessus v6 SCAP Assessments	Describes how to use Tenable's Nessus to generate SCAP content audits as well as view and export the scan results. (Last Updated November 18, 2014.)
Nessus and Antivirus	Outlines how several popular security software packages interact with Nessus, and provides tips or workarounds to allow the software to better co-exist without compromising your security or hindering your vulnerability scanning efforts. (Last Updated January 31, 2014.)
Comprehensive Malware Detection with SecurityCenter Continuous View and Nessus	Describes how Tenable's SecurityCenter CV can detect a variety of malicious software and identify and determine the extent of malware infections. (Last Updated February 3, 2015.)
Nessus Compliance Checks	This paper discusses what sort of configuration parameters and sensitive data can be audited, how to configure Nessus to perform these audits and how Tenable's SecurityCenter can be used to manage and automate this process. There is also information on how to use the various tools available to

	create audit policies. (Last Updated June 17, 2015.)
Nessus Compliance Checks Reference	This paper discusses the Nessus compliance language syntax and provides examples for those wishing to write their own audit files. (Last Updated June 17, 2015.)
Tenable Products Plugin Families	This document provides a description and summary of the plugin families for Nessus, Log Correlation Engine, and the Passive Vulnerability Scanner. (Last updated October 3, 2013.)
Nessus v2 File Format	This document explains how the .nessus v2 file format (which is XML-based) is set up and can help you process .nessus v2 files with your own tools. (Last Updated October 15, 2013.)