

Nessus 5.2 Installation and Configuration Guide

June 10, 2014

(Revision 26)

Table of Contents

| | |
|-----------------------------------------------------|----|
| Introduction | 4 |
| Standards and Conventions | 4 |
| Organization..... | 4 |
| New in Nessus 5.2 | 4 |
| Key Feature Updates | 5 |
| Operating System Support | 5 |
| Background | 5 |
| Prerequisites | 7 |
| Nessus Unix | 7 |
| Nessus Windows | 7 |
| Deployment Options | 7 |
| Host-Based Firewalls | 8 |
| Vulnerability Plugins | 8 |
| Nessus Product Types | 8 |
| IPv6 Support | 9 |
| Evaluation to Licensed Upgrade | 9 |
| Unix/Linux | 9 |
| Upgrading..... | 9 |
| Installation..... | 13 |
| Start the Nessus Daemon | 16 |
| Stop the Nessus Daemon..... | 16 |
| Removing Nessus..... | 17 |
| Windows | 19 |
| Upgrading..... | 19 |
| Upgrading from Nessus 4.x..... | 19 |
| Upgrading from Nessus 3.x..... | 20 |
| Installation..... | 20 |
| Downloading Nessus | 20 |
| Installing | 20 |
| Installation Questions..... | 21 |
| Starting and Stopping the Nessus Daemon..... | 23 |
| Removing Nessus..... | 24 |
| Mac OS X | 24 |
| Upgrading..... | 24 |
| Installation..... | 24 |
| Installation Questions..... | 24 |
| Starting and Stopping the Nessus Service | 28 |
| Removing Nessus..... | 29 |
| Feed Registration and UI Configuration | 29 |
| Configuration | 36 |
| LDAP Server..... | 37 |
| Mail Server | 37 |

| | |
|--------------------------------------------------------------|-----------|
| Multi Scanner Settings | 39 |
| Plugin Feed Settings | 39 |
| Proxy Settings | 40 |
| Resetting Activation Codes & Offline Updates..... | 41 |
| Advanced Configuration Options..... | 41 |
| Create and Manage Nessus Users | 43 |
| Create and Manage Nessus User Groups..... | 44 |
| Configure the Nessus Daemon (Advanced Users) | 45 |
| Configuration Options..... | 46 |
| Configuring Nessus with Custom SSL Certificate | 50 |
| Authenticating To Nessus with SSL Certificate | 51 |
| SSL Client Certificate Authentication..... | 51 |
| Configure Nessus for Certificates | 51 |
| Create Nessus SSL Certificates for Login | 52 |
| Enable Connections with Smart Card or CAC Card | 53 |
| Connect with Certificate or Card Enabled Browser | 55 |
| Nessus without Internet Access..... | 56 |
| Generate a Challenge Code | 56 |
| Obtain and Install Up-to-date Plugins | 57 |
| Using and Managing Nessus from the Command Line | 59 |
| Nessus Major Directories..... | 59 |
| Create and Manage Nessus Users with Account Limitations..... | 59 |
| Nessusd Command Line Options..... | 60 |
| Nessus Service Manipulation via Windows CLI | 62 |
| Working with SecurityCenter | 62 |
| SecurityCenter Overview | 62 |
| Configuring SecurityCenter to work with Nessus | 62 |
| Host-Based Firewalls | 63 |
| Nessus Windows Troubleshooting | 64 |
| Installation /Upgrade Issues | 64 |
| Scanning Issues | 64 |
| For Further Information | 65 |
| About Tenable Network Security..... | 67 |

Introduction

This document describes the installation and configuration of Tenable Network Security's **Nessus 5.2** vulnerability scanner. Please email any comments and suggestions to support@tenable.com.

Tenable Network Security, Inc. is the author and maintainer of the Nessus vulnerability scanner. In addition to constantly improving the Nessus engine, Tenable writes most of the plugins available to the scanner, as well as compliance checks and a wide variety of audit policies.

Prerequisites, deployment options, and a walk-through of an installation are described in this document. A basic understanding of Unix and vulnerability scanning is assumed.

Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font such as **setup.exe**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in **courier** (not bold). Following is an example running of the Unix **pwd** command:

```
# pwd  
/opt/nessus/  
#
```



Important notes and considerations are highlighted with this symbol and grey text boxes.



Tips, examples, and best practices are highlighted with this symbol and white on blue text.

Organization

Since the Nessus GUI is standard regardless of operating system, this document is laid out with operating system specific information first, followed by functionality that is common to all operating systems.

New in Nessus 5.2



With the release of Nessus 5, user management and Nessus server (daemon) configuration is managed from the Nessus UI, not via a standalone NessusClient or the **nessusd.conf** file. The Nessus GUI is a web-based interface that handles configuration, policy creation, scans, and all reporting.

As of August 22, 2013, Nessus product names have been revised as shown below:

| Former Product Name | New Product Name |
|--------------------------|-------------------------|
| Nessus Perimeter Service | Nessus Enterprise Cloud |
| Nessus ProfessionalFeed | Nessus |
| Nessus HomeFeed | Nessus Home |

The following list shows official Nessus product names:

- Nessus®
- Nessus Enterprise
- Nessus Enterprise Cloud
- Nessus Auditor Bundles
- Nessus Home

Key Feature Updates

The following are some of the features available in Nessus 5.2. For a complete list of changes, please refer to the Release Notes on the [Discussions Forum](#).

- IPv6 is now supported on most Windows installations.
- Activation code for registration can be obtained during the installation process, from within Nessus.
- Nessus can optionally take screenshots during a vulnerability scan that will be added to the report as evidence of the vulnerability.
- A system preferences pane for Nessus service management on Mac OS X.
- Digitally-signed Nessus RPM packages for supporting distributions.
- Smaller memory footprint and reduced disk space usage.
- Faster, more responsive web interface that uses less bandwidth.
- New functions added to NASL that allow for more complex plugins that use less code.
- After a scan has completed, the results can automatically be emailed to a user.

Operating System Support

Nessus is available and supported for a variety of operating systems and platforms:

- Debian 6 and 7 (i386 and x86-64)
- Fedora 19 and 20 (i386 and x86-64)
- FreeBSD 9 (i386 and x86-64)
- Mac OS X 10.8 and 10.9 (i386 and x86-64)
- Red Hat ES 4 / CentOS 4 (i386)
- 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]
- SuSE 10 (x86-64), 11 (i386 and x86-64)
- Ubuntu 10.04 (9.10 package), 11.10, 12.04, and 12.10 (i386 and x86-64)
- Windows XP, Server 2003, Server 2008, Server 2008 R2*, Server 2012, Vista, 7, and 8 (i386 and x86-64)



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



Nessus utilizes several third-party software packages distributed under varying licenses. Running `nessusd` (or `nessusd.exe` on Windows) with the `-1` argument will display a list of those third-party software licenses.

Background

Nessus is a powerful and easy to use network security scanner with an extensive plugin database that is updated on a daily basis. It is currently rated among the top products of its type throughout the security industry and is endorsed by professional information security organizations such as the SANS Institute. Nessus allows you to remotely audit a given network and determine if it has been compromised or misused in some way. Nessus also provides the ability to locally audit a specific machine for vulnerabilities, compliance specifications, content policy violations, and more.

- **Intelligent Scanning** – Unlike many other security scanners, Nessus does not take anything for granted. That is, it will not assume that a given service is running on a fixed port. This means if you run your web server on port 1234, Nessus will detect it and test its security appropriately. It will attempt to validate a vulnerability through exploitation when possible. In cases where it is not reliable or may negatively impact the target, Nessus may rely on a server banner to determine the presence of the vulnerability. In such cases, it will be clear in the report output if this method was used.
- **Modular Architecture** – The client/server architecture provides the flexibility to deploy the scanner (server) and connect to the GUI (client) from any machine with a web browser, reducing management costs (one server can be accessed by multiple clients).
- **CVE Compatible** – Most plugins link to CVE for administrators to retrieve further information on published vulnerabilities. They also frequently include references to Bugtraq (BID), OSVDB, and vendor security alerts.
- **Plugin Architecture** – Each security test is written as an external plugin and grouped into one of 42 families. This way, you can easily add your own tests, select specific plugins, or choose an entire family without having to read the code of the Nessus server engine, `nessusd`. The complete list of the Nessus plugins is available at <http://www.nessus.org/plugins/index.php?view=all>.
- **NASL** – The Nessus scanner includes NASL (Nessus Attack Scripting Language), a language designed specifically to write security tests easily and quickly.
- **Up-to-date Security Vulnerability Database** – Tenable focuses on the development of security checks for newly disclosed vulnerabilities. Our security check database is updated on a daily basis and all the newest security checks are available at <http://www.tenable.com/plugins/index.php?view=newest>.
- **Tests Multiple Hosts Simultaneously** – Depending on the configuration of the Nessus scanner system, you can test a large number of hosts concurrently.
- **Smart Service Recognition** – Nessus does not expect the target hosts to respect IANA assigned port numbers. This means that it will recognize a FTP server running on a non-standard port (e.g., 31337) or a web server running on port 8080 instead of 80.
- **Multiple Services** – If two or more web servers are run on a host (e.g., one on port 80 and another on port 8080), Nessus will identify and test all of them.
- **Plugin Cooperation** – The security tests performed by Nessus plugins cooperate so that unnecessary checks are not performed. If your FTP server does not offer anonymous logins, then anonymous login related security checks will not be performed.
- **Complete Reports** – Nessus will not only tell you what security vulnerabilities exist on your network and the risk level of each (Info, Low, Medium, High, and Critical), but it will also tell you how to mitigate them by offering solutions.
- **Full SSL Support** – Nessus has the ability to test services offered over SSL such as HTTPS, SMTPS, IMAPS and more.
- **Smart Plugins (optional)** – Nessus has an “optimization” option that will determine which plugins should or should not be launched against the remote host. For example, Nessus will not test sendmail vulnerabilities against Postfix.
- **Non-Destructive (optional)** – Certain checks can be detrimental to specific network services. If you do not want to risk causing a service failure on your network, enable the “safe checks” option of Nessus, which will make Nessus rely on banners rather than exploiting real flaws to determine if a vulnerability is present.
- **Open Forum** – Found a bug? Questions about Nessus? Start a discussion at <https://discussions.nessus.org/>.

Prerequisites

Tenable recommends the following hardware depending on how Nessus is used. Note that these resources are recommended specifically for running Nessus. Additional software or workload on the machine warrants additional resources.

| Scenario | CPU/Memory | Disk Space |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|------------|
| Nessus scanning smaller networks | CPU: 1 Pentium 4 dual-core 2 GHz CPU (dual-core Intel® for Mac OS X) Memory: 2 GB RAM (4 GB RAM recommended) | 30 GB |
| Nessus scanning large networks including audit trails and PDF report generation | CPU: 1 Pentium 4 dual-core 3 GHz CPU (2 dual-core recommended) Memory: 3 - 4 GB RAM (8 GB RAM recommended) | 30 GB |

Nessus can be run under a VMware instance, but if the 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.

Nessus Unix

Before installing Nessus on Unix/Linux, there are several libraries that are required. Many operating systems install these by default and typically do not require separate installation:

- [zlib](#)
- [GNU C Library](#) (i.e., libc)
- [Oracle Java](#) (for PDF reporting only)



Java must be installed on the host before Nessus is installed. If Java is installed afterwards, then Nessus will need to be reinstalled.



Nessus does not support installing to a directory or location via a symlink. If required disk space exists outside of the `/opt` file system, mount the desired target directory using `mount --bind <olddir> <newdir>`. Make sure that the file system is automatically mounted on reboot by editing the `/etc/fstab` file accordingly.

Nessus Windows

Microsoft has added changes to Windows XP SP2 and newer that can impact the performance of Nessus Windows. For increased performance and scan reliability, it is highly recommended that Nessus Windows be installed on a server product from the Microsoft Windows family such as Windows Server 2003. For more information on this issue, please see the "[Nessus Windows Troubleshooting](#)" section.

Deployment Options

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 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.

By default, port 8834 is used for the Nessus Web Server (user interface). On Microsoft XP Service Pack 2 (SP2) systems and later, clicking on the “**Security Center**” icon available in the “**Control Panel**” presents the user with the opportunity to manage the “Windows Firewall” settings. To open up TCP port 8834, choose the “**Exceptions**” tab and then add port “8834” to the list.

For other personal firewall software, consult the vendor’s documentation for configuration instructions.

Vulnerability Plugins

Numerous new vulnerabilities are made public by vendors, researchers, and other sources every day. Tenable strives to have checks for recently published vulnerabilities tested and available as soon as possible, usually within 24 hours of disclosure. The check for a specific vulnerability is known by the Nessus scanner as a “plugin”. A complete list of all the Nessus plugins is available at <http://www.tenable.com/plugins/index.php?view=all>. Tenable distributes the latest vulnerability plugins in two modes: Nessus and Nessus Home.

Plugins are downloaded directly from Tenable through an automated process within Nessus. Nessus verifies the digital signatures of all plugin downloads to ensure file integrity. For Nessus installations without access to the Internet, there is an [offline update process](#) that can be used to ensure the scanner stays up to date.



You are required to register for plugins and update them before Nessus will start and the Nessus scan interface becomes available. The plugin update occurs in the background after initial scanner registration and can take several minutes.

Nessus Product Types

Tenable provides commercial support, via the [Tenable Support Portal](#) or email, to Nessus customers who are using version 5 or later. Nessus also includes a set of host-based compliance checks for Unix and Windows that are very useful when performing compliance audits such as for SOX, FISMA, or PCI DSS.

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



If you are using Nessus in conjunction with Tenable’s SecurityCenter, SecurityCenter will automatically update your Nessus scanners.

If you are a 501(c)(3) charitable organization, you may be eligible to use Nessus at no cost. For more information, please visit the [Tenable Charitable Organization Subscription Program](#) web page.

If you are using Nessus at home for non-professional purposes, you may subscribe to Nessus Home. There is no charge to use Nessus Home, however, there is a separate subscription agreement for Nessus Home that users must agree to comply with.

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.



Older versions of Microsoft Windows lack some of the key APIs needed for IPv6 packet forgery (e.g., getting the MAC address of the router, routing table, etc.). This prevents the port scanner from working properly. As a result, IPv6 support is not available on Windows XP or Server 2003.



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”.

Evaluation to Licensed Upgrade

If you install Nessus with an evaluation license, it is strongly recommended that you uninstall it before migrating to a fully licensed copy. Any policies or scan results you created can be exported and re-imported into the new installation.

Unix/Linux

Upgrading

This section explains how to upgrade Nessus from a previous Nessus installation.

Download the latest version of Nessus from <http://www.tenable.com/products/nessus/select-your-operating-system> or through the [Tenable Support Portal](#). Confirm the integrity of the installation package by comparing the download MD5 checksum with the one listed in the `MD5.asc` file [here](#).



Unless otherwise noted, all commands must be performed as the system’s `root` user. Regular user accounts typically do not have the privileges required to install this software.

The following table provides upgrade instructions for the Nessus server on all previously supported platforms. Configuration settings and users that were created previously will remain intact.



Make sure any running scans have finished before stopping `nessusd`.

Any special upgrade instructions are provided in a note following the example. Nessus can be installed with several package managers including `rpm` and `yum`. Syntax for installation using `rpm` is shown below. These commands can be replaced by your package manager of choice in most cases. For example, administrators that prefer to use `yum` would use the following syntax:

```
# yum -y localinstall [pkg]
```

| Platform | Upgrade Instructions |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Red Hat ES 4 and CentOS 4 (32 bit); Red Hat ES 5, CentOS 5, and Oracle Linux 5 (32 and 64 bit); Red Hat ES 6, CentOS 6, and Oracle Linux 6 (32 and 64 bit) | |
| Upgrade Commands | <pre># service nessusd stop</pre> <p>Use one of the appropriate commands below that corresponds to the version of Red Hat you are running:</p> <pre># rpm -Uvh Nessus-5.2.6-es4.i386.rpm # rpm -Uvh Nessus-5.2.6-es5.i386.rpm # rpm -Uvh Nessus-5.2.6-es5.x86_64.rpm # rpm -Uvh Nessus-5.2.6-es6.i686.rpm # rpm -Uvh Nessus-5.2.6-es6.x86_64.rpm</pre> <p>Once the upgrade is complete, restart the <code>nessusd</code> service with the following command:</p> <pre># service nessusd start</pre> |
| Sample Output | <pre># service nessusd stop Shutting down Nessus services: [OK] # rpm -Uvh Nessus-5.2.6-es5.i386.rpm Preparing... ##### [100%] Shutting down Nessus services: /etc/init.d/nessusd: ... 1:Nessus ##### [100%] Fetching the newest plugins from nessus.org... Fetching the newest updates from nessus.org... Done. The Nessus server will start processing these plugins within a minute nessusd (Nessus) 5.2.6 [build R23016] for Linux (C) 1998 - 2014 Tenable Network Security, Inc. Processing the Nessus plugins... [#####] All plugins loaded - You can start nessusd by typing /sbin/service nessusd start - Then go to https://localhost:8834/ to configure your scanner# service nessusd start Starting Nessus services: [OK] #</pre> |
| Fedora 19 and 20 (32 and 64 bit) | |
| Upgrade Commands | <pre># service nessusd stop</pre> <p>Use one of the appropriate commands below that corresponds to the version of Fedora you are running:</p> <pre># rpm -Uvh Nessus-5.2.6-fc16.i686.rpm # rpm -Uvh Nessus-5.2.6-fc16.x86_64.rpm</pre> <p>Once the upgrade is complete, restart the <code>nessusd</code> service with the following command:</p> |

| | |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <pre># service nessusd start</pre> |
| Sample Output | <pre># service nessusd stop Shutting down Nessus services: [OK] # rpm -Uvh Nessus-5.2.6-fc16.i386.rpm [...]</pre> <pre># service nessusd start Starting Nessus services: [OK] #</pre> |
| SuSE 10 (64 bit), 11 (32 and 64 bit) | |
| Upgrade Commands | <pre># service nessusd stop</pre> <p>Use one of the appropriate commands below that corresponds to the version of SuSE you are running:</p> <pre># rpm -Uvh Nessus-5.2.6-suse10.x86_64.rpm # rpm -Uvh Nessus-5.2.6-suse11.i586.rpm # rpm -Uvh Nessus-5.2.6-suse11.x86_64.rpm</pre> <p>Once the upgrade is complete, restart the <code>nessusd</code> service with the following command:</p> <pre># service nessusd start</pre> |
| Sample Output | <pre># service nessusd stop Shutting down Nessus services: [OK] # rpm -Uvh Nessus-5.2.6-suse11.i586.rpm Preparing... [...]</pre> <pre># service nessusd start Starting Nessus services: [OK] #</pre> |
| Debian 6 and 7 (32 and 64 bit) | |
| Upgrade Commands | <pre># /etc/init.d/nessusd stop</pre> <p>Use one of the appropriate commands below that corresponds to the version of Debian you are running:</p> <pre># dpkg -i Nessus-5.2.6-debian6_i386.deb # dpkg -i Nessus-5.2.6-debian6_amd64.deb</pre> <pre># /etc/init.d/nessusd start</pre> |
| Sample Output | <pre># /etc/init.d/nessusd stop # dpkg -i Nessus-5.2.6-debian6_i386.deb (Reading database ... 19831 files and directories currently installed.) Preparing to replace nessus 5.2.5 (using Nessus-5.2.6-</pre> |

| | |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <pre> debian6_i386.deb) ... [..] # /etc/init.d/nessusd start Starting Nessus : . # </pre> |
| Ubuntu 10.04 (9.10 package), 11.10, 12.04, and 12.10 (i386 and x86-64) | |
| Upgrade Commands | <pre> # /etc/init.d/nessusd stop </pre> <p>Use one of the appropriate commands below that corresponds to the version of Ubuntu you are running:</p> <pre> # dpkg -i Nessus-5.2.6-ubuntu910_i386.deb # dpkg -i Nessus-5.2.6-ubuntu910_amd64.deb # dpkg -i Nessus-5.2.6-ubuntu1110_i386.deb # dpkg -i Nessus-5.2.6-ubuntu1110_amd64.deb </pre> <pre> # /etc/init.d/nessusd start </pre> |
| Sample Output | <pre> # /etc/init.d/nessusd stop # dpkg -i Nessus-5.2.6-ubuntu1110_i386.deb (Reading database ... 19831 files and directories currently installed.) Preparing to replace nessus 5.2.5 (using Nessus-5.2.6- ubuntu1110_i386.deb) ... [..] # /etc/init.d/nessusd start Starting Nessus : . # </pre> |
| FreeBSD 9 (32 and 64 bit) | |
| Upgrade Commands | <pre> # killall nessusd # pkg_info </pre> <p>This command will produce a list of all the packages installed and their descriptions. The following is example output for the previous command showing the Nessus package:</p> <pre> Nessus-5.2.5 A powerful security scanner </pre> <p>Remove the Nessus package using the following command:</p> <pre> # pkg_delete <package name> </pre> <p>Use one of the appropriate commands below that corresponds to the version of FreeBSD you are running:</p> <pre> # pkg_add Nessus-5.2.6-fbsd9.tbz </pre> |

| | |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <pre># pkg_add Nessus-5.2.6-fbsd9.amd64.tbz # /usr/local/nessus/sbin/nessusd -D</pre> |
| Sample Output | <pre># killall nessusd # pkg_delete Nessus-5.2.5 # pkg_add Nessus-5.2.6-fbsd9.tbz nessusd (Nessus) 5.2.6. for FreeBSD (C) 2014 Tenable Network Security, Inc. [...]</pre> <pre># /usr/local/nessus/sbin/nessusd -D nessusd (Nessus) 5.2.6. for FreeBSD (C) 2013 Tenable Network Security, Inc. Processing the Nessus plugins... [#####] All plugins loaded #</pre> |
| Notes | To upgrade Nessus on FreeBSD you must first uninstall the existing version and then install the newest release. This process will not remove the configuration files or files that were not part of the original installation. |

Installation

Download the latest version of Nessus from <http://www.tenable.com/products/nessus/select-your-operating-system> or through the [Tenable Support Portal](#). Confirm the integrity of the installation package by comparing the download MD5 checksum with the one listed in the MD5 .asc file [here](#).



Unless otherwise noted, all commands must be performed as the system's `root` user. Regular user accounts typically do not have the privileges required to install this software.

The following table provides installation instructions for the Nessus server on all supported platforms. Any special installation instructions are provided in a note following the example.

| Platform | Installation Instructions |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Red Hat ES 4 and CentOS 4 (32 bit); Red Hat ES 5, CentOS 5, and Oracle Linux 5 (32 and 64 bit); Red Hat ES 6, CentOS 6, and Oracle Linux 6 (32 and 64 bit) | |
| Install Command | <p>Use one of the appropriate commands below that corresponds to the version of Red Hat you are running:</p> <pre># rpm -ivh Nessus-5.2.6-es4.i386.rpm # rpm -ivh Nessus-5.2.6-es5.i386.rpm # rpm -ivh Nessus-5.2.6-es5.x86_64.rpm # rpm -ivh Nessus-5.2.6-es6.i686.rpm # rpm -ivh Nessus-5.2.6-es6.x86_64.rpm</pre> |
| Sample Output | <pre># rpm -ivh Nessus-5.2.6-es4.i386.rpm Preparing...</pre> |

| | |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <pre>##### [100%] 1:Nessus ##### [100%] nessusd (Nessus) 5.2.6 [build R23011] for Linux (C) 1998 - 2014 Tenable Network Security, Inc. Processing the Nessus plugins... [#####] All plugins loaded - You can start nessusd by typing /sbin/service nessusd start - Then go to https://localhost:8834/ to configure your scanner #</pre> |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Fedora 19 and 20 (32 and 64 bit)

| | |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Install Command | <p>Use one of the appropriate commands below that corresponds to the version of Fedora you are running:</p> <pre># rpm -ivh Nessus-5.2.6-fc16.i686.rpm # rpm -ivh Nessus-5.2.6-fc16.x86_64.rpm</pre> |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | |
|----------------------|----------------------------------------------------------------------|
| Sample Output | <pre># rpm -ivh Nessus-5.2.6-fc16.i386.rpm Preparing... [.] #</pre> |
|----------------------|----------------------------------------------------------------------|

SuSE 10 (64 bit), 11 (32 and 64 bit)

| | |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Install Command | <p>Use one of the appropriate commands below that corresponds to the version of SuSE you are running:</p> <pre># rpm -ivh Nessus-5.2.6-suse10.x86_64.rpm # rpm -ivh Nessus-5.2.6-suse11.i586.rpm # rpm -ivh Nessus-5.2.6-suse11.x86_64.rpm</pre> |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | |
|----------------------|------------------------------------------------------------------------------------------------------------|
| Sample Output | <pre># rpm -ivh Nessus-5.2.6-suse11.i586.rpm Preparing...##### [100%] 1:Nessus ##### [100%] [.] #</pre> |
|----------------------|------------------------------------------------------------------------------------------------------------|

Debian 6 and 7 (32 and 64 bit)

| | |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Install Command | <p>Use one of the appropriate commands below that corresponds to the version of Debian you are running:</p> <pre># dpkg -i Nessus-5.2.6-debian6_i386.deb # dpkg -i Nessus-5.2.6-debian6_amd64.deb</pre> |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sample Output | <pre># dpkg -i Nessus-5.2.6-debian6_i386.deb Selecting previously deselected package nessus. (Reading database ... 36954 files and directories currently</pre> |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <pre> installed.) Unpacking nessus (from Nessus-5.2.6-debian6_i386.deb) ... Setting up nessus (5.2.6) ... [.] # </pre> |
| Ubuntu 10.04 (9.10 package), 11.10, 12.04, and 12.10 (i386 and x86-64) | |
| Install Command | <p>Use one of the appropriate commands below that corresponds to the version of Ubuntu you are running:</p> <pre> # dpkg -i Nessus-5.2.6-ubuntu910_i386.deb # dpkg -i Nessus-5.2.6-ubuntu910_amd64.deb # dpkg -i Nessus-5.2.6-ubuntu1110_i386.deb # dpkg -i Nessus-5.2.6-ubuntu1110_amd64.deb </pre> |
| Sample Output | <pre> # dpkg -i Nessus-5.2.6-ubuntu1110_amd64.deb Selecting previously deselected package nessus. (Reading database ... 32444 files and directories currently installed.) Unpacking nessus (from Nessus-5.2.6-ubuntu1110_amd64.deb) ... Setting up nessus (5.2.6) ... [.] # </pre> |
| FreeBSD 9 (32 and 64 bit) | |
| Install Command | <p>Use one of the appropriate commands below that corresponds to the version of FreeBSD you are running:</p> <pre> # pkg_add Nessus-5.2.6-fbsd9.tbz # pkg_add Nessus-5.2.6-fbsd9.amd64.tbz </pre> |
| Sample Output | <pre> # pkg_add Nessus-5.2.6-fbsd9.tbz nessusd (Nessus) 5.2.6 for FreeBSD (C) 1998 - 2014 Tenable Network Security, Inc. [.] # </pre> |

When the installation is completed, start the **nessusd** daemon as instructed in the next section depending on the distribution. Once Nessus is installed, you must visit the scanner URL provided to complete the registration process.



Note: Unix-based installations may provide a URL containing a relative host name that is not in DNS (e.g., <https://myserver:8834/>). If the host name is not in DNS, you must connect to the Nessus server using an IP address or a valid DNS name.

After that process is complete, it is recommended that you authenticate and customize the configuration options for your environment as described in the “[Feed Registration and GUI Configuration](#)” section.



Nessus must be installed to `/opt/nessus`, although a symbolic link pointing to `/opt/nessus` is acceptable.

Start the Nessus Daemon

Start the Nessus service as `root` with the following command:

Linux:

```
# /opt/nessus/sbin/nessus-service -D
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessus-service -D
```

Below is an example of the screen output for starting `nessusd` for Red Hat:

```
[root@squirrel ~]# /sbin/service nessusd start
Starting Nessus services: [ OK ]
[root@squirrel ~]#
```

If you wish to suppress the output of the command, use the “`-q`” option as follows:

Linux:

```
# /opt/nessus/sbin/nessus-service -q -D
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessus-service -q -D
```

Alternatively, Nessus may be started using the following command depending on the operating system platform:

| Operating System | Command to Start <code>nessusd</code> |
|---------------------------------|-----------------------------------------------------|
| Red Hat, CentOS, & Oracle Linux | <code># /sbin/service nessusd start</code> |
| Fedora | <code># /sbin/service nessusd start</code> |
| SuSE | <code># /etc/rc.d/nessusd start</code> |
| Debian | <code># /etc/init.d/nessusd start</code> |
| FreeBSD | <code># /usr/local/etc/rc.d/nessusd.sh start</code> |
| Ubuntu | <code># /etc/init.d/nessusd start</code> |

Continue with the section “[Feed Registration and GUI Configuration](#)” to install the plugin Activation Code.

Stop the Nessus Daemon

If you need to stop the `nessusd` service for any reason, the following command will halt Nessus **and abruptly stop any on-going scans**:

```
# killall nessusd
```

It is recommended that you use the more graceful shutdown script provided by your operating system instead:

| Operating System | Command to Stop <code>nessusd</code> |
|---------------------------------|----------------------------------------------------|
| Red Hat, CentOS, & Oracle Linux | <code># /sbin/service nessusd stop</code> |
| Fedora | <code># /sbin/service nessusd stop</code> |
| SuSE | <code># /etc/rc.d/nessusd stop</code> |
| Debian | <code># /etc/init.d/nessusd stop</code> |
| FreeBSD | <code># /usr/local/etc/rc.d/nessusd.sh stop</code> |
| Ubuntu | <code># /etc/init.d/nessusd stop</code> |

Removing Nessus

The following table provides instructions for removing the Nessus server on all supported platforms. Except for the Mac OS X instructions, the instructions provided will not remove the configuration files or files that were not part of the original installation. Files that were part of the original package but have changed since installation will not be removed as well. To completely remove the remaining files use the following command:

Linux:

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

FreeBSD:

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

| Platform | Removal Instructions |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Red Hat ES 4 and CentOS 4 (32 bit); Red Hat ES 5, CentOS 5, and Oracle Linux 5 (32 and 64 bit); Red Hat ES 6, CentOS 6, and Oracle Linux 6 (32 and 64 bit) | |
| Remove Command | Determine the package name: <pre># rpm -qa grep Nessus</pre> Use the output from the above command to remove the package: <pre># rpm -e <Package Name></pre> |
| Sample Output | <pre># rpm -qa grep -i nessus Nessus-5.2.6-es5 # rpm -e Nessus-5.2.6-es5 #</pre> |
| Fedora 19 and 20 (32 and 64 bit) | |
| Remove Command | Determine the package name: <pre># rpm -qa grep Nessus</pre> |

| | |
|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>Use the output from the above command to remove the package:</p> <pre># rpm -e <Package Name></pre> |
| SuSE 10 (64 bit), 11 (32 and 64 bit) | |
| Remove Command | <p>Determine the package name:</p> <pre># rpm -qa grep Nessus</pre> <p>Use the output from the above command to remove the package:</p> <pre># rpm -e <Package Name></pre> |
| Debian 6 and 7 (32 and 64 bit) | |
| Remove Command | <p>Determine the package name:</p> <pre># dpkg -l grep -i nessus</pre> <p>Use the output from the above command to remove the package:</p> <pre># dpkg -r <package name></pre> |
| Sample Output | <pre># dpkg -l grep nessus ii nessus 5.2.6 Version 5 of the Nessus Scanner # dpkg -r nessus #</pre> |
| Ubuntu 10.04 (9.10 package), 11.10, 12.04, and 12.10 (i386 and x86-64) | |
| Remove Command | <p>Determine the package name:</p> <pre># dpkg -l grep -i nessus</pre> <p>Use the output from the above command to remove the package:</p> <pre># dpkg -r <package name></pre> |
| Sample Output | <pre># dpkg -l grep -i nessus ii nessus 5.2.6 Version 5 of the Nessus Scanner #</pre> |
| FreeBSD 9 (32 and 64 bit) | |
| Remove Command | <p>Stop Nessus:</p> <pre># killall nessusd</pre> <p>Determine the package name:</p> <pre># pkg_info grep -i nessus</pre> |

| | |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Remove the Nessus package: # <code>pkg_delete <package name></code> |
| Sample Output | # <code>killall nessusd</code> # <code>pkg_info grep -i nessus</code> Nessus-5.2.6 A powerful security scanner # <code>pkg_delete Nessus-5.2.4</code> # |

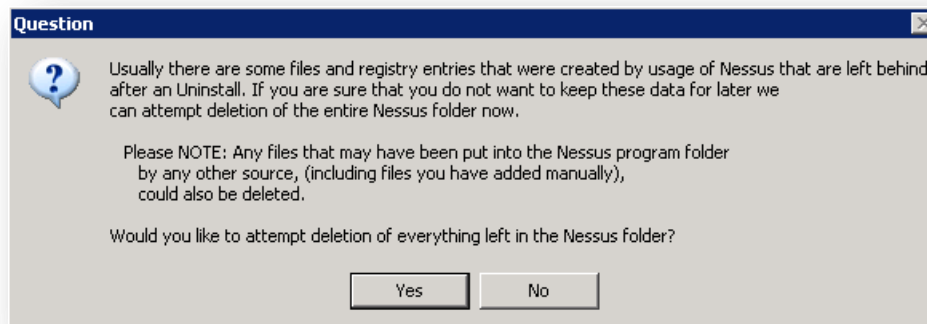
Windows

Upgrading

Upgrading from Nessus 5.x to a higher 5.x version is straightforward and does not require any special considerations.

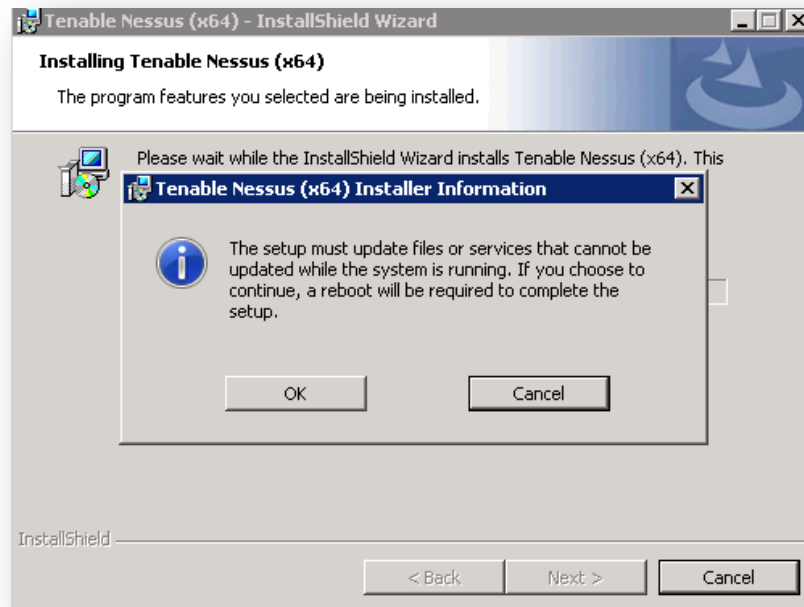
Upgrading from Nessus 4.x

When upgrading Nessus from a 4.x version to a newer 5.x distribution, the upgrade process will ask if the user wants to delete everything in the Nessus directory. Choosing this option (by selecting “Yes”) will mimic an uninstall process. If you choose this option, previously created users, existing scan policies, and scan results will be removed, and the scanner will become unregistered.



Click on “Yes” to allow Nessus to attempt to delete the entire Nessus folder along with any manually added files or “No” to maintain the Nessus folder along with existing scans, reports, etc. After the new version of Nessus is installed, they will still be available for viewing and exporting.

The user may also be prompted to reboot the system depending on the version being installed, and the version currently on the system:



Upgrading from Nessus 3.x

A direct upgrade from Nessus 3.0.x to Nessus 5.x is not supported. However, an upgrade to 4 can be used as an interim step to ensure that vital scan settings and policies are preserved. If scan settings do not need to be kept, uninstall Nessus 3.x first and then install a fresh copy of Nessus 5.



Selecting “Yes” will delete all files in the Nessus directory, including log files, manually added custom plugins, and more. Choose this option carefully!

Installation

Downloading Nessus

The latest version of Nessus is available at <http://www.tenable.com/products/nessus/select-your-operating-system> or through the [Tenable Support Portal](#). Nessus 5 is available for Windows XP, Server 2003, Server 2008, Vista, and Windows 7. Confirm the integrity of the installation package by comparing the download MD5 checksum with the one listed in the `MD5.asc` file [here](#).

Nessus distribution file sizes and names vary slightly from release to release, but are approximately 25 MB in size.

Installing

Nessus is distributed as an executable installation file. Place the file on the system it is being installed on or a shared drive accessible by the system.

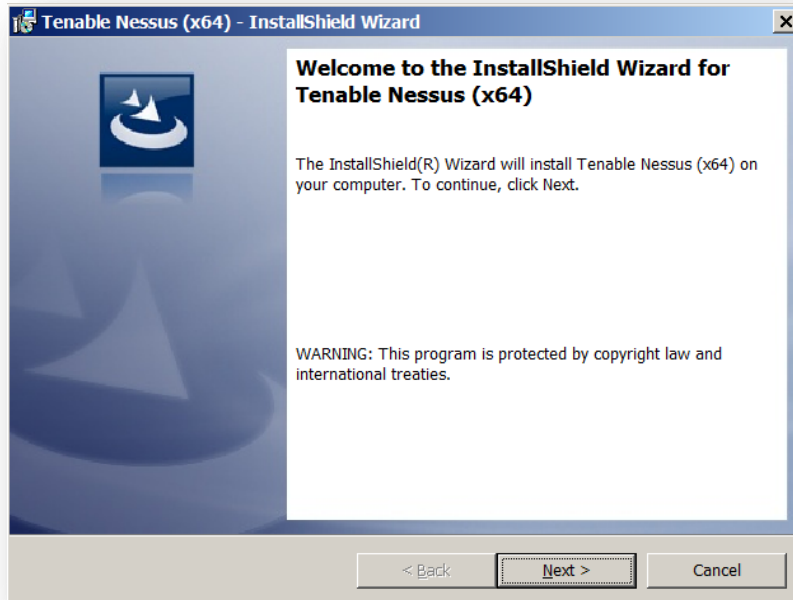
You must install Nessus using an administrative account and not as a non-privileged user. If you receive any errors related to permissions, “Access Denied”, or errors suggesting an action occurred due to lack of privileges, ensure that you are using an account with administrative privileges. If you receive these errors while using command line utilities, run `cmd.exe` with “Run as...” privileges set to “administrator”.



Some antivirus software packages can classify Nessus as a worm or some form of malware. This is due to the large number of TCP connections generated during a scan. If your AV software gives a warning, click on “allow” to let Nessus continue scanning. Most AV packages allow you to add processes to an exception list as well. Add `Nessus.exe` and `Nessus-service.exe` to this list to avoid such warnings.

It is recommended that you obtain a plugin feed activation code before starting the installation process, as that information will be required before you can authenticate to the Nessus GUI interface. For more information on obtaining an activation code, read the section titled [Vulnerability Plugins](#).

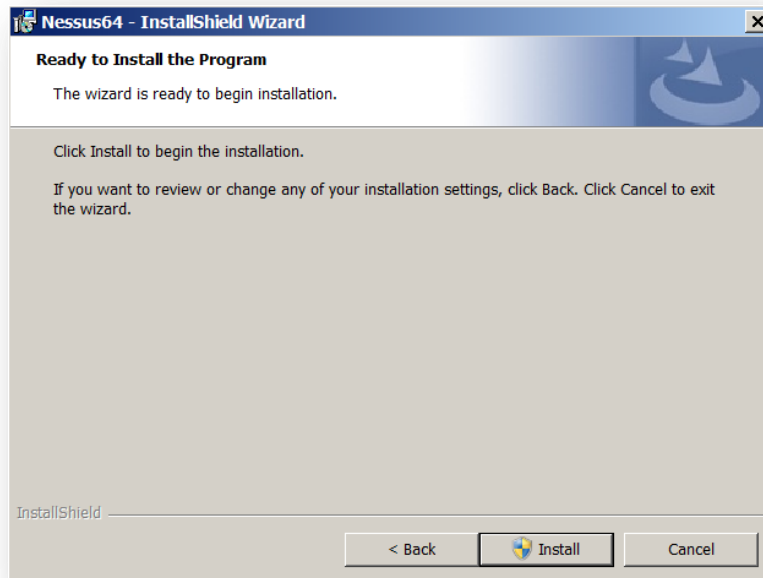
Installation Questions



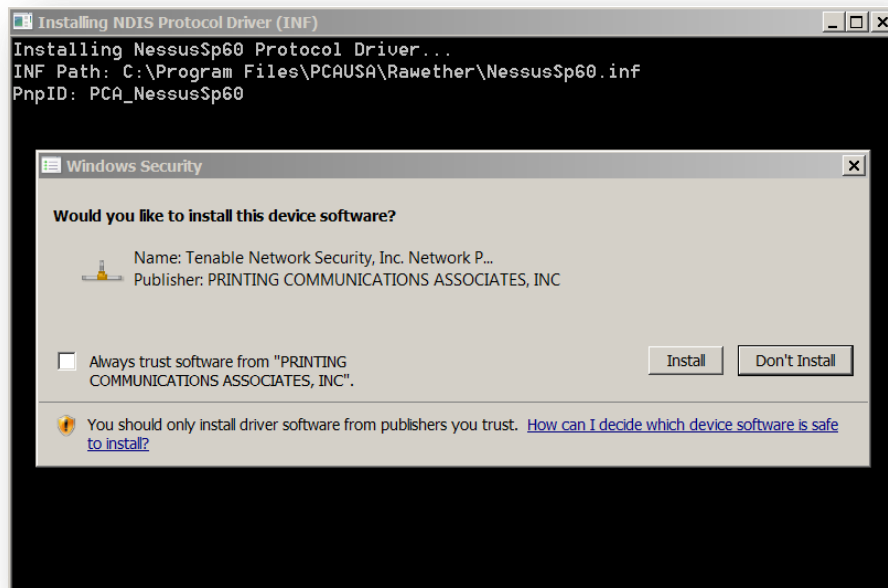
During the installation process, Nessus will prompt you for some basic information. Before you begin, you must read and agree to the license agreement:



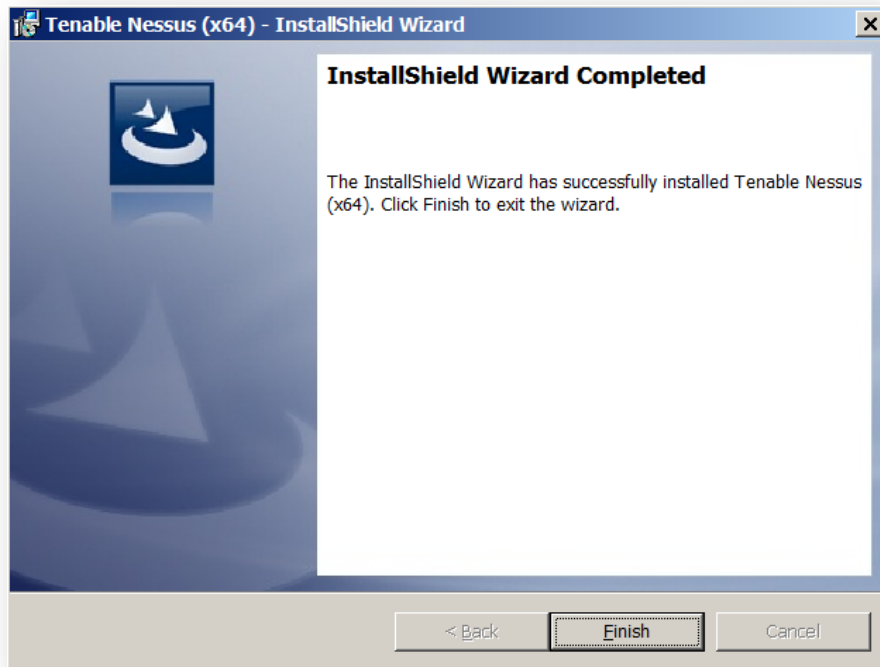
You will be prompted to confirm the installation:



After the initial installation is complete, Nessus will initiate the installation of a third-party driver that is used to support Ethernet communication for Nessus, if it is not already present on your system:



Once installation is complete, click “Finish”:



At this point, Nessus will continue by loading a page in your default web browser that will handle the initial configuration, which is discussed in the section [“Feed Registration and GUI Configuration”](#).

Starting and Stopping the Nessus Daemon

During the installation and daily operation of Nessus, manipulating the Nessus service is generally not required. There are times when an administrator may wish to temporarily stop or restart the service though.

This can be done on a Windows system by opening the “Start” menu and clicking “Run”. In the “Run” box, type in “services.msc” to open the Windows Service Manager:

| Name ^ | Description | Status | Startup Type | Log On As |
|---------------------------|---------------------------------------|---------|--------------|-----------------|
| Task Scheduler | Enables a user to configure and sc... | Started | Automatic | Local System |
| TCP/IP NetBIOS Helper | Provides support for the NetBIOS ... | Started | Automatic | Local Service |
| Telephony | Provides Telephony API (TAPI) sup... | | Manual | Network Service |
| Tenable Nessus | Tenable Nessus Network Security ... | Started | Automatic | Local System |
| Tenable PVS Proxy Service | Tenable Passive Vulnerability Scan... | | Automatic | Local System |
| Themes | Provides user experience theme m... | Started | Automatic | Local System |
| Thread Ordering Server | Provides ordered execution for a g... | | Manual | Local Service |

Right clicking on the “Tenable Nessus” service displays a dialogue box that allows you to start, stop, pause, resume, or restart the service depending on the current status.

In addition, the Nessus service can be manipulated via the command line. For more information, consult the [“Nessus Service Manipulation via Windows CLI”](#) section in this document.

Removing Nessus

To remove Nessus, under the Control Panel open “**Add or Remove Programs**”. Select “**Tenable Nessus**” and then click on the “**Change/Remove**” button. This will open the InstallShield Wizard. Follow the directions in this wizard to completely remove Nessus. You will be prompted to decide if you want to remove the entire Nessus folder. Reply “Yes” only if you do not want to retain any scan results or policies that you may have generated.



When uninstalling Nessus, Windows will ask if you want to continue, but display what appears to be an arbitrary `.msi` file that is unsigned. For example:

```
C:\Windows\Installer\778608.msi  
Publisher: Unknown
```

This is due to Windows keeping an internal copy of the Nessus installer and using it to initiate the uninstall process. It is safe to approve this request.

Mac OS X

Upgrading

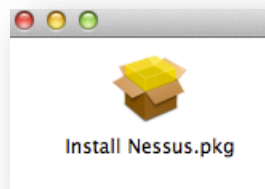
Upgrading from an older version of Nessus is the same as performing a fresh install. Download the file `Nessus-5.x.x.dmg.gz`, and then double-click on it to unzip it. Double click on the `Nessus-5.x.x.dmg` file, which will mount the disk image and make it appear under “Devices” in “Finder”. Once the volume “Nessus 5” appears in “Finder”, double click on the file Nessus 5. When the installation is complete, log into Nessus via your browser at <https://localhost:8834>.

Installation

The latest version of Nessus is available at <http://www.tenable.com/products/nessus/select-your-operating-system> or through the [Tenable Support Portal](#). Nessus is available for Mac OS X 10.8 and 10.9. Confirm the integrity of the installation package by comparing the download MD5 checksum with the one listed in the MD5.asc file [here](#).

The Nessus distribution file size for Mac OS X varies slightly from release to release, but is approximately 45 MB in size.

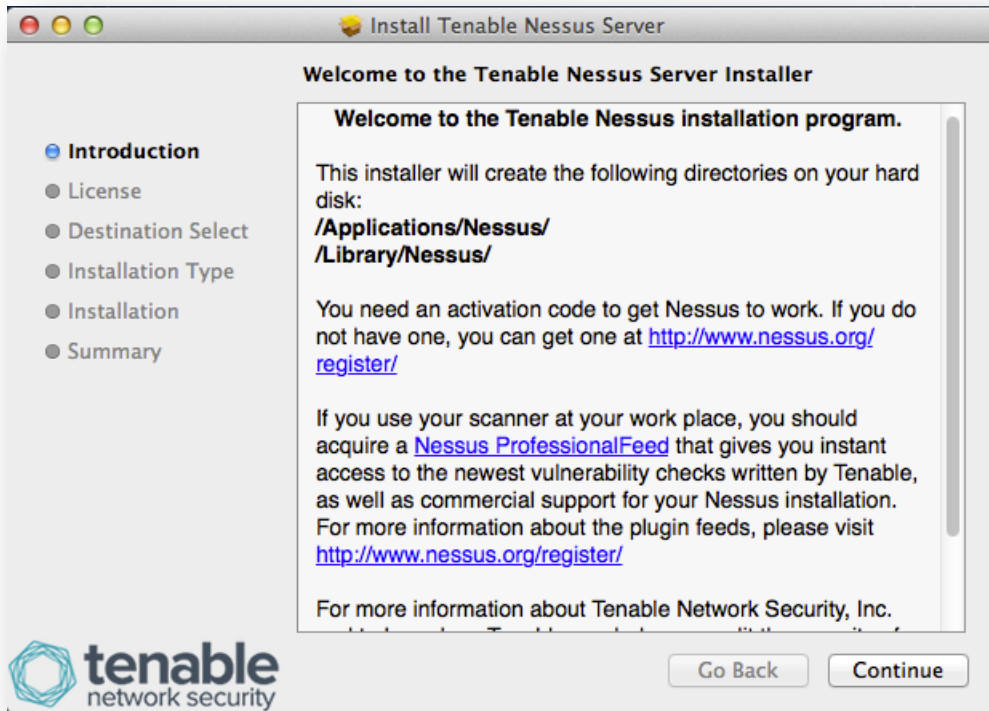
To install Nessus on Mac OS X, you need to download the file `Nessus-5.x.x.dmg.gz`, and then double click on it to unzip it. Double click on the `Nessus-5.x.x.dmg` file, which will mount the disk image and make it appear under “Devices” in “Finder”. Once the volume “Nessus 5” appears in “Finder”, double click on the file `Nessus 5` as shown below:



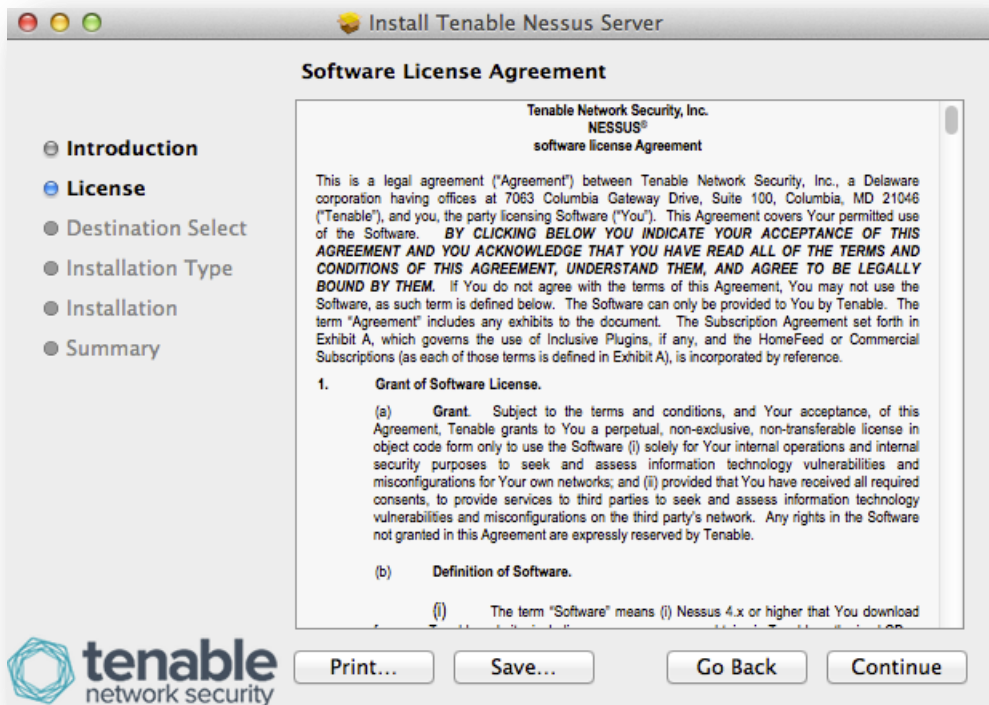
Note that you will be prompted for an administrator user name and password at one point during the installation.

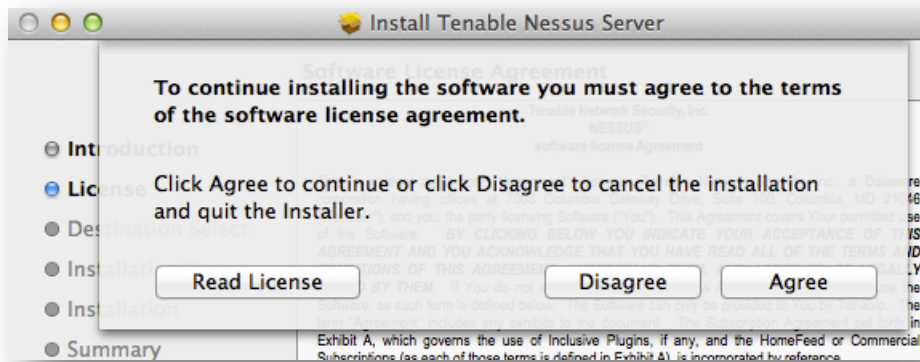
Installation Questions

The installation will be displayed as follows:

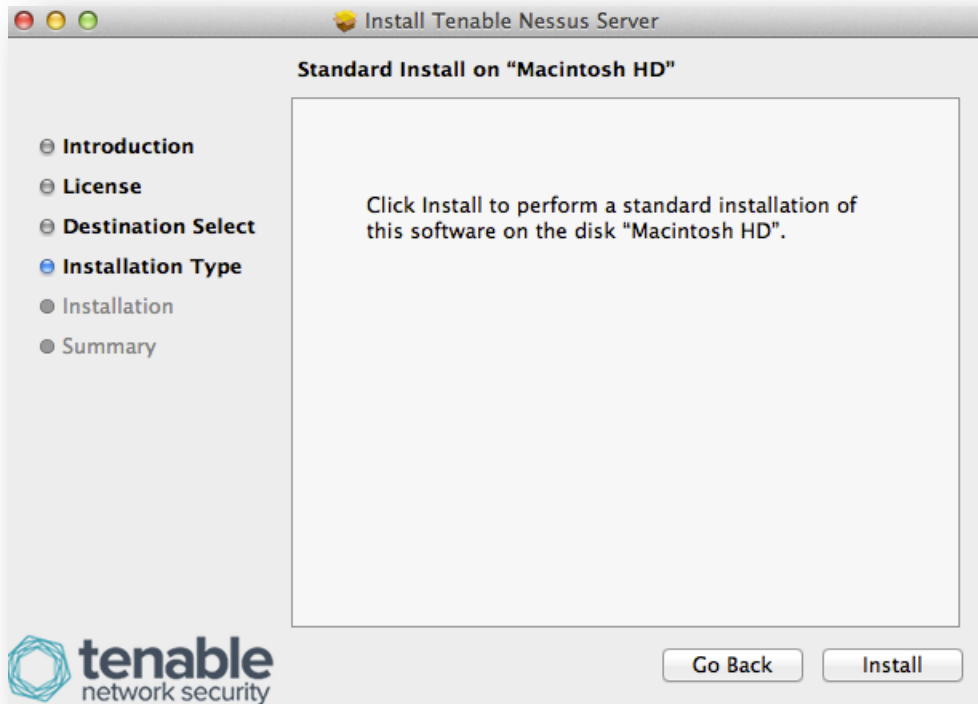


Click “Continue”, and the software license will be displayed. Click “Continue” again, and a dialog box will appear requiring that you accept the license terms before continuing:





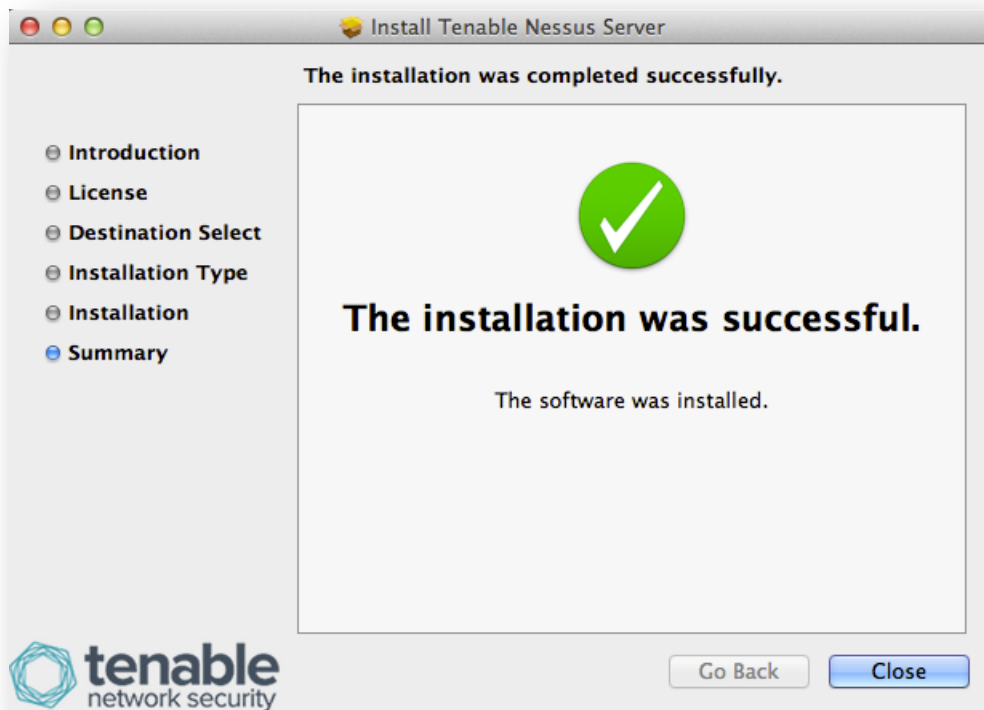
After accepting the license, another dialog box is displayed permitting you to change the default installation location as shown:



Click on the “Install” button to continue the installation. You will be required to enter the administrator username and password at this point:



The installation has successfully completed when the following screen is displayed:



At this point, Nessus will continue by loading a page in your default web browser that will handle the initial configuration, which is discussed in the section [“Feed Registration and GUI Configuration”](#).

Starting and Stopping the Nessus Service

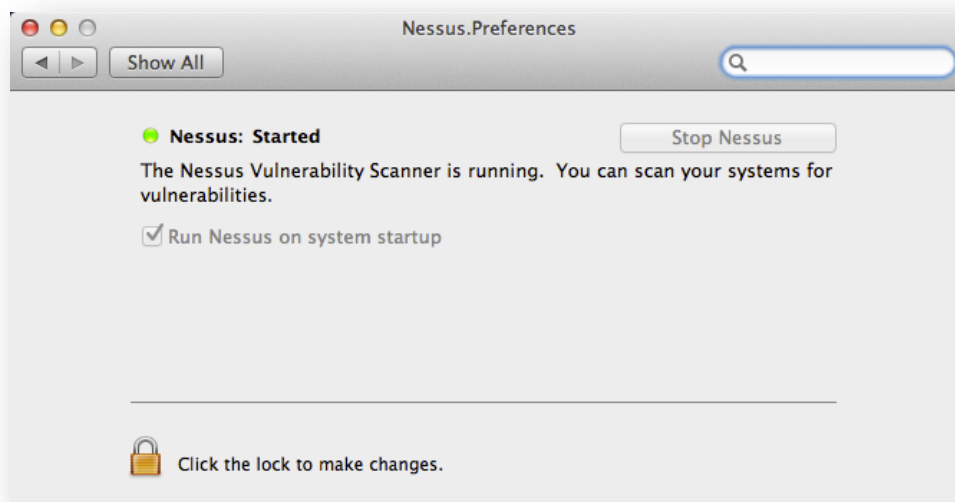
After the installation, the `nessusd` service will start. During each reboot, the service will automatically start. If there is a reason to start or stop the service, it can be done via a Terminal window (command line) or via System Preferences. If performed via the command line, it must be run as “root”, or via `sudo`:

| Action | Command to Manage <code>nessusd</code> |
|--------|---------------------------------------------------------------------------------------------|
| Start | <code># launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist</code> |
| Stop | <code># launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist</code> |

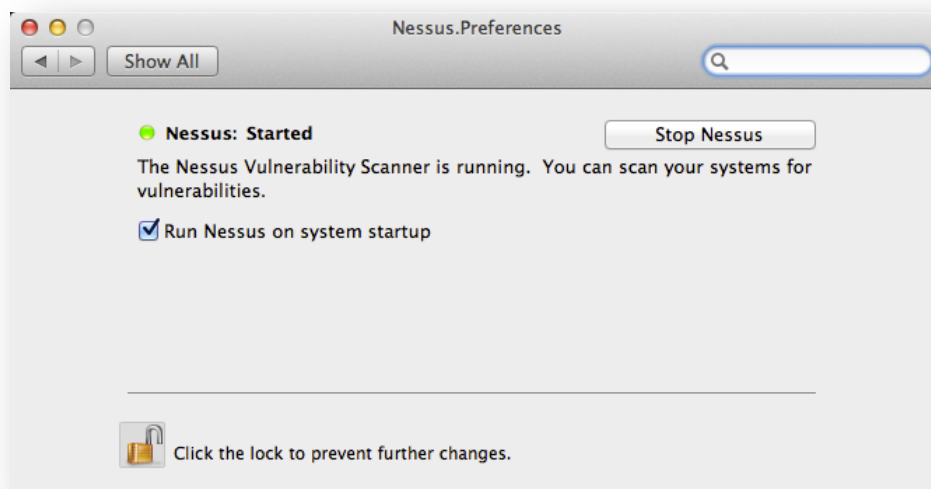
Alternately, the Nessus service can be managed via System Preferences:



Click on “Nessus” in System Preferences to load the Nessus.Preferences pane:



To make changes to the service state, click the lock icon and provide the root password. This will allow you to change the system startup setting, or start and stop the Nessus service:



Removing Nessus

To remove Nessus, delete the following directories (including subdirectories) and files:

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



If you are unfamiliar with Unix command line usage on a Mac OS X system, please contact Tenable Support for assistance.

There are freeware tools such as “DesInstaller.app” (<http://www.macupdate.com/info.php/id/7511>) and “CleanApp” (<http://www.macupdate.com/info.php/id/21453/cleanapp>) that can also be used to remove Nessus. Tenable has no affiliation with these tools and they have not been specifically tested for removing Nessus.

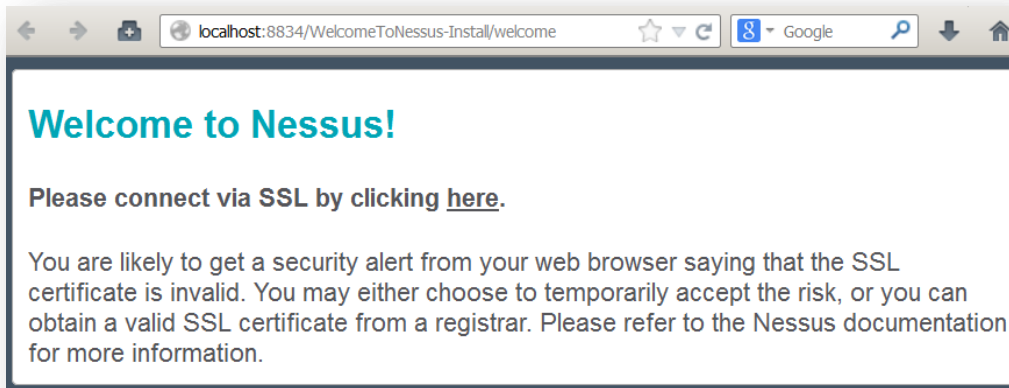
Feed Registration and UI Configuration

This section describes how to configure the Nessus 5 server on all platforms. As of Nessus 5, the initial configuration options such as proxy options and supplying an Activation Code is performed via a web-based process. After the installation of Nessus, you have six hours to complete the registration process for security reasons. If the registration is not completed in that time, restart `nessusd` and restart the registration process.



The Nessus Server Manager used in Nessus 4 has been deprecated.

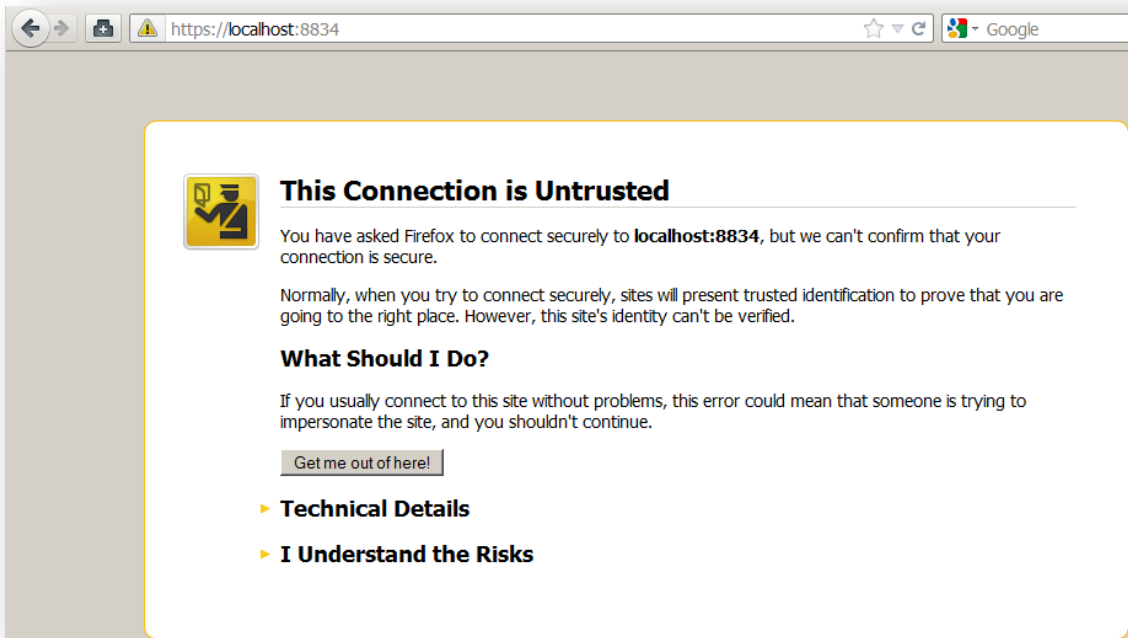
If the software installation does not open your web browser to the configuration page, you can load a browser and go to [http://\[Nessus Server IP\]:8834/WelcomeToNessus-Install/welcome](http://[Nessus Server IP]:8834/WelcomeToNessus-Install/welcome) (or the URL provided during the install process) to begin the process. Note: Unix-based installations may give a URL containing a relative host name that is not in DNS (e.g., <http://mybox:8834/>). If the host name is not in DNS, you must connect to the Nessus server using an IP address or a valid DNS name.



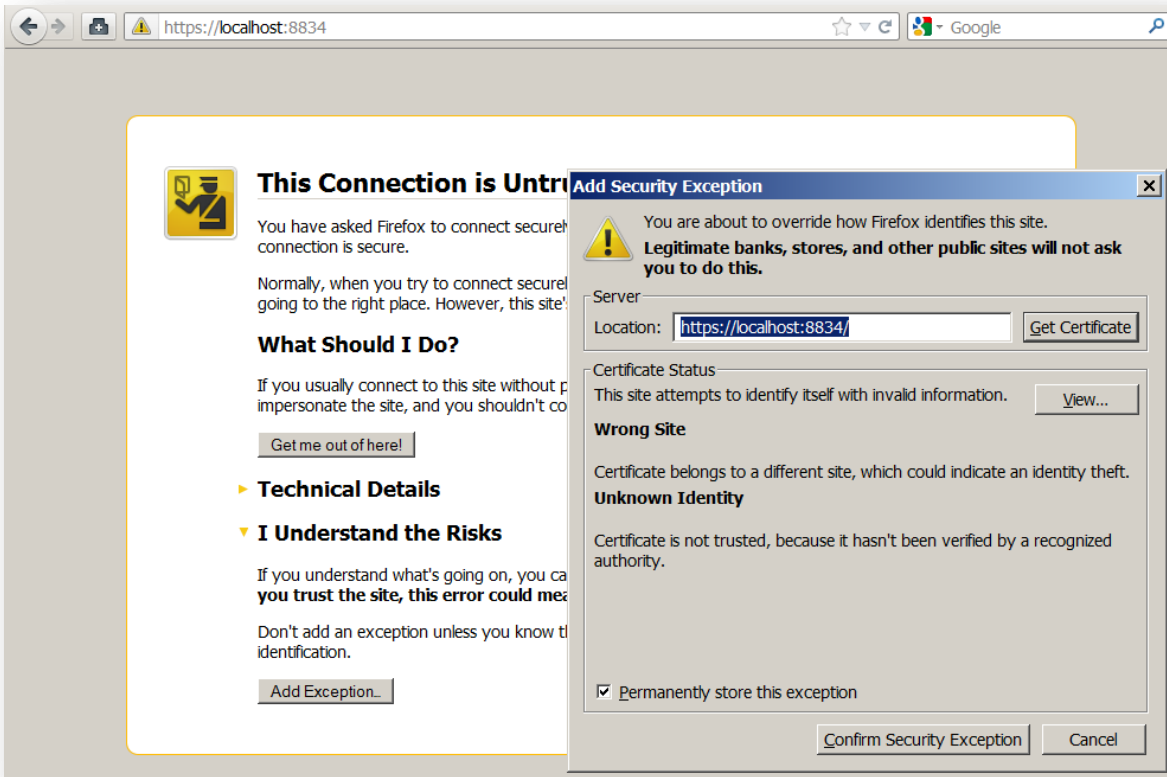
The initial screen serves as a warning that all traffic to the Nessus GUI uses SSL (HTTPS). The first time you connect to the Nessus web server, your browser will display some type of error indicating the connection is not trusted due to a self-signed SSL certificate. For the first connection, accept the certificate to continue configuration. Instructions for installing a custom certificate are covered later in this document, in the “[Configuring Nessus with Custom SSL Certificate](#)” section.



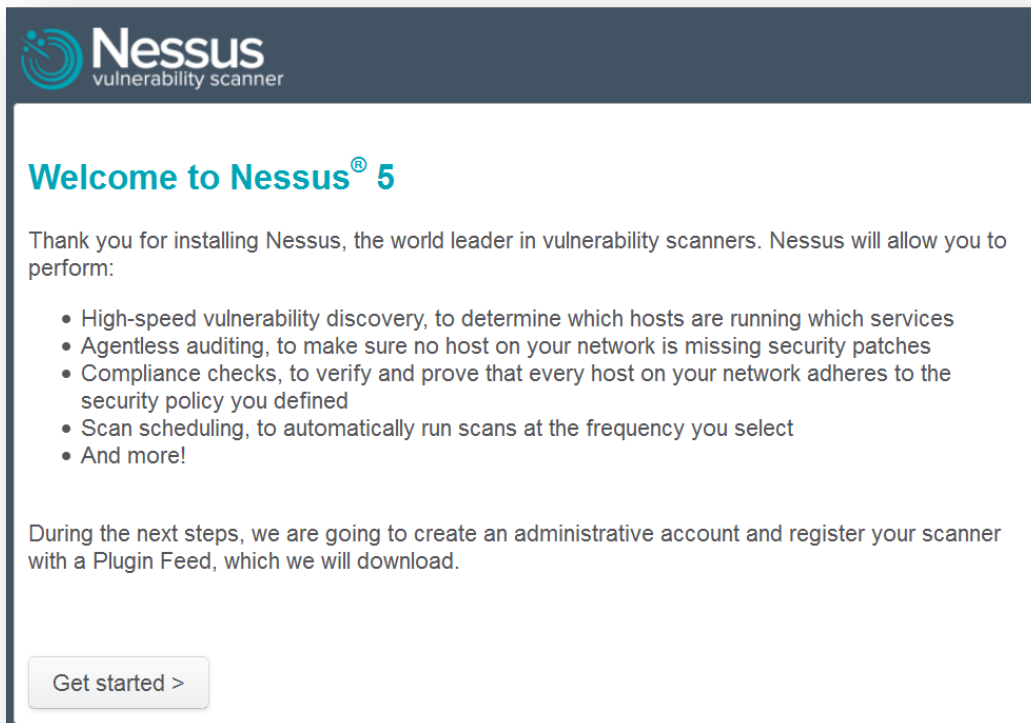
Due to the technical implementation of SSL certificates, it is not possible to ship a certificate with Nessus that would be trusted to browsers. In order to avoid this warning, a custom certificate to your organization must be used.



Depending on the browser you use, there may be an additional dialog that provides the ability to accept the certificate:

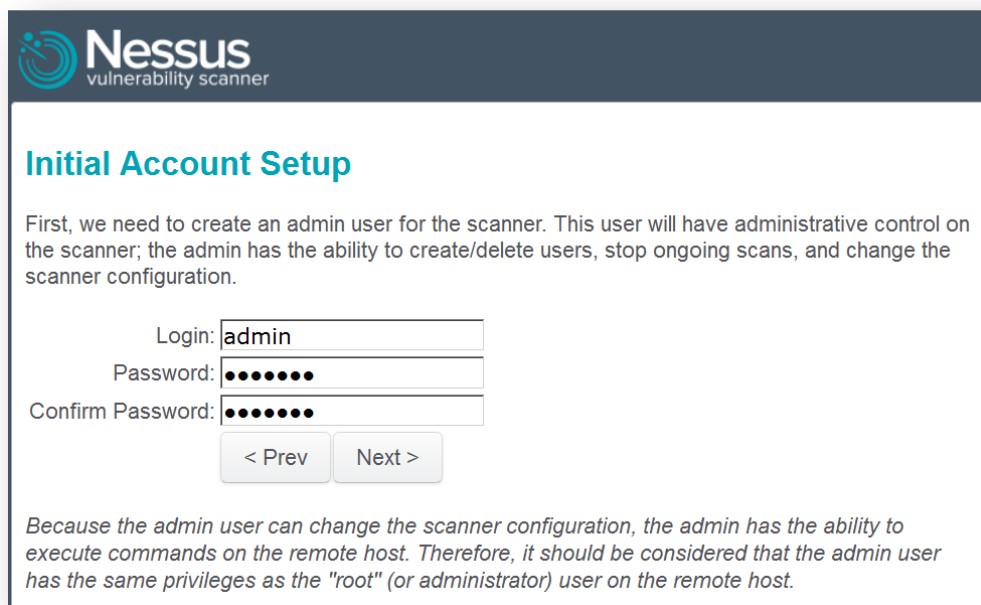


Once accepted, you will be redirected to the initial registration screen that begins the walk-through:



The screenshot shows the Nessus vulnerability scanner logo at the top left. Below it, the heading "Welcome to Nessus® 5" is displayed in a teal color. The main text reads: "Thank you for installing Nessus, the world leader in vulnerability scanners. Nessus will allow you to perform:" followed by a bulleted list of features: "High-speed vulnerability discovery, to determine which hosts are running which services", "Agentless auditing, to make sure no host on your network is missing security patches", "Compliance checks, to verify and prove that every host on your network adheres to the security policy you defined", "Scan scheduling, to automatically run scans at the frequency you select", and "And more!". Below the list, it says: "During the next steps, we are going to create an administrative account and register your scanner with a Plugin Feed, which we will download." At the bottom left, there is a button labeled "Get started >".

The first step is to create an account for the Nessus server. The initial account will be an administrator; this account has access to execute commands on the underlying OS of the Nessus installation, so it should be considered in the same manner as any other administrator account:



The screenshot shows the Nessus vulnerability scanner logo at the top left. Below it, the heading "Initial Account Setup" is displayed in a teal color. The main text reads: "First, we need to create an admin user for the scanner. This user will have administrative control on the scanner; the admin has the ability to create/delete users, stop ongoing scans, and change the scanner configuration." Below the text, there are three input fields: "Login:" with the text "admin" entered, "Password:" with seven black dots, and "Confirm Password:" with seven black dots. Below the input fields are two buttons: "< Prev" and "Next >". At the bottom, there is a note: "Because the admin user can change the scanner configuration, the admin has the ability to execute commands on the remote host. Therefore, it should be considered that the admin user has the same privileges as the 'root' (or administrator) user on the remote host."

The next screen requests a plugin Activation Code and allows you to configure optional proxy settings. If you do not have a code, you can obtain one via the Tenable Support Portal or through your sales channel. Once registered, you will then receive an email with a link to activate the code. You must activate your code within 24 hours for Nessus to continue to operate.



If you are using the Tenable SecurityCenter, the Activation Code and plugin updates are managed from SecurityCenter. Nessus needs to be started to be able to communicate with SecurityCenter, which it will normally not do without a valid Activation Code and plugins. To have Nessus ignore this requirement and start (so that it can get the information from SecurityCenter), input "SecurityCenter" (case sensitive) without quotes into the Activation Code box. After starting Nessus, SecurityCenter users have completed the initial installation and configuration of their Nessus scanner and can continue to the section "[Working with SecurityCenter](#)".

Nessus
vulnerability scanner

Plugin Feed Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. Enter your Activation Code below to subscribe to a "Plugin Feed".

Please enter your Activation Code:

- [Tenable SecurityCenter](#) users: Enter 'SecurityCenter' in the field above
- To perform offline plugin updates, enter 'offline' in the field above

Optional Proxy Settings

< Prev Next >



If you do not register your copy of Nessus, you will not receive any new plugins and will be unable to start the Nessus server. Note: The Activation Code is not case sensitive.

If your Nessus server is on a network that uses a proxy to communicate with the Internet, click on "**Optional Proxy Settings**" to enter the relevant information. Proxy settings can be added at any time after the installation has completed.

Plugin Feed Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. Enter your Activation Code below to subscribe to a "Plugin Feed".

Please enter your Activation Code:

- Tenable SecurityCenter users: Enter 'SecurityCenter' in the field above
- To perform offline plugin updates, enter 'offline' in the field above

Optional Proxy Settings

Proxy hostname:

Proxy username:

Proxy password:

Proxy password (again):

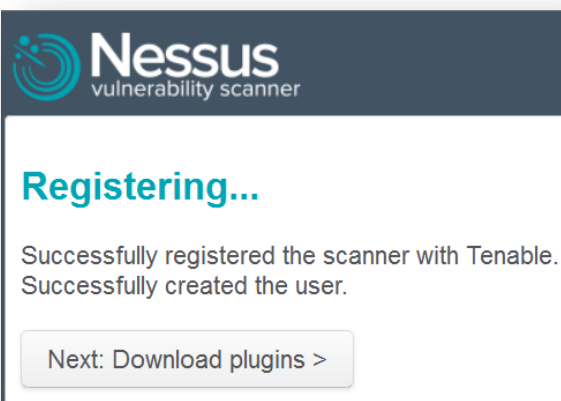
< Prev

Next >

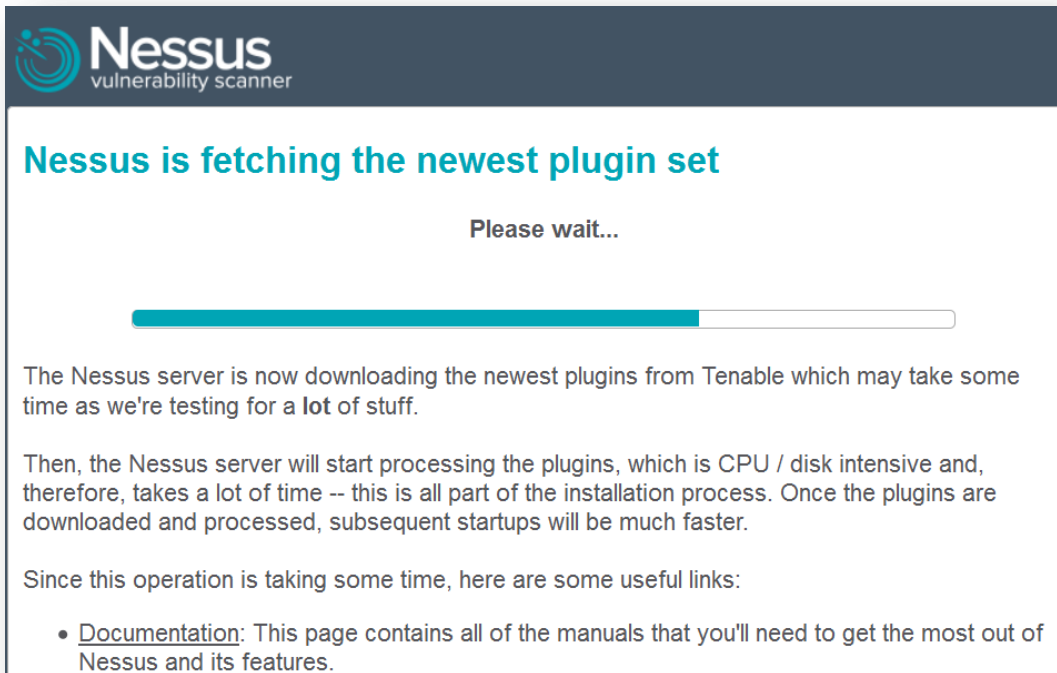


If you select offline for your activation, please note that "offline" is case sensitive.

The next step requires that you input the Activation Code you have already received via the Tenable Nessus registration page. Once the Activation Code and **optional** proxy setting configuration has been completed, click "**Next**" to register your scanner:



After registration, Nessus must download the plugins from Tenable. This process may take several minutes as it transfers a considerable amount of data to the machine, verifies file integrity, and compiles them into an internal database:



The screenshot shows the Nessus vulnerability scanner logo at the top left. The main heading is "Nessus is fetching the newest plugin set" in teal. Below it, the text "Please wait..." is centered. A teal progress bar is partially filled. The text below the bar explains that the Nessus server is downloading the newest plugins from Tenable, which may take some time. It then states that the server will start processing the plugins, which is CPU / disk intensive and takes a lot of time, but subsequent startups will be much faster. Finally, it provides a link to the documentation for more information.

Nessus
vulnerability scanner

Nessus is fetching the newest plugin set

Please wait...

The Nessus server is now downloading the newest plugins from Tenable which may take some time as we're testing for a lot of stuff.

Then, the Nessus server will start processing the plugins, which is CPU / disk intensive and, therefore, takes a lot of time -- this is all part of the installation process. Once the plugins are downloaded and processed, subsequent startups will be much faster.

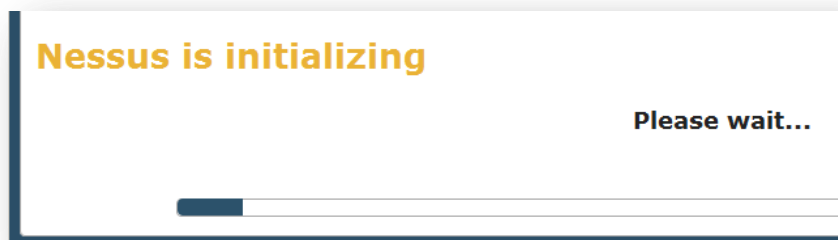
Since this operation is taking some time, here are some useful links:

- [Documentation](#): This page contains all of the manuals that you'll need to get the most out of Nessus and its features.



After the initial registration, Nessus will download and compile the plugins obtained from port 443 of plugins.nessus.org, plugins-customers.nessus.org, or plugins-us.nessus.org in the background.

Once the plugins have been downloaded and compiled, the Nessus GUI will initialize and the Nessus server will start:

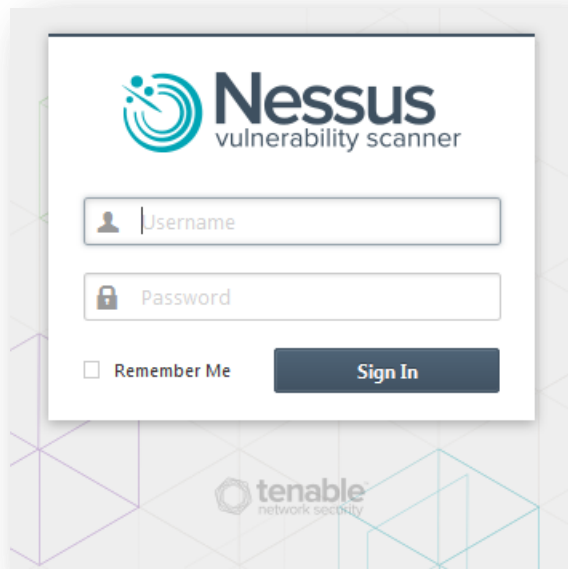


The screenshot shows the Nessus installation progress screen with the heading "Nessus is initializing" in orange. Below it, the text "Please wait..." is centered. A dark blue progress bar is partially filled.

Nessus is initializing

Please wait...

After initialization, Nessus is ready for use!



Using the administrative credentials created during the installation, log into the Nessus interface to verify access.

Once authenticated, click on the down arrow next to the username (e.g., “admin”) and select “**Settings**” to view information about Nessus and the current feed.



Configuration

With the release of Nessus 5, all Nessus server configuration is managed via the GUI. The `nessusd.conf` file is deprecated. In addition, proxy settings, subscription feed registration, offline updates, mail server, and LDAP server settings are managed via the GUI.

LDAP Server

The “LDAP Server” tab (under the “Settings” menu via the drop-down on the top left), allows you to configure an LDAP server so users can authenticate to the Nessus server using LDAP domain credentials.

The screenshot shows the 'Settings' window with the 'LDAP Server' tab selected. The left sidebar contains a navigation menu with categories: Overview, ACCOUNTS (Users, Groups), MISC SETTINGS (LDAP Server, Mail Server, Multi Scanner, Plugin Feed, Proxy, Scanners), and Advanced. The main content area is titled 'Settings / LDAP Server' and contains the following fields:

- Host: ldap.example.com
- Port: 389
- Username: nessus
- Password: [masked with dots]
- Base DN: cn=users,dc=tenable,dc=com
- Test LDAP Authentication: [button]
- Advanced Settings:

At the bottom of the form are 'Save' and 'Cancel' buttons.

Mail Server

The “Mail Server” tab (under the “Settings” menu via the drop-down on the top left), allows you to configure an SMTP server to allow completed scans to automatically email the results.

The screenshot shows the 'Settings / Mail Server' configuration window. On the left is a sidebar with navigation options: Overview, ACCOUNTS (Users, Groups), MISC SETTINGS (LDAP Server, **Mail Server**, Multi Scanner, Plugin Feed, Proxy, Scanners, Advanced). The main area contains the following fields:

- Host: smtp.example.com
- Port: 25
- From (sender email): badger@example.com
- Auth Method: CRAM-MD5 (dropdown)
- Username: nessus
- Password: [masked with dots]
- Encryption: Use TLS if available (dropdown)
- Nessus Server Hostname (for email links): 192.168.0.28

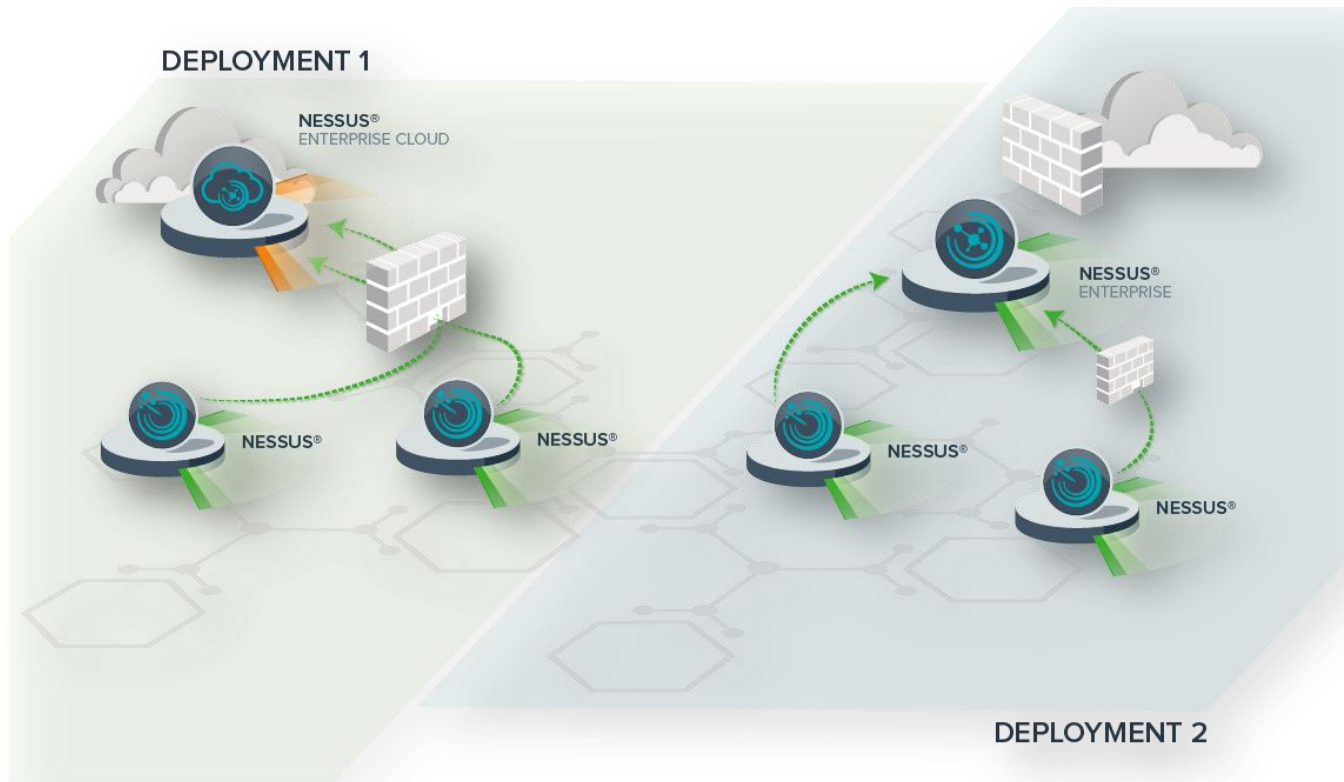
Buttons: Save, Cancel, Send Test Email

| Option | Description |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Host | The host or IP of the SMTP server (e.g., smtp.example.com). |
| Port | The port of the SMTP server (e.g., 25). |
| From (sender email) | Who the report should appear to be from. |
| Auth Method | Method for authenticating to the SMTP server. Support for None, Plain, NTLM, Login, and CRAM-MD5 are supported. |
| Username | The username used to authenticate to the SMTP server. |
| Password | The password associated with the username. |
| Encryption | Specify what type of encryption should be used. |
| Nessus Server Hostname (for email links) | The IP address or hostname for the Nessus server. Note that this will only work if the Nessus host is reachable to the user reading the report. |

Multi Scanner Settings

The Multi Scanner functionality gives your Nessus scanner the ability to delegate vulnerability scanning to multiple secondary servers, or be delegated to perform scans for another. You can use your own Nessus server to act as the primary, or you can configure your Nessus Enterprise Cloud scanner in the cloud to be the primary. This allows for consolidated reporting in a single Nessus user interface with scheduled scanning and emailing results.

The use of this functionality positions companies to create an extended network of Nessus scanners that give added value. Through strategic positioning of the scanners, you are able to not only test for vulnerabilities and misconfigurations, but also examine the system from different viewpoints on the network. This can greatly assist you in ensuring that network screening devices (e.g., firewalls, routers) are properly restricting access to a given system.

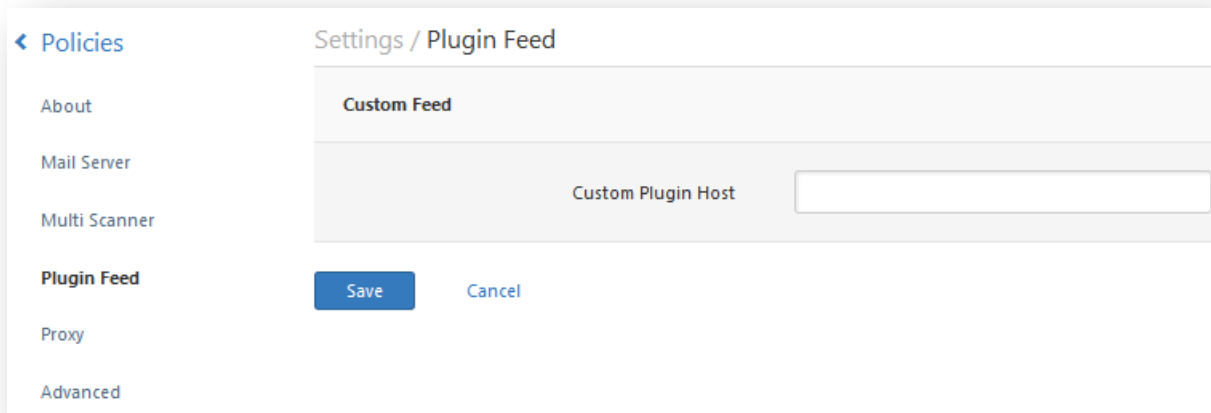


It is important to note that primary scanners do not reach out to the secondary scanners. Instead, secondary scanners periodically poll the primary scanner they are registered with to receive new instructions. When deploying a network of Nessus scanners using this functionality, this must be kept in mind to ensure that nothing will hinder the secondary scanner in connecting to its primary.

For more information on configuring multiple scanners, please see the [Nessus 5.2 HTML5 User Guide](#).

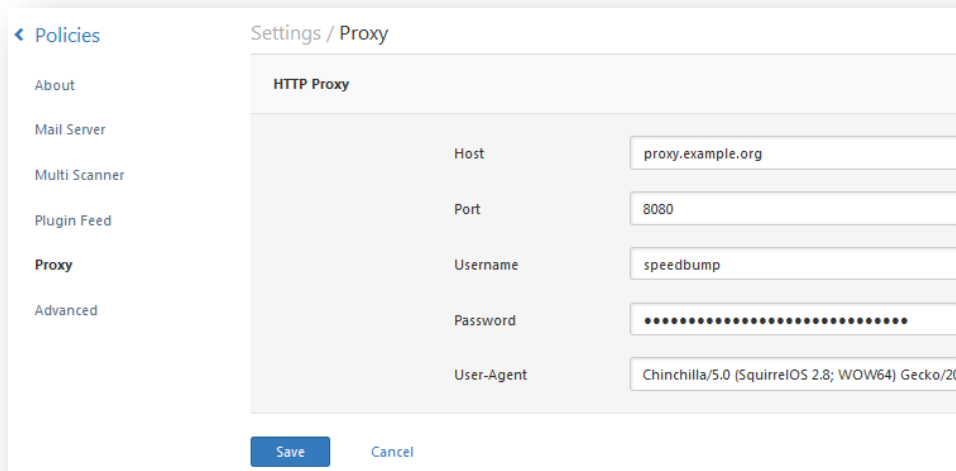
Plugin Feed Settings

The **“Plugin Feed”** tab (under the **“Settings”** menu via the drop-down on the top left), allows you to configure a custom plugin host. This can be used to force Nessus to update plugins from a specific host. For example, if plugins must be updated from a site residing in the U.S., you can specify **“plugins-us.nessus.org”**.



Proxy Settings

Under the “**Settings**” menu via the drop-down on the top left, the “**Proxy**” tab allows you to configure a web proxy for plugin updates. This is required if your organization requires that all web traffic be directed through a corporate proxy:



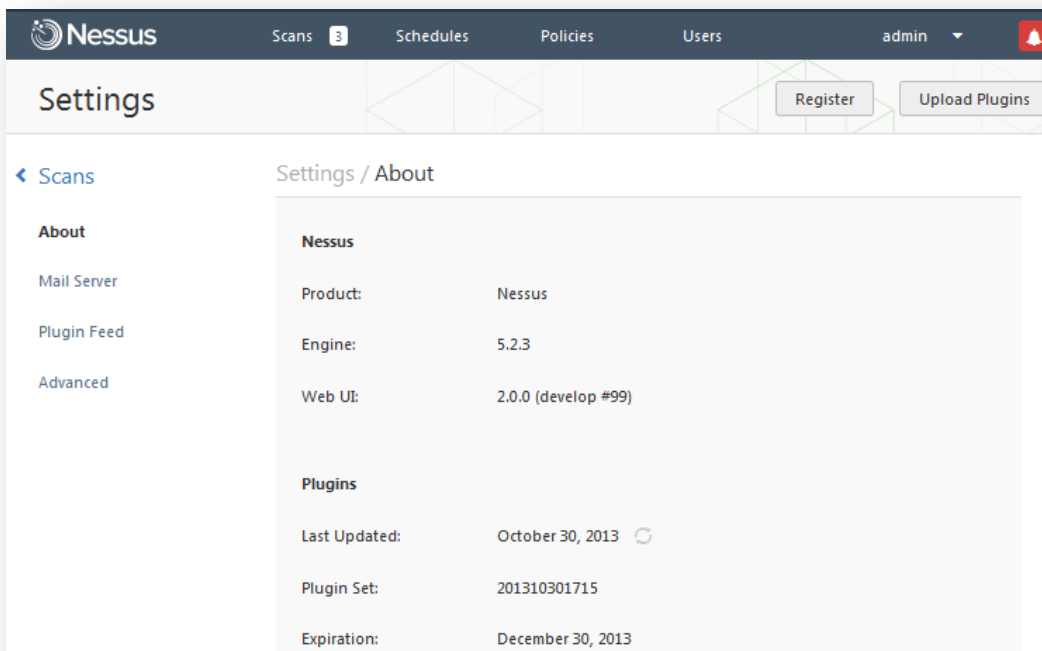
There are five fields that control proxy settings, but only the host and port are required. Optionally, a username and password can be supplied, if necessary.

| Option | Description |
|-----------------|---------------------------------------------------------------------|
| Host | The host or IP of the proxy (e.g., proxy.example.com). |
| Port | The port of the proxy (e.g., 8080). |
| Username | Optional: If a username is required for proxy usage (e.g., “jdoe”). |

| | |
|-------------------|---------------------------------------------------------------------------------------------------------------------|
| Password | Optional: If a password is required for proxy usage (e.g., “guineapigs”). |
| User-Agent | Optional: If the proxy you are using filters specific HTTP user agents, a custom user-agent string can be supplied. |

Resetting Activation Codes & Offline Updates

After the initial Activation Code is entered during the setup process, subsequent Activation Code changes are performed through the “**About**” tab under “**Settings**”. This can be accessed by clicking on the down arrow next to the username on the upper right of the UI and selecting “**Settings**”. From this screen, there are buttons on the upper right for “**Register**” and “**Upload Plugins**”. Inputting a new code in the “**Update Registration**” field of the “**Register**” button and clicking “**Save**” will update the Nessus scanner with the new code (e.g., if upgrading from Nessus Home to commercial Nessus).



The “**Upload Plugins**” button allows you to specify a plugin archive for processing. For more details on offline updating, consult the “[Nessus without Internet Access](#)” section later in this document.



The legacy client use via the NTP protocol is supported by Nessus 5, but only available to Nessus customers.



If at any time you need to verify the registration code for a given scanner, you can use the `--code-in-use` option to the `nessus-fetch` program. Note that this option requires administrative privileges and network connectivity.

Advanced Configuration Options

Nessus uses a wide variety of configuration options to offer more granular control of how the scanner operates. Under the “**Advanced**” tab via the drop-down on the top left, an administrative user can manipulate these settings.



WARNING: Any changes to the Nessus scanner configuration will affect ALL Nessus users. Edit these options carefully!

| Setting | Value |
|---------------------------------------------------|--------------------------------------------------------|
| <input type="checkbox"/> allow_post_scan_editing | yes |
| <input type="checkbox"/> auto_enable_dependencies | yes |
| <input type="checkbox"/> auto_update | yes |
| <input type="checkbox"/> auto_update_delay | 24 |
| <input type="checkbox"/> cgi_path | /cgi-bin/scripts |
| <input type="checkbox"/> checks_read_timeout | 5 |
| <input type="checkbox"/> disable_ntp | yes |
| <input type="checkbox"/> disable_xmlrpc | no |
| <input type="checkbox"/> dumpfile | C:\ProgramData\Tenable\Nessus\nessus\logs\nessusd.dump |
| <input type="checkbox"/> global.max_hosts | 535 |
| <input type="checkbox"/> global.max_scans | 0 |

Each option can be configured by editing the corresponding field and clicking the “Save” button at the bottom of the screen. In addition, the option can be removed completely by clicking the ✕ button.

By default, the Nessus GUI operates on port 8834. To change this port, edit the `xmlrpc_listen_port` to the desired port. The Nessus server will process the change within a few minutes.

If additional preferences are required, click on the “Add Preference Item” button, input the name and value, and click on “Save”. Once a preference has been updated and saved, Nessus will process the changes within a couple of minutes.

For details on each of the configuration options, consult the “[Configure the Nessus Daemon \(Advanced Users\)](#)” section of this document.

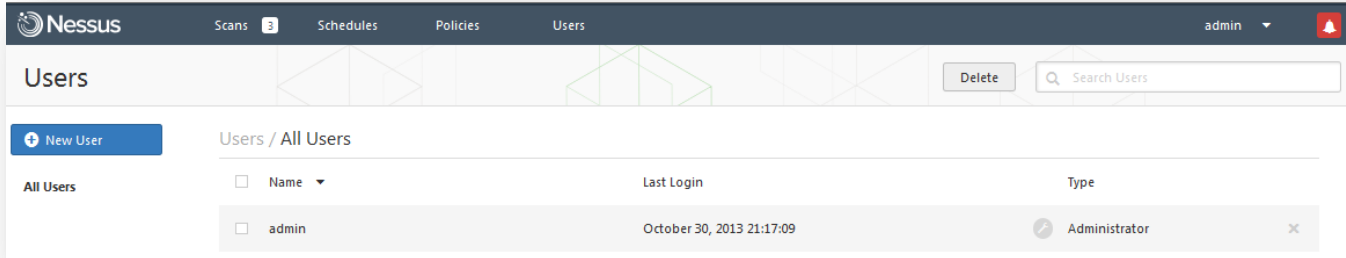


Note that there are two optional advanced preferences that are not default, but can be added to enhance the security of the Nessus installation:

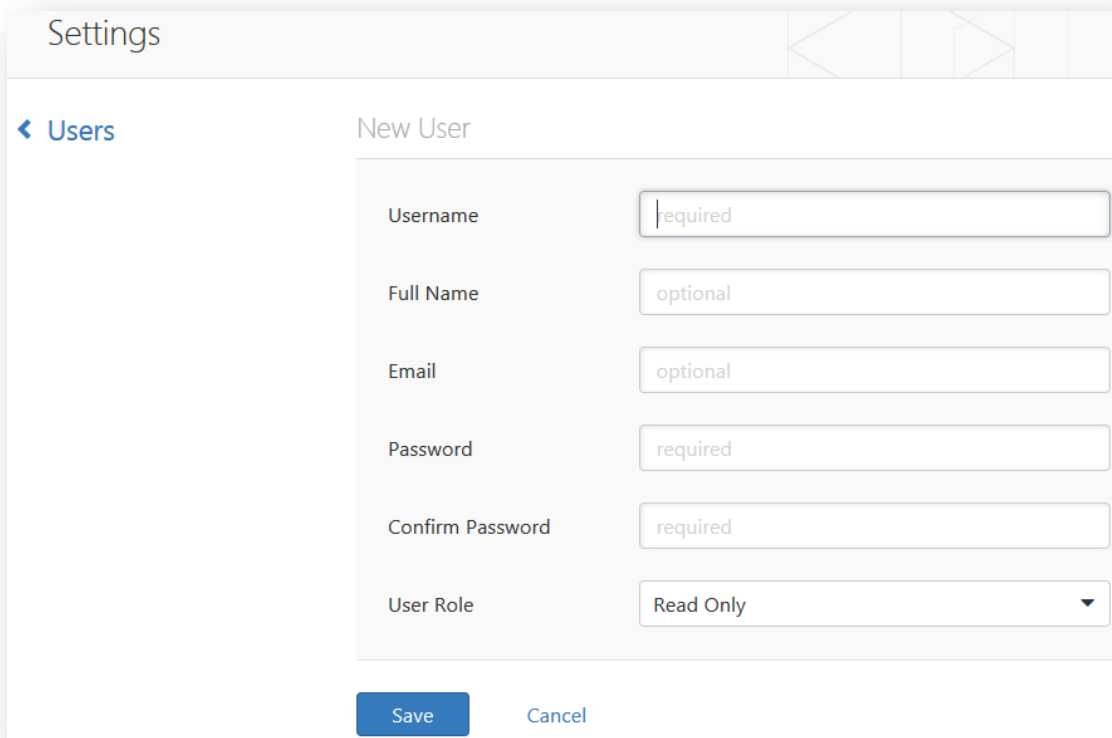
- Setting “`xmlrpc_hide_version`” to “yes” in the preferences prevents an unauthenticated user from getting the version of the Nessus server.
- Setting “`user_max_login_attempt`” to a numeric value (i.e., “3”) will lock a given account after *n* invalid login attempts. Unlocking the user requires the admin to edit the user.

Create and Manage Nessus Users

During the initial setup, one administrative user is created. Using the credentials specified during the setup, log in to the Nessus GUI. Once authenticated, click on the “**Users**” heading at the top:



To create a new user, click “**New User**” on the upper left. This will open a dialogue box prompting for required details:

A screenshot of the 'New User' settings dialog box. The dialog has a title bar 'Settings' and a back arrow labeled 'Users'. The form fields are: 'Username' (required), 'Full Name' (optional), 'Email' (optional), 'Password' (required), 'Confirm Password' (required), and 'User Role' (Read Only). At the bottom, there are 'Save' and 'Cancel' buttons.

Input the username and password, verify the password, and determine if the user will have administrator privileges.

If a user account needs to be modified, click on the user name:

Account Settings

| | |
|-----------|---------------------------------------|
| Username | admin |
| Full Name | <input type="text" value="admin"/> |
| Email | <input type="text" value="optional"/> |
| User Type | System Administrator |

Save
Cancel



You cannot rename a user. If you want to change the name of a user, delete the user and create a new user with the appropriate login name.

To remove a user, either select the check box to the right of the account name on the list and then **“Delete”** at the top, or click the **“X”** to the right of the account name.

Delete User "waffle"
×

Are you sure you want to delete this user?

Delete
Cancel

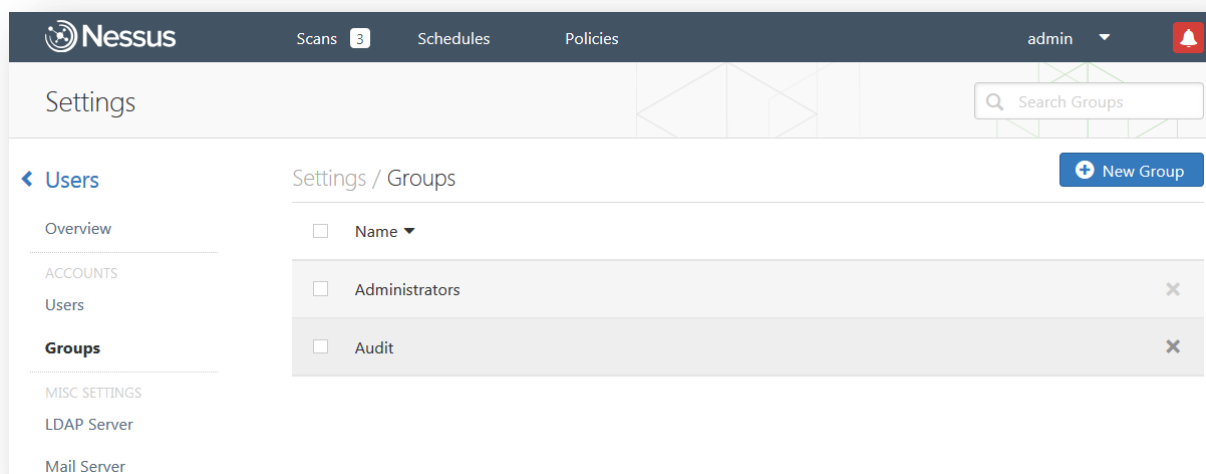


A non-admin user cannot upload plugins to Nessus, cannot restart it remotely (needed after a plugin upload), and cannot override the `max_hosts/max_checks` setting in the configuration section. If the user is intended to be used by SecurityCenter, it must be an admin user. SecurityCenter maintains its own user list and sets permissions for its users.

If you require a Nessus user account to have restrictions placed on it, use the command-line interface (CLI) which is covered later in this document in the [“Using and Managing Nessus from the Command Line”](#) section.

Create and Manage Nessus User Groups

Nessus Enterprise has an extensive set of user and group roles that allow for granular sharing of policies, schedules, and scan results.



For more information on creating and managing groups, please consult the [Nessus 5.2 Enterprise User Guide](#).

Configure the Nessus Daemon (Advanced Users)

The Nessus GUI configuration menu contains several configurable options. For example, this is where the maximum number of checks and hosts being scanned at one time, the resources you want `nessusd` to use and the speed at which data should be read are all specified, as well as many other options. It is recommended that these settings be reviewed and modified appropriately based on your scanning environment. The full list of configuration options is explained at the end of this section.

In particular, the `global_max_hosts`, `max_hosts`, and `max_checks` values can have a great impact on your Nessus system's ability to perform scans, as well as those systems being scanned for vulnerabilities on your network. Pay particular attention to these two settings.

Here are the two settings and their default values as seen in the configuration menu:

| Option | Value |
|-------------------------------|-------|
| <code>global_max_hosts</code> | 530 |
| <code>max_hosts</code> | 40 |
| <code>max_checks</code> | 5 |

Note that these settings will be over-ridden on a per-scan basis when using Tenable's SecurityCenter or within a custom policy in the Nessus User Interface. To view or modify these options for a scan template in SecurityCenter, edit the "Scan Options" in the template. In the Nessus User Interface, edit the scan policy and then click on the "Options" tab.



Note that the `max_checks` parameter has a hardcoded limit of 15. Any value over 5 will frequently lead to adverse effects as most servers cannot handle that many intrusive requests at once.

Notes on max_hosts:

As the name implies, this is the maximum number of target systems that will be scanned at any one time. The greater the number of simultaneously scanned systems by an individual Nessus scanner, the more taxing it is on that scanner system's RAM, processor, and network bandwidth. Take into consideration the hardware configuration of the scanner system and other applications running on it when setting the `max_hosts` value.

As a number of other factors that are unique to your scanning environment will also affect your Nessus scans (e.g., your organization's policy on scanning, other network traffic, the affect a particular type of scan has on your scan target hosts), experimentation will provide you with the optimal setting for `max_hosts`.

A conservative starting point to determine the best `max_hosts` setting in an enterprise environment is to set it to "20" on a Unix-based Nessus system and "10" on a Windows Nessus scanner.

In addition to `max_hosts`, the server allows a `global.max_hosts` setting that controls the total hosts that can be scanned across all users at the same time. Before Nessus 5.2.0, an administrator was exempt from the `max_hosts` restriction, but not the `global.max_hosts` setting. As of Nessus 5.2.0, administrators are bound by the same restrictions on both settings to avoid excessive load on the scanning server, which may have adverse effects on other users.

Notes on max_checks:

This is the number of simultaneous checks or plugins that will be run against a single target host during a scan. Note that setting this number too high can potentially overwhelm the systems you are scanning depending on which plugins you are using in the scan.


Multiply `max_checks` by `max_hosts` to find the number of concurrent checks that can potentially be running at any given time during a scan. Because `max_checks` and `max_hosts` are used in concert, setting `max_checks` too high can also cause resource constraints on a Nessus scanner system. As with `max_hosts`, experimentation will provide you with the optimal setting for `max_checks`, but it is recommended that this always be set relatively low.

Configuration Options

The following table provides a brief explanation of each configuration option available in the configuration menu. Many of these options can be configured through the user interface when creating a scan policy.

| Option | Description |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>allow_post_scan_editing</code> | Allows a user to make edits to scan results after the scan completes. |
| <code>auto_enable_dependencies</code> | Automatically activate the plugins that are depended on. If disabled, not all plugins may run despite being selected in a scan policy. |
| <code>auto_update</code> | Automatic plugin updates. If enabled and Nessus is registered, fetch the newest plugins from <code>plugins.nessus.org</code> automatically. Disable if the scanner is on an isolated network that is not able to reach the Internet. |
| <code>auto_update_delay</code> | Number of hours to wait between two updates. Four (4) hours is the minimum allowed interval. |
| <code>cgi_path</code> | During the testing of web servers, use this colon delimited list of CGI paths. |
| <code>checks_read_timeout</code> | Read timeout for the sockets of the tests. |
| <code>disable_ntp</code> | Disable the old NTP legacy protocol. |

| | |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| disable_xmlrpc | Disable the new XMLRPC (Web Server) interface. |
| dumpfile | Location of a dump file for debugging output if generated. |
| enable_listen_ipv4 | Directs Nessus to listen on IPv4. |
| enable_listen_ipv6 | Directs Nessus to listen on IPv6 if the system supports IPv6 addressing. |
| 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. |
| global.max_simult_tcp_sessions | Maximum number of simultaneous 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. |
| host.max_simult_tcp_sessions | Maximum number of simultaneous TCP sessions per scanned host. |
| listen_address | IPv4 address to listen for incoming connections. If set to 127.0.0.1, this will restrict access to local connections only. |
| listen_port | Port to listen to (old NTP protocol). Used for pre 4.2 NessusClient connections. |
| log_whole_attack | Log every detail of the attack? Helpful for debugging issues with the scan, but this may be disk intensive. |
| logfile | Location where the Nessus log file is stored. |
| login_banner | A text banner that will be displayed before the initial login to the Flash or HTML5 client. |
| max_hosts | Maximum number of hosts checked at one time during a scan. |
| max_checks | Maximum number of simultaneous checks against each host tested. |
| max_simult_tcp_sessions | Maximum number of simultaneous TCP sessions per scan. |
| nasl_log_type | Direct the type of NASL engine output in <code>nessusd.dump</code> . |
| nasl_no_signature_check | Determines if Nessus will consider all NASL scripts as being signed. Selecting "yes" is unsafe and not recommended. |
| nessus_syn_scanner.global_throughput.max | Sets the max number of syn packets that Nessus will send per second during its port scan (no matter how many hosts are scanned in parallel). Adjust this setting based on the sensitivity of the remote device to large numbers of syn packets. |
| non_simult_ports | Specifies ports against which two plugins cannot not be run simultaneously. |

| | |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| optimize_test | Optimize the test procedure. Changing this to “no” will cause scans to take longer and typically generate more false positives. |
| paused_scan_timeout | Kill a paused scan after the specified number of minutes (0 for no timeout). |
| plugin_upload | Designate if admin users may upload plugins. |
| plugin_upload_suffixes | Suffixes of the plugins the admin user can upload. |
| plugins_timeout | Maximum lifetime of a plugin’s activity (in seconds). |
| port_range | Range of the ports the port scanners will scan. Can use keywords “default” or “all”, as well as a comma 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. |
| 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. |
| reduce_connections_on_congestion | Reduce the number of TCP sessions in parallel when the network appears to be congested. |
| report_crashes | Anonymously report crashes to Tenable. |
| rules | Location of the Nessus Rules file (nessusd.rules). |
| |  <div style="border: 1px solid gray; padding: 5px; display: inline-block;"> <p>The nessusd.rules file applies to Nessus administrative users too.</p> </div> |
| safe_checks | Safe checks rely on banner grabbing rather than active testing for a vulnerability. |
| save_knowledge_base | Save the knowledge base on disk for later use. |
| 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. |
| 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, then 10.0.0.128, and so on). |
| source_ip | In the case of a multi-homed system with different IPs on the same subnet, this option tells the Nessus scanner which NIC/IP to use for the tests. If multiple IPs are provided, Nessus will cycle through them whenever it performs a connection. |

| | |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ssl_cipher_list | Make sure only “strong” SSL ciphers are used when connecting to port 1241. Supports the keyword “strong” or the general OpenSSL designations as listed at http://www.openssl.org/docs/apps/ciphers.html . |
| stop_scan_on_disconnect | Stop scanning a host that seems to have been disconnected during the scan. |
| stop_scan_on_hang | Stop a scan that seems to be hung. |
| throttle_scan | Throttle scan when CPU is overloaded. |
| use_kernel_congestion_detection | Use Linux’s TCP congestion messages to scale back scan activity as required. |
| www_logfile | Location where the Nessus Web Server (user interface) log is stored. |
| xmlrpc_idle_session_timeout | XMLRPC Idle Session Timeout in minutes. (0 for no timeout). |
| xmlrpc_import_feed_policies | If set to “no”, Nessus will not include default scan policies provided by Tenable. |
| xmlrpc_listen_port | Port for the Nessus Web Server to listen to (new XMLRPC protocol). |
| xmlrpc_min_password_len | Directs Nessus to enforce a policy for the length of a password for users of the scanner. |


By default, **report_crashes** is set to “yes”. Information related to a crash in Nessus will be sent to Tenable to help debug issues and provide the highest quality software possible. No personal or system-identifying information is sent to Tenable. This setting may be set to “no” by a Nessus admin user.



Some settings such as **source_ip** may require Nessus to be restarted to take effect.

Configuring Nessus with Custom SSL Certificate

The default installation of Nessus uses a self-signed SSL certificate. When first using the web interface to access the Nessus scanner, your web browser will display an error indicating the certificate is not trusted:



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.0.2:8834**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

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.

The following table lists the location of the certificate files based on the operating system:

| Operating System | Certificate File Locations |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Linux | <code>/opt/nessus/com/nessus/CA/servercert.pem</code> <code>/opt/nessus/var/nessus/CA/serverkey.pem</code> |
| FreeBSD | <code>/usr/local/nessus/com/nessus/CA/servercert.pem</code> <code>/usr/local/nessus/var/nessus/CA/serverkey.pem</code> |
| Windows Vista and later | <code>C:\ProgramData\Tenable\Nessus\nessus\CA\</code> |
| Windows XP / 2003 | <code>C:\Documents and Settings\All Users\Application Data\Tenable\Nessus\nessus\CA\</code> |
| Mac OS X | <code>/Library/Nessus/run/com/nessus/CA/servercert.pem</code> <code>/Library/Nessus/run/var/nessus/CA/serverkey.pem</code> |

Nessus 5 supports SSL certificate chains.



You can also visit `https://[IP address]:8834/getcert` to install the root CA in your browser, which will remove the warning.

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).

Authenticating To Nessus with SSL Certificate

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 `nessus-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.

1. (Optional) Create a new custom CA and server certificate for the Nessus server using the `nessus-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
```

Windows XP and 2003:

```
C:\> copy \Documents and Settings\All Users\Application  
Data\Tenable\Nessus\nessus\CA\cacert.pem C:\Documents and Settings\All  
Users\Application Data\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 Vista and later:

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

Windows XP and 2003:

Copy the organization's CA certificate to: `C:\Documents and Settings\All Users\Application Data\Tenable\Nessus\nessus\CA\`

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/nessus-fix --set force_pubkey_auth=yes
```

Windows:

```
C:\> \program files\Tenable\Nessus\nessus-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 `nessus-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 `nessus-mkcert-client` command.

Linux/Unix:

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

Windows (Run as a local Administrator user):

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

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

```
Do you want to register the users in the Nessus server as soon as you create their
certificates ? [n]: y
```

```
-----
                        Creation Nessus SSL client Certificate
-----
```

```
This script will now ask you the relevant information to create the SSL
client certificates for Nessus.
```

```
Client certificate life time in days [365]:
```

```
Your country (two letter code) [US]:
```

```
Your state or province name [NY]: MD
```

```
Your location (e.g. town) [New York]: Columbia
```

```
Your organization []: Content
```

```
Your organizational unit []: Tenable
```

```
*****
```

```
We are going to ask you some question for each client certificate
```

```
If some question have a default answer, you can force an empty answer by entering a
single dot '.'
```



```

*****
User #1 name (e.g. Nessus username) []: squirrel
Should this user be administrator? [n]: y
Country (two letter code) [US]:
State or province name [MD]:
Location (e.g. town) [Columbia]:
Organization [Content]:
Organizational unit [Tenable]:
e-mail []:

User rules
-----
nessusd has a rules system which allows you to restrict the hosts that firstuser has
the right to test. For instance, you may want him to be able to scan his own
host only.
Please see the nessus-adduser(8) man page for the rules syntax

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

User added to Nessus.
Another client certificate? [n]:
Your client certificates are in C:\Users\admin\AppData\Local\Temp\nessus-0000040e
You will have to copy them by hand

```



The client certificates will be 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”.



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.

- There will be two files created in the temporary directory, for example, `cert_squirrel.pem` and `key_squirrel.pem` (where “squirrel” is the hostname of the system used in this example). These 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_squirrel.pfx -inkey key_squirrel.pem -in
cert_squirrel.pem -chain -CAfile /opt/nessus/com/nessus/CA/cacert.pem -passout
pass:'SecretWord' -name 'Nessus User Certificate for: squirrel'
```

The resulting file `combined_squirrel.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.

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

```
Linux/Unix:
# /opt/nessus/sbin/nessus-mkcert-client
```

Windows (Run as a local Administrator user):

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

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.

```
Do you want to register the users in the Nessus server as soon as you create their
certificates ? [n]: y
```

```
-----
                          Creation Nessus SSL client Certificate
-----
```

```
This script will now ask you the relevant information to create the SSL
client certificates for Nessus.
```

```
Client certificate life time in days [365]:
```

```
Your country (two letter code) [US]:
```

```
Your state or province name [NY]: MD
```

```
Your location (e.g. town) [New York]: Columbia
```

```
Your organization []: Content
```

```
Your organizational unit []: Tenable
```

```
*****
```

```
We are going to ask you some question for each client certificate
```

```
If some question have a default answer, you can force an empty answer by entering a
single dot '.'
```

```
*****
```

```
User #1 name (e.g. Nessus username) []: squirrel
```

```
Should this user be administrator? [n]: y
```

```
Country (two letter code) [US]:
```

```
State or province name [MD]:
```

```
Location (e.g. town) [Columbia]:
```

```
Organization [Content]:
```

```
Organizational unit [Tenable]:
```

```
e-mail []:
```

```
User rules
```

```
-----
nessusd has a rules system which allows you to restrict the hosts that firstuser has
the right to test. For instance, you may want him to be able to scan his own host
only.
```

```
Please see the nessus-adduser(8) man page for the rules syntax
```

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

```
User added to Nessus.
```

```
Another client certificate? [n]:
```

```
Your client certificates are in C:\Users\admin\AppData\Local\Temp\nessus-0000040e
```

```
You will have to copy them by hand
```



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.

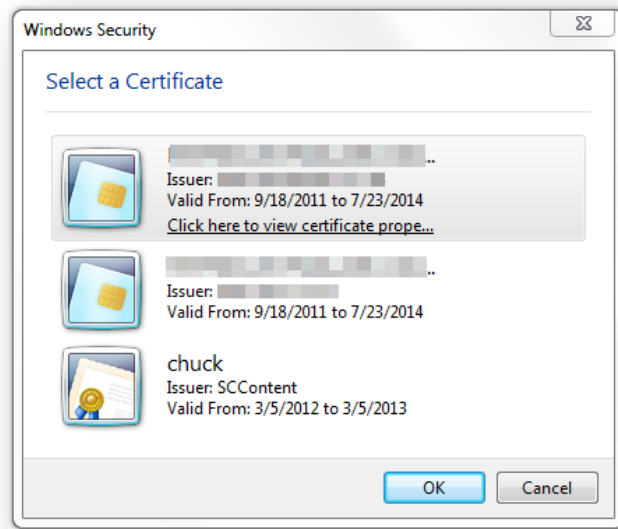
Connect with Certificate or Card Enabled Browser



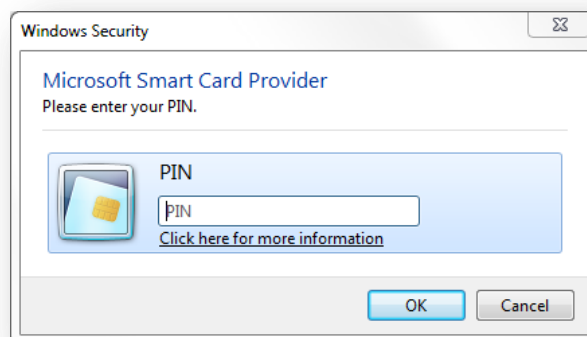
The following information is provided with the understanding that your browser is configured for SSL certificate authentication. This includes the proper trust of the CA by the web browser. Please refer to your browser's help files or other documentation to configure this feature.

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

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



- 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.

Nessus without Internet Access

This section describes the steps to register your Nessus scanner, install the Activation Code, and receive the latest plugins when your Nessus system does not have direct access to the Internet.



Activation Codes retrieved using the off-line process described below are tied to the Nessus scanner used during the off-line update process. You cannot use the downloaded plugin package with another Nessus scanner.

Begin by following the instructions provided by Nessus. When it requests an Activation Code, enter “Offline” as instructed.

Generate a Challenge Code

You must retrieve your Activation Code from either your [Tenable Support Portal](#) account for Nessus or your Nessus Home registration email.

Note that you can only use one Activation Code per scanner, unless the scanners are managed by SecurityCenter.

Once you have the Activation Code, run the following command on the system running Nessus:

Windows:

```
C:\Program Files\Tenable\Nessus>nessus-fetch.exe --challenge
```

Linux:

```
# /opt/nessus/bin/nessus-fetch --challenge
```

FreeBSD:

```
# /usr/local/nessus/bin/nessus-fetch --challenge
```

Mac OS X:

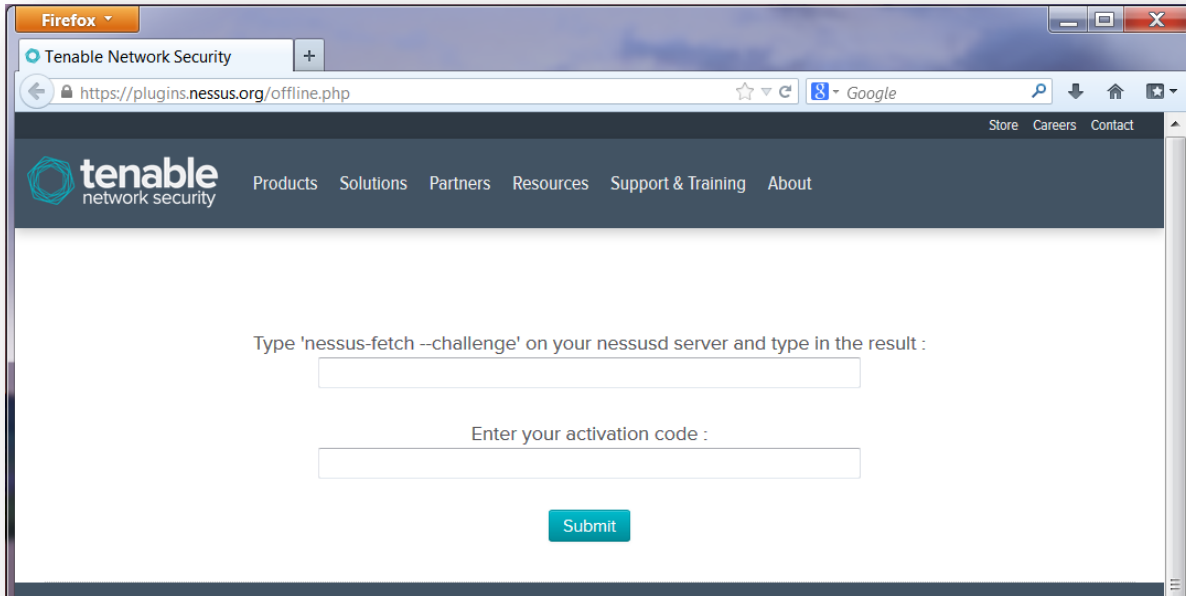
```
# /Library/Nessus/run/bin/nessus-fetch --challenge
```

This will produce a string called a “challenge code” that looks like the following:

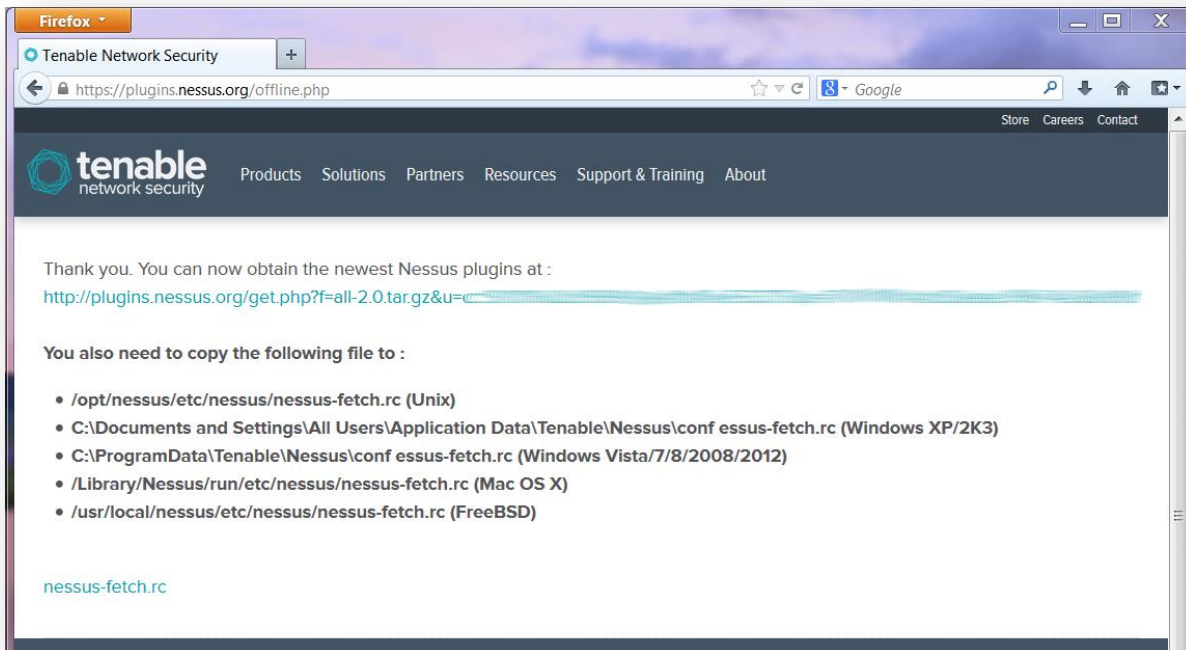
```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Obtain and Install Up-to-date Plugins

Next, go to <https://plugins.nessus.org/offline.php> and copy and paste the “challenge” string as well as the Activation Code that you received previously into the appropriate text boxes:



This will produce a URL similar to the screen capture below:



This screen gives you access to download the latest Nessus plugin feed (`all-2.0.tar.gz`) along with a link to the `nessus-fetch.rc` file at the bottom of the screen.



Save this URL because you will use it every time you update your plugins, as described below.



A registration code used for offline updating cannot then be used on the same Nessus scanner server via the Nessus Server Manager.

Next, run the following command to register Nessus offline, and install the `nessus-fetch.rc` file to the Nessus directory on the host:

Windows XP/2K3:

```
C:\Program Files\Tenable\Nessus>nessus-fetch.exe --register-offline "C:\Documents and Settings\All Users\Application Data\Tenable\Nessus\conf\nessus-fetch.rc"
```

Windows Vista/7/8/2008/2012:

```
C:\Program Files\Tenable\Nessus>nessus-fetch.exe --register-offline "C:\ProgramData\Tenable\Nessus\conf\nessus-fetch.rc"
```

Note: The location of the configuration files changed between Nessus 5.0 and 5.2.

Linux:

```
# /opt/nessus/bin/nessus-fetch --register-offline /opt/nessus/etc/nessus/nessus-fetch.rc
```

FreeBSD:

```
# /usr/local/nessus/bin/nessus-fetch --register-offline  
/usr/local/nessus/etc/nessus/nessus-fetch.rc
```

Mac OS X:

```
# /Library/Nessus/run/bin/nessus-fetch --register-offline  
/Library/Nessus/run/etc/nessus/nessus-fetch.rc
```

Note that, by default, Nessus will attempt to update its plugins every 24 hours after you have registered it. If you do not want this online update attempted, edit the `auto_update` setting to `no` under the **Configuration** -> **Advanced** menu.



Perform this step each time you perform an offline update of your plugins.

Once downloaded, move the `all-2.0.tar.gz` file to the Nessus directory. Next, instruct Nessus to process the plugin archive:

Windows:

```
C:\Program Files\Tenable\Nessus>nessus-update-plugins.exe all-2.0.tar.gz
```

Unix and Mac OS X (modify path for your installation):

```
# /opt/nessus/sbin/nessus-update-plugins all-2.0.tar.gz
```

Once processed, Nessus must be restarted for the changes to take effect. Consult the [“Nessus Service Manipulation via Windows CLI”](#) or [“Start/Stop the Nessus Daemon”](#) (Unix) sections for details on performing a restart.

Once the plugins have been installed, you do not need to keep the `all-2.0.tar.gz` file. However, Tenable recommends that you retain the latest version of the downloaded plugin file in case it is needed again.

Now, you will have the latest plugins available. Each time you wish to update your plugins while not having Internet access, you must go to the provided URL, obtain the `tar/gz` file, copy it to the system running Nessus, and repeat the process above.

Using and Managing Nessus from the Command Line

Nessus Major Directories

The following table lists the installation location and primary directories used by Nessus on *nix/Linux:

| Nessus Home Directory | Nessus Sub-Directories | Purpose |
|-----------------------------------------------|------------------------------------|----------------------------------|
| Unix Distributions | | |
| Red Hat, SuSE, Debian, Ubuntu: /opt/nessus | ./etc/nessus/ | Configuration files |
| | ./var/nessus/users/<username>/kbs/ | User knowledgebase saved on disk |
| FreeBSD: /usr/local/nessus | ./lib/nessus/plugins/ | Nessus plugins |
| Mac OS X: /Library/Nessus/run | ./var/nessus/logs/ | Nessus log files |

The following table lists the installation location and primary directories used by Nessus on Windows:

| Nessus Home Directory | Nessus Sub-Directories | Purpose |
|-------------------------------|------------------------------|----------------------------------|
| Windows | | |
| \Program Files\Tenable\Nessus | \conf | Configuration files |
| | \data | Stylesheet templates |
| | \nessus\plugins | Nessus plugins |
| | \nessus\users\<username>\kbs | User knowledgebase saved on disk |
| | \nessus\logs | Nessus log files |

Create and Manage Nessus Users with Account Limitations

A single Nessus scanner can support a complex arrangement of multiple users. For example, an organization may need multiple personnel to have access to the same Nessus scanner but have the ability to scan different IP ranges, allowing only some personnel access to restricted IP ranges.

The following example highlights the creation of a second Nessus user with password authentication and user rules that restrict the user to scanning a class B subnet, 172.20.0.0/16. For further examples and the syntax of user rules please see the man pages for `nessus-adduser`.

```

# /opt/nessus/sbin/nessus-adduser
Login : tater-nessus
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...) (y/n)
    [n]: y
User rules
-----
nessusd has a rules system which allows you to restrict the hosts
that tater-nessus has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)
accept 172.20.0.0/16
deny 0.0.0.0/0

Login          : tater-nessus
Password       : *****
This user will have 'admin' privileges within the Nessus server
Rules          :
accept 172.20.0.0/16
deny 0.0.0.0/0
Is that ok ? (y/n) [y] y
User added

```



To view the `nessus-adduser(8)` man page, on some operating systems you may have to perform the following commands:

```

# export MANPATH=/opt/nessus/man
# man nessus-adduser

```

Nessusd Command Line Options

In addition to running the `nessusd` server, there are several command line options that can be used as required. The following table contains information on these various optional commands.

| Option | Description |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-c <config-file></code> | When starting the <code>nessusd</code> server, this option is used to specify the server-side <code>nessusd</code> configuration file to use. It allows for the use of an alternate configuration file instead of the standard <code>/opt/nessus/etc/nessus/nessusd.db</code> (or <code>/usr/local/nessus/etc/nessus/nessusd.db</code> for FreeBSD). |
| <code>-a <address></code> | When starting the <code>nessusd</code> server, this option is used to tell the server to only listen to connections on the address <code><address></code> that is an IP, not a machine name. This option is useful if you are running <code>nessusd</code> on a gateway and if you do not want people on the outside to connect to your <code>nessusd</code> . |

| | |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-S <ip[,ip2,...]></code> | When starting the <code>nessusd</code> server, force the source IP of the connections established by Nessus during scanning to <code><ip></code> . 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 <code>nessusd</code> must have multiple NICs with these IP addresses set. |
| <code>-p <port-number></code> | When starting the <code>nessusd</code> server, this option will tell the server to listen for client connections on the port <code><port-number></code> rather than listening on port 1241, which is the default. |
| <code>-D</code> | When starting the <code>nessusd</code> server, this option will make the server run in the background (daemon mode). |
| <code>-v</code> | Display the version number and exit. |
| <code>-l</code> | Display the plugin feed license information and exit. |
| <code>-h</code> | Show a summary of the commands and exit. |
| <code>--ipv4-only</code> | Only listen on IPv4 socket. |
| <code>--ipv6-only</code> | Only listen on IPv6 socket. |
| <code>-q</code> | Operate in “quiet” mode, suppressing all messages to <code>stdout</code> . |
| <code>-R</code> | Force a re-processing of the plugins. |
| <code>-t</code> | Check the timestamp of each plugin when starting up to only compile newly updated plugins. |
| <code>-K</code> | Set a master password for the scanner. |

If a master password is set, Nessus will cipher all policies and any credentials contained in them with the user-supplied key (considerably more secure than the default key). If a password is set, the web interface will prompt you for the password during startup.



WARNING: If the master password is set and lost, it cannot be recovered by your administrator or Tenable Support.

An example of the usage is shown below:

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,...]>]
```

Nessus Service Manipulation via Windows CLI

Nessus can also be started or stopped from the command line. Note that the command window must be called with Administrative privileges:

```
C:\Windows\system32>net stop "Tenable Nessus"  
The Tenable Nessus service is stopping.  
The Tenable Nessus service was stopped successfully.
```

```
C:\Windows\system32>net start "Tenable Nessus"  
The Tenable Nessus service is starting.  
The Tenable Nessus service was started successfully.
```

```
C:\Windows\system32>
```

Working with SecurityCenter

SecurityCenter Overview

Tenable's SecurityCenter is a web-based management console that unifies the process of vulnerability detection and management, event and log management, compliance monitoring, and reporting on all of the above. SecurityCenter enables efficient communication of security events to IT, management, and audit teams.

SecurityCenter supports the use of multiple Nessus scanners in concert for the scanning of virtually any size network on a periodic basis. Using the Nessus API (a custom implementation of the XML-RPC protocol), SecurityCenter communicates with associated Nessus scanners to send scanning instructions and receive results.

SecurityCenter enables multiple users and administrators with different security levels to share vulnerability information, prioritize vulnerabilities, show which network assets have critical security issues, make recommendations to system administrators for fixing these security issues and to track when the vulnerabilities are mitigated. SecurityCenter also receives data from many leading intrusion detection systems such as Snort and ISS via the Log Correlation Engine (LCE).

SecurityCenter can also receive passive vulnerability information from Tenable's Passive Vulnerability Scanner (PVS) such that end users can discover new hosts, applications, vulnerabilities, and intrusions without the need for active scanning with Nessus.



Note that if Nessus Enterprise manages secondary scanners, those scanners will **not** be available to SecurityCenter. Any secondary scanners will remain exclusive to Nessus Enterprise.

Configuring SecurityCenter to work with Nessus

The SecurityCenter administration interface is used to configure access and control of any Nessus scanner that is version 4.2.x or higher. Click the "**Resources**" tab and then click "**Nessus Scanners**". Click "**Add**" to open the "**Add Scanner**" dialog. The Nessus scanner's IP address or hostname, Nessus port (default: 8834), authentication type (created while configuring Nessus), administrative login ID and password or certificate information, and a name are required. The password fields are not available if "SSL Certificate" authentication is selected. The ability to Verify Hostname is provided to check the CommonName (CN) of the SSL certificate presented by the Nessus server. The state of the Nessus scanner may be set to Enabled or Disabled as needed, the use of a proxy may be selected, and selection of Scan Zones for the Nessus scanner to be assigned to can be selected.

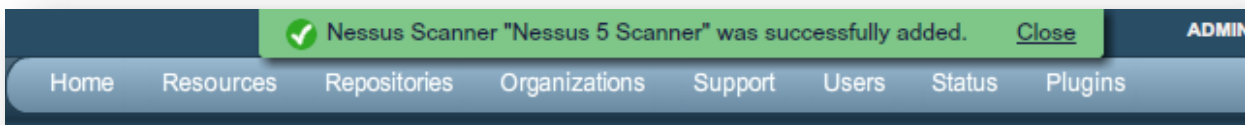
An example screen capture of the SecurityCenter 4.7 “Add Scanner” page is shown below:

The screenshot shows the 'Add Scanner' configuration page in SecurityCenter 4.7. The form is organized into several sections:

- Name:** Local Scanner
- Description:** Local SecurityCenter Scanner
- Scanner:**
 - Host: 127.0.0.1
 - Port: 8834
 - State: Enabled Disabled
 - Verify Hostname:
 - Use Proxy:
- Authentication:**
 - Authentication Type: Password
 - Username: nessusadmin
 - Password: [masked]
- Zones:**
 - Target Zone: Web Farm Zone, Database Servers

Buttons for 'Cancel' and 'Submit' are located at the bottom right of the form.

After successfully adding the scanner, the following banner is displayed:



For more information on integrating Nessus and SecurityCenter, please refer to the “SecurityCenter Administration Guide” available on the [Tenable Support Portal](#).

Host-Based Firewalls

If your Nessus server is configured with a local firewall such as ZoneAlarm, BlackICE, the Windows XP firewall, or any other firewall software, it is required that connections be opened from SecurityCenter’s IP address.

By default, port 8834 is used to communicate with SecurityCenter. On Microsoft XP Service Pack 2 systems and later, clicking on the “**Security Center**” icon available in the “**Control Panel**” presents the user with the opportunity to manage the “Windows Firewall” settings. To open up port 8834 choose the “**Exceptions**” tab and then add port “8834” to the list.

Nessus Windows Troubleshooting

Installation /Upgrade Issues

Issue: The `nessusd.messages` log indicates `nessusd` started, but it hasn't.

Solution: The “`nessusd <version> started`” message only indicates that the `nessusd` program was executed. The message “`nessusd is ready`” indicates that the Nessus server is running and ready to accept connections.

Issue: I am receiving the following error when I try to install Nessus Windows:

“1607: Unable to install InstallShield Scripting Runtime”

Solution: This error code can be produced if the Windows Management Instrumentation (WMI) service has been disabled for any reason. Please verify that the service is running.

If the WMI service is running, then this may be a problem between the Microsoft Windows Operating System settings and the InstallShield product that is used for installing and removing Nessus Windows. There are knowledge base articles from both Microsoft and InstallShield that detail potential causes and the resolution of the issue.

- Microsoft Knowledge Base Article ID 910816:
<http://support.microsoft.com/?scid=kb;en-us;910816>
- InstallShield Knowledge Base Article ID Q108340:
<http://consumer.installshield.com/kb.asp?id=Q108340>

Scanning Issues

Issue: I cannot scan over my PPP or PPTP connection.

Solution: Currently, this is not supported. Future revisions of Nessus Windows will include this functionality.

Issue: A virus scan of my system reports a large number of viruses or malware in Nessus Windows.

Solution: Certain anti-virus applications may show some of the Nessus plugins as viruses. Exclude the plugins directory from virus scans since there are no executable programs in this directory. For more information on using Nessus in conjunction with Anti Malware software, consult the “[Nessus 5 and Antivirus](#)” document.

Issue: I am scanning an unusual device, such as a RAID controller, and the scan is aborted because Nessus has detected it as a printer.

Solution: Disable “Safe Checks” in the scan policy before scanning the device. A scan of a printer will usually result in the printer needing to be restarted, therefore when “Safe Checks” is set, devices detected as printers are not scanned.

Issue: SYN scans do not appear to wait for the port connection to be established in Nessus Windows.

Solution: This is correct in that the SYN scan does not establish a full TCP connect, however it does not change the scan results.

Issue: When performing a scan, what factors affect performance when running Nessus Windows on a Windows XP system?

Solution: Microsoft has added changes to Windows XP Service Pack 2 and 3 (Home and Pro) that can impact the performance of Nessus Windows and cause false negatives. The TCP/IP stack now limits the number of simultaneous incomplete outbound TCP connection attempts. After the limit has been reached, subsequent connection attempts are put in a queue and will be resolved at a fixed rate (10 per second). If too many enter the queue, they may be dropped. See the following Microsoft TechNet page for more information:

<http://technet.microsoft.com/en-us/library/bb457156.aspx>

This has the effect of causing a Nessus scan on Windows XP to potentially have false negatives as XP only allows for 10 new connections per second that are incomplete (in a SYN state). For better accuracy, it is recommended that Nessus on a Windows XP system have its port scan throttle setting down to the following that is found in the individual scan configuration for each scan policy:

Max number of hosts: 10

Max number of security checks: 4

For increased performance and scan reliability, it is highly recommended that Nessus Windows be installed on a server product from the Microsoft Windows family such as Windows Server 2003 or Windows Server 2008.



Note that Windows XP support will be dropped completely as of Nessus 5.3 and later.

For Further Information

Tenable has produced a variety of other documents detailing Nessus' deployment, configuration, user operation, and overall testing. These are listed here:

- **Nessus 5.2 User Guide** – describes use of the Nessus vulnerability scanner including scan configuration and reporting
- **Nessus 5.2 Enterprise User Guide** – how to configure and operate the Nessus User Interface for Nessus Enterprise
- **Nessus Enterprise Cloud User Guide** – describes use of Nessus Enterprise Cloud and includes subscription and activation, vulnerability scanning, compliance reporting, and Nessus Enterprise Cloud support
- **Nessus Credential Checks for Unix and Windows** – information on how to perform authenticated network scans with the Nessus vulnerability scanner
- **Nessus Compliance Checks** – high-level guide to understanding and running compliance checks using Nessus and SecurityCenter
- **Nessus Compliance Checks Reference** – comprehensive guide to Nessus Compliance Check syntax
- **Nessus v2 File Format** – describes the structure for the `.nessus` file format, which was introduced with Nessus 3.2 and NessusClient 3.2
- **Nessus 5.0 REST Protocol Specification** – describes the REST protocol and interface in Nessus

- **Nessus 5 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
- **Nessus 5 and Mobile Device Scanning** – describes how Nessus integrates with Microsoft Active Directory and mobile device management servers to identify mobile devices in use on the network
- **Nessus 5.0 and Scanning Virtual Machines** – describes how Tenable Network Security's Nessus vulnerability scanner can be used to audit the configuration of virtual platforms as well as the software that is running on them
- **Strategic Anti-malware Monitoring with Nessus, PVS, and LCE** – describes how Tenable's USM platform can detect a variety of malicious software and identify and determine the extent of malware infections
- **Patch Management Integration** – document describes how Nessus and SecurityCenter can leverage credentials on the IBM TEM, Microsoft WSUS and SCCM, VMware Go, and Red Hat Network Satellite patch management systems to perform patch auditing on systems for which credentials may not be available to the Nessus scanner
- **Real-Time Compliance Monitoring** – outlines how Tenable's solutions can be used to assist in meeting many different types of government and financial regulations
- **Tenable Products Plugin Families** – provides a description and summary of the plugin families for Nessus, Log Correlation Engine, and the Passive Vulnerability Scanner
- **SecurityCenter Administration Guide**

Other online resources are listed below:

- Nessus Discussions Forum: <https://discussions.nessus.org/>
- Tenable Blog: <http://www.tenable.com/blog>
- Tenable Podcast: <http://www.tenable.com/podcast>
- Example Use Videos: <http://www.youtube.com/user/tenablesecurity>
- Tenable Twitter Feed: <http://twitter.com/tenablesecurity>

Please feel free to contact Tenable at support@tenable.com, sales@tenable.com, or visit our website at <http://www.tenable.com/>.

About Tenable Network Security

Tenable Network Security is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard to identify vulnerabilities, prevent attacks and comply with a multitude of regulatory requirements. For more information, please visit www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com

