Nessus 4.4
Installation Guide

December 2, 2010
(Revision 3)

The newest version of this document is available at the following URL:
http://www.nessus.org/documentation/nessus_4.4_installation_guide.pdf

Table of Contents

Introduction

This document describes the installation and configuration of Tenable Network Security's **Nessus 4.4** vulnerability scanner. Please share your comments and suggestions with us by emailing them to support@tenable.com.

Tenable Network Security, Inc. is the author and manager of the Nessus Security 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 will be discussed in this document. A basic understanding of Unix and vulnerability scanning is assumed.

Starting with Nessus 4.4, user management of the Nessus server is conducted through a web interface and it is no longer necessary to use a standalone NessusClient. The standalone NessusClient will still connect and operate the scanner, but it will not be updated.

OS Support

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

- Debian 5 (i386 and x86-64)
- Fedora Core 12, 13 and 14 (i386 and x86-64)
- FreeBSD 8 (i386 and x86-64)
- Mac OS X 10.4, 10.5 and 10.6 (i386, x86-64, ppc)
- Red Hat ES 4 / CentOS 4 (i386)
- Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 and x86-64)
- Red Hat ES 6 (i386 and x86-64)
- Solaris 10 (sparc)
- SuSE 9.3 (i386)
- SuSE 10.0 (i386 and x86-64)
- Ubuntu 8.04, 9.10, 10.04 and 10.10 (i386 and x86-64)
- Windows XP, Server 2003, Server 2008, Server 2008 R2, Vista and 7 (i386 and x86-64)

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 will also be printed with the **`courier bold`** font. Command line options may or may not include the command line prompt and output text from the results of the command. Often, the command being run will be **boldfaced** to indicate what the user typed. Below 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.

Background

Nessus is a powerful, up-to-date and easy to use network security scanner. 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 broken into 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. Note that security checks can also be written in the C programming language.

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.nessus.org/scripts.php.

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 (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 will determine which plugins should or should not be launched against the remote host. For example, Nessus will not test sendmail vulnerabilities against Postfix. This option is called "optimization".

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 a minimum of 1 GB of memory to operate Nessus. To conduct larger scans of multiple networks, at least 2 GB of memory is recommended, but it may require up to 4 GB.

A Pentium 3 processor running at 2 GHz or higher is recommended. When running on Mac OS X, a dual-core Intel® processor running at 2 GHz or higher is recommended.

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

- OpenSSL (e.g., openssl, libssl, libcrypto)
- zlib
- GNU C Library (i.e., libc)

Nessus Windows

Microsoft has added changes to Windows XP SP-2 and newer (Home and Pro) 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.

Vulnerability Plugin Subscriptions

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.nessus.org/plugins/index.php?view=all. Tenable distributes the latest vulnerability plugins in two modes for Nessus; the ProfessionalFeed and the HomeFeed.

> ⚠ With Nessus 4, you are required to register for a plugin feed and update the plugins 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.

Which Feed is For You?

Specific directions to configure Nessus to receive either a HomeFeed or ProfessionalFeed are provided later in this document. To determine which Nessus feed is appropriate for your environment, consider the following:

HomeFeed

If you are using Nessus at home for non-professional purposes, you may subscribe to the HomeFeed. New plugins for the latest security vulnerabilities are immediately released to HomeFeed users. There is no charge to use the HomeFeed, however, there is a separate license for the HomeFeed that users must agree to comply with. To register for the HomeFeed, visit http://www.nessus.org/register/ and register your copy of Nessus to use the HomeFeed. Use the Activation Code you receive from the registration process when configuring Nessus to do updates. HomeFeed users do not receive access to the Tenable Support Portal, compliance checks or content audit policies.

ProfessionalFeed

If you are using Nessus for commercial purposes (e.g., consulting), in a business environment or in a government environment, you must purchase a ProfessionalFeed. New plugins for the latest security vulnerabilities are immediately released to ProfessionalFeed users. SecurityCenter customers are automatically subscribed to the ProfessionalFeed and do not need to purchase an additional feed unless they have a Nessus scanner that is not managed by SecurityCenter.

Tenable provides commercial support, via the Tenable Support Portal or email, to ProfessionalFeed customers who are using Nessus 4. The ProfessionalFeed also includes a set of host-based compliance checks for Unix and Windows that are very useful when performing compliance audits such as SOX, FISMA or FDCC.

You may purchase a ProfessionalFeed either through Tenable's e-commerce site at https://products.nessus.org/ or, via a purchase order through Authorized ProfessionalFeed 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 have access to the ProfessionalFeed and will automatically update your Nessus scanners.

> 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.

Unix/Linux

Upgrading

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

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.

Platform	Upgrade Instructions
Red Hat ES 4 (32 bit), ES 5 (32 and 64 bit)	
Upgrade Commands	`# service nessusd stop` Use one of the appropriate commands below that corresponds to the version of Red Hat you are running:

```
# rpm -Uvh Nessus-4.4.0-es4.i386.rpm
# rpm -Uvh Nessus-4.4.0-es5.i386.rpm
# rpm -Uvh Nessus-4.4.0-es5.x86_64.rpm
```

Once the upgrade is complete, restart the **nessusd** service with the following command:

```
# service nessusd start
```

Sample Output

```
# service nessusd stop
Shutting down Nessus services:                [  OK  ]
# rpm -Uvh Nessus-4.4.0-es4.i386.rpm
Preparing...
########################################### [100%]
Shutting down Nessus services:
   1:Nessus
########################################### [100%]
nessusd (Nessus) 4.4.0 for Linux
(C) 1998 - 2009 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
 - Please run /opt/nessus/sbin/nessus-adduser to add an
admin user
 - Register your Nessus scanner at
http://www.nessus.org/register/ to
   obtain all the newest plugins
 - You can start nessusd by typing /sbin/service
nessusd start

# service nessusd start
Starting Nessus services:                     [  OK  ]
#
```

Fedora Core 12, 13 and 14 (32 and 64 bit)

Upgrade Commands

```
# service nessusd stop
```

Use one of the appropriate commands below that corresponds to the version of Fedora Core you are running:

```
# rpm -Uvh Nessus-4.4.0-fc12.i386.rpm
# rpm -Uvh Nessus-4.4.0-fc12.x86_64.rpm
# rpm -Uvh Nessus-4.4.0-fc14.i386.rpm
# rpm -Uvh Nessus-4.4.0-fc14.x86_64.rpm
```

Once the upgrade is complete, restart the **nessusd** service with the following command:

```
# service nessusd start
```

Sample Output

```
# service nessusd stop
Shutting down Nessus services:                [  OK  ]
# rpm -Uvh Nessus-4.4.0-fc12.i386.rpm
Preparing...
########################################### [100%]
Shutting down Nessus services:
   1:Nessus
########################################### [100%]
nessusd (Nessus) 4.4.0 for Linux
(C) 1998 - 2009 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
 - Please run /opt/nessus/sbin/nessus-adduser to add an
admin user
 - Register your Nessus scanner at
http://www.nessus.org/register/ to
   obtain all the newest plugins
 - You can start nessusd by typing /sbin/service
nessusd start

# service nessusd start
Starting Nessus services:                     [  OK  ]
#
```

SuSE 9.3 (32 bit), 10 (32 and 64 bit)

Upgrade Commands

```
# service nessusd stop
```

Use one of the appropriate commands below that corresponds to the version of SuSE you are running:

```
# rpm -Uvh Nessus-4.4.0-suse9.3.i586.rpm
# rpm -Uvh Nessus-4.4.0-suse10.0.i586.rpm
# rpm -Uvh Nessus-4.4.0-suse10.x86_64.rpm
```

Once the upgrade is complete, restart the `nessusd` service with the following command:

```
# service nessusd start
```

Sample Output

```
# service nessusd stop
Shutting down Nessus services:                [  OK  ]
# rpm -Uvh Nessus-4.4.0-suse10.0.i586.rpm
Preparing...
########################################### [100%]
Shutting down Nessus services:
   1:Nessus
########################################### [100%]
nessusd (Nessus) 4.4.0 for Linux
(C) 1998 - 2009 Tenable Network Security, Inc.

Processing the Nessus plugins...
```

	[##] All plugins loaded - Please run /opt/nessus/sbin/nessus-adduser to add an admin user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /sbin/service nessusd start # **service nessusd start** Starting Nessus services: [OK] #
Debian 5 (32 and 64 bit)	
Upgrade Commands	# **/etc/init.d/nessusd stop** Use one of the appropriate commands below that corresponds to the version of Debian you are running: # **dpkg -i Nessus-4.4.0-debian5_i386.deb** # **dpkg -i Nessus-4.4.0-debian5_amd64.deb** # **/etc/init.d/nessusd start**
Sample Output	# **/etc/init.d/nessusd stop** # **dpkg -i Nessus-4.4.0-debian5_i386.deb** (Reading database ... 19831 files and directories currently installed.) Preparing to replace nessus 4.4.0 (using Nessus-4.4.0-debian5_i386.deb) ... Shutting down Nessus : . Unpacking replacement nessus ... Setting up nessus (4.4.0) ... nessusd (Nessus) 4.4.0. for Linux (C) 2009 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded - Please run /opt/nessus/sbin/nessus-adduser to add an admin user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /etc/init.d/nessusd start

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

Starting Nessus : .
#
```

Ubuntu 8.04, 9.10, 10.04 and 10.10 (32 and 64 bit)

Upgrade Commands

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

Use one of the appropriate commands below that corresponds to the version of Ubuntu you are running:

```
# dpkg -i Nessus-4.4.0-ubuntu804_i386.deb
# dpkg -i Nessus-4.4.0-ubuntu804_amd64.deb
# dpkg -i Nessus-4.4.0-ubuntu910_i386.deb
# dpkg -i Nessus-4.4.0-ubuntu910_amd64.deb
# dpkg -i Nessus-4.4.0-ubuntu1010_amd64.deb
# dpkg -i Nessus-4.4.0-ubuntu1010_i386.deb

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

Sample Output

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

# dpkg -i Nessus-4.4.0-ubuntu804_i386.deb
(Reading database ... 19831 files and directories
currently installed.)
Preparing to replace nessus 4.4.0 (using Nessus-4.4.0-
ubuntu810_i386.deb) ...
Shutting down Nessus : .
Unpacking replacement nessus ...

Setting up nessus (4.4.0) ...

nessusd (Nessus) 4.4.0. for Linux
(C) 2009 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded

 - Please run /opt/nessus/sbin/nessus-adduser to add an
admin user
 - Register your Nessus scanner at
http://www.nessus.org/register/ to
   obtain all the newest plugins
 - You can start nessusd by typing /etc/init.d/nessusd
start

# /etc/init.d/nessusd start

Starting Nessus : .
#
```

Solaris 10 (sparc)

Upgrade Commands

```
# /etc/init.d/nessusd stop
# pkginfo | grep nessus
```

The following is example output for the previous command showing the Nessus package:

```
application TNBLnessus               The Nessus Network
Vulnerability Scanner
```

To remove the Nessus package on a Solaris system, run the following command:

```
# pkgrm <package name>

# gunzip Nessus-4.x.x-solaris-sparc.pkg.gz
# pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg

The following packages are available:
  1  TNBLnessus-4-2-0     TNBLnessus
                          (sparc) 4.4.0

Select package(s) you wish to process (or 'all' to
process
all packages). (default: all) [?,??,q]: 1

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

Sample Output

```
# /etc/init.d/nessusd stop
# pkginfo | grep nessus

application TNBLnessus               The Nessus Network
Vulnerability Scanner

# pkgrm TNBLnessus
(output redacted)
## Updating system information.

Removal of <TNBLnessus> was successful.

# gunzip Nessus-4.4.0-solaris-sparc.pkg.gz
# pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg

The following packages are available:
    1  TNBLnessus     The Nessus Network Vulnerability
Scanner
                    (sparc) 4.4.0
Select package(s) you wish to process (or 'all' to
process
all packages). (default: all) [?,??,q]: 1

Processing package instance <TNBLnessus> from
</export/home/cbf/TENABLE/Nessus-4.4.0-solaris-
sparc.pkg>

The Nessus Network Vulnerability Scanner
```

```
(sparc) 4.4.0
## Processing package information.
## Processing system information.
   13 package pathnames are already properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be executed
with super-user
permission during the process of installing this
package.

Do you want to continue with the installation of
<TNBLnessus> [y,n,?]

Installing The Nessus Network Vulnerability Scanner as
<TNBLnessus>

## Installing part 1 of 1.
(output redacted)
## Executing postinstall script.

 - Please run /opt/nessus/sbin/nessus-adduser to add a
user
 - Register your Nessus scanner at
http://www.nessus.org/register/ to obtain
   all the newest plugins
 - You can start nessusd by typing /etc/init.d/nessusd
start


Installation of <TNBLnessus> was successful.

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

Notes

To upgrade Nessus on Solaris, 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.

If you encounter library compatibility errors, make sure you have applied the latest Solaris Recommended Patch Cluster from Sun.

FreeBSD 8 (32 and 64 bit)

Upgrade Commands

```
# killall nessusd
# pkg_info
```

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:

```
Nessus-4.2.2       A powerful security scanner
```

Remove the Nessus package using the following command:

```
# pkg_delete <package name>
```

Use one of the appropriate commands below that corresponds to the version of FreeBSD you are running:

```
# pkg_add Nessus-4.4.0-fbsd8.tbz
# pkg_add Nessus-4.4.0-fbsd8.amd64.tbz

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

Sample Output

```
# killall nessusd
# pkg_delete Nessus-4.2.2
# pkg_add Nessus-4.4.0-fbsd8.tbz

nessusd (Nessus) 4.4.0. for FreeBSD
(C) 2009 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded

 - Please run /usr/local/nessus/sbin/nessus-adduser to
add an
   admin user
 - Register your Nessus scanner at
http://www.nessus.org/register/ to
   obtain all the newest plugins
 - You can start nessusd by typing
/usr/local/etc/rc.d/nessusd.sh start

# /usr/local/nessus/sbin/nessusd -D

nessusd (Nessus) 4.4.0. for FreeBSD
(C) 2009 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
#
```

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

⚠ The first time Nessus updates and processes the plugins, it may take several minutes. The web server will show a "Nessus is initializing.." message and will reload when ready.

Download the latest version of Nessus from http://www.nessus.org/download/ or through the Tenable Support Portal.

⚠ Unless otherwise noted, all commands must be performed as the system's root user.

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 (32 bit), ES 5 (32 and 64 bit)	

Install Command	Use one of the appropriate commands below that corresponds to the version of Red Hat you are running:
	`# rpm -ivh Nessus-4.4.0-es4.i386.rpm`
	`# rpm -ivh Nessus-4.4.0-es5.i386.rpm`
	`# rpm -ivh Nessus-4.4.0-es5.x86_64.rpm`

Sample Output	`# rpm -ivh Nessus-4.4.0-es4.i386.rpm`
	`Preparing...`
	`########################################### [100%]`
	`   1:Nessus`
	`########################################### [100%]`
	`nessusd (Nessus) 4.4.0. for Linux`
	`(C) 1998 - 2009 Tenable Network Security, Inc.`
	
	` - Please run /opt/nessus//sbin/nessus-adduser to add a`
	`user`
	` - Register your Nessus scanner at`
	`http://www.nessus.org/register/ to obtain`
	`   all the newest plugins`
	` - You can start nessusd by typing /sbin/service nessusd`
	`start`
	`#`

Fedora Core 12, 13 and 14 (32 and 64 bit)	

Install Command	Use one of the appropriate commands below that corresponds to the version of Fedora Core you are running:
	`# rpm -ivh Nessus-4.4.0-fc12.i386.rpm`
	`# rpm -ivh Nessus-4.4.0-fc12.x86_64.rpm`
	`# rpm -ivh Nessus-4.4.0-fc14.i386.rpm`
	`# rpm -ivh Nessus-4.4.0-fc14.x86_64.rpm`

Sample Output	`# rpm -ivh Nessus-4.4.0-fc12.i386.rpm`
	`Preparing...`

	## [100%] 1:Nessus ## [100%] nessusd (Nessus) 4.4.0. for Linux (C) 1998 - 2009 Tenable Network Security, Inc. - Please run /opt/nessus//sbin/nessus-adduser to add a user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /sbin/service nessusd start #
SuSE 9.3 (32 bit), 10 (32 and 64 bit)	
Install Command	Use one of the appropriate commands below that corresponds to the version of SuSE you are running: # **rpm -ivh Nessus-4.4.0-suse9.3.i586.rpm** # **rpm -ivh Nessus-4.4.0-suse10.0.i586.rpm** # **rpm -ivh Nessus-4.4.0-suse10.x86_64.rpm**
Sample Output	# **rpm -ivh Nessus-4.4.0-suse10.0.i586.rpm** Preparing... ################################## [100%] 1:Nessus ################################## [100%] Nessusd {Nessus} 4.4.0. for Linux (C) 1998 - 2009 Tenable Network Security, Inc. - Please run /opt/nessus//sbin/nessus-adduser to add a user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /etc/rc.d/nessusd start #
Debian 5 (32 and 64 bit)	
Install Command	Use one of the appropriate commands below that corresponds to the version of Debian you are running: # **dpkg -i Nessus-4.4.0 -debian5_i386.deb** # **dpkg -i Nessus-4.4.0 -debian5_amd64.deb**
Sample Output	# **dpkg -i Nessus-4.4.0-debian5_i386.deb** Selecting previously deselected package nessus. (Reading database ... 36954 files and directories currently installed.) Unpacking nessus (from Nessus-4.4.0-debian5_i386.deb) ...

```
Setting up nessus (4.4.0) ...
nessusd (Nessus) 4.4.0. for Linux
(C) 1998 - 2009 Tenable Network Security, Inc.


 - Please run /opt/nessus/sbin/nessus-adduser to add a
user
 - Register your Nessus scanner at
http://www.nessus.org/register/ to obtain
   all the newest plugins
 - You can start nessusd by typing /etc/init.d/nessusd
start
#
```

Notes

The Nessus daemon cannot be started until Nessus has been registered and a plugin download has occurred. By default Nessus comes with an empty plugin set. If you attempt to start Nessus without plugins, the following output is returned:

```
# /etc/init.d/nessusd start
Starting Nessus : .
# Missing plugins. Attempting a plugin update...
Your installation is missing plugins. Please register and
try again.
To register, please visit http://www.nessus.org/register/
```

Ubuntu 8.04, 9.10, 10.04 and 10.10 (32 and 64 bit)

Install Command

Use one of the appropriate commands below that corresponds to the version of Ubuntu you are running:

```
# dpkg -i Nessus-4.4.0-ubuntu804_i386.deb
# dpkg -i Nessus-4.4.0-ubuntu804_amd64.deb
# dpkg -i Nessus-4.4.0-ubuntu910_i386.deb
# dpkg -i Nessus-4.4.0-ubuntu910_amd64.deb
# dpkg -i Nessus-4.4.0-ubuntu1010_amd64.deb
# dpkg -i Nessus-4.4.0-ubuntu1010_i386.deb
```

Sample Output

```
# dpkg -i Nessus-4.4.0-ubuntu804_amd64.deb
Selecting previously deselected package nessus.
(Reading database ... 32444 files and directories
currently installed.)
Unpacking nessus (from Nessus-4.4.0-ubuntu804_amd64.deb)
...
Setting up nessus (4.4.0) ...

 - Please run /opt/nessus/sbin/nessus-adduser to add a
user
 - Register your Nessus scanner at
http://www.nessus.org/register/ to obtain
   all the newest plugins
 - You can start nessusd by typing /etc/init.d/nessusd
start
#
```

Solaris 10 (sparc)

Install Command

```
# gunzip Nessus-4.4.0-solaris-sparc.pkg.gz
# pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg

The following packages are available:
  1  TNBLnessus     The Nessus Network Vulnerability
Scanner
                    (sparc) 4.4.0

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:1
```

Sample Output

```
# gunzip Nessus-4.4.0-solaris-sparc.pkg.gz
# pkgadd -d ./Nessus-4.4.0-solaris-sparc.pkg

The following packages are available:
  1  TNBLnessus     The Nessus Network Vulnerability
Scanner
                    (sparc) 4.4.0

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:1
Processing package instance <TNBLnessus> from
</tmp/Nessus-4.4.0-solaris-sparc.pkg>

The Nessus Network Vulnerability Scanner(sparc) 4.4.0
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with
super-user
permission during the process of installing this package.

Do you want to continue with the installation of
<TNBLnessus> [y,n,?]
Installing The Nessus Network Vulnerability Scanner as
<TNBLnessus>

## Installing part 1 of 1.
(output redacted)
## Executing postinstall script.

 - Please run /opt/nessus/sbin/nessus-adduser to add a
user
 - Register your Nessus scanner at
http://www.nessus.org/register/ to obtain
   all the newest plugins
 - You can start nessusd by typing /etc/init.d/nessusd
start
```

	Installation of <TNBLnessus> was successful. # **/etc/init.d/nessusd start** #
Notes	If you encounter library compatibility errors, make sure you have applied the latest Solaris Recommended Patch Cluster from Sun.
FreeBSD 8 (32 and 64 bit)	
Install Command	Use one of the appropriate commands below that corresponds to the version of FreeBSD you are running: # **pkg_add Nessus-4.4.0-fbsd8.tbz** # **pkg_add Nessus-4.4.0-fbsd8.amd64.tbz**
Sample Output	# **pkg_add Nessus-4.4.0-fbsd8.tbz** nessusd (Nessus) 4.4.0 for FreeBSD (C) 1998 - 2009 Tenable Network Security, Inc. Processing the Nessus plugins... [##] All plugins loaded - Please run /usr/local/nessus/sbin/nessus-adduser to add an admin user - Register your Nessus scanner at http://www.nessus.org/register/ to obtain all the newest plugins - You can start nessusd by typing /usr/local/etc/rc.d/nessusd.sh start #

Once Nessus is installed, it is recommended that you customize the provided configuration file for your environment as described in the "Configuration" section.

Configuration

Nessus Major Directories

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

Nessus Home Directory	Nessus Sub-Directories	Purpose
Unix Distributions		
Red Hat, SuSE,	**./etc/nessus/**	Configuration files

Debian, Ubuntu, Solaris: **/opt/nessus**	**./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

Create a Nessus User

At a minimum, create one Nessus user so client utilities can log into Nessus to initiate scans and retrieve results.

> Unless otherwise noted, perform all commands as the system’s root user.

For password authentication use the **nessus-adduser** command to add users. For the first user created, it is recommended to be the admin user.

Each Nessus user has a set of rules referred to as “user rules” that control what they can and cannot scan. By default, if user rules are not entered during the creation of a new Nessus user, then the user can scan any IP range. Nessus supports a global set of rules maintained in the “**nessusd.rules**” file. These rules are honored over any user-specific rules. When creating rules specific to a user, they are to further refine any existing global rules.

```
# /opt/nessus/sbin/nessus-adduser
Login : sumi_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 sumi_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)



Login             : sumi_nessus
Password         : ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
Is that ok ? (y/n) [y] y
```

```
User added
#
```

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 `nessusd.conf`. **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.

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]: n
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         : ***********
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
```

⚠ In Nessus 4.0.x and before, authentication between the Nessus Client and Nessus Server was configurable using SSL certificates. This is no longer required as the Nessus server is accessed via SSL web authentication and not a separate Nessus Client. The only exception is authentication between SecurityCenter and the Nessus server since SecurityCenter functions as a Nessus client. Information on SSL certificate authentication for this configuration is available in the SecurityCenter documentation.

Installing the Plugin Activation Code

⚠ If you are using the Tenable SecurityCenter, the Activation Code and plugin updates are managed from SecurityCenter. In order to communicate with SecurityCenter, Nessus needs to be started, 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 plugin updates from SecurityCenter), run the following command:

```
# nessus-fetch --security-center
```

Immediately after running the "**nessus-fetch**" command above, use the applicable command to start the Nessus server. The Nessus server can now be added to the SecurityCenter via the SecurityCenter web interface. Please refer to the SecurityCenter documentation for the configuration of a centralized plugin feed for multiple Nessus scanners.

Before Nessus starts for the first time, you must provide an Activation Code to download the current plugins. The initial download and processing of plugins will require extra time before the Nessus Server is ready.

Depending on your subscription service, you will have received an Activation Code that entitles you to receive either the ProfessionalFeed or the HomeFeed plugins. This synchronizes your Nessus scanner with all available plugins. Activation Codes may be 16 or 20 character alpha-numeric strings with dashes.

To install the Activation Code, type the following command on the system running Nessus, where **<license code>** is the registration code that you received:

Linux and Solaris:

```
# /opt/nessus/bin/nessus-fetch --register <Activation Code>
```

FreeBSD:

```
# /usr/local/nessus/bin/nessus-fetch --register <Activation Code>
```

⚠ After the initial registration, Nessus will download and compile the plugins obtained from plugins.nessus.org in the background. The first time this occurs, it may take up to 10 minutes before the Nessus server is ready. When the message "nessusd is ready" appears in the **nessusd.messages** log, the Nessus server will accept client connections and the scan interface will become available. The activation code is **not** case sensitive.

An Internet connection is required for this step. If you are running Nessus on a system that does not have an internet connection, follow the steps in the section "Nessus without Internet Access" to install your activation code.

The example below shows the steps involved in registering the plugin Activation Code, retrieving the latest plugins from the Nessus website and verifying a successful download.

```
# /opt/nessus/bin/nessus-fetch --register XXXX-XXXX-XXXX-XXXX-XXXX
Your activation code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
# cat /opt/nessus/lib/nessus/plugins/plugin_feed_info.inc
PLUGIN_SET = "200912160934";
PLUGIN_FEED = "ProfessionalFeed (Direct)";
```

The file **`plugin_feed_info.inc`**, located in the directory **`/opt/nessus/lib/nessus/plugins/`**, will verify which plugin set and type of feed you have. Reviewing this file helps you ensure that you have the latest plugins available.

Start the Nessus Daemon

Nessus will not start until the scanner is registered and the plugins have been downloaded. SecurityCenter users that have entered the following command will not need to provide a registration code or download plugins:

```
# nessus-fetch --security-center
```

Start the Nessus service as root with the following command:

Linux and Solaris:

```
# /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:

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

nessusd (Nessus) 4.4.0 for Linux
(C) 1998 - 2008 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
#
```

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

Linux and Solaris:

```
# /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 `nessusd`
Red Hat	`# /sbin/service nessusd start`
Fedora Core	`# /sbin/service nessusd start`
SuSE	`# /etc/rc.d/nessusd start`
Debian	`# /etc/init.d/nessusd start`
FreeBSD	`# /usr/local/etc/rc.d/nessusd.sh start`
Solaris	`# /etc/init.d/nessusd start`
Ubuntu	`# /etc/init.d/nessusd start`

After starting the **`nessusd`** service, SecurityCenter users have completed the initial installation and configuration of their Nessus 4 scanner. If you are not using SecurityCenter to connect to **`nessusd`**, then continue with the following instructions 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 also abruptly stop any on-going scans:

```
# killall nessusd
```

It is recommended that you use the more graceful shutdown scripts instead:

Operating System	Command to Stop `nessusd`
Red Hat	`# /sbin/service nessusd stop`
Fedora Core	`# /sbin/service nessusd stop`

SuSE	`# /etc/rc.d/nessusd stop`
Debian	`# /etc/init.d/nessusd stop`
FreeBSD	`# /usr/local/etc/rc.d/nessusd.sh stop`
Solaris	`# /etc/init.d/nessusd stop`
Ubuntu	`# /etc/init.d/nessusd stop`

Nessusd Command Line Options

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

Option	Description
-c <config-file>	When starting the **nessusd** server, this option is used to specify the server-side **nessusd** configuration file to use. It allows for the use of an alternate configuration file instead of the standard **/opt/nessus/etc/nessus/nessusd.conf** (or **/usr/local/nessus/etc/nessus/nessusd.conf** for FreeBSD).
-a <address>	When starting the **nessusd** server, this option is used to tell the server to only listen to connections on the address <address> that is an IP, not a machine name. This option is useful if you are running **nessusd** on a gateway and if you do not want people on the outside to connect to your **nessusd.**
-S <ip[,ip2,...]>	When starting the **nessusd** server, force the source IP of the connections established by Nessus during scanning to <ip>. This option is only useful if you have a multi-homed machine with multiple public IP addresses that you would like to use instead of the default one. For this setup to work, the host running **nessusd** must have multiple NICs with these IP addresses set.
-p <port-number>	When starting the **nessusd** server, this option will tell the server to listen for client connections on the port <port-number> rather than listening on port 1241, which is the default.
-D	When starting the **nessusd** server, this option will make the server run in the background (daemon mode).
-v	Display the version number and exit.
-l	Display the plugin feed license information and exit.
-h	Show a summary of the commands and exit.

--ipv4-only	Only listen on IPv4 socket.
--ipv6-only	Only listen on IPv6 socket.
-q	Operate in "quiet" mode, suppressing all messages to **stdout**.
-R	Force a re-processing of the plugins.
-t	Check the timestamp of each plugin when starting up.
-K	Set a master password for the scanner.

If a master password is set, Nessus will safely cipher all policies and any credentials contained in them. 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,...]>]
```

Connecting with a Client

Once the installation has finished and the plugins have been updated and processed, the Nessus server is ready to be connected to by a client. Tenable supports access to the Nessus server through a native web server (port 8834 by default), the command line or the SecurityCenter interface (which is discussed in the section titled "Working with SecurityCenter"). Information on accessing the Web Server/user interface and command line operation is available in the "Nessus User Guide" located at http://www.tenable.com/documentation/.

The first time Nessus updates and processes the plugins, it may take several minutes. The web server will be available but not allow login until plugin processing has completed.

Updating Plugins

The following command is used to update the Nessus scanner with the most recent plugins:

Linux and Solaris:

```
# /opt/nessus/sbin/nessus-update-plugins
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessus-update-plugins
```

As new flaws are being discovered and published every day, new Nessus plugins are written on a daily basis. To keep your Nessus scanner up-to-date with the latest plugins, making your scans as accurate as possible, you need to update your plugins frequently.

How Often Should I Update Plugins?

In general, updating your Nessus plugins once a day is sufficient for most organizations. If you absolutely need the most current plugins and intend to update continuously throughout the day, updating no more than once every four hours is sufficient, as there is virtually no benefit in updating more frequently.

Updating Plugins Automatically

Since version 3.0, Nessus will fetch the newest plugins on a regular basis automatically. This is done with the **`auto_update`** option located in the **`nessusd.conf`** file. The default for this option is set to "yes". The option **`auto_update_delay`** determines how often Nessus will update its plugins in hours, which has a default value of 24. A minimum value of 4 hours can be used. The plugins update will take place the set number of hours after **`nessusd`** is started and will continue every N number of hours after that.

For this option to work properly, you must ensure that the scanner has a plugin feed activation code that is correctly registered. Use the following command to verify this:

Linux and Solaris:

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

FreeBSD:

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

Automatic plugin updates are only tried if:

- The **`auto_update`** option is set to yes in the **`nessusd.conf`** file;
- The plugin feed activation code has been registered via **`nessus-fetch`** from this scanner while directly connected to the internet; and
- The scanner is not being remotely managed by a Tenable SecurityCenter.

Note that an offline plugin feed registration will not enable Nessus to fetch the newest plugins automatically.

Scheduling Plugins Updates with Cron

If your organization has some technical or logistical reason for not permitting Nessus to update its plugins automatically, you can also set up a cron job to do this.

To configure your system to update plugins every night via cron, perform the following steps:

- Become root by typing **`su root`** (or **`sudo bash`** if you have sudo privileges).
- As root, type **`crontab -e`** to edit the crontab of the root user.
- Add the following line in your crontab:
  ```
  28 3 * * * /opt/nessus/sbin/nessus-update-plugins
  ```

The above configuration will call the command **`nessus-update-plugins`** every night at 3:28 am. Since **`nessus-update-plugins`** restarts **`nessusd`** automatically without interrupting the on-going scans, you do not need to do anything else.

When configuring cron for plugin updates, make sure that you **do not initiate the update at the top of the hour.** When setting up a schedule, pick a random minute after the top of the hour between :05 and :55 and initiate your download then.

> As of 4.4, Nessus can update plugins while scans are in progress. Once the update is complete, any subsequent scans will begin using the updated plugin set. A user does not have to log out of the web interface during this process.

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 and Solaris:

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

FreeBSD:

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

<table>
<tr><th>Platform</th><th>Removal Instructions</th></tr>
<tr><td colspan="2"><b>Red Hat ES 4 (32 bit), ES 5 (32 and 64 bit)</b></td></tr>
<tr><td><b>Remove Command</b></td><td>Determine the package name:
<code># rpm -qa | grep Nessus</code>
Use the output from the above command to remove the package:
<code># rpm -e <Package Name&gt;</code></td></tr>
<tr><td><b>Sample Output</b></td><td><code># rpm -qa | grep -i nessus</code>
<code>Nessus-4.4.0-es5</code>
<code># rpm -e Nessus-4.4.0-es5</code>
<code>#</code></td></tr>
</table>

Fedora Core 12, 13 and 14 (32 and 64 bit)	

Remove Command	Determine the package name:
	`# rpm -qa | grep Nessus`
	Use the output from the above command to remove the package:
	`# rpm -e <Package Name>`

SuSE 9.3 (32 bit), 10 (32 and 64 bit)	

Remove Command	Determine the package name:
	`# rpm -qa | grep Nessus`
	Use the output from the above command to remove the package:
	`# rpm -e <Package Name>`

Debian 5 (32 and 64 bit)	

Remove Command	Determine the package name:
	`# dpkg -l | grep -i nessus`
	Use the output from the above command to remove the package:
	`# dpkg -r <package name>`

Sample Output	`# dpkg -l | grep nessus`
	`ii  nessus         4.4.0      Version 4 of the Nessus Scanner`
	
	`# dpkg -r nessus`
	`#`

Ubuntu 8.04, 9.10, 10.04 and 10.10 (32 and 64 bit)	

Remove Command	Determine the package name:
	`# dpkg -l | grep -i nessus`
	Use the output from the above command to remove the package:
	`# dpkg -r <package name>`

Sample Output	`# dpkg -l | grep -i nessus`
	`ii  nessus        4.4.0      Version 4 of the Nessus Scanner`
	`#`

Solaris 10 (sparc)	

<table>
<tr><td>Remove Command</td><td>Stop the nessusd service:
/etc/init.d/nessusd stop
Determine the package name:
pkginfo | grep –i nessus
Remove the Nessus package:
pkgrm <package name></td></tr>
<tr><td>Sample Output</td><td>The following is example output for the previous command showing the Nessus package:
pkginfo | grep –i nessus
application TNBLnessus   The Nessus Network Vulnerability Scanner
pkgrm TNBLnessus
#</td></tr>
<tr><td colspan="2">FreeBSD 8 (32 and 64 bit)</td></tr>
<tr><td>Remove Command</td><td>Stop Nessus:
killall nessusd
Determine the package name:
pkg_info | grep -i nessus
Remove the Nessus package:
pkg_delete <package name></td></tr>
<tr><td>Sample Output</td><td># killall nessusd
pkg_info | grep -i nessus
Nessus-4.4.0   A powerful security scanner
pkg_delete Nessus-4.4.0
#</td></tr>
<tr><td colspan="2">Mac OS X</td></tr>
<tr><td>Remove Command</td><td>Launch a terminal window: From “Applications” click on “Utilities” and then click on either “Terminal” or “X11”. From the shell prompt, use the “sudo” command to run a root shell and remove the Nessus directories as follows:
$ sudo /bin/sh
Password:
ls -ld /Library/Nessus</td></tr>
</table>

	`# rm -rf /Library/Nessus`
	`# ls -ld /Library/Nessus`
	`# ls -ld /Applications/Nessus`
	`# rm -rf /Applications/Nessus`
	`# ls -ld /Applications/Nessus`
	`# ls -ld /Library/Receipts/Nessus*`
	`# rm -rf /Library/Receipts/Nessus*`
	`# ls -ld /Library/Receipts/Nessus*`
	`# exit`

Sample Output	`$ sudo /bin/sh`
	`Password:`
	`# ls -ld /Library/Nessus`
	`drwxr-xr-x  6 root  admin  204 Apr  6 15:12`
	`/Library/Nessus`
	`# rm -rf /Library/Nessus`
	`# ls -ld /Library/Nessus`
	`ls: /Library/Nessus: No such file or directory`
	`# ls -ld /Applications/Nessus`
	`drwxr-xr-x  4 root  admin  136 Apr  6 15:12`
	`/Applications/Nessus`
	`# rm -rf /Applications/Nessus`
	`# ls -ld /Applications/Nessus`
	`# ls -ld /Library/Receipts/Nessus*`
	`drwxrwxr-x  3 root  admin  102 Apr  6 15:11`
	`/Library/Receipts/Nessus Client.pkg`
	`drwxrwxr-x  3 root  admin  102 Apr  6 15:11`
	`/Library/Receipts/Nessus Server.pkg`
	`# rm -rf /Library/Receipts/Nessus*`
	`# ls -ld /Library/Receipts/Nessus*`
	`ls: /Library/Receipts/Nessus*: No such file or directory`
	`# exit`
	`$`

Notes	Do not attempt this process unless you are familiar with Unix shell commands. The "ls" commands are included to verify that the path name is typed correctly.

Windows

Upgrading

Upgrading from Nessus 4.0 - 4.0.x

When upgrading Nessus from a 4.x version to a newer 4.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.

Upgrading from Nessus 3.0 - 3.0.x

A direct upgrade from Nessus 3.0.x to Nessus 4.x is not supported, however, an upgrade to 3.2 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 4.

If you choose to upgrade to 3.2 as an interim step, please consult the Nessus 3.2 Installation Guide for more information.

Upgrading from Nessus 3.2 and later

If you are using Nessus 3.2 or later, you can download the Nessus 4 package and install it without uninstalling the existing version. All previous vulnerability scan reports and policies will be saved and will not be deleted. After the new version of Nessus is installed, they will still be available for viewing and exporting.

Installation

Downloading Nessus

The latest version of Nessus is available at http://www.nessus.org/download/. Nessus 4.4 is available for Windows XP, Server 2003, Server 2008, Vista and Windows 7.

Nessus distribution file sizes and names vary slightly from release to release, but are approximately 12 MB in size.

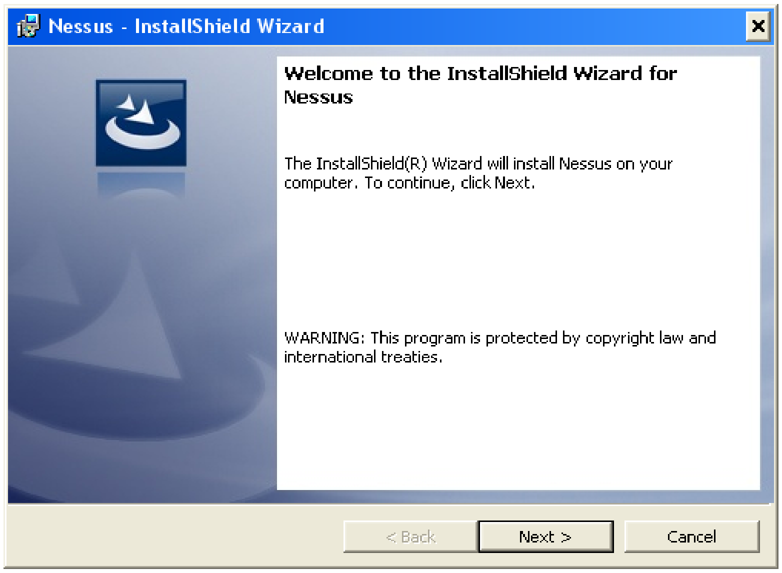
Installing

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".

Installation Questions

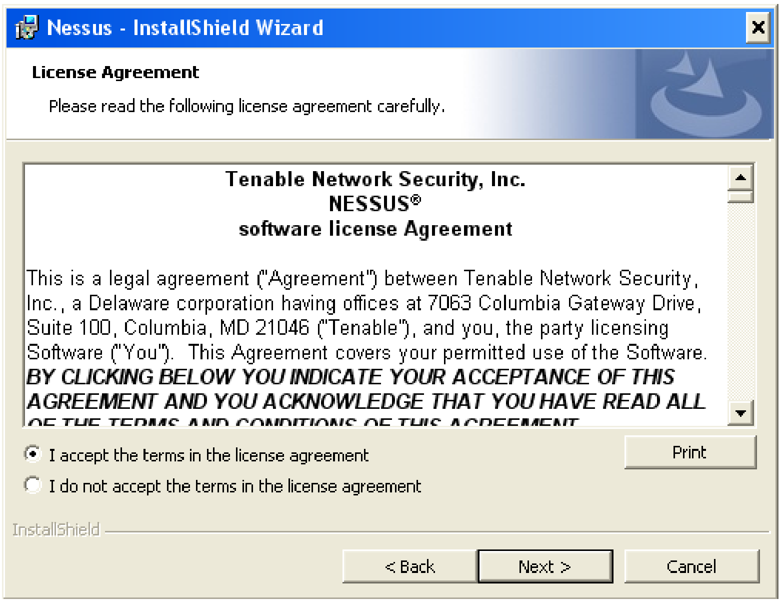


Welcome to the InstallShield Wizard for Nessus

The InstallShield(R) Wizard will install Nessus on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



License Agreement

Please read the following license agreement carefully.

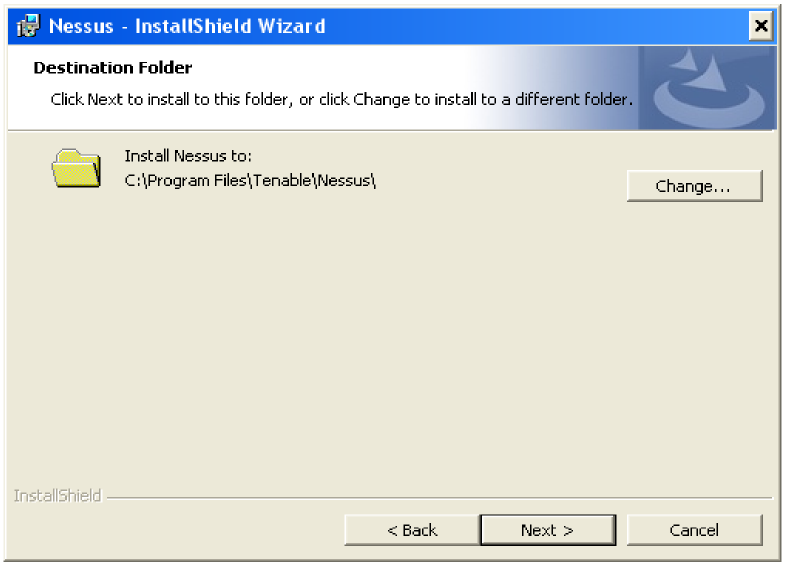
Tenable Network Security, Inc.
NESSUS®
software license Agreement

This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers your permitted use of the Software. ***BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT***

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

After agreeing, you can configure where Nessus will be installed:



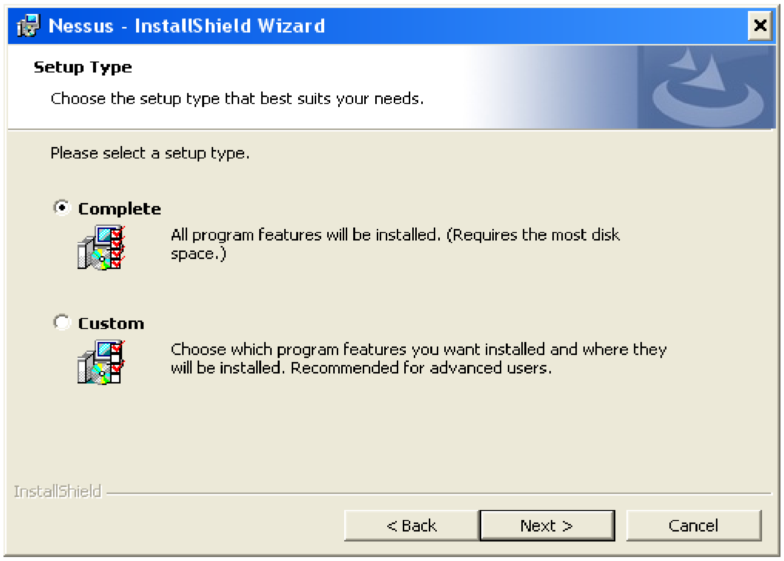
Nessus - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Nessus to:
C:\Program Files\Tenable\Nessus\

When prompted to select the “Setup Type”, select “Complete”.



Nessus - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

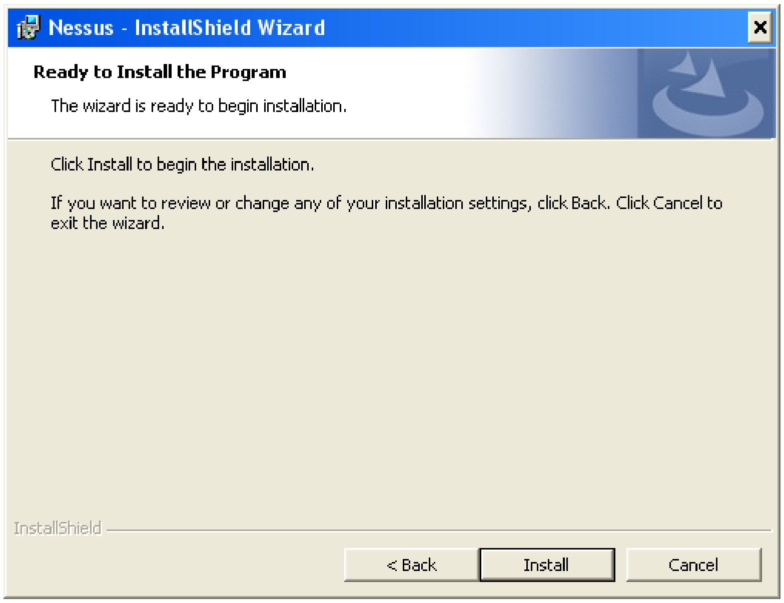
● **Complete**

All program features will be installed. (Requires the most disk space.)

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

You will be prompted to confirm the installation:



Nessus - InstallShield Wizard

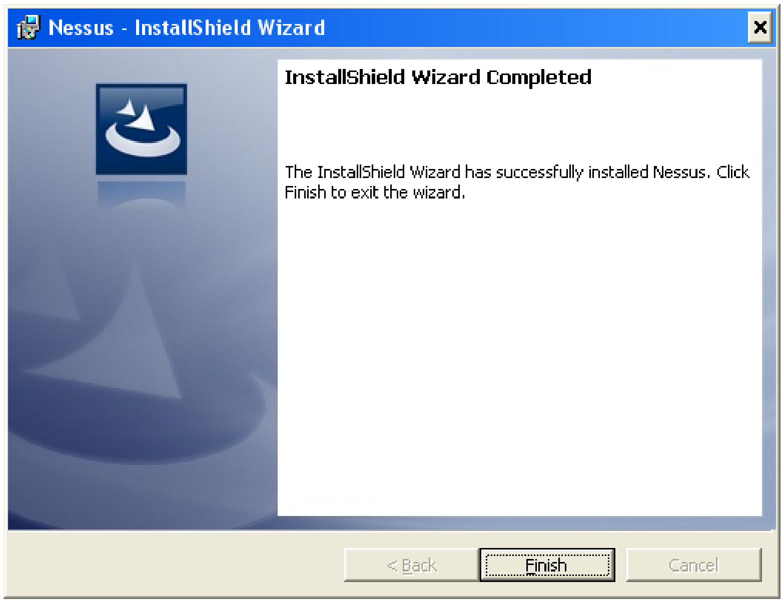
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Once installation is complete, click on "Finish".



Nessus - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Nessus. Click Finish to exit the wizard.

Nessus Major Directories

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

> If the required disk space to maintain logs exists outside of the **/opt** file system, mount the desired target directory using “**mount --bind <olddir> <newdir>**” or the appropriate syntax for your distribution. Symbolic links cannot be used to achieve this.

Configuration

The section describes how to configure the Nessus 4 server on a Windows system.

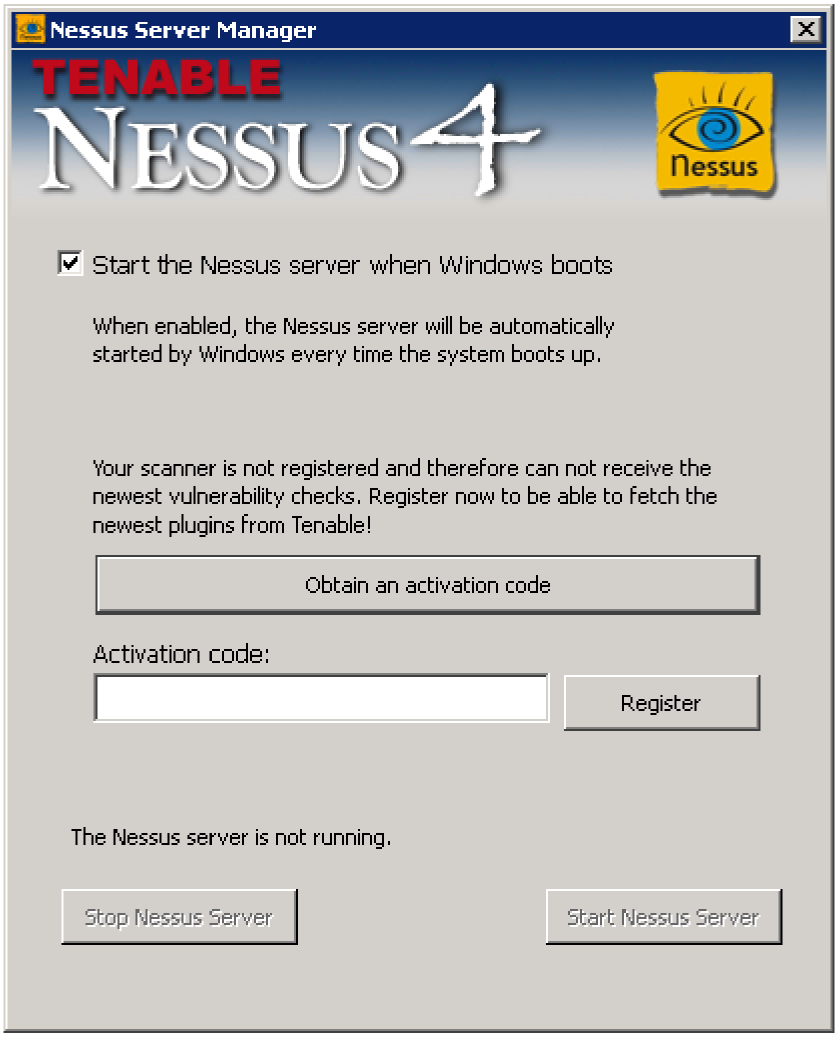
Nessus Server Manager

To start, stop and configure the Nessus server, use the Nessus Server Manager.

This interface allows you to:

- Register your Nessus Server to nessus.org in order to receive updated plugins
- Perform a plugin update
- Configure whether or not the Nessus server starts whenever Windows starts
- Manage Nessus users
- Start or Stop the Nessus Server

Navigate to the Nessus Server Manager via the Start menu as follows: *Start -> Programs -> Tenable Network Security -> Nessus -> Nessus Server Manager*. This will load the Nessus Server Manager (nessussvrmanager.exe) as shown below:



☑ Start the Nessus server when Windows boots

When enabled, the Nessus server will be automatically started by Windows every time the system boots up.

Your scanner is not registered and therefore can not receive the newest vulnerability checks. Register now to be able to fetch the newest plugins from Tenable!

Activation code:

The Nessus server is not running.

The “Start Nessus Server” button will remain unavailable until the Nessus Server has been registered.

Changing Default Nessus Port

To change the port that the Nessus Server listens on, edit the **nessusd.conf** file located in **C:\Program Files\Tenable\Nessus\conf\**. The following configuration directives can be edited to alter the Nessus service listener and Web Server preferences:

```
# Port to listen to (old NTP protocol). Used for pre 4.2 NessusClient
# connections :
listen_port = 1241

# Port for the Nessus Web Server to listen to (new XMLRPC protocol) :
xmlrpc_listen_port = 8834
```

After changing these values, stop the Nessus service via the Nessus Server Manager and restart it.

The legacy client use via the NTP protocol is only available to ProfessionalFeed customers.

Registering your Nessus Installation

If you are using the Tenable SecurityCenter, the Activation Code and plugin updates are managed from SecurityCenter. In order to communicate with SecurityCenter, Nessus needs to be started, 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), run the following command from the MS-DOS prompt:

```
C:\Program Files\Tenable\Nessus>nessus-fetch --security-center
```

Immediately after running the "**nessus-fetch**" command above, use the Windows service manager to start the Nessus server. The Nessus server can now be added to the SecurityCenter via the SecurityCenter web interface. Please refer to the SecurityCenter documentation for the configuration of a centralized plugin feed for multiple Nessus scanners.

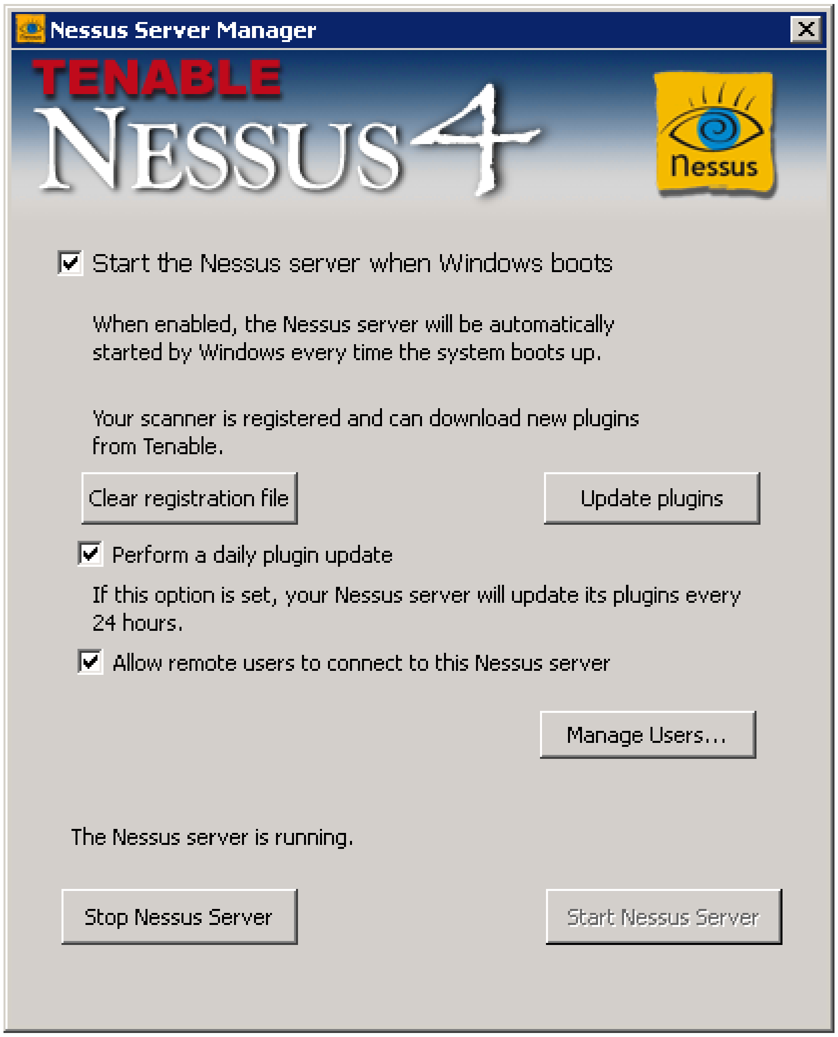
After installation, the first thing to do is to register your Nessus Server. Registering your server provides access to the newest plugins from nessus.org and ensures your audits are up-to-date.

After the initial registration, Nessus will download and compile the plugins obtained from plugins.nessus.org in the background. The first time this occurs, it may take up to 10 minutes before the Nessus server is ready. Until the plugins are downloaded and compiled, the web server interface will not be available. The activation code is **not** case sensitive.

To register Nessus, click on "Obtain an activation code", which will take you to http://www.nessus.org/plugins/?view=register-info. Here you can obtain a ProfessionalFeed or HomeFeed. A ProfessionalFeed is required for commercial use and offers plugin updates, customer support, configuration audits, virtual appliance and more. A HomeFeed is required for home users and not licensed for professional or commercial use. Once the required information is provided and processed, you will receive an email that contains an Activation Code that entitles you to either the ProfessionalFeed or the HomeFeed of plugins. Enter it in the appropriate field and click on the "Register" button. Note that you will be prompted to enter the administrator username and password. Once the Nessus Server Manager authorizes the Feed Activation Code, an update of the Nessus plugins will begin. This process may take several minutes, as the initial plugin download is a large file.

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.

Once registered, the Nessus Server Manager interface displays the following:



☑ Start the Nessus server when Windows boots

When enabled, the Nessus server will be automatically started by Windows every time the system boots up.

Your scanner is registered and can download new plugins from Tenable.

☑ Perform a daily plugin update

If this option is set, your Nessus server will update its plugins every 24 hours.

☑ Allow remote users to connect to this Nessus server

The Nessus server is running.

<u>Resetting Activation Codes</u>

At some point, you may find the need to change the Activation Codes (e.g., upgrading from a HomeFeed to a ProfessionalFeed). This can be accomplished by using the "Clear registration file" button on the Nessus Server Manager interface. After confirmation, this will unregister your copy of Nessus until a new Activation Code is obtained and the product is registered again.

Create and Manage Nessus Users

<u>Allowing Remote Connections</u>

If you intend for the Nessus scanner to be used remotely (such as with SecurityCenter), you must select "**Allow remote users to connect to this server**".

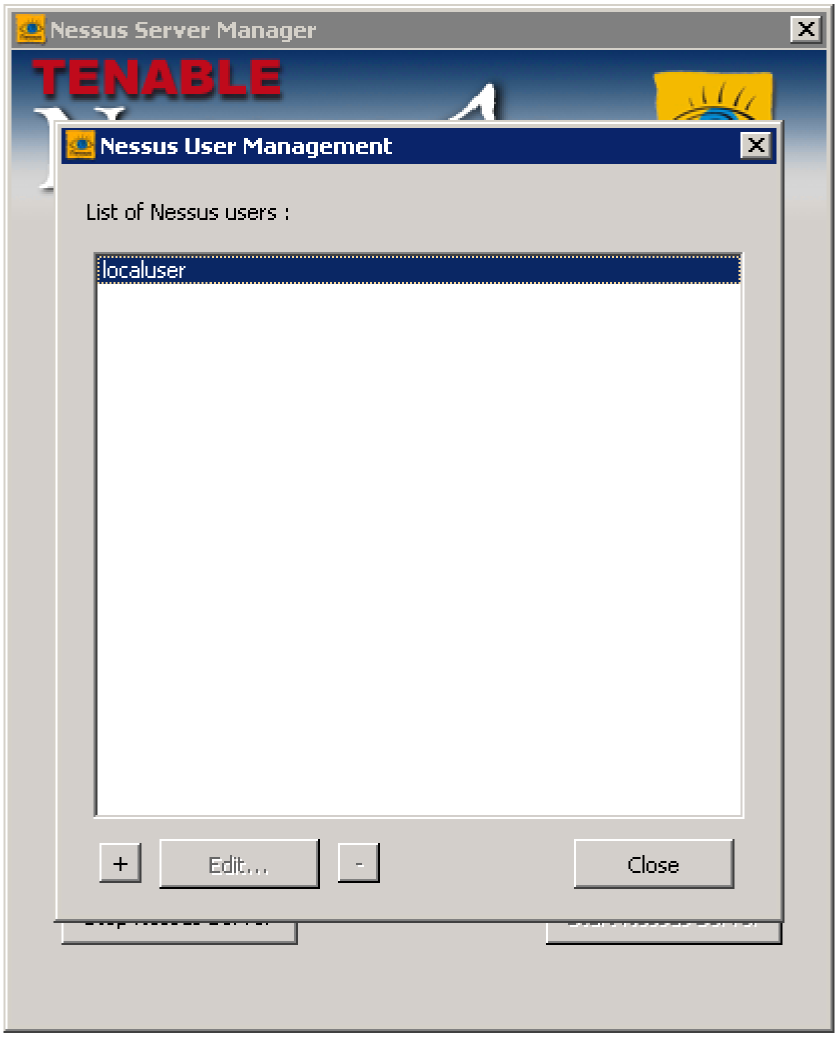
If this box is unchecked, the Nessus Server will only be available to local clients.

If this box is checked, the Nessus Server can be accessed using either clients installed on the localhost, clients installed on a remote host or the SecurityCenter interface (which is discussed later in this document in the section titled "Working with SecurityCenter").

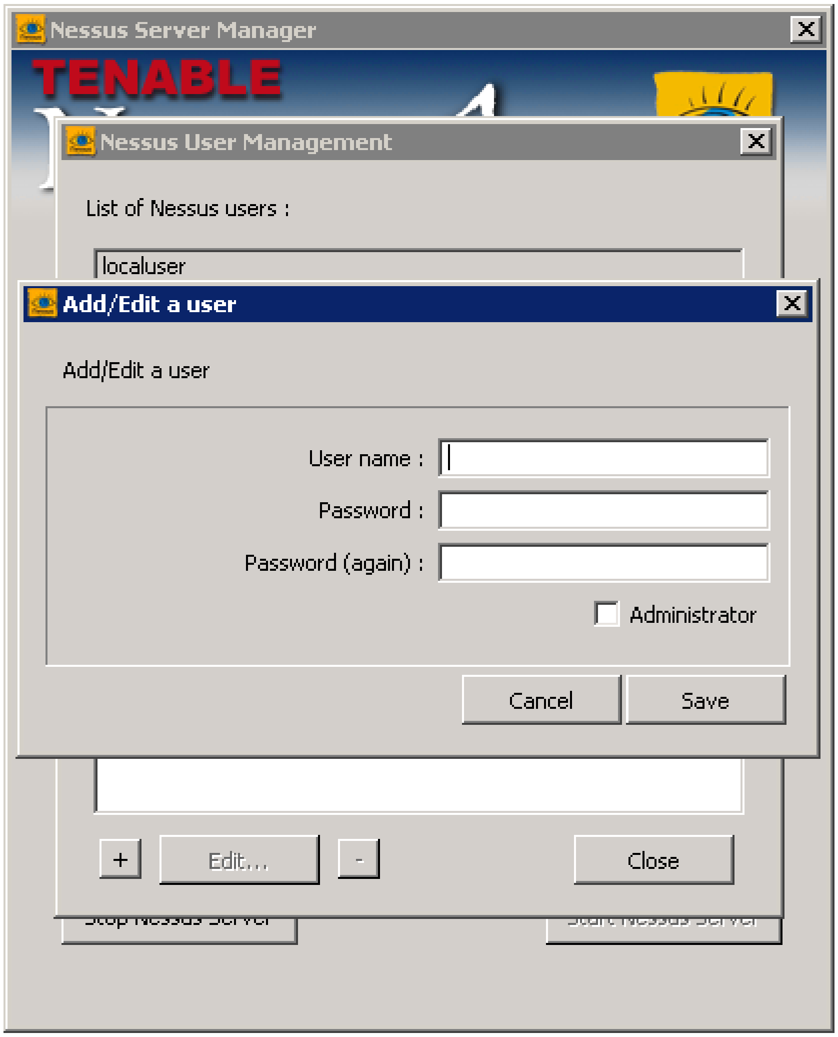
Information on Nessus clients is available in the "Nessus 4.4 User Guide".

Adding User Accounts

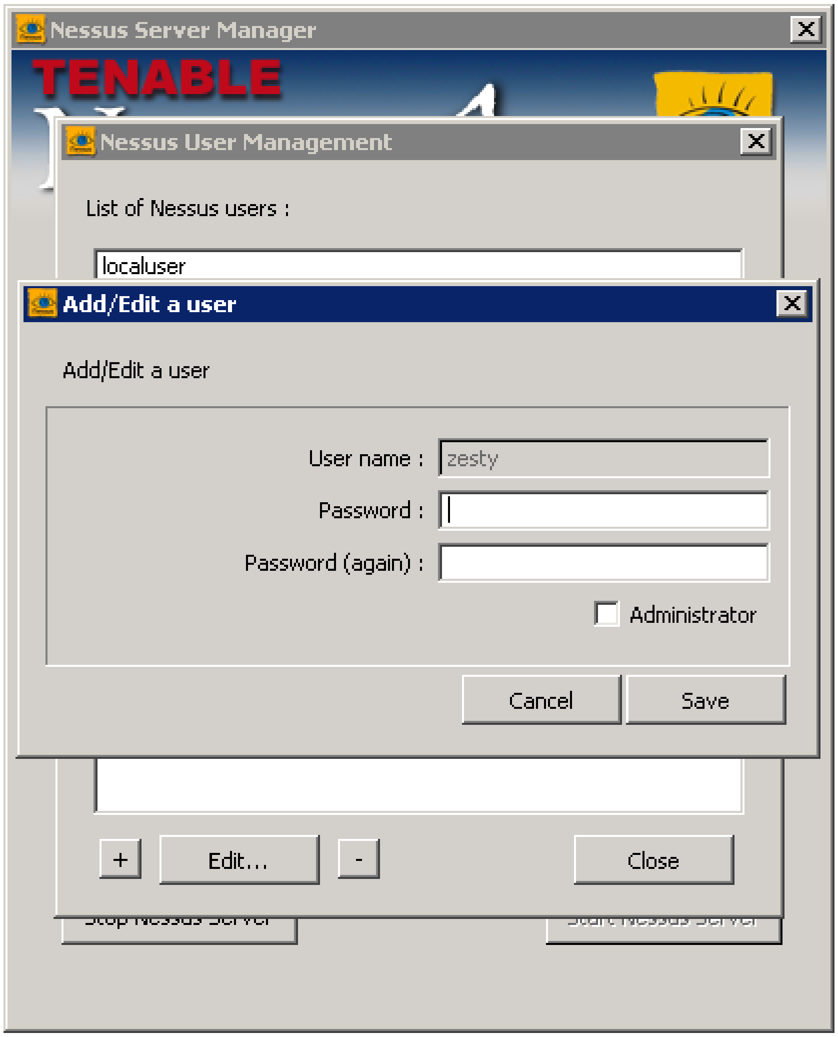
Clicking on "Manage Users…" allows you to create and manage accounts for the Nessus server:



To create a user, click on the "+" button and enter a new username and password. Select the "Administrator" checkbox if the user will be an administrator:



Selecting a name from the list and clicking the "Edit…" button will allow you to change the user's password (see screenshot below). Clicking on the "-" button with a user selected will delete the user after confirmation.



List of Nessus users :

localuser

Add/Edit a user

User name : zesty

Password :

Password (again) :

☐ Administrator

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.

Please note that Nessus uses an internal administrative account for local communication between the Nessus GUI and the Tenable Nessus Service. This account cannot be used for remote connection from a Nessus client.

Host-Based Firewalls

If your Nessus Server is configured on a host with a "personal" firewall such as Zone Alarm, Sygate, Windows XP 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 port 8834 choose the "**Exceptions**" tab and then add port "8834" to the list.

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

Launch the Nessus Daemon

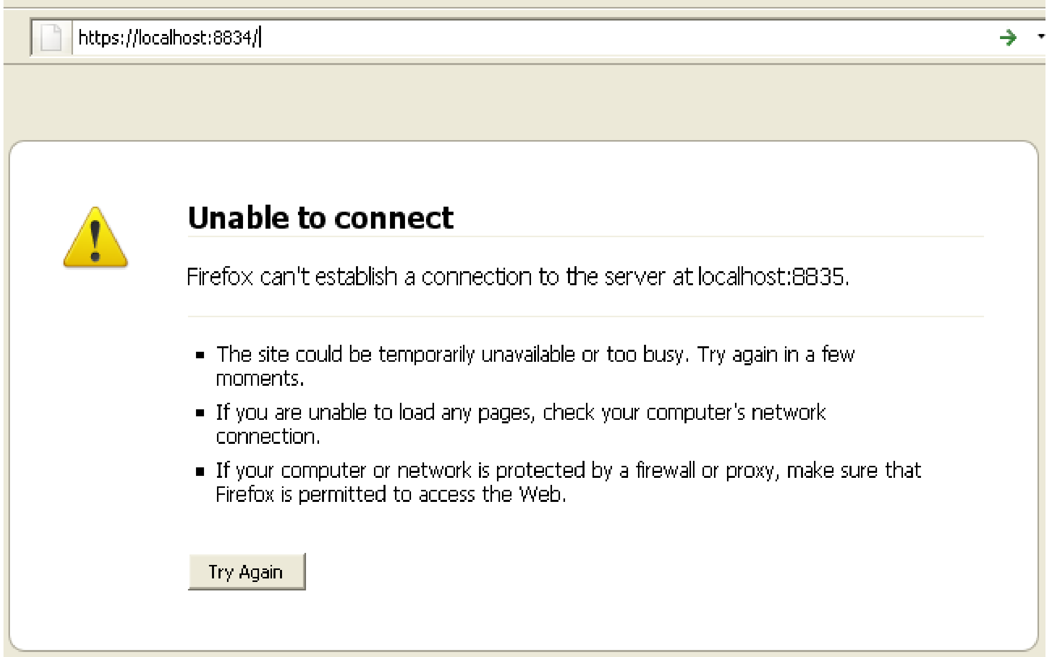
To start the Nessus daemon, click on the button "**Start Nessus Server**" in the Nessus Server Manager.

If you want Nessus to be started automatically, then click on the checkbox "**Start the Nessus Server when Windows boots**".

Nessus is installed as the "Tenable Nessus" service under Windows and configured to automatically start if the system reboots. This is configured using the "Start the Nessus Server when Windows boots" check box.

After starting the **nessusd** service, SecurityCenter users have completed the initial installation and configuration of their Nessus 4 scanner and can continue to the section "Working with SecurityCenter".

If the Nessus daemon is not running or the user interface is not available, your web browser will give an error message indicating it could not connect:



https://localhost:8834/

Unable to connect

Firefox can't establish a connection to the server at localhost:8835.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

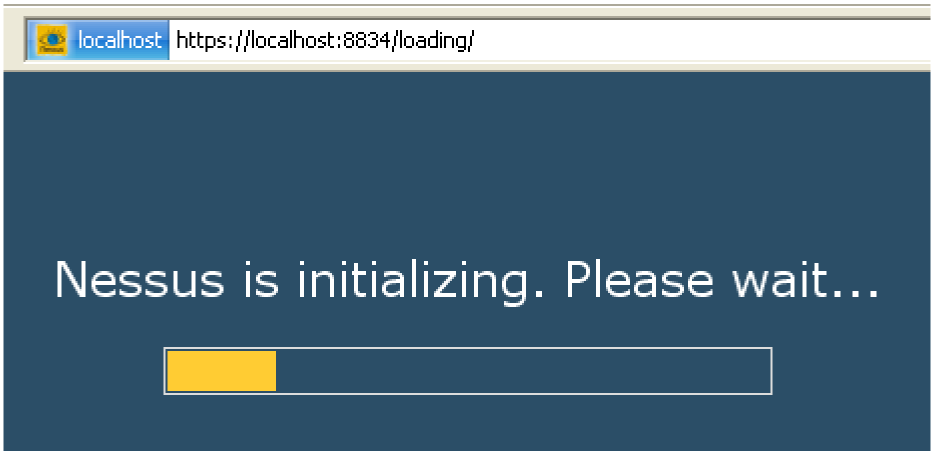
The Nessus Server will run on localhost (127.0.0.1) and listen on port 1241 for legacy clients by default. To verify that Nessus is listening on port 1241, from the Windows command line use the "**netstat -an | findstr 1241**" command as shown below:

```
C:\Documents and Settings\admin>netstat -an | findstr 1241
  TCP    0.0.0.0:1241           0.0.0.0:0              LISTENING
```

Notice that the output contains "0.0.0.0:1241", which means a server is listening on that port. This can be used to verify the Web Server (user interface) is available by changing "1241" to "8834" in the command above.

Note that the Nessus Service is started automatically only after the installation **and** plugin update has occurred.

The first time Nessus updates and processes the plugins, it may take several minutes. The web server will show a "Nessus is initializing." message and will reload when ready:

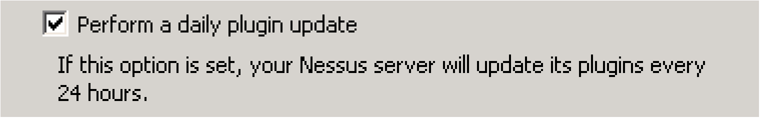


Nessus is initializing. Please wait...

Updating Plugins

Nessus has tens of thousands of plugins (or scripts) that test for network and host vulnerabilities. New vulnerabilities are regularly being discovered and new plugins are developed to detect these vulnerabilities. To keep your Nessus scanner up-to-date with the latest plugins, making your scans as accurate as possible, you need to update your plugins daily.

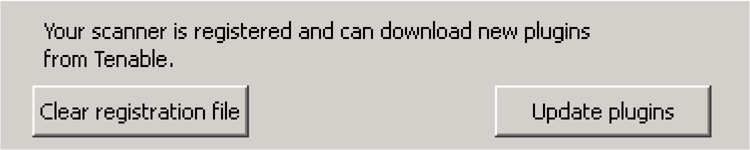
The "**Perform a daily plugin update**" option configures the Nessus server to automatically update plugins from Tenable every 24 hours. This occurs roughly at the time of day that you started Nessus.



☑ Perform a daily plugin update

If this option is set, your Nessus server will update its plugins every 24 hours.

You can force a plugin update by clicking on the "**Update Plugins**" button as shown below:



Your scanner is registered and can download new plugins from Tenable.

How Often Should I Update Plugins?

In general, updating your Nessus plugins once a day is sufficient for most organizations. If you absolutely need the most current plugins and intend to update continuously throughout the day, then updating no more than once every four hours is sufficient as there is virtually no benefit in updating more than this.

Updating Plugins through Web Proxies

Nessus on Windows supports product registration and plugins updates through web proxies that require basic authentication. Proxy settings can be found in **`C:\Program Files\Tenable\Nessus\conf\nessus-fetch.rc`** file. There are four relevant lines that control proxy based connectivity. Below are the lines with example syntax:

```
proxy=myproxy.example.com
proxy_port=8080
proxy_username=juser
proxy_password=guineapig
```

For the "proxy" directive, a DNS host name or IP address may be used. Only one proxy may be specified in the `nessus-fetch.rc` file. In addition, a `user_agent` directive may be specified if required, which directs Nessus to use a custom HTTP user agent.

> As of Nessus 4.2, installations on Microsoft Windows support proxy authentication including NTLM.

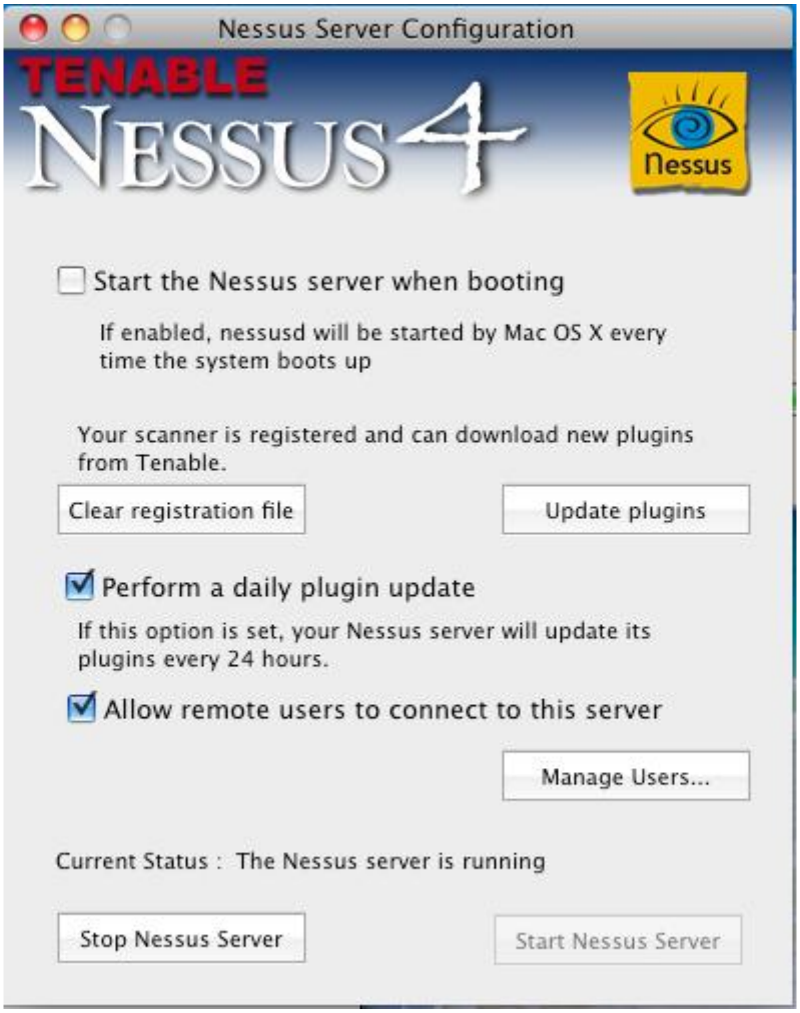
Removing Nessus

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.

Mac OS X

Upgrading

Upgrading from an older version of Nessus is similar to doing a fresh install. However, you will need to stop and restart the Nessus server at the end of the installation. Download the file **`Nessus-4.x.x.dmg.gz`**, and then double click on it to unzip it. Double click on the **`Nessus-4.x.x.dmg`** file, which will mount the disk image and make it appear under "Devices" in "Finder". Once the volume "Nessus 4" appears in "Finder", double click on the file **`Nessus 4`**. When the installation is complete, go to **`/Applications/Nessus/`** and run the Nessus Server Manager. To complete the upgrade you will need to click the "Update Plugins" button:



Nessus Server Configuration

☐ Start the Nessus server when booting

If enabled, nessusd will be started by Mac OS X every time the system boots up

Your scanner is registered and can download new plugins from Tenable.

☑ Perform a daily plugin update

If this option is set, your Nessus server will update its plugins every 24 hours.

☑ Allow remote users to connect to this server

Current Status : The Nessus server is running

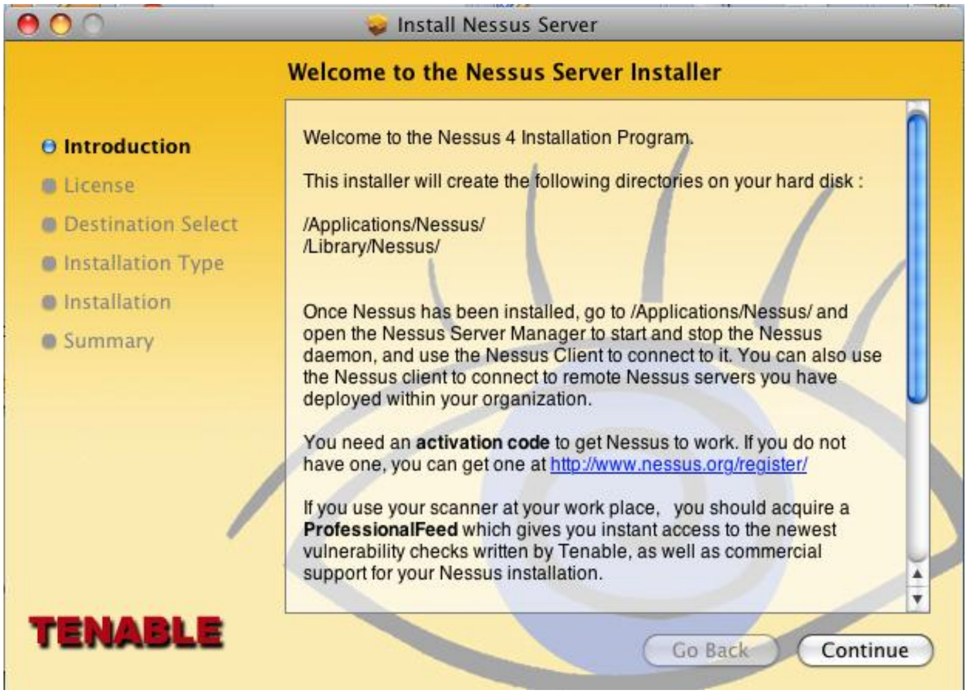
Installation

The latest version of Nessus is available from http://www.nessus.org/download/. Nessus is available for Mac OS X 10.4 and 10.5.

To install Nessus on Mac OS X, you need to download the file **`Nessus-4.x.x.dmg.gz`**, and then double click on it to unzip it. Double click on the **`Nessus-4.x.x.dmg`** file, which will mount the disk image and make it appear under "Devices" in "Finder". Once the volume "Nessus 4" appears in "Finder", double click on the file **`Nessus 4`** as shown below:

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

The installation will be displayed as follows:



Welcome to the Nessus Server Installer

Welcome to the Nessus 4 Installation Program.

This installer will create the following directories on your hard disk :

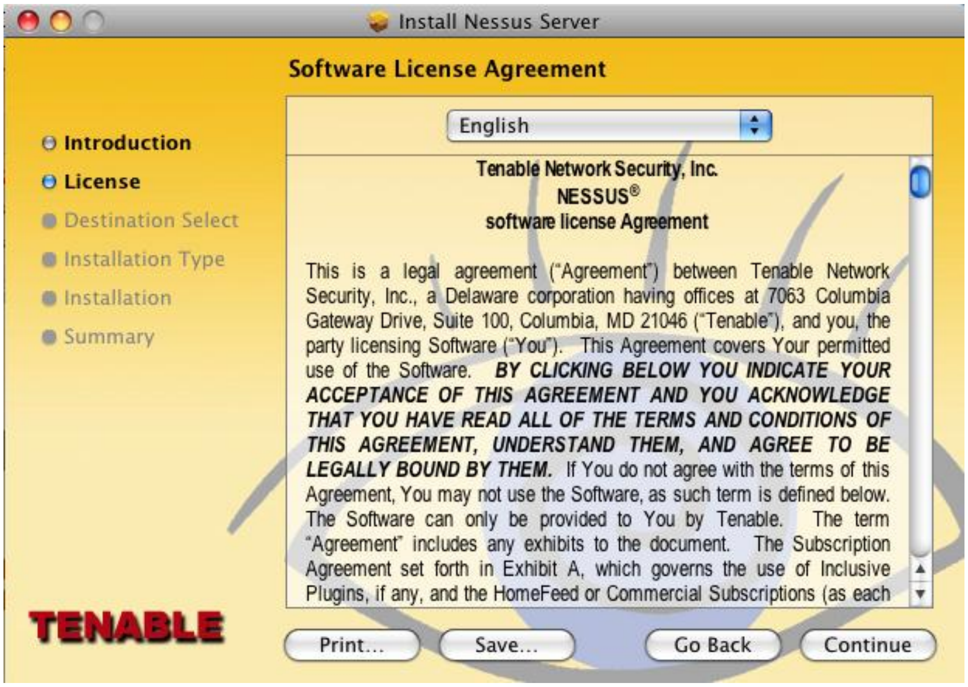
/Applications/Nessus/
/Library/Nessus/

Once Nessus has been installed, go to /Applications/Nessus/ and open the Nessus Server Manager to start and stop the Nessus daemon, and use the Nessus Client to connect to it. You can also use the Nessus client to connect to remote Nessus servers you have deployed within your organization.

You need an **activation code** to get Nessus to work. If you do not have one, you can get one at http://www.nessus.org/register/

If you use your scanner at your work place, you should acquire a **ProfessionalFeed** which gives you instant access to the newest vulnerability checks written by Tenable, as well as commercial support for your Nessus installation.

Click on "Continue" and a dialog box will be displayed requiring that you accept the license terms before continuing:

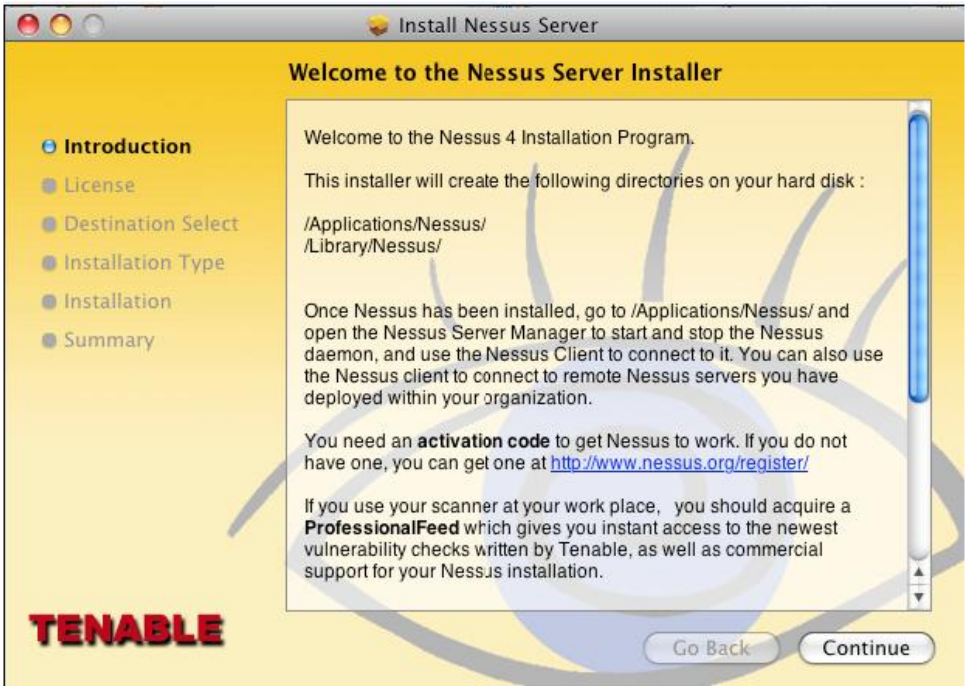


Software License Agreement

Tenable Network Security, Inc.
NESSUS®
software license Agreement

This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers Your permitted use of the Software. ***BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM.*** If You do not agree with the terms of this Agreement, You may not use the Software, as such term is defined below. The Software can only be provided to You by Tenable. The term "Agreement" includes any exhibits to the document. The Subscription Agreement set forth in Exhibit A, which governs the use of Inclusive Plugins, if any, and the HomeFeed or Commercial Subscriptions (as each

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



Welcome to the Nessus 4 Installation Program.

This installer will create the following directories on your hard disk :

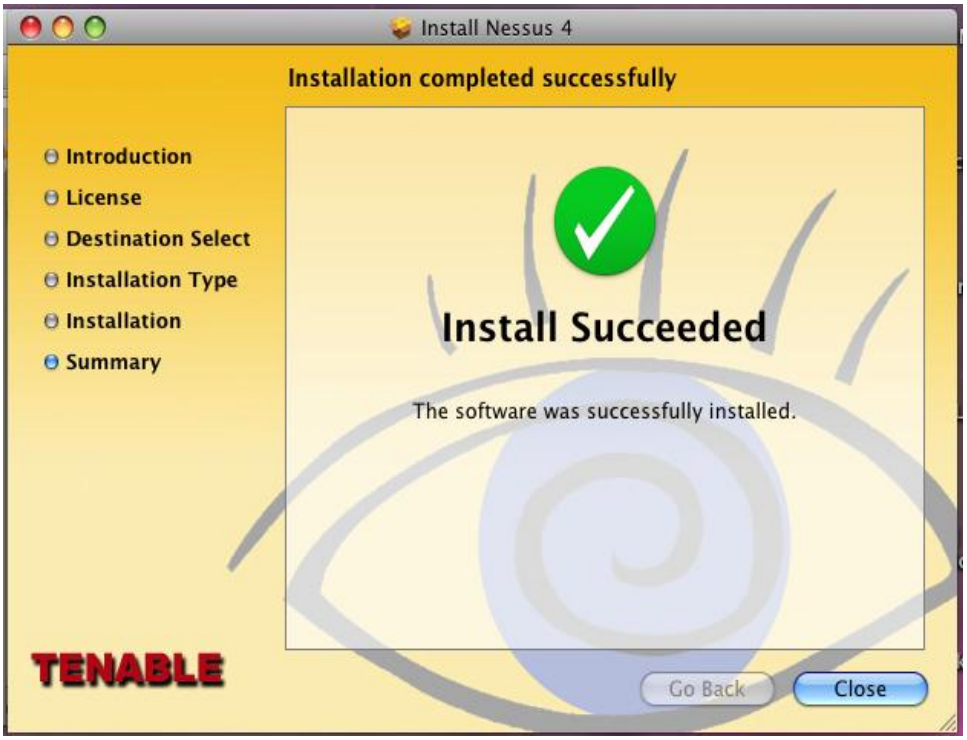
/Applications/Nessus/
/Library/Nessus/

Once Nessus has been installed, go to /Applications/Nessus/ and open the Nessus Server Manager to start and stop the Nessus daemon, and use the Nessus Client to connect to it. You can also use the Nessus client to connect to remote Nessus servers you have deployed within your organization.

You need an **activation code** to get Nessus to work. If you do not have one, you can get one at http://www.nessus.org/register/

If you use your scanner at your work place, you should acquire a **ProfessionalFeed** which gives you instant access to the newest vulnerability checks written by Tenable, as well as commercial support for your Nessus installation.

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:



Install Succeeded

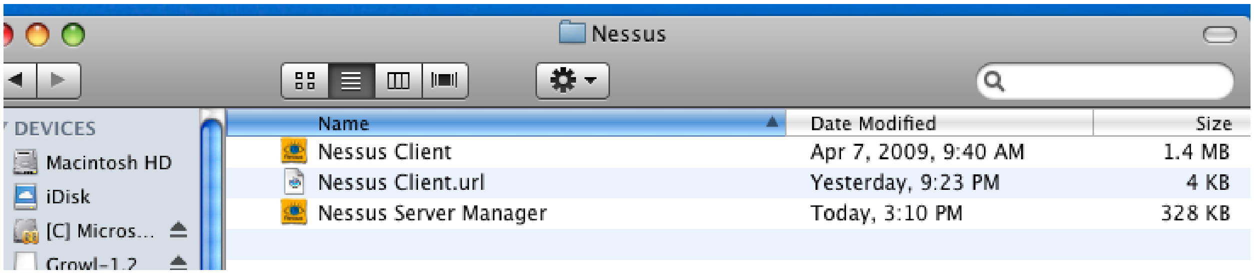
The software was successfully installed.

Configuration

The section describes how to configure the Nessus 4 server on a Mac OS X system.

Nessus Server Manager

To start, stop, and configure the Nessus server, use the program Nessus Server Manager located under **`/Applications/Nessus/`**:



Name	Date Modified	Size
Nessus Client	Apr 7, 2009, 9:40 AM	1.4 MB
Nessus Client.url	Yesterday, 9:23 PM	4 KB
Nessus Server Manager	Today, 3:10 PM	328 KB

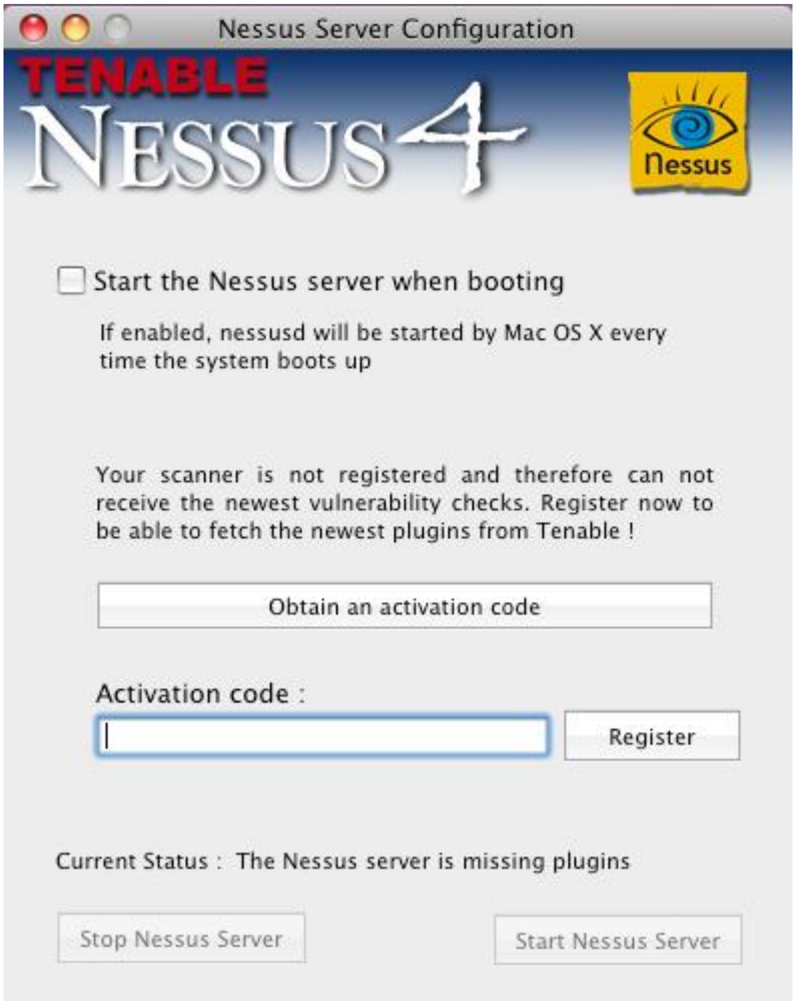
> Note that if you have upgraded Nessus, the Nessus Client will still be listed in the Nessus folder. It is no longer necessary to use the Nessus Client to manage Nessus scans and it can be removed, if desired. The "Nessus Client.url" is a link to manage Nessus through your web browser. New installations will not include the Nessus Client.

The Nessus Server Manager interface allows you to:

- Register your Nessus Server to nessus.org to receive updated plugins
- Perform a plugin update
- Configure whether or not the Nessus server will start whenever Mac OS X starts
- Manage Nessus users
- Start or Stop the Nessus Server

> Whenever you start "Nessus Server Manager", you will be prompted for an administrator user name and password since interacting with the Nessus server requires root privileges.

To start the Nessus Server Manager, double-click on the icon and an initial screen will be displayed as follows:



□ Start the Nessus server when booting

If enabled, nessusd will be started by Mac OS X every time the system boots up

Your scanner is not registered and therefore can not receive the newest vulnerability checks. Register now to be able to fetch the newest plugins from Tenable !

Activation code :

Current Status : The Nessus server is missing plugins

The "Start Nessus Server" button will remain unavailable until the Nessus Server has been registered.

Registering your Nessus Installation

If you are using the Tenable SecurityCenter, the Activation Code and plugin updates are managed from SecurityCenter. In order to communicate with SecurityCenter, Nessus needs to be started, 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), run the following command from a root shell prompt:

```
# /Library/Nessus/run/bin/nessus-fetch --security-center
```

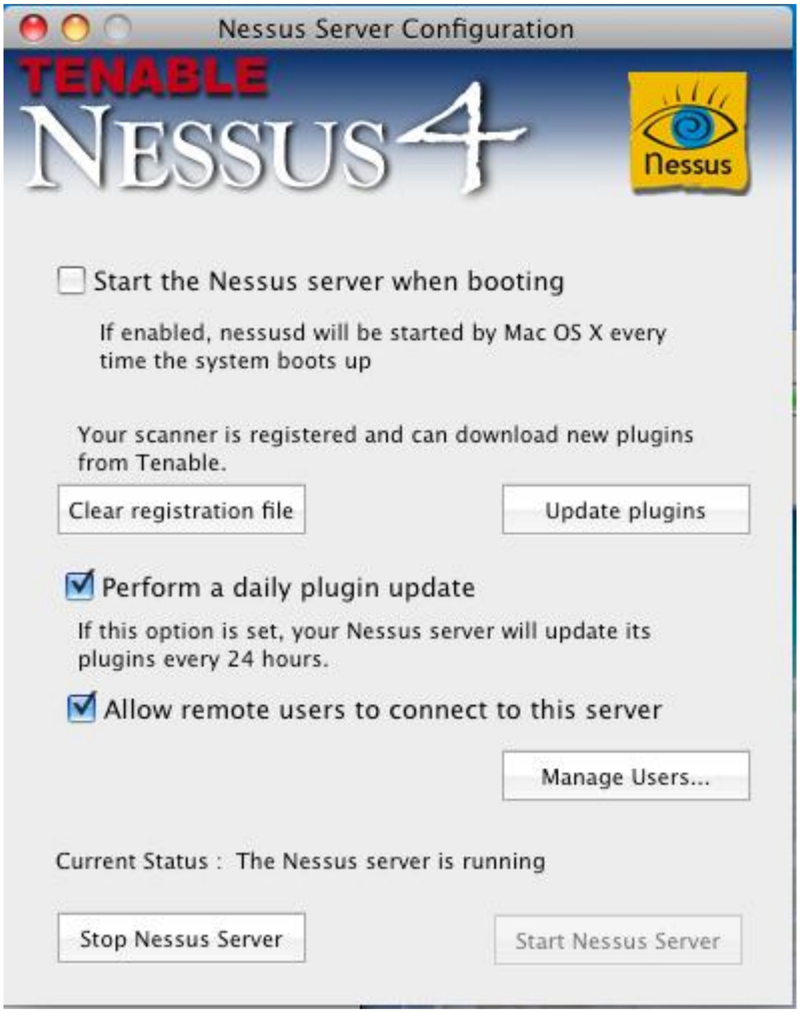
Immediately after running the "**nessus-fetch**" command above, use the applicable command to start the Nessus server. The Nessus server can now be added to the SecurityCenter via the SecurityCenter web interface. Please refer to the SecurityCenter documentation for the configuration of a centralized plugin feed for multiple Nessus scanners.

After installation, the first thing to do is to register your Nessus Server. Registering your server provides access to the newest plugins from nessus.org and ensures your audits are up-to-date.

To register Nessus, click on "Obtain an activation code", which will take you to http://www.nessus.org/plugins/?view=register-info. Here you can obtain a ProfessionalFeed or HomeFeed. A ProfessionalFeed is required for commercial use and offers plugin updates, customer support, configuration audits, virtual appliance and more. A HomeFeed is required for home users and not licensed for professional or commercial use. Once the required information is provided and processed, you will receive an email that contains an Activation Code that entitles you to either the ProfessionalFeed or the HomeFeed of plugins., Enter it in the appropriate field and click on the "Register" button. Note that you will be prompted to enter the administrator username and password. Once the Nessus Server Manager authorizes the Feed Activation Code, an update of the Nessus plugins will begin. This process may take several minutes as the initial plugin download is a large file.

⚠ 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.

Once registered, the Nessus Server Manager interface displays the following:



□ Start the Nessus server when booting

If enabled, nessusd will be started by Mac OS X every time the system boots up

Your scanner is registered and can download new plugins from Tenable.

☑ Perform a daily plugin update

If this option is set, your Nessus server will update its plugins every 24 hours.

☑ Allow remote users to connect to this server

Current Status : The Nessus server is running

Resetting Activation Codes

At some point, you may find the need to change the Activation Code (e.g., upgrading from a HomeFeed to a ProfessionalFeed). This can be accomplished by using the "Clear registration file" button on the Nessus Server Manager interface. After confirmation, this will unregister your copy of Nessus until a new Activation Code is obtained and the product is registered again.

Create and Manage Nessus Users

Allowing Remote Connections

If you intend your Nessus scanner to be used remotely (such as with SecurityCenter), you need to select "**Allow remote users to connect to this server**".

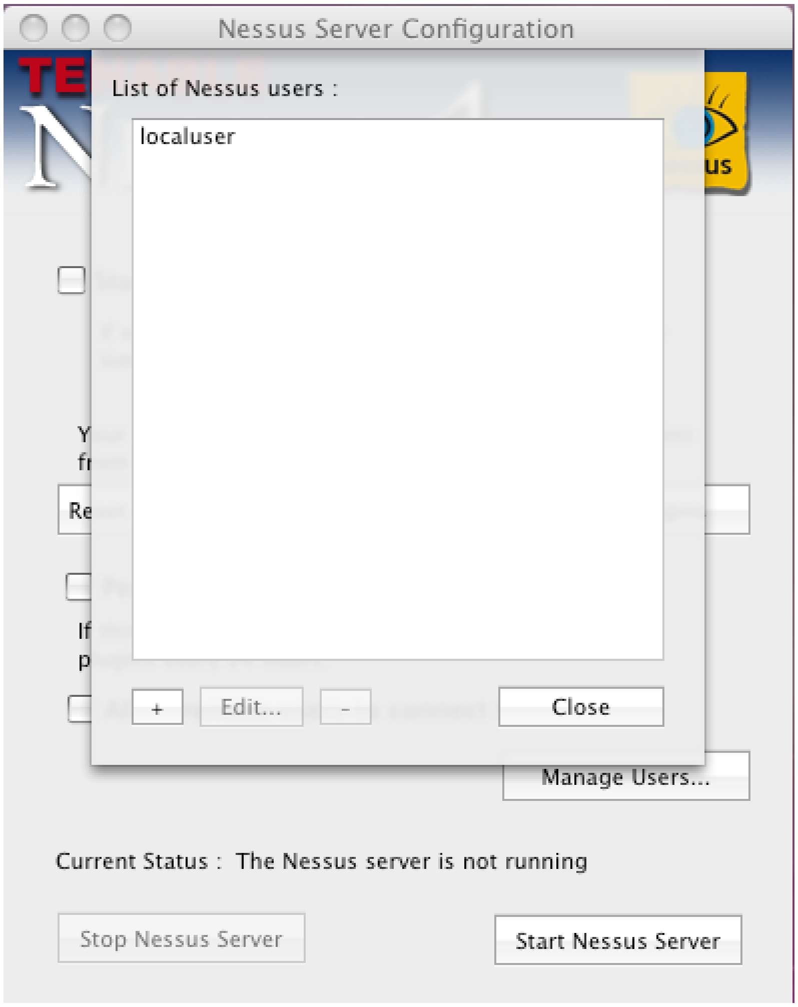
If this box is unchecked, the Nessus Server will only be available to the local Nessus client.

If this box is checked, the Nessus Server can be accessed using either clients installed on the localhost, clients installed on a remote host or the SecurityCenter interface (which is discussed later in this document in the section titled "Working with SecurityCenter").

Information on Nessus clients is available in the "Nessus 4.4 User Guide".

Adding User Accounts

Clicking on "Manage Users…" allows you to create and manage accounts for the Nessus server:



Unless you are experienced, do not edit or delete the user "localuser", as it will break the `Local Connection` server for Nessus .

To create a user, click on the "+" button and enter a new username and password. Select the "Administrator" checkbox if the user will be an administrator. Selecting a name from the list and clicking the "Edit…" button will allow you to change the user's password (see screenshot below). Clicking the "-" button with a user selected will delete the user after confirmation.

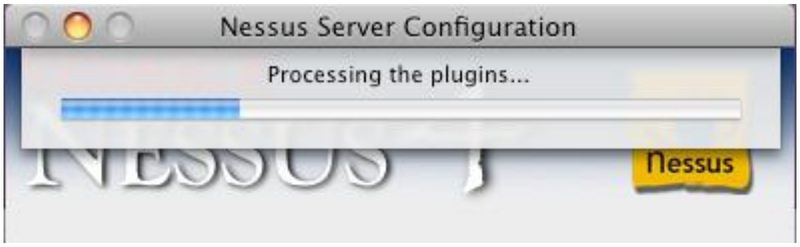
You cannot rename a user. If you want to change the name of a user, delete the user and create a new user with the appropriate login name.

Launch the Nessus Daemon

To start the Nessus daemon, click on the button "**Start Nessus Server**" in the Nessus Server Manager.

If you want Nessus to be started automatically, then click on the checkbox "**Start the Nessus Server at bootup**".

When the **nessusd** service is started, it will take a few minutes to process the plugins as shown:



Nessus Server Configuration

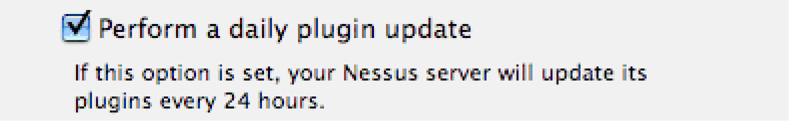
Processing the plugins...

After starting the **nessusd** service, SecurityCenter users have completed the initial installation and configuration of their Nessus 4 scanner and can continue to the section "Working with SecurityCenter".

Updating Plugins

Nessus has tens of thousands of plugins (or scripts) that test for network and host vulnerabilities. New vulnerabilities are regularly being discovered and new plugins are developed to detect these vulnerabilities. To keep your Nessus scanner up-to-date with the latest plugins, making your scans as accurate as possible, you need to update your plugins daily.

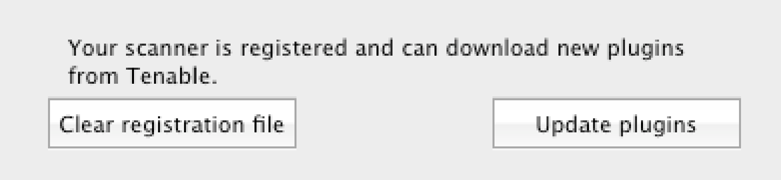
The "**Perform a daily plugin update**" option configures the Nessus server to automatically update plugins from Tenable every 24 hours. This occurs roughly at the time of day that you started Nessus.



☑ Perform a daily plugin update

If this option is set, your Nessus server will update its plugins every 24 hours.

You can force a plugin update by clicking on the "Update Plugins" button as shown below:



Your scanner is registered and can download new plugins from Tenable.

<u>How Often Should I Update Plugins?</u>

In general, updating your Nessus plugins once a day is sufficient for most organizations. If you absolutely need the most current plugins and intend to update continuously throughout the day, then updating no more than once every four hours is sufficient as there is virtually no benefit in updating more than this.

Selecting the check box "Start the Nessus server when booting" permits remote user access and updates plugins daily.

Removing Nessus

To remove Nessus, stop the Nessus service and delete the following directories:

```
/Library/Nessus
/Applications/Nessus
/Library/Receipts/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.

Configure the Nessus Daemon (Advanced Users)

The file **/opt/nessus/etc/nessus/nessusd.conf** 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. This file is created automatically with default settings, but it is recommended that these settings be reviewed and modified appropriately based on your scanning environment. The full list of configuration options are explained at the end of this section.

In particular, the **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 shown in the **nessusd.conf** file:

```
# Maximum number of simultaneous hosts tested:
max_hosts = 40

# Maximum number of simultaneous checks against each host tested:
max_checks = 5
```

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

Remember that the settings in **nessusd.conf** will always be over-ridden by the values set in the SecurityCenter Scan Template or Nessus web client policy options when performing a scan via these tools.

⚠ 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 for determining the best **`max_hosts`** setting in an enterprise environment would be to set it to "20" on a Unix-based Nessus system and "10" on a Windows Nessus scanner.

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.

If you edit the **`nessusd.conf`** file, you must restart Nessus for the changes to take effect.

During the upgrade process to 4.4, Nessus will not overwrite the current `nessusd.conf` file. This will result in several options not being included in the configuration file. For options that are not included, Nessus will use the default setting as included in a fresh install of 4.4.

The following table provides a brief explanation of each configuration option available in the **`nessusd.conf`** file. Many of these options are configurable through the user interface when creating a scan policy. Options that are new with 4.4 are bolded.

Option	Description
auto_update	Automatic plugin updates - if enabled and Nessus is registered, then fetch the newest plugins from plugins.nessus.org automatically. Disable if the scanner is on an isolated network not able to reach the Internet.
auto_update_delay	Number of hours to wait between two updates. Four (4) hours is the minimum allowed interval.

purge_plugin_db	Should Nessus purge the plugin database at each update. Choosing yes will cause each update to be considerably slower.
throttle_scan	Throttle scan when CPU is overloaded.
logfile	Where the Nessus log file is stored.
www_logfile	Where the Nessus Web Server (user interface) log is stored.
log_whole_attack	Log every detail of the attack? Helpful for debugging issues with the scan, but this may be disk intensive.
dumpfile	Location of a dump file for debugging output if generated.
rules	Location of the Nessus Rules file.
cgi_path	During the testing of web servers, use this colon delimited list of CGI paths.
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.
optimize_test	Optimize the test procedure. Changing this to "no" will cause scans to take longer and typically generate more false positives.
checks_read_timeout	Read timeout for the sockets of the tests.
non_simult_ports	Ports against which two plugins should not be run simultaneously.
plugins_timeout	Maximum lifetime of a plugin's activity (in seconds).
safe_checks	Safe checks rely on banner grabbing rather than active testing for a vulnerability.
auto_enable_dependencies	Automatically activate the plugins that are depended on. If disabled, not all plugins may run despite being selected in a scan policy.
silent_dependencies	If enabled, the list of plugin dependencies and their output are not included in the report.
use_mac_addr	Designate hosts by MAC address, not IP address (useful for DHCP networks).
save_knowledge_base	Save the knowledge base on disk for later use.

plugin_upload	Designate if admin users may upload plugins.
plugin_upload_suffixes	Suffixes of the plugins the admin user can upload.
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...).
listen_address	IPv4 address to listen for incoming connections.
listen_port	Port to listen to (old NTP protocol). Used for pre 4.2 NessusClient connections.
xmlrpc_listen_port	Port for the Nessus Web Server to listen to (new XMLRPC protocol).
xmlrpc_idle_session_timeout	XMLRPC Idle Session Timeout (in min).
xmlrpc_min_password_len	Directs Nessus to enforce a policy for the length of a password for users of the scanner.
enable_listen_ipv4	Directs Nessus to listen on IPv4.
enable_listen_ipv6	Directs Nessus to listen on IPv6 if the system supports IPv6 addressing.
source_ip	In the case of a multi-homed system with different IPs on the same subnet, this option tells the Nessus scaner 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.
disable_ntp	Disable the old NTP legacy protocol.
disable_xmlrpc	Disable the new XMLRPC (Web Server) interface.
nasl_no_signature_check	Should Nessus consider all NASL scripts as being signed? Selecting "yes" is unsafe and not recommended.
nasl_log_type	Direct the type of NASL engine output in **nessusd.dump**.

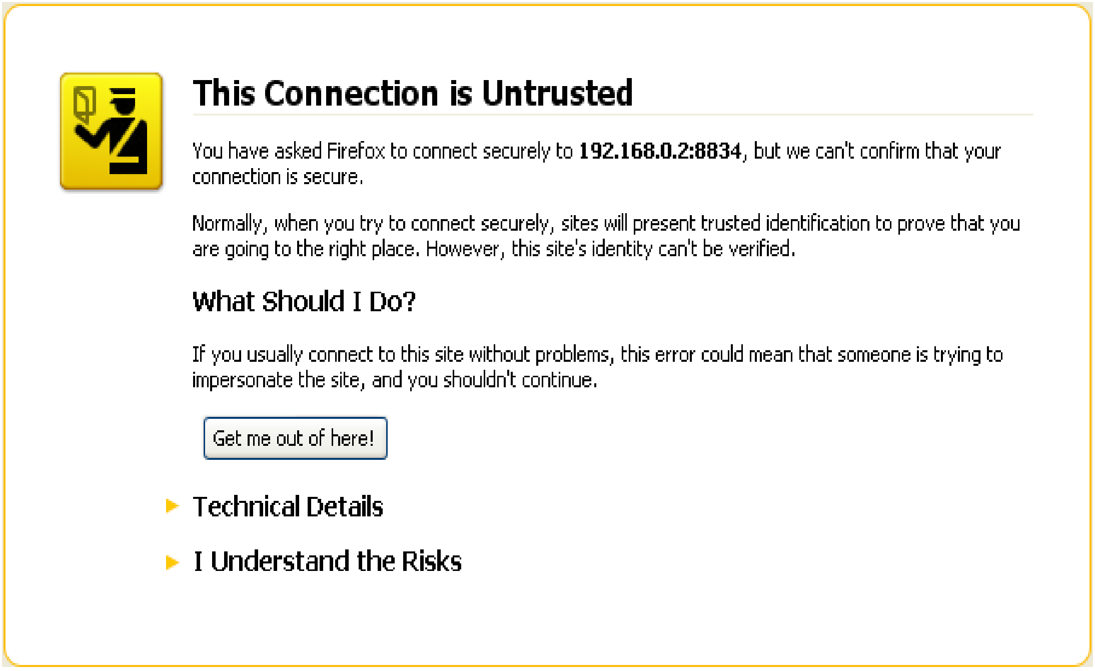
use_kernel_congestion_detection	Use Linux’s TCP congestion messages to scale back scan activity as required.
global.max_scans	If set to non-zero, this defines the maximum number of scans that may take place in parallel. **Note**: If this option is not used, no limit is enforced.
global.max_web_users	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.
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.
max_simult_tcp_sessions	Maximum number of simultaneous TCP sessions per scan.
host.max_simult_tcp_sessions	Maximum number of simultaneous TCP sessions per scanned host.
reduce_connections_on_congestion	Reduce the number of TCP sessions in parallel when the network appears to be congested.
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.
paused_scan_timeout	Kill a paused scan after how many minutes (0 for no timeout).
report_crashes	Anonymously report crashes to Tenable?
qdb_mem_usage	Direct 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.

⚠ Settings in **`nessusd.conf`** can be overridden by user settings in a **`.nessusrc`** file.

By default, a HomeFeed subscription will set **`report_crashes`** to “yes” and a ProfessionalFeed subscription will set **`report_crashes`** to “no”. 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.

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.

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 and Solaris	/opt/nessus/com/nessus/CA/servercert.pem /opt/nessus/var/nessus/CA/serverkey.pem
FreeBSD	/usr/local/nessus/com/nessus/CA/servercert.pem /usr/local/nessus/var/nessus/CA/serverkey.pem
Windows	C:\Program Files\Tenable\Nessus\nessus\CA\
Mac OS X	/Library/Nessus/run/com/nessus/CA/servercert.pem /Library/Nessus/run/var/nessus/CA/serverkey.pem

As of 4.4, Nessus supports SSL certificate chains.

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 initial process. You cannot use the downloaded plugin package with another Nessus scanner.

Register your Nessus Scanner

You must retrieve your Activation Code for the Nessus Subscription from either your Tenable Support Portal account for the ProfessionalFeed or your HomeFeed registration email. You must subscribe to the ProfessionalFeed to use Nessus in a professional environment even if it is not directly for commercial purposes. This includes scanning your desktop at work or a home computer that is used for business purposes. Please review the Subscription Agreement for more details on the type of subscription for which you are qualified. Users qualified for a HomeFeed subscription can register by going to http://www.nessus.org/register/ and entering the email address for the registered user. To purchase the ProfessionalFeed, please contact Tenable at sales@tenable.com or go to the e-commerce site at https://products.nessus.org/. Tenable will then send you an Activation Code for the ProfessionalFeed.

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 and Solaris:

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

FreeBSD:

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

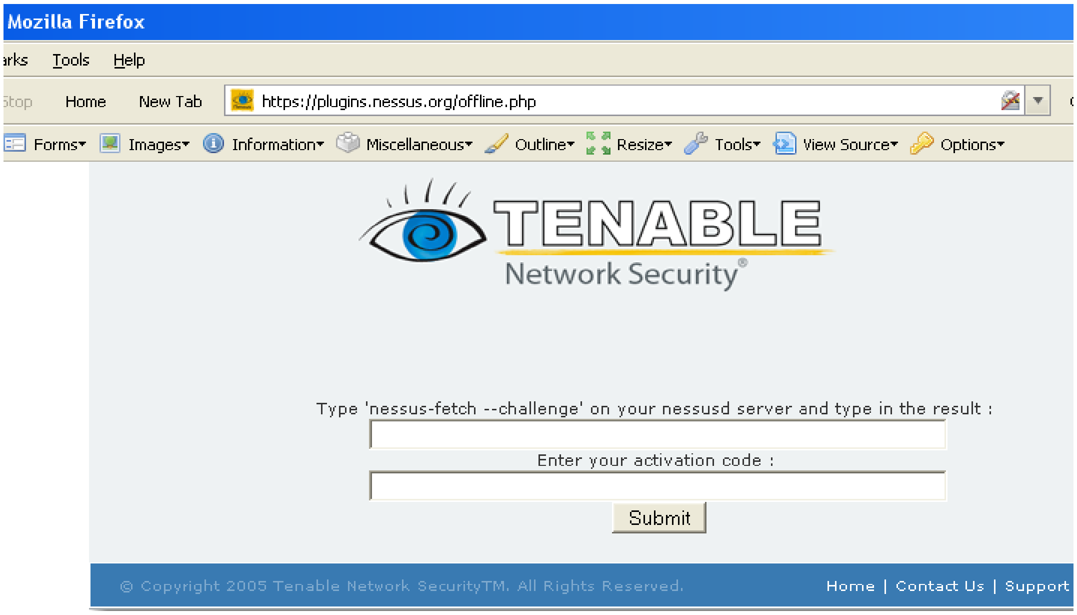
Mac OS X:

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

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

```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

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:


Mozilla Firefox
arks Tools Help
Stop Home New Tab
https://plugins.nessus.org/offline.php
Forms Images Information Miscellaneous Outline Resize Tools View Source Options
TENABLE Network Security

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

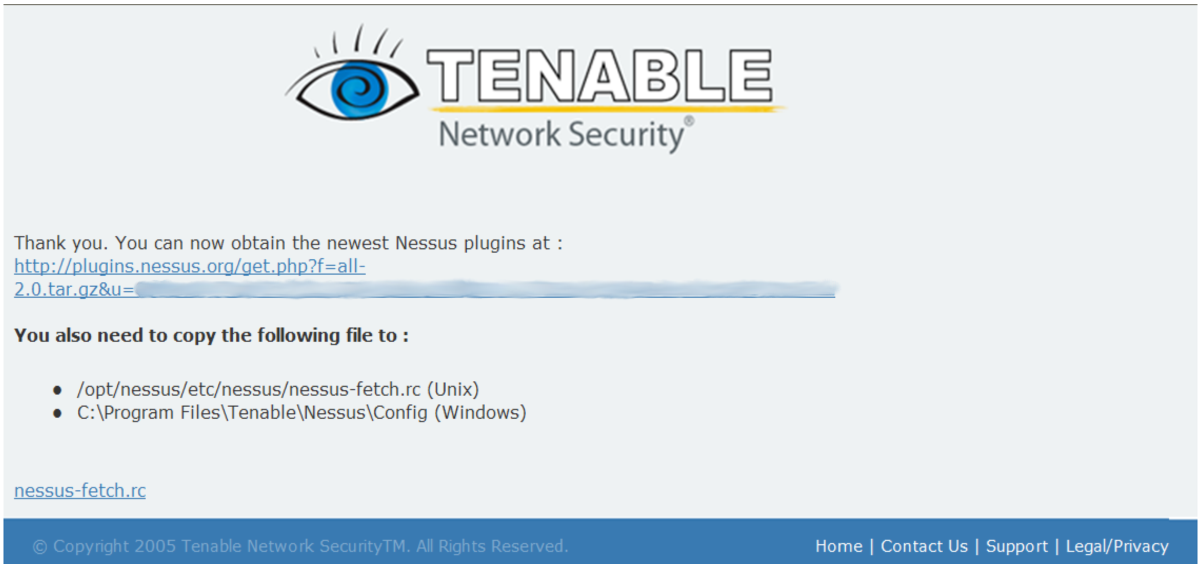
Enter your activation code :

Submit

© Copyright 2005 Tenable Network SecurityTM. All Rights Reserved.

Home | Contact Us | Support

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



Thank you. You can now obtain the newest Nessus plugins at :
http://plugins.nessus.org/get.php?f=all-2.0.tar.gz&u=[redacted]

You also need to copy the following file to :

- /opt/nessus/etc/nessus/nessus-fetch.rc (Unix)
- C:\Program Files\Tenable\Nessus\Config (Windows)

nessus-fetch.rc

© Copyright 2005 Tenable Network SecurityTM. All Rights Reserved.

Home | Contact Us | Support | Legal/Privacy

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 decribed in the next section.

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

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.

Copy the **nessus-fetch.rc** file to the host running Nessus in the following directory:

Windows:

C:\Program Files\Tenable\Nessus\conf

Linux and Solaris:

/opt/nessus/etc/nessus/

FreeBSD:

/usr/local/nessus/etc/nessus/

Mac OS X:

/Library/Nessus/run/etc/nessus/

The **nessus-fetch.rc** file only needs to be copied one time. Subsequent downloads of the Nessus plugins will need to be copied into the appropriate directory each time, as described in the next section.

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, simply edit **nessusd.conf** and set “**auto_update**” to “**no**”.

Obtain and Install Up-to-date Plugins

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

Windows

To obtain the newest plugins, go to the URL that was provided in the previous step, download the file named “**all-2.0.tar.gz**” and save it in the directory **C:\Program Files\Tenable\Nessus\**. To install the plugins, perform the following command:

```
C:\Program Files\Tenable\Nessus>nessus-update-plugins.exe all-2.0.tar.gz
Expanding all-2.0.tar.gz
Done. You need to restart the Nessus server for the changes to take effect

C:\Program Files\Tenable\Nessus>
```

Then, using the Nessus Server Manager, stop and restart the Nessus server.

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 you must go to the provided URL, obtain the tarball, copy it to the system running Nessus and run the command above.

Linux, Solaris and FreeBSD

To obtain the newest plugins, go to the URL that was provided in the previous step, download the file named "all-2.0.tar.gz" and save it in the directory **/opt/nessus/sbin/** (or **/usr/local/nessus/sbin/** for FreeBSD). To install the plugins, perform the following command:

Linux and Solaris:

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

FreeBSD:

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

Next, restart the Nessus process from the command-line so that Nessus uses the new plugins. For instructions on restarting the Nessus daemon, see the sections titled: "Stop the Nessus Daemon" and "Start the Nessus Daemon".

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 you must go to the provided URL, obtain the tar archive, copy it to the system running Nessus and run the command above.

Mac OS X

To obtain the newest plugins, go to the URL that was provided in the previous step, download the file named "**all-2.0.tar.gz**" and save it in the directory **/Library/Nessus/run/sbin/**. To install the plugins, perform the following command:

```
# /Library/Nessus/run/sbin/nessus-update-plugins all-2.0.tar.gz
```

Then, using the Nessus Server Manager, stop and restart the Nessus server.

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 you must go to the provided URL, obtain the tar archive, copy it to the system running Nessus and run the command above.

Working with SecurityCenter

SecurityCenter Overview

The Tenable 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.

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.

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

Configuring Nessus to Work with SecurityCenter

To enable any Nessus scanner for control by SecurityCenter, a specific username and password must be available to upload plugins and perform a scan. This user must be an "admin user" as configured during the "nessus-adduser" process to ensure privileges required to upload plugins along with other administrative functions.

> If a Nessus scanner is configured to only scan certain IP ranges, it can still be used by SecurityCenter. However, if SecurityCenter attempts to scan outside of those ranges, no vulnerability data will be reported.

Unix/Mac OS X

For Unix command line systems, follow the directions for adding users in the "Create a Nessus User" section. Make sure the user created is an "admin" user.

For Mac OS X systems, follow the directions for creating a user in the "Create and Manage Nessus Users" section. By default, Nessus users on the Mac are created with admin privileges.

Windows

Configuring Nessus to Listen as a Network Daemon

Nessus can be configured to communicate with SecurityCenter. To do this, we need to complete two tasks. We need to add an account for SecurityCenter to log into Nessus, and then we need to enable the Nessus service to listen to inbound network connections from SecurityCenter.

Adding User Accounts in Windows

If you are using Nessus for Windows and SecurityCenter, you will need to create one user via the command line and register it. This will allow the admin to start the nessusd service and SecurityCenter to upload the plugins. To perform this task, open a DOS command shell (Start -> Run -> cmd) and navigate to **`C:\Program Files\Tenable\Nessus`**. Enter the following commands to add a user and direct Nessus to receive plugins from SecurityCenter:

```
C:\Program Files\Tenable\Nessus>nessus-adduser.exe
Login : admin
Authentication (pass/cert) : [pass]
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 admin 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)


Login             : admin
Password         : ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
Is that ok ? (y/n) [y] y
User added
```

SecurityCenter users must always be an admin user.

Enabling the Nessus service in Windows

After adding the Nessus user, the Nessus server must be configured to enable the Nessus service. This allows SecurityCenter to actually add the Nessus server. Use the following command:

```
C:\Program Files\Tenable\Nessus>nessus-fetch.exe --security-center
nessusd can now be started, SecurityCenter will upload the plugins

C:\Program Files\Tenable\Nessus>
```

Use the Windows service manager to start the "Tenable Nessus" service. To verify that Nessus is indeed listening on port 1241, from the Windows command line use the "**`netstat -an | findstr 1241`**" command as shown below:

```
C:\Documents and Settings\admin>netstat -an | findstr 1241
  TCP    0.0.0.0:1241           0.0.0.0:0              LISTENING
```

Notice that the output contains "0.0.0.0:1241", which means a server is listening on that port. The Nessus server can now be added to the SecurityCenter via the SecurityCenter web interface.

Host-Based Firewalls

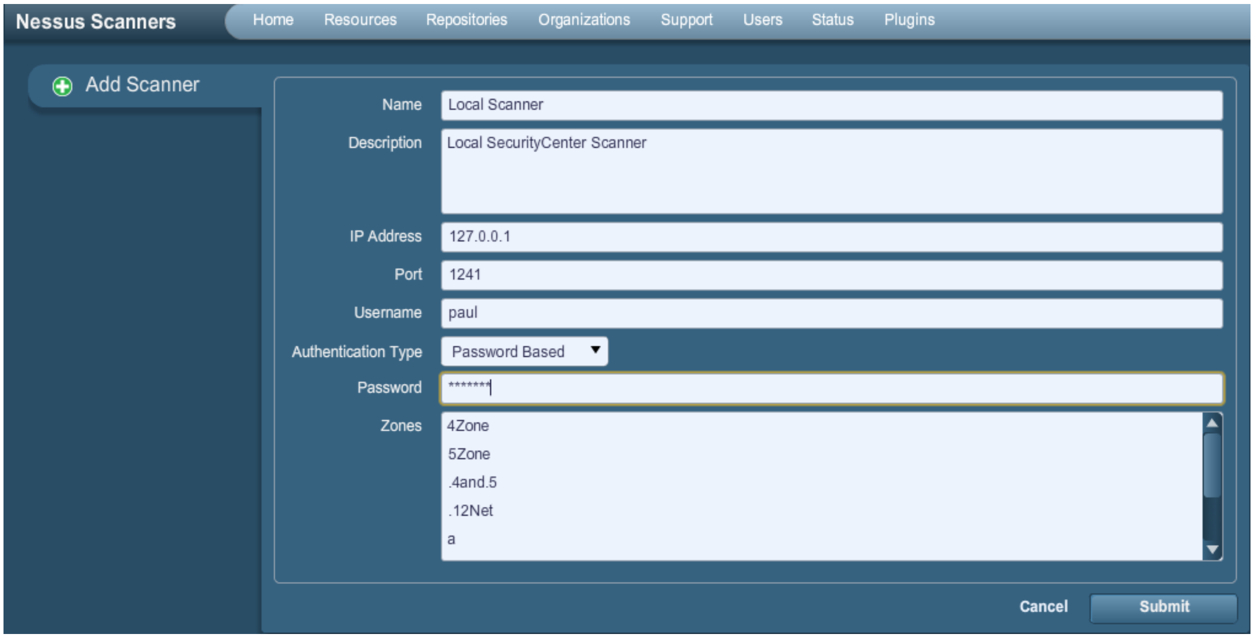
If your Nessus server is configured with a local firewall such as Zone Alarm, Sygate, BlackICE, the Windows XP firewall, or any other firewall software, it is required that connections be opened from SecurityCenter's IP address.

By default, port 1241 is used. 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 1241 choose the "**Exceptions**" tab and then add port "1241" to the list.

Configuring SecurityCenter to work with Nessus

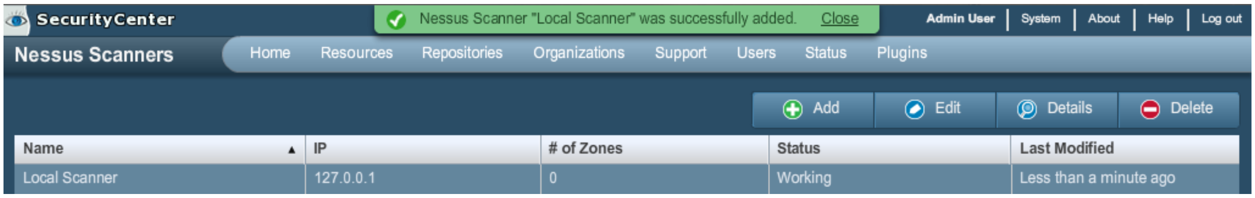
A "Nessus Server" can be added through the SecurityCenter administration interface. Using this interface, SecurityCenter can be configured to access and control virtually any Nessus scanner. Click on the "Resources" tab and then click on "**Nessus Scanners**". Click on "**Add**" to open the "Add Scanner" dialog. The Nessus scanner's IP address, Nessus port (default: 1241), administrative login ID, authentication type and password (created while configuring Nessus) are required. The password fields are not available if "SSL Certificate" authentication is selected. In addition, Zones that the Nessus scanner will be assigned to are selectable.

An example screen shot of the SecurityCenter scanner add page is shown below:



Name	Local Scanner
Description	Local SecurityCenter Scanner
IP Address	127.0.0.1
Port	1241
Username	paul
Authentication Type	Password Based
Password	*******
Zones	4Zone 5Zone .4and.5 .12Net a

After successfully adding the scanner, the following page is displayed after the scanner is selected:



Nessus Scanner "Local Scanner" was successfully added. Close

Name	IP	# of Zones	Status	Last Modified
Local Scanner	127.0.0.1	0	Working	Less than a minute ago

For more information please refer to the "SecurityCenter Administration Guide".

Nessus Windows Troubleshooting

Installation /Upgrade Issues

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

Solution: The "nesssud <version> started" message only indicates that the nessusd program was executed. The message "nessusd is ready" indicates that the Nessus Server is running and read 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 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.

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.

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 User Guide** – how to configure, and operate the Nessus User Interface
- **Nessus Credential Checks for Unix and Windows –** information on how to perform authenticated network scans with the Nessus vulnerability 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

Please feel free to contact us at support@tenable.com, sales@tenable.com or visit our web site at http://www.tenable.com/. For more information about Nessus, please visit http://www.nessus.org/.

Non-Tenable License Declarations

Below you will find 3rd party software packages that Tenable provides for use with Nessus. Any Third Party Component that is not marked as copyrighted by Tenable is subject to other license terms that are specified in the documentation.

Third party plugins are considered “Vulnerability detection plugins” and covered as follows.

Section 1 (a) of the Nessus License Agreement reads:

Any plugins or components that are not marked as copyrighted by Tenable are not Plugins as defined under this Subscription Agreement and are subject to other license terms.

Section 1 (b) (i) of the Nessus License Agreement reads:

The Subscription includes vulnerability detection programs not developed by Tenable or its licensors and which are licensed to You under separate agreements. The terms and conditions of this Subscription Agreement do not apply to such vulnerability detection programs.

Portions of this Tenable Network Security Software may utilize the following copyrighted material, the use of which is hereby acknowledged:

Portions Copyright (c) 1997-2008 University of Cambridge (libpcre)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 2000 The NetBSD Foundation, Inc. All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1995-1999 Kungliga Tekniska Hogskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper
Portions Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/) Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES

About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at http://www.tenable.com/.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 410-872-0555
http://www.tenable.com/