Nessus 3.0
Installation Guide

October 15, 2007
(Revision 33)

The newest version of this document is available at the following URL:
http://www.nessus.org/documentation/nessus_3.0_installation_guide.pdf

Table of Contents

Introduction

Welcome

Welcome to Tenable Network Security's **Nessus 3.0** Installation Guide. As you read this document, please share your comments and suggestions with us by emailing them to support@tenablesecurity.com.

This document will discuss the installation and configuration of the Nessus Vulnerability Scanner. Tenable Network Security, Inc. is the author and manager of the Nessus Security Scanner. In addition to constantly improving the Nessus engine, Tenable is in charge of writing most of the plugins available to the scanner.

Nessus is available for a variety of operating systems which include Red Hat ES3, ES4, Fedora Core 1, 3, 4, and 5, SUSE 9.3 and 10.0, Debian 3.1, FreeBSD 5.4 and 6.0, Solaris 9 and 10, Mac OS X, and Windows 2000, XP, and Server 2003. In addition, Nessus is available for the Enterasys Dragon appliance running Dragon 7.2 or later.

Prerequisites, deployment options, and a walk-through of an installation will be discussed.

A basic understanding of UNIX and vulnerability scanning is assumed.

This document explains how to install and start the **Nessus Server** only. Nessus is composed of a server which is in charge of doing the vulnerability audits, and a client to "drive" it. For further information about the clients available for Nessus, please refer to the "Nessus Client Guide".

Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with an italicized font such as *setup.exe.*

Command line options and keywords are printed with the following 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 remote 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 will allow you to audit remotely a given network and determine whether it has been broken into or misused in some way.

Intelligent Scanning – Unlike many other security scanners, Nessus does not take anything for granted. That is, it will not consider 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 also not determine if a security vulnerability is present by just regarding the version number of the remote service, but will really attempt to exploit the vulnerability.

Modular Architecture – The client/server architecture allows you the flexibility to deploy the scanner (server) and the GUI (client) in multiple configurations reducing management costs (one server can be accessed by multiple clients)

CVE Compatible – Each plugin links to CVE for administrators to retrieve further information on published vulnerabilities. They also include references to CERT, Bugtraq, and vendor security alerts.

Plug-in Architecture – Each security test is written as an external plugin. This way, you can easily add your own tests without having to read the code of the Nessus server engine, *nessusd*. The complete list of the Nessus plugins is available at http://cgi.nessus.org/plugins.

NASL – The Nessus Security Scanner includes NASL (Nessus Attack Scripting Language), a language designed 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 mainly focuses on the development of security checks for recently found vulnerabilities. Our security checks database is updated on a daily basis and all the newest security checks are available at http://www.nessus.org/scripts.php as well as on the FTP servers and mirrors.

Tests Multiple Hosts Simultaneously – Depending on the configuration of the Nessus scanner system, you can test a large number of hosts all at once.

Smart Service Recognition – Nessus does not believe that the target hosts will respect the IANA assigned port numbers. This means that it will recognize a FTP server running on a non-standard port (i.e. 31337) or a web server running on port 8080.

Multiples Services – Imagine that you run two web servers (or more) on your host, one on port 80 and another on port 8080. When it comes to testing their security, Nessus will test both of them.

Tests Cooperation – The security tests performed by Nessus cooperate so that no unnecessary checks are performed. If your FTP server does not offer anonymous logins, then anonymous-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 (from Low to Very High), but it will also tell you how to prevent them from being exploited in most cases.

Full SSL Support – Nessus has the ability to test services offered over SSL such as https, smtps, imaps, and more. You can even supply Nessus with a certificate so that it can integrate into a PKI environment.

Smart Plugins (optional) – Nessus will determine which plugins should or should not be launched against the remote host (for instance, this prevents the testing of Sendmail vulnerabilities against Postfix). This option is called "optimizations".

Non-Destructive (optional) – Certain checks can be detrimental to specific network services. If you do not want to risk causing a service failure on you network, you can 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 Bug Tracking System – Found a bug? Report it here: http://bugs.nessus.org.

Prerequisites

Tenable recommends a minimum of 256MB of memory to operate Nessus on a local "Class C" network. To conduct larger scans of multiple networks, at least 1 GB of memory is recommended, but it can require up to 4 GB.

A Pentium 3 processor running at 733 MHz or higher is recommended. When running on Mac OS X, a G4 processor running at 733 MHz or higher is recommended.

Nessus for Mac OS X is a Universal Binary. It works as well on a PowerPC processor and an Intel

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 Windows

Microsoft has added changes to Windows XP SP-2 (Home & Pro) that can impact the performance of Nessus Windows and cause false negatives. 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 "Appendix 1: Nessus Windows Troubleshooting" at the end of the document.

Deployment Options

When deploying Nessus, knowledge of routing, filters, and firewall policies should be considered. Nessus should 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 inside of that device's 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. Also, if the system running Nessus has personal or desktop firewalls in place, these tools can drastically limit the effectiveness of a 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

Tenable manages the Nessus vulnerability scanner. Numerous new vulnerabilities are made public by vendors, researchers, and other sources every day. Tenable endeavors to have checks for recently published vulnerabilities as soon as possible, and this is usually within 24 hours of disclosure. The checks for a specific vulnerability are known in 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. These are the direct and the registered feed.

Direct Plugin Feed

As Tenable writes new plugins for the latest security vulnerabilities they are immediately released to commercially subscribed customers. These include organizations that use Nessus and purchase the direct feed for each scanner and organizations that purchase Tenable's Security Center (formerly Lightning Console).

Tenable also provides commercial support via email to direct plugin feed customers who are using Nessus 3. The direct feed also includes a set of host-based compliance checks for UNIX and Windows which is very useful when performing SOX or FISMA audits.

Registered Plugin Feed

Tenable makes all of the vulnerability research it does available to the public, seven days after new checks have been released to the direct feed. There is no charge to use the registered feed, however, there is a separate license for the registered feed which users must agree to comply with.

To register a Nessus scanner to receive plugins through the registered feed, visit http://www.nessus.org and follow the directions. This involves submitting an email address for contacting you and sending you an activation code. You will use this activation code later on to configure your Nessus scanner to receive the updates.

Which Feed is For You?

Later on in this document, we will discuss how to configure your Nessus to receive either a registered or direct feed. However, what you need to do regarding how you are using the Nessus technology may seem confusing. Here is a short list of scenarios:

- **Complimentary Nessus User** - You should visit http://www.nessus.org and register your Nessus to use the seven-day delayed feeds. Use the activation code you receive from the registration process when configuring Nessus to do updates.

- **Complimentary Nessus User, but Purchased Direct Feed** - If you are using the complimentary Nessus, but have purchased a direct feed, you will receive an activation code from Tenable. This code should be used when configuring your Nessus for updates.

- **Nessus Managed by Security Center –** If you are using Nessus in conjunction with Tenable's Security Center, the Security Center will have access to the direct plugin feed and will automatically update your Nessus scanners.

UNIX/Linux

Upgrading from Nessus 3.x

This section will explain how to upgrade Nessus when upgrading from a previous Nessus 3.x installation.

Red Hat and SUSE

If you have used a Nessus RPM to install Nessus 3.x, an upgrade is simple and retains configuration settings. Also, the users that were created previously will still be intact. Use the Nessus 3 RPM and use standard RPM switches to apply a package upgrade.

Download the latest version of Nessus from http://www.nessus.org/download/.

Before upgrading the package, stop the *nessusd* service by using this command:

```
# killall nessusd
```

The command `killall nessusd` will abruptly stop any on-going scans.

Then, use the following command to upgrade Nessus depending on your version:

```
# rpm -Uvh <newest release>
```

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

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

There is an example of the screen output for upgrading Nessus on Red Hat ES3 below:

```
# killall nessusd
# rpm -Uvh Nessus-3.0.5-es3.i386.rpm
Preparing...           ########################################### [100%]
Shutting down Nessus services:
   1:Nessus            ########################################### [100%]

nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

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

All plugins loaded
 - Please run /opt/nessus/sbin/nessus-add-first-user 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

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

```
nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

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

All plugins loaded
#
```

Debian

An upgrade for Nessus on Debian is simple and retains configuration settings. Also, the users that were created previously will still be intact.

Download the latest version of Nessus from http://www.nessus.org/download/.

Before upgrading the package, stop the *nessusd* service by using this command:

```
# killall nessusd
```

The command `killall nessusd` will abruptly stop any on-going scans.

Then, use the following command to upgrade Nessus:

```
# dpkg –i <newest release>
```

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

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

There is an example of the screen output for upgrading Nessus on Debian 3 below:

```
# dpkg -i Nessus-3.0.5-debian3_i386.deb
(Reading database ... 19831 files and directories currently installed.)
Preparing to replace nessus 3.0.4 (using Nessus-3.0.5-debian3_i386.deb) ...
Shutting down Nessus : .
Unpacking replacement nessus ...

Setting up nessus (3.0.5) ...

nessusd (Nessus) 3.0.5. for Linux
(C) 2005 Tenable Network Security, Inc.

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

All plugins loaded

 - Please run /opt/nessus/sbin/nessus-add-first-user 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
```

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

nessusd (Nessus) 3.0.5. for Linux
(C) 2005 Tenable Network Security, Inc.

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

All plugins loaded
#
```

Solaris

Download the latest version of Nessus from http://www.nessus.org/download/. 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.

Before uninstalling the package, stop the *nessusd* service by using this command:

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

The command `/etc/init.d/nessusd stop` will abruptly stop any on-going scans.

To remove the package, you must first determine what package name Nessus is registered as within the system's database. This name will not be the same as the filename used for installation. Use the following command to determine the package name:

```
# 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>
```

For example, with the package name that was determined in the previous step the command to uninstall Nessus is:

```
# pkgrm TNBLnessus
```

This 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 install the new package from the directory where it was downloaded it to, use the following commands:

```
# gunzip <package name>.pkg.gz
```

pkgadd –d ./<package name>

You can also specify the full path of the location of the new package, as shown in this example:

pkgadd –d /export/home/sysadmin/Nessus-3.0.5-solaris-sparc.pkg

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

/opt/nessus/sbin/nessusd -D

An example of the screen output for upgrading Nessus on Solaris is as follows (the output of the installation files has been redacted for readability):

```
# /etc/init.d/nessusd stop
# pkginfo | grep nessus
application TNBLnessus              The Nessus Network Vulnerability Scanner
# pkgrm TNBLnessus

The following package is currently installed:
   TNBLnessus  The Nessus Network Vulnerability Scanner
               (sparc) 3.0.4

Do you want to remove this package? [y,n,?,q] y

## Removing installed package instance <TNBLnessus>
## Verifying package <TNBLnessus> dependencies in global zone
## Processing package information.
## Removing pathnames in class <none>
/opt/nessus/var/nessus/users <non-empty directory not removed>
/opt/nessus/var/nessus/tmp
/opt/nessus/var/nessus/nessus_org.pem
.
.
.
/etc/rc1.d/K90nessusd
/etc/init.d/nessusd
## Updating system information.

Removal of <TNBLnessus> was successful.
# gunzip Nessus-3.0.5-solaris-sparc.pkg.gz
# pkgadd -d ./Nessus-3.0.5-solaris-sparc.pkg

The following packages are available:
  1  TNBLnessus     The Nessus Network Vulnerability Scanner
                    (sparc) 3.0.5

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

Processing package instance <TNBLnessus> from </export/home/sysadmin/Nessus-
3.0.5-solaris-sparc.pkg>

The Nessus Network Vulnerability Scanner(sparc) 3.0.5
## Processing package information.
```

```
## Processing system information.
   9 package pathnames are already properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.

The following files are already installed on the system and are being
used by another package:
* /opt/nessus/var/nessus <attribute change only>

* - conflict with a file which does not belong to any package.

Do you want to install these conflicting files [y,n,?,q] y
## 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,?] y

Installing The Nessus Network Vulnerability Scanner as <TNBLnessus>

## Installing part 1 of 1.
/etc/init.d/nessusd
/etc/rc1.d/K90nessusd <symbolic link>
/etc/rc2.d/S90nessusd <symbolic link>
/etc/rc3.d/S90nessusd <symbolic link>
/etc/rcS.d/K90nessusd <symbolic link>
/opt/nessus/bin/c_rehash
.
.
.
/opt/nessus/var/nessus/nessus-services
/opt/nessus/var/nessus/nessus_org.pem
[ verifying class <none> ]
## Executing postinstall script.
nessusd (Nessus) 3.0.5. for SunOS
(C) 1998 - 2007 Tenable Network Security, Inc.

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

All plugins loaded

 - Please run /opt/nessus/sbin/nessus-add-first-user 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


Installation of <TNBLnessus> was successful.
/opt/nessus/bin/nasl
# /opt/nessus/sbin/nessusd -D

nessusd (Nessus) 3.0.5. for SunOS
(C) 1998 - 2007 Tenable Network Security, Inc.
```

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

All plugins loaded
#
```

FreeBSD

Download the latest version of Nessus from http://www.nessus.org/download/. In order 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.

Before uninstalling the package, stop the *nessusd* service by using this command:

killall nessusd

The command `killall nessusd` will abruptly stop any on-going scans.

In order to remove the package, you must first determine what package name Nessus is registered as within the system's database. This name will not be the same as the filename used for installation. Use the following command to determine the package name:

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-3.0.3        A powerful security scanner
```

Then, to remove the Nessus package on a FreeBSD system the command is:

pkg_delete <package name>

For example, with the package name that was determined in the previous step the command to uninstall Nessus is:

pkg_delete Nessus-3.0.3

This 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.

Then, use the following command to install the newest release of Nessus depending on your version:

pkg_add <newest release>

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

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

There is an example of the screen output for upgrading Nessus on FreeBSD 6.0 below:

```
# killall nessusd
# pkg_delete Nessus-3.0.4
# pkg_add Nessus-3.0.5-fbsd6.tbz

nessusd (Nessus) 3.0.5. for FreeBSD
(C) 2005 Tenable Network Security, Inc.

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

All plugins loaded

 - Please run /usr/local/nessus/sbin/nessus-add-first-user 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) 3.0.5. for FreeBSD
(C) 2005 Tenable Network Security, Inc.

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

All plugins loaded
#
```

Enterasys Dragon IDS

Contact Tenable to download the latest version of Nessus for the Enterasys Dragon appliance.

Before upgrading the package, stop the *nessusd* service by using this command:

```
# killall nessusd
```

The command `killall nessusd` will abruptly stop any on-going scans.

Then, use the following command to upgrade Nessus depending on your version:

```
# installpkg <newest release>
```

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

```
# /opt/nessus/sbin/nessusd –D –S <IP Address>
```

There is an example of the screen output for upgrading Nessus on Dragon below:

```
# installpkg Nessus-3.0.5-dragon-skw-i386.tgz
 Installing package Nessus-3.0.5-dragon-skw-i386...
 PACKAGE DESCRIPTION:

Executing install script for Nessus-3.0.5-dragon-skw-i386(2)...
 - 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
 - Package Removal : /opt/nessus/scripts/nessus-remove
 - You can start nessusd by typing /opt/nessus/sbin/nessusd -D -S <IP
Address>
nessusd (Nessus) 3.0.5. for Linux
(C) 1998 - 2006 Tenable Network Security, Inc.

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

All plugins loaded

# /opt/nessus/sbin/nessusd -D -S 192.168.20.237
nessusd (Nessus) 3.0.5. for Linux
(C) 1998 - 2006 Tenable Network Security, Inc.

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

All plugins loaded
#
```

Depending on how the users' system is configured the upgrade may produce messages such as:

```
/sbin/ldconfig: File /usr/lib/libcprts.so is too small, not checked.
```

These are not errors, just informational messages.

Due to the resource utilization of the Dragon IDS, installation of Nessus on the Dragon appliance can take an hour to complete.

Upgrading Nessus 2.x to Nessus 3.x

This section will explain how to upgrade a Nessus 2.x installation to Nessus 3.x. Since Nessus 3 is installed under a different directory, (*/usr/local/nessus/* for FreeBSD versions and */opt/nessus/* for all the other versions) required files from the old installation will need to be manually copied. Note that the instructions below assume that all files for Nessus 2 have been previously installed under the */usr/local/* directory structure (the directory named "nessus" did not exist in the past).

Download the latest version of Nessus from http://www.nessus.org/download/.

FreeBSD Platforms

Nessus 2 and Nessus 3 are installed under different paths; because of this they can be installed on the same system at the same time. The first step in upgrading your Nessus 2 to Nessus 3 is to stop the Nessus 2 installation's *nessusd* service using the following command:

```
# killall nessusd
```

The command `killall nessusd` will abruptly stop any on-going scans.

Next, install Nessus 3 by following the instructions in the "Installation" section for FreeBSD located later in this document.

Next, you must copy the users from Nessus 2 into Nessus 3. User management is directory based in Nessus, so moving user accounts is fairly straightforward. Copy the users with the command as follows:

```
# cp –r /usr/local/var/nessus/users/* /usr/local/nessus/var/nessus/users/
```

Next, you must copy the file *nessus-fetch.rc* to the appropriate Nessus 3 directory to save your plugin activation code. If you do not, you will have to contact Tenable Support in order to have the activation code reset. Copy the file with the command below:

```
# cp /usr/local/etc/nessus/nessus-fetch.rc /usr/local/nessus/etc/nessus/
```

Then, make sure the permissions are as follows:

```
-rw-------  1 root root 398 Nov  3 03:12 nessus-fetch.rc
```

The next step is to edit the file */usr/local/nessus/etc/nessus/nessusd.conf* to make sure that the `admin_user` is set properly. To do this, make sure that that the following options are correct:

```
plugin_upload = yes
admin_user = <ADMIN>
```

Where <ADMIN> is the name of the admin user defined in the Nessus 2 file */usr/local/etc/nessus/nessud.conf*.

Now you are ready to configure Nessus 3, start *nessusd*, and run a scan using one of the client options. This is all described later in this document as well as in the "Nessus Client Guide".

Finally, once you have verified that Nessus 3 is configured and running properly, the last step is to uninstall Nessus 2.x with the following command:

```
# /usr/local/sbin/uninstall-nessus
```

Non-FreeBSD Platforms

Nessus 2 and Nessus 3 are installed under different paths; because of this they can be installed on the same system at the same time. The first step in upgrading your Nessus 2

to Nessus 3 is to stop the Nessus 2 installation's *nessusd* service using the following command:

```
# killall nessusd
```

The command `killall nessusd` will abruptly stop any on-going scans.

Next, install Nessus 3 by following the instructions in the "Installation" section that are appropriate for your operating system:

- Red Hat and SUSE
- Debian
- Solaris

Next, you must copy the users from Nessus 2 into Nessus 3. User management is directory based in Nessus, so moving user accounts is fairly straightforward. Copy the users with the command as follows:

```
# cp –r /usr/local/var/nessus/users/* /opt/nessus/var/nessus/users/
```

Next, you must copy the file *nessus-fetch.rc* to the appropriate Nessus 3 directory to save your plugin activation code. If you do not, you will have to contact Tenable Support in order to have the activation code reset. Copy the file with the command below:

```
# cp /usr/local/etc/nessus/nessus-fetch.rc /opt/nessus/etc/nessus/
```

Then, make sure the permissions are as follows:

```
-rw-------  1 root root 398 Nov  3 03:12 nessus-fetch.rc
```

The next step is to edit the file */opt/nes*sus/etc/nessus/*nessusd.conf* to make sure that the `admin_user` is set properly. To do this, make sure that that the following options are correct:

```
plugin_upload = yes
admin_user = <ADMIN>
```

Where <ADMIN> is the name of the admin user defined in the Nessus 2 file */usr/local/etc/nessus/nessud.conf*.

Now you are ready to configure Nessus 3, start *nessusd*, and run a scan using one of the client options. This is all described later in this document as well as in the "Nessus Client Guide".

Finally, once you have verified that Nessus 3 is configured and running properly, the last step is to uninstall Nessus 2.x with the following command:

```
# /usr/local/sbin/uninstall-nessus
```

Installation

Red Hat and SUSE

Download the latest version of Nessus from http://www.nessus.org/download/. Nessus is available for Red Hat ES 3, ES 4, and Fedora Core 4, and SUSE 9.3 and 10.0.

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

Then, install it with the following command depending on your version:

```
# rpm –ivh Nessus-3.0.5-es3.i386.rpm
```

This will install Nessus into the directory */opt/nessus/*. Below is an example of the screen output for installation on Red Hat ES3:

```
# rpm –ivh Nessus-3.0.5-es3.i386.rpm
Preparing...                ########################################### [100%]
   1:Nessus                 ########################################### [100%]

nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

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

All plugins loaded
- Please run /opt/nessus/sbin/nessus-add-first-user 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
#
```

After the installation is complete you can continue to the next section entitled "Configuration".

Debian

Download the latest version of Nessus from http://www.nessus.org/download/. Nessus is available for Debian 3.

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

Then, install it with the following command:

```
# dpkg -i Nessus-3.0.5-debian3_i386.deb
```

This will install Nessus into the directory */opt/nessus/*. Below is an example of the screen output:

```
# dpkg –i Nessus-3.0.5-debian3_i386.deb
(Reading database ... 10027 files and directories currently installed.)
Unpacking nessus (from Nessus-3.0.5-debian3_i386.deb) ...
```

```
Setting up nessus (3.0.5) ...

nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

/opt/nessus/var/nessus/CA created
/opt/nessus/com/nessus/CA created

nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

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

All plugins loaded

- Please run /opt/nessus/sbin/nessus-add-first-user 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

#
```

After the installation is complete you can continue to the next section entitled "Configuration".

Solaris

Download the latest version of Nessus from http://www.nessus.org/download/. Nessus is available for Solaris 9 and 10.

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

First, uncompress the package with the following command:

```
# gunzip Nessus-3.0.5-solaris-sparc.pkg.gz
```

Then, install it with the following command:

```
# pkgadd -d ./Nessus-3.0.5-solaris-sparc.pkg
```

This will install Nessus into the directory */opt/nessus/*. Below is an example of the screen output:

```
Processing package instance <TNBLnessus> from </tenable/Nessus-3.0.5-
solaris-sparc.pkg>

The Nessus Network Vulnerability Scanner(sparc) 3.0.5
## 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,?] y

Installing The Nessus Network Vulnerability Scanner as <TNBLnessus>

## Installing part 1 of 1.
 [ verifying class <none> ]
## Executing postinstall script.
nessusd (Nessus) 3.0.5. for SunOS
(C) 1998 - 2006 Tenable Network Security, Inc.

/opt/nessus//var/nessus/CA created
/opt/nessus//com/nessus/CA created
nessusd (Nessus) 3.0.5. for SunOS
(C) 1998 - 2006 Tenable Network Security, Inc.

Processing the Nessus plugins...

 [##################################################]

All plugins loaded

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


Installation of <TNBLnessus> was successful.
```

After the installation is complete you can continue to the next section entitled "Configuration".

FreeBSD

Download the latest version of Nessus from http://www.nessus.org/download/. Nessus is available for FreeBSD 5.0 and 6.0.

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

Then, install it with the following command:

pkg_add Nessus-3.0.5-fbsd5.tbz

This will install Nessus into the directory */usr/local/nessus/*. Below is an example of the screen output:

```
# pkg_add Nessus-3.0.5-fbsd5.tbz

nessusd (Nessus) 3.0.5 for FreeBSD
(C) 2005 Tenable Network Security, Inc.

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

All plugins loaded

- Please run /usr/local/nessus/sbin/nessus-add-first-user 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

#
```

After the installation is complete you can continue to the next section entitled "Configuration".

Enterasys Dragon IDS

Contact Tenable to download the latest version of Nessus for the Enterasys Dragon appliance running Dragon 7.2 or later. Refer to "Appendix 2: Best Practices for the Enterasys Dragon IDS" for more information on configuring your Dragon appliance for use with Nessus.

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

Then, install it with the following command:

```
# installpkg Nessus-3.0.5-dragon-skw-i386.tgz
```

This will install Nessus into the directory */opt/nessus/*. Below is an example of the screen output:

```
# installpkg Nessus-3.0.5-dragon-skw-i386.tgz
Installing package Nessus-3.0.5-dragon-skw-i386(2)...
PACKAGE DESCRIPTION:
/sbin/ldconfig: File /usr/lib/libcprts.so is too small, not checked.
/sbin/ldconfig: File /usr/lib/libcxa.so is too small, not checked.
/sbin/ldconfig: File /usr/lib/libcxaguard.so is too small, not checked.
/sbin/ldconfig: File /usr/lib/libunwind.so is too small, not checked.
Executing install script for Nessus-3.0.5-dragon-skw-i386(2)...
 - 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
 - Package Removal : /opt/nessus/scripts/nessus-remove
 - You can start nessusd by typing /opt/nessus/sbin/nessusd -D -S <IP
Address>
nessusd (Nessus) 3.0.5. for Linux
```

```
(C) 1998 - 2006 Tenable Network Security, Inc.

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

All plugins loaded
/sbin/ldconfig: File /usr/lib/libcprts.so is too small, not checked.
/sbin/ldconfig: File /usr/lib/libcxa.so is too small, not checked.
/sbin/ldconfig: File /usr/lib/libcxaguard.so is too small, not checked.
/sbin/ldconfig: File /usr/lib/libunwind.so is too small, not checked.
```

Depending on how the users' system is configured the installation may produce messages such as:

`/sbin/ldconfig: File /usr/lib/libcprts.so is too small, not checked.`

These are not errors, just informational messages.

Due to the resource utilization of the Dragon IDS, installation of Nessus on the Dragon appliance can take an hour to complete.

After the installation is complete you can continue to the next section entitled "Configuration".

Configuration

Create a Nessus User

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

To enter each command you must use the complete path name. You can not first enter the directory and then use "./" to perform the command.

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

For password authentication use the `nessus-add-first-user` command to add the first user and use the default authentication method "pass" (password). For those configuring Nessus on the Dragon appliance, use the command `nessus-adduser` to add all users to Nessus. This command is discussed in more detail later in this section.

Each Nessus user has a set of rules referred to as "user rules" which control what they can and can not 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.

The commands for this section assume that Nessus is installed in the directory */opt/nessus/*. If you are using a version for FreeBSD, Nessus is installed in the directory */usr/local/nessus/*. Therefore "*/usr/local/nessus/*" must replace "*/opt/nessus/*" in every command performed.

```
# /opt/nessus/sbin/nessus-add-first-user
nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

Using /var/tmp as a temporary file holder

Add a new nessusd user
----------------------


Login : admin
Authentication (pass/cert) [pass]:
Login password:
Login password (again):

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(8) man page for the rules syntax

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)


Login      :admin
Password      :********
DN        :
Rules       :


Is that ok ? (y/n) [y]
User added.
Thank you. You can now start Nessus by typing:
/opt/nessus/sbin/nessusd –D
#
```

A single Nessus scanner can support a complex arrangement of multiple users. For example, maybe an organization needs multiple personnel to have access to the same Nessus scanner but have the ability to scan different IP ranges, perhaps 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 C subnet, 192.168.2.0/24. Please note that the command `nessus-adduser` is used to create further password authenticated users after the first password authenticated user was previously created using the command `nessus_add_first_user`. For further examples and the syntax of user rules please see the man pages for `nessus-adduser`.

```
# /opt/nessus/sbin/nessus-adduser
nessusd (Nessus) 3.0.5 for Linux
```

```
(C) 2005 Tenable Network Security, Inc.

Using /var/tmp as a temporary file holder

Add a new nessusd user
----------------------


Login : restricteduser
Authentication (pass/cert) [pass]:
Login password:
Login password (again):

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

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

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)
accept 192.168.2.0/24
default deny


Login      :restricteduser
Password      :************
DN        :
Rules       :
accept 192.168.2.0/24
default deny


Is that ok ? (y/n) [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
```

Configure the Nessus Daemon (Advanced Users)

In the file */opt/nessus/etc/nessus/nessusd.conf* there are several options that can be configured. 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 is all specified, as well as many other options. This file is created automatically with default settings, but these settings should be reviewed and modified appropriately based on your scanning environment.

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 Security Center or a client for Nessus such as NessusWX. To view/change these options for a scan template in the Security Center, edit a Scan Template's Scan Options. In NessusWX, edit a Session's properties, 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 Security Center Scan Template or NessusWX Session Options when performing a scan via these tools.

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. The hardware configuration of the scanner system and other applications running on it should be taken into consideration 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 (your organization's policy on scanning, other network traffic, the affect a particular type of scan has on your scan target hosts, etc.), 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 Linux 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 scan 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 this should always be set relatively low.

Setting max_checks to a value of "3" would be adequate for most organizations, and rarely would it be set any higher than "4".

Launch the Nessus Daemon

Start the Nessus service as root with the following command:

/opt/nessus/sbin/nessusd -D

Since there are multiple network interfaces in all of the Dragon sensors, the customer will want to specify which interface they want Nessus to bind to by including the –S <ip address> parameter. Therefore, users of Nessus on Dragon appliances must enter the following command to start the Nessus service:

/opt/nessus/sbin/nessusd –D –S <ip address>

The <ip address> should be on a different NIC than Dragon and PVS.

If you would like Nessus to start automatically when the system starts then place the above command in the following file:

/etc/rc.d/rc.local

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

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

nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

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

All plugins loaded
#
```

Alternatively, Nessus may be stared using the following command depending on the appropriate Operating System:

Operating System	Command to Start *nessusd*
Red Hat	# **/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**

After starting the *nessusd* service, Security Center users have completed the initial installation and configuration of their Nessus 3 scanner. If you are not using the Security Center 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, then use the following command which will also abruptly stop any on-going scans:
killall nessusd

Users of Nessus on Solaris will use the following command to stop the nessusd service:
/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 if needed. 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 you use an alternate configuration file instead of the standard */opt/nessus//etc/nessus/nessusd.conf*.
-a <address>	When staring the *nessusd* server, this option is used to tell the server to only listen to connections on the address <address> which 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* should 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 staring the *nessusd* server, this option will make the server run in the background (daemon mode).
-v	Display the version number and exit.
-h	Show a summary of the commands and exit.

An example of the usage is shown below:

/opt/nessus/sbin/nessusd [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]

Installing the Plugin Activation Code

When starting the Nessus service for the first time the Nessus plugins that where included with the install package are compiled, therefore this process may require a little time before the initial start-up is completed.

Depending on your subscription service, you will have received an activation code which entitles you to either the direct feed of plugins or the registered, seven-day delayed feed of plugins. If you have purchased a direct feed, you can use in the activation code you have received from Tenable. Users who have downloaded Nessus from the regular download page should have received an email containing an activation code for the registered feed. Otherwise, you can go to http://www.nessus.org/register to register your Nessus scanner in order to receive a plugin activation code for the registered feed.

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

```
# /opt/nessus/bin/nessus-fetch --register <license code>
```

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.

```
# cat /opt/nessus/lib/nessus/plugins/plugin_feed_info.inc
PLUGIN_SET = "200510041848";
PLUGIN_FEED = "Release";
# /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.
# date
Thu Oct 13 11:15:35 EDT 2005
# cat /opt/nessus/lib/nessus/plugins/plugin_feed_info.inc
PLUGIN_SET = "200510131015";
PLUGIN_FEED = "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. Looking at this file helps you ensure that you have the latest plugins available depending on the type of feed you have.

Tenable Security Center users should refer to their Security Center Documentation for the configuration of a centralized plugin feed for multiple Nessus scanners.

If a fresh install of a Nessus scanner is required because of a machine or software failure and a Security Center is already configured with correct user credentials to log into the scanner, then a conflict may occur between the Security Center and the Nessus scanner.

This happens when the Security Center attempts to push new plugins to the scanner at the same time the Nessus service is starting for the first time because the Nessus service is compiling the plugins it was shipped with. It is better to remove the association of the Nessus scanner with the Security Center in the Security Center settings and add it back after the Nessus service has been successfully started or temporarily stop the Security Center services and restart them after the Nessus service has been started successfully.

Connecting with a Client

Now the Nessus server is ready to be connected to with a client. There are multiple ways to connect to the Nessus server depending on your type of system. NessusWX is a client available for Windows platforms and NessusClient is an X11/GTK GUI. Command line operation can also be used instead of a client. Information on all of these is available in the "Nessus Client Guide".

Updating Plugins

The commands for this section assume that Nessus is installed in the directory */opt/nessus/*. If you are using a version for FreeBSD, Nessus is installed in the directory */usr/local/nessus/*. Therefore "*/usr/local/nessus/*" must replace "*/opt/nessus/*" in every command.

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

```
# /opt/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 often.

How Often Should I Update Plugins?

In general, updating your Nessus plugins once a day should be sufficient for most organizations. If you absolutely need the most current plugins and intend to update continuously throughout the day, then you should not update more than once every four hours as there is virtually no benefit in updating more than this.

Updating Plugins Automatically

There is a new feature in version 3.0 where Nessus will now 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 have to make sure that the scanner has a plugin feed activation code that is correctly registered. Use the following command to verify this:

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

Automatic plugins updates are only tried if:

- The `auto_update` option is set to yes in the *nessusd.conf* file;
- The plugins 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 Security Center.

Note that an offline plugins feed registration will not set 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 any thing else.

When configuring cron for plugins 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 downloads then.

Nessus without Internet Access

The commands for this section assume that Nessus is installed in the directory */opt/nessus/*. If you are using a version for FreeBSD, Nessus is installed in the directory */usr/local/nessus/*. Therefore "*/usr/local/nessus/*" must replace "*/opt/nessus/*" in every command.

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.

Register your Nessus Scanner

If you have not received an activation code, you need to register your Nessus scanner. Do this by going to http://www.nessus.org/register/ and enter your email address. You will then receive an activation code for the registered feed. For an activation code for the direct feed of plugins please contact Tenable at sales@tenablesecurity.com.

Then, on the system running Nessus type the following command:

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

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

```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Then with a browser, go to https://plugins.nessus.org/offline.php and copy and paste the “challenge” string as well as the activation code that you received previously into the appropriate text boxes. This will produce a URL which will give you direct access to the Nessus plugin feed, as well as a file called *nessus-fetch.rc*. Copy this file to the host running Nessus in the directory */opt/nessus/etc/nessus/*. Save this URL because you will use it every time you update your plugins.

Receive Up-to-date Plugins

You can obtain the newest plugins by going to the URL that was provided in the previous step. Here, you will receive a tarball (i.e. all-2.0.tar.gz). Copy the tarball to the Nessus scanner and then type the following command:

```
# tar -zxvf all-2.0.tar.gz -C /opt/nessus/lib/nessus/plugins/
```

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, and copy it to the system running Nessus.

Working with the Security Center

What is the Security Center?

Tenable offers an enterprise vulnerability and security management tool named the “Security Center”. With regard to Nessus, the Security Center allows multiple scanners to be used in concert to scan virtually any size network on a periodic basis.

The Security Center allows for 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. The Security Center also receives data from many leading intrusion detection systems such as Snort and ISS.

The Security Center can also receive passive vulnerability information from Tenable’s Passive Vulnerability Scanner (formerly NeVO) such that end users can discover new hosts, applications, vulnerabilities, and intrusions without the need for active scanning with Nessus.

Configuring Nessus

To enable any Nessus scanner for control by the Security Center, a specific username and password must be available to upload plugins and perform a scan.

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

A slight modification of the Nessus scanner is required prior to working with the Security Center. This involves editing the Nessus configuration file (*nessusd.conf*), which is usually located in at */opt/nessus/etc/nessus/nessusd.conf*.

For whichever user the Security Center will use to access this Nessus scanner, that username should be made an administrator. To do this, change the line in the *nessusd.conf* file which specifies the *admin_user* variable with a setting of the username used to log into the Nessus scanner by the Security Center. This is the user that is created in Nessus when the `nessus-add-first-user` command is used. In addition, the variables *plugin_upload* and *plugin_upload_suffixes* are also required to be enabled and to allow uploading of NASL scripts as well as their "include" files as shown in the example below for a user named "admin".

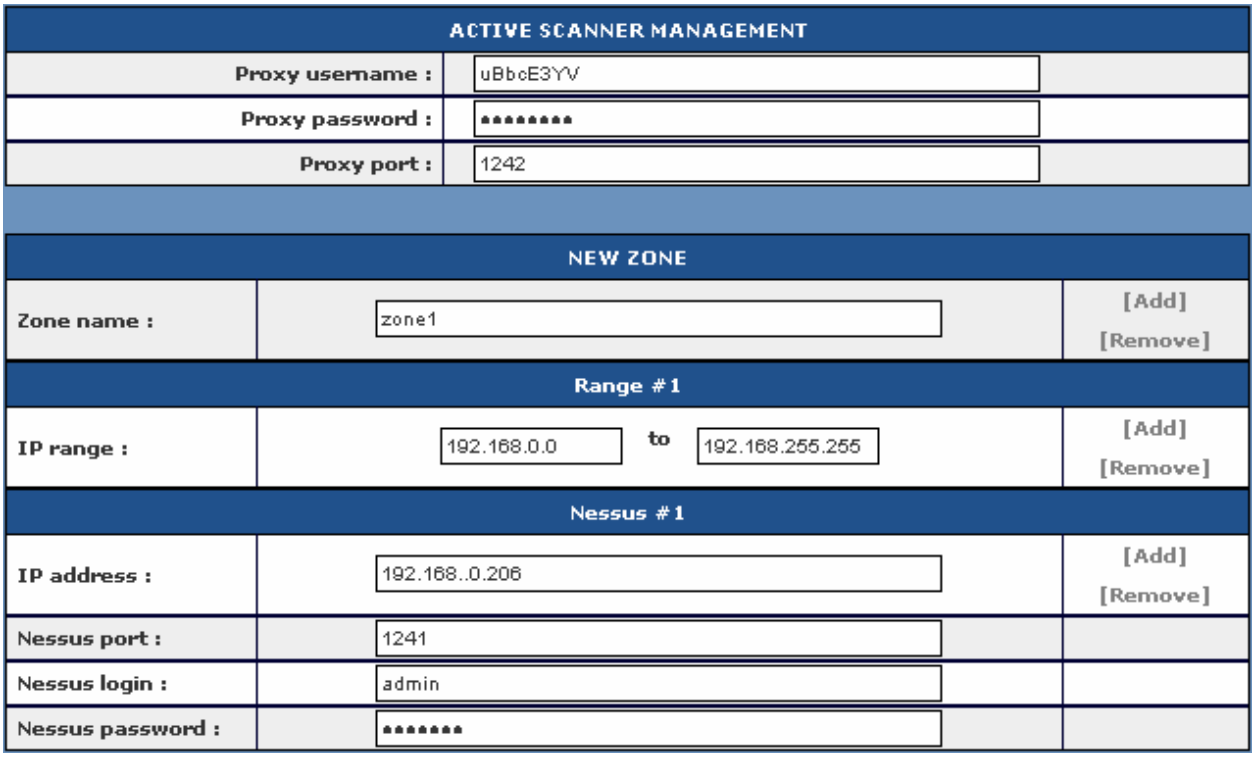
```
admin_user = admin
plugin_upload = yes
plugin_upload_suffixes = .nasl, .inc
```

The Nessus scanner must be restarted for these changes to take effect. It can be restarted with the `kill` command as in `kill –HUP <process id of nessusd>`.

Configuring the Security Center

At the Security Center, a "Nessus Server" can be added through the administration interface. Using this interface, Security Center can be configured to access and control virtually any Nessus scanner. Click on the "Console" tab and then click on "Add/Remove a Nessus Scanner". The Nessus scanner's IP address, administrative login ID, and password (created when installing/configuring Nessus) is required, as well as the associated zone and network IP range that the scanner will be tasked with covering. The network IP range is applicable when Security Center initiates a scan; only IP addresses that fall within this range will be scanned by this particular Nessus system. Multiple Nessus systems per Security Center system are not only possible, but recommended.

An example screen shot of the Security Center interface is shown below:



For more information please see the “Security Center Documentation”.

Removing Nessus

Red Hat and SUSE

Before you remove the package, stop the *nessusd* service by using the command:

```
# killall nessusd
```

In order to remove the package, you must first determine what package name Nessus is registered as within the system’s RPM database. This name will not be the same as the filename used for installation. Use the following command to determine the <package name>:

```
# rpm –qa | grep Nessus
```

The following is example output for the previous command:

```
Nessus-3.0.5-es3
```

Then, to remove the Nessus package on a Red Hat or SUSE system the command is:

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

For example, with the package name that was determined in the previous step the command to uninstall Nessus installed on Red Hat ES3 is:

rpm -e Nessus-3.0.5-es3

This 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. In order to completely remove the remaining files use the following command:

rm -rf /opt/nessus

Debian

Before you remove the package, stop the *nessusd* service by using the command:

killall nessusd

In order to remove the package, you must first determine what package name Nessus is registered as within the system's database. This name will not be the same as the filename used for installation. Use the following command to determine the package name:

dpkg –l | grep nessus

The following is example output for the previous command:

```
ii  nessus         3.0.5      Version 3 of the Nessus Scanner
```

Then, to remove the Nessus package on a Debian system the command is:

dpkg -r <package name>

For example, with the package name that was determined in the previous step the command to uninstall Nessus is:

dpkg -r nessus

This 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. In order to completely remove the remaining files use the following command:

rm -rf /opt/nessus

Solaris

Before you remove the package, stop the *nessusd* service by using the command:

/etc/init.d/nessusd stop

To remove the package, you must first determine what package name Nessus is registered as within the system's database. This name will not be the same as the filename used for installation. Use the following command to determine the package name:

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>

For example, with the package name that was determined in the previous step the command to uninstall Nessus is:

pkgrm TNBLnessus

This 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.

To completely remove all Nessus files, including those locally modified, run the following command:

rm –rf /opt/nessus

FreeBSD

Before you remove the package, stop the *nessusd* service by using the command:

killall nessusd

In order to remove the package, you must first determine what package name Nessus is registered as within the system's database. This name will not be the same as the filename used for installation. Use the following command to determine the package name:

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-3.0.5        A powerful security scanner
```

Then, to remove the Nessus package on a FreeBSD system the command is:

pkg_delete <package name>

For example, with the package name that was determined in the previous step the command to uninstall Nessus is:

pkg_delete Nessus-3.0.5

This 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. In order to completely remove the remaining files use the following command:

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

Enterasys Dragon IDS

Before you remove the package, stop the *nessusd* service by using the command:

```
# killall nessusd
```

Remove the Nessus package with the following command:

```
# /opt/nessus/scripts/nessus-remove
```

This script removes the package and cleans up any files left behind from Nessus in */opt*.

Windows

Upgrading Nessus

As newer versions of Nessus Windows are released by Tenable, upgrading is accomplished by downloading the executable installation file onto the system and running the InstallShield Wizard. There is no need to un-install the previous 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.

For users of NeWT, the InstallShield Wizard will upgrade NeWT to Nessus Windows. It will also move the old reports and address book to the new directory. Therefore, there is no reason to uninstall NeWT before installing Nessus Windows.

Installation

Downloading Nessus

The latest version of Nessus is available at http://www.nessus.org. The public is required to enter in contact information to obtain the Nessus software. Nessus customers can request a static download site if they require it. Nessus distribution file sizes and names vary slightly from release to release, but are approximately 14 MB in size.

Self Installing Executable

Nessus is distributed as an executable installation file. The file should be placed onto the system it is being installed upon. This will install both the server and the client.

Installing as an Administrator

For Windows 2000 and Server 2003 systems, Nessus should only be installed using an administrative account and not by a user of less privilege.

Answering the Installation Questions

Nessus will prompt the user for some basic information such as installation directory location.

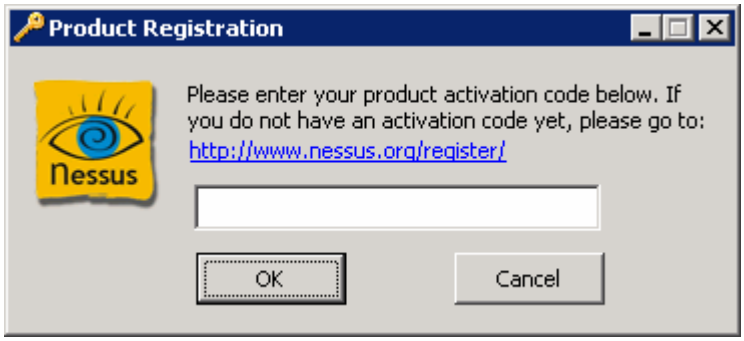
Installing the Plugin Update Activation Code

Next, a window will prompt the user to enter the product registration code.

Depending on your subscription service, users who have obtained Nessus from Tenable should have received an email containing a registration code which entitles you to either the direct feed of plugins or the registered, seven-day delayed feed of plugins. This synchronizes your Nessus with all of the plugins available on the registered feed or direct feed.

Users who have obtained Nessus from Tenable Network Security, Inc. and have received an email containing an activation code should select "yes" and then enter the code into the next window.

To enable your Nessus from the start menu, find the Nessus set of programs and invoke the "Product Registration" application. This will produce a simple dialogue as shown below:

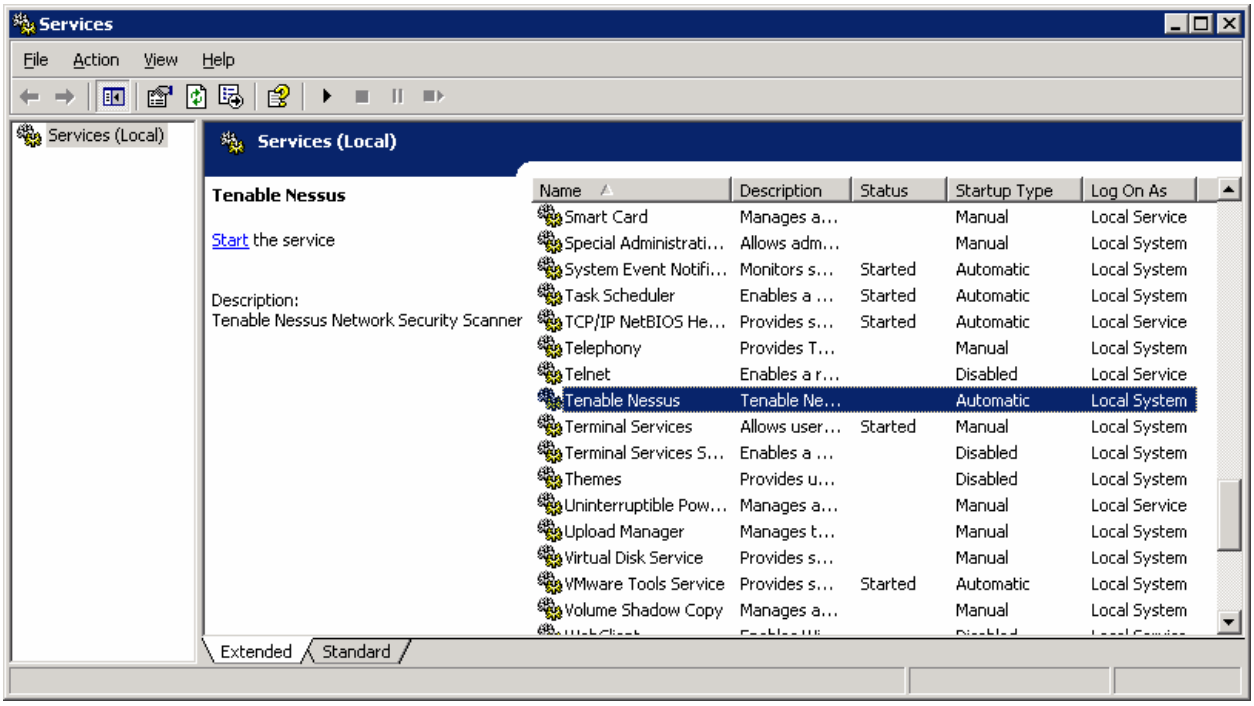


If you have obtained an activation code for your Nessus, enter it in this dialogue box and then click "OK". If you change your registration code at a later time, simply re-enter the code into this application. The changes do not go into effect until the next time an update of the plugins occurs.

If you do nothing, your Nessus will use the default feed which is GPL.

Tenable Nessus Service

Nessus requires a Windows service to perform the vulnerability scans. Upon installation, the "Tenable Nessus" service will be installed, configured to automatically start if the system reboots, and launched. To view this service, as an administrator, log onto the "Control Panel", select the "Administrative Tools", and then select the "Services" shortcut. The "Tenable Nessus" services should be listed as shown below:



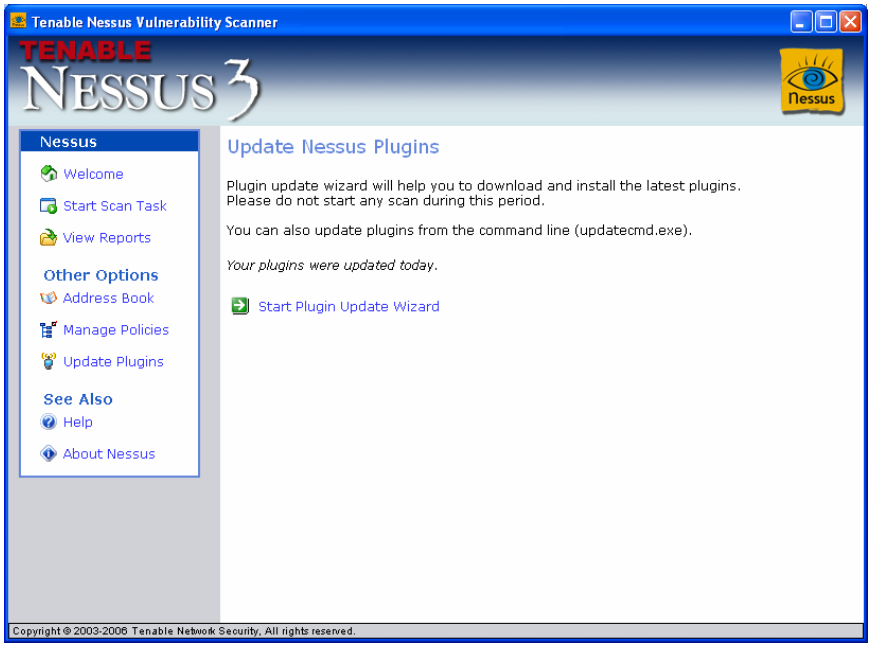
This service can be configured to be launched manually, but the Nessus user must then remember to start it before performing a scan. If the "Tenable Nessus" service is not running, the following error will be displayed when a scan is launched:

Updating Plugins

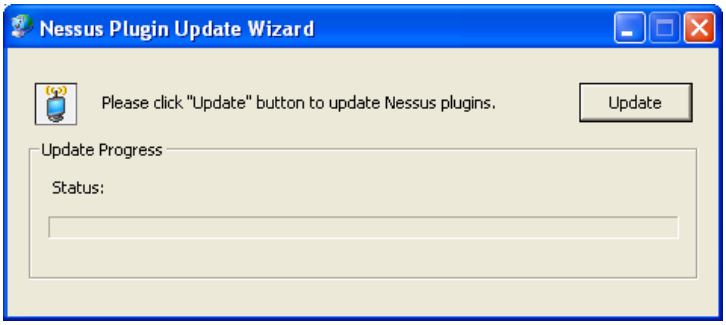
Nessus has thousands of plugins (or scripts) that test for network and host vulnerabilities. New vulnerabilities are regularly being discovered and new plugins are developed to detect these vulnerabilities. To keep your Nessus scanner up-to-date with the latest plugins, making your scans as accurate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

Tenable distributes the latest vulnerability plugins in two modes for Nessus. These are the direct and the registered feed. These are discussed in more detail in the section "Vulnerability Plugin Subscriptions" located earlier in this document.

Nessus has an update wizard that will automatically retrieve the latest vulnerability plugins. To perform an update, click on “Update Plugins” from the menu on the left. On the Update Plugins page, select “Start Plugin Update Wizard”:



Click “Update” in the Nessus Plugin Update Wizard:



Nessus organizes its vulnerability checks by “plugin” and “plugin family”. If a family is turned on completely, all of the plugins within that family are enabled. When the plugins are updated, any new plugins within this family will be automatically enabled. If some or none of the individual plugins within a family are enabled and there are new plugins added during and update, they will not be automatically enabled and must be manually enabled.

Updating Plugins through Web Proxies

Nessus Windows supports product registration and plugins updates through web proxies that require basic authentication or Windows Integrated Authentication. When updating plugins or registering activation codes, the user should be presented with a pop-up window asking for login credentials. For example, after following the steps to perform a plugins update in the previous section, a new window should pop-up asking for the web proxy credentials:

Once the user name and password have been entered, Nessus should begin looking for and downloading new plugins.

Nessus Windows cannot support proxy authentication which would redirect a web-browser to a page where credentials would be entered. Although Nessus uses Internet Explorer settings for some of its configuration, it is not a browser and cannot support this functionality.

How Often Should I Update Plugins?

In general, updating your Nessus plugins once a day should be sufficient for most organizations. If you absolutely need the most current plugins and intend to update continuously throughout the day, then you should not update more than once every four hours as there is virtually no benefit in updating more than this.

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.

Register your Nessus Scanner

If you have not received an activation code, you need to register your Nessus scanner. Do this by going to http://www.nessus.org/register/ and enter your email address. You will then receive an activation code for the registered feed. For an activation code for the direct feed of plugins please contact Tenable at sales@tenablesecurity.com.

With a browser, go to http://plugins.nessus.org/manual-register.php and copy and paste the activation code that you received previously. This will produce a link which will give you direct access to the Nessus plugin feed. Save this link because you will use it every time you update your plugins.

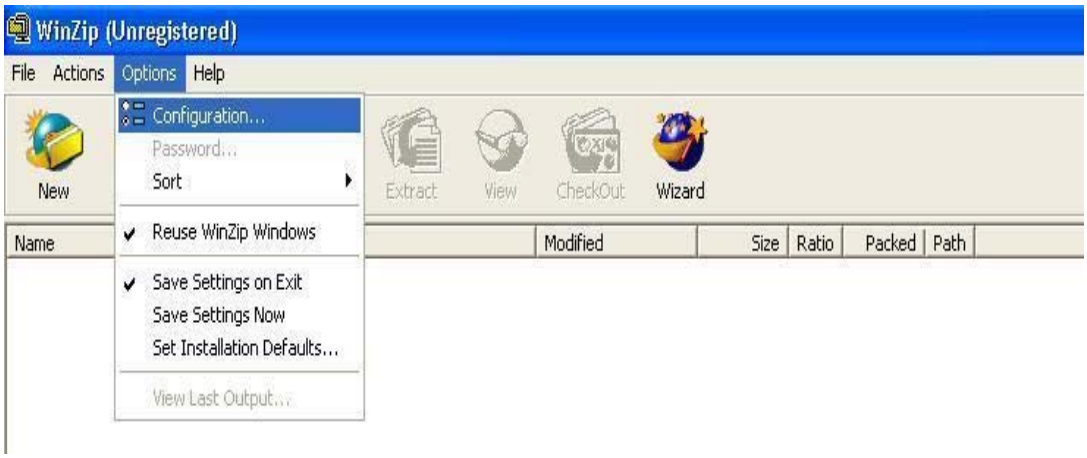
Receive Up-to-date Plugins

You can obtain the newest plugins by going to the URL that was provided in the previous step. Here, you will receive a tarball (i.e. all-2.0.tar.gz). Copy the tarball to the Nessus scanner.

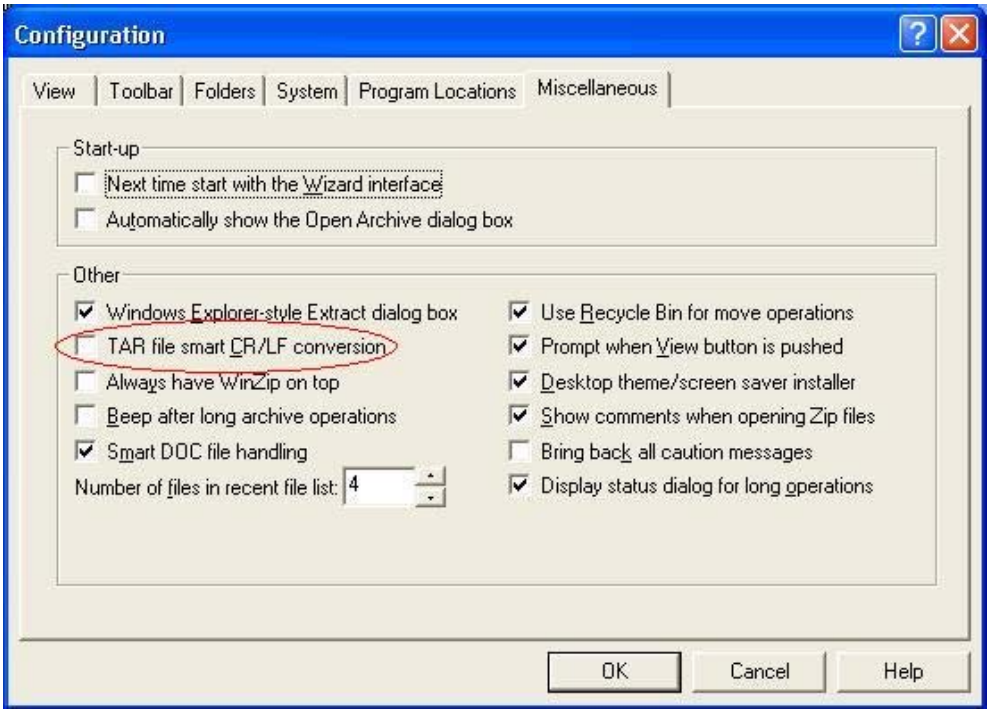
Next, you will need to extract the plugins to the directory C:*Program Files**Tenable**Nessus**plugins**scripts*.

Note: There is a known issue with some decompression utilities automatically using CR/LF Conversion. The resolution for this is to simply disable this feature.

For example, if WinZip is used, before you unzip the plugins perform the following steps. First, open WinZip, and go to the "Options" menu and click on "Configuration" as shown below:



On the "Miscellaneous" tab, uncheck the "TAR file smart CR/LF conversion" checkbox, and then click "OK" as shown below:



After you have confirmed the placement of the new plugins in the directory mentioned above, run the following command:

```
C:\Program Files\Tenable\Nessus\build.exe
```

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, and copy it to the system running Nessus.

Working with the Security Center

What is the Security Center?

Tenable offers an enterprise vulnerability and security management tool named the "Security Center". With regard to Nessus, the Security Center allows multiple scanners to be used in concert to scan virtually any size network on a periodic basis.

The Security Center allows for 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. The Security Center also receives data from many leading intrusion detection systems such as Snort and ISS.

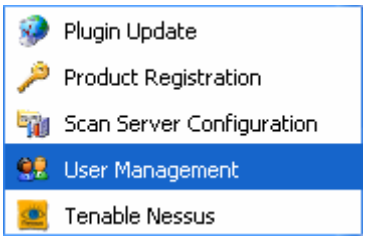
The Security Center can also receive passive vulnerability information from Tenable's Passive Vulnerability Scanner (formerly NeVO) such that end users can discover new hosts, applications, vulnerabilities, and intrusions without the need for active scanning with Nessus.

Configuring Nessus to Listen as a Network Daemon

Nessus can be configured to communicate with the Security Center. To do this, we need to complete two tasks. We need to add an account for the Security Center to log into Nessus with, and then we need to enable Nessus to listen to inbound network connections from the Security Center as well. By default, Nessus only listens to localhost connections and we need to configure it to be bound to a specific network interface.

Adding User Accounts

To manage the user accounts for Nessus, invoke the "User Management" tool which is accessible from the Start button by following the Start / All Programs / Tenable Network Security / Nessus series of options as shown below:



Please note that user accounts for Nessus refer to a specific username and password to be used by the Security Center to log in remotely to launch scans and retrieve vulnerability data.

Choose a unique username and password to be used by the Security Center and keep it handy when adding this Nessus to the Security Center.

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 the Security Center.

Enabling Network Connections

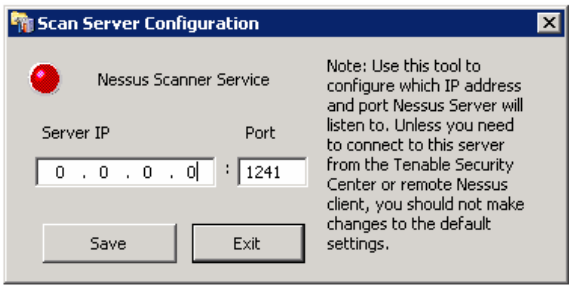
To allow a remote connection to Nessus from the Security Center, run the "Scan Server Configuration" tool. This tool allows the port and bound interface of the Nessus daemon to be configured. By default, the Nessus daemon listens to connections on localhost (127.0.0.1) and port 1241.

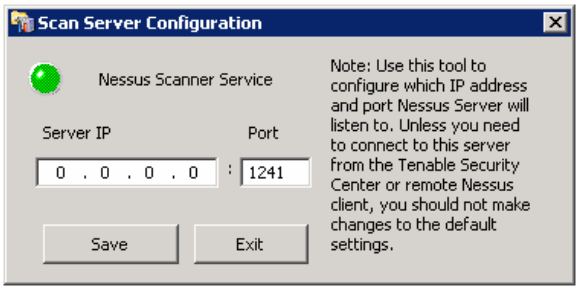
To enable connectivity from the Security Center, Nessus must be configured to listen for connections either on one network interface, or any interface. Type in the IP address of the Nessus network interface it should be bound to.

- If your server only has one IP address and network card, then type in that IP address.
- If your server has multiple IP addresses and you only want it to listen for connections on port 1241 on one of those, type in the IP address of that interface.
- If your server has multiple IP addresses and you want it to listen on all interfaces, use an IP address of 0.0.0.0.

Here are two screen shots of the "Scan Server Configuration" tool. They both have been bound to all network cards with an IP address of 0.0.0.0, and they are both listening on port 1241.

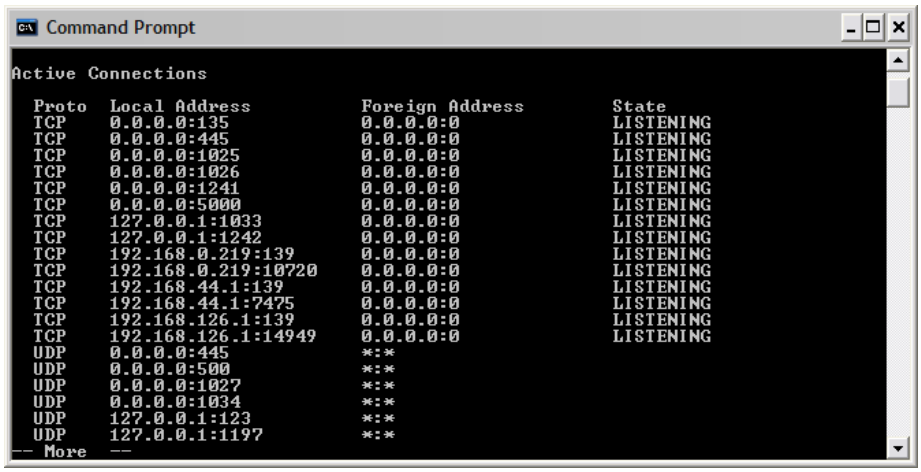
The image on the left with the red indicator shows that the “Tenable Nessus” service is not running. Clicking on the red button will start the service. If this is attempted, the indicator will turn yellow and then green if successful.





Any change to the information in the dialogue box of the “Scan Server Configuration” tool will also prompt the user to see if they want to restart the “Tenable Nessus” service.

To verify that Nessus is indeed listening on port 1241, from the Windows command line use the *netstat –an* command as shown below:



Notice that the fifth TCP line contains “0.0.0.0:1241” which means a server is listening on that port.

Host-Based Firewalls

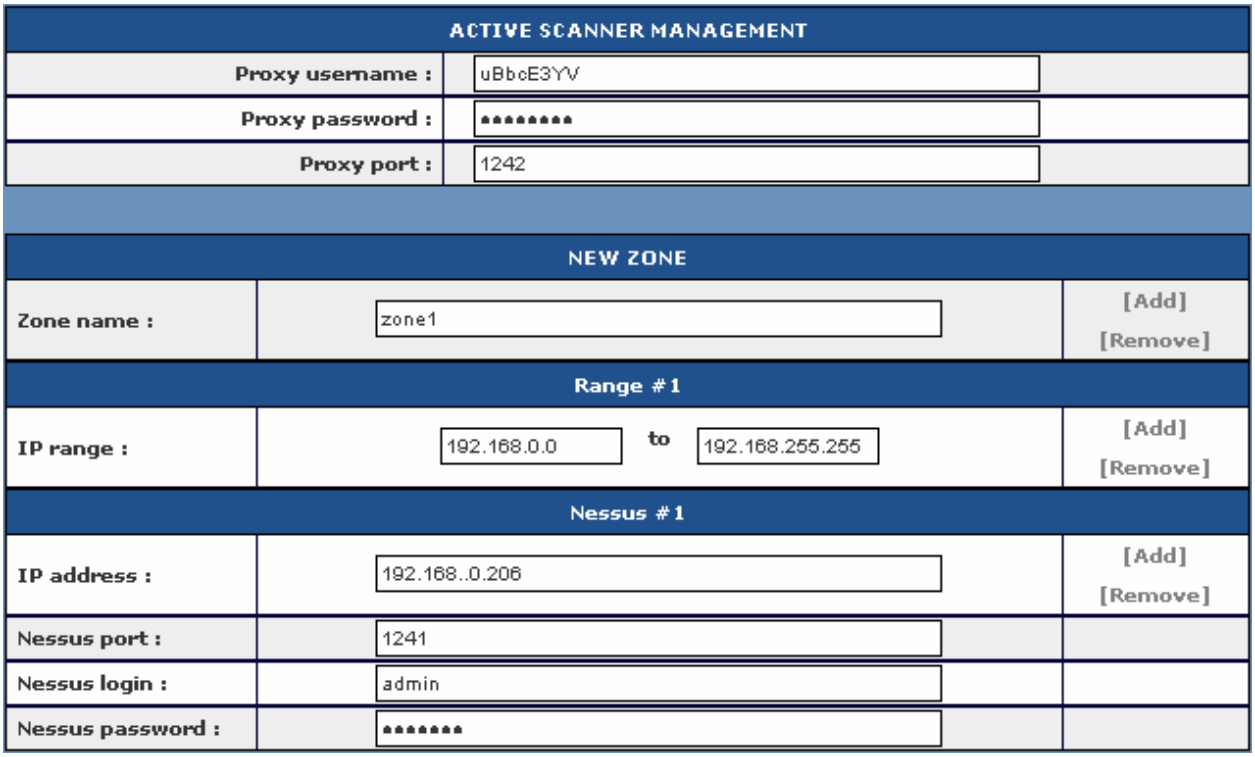
If your Nessus server is configured with a local firewall such as Zone Alarm, Sygate, BlackICE, the Windows XP firewall, or any other, it is required that connections be opened from the Security Center’s IP address.

By default, port 1241 is used. On Microsoft XP service pack 2 systems running the “Security Center” icon available in the Control Panel will present 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 the Security Center

At the Security Center, a “Nessus Server” can be added through the administration interface. Using this interface, Security Center can be configured to access and control virtually any Nessus scanner. Click on the “Console” tab and then click on “Add/Remove a Nessus Scanner”. The Nessus scanner’s IP address, administrative login ID, and password (created when installing/configuring Nessus) is required, as well as the associated zone and network IP range that the scanner will be tasked with covering. The network IP range is applicable when Security Center initiates a scan; only IP addresses that fall within this range will be scanned by this particular Nessus system. Multiple Nessus systems per Security Center system are not only possible, but recommended.

An example screen shot of the Security Center interface is shown below:



For more information please see the “Security Center Documentation”.

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.

Mac OS X

Upgrading from Nessus 3.x

Upgrading from an older version of Nessus 3.x is similar to doing a fresh install. However, you will need to stop and restart the Nessus server at the end of the installation.

Upgrading Nessus 2.x to Nessus 3.x

This section will explain how to upgrade a Nessus 2.x installation to Nessus 3.x.

If you have compiled Nessus 2.x yourself on Mac OS X, you can easily upgrade to Nessus 3.x. It is even possible to make your Nessus 2 and Nessus 3 installations coexist peacefully on the same host since Nessus 3 is installed under a different directory (*/Library/Nessus*) than the default installation path of Nessus 2 (typically, */usr/local*). However, the two processes can not run at the same time.

If your older version of Nessus 2 is registered, you will need to copy over the *nessus-fetch.rc* configuration file instead of re-registering.

Nessus 2 and Nessus 3 are installed under different paths; because of this they can be installed on the same system at the same time. The first step in upgrading your Nessus 2 to Nessus 3 is to stop the Nessus 2 installation's *nessusd* service using the following command:

```
# killall nessusd
```

The command `killall nessusd` will abruptly stop any on-going scans.

Next, install Nessus 3 by following the instructions in the section called "Installation" located later in this document.

Next, you must copy the users from Nessus 2 into Nessus 3. User management is directory based in Nessus, so moving user accounts is fairly straightforward. Copy the users with the command as follows:

```
# cp –r /usr/local/var/nessus/users/* /Library/Nessus/run/var/nessus/users/
```

Next, you must copy the file *nessus-fetch.rc* to the appropriate Nessus 3 directory to save your plugin activation code. If you do not, you will have to contact Tenable Support in order to have the activation code reset. Copy the file with the command below:

```
# cp /usr/local/etc/nessus/nessus-fetch.rc
/Library/Nessus/run/var/nessus/etc/nessus/
```

Then, make sure the permissions are as follows:

```
-rw-------  1 root root 398 Nov  3 03:12 nessus-fetch.rc
```

The next step is to edit the file */Library/Nessus/run/etc/nessus/nessusd.conf* to make sure that the `admin_user` is set properly. To do this, make sure that that the following options are correct:

```
plugin_upload = yes
admin_user = <ADMIN>
```

Where <ADMIN> is the name of the admin user defined in the Nessus 2 file */usr/local/etc/nessus/nessud.conf*.

Now you are ready to configure Nessus 3, start the Nessus server, and run a scan using one of the client options. This is all described later in this document as well as in the "Nessus Client Guide".

Finally, once you have verified that Nessus 3 is configured and running properly, the last step is to uninstall Nessus 2.x with the following command:

/usr/local/sbin/uninstall-nessus

Installation

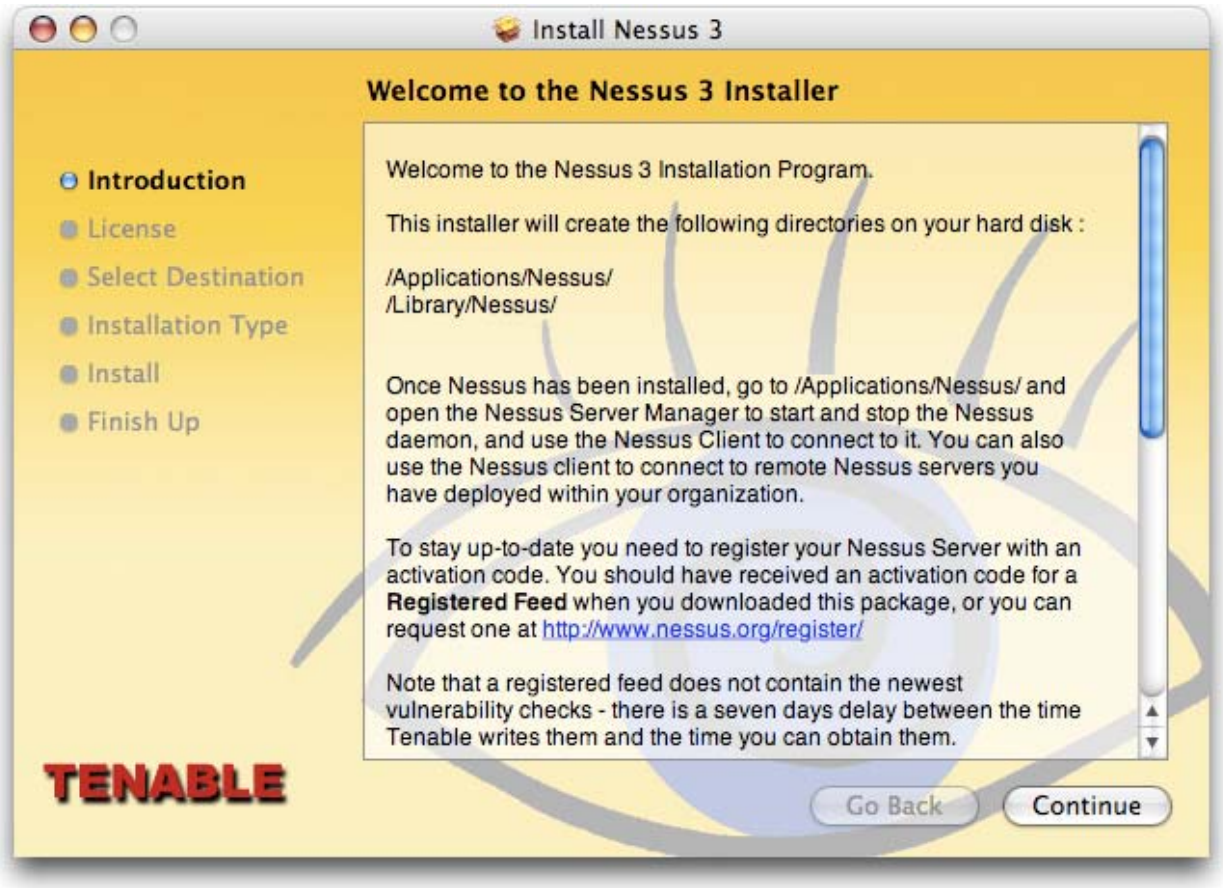
The latest version of Nessus is available from http://www.nessus.org/download/. Nessus is available for Mac OS X 10.4.

To install Nessus on Mac OS X, you need to download the file *Nessus-3.x.x.dmg.gz*, and then double click on it to mount it on the desktop. Once the volume "Nessus 3" appears on the desktop, double click on the file *Nessus 3.mpkg* as shown below:

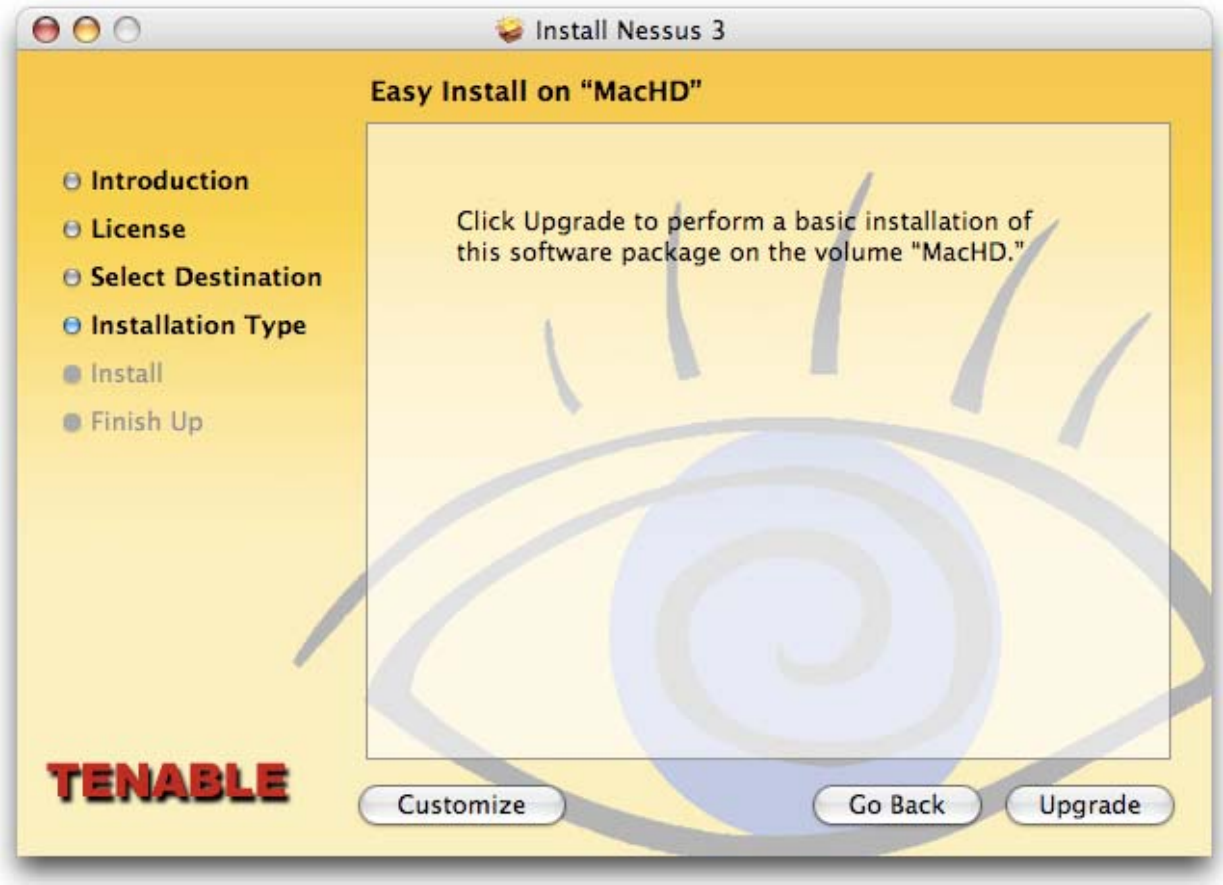
Nessus 3.mpkg

Once you double-click on it, simply follow the steps of the Installer.

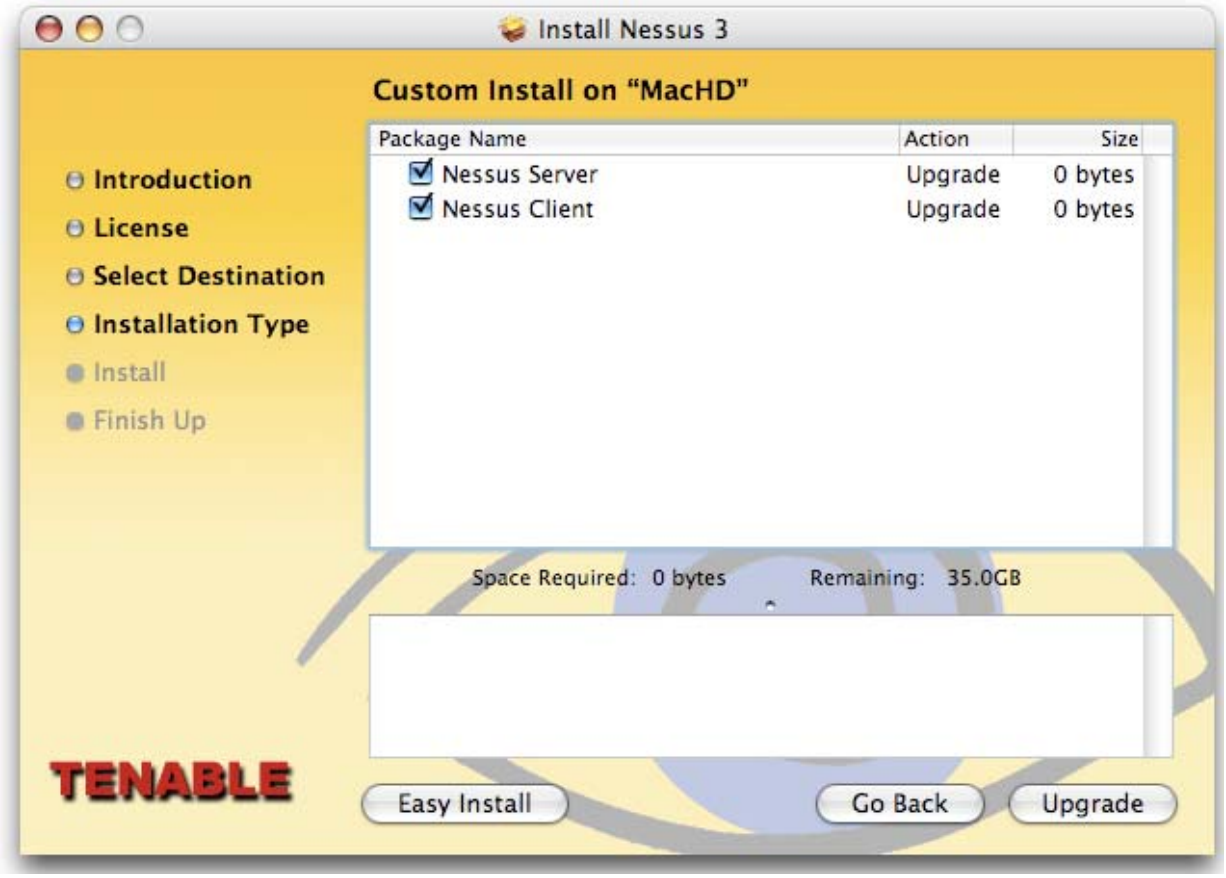
Note that you will be prompted for an administrator user name and password during the installation.



You can select to either install the Nessus server, client, or both buy selecting the "Customize" button in the installer when you reach the "Installation Type" step. By default, both modules are installed on the system.

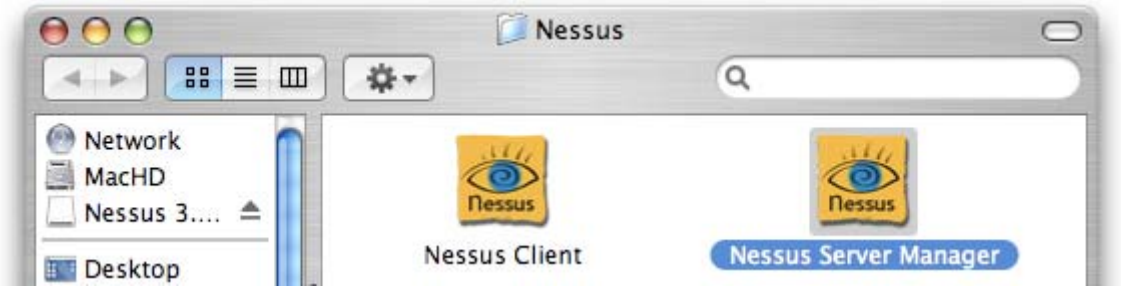


Clicking on “Customize” takes you to the following screen:



Configuration

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



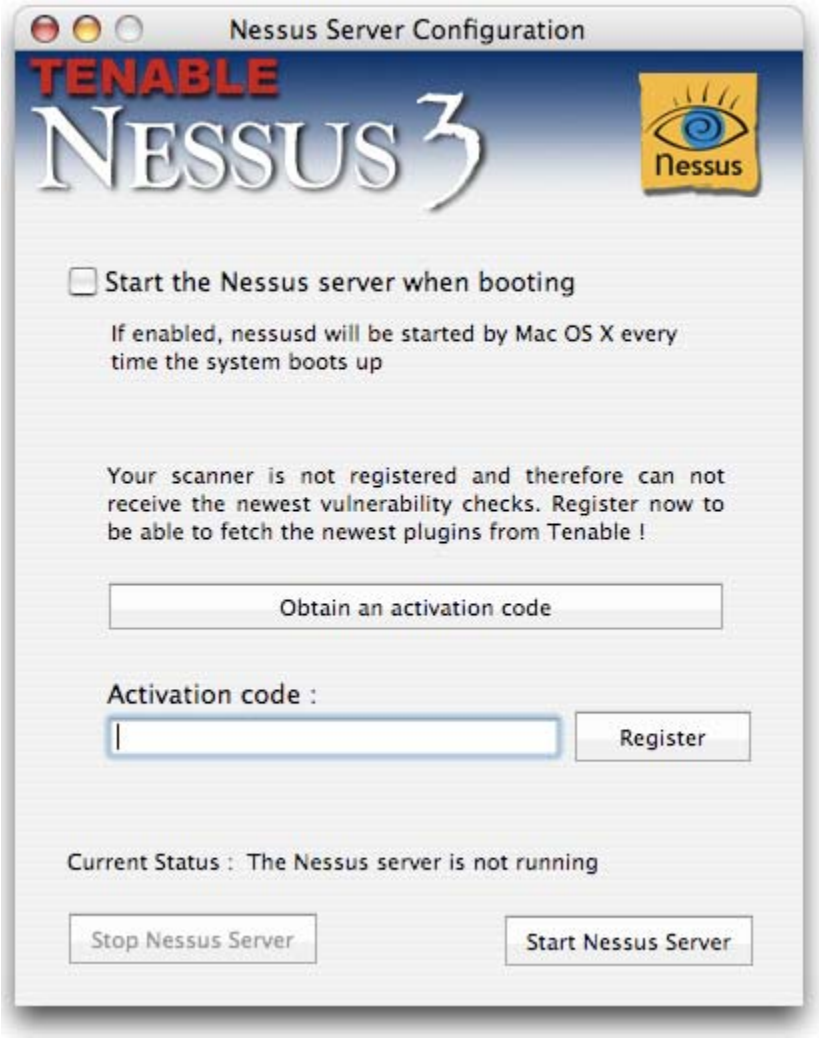
This program allows you to:

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

Whenever you start "Nessus Server Manager", you will be prompted for an administrator user name and password because interacting with the Nessus server

requires root privileges.

When you start the Nessus Server Manager, the initial screen looks like as follows:

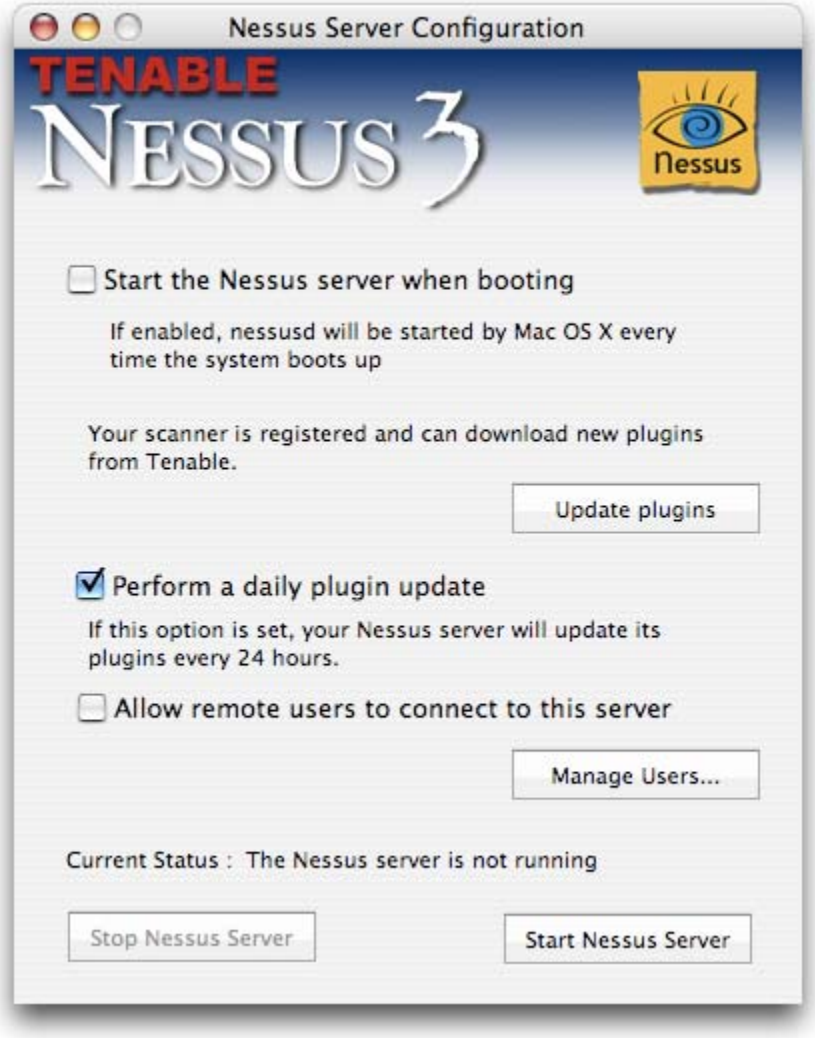


Registering your Nessus Installation

The first thing to do is to register your Nessus Server. Registering your server gives you access to the newest plugins from nessus.org and therefore makes sure your audits are up-to-date.

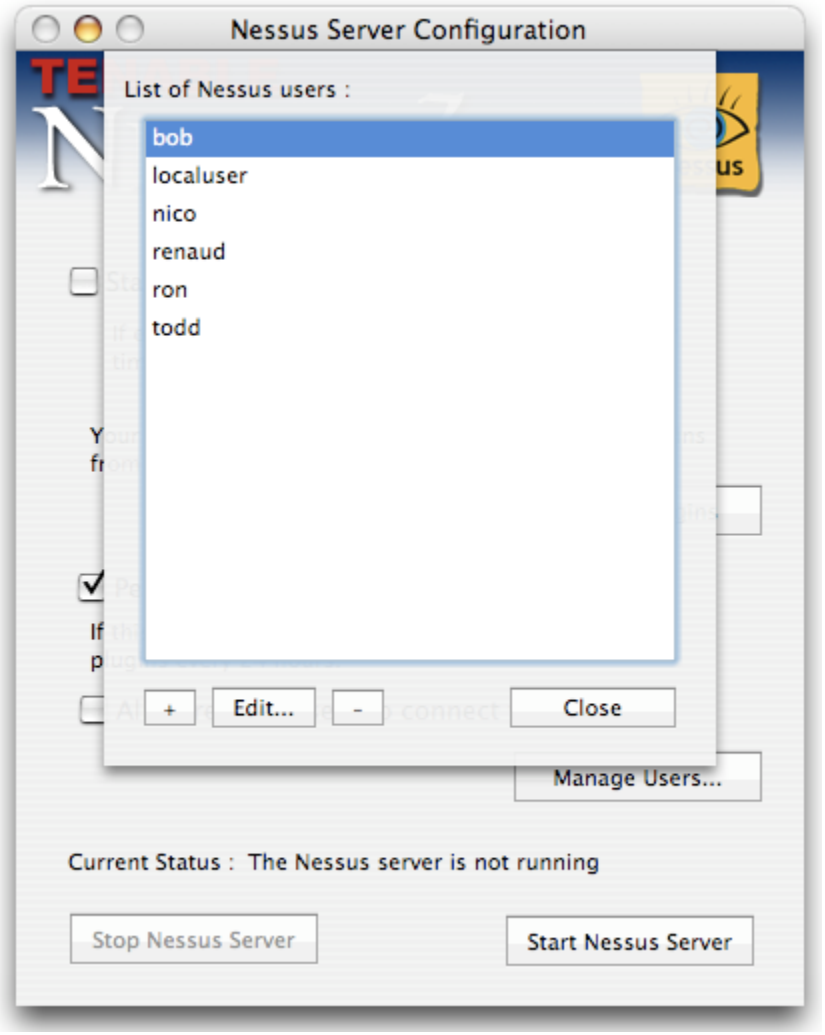
To register Nessus, obtain an activation code from http://www.nessus.org/register and enter it in the appropriate field. Then click on “Register”.

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



Create and Manage Nessus Users

If you intend your Nessus scanner to be used remotely (such as with the Security Center), you need to add users to it. To do so, click on the "Manager Users" button and you will be shown a list of users:



Unless you are experienced, you should never edit nor delete the user “localuser”, as it would break the *Local Connection* server in the Nessus Client.

To create a user, click on “+”. To delete a user, select the name of the user you want to delete and click on “-” button. To change the password of a user, select the user and click on the “Edit” button.

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.

Configure the Nessus Daemon (Advanced Users)

Skip this section if you are not familiar with the terminal.

In the file */Library/Nessus/run/etc/nessus/nessusd.conf* there are several options that can be configured. 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 is all specified, as well as many other options. This file is created

automatically with default settings, but these settings should be reviewed and modified appropriately based on your scanning environment.

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 Security Center or a Client for Nessus such as NessusWX. To view/change these options for a scan template in the Security Center, edit a Scan Template's Scan Options. In NessusWX, edit a Session's properties, 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 Security Center Scan Template or NessusWX Session Options when performing a scan via these tools.

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. The hardware configuration of the scanner system and other applications running on it should be taken into consideration 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 (your organization's policy on scanning, other network traffic, the affect a particular type of scan has on your scan target hosts, etc.), 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 Linux 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 scan 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 this should always be set relatively low.

Setting max_checks to a value of "3" would be adequate for most organizations, and rarely would it be set any higher than "4".

Launch the Nessus Daemon

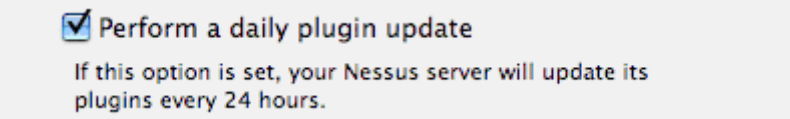
To start the Nessus daemon, click on the button "Start Nessus Server" in the Nessus Server Manager.

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

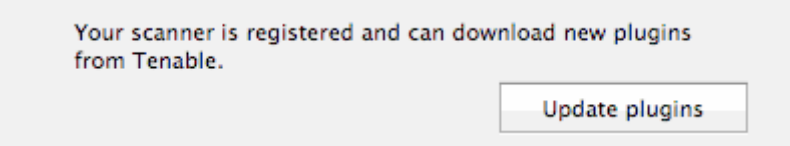
After starting the *nessusd* service, Security Center users have completed the initial installation and configuration of their Nessus 3 scanner and should continue to the section "Working with the Security Center".

Updating Plugins

If you enable the appropriate check box in the Nessus Server Manager tool, your Nessus server will update its set of plugins automatically every 24 hours as shown below:



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



How Often Should I Update Plugins?

In general, updating your Nessus plugins once a day should be sufficient for most organizations. If you absolutely need the most current plugins and intend to update continuously throughout the day, then you should not update more than once every four hours as there is virtually no benefit in updating more than this.

Nessus without Internet Access (Advanced Users)

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.

Register your Nessus Scanner

If you have not received an activation code, you need to register your Nessus scanner. Do this by going to http://www.nessus.org/register/ and enter your email address. You will then receive an activation code for the registered feed.

Then, on the system running Nessus type the following command:

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

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

```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Then, go to https://plugins.nessus.org/offline.php and copy and paste the “challenge” string as well as the activation code that you received previously into the appropriate text boxes. This will produce a link which will give you direct access to the Nessus plugin feed, as well as a file called *nessus-fetch.rc*. Copy this file to the host running Nessus in the directory */Library/Nessus/run/etc/nessus/*.

Receive Up-to-date Plugins

You can obtain the newest plugins by going to the URL that was provided in the previous step. Here, you will receive a tarball (i.e. all-2.0.tar.gz). Copy the tarball to the Nessus scanner and then type the following command:

```
# tar -zxvf all-2.0.tar.gz -C /Library/Nessus/run/lib/nessus/plugins/
```

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, and copy it to the system running Nessus.

Working with the Security Center

What is the Security Center?

Tenable offers an enterprise vulnerability and security management tool named the “Security Center”. With regard to Nessus, the Security Center allows scanners to be used in concert to scan virtually any size network on a periodic basis.

The Security Center allows for 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. Security Center also receives data from many leading intrusion detection systems such as Snort and ISS.

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

Configuring Nessus

To enable any Nessus scanner for control by the Security Center, a specific username and password must be available to upload plugins and perform a scan.

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

A slight modification of the Nessus scanner is required prior to working with the Security Center. This involves editing the Nessus configuration file (*nessusd.conf*), which is usually located in at */Library/Nessus/run/etc/nessus/nessusd.conf*.

For whichever user the Security Center will use to access this Nessus scanner, that username should be made an administrator. To do this, change the line in the *nessusd.conf* file which specifies the *admin_user* variable with a setting of the username used to log into the Nessus scanner by the Security Center. This is the user that is created in Nessus when the `nessus-add-first-user` command is used. In addition, the variables *plugin_upload* and *plugin_upload_suffixes* are also required to be enabled and to allow uploading of NASL scripts as well as their "include" files as shown in the example below for a user named "admin".

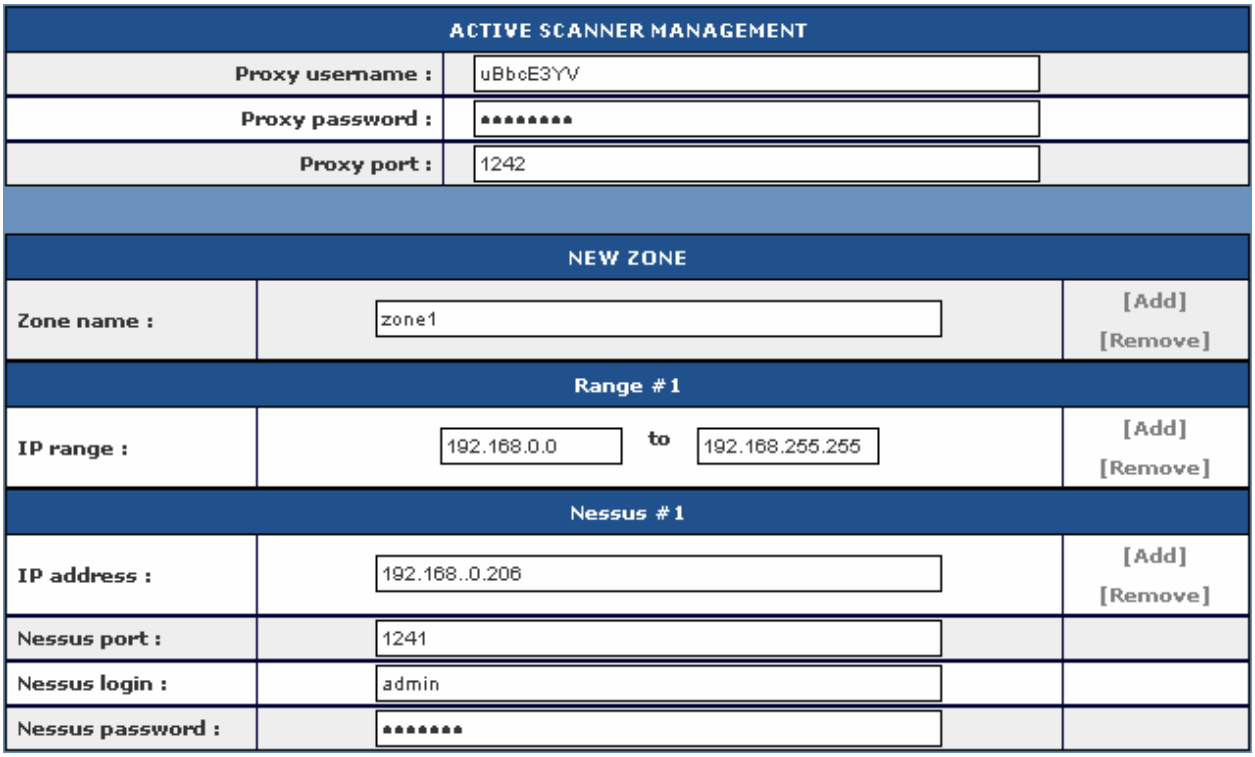
```
admin_user = admin
plugin_upload = yes
plugin_upload_suffixes = .nasl, .inc,.nbin,.audit
```

The Nessus scanner must be restarted for these changes to take effect. It can be restarted with the `kill` command as in `kill –HUP <process id of nessusd>`.

Configuring the Security Center

At the Security Center, a "Nessus Server" can be added through the administration interface. Using this interface, Security Center can be configured to access and control virtually any Nessus scanner. Click on the "Console" tab and then click on "Add/Remove a Nessus Scanner". The Nessus scanner's IP address, administrative login ID, and password (created when installing/configuring Nessus) is required, as well as the associated zone and network IP range that the scanner will be tasked with covering. The network IP range is applicable when Security Center initiates a scan; only IP addresses that fall within this range will be scanned by this particular Nessus system. Multiple Nessus systems per Security Center system are not only possible, but recommended.

An example screen shot of the Security Center interface is shown below:



For more information please see the “Security Center Documentation”.

Removing Nessus

To remove Nessus, the easiest way is to delete the following directories:

```
/Library/Nessus
/Application/Nessus
/Library/Receipts/Nessus*
```

A freeware tool called “DeInstaller.app” can also be used to remove the Nessus Client and Nessus Server packages.

For Further Information

Tenable hopes your experience with Nessus is very positive, and we strongly encourage you to contact us via email or phone to discuss any issues you have. Tenable has produced a variety of other documents detailing Nessus’ deployment, configuration, user operation, and overall testing. These are listed here:

- **Nessus Client Guide** – how to install, configure, and operate the various clients available for Nessus
- **Nessus Advanced User Guide** – elaborates on some of Nessus’ “dustier corners” by explaining additional features
- **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@tenablesecurity.com, sales@tenablesecurity.com or visit our web site at http://www.tenablesecurity.com. For more information about Nessus, please visit http://www.nessus.org.

This program uses the “libnessusrx” library which is released under the LGPL. The source code of this library is available at ftp://ftp.nessus.org/pub/libnessusrx/.

This product includes cryptographic software written by Eric A. Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptosft.com).

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

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.tenablesecurity.com.

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

Appendix 1: Nessus Windows Troubleshooting

Installation Issues

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 which both 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: While starting or operating Nessus Windows I receive the following error:

"A Runtime Error Has Occurred. Do you wish to debug?
Line 31: Error: Object doesn't support this property or method"

Clicking on Continue launches the debugger. If you choose not to debug by clicking "No", you are returned to the main Nessus screen.

Attempting subsequent Nessus operations, such as New Scan Task, returns the following error:

"Error: line 154"

Continuing through the above error message returns:

"No scan control"

Solution: COM registration for Nessus has failed on the system during installation. Since the installer can not fix the problem, please perform the following steps:

1. From Start menu, click on "All Programs", then "Accessories".
2. Right click on "Command Prompt" and select "Run as Administrator".
3. Type "cd c:\Program File\Tenable\Nessus".
4. Type "regsvr32 scan.dll".

The steps above will install the COM component manually. Nessus should now start and operate without issue.

Issue: When attempting to perform a scan using Nessus Windows I receive the following error message:

"Error: Automation server can't create object"

Or

"Error 1935. An error occurred during the installation of assembly "Microsoft.MSXML..."

Solution: This is an issue with the XML Parser on the system Nessus Windows is installed on. Either it is not up to date or it may need to be re-installed.

If the system is up to date, please refer to the following Microsoft knowledge base article for more information regarding the msxml.dll parser:

http://support.microsoft.com/kb/269238/

To re-install the MS XML Parser on the system, access a command prompt and execute the following command:

```
regsvr32 %windir%\system32\msxml4.dll
```

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. You should exclude the plugins directory from virus scans. 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 it 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: I am not able to use Nmap to conduct port scans as with previous versions of Nessus.

Solution: Please see the following URL:

http://www.nessus.org/documentation/index.php?doc=nmap-usage

Issue: I am not able to conduct a TCP Connect scan using Nessus Windows.

Solution: Because of the limitations of the Windows TCP/IP stack, Nessus Windows cannot perform TCP Connect scans.

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 false negative results when running Nessus Windows on a Windows XP system?

Solution: Microsoft has added changes to Windows XP Service Pack 2 (Home & 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://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx

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 which is found in the individual scan configuration for each scan policy:

Max number of hosts: 10
Max number of security checks: 4
Max number of packets per second for a port scan: 50

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

Appendix 2: Best Practices for the Enterasys Dragon IDS

The following are best practices to configure your Enterasys Dragon IDS appliance for use with Nessus and/or PVS.

Dragon Appliance Network Interface Configuration

You should have a Dragon appliance running Dragon 7.2 or later that has at least three network interfaces with one assigned to Dragon (eth0). PVS can be assigned to eth0, which is done during the configuration of PVS, along with Dragon. Eth1 can be used as the management interface and eth2 can be assigned to Nessus. You will need to edit the file */etc/rc.d/rc.inet1.conf* to add the other two IPs for eth1 and eth2. Reboot your system after you have completed making the change. An example of the *rc.inet1.conf* file is shown below:

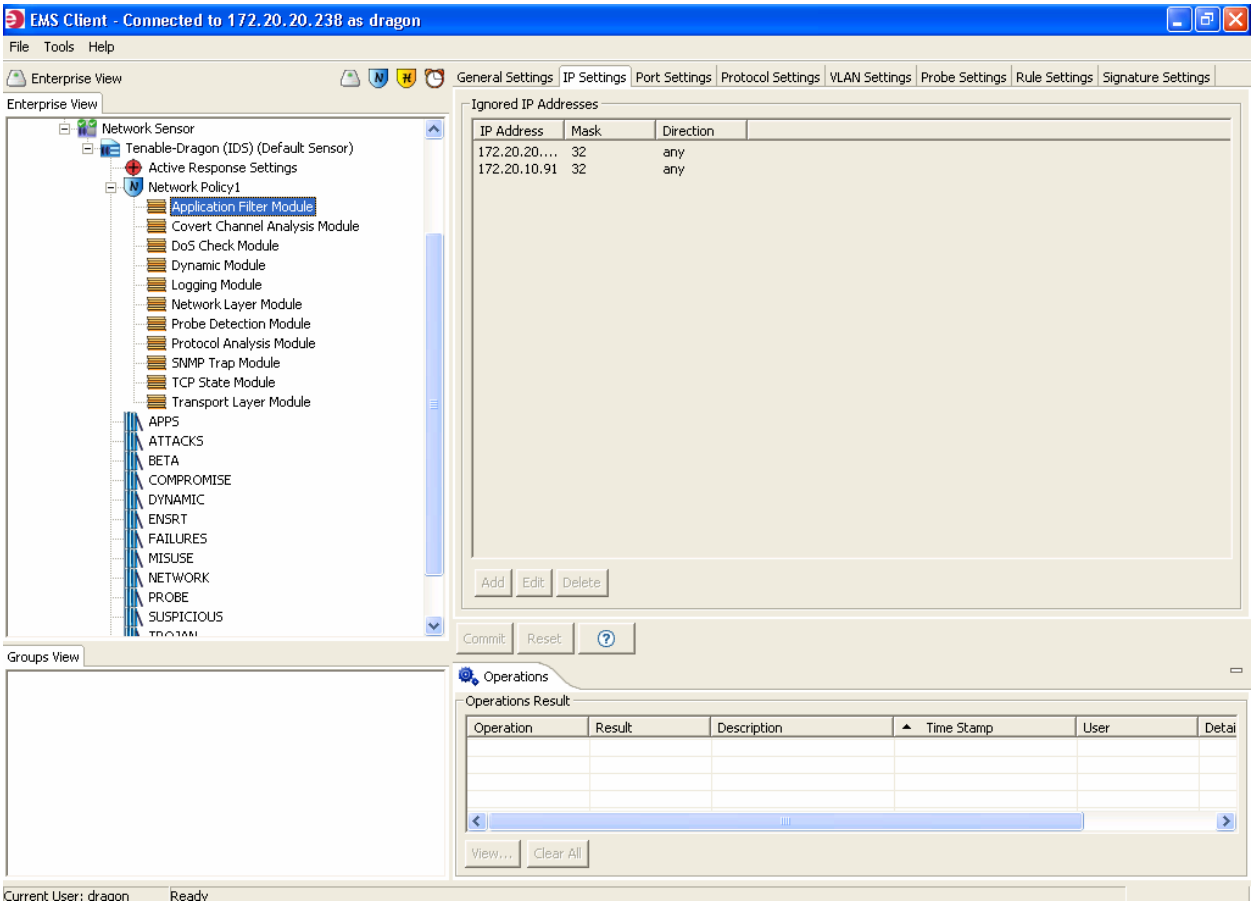
```
# /etc/rc.d/rc.inet1.conf
#
# This file contains the configuration settings for network interfaces.
# If USE_DHCP[interface] is set to "yes", this overrides any other settings.
# If you don't have an interface, leave the settings null ("").

# Config information for eth0:
IPADDR[0]="192.168.1.100"
NETMASK[0]="255.255.255.0"
USE_DHCP[0]=""
DHCP_HOSTNAME[0]=""

# Config information for eth1:
IPADDR[1]="192.168.1.101"
NETMASK[1]="255.255.255.0"
USE_DHCP[1]=""
DHCP_HOSTNAME[1]=""

# Config information for eth2:
IPADDR[2]="192.168.1.102"
NETMASK[2]="255.255.255.0"
USE_DHCP[2]=""
DHCP_HOSTNAME[2]=""

# Config information for eth3:
IPADDR[3]=""
NETMASK[3]=""
USE_DHCP[3]=""
DHCP_HOSTNAME[3]=""

# Default gateway IP address:
GATEWAY="192.168.1.1"

# Change this to "yes" for debugging output to stdout.  Unfortunately,
# /sbin/hotplug seems to disable stdout so you'll only see debugging output
# when rc.inet1 is called directly.
DEBUG_ETH_UP="no"
```

In order to assign eth2 to Nessus, when you start the Nessus service be sure to add "-S <IP address>" to the start command, where <IP address> is the IP you previously assigned to eth2. For example, the command to start Nessus will be:

/opt/nessus/sbin/nessusd –D –S <ip address>

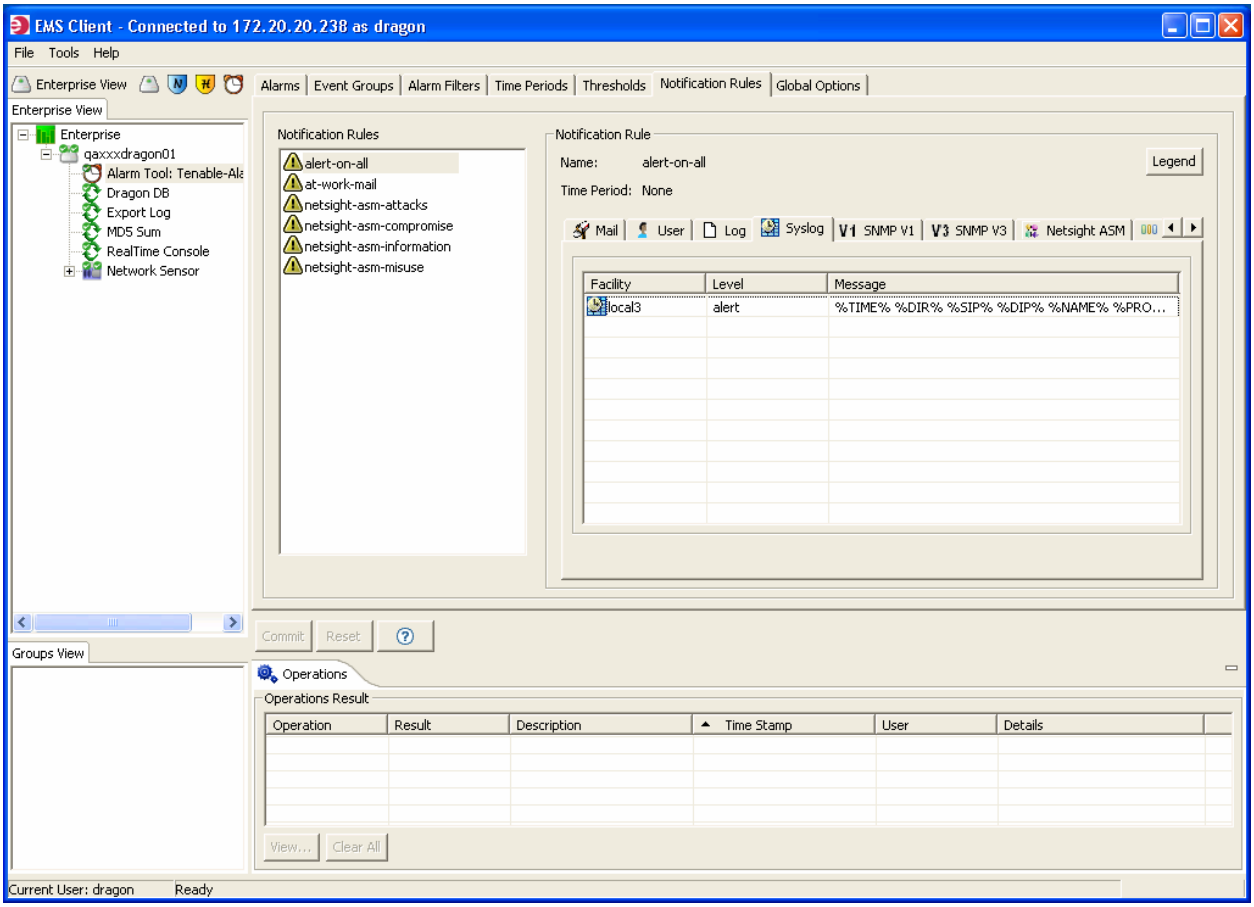
Enable Dragon to Filter Nessus IP

When running Nessus on a Dragon appliance the IP used for Nessus should be ignored by Dragon. Under the Network Sensor's Network Policy is the "Application Filter Module". You will need to ignore the IP that is associated with the Nessus sensor by using the "any" option. Otherwise, Dragon will see all the incoming/outgoing traffic from the scan itself. Refer to the screen capture shown below.



Dragon Appliance Event Forwarding to Security Center

Alarmtool and syslog can be configured to forward events from Dragon to SC3. Please refer to the section entitled "Enterasys Dragon" located in Appendix 1 of the Security Center Documentation for more information. An example screen capture of the configuration is shown below:



Events can be filtered through Alarmtool as shown in the screen capture below. Note the Event Group names and Notification Rule name.