# Table of Contents

- **Introduction** ........................................................................................................... 4
- **Standards and Conventions** .................................................................................. 4
- **Organization** ........................................................................................................... 4
- **New in Nessus 5** .................................................................................................... 4
  - Key Feature Updates ............................................................................................... 4
    - Navigation ............................................................................................................. 4
    - Analysis ............................................................................................................... 5
    - Reporting ............................................................................................................. 5
    - New Server GUI ................................................................................................. 5
- **Operating System Support** .................................................................................. 5
- **Background** ........................................................................................................... 6
- **Prerequisites** .......................................................................................................... 7
  - Nessus Unix ............................................................................................................ 7
  - Nessus Windows .................................................................................................... 7
- **Deployment Options** ............................................................................................ 7
  - Host-Based Firewalls .............................................................................................. 8
- **Vulnerability Plugin Subscriptions** ........................................................................ 8
  - Subscription Types ............................................................................................... 8
- **IPv6 Support** ......................................................................................................... 8
- **Unix/Linux** ............................................................................................................ 9
  - Upgrading .............................................................................................................. 9
  - Installation ............................................................................................................. 13
  - Start the Nessus Daemon ...................................................................................... 15
  - Stop the Nessus Daemon ..................................................................................... 16
  - Removing Nessus ................................................................................................. 17
- **Windows** ................................................................................................................ 19
  - Upgrading .............................................................................................................. 19
    - Upgrading from Nessus 4.x ................................................................................ 19
    - Upgrading from Nessus 3.x ................................................................................ 20
  - Installation ............................................................................................................. 20
    - Downloading Nessus ......................................................................................... 20
    - Installing ............................................................................................................ 20
    - Installation Questions ......................................................................................... 21
  - Starting and Stopping the Nessus Daemon ............................................................ 24
  - Removing Nessus ................................................................................................. 25
- **Mac OS X** ............................................................................................................. 25
  - Upgrading .............................................................................................................. 25
  - Installation ............................................................................................................. 25
    - Installation Questions ......................................................................................... 26
  - Starting and Stopping the Nessus Service ............................................................ 29
  - Removing Nessus ................................................................................................. 29
# Table of Contents

- Feed Registration and GUI Configuration .......................................................... 29
  - Configuration ........................................................................................................ 36
  - Web Proxy Settings .............................................................................................. 36
  - Resetting Activation Codes & Offline Updates ...................................................... 38
  - Advanced Configuration Options ........................................................................ 38
- Create and Manage Nessus Users .......................................................................... 39
- Configure the Nessus Daemon (Advanced Users) .................................................... 41
  - Configuration Options ......................................................................................... 42
- Configuring Nessus with Custom SSL Certificate ................................................... 45
- Authenticating To Nessus with SSL Certificate ....................................................... 46
  - SSL Client Certificate Authentication .................................................................. 46
  - Configure Nessus for Certificates ........................................................................ 46
  - Create Nessus SSL Certificates for Login ............................................................ 47
  - Enable Connections with Smart Card, or CAC Card ............................................ 48
  - Connect with Certificate or Card Enabled Browser ............................................. 50
- Nessus without Internet Access .............................................................................. 51
  - Generate a Challenge Code .................................................................................. 51
  - Obtain and Install Up-to-date Plugins .................................................................. 52
- Using and Managing Nessus from the Command Line ............................................. 54
  - Nessus Major Directories .................................................................................... 54
  - Create and Manage Nessus Users With Account Limitations .............................. 54
  - Nessusd Command Line Options ....................................................................... 55
  - Nessus Service Manipulation via Windows CLI .................................................. 56
- Working with SecurityCenter .................................................................................. 57
  - SecurityCenter Overview ................................................................................... 57
  - Configuring SecurityCenter 4.0-4.2 to work with Nessus ...................................... 57
  - Configuring SecurityCenter 4.4 to work with Nessus .......................................... 58
    - Host-Based Firewalls ......................................................................................... 59
- Nessus Windows Troubleshooting .......................................................................... 60
  - Installation /Upgrade Issues ................................................................................ 60
  - Scanning Issues .................................................................................................... 60
- For Further Information .......................................................................................... 62
- About Tenable Network Security ............................................................................ 63
Introduction
This document describes the installation and configuration of Tenable Network Security’s **Nessus 5.0** vulnerability scanner. Please email any comments and suggestions to **support@tenable.com**.

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

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

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

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

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

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

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

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

New in Nessus 5

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

Key Feature Updates
The following are some of the new features available in Nessus 5. For a complete list of changes, please refer to the Release Notes on the [Discussions Forum](#).

Navigation
- New host summary dashboard: Host summary and vulnerability summary dashboards make it easy to see risk level without running a report.
- Graphical bars instantly show hosts that are the most vulnerable.
**Analysis**
- Nessus 5 now has five severity levels: Informational, Low Risk, Medium Risk, High Risk, and Critical Risk.
- Users can select multiple filtering criteria, such as Vulnerability Publication Date, vulnerability database ID (e.g., CVE, OSVDB, Bugtraq ID, CERT, Secunia), Plugin type (local or remote), Information Assurance Vulnerability Alert (IAVA), and more.
- “Audit trail” feature logs why a vulnerability does NOT show up in the report for a particular host.

**Reporting**
- Chapter-based reporting system, organized between vulnerabilities and compliance.
- Reports can be generated in native Nessus formats, HTML, and now PDF formats (requires Oracle Java be installed on the Nessus server).

**New Server GUI**
- Web-based interface that now handles configuration and user management, in addition to policy creation, scans, and all reporting.
- Plugin updates can be initiated from the web interface.
- The Nessus Web Server is IPv6 compatible.

**Operating System Support**
Nessus is available and supported for a variety of operating systems and platforms:
- Debian 6 (i386 and x86-64)
- Fedora Core 16 (i386 and x86-64)
- FreeBSD 9 (i386 and x86-64)
- Mac OS X 10.6 and 10.7 (i386 and x86-64)
- Red Hat ES 4 / CentOS 4 (i386)
- Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 and x86-64)
- Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (i386 and x86-64) [Server, Desktop, Workstation]
- Solaris 10
- SuSE 10 (x86-64), 11 (i386 and x86-64)
- Ubuntu 8.04, 9.10, 10.04, 10.10, 11.10, and 12.04 (i386 and x86-64)
- Windows XP, Server 2003, Server 2008, Server 2008 R2 *, Vista, and 7 (i386 and x86-64)

Note than on Windows Server 2008 R2, the bundled version of Microsoft IE does not interface with a Java installation properly. This causes Nessus not to perform as expected in some situations. Further, Microsoft’s policy recommends not using MSIE on server operating systems. Tenable recommends that registration and scanning activity be performed from a Desktop system.

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

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

- **Intelligent Scanning** – Unlike many other security scanners, Nessus does not take anything for granted. That is, it will not assume that a given service is running on a fixed port. This means if you run your web server on port 1234, Nessus will detect it and test its security appropriately. It will attempt to validate a vulnerability through exploitation when possible. In cases where it is not reliable or may negatively impact the target, Nessus may rely on a server banner to determine the presence of the vulnerability. In such cases, it will be clear in the report output if this method was used.

- **Modular Architecture** – The client/server architecture provides the flexibility to deploy the scanner (server) and connect to the GUI (client) from any machine with a web browser, reducing management costs (one server can be accessed by multiple clients).

- **CVE Compatible** – Most plugins link to CVE for administrators to retrieve further information on published vulnerabilities. They also frequently include references to Bugtraq (BID), OSVDB, and vendor security alerts.

- **Plugin Architecture** – Each security test is written as an external plugin and grouped into one of 42 families. This way, you can easily add your own tests, select specific plugins, or choose an entire family without having to read the code of the Nessus server engine, `nessusd`. The complete list of the Nessus plugins is available at [http://www.nessus.org/plugins/index.php?view=all](http://www.nessus.org/plugins/index.php?view=all).

- **NASL** – The Nessus scanner includes NASL (Nessus Attack Scripting Language), a language designed specifically to write security tests easily and quickly.

- **Up-to-date Security Vulnerability Database** – Tenable focuses on the development of security checks for newly disclosed vulnerabilities. Our security check database is updated on a daily basis and all the newest security checks are available at [http://www.nessus.org/scripts.php](http://www.nessus.org/scripts.php).

- **Tests Multiple Hosts Simultaneously** – Depending on the configuration of the Nessus scanner system, you can test a large number of hosts concurrently.

- **Smart Service Recognition** – Nessus does not expect the target hosts to respect IANA assigned port numbers. This means that it will recognize a FTP server running on a non-standard port (e.g., 31337) or a web server running on port 8080 instead of 80.

- **Multiple Services** – If two or more web servers are run on a host (e.g., one on port 80 and another on port 8080), Nessus will identify and test all of them.

- **Plugin Cooperation** – The security tests performed by Nessus plugins cooperate so that unnecessary checks are not performed. If your FTP server does not offer anonymous logins, then anonymous login related security checks will not be performed.

- **Complete Reports** – Nessus will not only tell you what security vulnerabilities exist on your network and the risk level of each (Info, Low, Medium, High, and Critical), but it will also tell you how to mitigate them by offering solutions.

- **Full SSL Support** – Nessus has the ability to test services offered over SSL such as HTTPS, SMTPS, IMAPS and more.
• **Smart Plugins (optional)** – Nessus has an “optimization” option that will determine which plugins should or should not be launched against the remote host. For example, Nessus will not test sendmail vulnerabilities against Postfix.

• **Non-Destructive (optional)** – Certain checks can be detrimental to specific network services. If you do not want to risk causing a service failure on your network, enable the “safe checks” option of Nessus, which will make Nessus rely on banners rather than exploiting real flaws to determine if a vulnerability is present.

• **Open Forum** – Found a bug? Questions about Nessus? Start a discussion at [https://discussions.nessus.org/](https://discussions.nessus.org/).

**Prerequisites**

Tenable recommends a minimum of 2 GB of memory to operate Nessus. To conduct larger scans of multiple networks, at least 3 GB of memory is recommended, but it may require up to 4 GB for heavy usage including audit trails and PDF report generation.

A Pentium 4 processor running at 2 GHz or higher is recommended. When running on Mac OS X, a dual-core Intel® processor running at 2 GHz or higher is recommended. Deploying Nessus on 64-bit systems is preferred. The system should have at least 30 GB of free disk space for Nessus and subsequent scan data.

Nessus can be run under a VMware instance, but if the virtual machine is using Network Address Translation (NAT) to reach the network, many of Nessus’ vulnerability checks, host enumeration and operating system identification will be negatively affected.

**Nessus Unix**

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

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

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

**Nessus Windows**

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

**Deployment Options**

When deploying Nessus, knowledge of routing, filters, and firewall policies is often helpful. It is recommended that Nessus be deployed so that it has good IP connectivity to the networks it is scanning. Deploying behind a NAT device is not desirable unless it is scanning the internal network. Any time a vulnerability scan flows through a NAT or application proxy of some sort, the check can be distorted and a false positive or negative can result. In addition, if the system running Nessus has personal or desktop firewalls in place, these tools can drastically limit the effectiveness of a remote vulnerability scan.

Host-based firewalls can interfere with network vulnerability scanning. Depending on your firewall’s configuration, it may prevent, distort, or hide the probes of a Nessus scan.
Certain network devices that perform stateful inspection, such as firewalls, load balancers, and Intrusion Detection/Prevention Systems, may react negatively when a scan is conducted through them. Nessus has a number of tuning options that can help reduce the impact of scanning through such devices, but the best method to avoid the problems inherent in scanning through such network devices is to perform a credentialed scan.

Host-Based Firewalls
If your Nessus server is configured on a host with a “personal” firewall such as ZoneAlarm, Sygate, Windows firewall, or any other firewall software, it is required that connections be allowed from the Nessus client’s IP address.

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

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

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

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

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

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

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

If you are using Nessus in conjunction with Tenable’s SecurityCenter, SecurityCenter will have access to the ProfessionalFeed and will automatically update your Nessus scanners.

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

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

IPv6 Support
Nessus supports scanning of IPv6 based resources. Many operating systems and devices are shipping with IPv6 support enabled by default. To perform scans against IPv6 resources, at least one IPv6 interface must be configured on the host.
where Nessus is installed, and Nessus must be on an IPv6 capable network (Nessus cannot scan IPv6 resources over IPv4, but it can enumerate IPv6 interfaces via credentialed scans over IPv4). Both full and compressed IPv6 notation is supported when initiating scans.

Microsoft Windows lacks some of the key APIs needed for IPv6 packet forgery (e.g., getting the MAC address of the router, routing table, etc.). This prevents the port scanner from working properly. Tenable is working on enhancements that will effectively bypass the API restrictions for future versions of Nessus. Until that time, IPv6 support is only available on *nix platforms.

Scanning IPv6 Global Unicast IP address ranges is not supported unless the IPs are entered separately (i.e., list format). Nessus does not support ranges expressed as hyphenated ranges or CIDR addresses. Nessus does support Link-local ranges with the “link6” directive as the scan target or local link with “%eth0”.

Unix/Linux

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

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

Make sure any running scans have finished before stopping nessusd.

Any special upgrade instructions are provided in a note following the example.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Upgrade Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat ES 4 and CentOS 4 (32 bit); Red Hat ES 5, CentOS 5, and Oracle Linux 5 (32 and 64 bit); Red Hat ES 6, CentOS 6, and Oracle Linux 6 (32 and 64 bit)</td>
<td># service nessusd stop</td>
</tr>
<tr>
<td>Upgrade Commands</td>
<td>Use one of the appropriate commands below that corresponds to the version of Red Hat you are running:</td>
</tr>
<tr>
<td></td>
<td># rpm -Uvh Nessus-5.0.1-es4.i386.rpm</td>
</tr>
<tr>
<td></td>
<td># rpm -Uvh Nessus-5.0.1-es5.i386.rpm</td>
</tr>
<tr>
<td></td>
<td># rpm -Uvh Nessus-5.0.1-es5.x86_64.rpm</td>
</tr>
<tr>
<td></td>
<td># rpm -Uvh Nessus-5.0.1-es6.i686.rpm</td>
</tr>
<tr>
<td></td>
<td># rpm -Uvh Nessus-5.0.1-es6.x86_64.rpm</td>
</tr>
<tr>
<td></td>
<td>Once the upgrade is complete, restart the nessusd service with the following command:</td>
</tr>
<tr>
<td></td>
<td># service nessusd start</td>
</tr>
<tr>
<td>Sample Output</td>
<td># service nessusd stop</td>
</tr>
<tr>
<td></td>
<td>Shutting down Nessus services:              [ OK ]</td>
</tr>
<tr>
<td></td>
<td># rpm -Uvh Nessus-5.0.1-es5.i386.rpm</td>
</tr>
<tr>
<td></td>
<td>Preparing...</td>
</tr>
<tr>
<td></td>
<td>############################################### [100%]</td>
</tr>
<tr>
<td></td>
<td>Shutting down Nessus services: /etc/init.d/nessusd: ...</td>
</tr>
</tbody>
</table>
1:Nessus
########################################### [100%]
Fetching the newest plugins from nessus.org...
Fetching the newest updates from nessus.org...
Done. The Nessus server will start processing these plugins
within a minute
nessusd (Nessus) 5.0.1 [build R23016] for Linux
(C) 1998 - 2012 Tenable Network Security, Inc.

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

All plugins loaded
- You can start nessusd by typing /sbin/service nessusd start
- Then go to https://localhost:8834/ to configure your scanner

# service nessusd start
Starting Nessus services: [ OK ]

Fedora Core 16 (32 and 64 bit)

Upgrade Commands
# service nessusd stop

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

# rpm -Uvh Nessus-5.0.1-fc16.i686.rpm
# rpm -Uvh Nessus-5.0.1-fc16.x86_64.rpm

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

# service nessusd start

Sample Output
# service nessusd stop
Shutting down Nessus services: [ OK ]
# rpm -Uvh Nessus-5.0.1-fc16.i386.rpm
[..]
# service nessusd start
Starting Nessus services: [ OK ]

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

Upgrade Commands
# service nessusd stop

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

# rpm -Uvh Nessus-5.0.1-suse10.x86_64.rpm
# rpm -Uvh Nessus-5.0.1-suse11.i586.rpm
# rpm -Uvh Nessus-5.0.1-suse11.x86_64.rpm

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

# service nessusd start
<table>
<thead>
<tr>
<th>Sample Output</th>
<th>Upgrade Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# service nessusd stop
Shutting down Nessus services: [ OK ]
# rpm -Uvh Nessus-5.0.1-suse11.i586.rpm
Preparing...
[..]                                       | 
# service nessusd start
Starting Nessus services: [ OK ]
# /etc/init.d/nessusd stop

**Debian 6 (32 and 64 bit)**

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

# dpkg -i Nessus-5.0.1-debian6_i386.deb
# dpkg -i Nessus-5.0.1-debian6_amd64.deb
# /etc/init.d/nessusd start

**Ubuntu 8.04, 9.10, 10.04, 10.10, and 11.10 (32 and 64 bit)**

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

# dpkg -i Nessus-5.0.1-ubuntu804_i386.deb
# dpkg -i Nessus-5.0.1-ubuntu804_amd64.deb
# dpkg -i Nessus-5.0.1-ubuntu910_i386.deb
# dpkg -i Nessus-5.0.1-ubuntu910_amd64.deb
# dpkg -i Nessus-5.0.1-ubuntu1010_i386.deb
# dpkg -i Nessus-5.0.1-ubuntu1010_amd64.deb
# /etc/init.d/nessusd start
Sample Output

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

# dpkg -i Nessus-5.0.1-ubuntu804_i386.deb
(Reading database ... 19831 files and directories currently installed.)
Preparing to replace nessus 4.4.0 (using Nessus-5.0.1-ubuntu810_i386.deb) ...

[...]

# /etc/init.d/nessusd start
Starting Nessus :
```

FreeBSD 9 (32 and 64 bit)

Upgrade Commands

```
# killall nessusd
# pkg_info

This command will produce a list of all the packages installed and their descriptions. The following is example output for the previous command showing the Nessus package:

Nessus-4.4.4       A powerful security scanner

Remove the Nessus package using the following command:

# pkg_delete <package name>

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

# pkg_add Nessus-5.0.1-fbsd9.tbz
# pkg_add Nessus-5.0.1-fbsd9.amd64.tbz

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

Sample Output

```
# killall nessusd
# pkg_delete Nessus-4.4.4
# pkg_add Nessus-5.0.1-fbsd9.tbz

nessusd (Nessus) 5.0.1. for FreeBSD
(C) 2011 Tenable Network Security, Inc.

[...]

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

nessusd (Nessus) 5.0.1. for FreeBSD
(C) 2011 Tenable Network Security, Inc.

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

To upgrade Nessus on FreeBSD you must first uninstall the existing version and then install the newest release. This process will not remove the configuration files or files that were not part of the original installation.

### Installation

Download the latest version of Nessus from [http://www.nessus.org/products/nessus/nessus-download-agreement](http://www.nessus.org/products/nessus/nessus-download-agreement) or through the Tenable Support Portal. Confirm the integrity of the installation package by comparing the download MD5 checksum with the one listed in the MD5.asc file [here](http://www.nessus.org/products/nessus/nessus-download-agreement).

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

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

<table>
<thead>
<tr>
<th>Platform</th>
<th>Installation Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat ES 4 and CentOS 4 (32 bit); Red Hat ES 5, CentOS 5, and Oracle Linux 5 (32 and 64 bit); Red Hat ES 6, CentOS 6, and Oracle Linux 6 (32 and 64 bit)</td>
<td>Use one of the appropriate commands below that corresponds to the version of Red Hat you are running:</td>
</tr>
<tr>
<td></td>
<td># rpm -ivh Nessus-5.0.1-es4.i386.rpm</td>
</tr>
<tr>
<td></td>
<td># rpm -ivh Nessus-5.0.1-es5.i386.rpm</td>
</tr>
<tr>
<td></td>
<td># rpm -ivh Nessus-5.0.1-es5.x86_64.rpm</td>
</tr>
<tr>
<td></td>
<td># rpm -ivh Nessus-5.0.1-es6.i686.rpm</td>
</tr>
<tr>
<td></td>
<td># rpm -ivh Nessus-5.0.1-es6.x86_64.rpm</td>
</tr>
<tr>
<td></td>
<td>Sample Output</td>
</tr>
<tr>
<td></td>
<td># rpm -ivh Nessus-5.0.1-es4.i386.rpm</td>
</tr>
<tr>
<td></td>
<td>Preparing...</td>
</tr>
<tr>
<td></td>
<td>1:Nessus</td>
</tr>
<tr>
<td></td>
<td>Processing the Nessus plugins...</td>
</tr>
<tr>
<td></td>
<td>All plugins loaded</td>
</tr>
<tr>
<td></td>
<td>- You can start nessusd by typing /sbin/service nessusd start</td>
</tr>
<tr>
<td></td>
<td>- Then go to <a href="https://squirrel:8834/">https://squirrel:8834/</a> to configure your scanner</td>
</tr>
<tr>
<td>Fedora Core 16 (32 and 64 bit)</td>
<td>Use one of the appropriate commands below that corresponds to the version of Fedora Core you are running:</td>
</tr>
<tr>
<td></td>
<td># rpm -ivh Nessus-5.0.1-fc16.i686.rpm</td>
</tr>
<tr>
<td></td>
<td># rpm -ivh Nessus-5.0.1-fc16.x86_64.rpm</td>
</tr>
</tbody>
</table>
SuSE 10 (64 bit), 11 (32 and 64 bit)

Install Command | Use one of the appropriate commands below that corresponds to the version of SuSE you are running:
--- | ---
# rpm -ivh Nessus-5.0.1-suse10.x86_64.rpm
# rpm -ivh Nessus-5.0.1-suse11.i586.rpm
# rpm -ivh Nessus-5.0.1-suse11.x86_64.rpm

Sample Output | # rpm -ivh Nessus-5.0.1-suse11.i586.rpm
Preparing...##################################################### [100%]
1:Nessus ########################################################### [100%]
[..]
#

Debian 6 (32 and 64 bit)

Install Command | Use one of the appropriate commands below that corresponds to the version of Debian you are running:
--- | ---
# dpkg -i Nessus-5.0.1-debian6_i386.deb
# dpkg -i Nessus-5.0.1-debian6_amd64.deb

Sample Output | # dpkg -i Nessus-5.0.1-debian6_i386.deb
Selecting previously deselected package nessus. (Reading database ... 36954 files and directories currently installed.)
Unpacking nessus (from Nessus-5.0.1-debian6_i386.deb) ...
Setting up nessus (5.0.1) ...
[..]
#

Ubuntu 8.04, 9.10, 10.04, 10.10, and 11.10 (32 and 64 bit)

Install Command | Use one of the appropriate commands below that corresponds to the version of Ubuntu you are running:
--- | ---
# dpkg -i Nessus-5.0.1-ubuntu804_i386.deb
# dpkg -i Nessus-5.0.1-ubuntu804_amd64.deb
# dpkg -i Nessus-5.0.1-ubuntu910_i386.deb
# dpkg -i Nessus-5.0.1-ubuntu910_amd64.deb
# dpkg -i Nessus-5.0.1-ubuntu1010_i386.deb
# dpkg -i Nessus-5.0.1-ubuntu1010_amd64.deb
# dpkg -i Nessus-5.0.1-ubuntu1110_i386.deb
# dpkg -i Nessus-5.0.1-ubuntu1110_amd64.deb
Sample Output

```
# dpkg -i Nessus-5.0.1-ubuntu804_amd64.deb
Selecting previously deselected package nessus.
(Reading database ... 32444 files and directories currently
installed.)
Unpacking nessus (from Nessus-5.0.1-ubuntu804_amd64.deb) ...
Setting up nessus (5.0.1) ...
[...
```

FreeBSD 9 (32 and 64 bit)

<table>
<thead>
<tr>
<th>Install Command</th>
<th>Use one of the appropriate commands below that corresponds to the version of FreeBSD you are running:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample Output</td>
<td># pkg_add Nessus-5.0.1-fbsd9.tbz</td>
</tr>
<tr>
<td></td>
<td># pkg_add Nessus-5.0.1-fbsd9.amd64.tbz</td>
</tr>
<tr>
<td>Sample Output</td>
<td># pkg_add Nessus-5.0.1-fbsd9.tbz</td>
</tr>
</tbody>
</table>

nessusd (Nessus) 5.0.1 for FreeBSD
(C) 1998 - 2012 Tenable Network Security, Inc.
[...

Upon completion of the install, start the `nessusd` daemon as instructed in the next section depending on the distribution. Once Nessus is installed, you must visit the scanner URL provided to complete the registration process.

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

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

Nessus must be installed to `/opt/nessus`. However, if `/opt/nessus` is a symlink pointing to somewhere else, this is accepted.

**Start the Nessus Daemon**

Start the Nessus service as root with the following command:

**Linux and Solaris:**

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

**FreeBSD:**

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

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

```
[root@squirrel ~]# /sbin/service nessusd start
Starting Nessus services: [ OK ]
[root@squirrel ~]#```
If you wish to suppress the output of the command, use the "-q" option as follows:

**Linux and Solaris:**
# /opt/nessus/sbin/nessus-service -q -D

**FreeBSD:**
# /usr/local/nessus/sbin/nessus-service -q -D

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command to Start nessusd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat, CentOS, &amp; Oracle Linux</td>
<td># /sbin/service nessusd start</td>
</tr>
<tr>
<td>Fedora Core</td>
<td># /sbin/service nessusd start</td>
</tr>
<tr>
<td>SuSE</td>
<td># /etc/rc.d/nessusd start</td>
</tr>
<tr>
<td>Debian</td>
<td># /etc/init.d/nessusd start</td>
</tr>
<tr>
<td>FreeBSD</td>
<td># /usr/local/etc/rc.d/nessusd.sh start</td>
</tr>
<tr>
<td>Solaris</td>
<td># /etc/init.d/nessusd start</td>
</tr>
<tr>
<td>Ubuntu</td>
<td># /etc/init.d/nessusd start</td>
</tr>
</tbody>
</table>

Continue with the section “Feed Registration and GUI Configuration” to install the plugin Activation Code.

**Stop the Nessus Daemon**

If you need to stop the nessusd service for any reason, the following command will halt Nessus and abruptly stop any ongoing scans:

# killall nessusd

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command to Stop nessusd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat, CentOS, &amp; Oracle Linux</td>
<td># /sbin/service nessusd stop</td>
</tr>
<tr>
<td>Fedora Core</td>
<td># /sbin/service nessusd stop</td>
</tr>
<tr>
<td>SuSE</td>
<td># /etc/rc.d/nessusd stop</td>
</tr>
<tr>
<td>Debian</td>
<td># /etc/init.d/nessusd stop</td>
</tr>
</tbody>
</table>
### Removing Nessus

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

**Linux and Solaris:**

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

**FreeBSD:**

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

<table>
<thead>
<tr>
<th>Platform</th>
<th>Removal Instructions</th>
</tr>
</thead>
</table>
| **Red Hat ES 4 and CentOS 4 (32 bit); Red Hat ES 5, CentOS 5, and Oracle Linux 5 (32 and 64 bit); Red Hat ES 6, CentOS 6, and Oracle Linux 6 (32 and 64 bit)** | **Remove Command** Determine the package name:  
```
rpm -qa | grep Nessus
```
Use the output from the above command to remove the package:  
```
rpm -e <Package Name>
```
| **Sample Output** |  
```
rpm -qa | grep -i nessus
Nessus-5.0.1-es5
rpm -e Nessus-5.0.1-es5
```

| **Fedora Core 16 (32 and 64 bit)** | **Remove Command** Determine the package name:  
```
rpm -qa | grep Nessus
```
Use the output from the above command to remove the package:  
```
rpm -e <Package Name>
```

| **SuSE 10 (64 bit), 11 (32 and 64 bit)** | **Remove Command** Determine the package name:  
```
rpm -qa | grep Nessus
```
Use the output from the above command to remove the package:  
```
rpm -e <Package Name>
```
### Debian 6 (32 and 64 bit)

**Remove Command**

Determine the package name:

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

Use the output from the above command to remove the package:

```
# dpkg -r <package name>
```

**Sample Output**

```
# dpkg -l | grep nessus
ii  nessus         5.0.1      Version 4 of the Nessus Scanner
```

### Ubuntu 8.04, 9.10, 10.04 10.10, and 11.10 (32 and 64 bit)

**Remove Command**

Determine the package name:

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

Use the output from the above command to remove the package:

```
# dpkg -r <package name>
```

**Sample Output**

```
# dpkg -l | grep -i nessus
ii  nessus        5.0.1      Version 4 of the Nessus Scanner
```

### Solaris 10 (sparc)

**Remove Command**

Stop the `nessusd` service:

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

Determine the package name:

```
# pkginfo | grep -i nessus
```

Remove the Nessus package:

```
# pkgrm <package name>
```

**Sample Output**

```
# pkginfo | grep -i nessus
application TNBLnessus               The Nessus Network Vulnerability Scanner
```

```
# pkgrm TNBLnessus
```
FreeBSD 9 (32 and 64 bit)

Remove Command

Stop Nessus:

```bash
# killall nessusd
```

Determine the package name:

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

Remove the Nessus package:

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

Sample Output

```bash
# killall nessusd
# pkg_info | grep -i nessus
```

Nessus-5.0.1 A powerful security scanner
```bash
# pkg_delete Nessus-5.0.1
```

Windows

Upgrading

Upgrading from Nessus 4.x

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

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

The user may also be prompted to reboot the system depending on the version being installed, and the version currently on the system:
Upgrading from Nessus 3.x
A direct upgrade from Nessus 3.0.x to Nessus 5.x is not supported. However, an upgrade to 4 can be used as an interim step to ensure that vital scan settings and policies are preserved. If scan settings do not need to be kept, uninstall Nessus 3.x first and then install a fresh copy of Nessus 5.

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

Installation

Downloading Nessus

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

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

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

⚠️ Some antivirus software packages can classify Nessus as a worm or some form of malware. This is due to the large number of TCP connections generated during a scan. If your AV software gives a warning, click on “allow” to let Nessus continue scanning. Most AV packages allow you to add processes to an exception list as well. Add Nessus.exe and Nessus-service.exe to this list to avoid such warnings.
It is recommended that you obtain a plugin feed activation code before starting the installation process, as that information will be required before you can authenticate to the Nessus GUI interface. For more information on obtaining an activation code, read the section titled Vulnerability Plugin Subscriptions.

**Installation Questions**

During the installation process, Nessus will prompt the user for some basic information. Before you begin, you must read and agree to the license agreement:
After agreeing, you can configure where Nessus will be installed:

When prompted to select the “Setup Type”, select “Complete”: 
You will be prompted to confirm the installation:

After the initial installation is complete, Nessus will initiate the installation of a third-party driver that is used to support Ethernet communication for Nessus:
Once installation is complete, click “Finish”:

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

**Starting and Stopping the Nessus Daemon**

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

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

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

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

In addition, the Nessus service can be manipulated via the command line. For more information, consult the “Nessus Service Manipulation via Windows CLI” section in this document.
Removing Nessus
To remove Nessus, under the Control Panel open “Add or Remove Programs”. Select “Tenable Nessus” and then click on the “Change/Remove” button. This will open the InstallShield Wizard. Follow the directions in this wizard to completely remove Nessus. You will be prompted to decide if you want to remove the entire Nessus folder. Reply “Yes” only if you do not want to retain any scan results or policies that you may have generated.

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

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

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

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

Installation
The latest version of Nessus is available at http://www.nessus.org/products/nessus/nessus-download-agreement or through the Tenable Support Portal. Nessus is available for Mac OS X 10.6 and 10.7. Confirm the integrity of the installation package by comparing the download MD5 checksum with the one listed in the MD5.asc file here.

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

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

Note that you will be prompted for an administrator user name and password at one point during the installation.
Installation Questions
The installation will be displayed as follows:

Click “Continue”, and the software license will be displayed. Click “Continue” again, and a dialog box will appear requiring that you accept the license terms before continuing:
After accepting the license, another dialog box is displayed permitting you to change the default installation location as shown:
Click on the “Install” button to continue the installation. You will be required to enter the administrator username and password at this point:

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

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

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Command to Manage nessusd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td><code>launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist</code></td>
</tr>
<tr>
<td>Stop</td>
<td><code>launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist</code></td>
</tr>
</tbody>
</table>

Removing Nessus

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

/Library/Receipts/Nessus*/Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
/Library/Nessus
/Applications/Nessus

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

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

Feed Registration and GUI Configuration

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

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

If the software installation does not open your web browser to the configuration page, you can load a browser and go to http://[Nessus Server IP]:8834/WelcomeToNessus-Install/welcome (or the URL provided during the install process) to begin the process. Note: Unix-based installations may give a URL containing a relative host name that is not in DNS (e.g., http://mybox:8834/). If the host name is not in DNS, you must connect to the Nessus server using an IP address or a valid DNS name.
The initial screen serves as a warning that all traffic to the Nessus GUI is done over SSL (HTTPS). The first time you connect to the Nessus web server, your browser will display some type of error indicating the connection is not trusted due to a self-signed SSL certificate. For the first connection, accept the certificate to continue configuration. Instructions for installing a custom certificate are covered later in this document, in the “Configuring Nessus with Custom SSL Certificate” section.

⚠️ Due to the technical implementation of SSL certificates, it is not possible to ship a certificate with Nessus that would be trusted to browsers. In order to avoid this warning, a custom certificate to your organization must be used.
Depending on the browser you use, there may be an additional dialog that provides the ability to accept the certificate:
Once accepted, you will be redirected to the initial registration screen that begins the walk-through:

Welcome to Nessus 5

Thank you for installing Nessus, the world-leader in vulnerability scanners. Nessus will allow you to perform:

- High speed vulnerability discovery, to determine which hosts are running which services
- Agentless auditing, to make sure no host on your network is missing security patches
- Compliance checks, to verify and prove that all the hosts on your network adhere to the security policy you defined
- Scan scheduling, to automatically run scans at the frequency you define
- And more!

During the next steps, we are going to create an administrative account and register your scanner with a Plugin Feed, which we will download. You will need an activation code before you can use Nessus; if you do not have one already, please go to http://www.nessus.org/register/ to get one now.

Get started >

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

Initial Account Setup

First, we need to create an admin user for the scanner. This user will have administrative control on the scanner; it has the ability to create/delete users, stop ongoing scans, and change the scanner configuration:

Login: 
Password: 
Password (again): 
< Prev Next >

Because the admin user can change the scanner configuration, it has the ability to execute commands on the remote host. Therefore, it should be considered that the admin user has the same privileges as the "root" (or administrator) user on the remote host.
The next screen requests a plugin Activation Code and allows you to configure optional proxy settings.

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

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

If your Nessus server is on a network that uses a proxy to communicate with the Internet, click on “Optional Proxy Settings” to enter the relevant information. Proxy settings can be added at any time after the installation has completed.
Once the Activation Code and optional proxy setting configuration has been completed, click “Next” to register your scanner:

After registration, Nessus must download the plugins from Tenable. This process may take several minutes as it transfers a considerable amount of data to the machine, verifies file integrity, and compiles them into an internal database:
After the initial registration, Nessus will download and compile the plugins obtained from port 443 of plugins.nessus.org, plugins-customers.nessus.org, or plugins-us.nessus.org in the background.

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

After initialization, Nessus is ready for use!
Using the administrative credentials created during the installation, log into the Nessus interface to verify access.

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

Web Proxy Settings
Under the “Configuration” heading, the “Settings” tab allows you to configure a web proxy for plugin updates. This is required if your organization requires that all web traffic be directed through a corporate proxy:
There are six fields that control proxy settings, but only the host and port are required. Optionally, a username and password can be supplied if necessary.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The host or IP of the proxy (e.g., proxy.example.com).</td>
</tr>
<tr>
<td>Port</td>
<td>The port of the proxy (e.g., 8080).</td>
</tr>
<tr>
<td>Username</td>
<td>Optional: If a username is required for proxy usage (e.g., “jdoe”).</td>
</tr>
<tr>
<td>Password</td>
<td>Optional: If a password is required for proxy usage (e.g., “guineapigs”).</td>
</tr>
<tr>
<td>User-Agent</td>
<td>Optional: If the proxy you are using filters specific HTTP user agents, a custom user-agent string can be supplied.</td>
</tr>
<tr>
<td>Custom Update Host</td>
<td>Optional: This can be used to force Nessus to update plugins from a specific host. For example, if plugins must be updated from a site residing in the U.S., you can specify “plugins-us.nessus.org”.</td>
</tr>
</tbody>
</table>

As of Nessus 4.2, Microsoft Windows scanners support proxy authentication including NTLM.
**Resetting Activation Codes & Offline Updates**

After the initial Activation Code is entered during the setup process, subsequent Activation Code changes are performed through the “Feed Settings” tab. Inputting a new code in the “Activation Code” field and clicking “Save” will update the Nessus scanner with the new code (e.g., if upgrading from a HomeFeed to ProfessionalFeed).

You can also force a plugin update at any time by clicking “Update Plugins”. If a plugin update fails for any reason (e.g., network connectivity interruption), Nessus will retry 10 minutes later.

The “Offline Update” section allows you to specify a plugin archive for processing. For more details on offline updating, consult the “Nessus without Internet Access” section later in this document.

![System Configurations](image)

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

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

**Advanced Configuration Options**

Nessus uses a wide variety of configuration options to offer more granular control of how the scanner operates. Under the “Advanced” tab under the “Configuration” option, an administrative user can manipulate these settings.

**WARNING:** Any changes to the Nessus scanner configuration will affect ALL Nessus users. Edit these options carefully!
Each option can be configured by editing the corresponding field and clicking the “Save” button at the bottom of the screen. In addition, the option can be removed completely by clicking the ✗ button.

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

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

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

**Create and Manage Nessus Users**

During the initial setup, one administrative user is created. Using the credentials specified during the setup, log into the Nessus GUI. Once authenticated, click on the “Users” heading at the top:
To create a new user, click “New User” on the upper right. This will open a dialogue asking for required details:

- Input the username and password, verify the password, and determine if the user should have administrator privileges.
- If a user account needs to be modified, double-click on the user:

```
Edit User biscuit
```

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

To remove a user, select the check box next to the account on the list, select “Options” on the upper right, and then click “Delete User” and confirm:
A non-admin user cannot upload plugins to Nessus, cannot restart it remotely (needed after a plugin upload), and cannot override the max_hosts/max_checks setting in the configuration section. If the user is intended to be used by SecurityCenter, it must be an admin user. SecurityCenter maintains its own user list and sets permissions for its users.

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

**Configure the Nessus Daemon (Advanced Users)**

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_hosts</td>
<td>40</td>
</tr>
<tr>
<td>max_checks</td>
<td>5</td>
</tr>
</tbody>
</table>

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

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

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

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

A conservative starting point for determining the best max_hosts setting in an enterprise environment would be to set it to “20” on a Unix-based Nessus system and “10” on a Windows Nessus scanner.

Notes on max_checks:

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

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

Configuration Options:

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto_enable_dependencies</td>
<td>Automatically activate the plugins that are depended on. If disabled, not all plugins may run despite being selected in a scan policy.</td>
</tr>
<tr>
<td>auto_update</td>
<td>Automatic plugin updates. If enabled and Nessus is registered, then fetch the newest plugins from plugins.nessus.org automatically. Disable if the scanner is on an isolated network not able to reach the Internet.</td>
</tr>
<tr>
<td>auto_update_delay</td>
<td>Number of hours to wait between two updates. Four (4) hours is the minimum allowed interval.</td>
</tr>
<tr>
<td>cgi_path</td>
<td>During the testing of web servers, use this colon delimitied list of CGI paths.</td>
</tr>
<tr>
<td>checks_read_timeout</td>
<td>Read timeout for the sockets of the tests.</td>
</tr>
<tr>
<td>disable_ntp</td>
<td>Disable the old NTP legacy protocol.</td>
</tr>
<tr>
<td>disable_xmlrpc</td>
<td>Disable the new XMLRPC (Web Server) interface.</td>
</tr>
<tr>
<td>dumpfile</td>
<td>Location of a dump file for debugging output if generated.</td>
</tr>
<tr>
<td>enable_listen_ipv4</td>
<td>Directs Nessus to listen on IPv4.</td>
</tr>
<tr>
<td>Configuration Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>enable_listen_ipv6</td>
<td>Directs Nessus to listen on IPv6 if the system supports IPv6 addressing.</td>
</tr>
<tr>
<td>global.max_scans</td>
<td>If set to non-zero, this defines the maximum number of scans that may take place in parallel. Note: If this option is not used, no limit is enforced.</td>
</tr>
<tr>
<td>global.max_simult_tcp_sessions</td>
<td>Maximum number of simultaneous TCP sessions between all scans. Note: If this option is not used, no limit is enforced.</td>
</tr>
<tr>
<td>global.max_web_users</td>
<td>If set to non-zero, this defines the maximum of (web) users who can connect in parallel. Note: If this option is not used, no limit is enforced.</td>
</tr>
<tr>
<td>host.max_simult_tcp_sessions</td>
<td>Maximum number of simultaneous TCP sessions per scanned host.</td>
</tr>
<tr>
<td>listen_address</td>
<td>IPv4 address to listen for incoming connections. If set to 127.0.0.1, this will restrict access to local connections only.</td>
</tr>
<tr>
<td>listen_port</td>
<td>Port to listen to (old NTP protocol). Used for pre 4.2 NessusClient connections.</td>
</tr>
<tr>
<td>log_whole_attack</td>
<td>Log every detail of the attack? Helpful for debugging issues with the scan, but this may be disk intensive.</td>
</tr>
<tr>
<td>logfile</td>
<td>Where the Nessus log file is stored.</td>
</tr>
<tr>
<td>max_hosts</td>
<td>Maximum number of hosts checked at one time during a scan.</td>
</tr>
<tr>
<td>max_checks</td>
<td>Maximum number of simultaneous checks against each host tested.</td>
</tr>
<tr>
<td>max_simult_tcp_sessions</td>
<td>Maximum number of simultaneous TCP sessions per scan.</td>
</tr>
<tr>
<td>nasl_log_type</td>
<td>Direct the type of NASL engine output in nessusd.dump.</td>
</tr>
<tr>
<td>nasl_no_signature_check</td>
<td>Should Nessus consider all NASL scripts as being signed? Selecting “yes” is unsafe and not recommended.</td>
</tr>
<tr>
<td>nessus_syn_scanner.global_throughput.max</td>
<td>Sets the max number of syn packets that Nessus will send per second during its port scan (no matter how many hosts are scanned in parallel). Adjust this setting based on the sensitivity of the remote device to large numbers of syn packets.</td>
</tr>
<tr>
<td>non_simult_ports</td>
<td>Ports against which two plugins should not be run simultaneously.</td>
</tr>
<tr>
<td>optimize_test</td>
<td>Optimize the test procedure. Changing this to “no” will cause scans to take longer and typically generate more false positives.</td>
</tr>
<tr>
<td>paused_scan_timeout</td>
<td>Kill a paused scan after how many minutes (0 for no timeout).</td>
</tr>
<tr>
<td>plugin_upload</td>
<td>Designate if admin users may upload plugins.</td>
</tr>
<tr>
<td>plugin_upload_suffixes</td>
<td>Suffixes of the plugins the admin user can upload.</td>
</tr>
<tr>
<td><strong>plugins_timeout</strong></td>
<td>Maximum lifetime of a plugin's activity (in seconds).</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td><strong>port_range</strong></td>
<td>Range of the ports the port scanners will scan. Can use keywords &quot;default&quot; or &quot;all&quot;, as well as a comma delimited list of ports or ranges of ports.</td>
</tr>
<tr>
<td><strong>purge_plugin_db</strong></td>
<td>Should Nessus purge the plugin database at each update. This directs Nessus to remove, re-download, and re-build the plugin database for each update. Choosing yes will cause each update to be considerably slower.</td>
</tr>
<tr>
<td><strong>qdb_mem_usage</strong></td>
<td>Direct Nessus to use more or less memory when idle. If Nessus is running on a dedicated server, setting this to &quot;high&quot; will use more memory to increase performance. If Nessus is running on a shared machine, settings this to &quot;low&quot; will use considerably less memory, but at the price of a moderate performance impact.</td>
</tr>
<tr>
<td><strong>reduce_connections_on_congestion</strong></td>
<td>Reduce the number of TCP sessions in parallel when the network appears to be congested.</td>
</tr>
<tr>
<td><strong>report_crashes</strong></td>
<td>Anonymously report crashes to Tenable?</td>
</tr>
<tr>
<td><strong>rules</strong></td>
<td>Location of the Nessus Rules file (nessusd.rules).</td>
</tr>
<tr>
<td><strong>safe_checks</strong></td>
<td>Safe checks rely on banner grabbing rather than active testing for a vulnerability.</td>
</tr>
<tr>
<td><strong>save_knowledge_base</strong></td>
<td>Save the knowledge base on disk for later use.</td>
</tr>
<tr>
<td><strong>silent_dependencies</strong></td>
<td>If enabled, the list of plugin dependencies and their output are not included in the report. A plugin may be selected as part of a policy that depends on other plugins to run. By default, Nessus will run those plugin dependencies, but will not include their output in the report. Setting this option to no will cause both the selected plugin, and any plugin dependencies to all appear in the report.</td>
</tr>
<tr>
<td><strong>slice_network_addresses</strong></td>
<td>If this option is set, Nessus will not scan a network incrementally (10.0.0.1, then 10.0.0.2, then 10.0.0.3, and so on) but will attempt to slice the workload throughout the whole network (e.g., it will scan 10.0.0.1, then 10.0.0.127, then 10.0.0.2, then 10.0.0.128, and so on).</td>
</tr>
<tr>
<td><strong>source_ip</strong></td>
<td>In the case of a multi-homed system with different IPs on the same subnet, this option tells the Nessus scanner which NIC/IP to use for the tests. If multiple IPs are provided, Nessus will cycle through them whenever it performs a connection.</td>
</tr>
<tr>
<td><strong>ssl_cipher_list</strong></td>
<td>Make sure only “strong” SSL ciphers are used when connecting to port 1241. Supports the keyword &quot;strong&quot; or the general OpenSSL designations as listed at <a href="http://www.openssl.org/docs/apps/ciphers.html">http://www.openssl.org/docs/apps/ciphers.html</a>.</td>
</tr>
<tr>
<td><strong>stop_scan_on_disconnect</strong></td>
<td>Stop scanning a host that seems to have been disconnected during the scan.</td>
</tr>
<tr>
<td><strong>stop_scan_on_hang</strong></td>
<td>Stop a scan that seems to be hung.</td>
</tr>
<tr>
<td><strong>throttle_scan</strong></td>
<td>Throttle scan when CPU is overloaded.</td>
</tr>
<tr>
<td><strong>use_kernel_congestion_detection</strong></td>
<td>Use Linux’s TCP congestion messages to scale back scan activity as required.</td>
</tr>
</tbody>
</table>
www_logfile | Where the Nessus Web Server (user interface) log is stored.
--- | ---
xmlrpc_idle_session_timeout | XMLRPC Idle Session Timeout (in minutes).
xmlrpc_import_feed_policies | If set to “no”, Nessus will not include default scan policies provided by Tenable.
xmlrpc_listen_port | Port for the Nessus Web Server to listen to (new XMLRPC protocol).
xmlrpc_min_password_len | Directs Nessus to enforce a policy for the length of a password for users of the scanner.

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

**Configuring Nessus with Custom SSL Certificate**

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

![This Connection is Untrusted](image)

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

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

The following table lists the location of the certificate files based on the operating system:
### Certificate File Locations

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Certificate File Locations</th>
</tr>
</thead>
</table>
| Linux and Solaris| /opt/nessus/com/nessus/CA/servercert.pem  
/opt/nessus/var/nessus/CA/serverkey.pem |
| FreeBSD          | /usr/local/nessus/com/nessus/CA/servercert.pem  
/usr/local/nessus/var/nessus/CA/serverkey.pem |
| Windows          | C:\Program Files\Tenable\Nessus\nessus\CA\ |
| Mac OS X         | /Library/Nessus/run/com/nessus/CA/servercert.pem  
/Library/Nessus/run/var/nessus/CA/serverkey.pem |

Nessus 5 supports SSL certificate chains.

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

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

### Authenticating To Nessus with SSL Certificate

#### SSL Client Certificate Authentication

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

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

#### Configure Nessus for Certificates

The first step to allow SSL certificate authentication is to configure the Nessus web server with a server certificate and CA. This process allows the web server to trust certificates created by the Certificate Authority (CA) for authentication purposes. Generated files related to certificates must be owned by `root:root`, and default permissions are good.

1. (Optional) Create a new custom CA and server certificate for the Nessus server using the `nessus-mkcert` command at the command line. This will place the certificates in their correct directories.

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

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

   **Linux/Unix:**
   ```
   # cp /opt/nessus/com/nessus/CA/cacert.pem /opt/nessus/com/nessus/CA/ORIGcacert.pem
   ```

   **Windows:**
   ```
   C:\> copy \Program Files\Tenable\Nessus\Nessus\CA\cacert.pem C:\Program Files\Tenable\Nessus\nessus\CA\ORIGcacert.pem
   ```
3. If the certificates to be used for authentication are created by a CA other than the Nessus server, the CA certificate must be installed on the Nessus server:

   Linux/Unix:
   Copy the organization’s CA certificate to /opt/nessus/com/nessus/CA/cacert.pem

   Windows:
   Copy the organization’s CA certificate to C:\Program Files\Tenable\Nessus\Nessus\CA\cacert.pem

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

   Linux/Unix:
   # /opt/nessus/sbin/nessus-fix --set force_pubkey_auth=yes

   Windows:
   C:\> \program files\Tenable\Nessus\nessus-fix --set force_pubkey_auth=yes

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

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

**Create Nessus SSL Certificates for Login**

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

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

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

   Windows (Run as a local Administrator user):
   C:\> \Program Files\Tenable\Nessus\nessus-mkcert-client

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

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

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

   This script will now ask you the relevant information to create the SSL client certificates for Nessus.
   Client certificate life time in days [365]:
   Your country (two letter code) [US]:
   Your state or province name [NY]: MD
   Your location (e.g. town) [New York]: Columbia
   Your organization []: Content
Your organizational unit []: **Tenable**

We are going to ask you some question for each client certificate
If some question have a default answer, you can force an empty answer by entering a single dot '.'

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

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

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

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

---

The client certificates will be created in a randomized temporary directory appropriate to the system. The temporary directory will be identified on the line beginning with "Your client certificates are in".

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

3. There will be two files created in the temporary directory, `cert_squirrel.pem` and `key_squirrel.pem`. These files must be combined and exported into a format that may be imported into the web browser such as `.pfx`. This may be accomplished with the `openssl` program and the following command:

```
```

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

**Enable Connections with Smart Card, or CAC Card**

Once the CACert for the smart card, CAC, or similar device has been put in place, corresponding users must be created to match within Nessus. During this process, the users created must match the CN used on the card with which the user will use to connect.
1. On the Nessus server, run the **nessus-mkcert-client** command.

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

   **Windows (Run as a local Administrator user):**
   ```powershell
   C:\> \Program Files\Tenable\Nessus\nessus-mkcert-client.exe
   ```

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

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

   Creation Nessus SSL client Certificate

   This script will now ask you the relevant information to create the SSL client certificates for Nessus.
   Client certificate life time in days [365]:
   Your country (two letter code) [US]:
   Your state or province name [NY]: MD
   Your location (e.g. town) [New York]: Columbia
   Your organization []: Content
   Your organizational unit []: Tenable
   
   We are going to ask you some question for each client certificate
   If some question have a default answer, you can force an empty answer by entering a single dot '.
   
   User #1 name (e.g. Nessus username) []: squirrel
   Should this user be administrator? [n]: y
   Country (two letter code) [US]:
   State or province name [MD]:
   Location (e.g. town) [Columbia]:
   Organization [Content]:
   Organizational unit [Tenable]:
   e-mail []:

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

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

   User added to Nessus.
   Another client certificate? [n]:
   Your client certificates are in C:\Users\admin\AppData\Local\Temp\nessus-0000040e
   You will have to copy them by hand
3. Once created, a user with the proper card may access the Nessus server and authenticate automatically once their PIN or similar secret is provided.

**Connect with Certificate or Card Enabled Browser**

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

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

1. Launch a browser and navigate to the Nessus server.

2. The browser will present a list of available certificate identities to select from:

   ![Windows Security](image)

   Once a certificate has been selected, a prompt for the PIN or password for the certificate is presented (if required) to access your certificate. When the PIN or password is successfully entered, the certificate will be available for the current session with Nessus.
4. Upon navigating to the Nessus web interface, the user may briefly see the username and password screen followed by an automatic login as the designated user. The Nessus user interface may be used normally.

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

**Nessus without Internet Access**

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

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

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

**Generate a Challenge Code**

You must retrieve your Activation Code for the Nessus Subscription from either your Tenable Support Portal account for the ProfessionalFeed or your HomeFeed registration email.

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

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

**Windows:**

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

**Linux and Solaris:**

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

**FreeBSD:**

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

**Mac OS X:**

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

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

569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
Obtain and Install Up-to-date Plugins
Next, go to https://plugins.nessus.org/offline.php and copy and paste the “challenge” string as well as the Activation Code that you received previously into the appropriate text boxes:

This will produce a URL similar to the screen capture below:
This screen gives you access to download the latest Nessus plugin feed (all-2.0.tar.gz) along with a link to the nessus-fetch.rc file at the bottom of the screen.

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

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

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

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

**Linux and Solaris:**
# /opt/nessus/bin/nessus-fetch --register-offline /opt/nessus/etc/nessus/nessus-fetch.rc

**FreeBSD:**
# /usr/local/nessus/bin/nessus-fetch --register-offline /usr/local/nessus/etc/nessus/nessus-fetch.rc

**Mac OS X:**
# /Library/Nessus/run/bin/nessus-fetch --register-offline /Library/Nessus/run/etc/nessus/nessus-fetch.rc

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

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

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

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

**Unix (modify path for your installation):**
# /opt/nessus/sbin/nessus-update-plugins all-2.0.tar.gz

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

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

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

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

<table>
<thead>
<tr>
<th>Nessus Home Directory</th>
<th>Nessus Sub-Directories</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unix Distributions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat, SuSE, Debian, Ubuntu, Solaris: /opt/nessus</td>
<td>./etc/nessus/</td>
<td>Configuration files</td>
</tr>
<tr>
<td></td>
<td>./var/nessus/users/&lt;username&gt;/kbs/</td>
<td>User knowledgebase saved on disk</td>
</tr>
<tr>
<td>FreeBSD: /usr/local/nessus</td>
<td>./lib/nessus/plugins/</td>
<td>Nessus plugins</td>
</tr>
<tr>
<td>Mac OS X: /Library/Nessus/run</td>
<td>./var/nessus/logs/</td>
<td>Nessus log files</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Nessus Home Directory</th>
<th>Nessus Sub-Directories</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>\Program Files\Tenable\Nessus</td>
<td>\conf</td>
<td>Configuration files</td>
</tr>
<tr>
<td></td>
<td>\data</td>
<td>Stylesheet templates</td>
</tr>
<tr>
<td></td>
<td>\nessus\plugins</td>
<td>Nessus plugins</td>
</tr>
<tr>
<td></td>
<td>\nessus\users&lt;username&gt;\kbs</td>
<td>User knowledgebase saved on disk</td>
</tr>
<tr>
<td></td>
<td>\nessus\logs</td>
<td>Nessus log files</td>
</tr>
</tbody>
</table>

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

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

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

Please see the nessus-adduser manual for the rules syntax

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

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

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c &lt;config-file&gt;</td>
<td>When starting the nessusd server, this option is used to specify the server-side nessusd configuration file to use. It allows for the use of an alternate configuration file instead of the standard /opt/nessus/etc/nessus/nessusd.db (or /usr/local/nessus/etc/nessus/nessusd.db for FreeBSD).</td>
</tr>
<tr>
<td>-a &lt;address&gt;</td>
<td>When starting the nessusd server, this option is used to tell the server to only listen to connections on the address &lt;address&gt; that is an IP, not a machine name. This option is useful if you are running nessusd on a gateway and if you do not want people on the outside to connect to your nessusd.</td>
</tr>
<tr>
<td>-S &lt;ip[,ip2,...]&gt;</td>
<td>When starting the nessusd server, force the source IP of the connections established by Nessus during scanning to &lt;ip&gt;. This option is only useful if you have a multi-homed machine with multiple public IP addresses that you would like to use instead of the default one. For this setup to work, the host running nessusd must have multiple NICs with these IP addresses set.</td>
</tr>
</tbody>
</table>
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.

When starting the nessusd server, this option will make the server run in the background (daemon mode).

Display the version number and exit.

Display the plugin feed license information and exit.

Show a summary of the commands and exit.

Only listen on IPv4 socket.

Only listen on IPv6 socket.

Operate in "quiet" mode, suppressing all messages to stdout.

Force a re-processing of the plugins.

Check the timestamp of each plugin when starting up to only compile newly updated plugins.

Set a master password for the scanner.

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

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

An example of the usage is shown below:

**Linux:**
```
# /opt/nessus/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a <address>] [-S <ip[,ip,...]>]
```

**FreeBSD:**
```
```

**Nessus Service Manipulation via Windows CLI**
Nessus can also be started or stopped from the command line. Note that the command window must be called with Administrative privileges:

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

C:\Windows\system32>

**Working with SecurityCenter**

**SecurityCenter Overview**

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

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

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

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

**Configuring SecurityCenter 4.0-4.2 to work with Nessus**

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

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

For more information please refer to the “SecurityCenter Administration Guide”.

**Configuring SecurityCenter 4.4 to work with Nessus**

The SecurityCenter administration interface is used to configure access and control of any Nessus scanner that is version 4.2.x or higher. Click the **Resources** tab and then click **Nessus Scanners**. Click “Add” to open the “Add Scanner” dialog. The Nessus scanner’s IP address or hostname, Nessus port (default: 8834), authentication type (created while configuring Nessus), and administrative login ID and password or certificate information are required. The password fields are not available if “SSL Certificate” authentication is selected. The ability to Verify Hostname is provided to check the CommonName (CN) of the SSL certificate presented by the Nessus server. The state of the Nessus scanner may be set to Enabled or Disabled as needed, with a default of Enabled. Zones the Nessus scanner may be assigned to can be selected.
An example screen capture of the SecurityCenter 4.4 “Add Scanner” page is shown below:

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

For more information on integrating Nessus and SecurityCenter, please refer to the “SecurityCenter Administration Guide”.

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

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

If SecurityCenter is using the deprecated NTP protocol over port 1241, the above commands would use 1241 in place of 8834.
Nessus Windows Troubleshooting

Installation /Upgrade Issues

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

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

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

“1607: Unable to install InstallShield Scripting Runtime”

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

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

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

Scanning Issues

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

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

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

Solution: Certain anti-virus applications may show some of the Nessus plugins as viruses. Exclude the plugins directory from virus scans since there are no executable programs in this directory.

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

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

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

Solution: This is correct in that the SYN scan does not establish a full TCP connect, however it does not change the scan results.
**Issue:** When performing a scan, what factors affect performance when running Nessus Windows on a Windows XP system?

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


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

- Max number of hosts: 10
- Max number of security checks: 4

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

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

- **Nessus User Guide** – how to configure and operate the Nessus User Interface
- **Nessus Credential Checks for Unix and Windows** – information on how to perform authenticated network scans with the Nessus vulnerability scanner
- **Nessus Compliance Checks** – high-level guide to understanding and running compliance checks using Nessus and SecurityCenter
- **Nessus Compliance Checks Reference** – comprehensive guide to Nessus Compliance Check syntax
- **Nessus v2 File Format** – describes the structure for the .nessus file format, which was introduced with Nessus 3.2 and NessusClient 3.2
- **Nessus XML-RPC Protocol Specification** – describes the XML-RPC protocol and interface in Nessus
- **Real-Time Compliance Monitoring** – outlines how Tenable’s solutions can be used to assist in meeting many different types of government and financial regulations

**SecurityCenter Administration Guide**

Other online resources are listed below:

- Nessus Discussions Forum: [https://discussions.nessus.org/](https://discussions.nessus.org/)
- Example Use Videos: [http://www.youtube.com/user/tenablesecurity](http://www.youtube.com/user/tenablesecurity)
- Tenable Twitter Feed: [http://twitter.com/tenablesecurity](http://twitter.com/tenablesecurity)

Please feel free to contact Tenable at support@tenable.com, sales@tenable.com, or visit our website at [http://www.tenable.com/](http://www.tenable.com/).
About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable’s award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.