Nessus 6.4 Installation and Configuration Guide

July 7, 2015

(Revision 3)

Table of Contents

Introduction 5

Standards and Conventions 5

Official Nessus Product Names 5

New in Nessus 6.4 5

Operating System Support 6

Background 7

On Premises Nessus Product Prerequisites 8

Nessus PDF Export 8

Nessus Unix 8

Nessus Windows 9

Deployment Options 9

Host-Based Firewalls 9

Nessus Agents Deployment 9

Vulnerability Plugins 9

IPv6 Support 10

Nessus Installation, Upgrade, and Configuration 10

Unix/Linux 10

Evaluation to Licensed Upgrade 10

Upgrading 10

Installation 14

Start the Nessus Daemon 17

Stop the Nessus Daemon 17

Removing Nessus 18

Migrating Nessus 20

Windows 22

Evaluation to Licensed Upgrade 22

Upgrading 22

Installation 22

Starting and Stopping the Nessus Daemon 28

Removing Nessus 28

Migrating Nessus 28

Mac OS X 30

Evaluation to Licensed Upgrade....30

Upgrading....30

Installation....30

Starting and Stopping the Nessus Service....34

Removing Nessus....36

Migrating Nessus....37

Feed Registration and UI Configuration....38

Nessus Cloud Prerequisites....46

Subscription and Activation....47

Connecting to your Nessus Cloud Account....47

Configuration....49

Resetting Activation Codes....50

Resetting Activation Codes Online....50

Resetting Activation Codes Offline....51

Local Settings....53

Overview....53

Link....53

Software Update....54

Permissions....55

Multi-Scanner....56

Accounts....62

Create and Manage Nessus Users....62

Create and Manage Nessus Manager User Roles and Groups....64

Communication....68

Proxy Settings....68

SMTP Server....70

LDAP Server....71

Cisco ISE....73

Advanced....74

Configure the Nessus Daemon (Advanced Users)....76

Configuration Options....77

Configuring Nessus with Custom SSL Certificate....80

Authenticating To Nessus with SSL Certificate....81

SSL Client Certificate Authentication....81

Configure Nessus for Certificates....81

Create Nessus SSL Certificates for Login....82

Enable Connections with Smart Card or CAC Card 84
Connect with Certificate or Card Enabled Browser 85
Nessus without Internet Access 86
Generate a Challenge Code 86
Obtain and Install Up-to-date Plugins 87
Using and Managing Nessus from the Command Line 90
Nessus Major Directories 90
Create and Manage Nessus Users with Account Limitations 90
`nessusd` Command Line Options 91
Nessus Service Manipulation via Windows CLI 92
Nessus Agents 93
Installation 93
Download Nessus Agent Software 94
Unix Installation 94
Windows Installation 95
Mac OS X Installation 100
Configuration 101
Working with SecurityCenter 105
SecurityCenter Overview 105
Configuring SecurityCenter to work with Nessus 105
Host-Based Firewalls 106
Nessus Windows Troubleshooting 107
Installation/Upgrade Issues 107
Scanning Issues 107
Getting Support 108
Additional Resources 108
About Tenable Network Security 109

Introduction

This document describes the installation and configuration of Tenable Network Security's **Nessus 6.4** vulnerability scanner. Please email any comments and suggestions to support@tenable.com.

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

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

Standards and Conventions

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

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

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

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

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

Official Nessus Product Names

- Nessus®
- Nessus Home
- Nessus Professional
- Nessus Manager
- Nessus Cloud
- Nessus Agent

New in Nessus 6.4

The following are some of the features available in Nessus 6.4.

- Unix Agents: Nessus 6.4 includes support for the following new, Unix-based Nessus Agents:
  - Red Hat Enterprise Linux and CentOS versions 5, 6, and 7
  - Mac OS X (10.8 or higher)
  - Fedora Core version 20 or higher

- Scan Copy: In Nessus 6.4, you now have the ability to make copies of your existing scans. This feature allows Nessus administrators to copy pre-existing, configured scans, and make modifications to the new copied scan, while still having the original scan and its configuration unchanged.
- API Keys (an Access Key and a Secret Key) are used to authenticate with the Nessus REST API (version 6.4 or greater) and passed with requests using the "X-ApiKeys" HTTP header.

For a complete list of changes, please refer to the release notes.

Operating System Support

Nessus Manager and Nessus Professional are available and supported for a variety of operating systems and platforms:

- Debian 6 and 7 / Kali Linux (i386 and x86-64)
- Fedora 20 and 21 (x86-64)
- FreeBSD 10 (x86-64)
- Mac OS X 10.8, 10.9, and 10.10 (x86-64)
- Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 and x86-64)
- Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (i386 and x86-64) [Server, Desktop, Workstation]
- Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (x86-64) [Server, Desktop, Workstation]
- SUSE 10 (x86-64) and 11 (i386 and x86-64)
- Ubuntu 10.04 (9.10 package), 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 (i386 and x86-64)
- Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2 (x86-64)
- Windows 7 and 8 (i386 and x86-64)

Nessus Agents are available and supported for the following operating systems and platforms:

- Fedora 20 and 21 (x86-64)
- Mac OS X 10.8, 10.9, and 10.10 (x86-64)
- Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (i386 and x86-64)
- Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (i386 and x86-64) [Server, Desktop, Workstation]
- Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (x86-64) [Server, Desktop, Workstation]
- Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2 (x86-64)
- Windows 7 and 8 (i386 and x86-64)

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

Nessus utilizes several third-party software packages distributed under varying licenses. Running `nessusd` (or `nessusd.exe` on Windows) with the `-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 a Nessus scan 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 web UI (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 the plugin families. This way, you can easily add your own tests, select specific plugins, or choose an entire family without having to read the code of the Nessus server engine, **`nessusd`**. The complete list of the Nessus plugins is available at http://www.nessus.org/plugins/index.php?view=all.

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

- **Up-to-date Security Vulnerability Database –** Tenable focuses on the development of security checks for newly disclosed vulnerabilities. Our security check database is updated on a daily basis and all the newest security checks are available at http://www.tenable.com/plugins/index.php?view=newest.

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

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

- **Multiple Services –** If two or more web servers are run on a host (e.g., one on TCP port 80 and another on TCP 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/TLS 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.tenable.com/.

On Premises Nessus Product Prerequisites

Tenable recommends the following minimum hardware requirements for running Nessus Manager and Nessus Professional.

Scenario	CPU/Memory	Disk Space
Scanning smaller networks.	CPU: 1 Dual-core 2GHz Intel CPU (dual-core Intel® for Mac OS X) Memory: 2 GB RAM (4 GB RAM recommended)	30 GB
Scanning large networks, processing audit trails, and .pdf report generation.	CPU: 1 Dual-core 2GHz Intel CPU (2 dual-core recommended) Memory: 3 - 4 GB RAM (8 GB RAM recommended)	30 GB

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

Nessus PDF Export

The latest version of Oracle Java is required to export reports in PDF format.

Nessus requires the installation of Java on the host computer(s) prior to its installation.

Oracle Java and Nessus product version(s) must both be either 32 or 64-bit.

Warning: If Java is installed after the installation of Nessus, Nessus will need to be reinstalled.

Nessus Unix

Nessus operations require the installation of software libaries. The GNU C Library (glibc) is required and in most cases installed by default.

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

Nessus Windows

For increased performance and scan reliability when installing on a Windows platform, it is highly recommended that Nessus be installed on a server product from the Microsoft Windows family such as Windows Server 2008 R2. 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 device or application proxy of some sort, the check can be distorted and a false positive or negative can result. In addition, if the system running Nessus has personal or desktop firewalls in place, these tools can drastically limit the effectiveness of a remote vulnerability scan.

> Host-based firewalls can interfere with network vulnerability scanning. Depending on your firewall's configuration, it may prevent, distort, or hide the probes of a Nessus scan.

> Certain network devices that perform stateful inspection, such as firewalls, load balancers, and Intrusion Detection/Prevention Systems, may react negatively when a scan is conducted through them. Nessus has a number of tuning options that can help reduce the impact of scanning through such devices, but the best method to avoid the problems inherent in scanning through such network devices is to perform a credentialed scan.

Host-Based Firewalls

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

By default, TCP port 8834 is used for Nessus (UI). To open up TCP port 8834, choose the "**Exceptions**" tab and then add port "8834" to the list.

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

Nessus Agents Deployment

Nessus Agents can be deployed with a standard Windows service such as Active Directory (AD), Systems Management Server (SMS), or other software delivery system for MSI packages.

> The Windows Agent install may require a reboot to complete installation on Windows 7 x64 Enterprise, Windows 8 Enterprise, and Windows Server 2012.

Nessus Agents can be installed individually. For more information, refer to Nessus Agents section.

Vulnerability Plugins

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

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

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

IPv6 Support

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

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

Nessus Installation, Upgrade, and Configuration

Unix/Linux

Evaluation to Licensed Upgrade

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

Upgrading

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

Download the latest version of Nessus from the Nessus download page 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 product release notes.

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

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

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

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

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

Platform	Upgrade Instructions
Red Hat, CentOS, and Oracle Linux	

Upgrade Commands	`# service nessusd stop`
	
	Use one of the appropriate commands below that corresponds to the version of Red Hat you are running:
	
	`# rpm -Uvh Nessus-6.4.0-es5.i386.rpm`
	`# rpm -Uvh Nessus-6.4.0-es5.x86_64.rpm`
	`# rpm -Uvh Nessus-6.4.0-es6.i386.rpm`
	`# rpm -Uvh Nessus-6.4.0-es6.x86_64.rpm`
	`# rpm -Uvh Nessus-6.4.0-es7.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-6.4.0-es7.x86_64.rpm`
	`Preparing...`
	`########################################### [100%]`
	`Shutting down Nessus services: /etc/init.d/nessusd: …`
	`1:Nessus`
	`########################################### [100%]`
	`Fetching the newest plugins from nessus.org...`
	`Fetching the newest updates from nessus.org...`
	`Done. The Nessus server will start processing these plugins`
	`within a minute`
	`nessusd (Nessus) 6.4.0 [build R23016] for Linux`
	`(C) 1998 - 2015 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	
Upgrade Commands	`# service nessusd stop` Use one of the appropriate commands below that corresponds to the version of Fedora

you are running:

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

[..]

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

SUSE

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-6.4.0-suse10.x86_64.rpm
# rpm -Uvh Nessus-6.4.0-suse11.i586.rpm
# rpm -Uvh Nessus-6.4.0-suse11.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-6.4.0-suse11.x86_64.rpm
Preparing...

[..]

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

Debian/Kali

Upgrade Commands

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

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

```
# dpkg -i Nessus-6.4.0-debian6_i386.deb
# dpkg -i Nessus-6.4.0-debian6_amd64.deb

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

Sample Output

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

# dpkg -i Nessus-6.4.0-debian6_amd64.deb
(Reading database ... 19831 files and directories currently
installed.)
Preparing to replace nessus 6.3.7 (using Nessus-6.4.0-
debian6_amd64.deb) ...

[..]

# /etc/init.d/nessusd start

Starting Nessus : .
#
```

Ubuntu

Upgrade Commands

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

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

```
# dpkg -i Nessus-6.4.0-ubuntu910_i386.deb
# dpkg -i Nessus-6.4.0-ubuntu910_amd64.deb
# dpkg -i Nessus-6.4.0-ubuntu1110_i386.deb
# dpkg -i Nessus-6.4.0-ubuntu1110_amd64.deb

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

Sample Output

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

# dpkg -i Nessus-6.4.0-ubuntu1110_amd64.deb
(Reading database ... 19831 files and directories currently
installed.)
Preparing to replace nessus 6.3.7 (using Nessus-6.4.0-
ubuntu1110_amd64.deb) ...

[..]

# /etc/init.d/nessusd start

Starting Nessus : .
#
```

FreeBSD

Upgrade Commands

```
# service nessusd stop
# pkg info | grep -i nessus
```

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-6.4.0       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-6.4.0-fbsd10-amd64.txz`
	
	`# service nessusd start`

Sample Output	`# killall nessusd`
	`# pkg delete Nessus-6.2.0`
	`# pkg add Nessus-6.4.0-fbsd10.amd64.tbz`
	
	`nessusd (Nessus) 6.4.0 for FreeBSD`
	`(C) 2015 Tenable Network Security, Inc.`
	
	`[..]`
	
	`# /usr/local/nessus/sbin/nessusd -D`
	
	`nessusd (Nessus) 6.4.0 for FreeBSD`
	`(C) 2015 Tenable Network Security, Inc.`
	
	`Processing the Nessus plugins...`
	`[##################################################]`
	
	`All plugins loaded`
	`#`

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

Installation

Download the latest version of Nessus from the Nessus download page 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 product release notes.

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

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

Platform	Installation Instructions
Red Hat, CentOS, and Oracle Linux	
Install Command	Use one of the appropriate commands below that corresponds to the version of Red Hat you are running: `# rpm -ivh Nessus-6.4.0-es5.i386.rpm`

```
# rpm -ivh Nessus-6.4.0-es5.x86_64.rpm
# rpm -ivh Nessus-6.4.0-es6.i386.rpm
# rpm -ivh Nessus-6.4.0-es6.x86_64.rpm
# rpm -ivh Nessus-6.4.0-es7.x86_64.rpm
```

Sample Output

```
# rpm -ivh Nessus-6.4.0-es7.x86_64.rpm
Preparing...
########################################### [100%]
   1:Nessus
########################################### [100%]
nessusd (Nessus) 6.4.0 [build R20541] for Linux
(C) 1998 - 2015 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
#
```

Fedora

Install Command

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

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

Sample Output

```
Preparing...
[..]

#
```

SUSE

Install Command

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

```
# rpm -ivh Nessus-6.4.0-suse10.x86_64.rpm
# rpm -ivh Nessus-6.4.0-suse11.i586.rpm
# rpm -ivh Nessus-6.4.0-suse11.x86_64.rpm
```

Sample Output

```
# rpm -ivh Nessus-6.4.0-suse11.x86_64.rpm
Preparing...################################## [100%]
   1:Nessus ################################## [100%]

[..]

#
```

Debian/Kali

Install Command

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

```
# dpkg -i Nessus-6.4.0-debian6_i386.deb
```

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

Sample Output	`# dpkg -i Nessus-6.4.0-debian6_amd64.deb`
	`Selecting previously deselected package nessus.`
	`(Reading database ... 36954 files and directories currently installed.)`
	`Unpacking nessus (from Nessus-6.4.0-debian6_amd64.deb) ...`
	`Setting up nessus (6.4.0) ...`
	
	`[..]`
	
	`#`

Ubuntu	

Install Command	Use one of the appropriate commands below that corresponds to the version of Ubuntu you are running:
	
	`# dpkg -i Nessus-6.4.0-ubuntu910_i386.deb`
	`# dpkg -i Nessus-6.4.0-ubuntu910_amd64.deb`
	`# dpkg -i Nessus-6.4.0-ubuntu1110_i386.deb`
	`# dpkg -i Nessus-6.4.0-ubuntu1110_amd64.deb`

Sample Output	`# dpkg -i Nessus-6.4.0-ubuntu1110_amd64.deb`
	`Selecting previously deselected package nessus.`
	`(Reading database ... 32444 files and directories currently installed.)`
	`Unpacking nessus (from Nessus-6.4.0-ubuntu1110_amd64.deb) ...`
	`Setting up nessus (6.4.0) ...`
	
	`[..]`
	`#`

FreeBSD	
Install Command	Use one of the appropriate commands below that corresponds to the version of FreeBSD you are running: `# pkg add Nessus-6.4.0-fbsd10-amd64.txz`

Sample Output	`# pkg add Nessus-6.4.0-fbsd10-amd64.txz`
	
	`nessusd (Nessus) 6.4.0 for FreeBSD`
	`(C) 1998 - 2015 Tenable Network Security, Inc.`
	
	`[..]`
	`#`

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

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

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

Start the Nessus Daemon

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

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

FreeBSD:
```
# service nessusd start
```

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

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

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

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

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

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

Operating System	Command to Start `nessusd`
Red Hat, CentOS, and Oracle Linux	`# /sbin/service nessusd start`
Fedora	`# /sbin/service nessusd start`
SUSE	`# /etc/rc.d/nessusd start`
Debian/Kali	`# /etc/init.d/nessusd start`
FreeBSD	`# service nessusd start`
Ubuntu	`# /etc/init.d/nessusd start`

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

Stop the Nessus Daemon

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

Operating System	Command to Stop `nessusd`
Red Hat, CentOS, and Oracle Linux	`# /sbin/service nessusd stop`
Fedora	`# /sbin/service nessusd stop`
SUSE	`# /etc/rc.d/nessusd stop`
Debian/Kali	`# /etc/init.d/nessusd stop`
FreeBSD	`# service nessusd stop`
Ubuntu	`# /etc/init.d/nessusd stop`

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

```
# killall nessusd
```

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 either. To completely remove the remaining files use the following command:

Linux:

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

FreeBSD:

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

Platform	Removal Instructions
Red Hat, CentOS, and Oracle Linux	

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-6.4.0-es6`
	`# rpm -e Nessus-6.4.0-es6`

Fedora	

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	

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/Kali	

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         6.4.0      Version 6 of the Nessus Scanner`
	
	`# dpkg -r nessus`
	`#`

Ubuntu	

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        6.4.0      Version 6 of the Nessus Scanner`
	`#`

FreeBSD	
Remove Command	Stop Nessus:

	`# killall nessusd`
	Determine the package name:
	`# pkg_info | grep -i nessus`
	Remove the Nessus package:
	`# pkg_delete <package name>`

Sample Output	`# killall nessusd`
	`# pkg_info | grep -i nessus`
	`Nessus-6.3.0        A powerful security scanner`
	`# pkg_delete Nessus-6.4.0`
	`#`

Migrating Nessus

It is not uncommon for a system administrator to have to migrate a Nessus implementation from one machine to another. To migrate a Nessus installation from one Linux system to another, follow the steps below. The steps cover copying over the critical files needed as well as correctly installing Nessus on the new system.

The important files that need to be migrated from the old installation to the new installation are:

- `/opt/nessus/var/nessus/global.db`
- `/opt/nessus/var/nessus/master.key`
- `/opt/nessus/var/nessus/policies.db`

The important directories that need to be migrated from the old installation to the new installation are:

- `/opt/nessus/var/nessus/`
- `/opt/nessus/etc/nessus`
- `/opt/nessus/sbin`

> The migration steps works for Nessus 5 and higher. You will be able to migrate from Nessus 5.2.7 to Nessus 6, but not be able to downgrade.

The first steps are done on the original system where you have Nessus installed.

1. Open a terminal window and run the **sudo** or **su** command to enable root privileges. You will be prompted for the user password:

   ```
   # sudo -s
   Password:
   ```

2. Stop the Nessus service:

   ```
   # /sbin/service nessusd stop
   ```

3. Change to the root directory:

   ```
   # cd /
   ```

4. Backup the critical files in **/opt/nessus/var/nessus** and all of the **/opt/nessus/etc/nessus** directory. Given these will be copied to another system, Tenable recommends creating a tar ball of the files and directories:

   ```
   # tar -zcvf /tmp/tarOfMyNessusInstallation.tar.gz
   /opt/nessus/var/nessus/global.db
   /opt/nessus/var/nessus/master.key
   /opt/nessus/var/nessus/policies.db
   /opt/nessus/var/nessus/users
   /opt/nessus/etc/nessus
   ```

   This will create a tarball in the **/tmp** directory with the name **tarOfMyNessusInstallation.tar** format.

5. Copy over the tar ball to the new server:

   ```
   # scp /tmp/tarOfMyNessusInstallation.tar.gz mynewsystem:/tmp
   ```

On the new server, perform the following steps:

1. Install the Nessus 6.4 Linux package appropriate to your operating system and architecture, according to the installation instructions at the beginning of the Linux section of this document.

2. Open a terminal window and run the **sudo** command. You will be prompted for the user password:

   ```
   # sudo –s
   Password:
   ```

3. Log in to the Tenable Support Portal and reset the Nessus activation code for this installation.

4. Restore and overwrite the critical files from the older server. To do this, untar the tar ball in the correct directory:

   ```
   # mv /tmp/tarOfMyNessusInstallation.tar.gz /
   # tar -xvf tarOfMyNessusInstallation.tar.gz
   ```

5. Register the activation code with this installation. This will also have Nessus fetch the latest plugins.

   ```
   # /opt/nessus/sbin/nessuscli fetch --register <activation code>
   ```

6. Reindex Nessus plugins. This may take up to 15-20 minutes, depending on your system.

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

7. Once Nessus completes the reindexing process, restart the Nessus service:

   ```
   # /sbin/service nessusd start
   ```

8. Log in to your Nessus scanner using the Nessus UI at https://yoursystem:8834.

9. Once you confirm your new system is working correctly and all the files are migrated, go through the removal process on the original system listed in the Mac OS X section of this document.

For backing up and/or restoring a complete Nessus installation, please contact Tenable Support if you have any questions. This will help to ensure there are no deviations from a normal installation that may prevent critical data from being maintained.

Windows

Evaluation to Licensed Upgrade

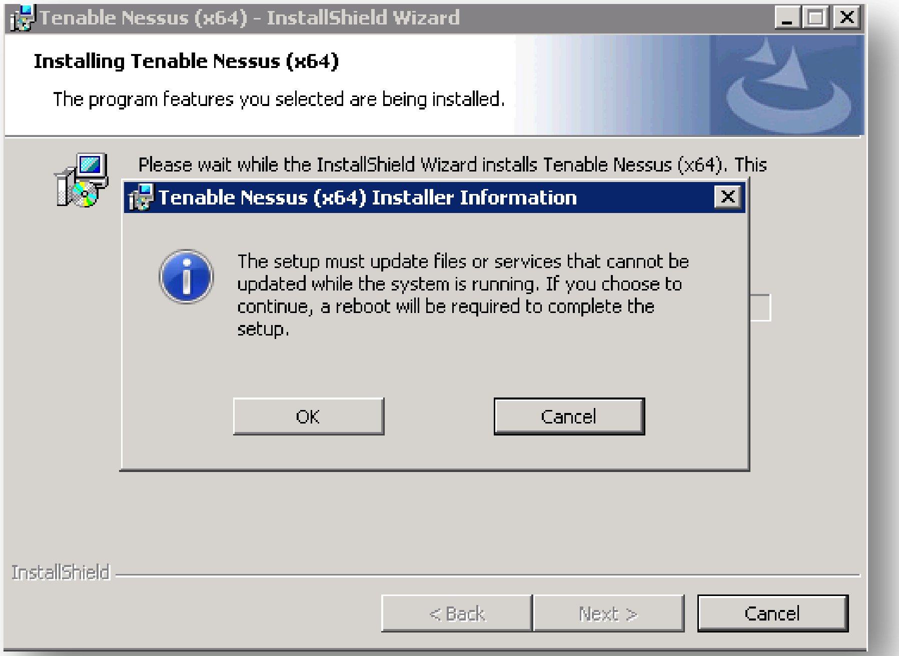
If you install Nessus with an evaluation license, it is strongly recommended that you uninstall it before migrating to a fully licensed copy. Any policies or scan results you created can be exported and re-imported into the new installation.

Upgrading

Upgrading from 5.x to 6 is straightforward and does not require any special considerations. Instructions are below.

Download the latest version of Nessus from the Nessus download page 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 product release notes.

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


Tenable Nessus (x64) - InstallShield Wizard
Installing Tenable Nessus (x64)
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs Tenable Nessus (x64). This
Tenable Nessus (x64) Installer Information
OK
Cancel
InstallShield
< Back
Next >
Cancel

The setup must update files or services that cannot be updated while the system is running. If you choose to continue, a reboot will be required to complete the setup.

Installation

Download the latest version of Nessus from the Nessus download page 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 product release notes. Nessus 6 is available for Windows 7, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, and Windows 8.

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

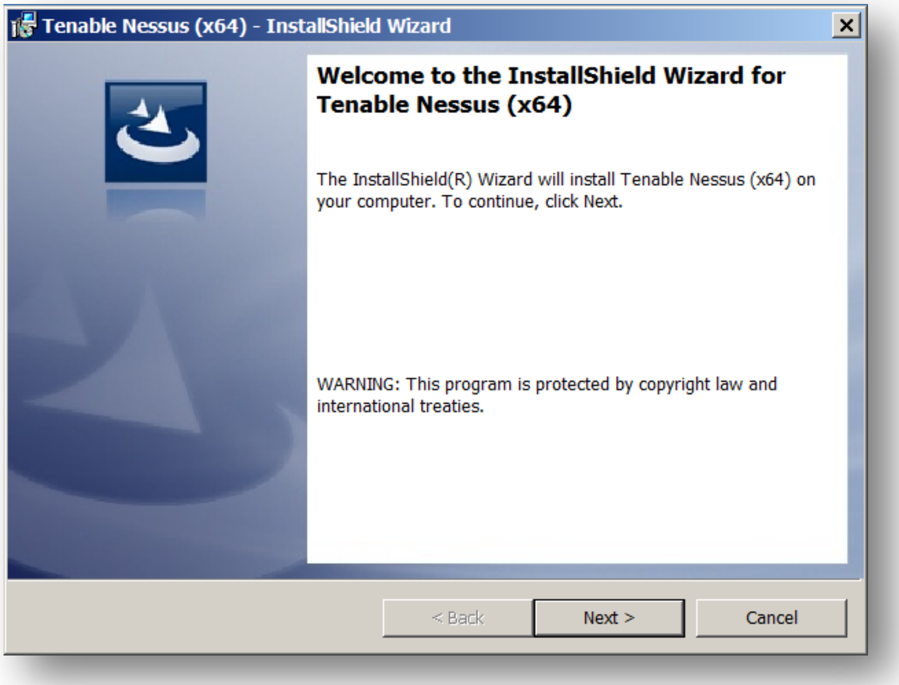
Nessus is distributed as an executable installation file. Place the file on the system it is being installed on or a shared drive accessible by the system.

Download the file `Nessus-6.4.0-Win32.msi` or `Nessus-6.4.0-x64.msi`, and then double-click on it. This will start the install procedure.

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

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

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

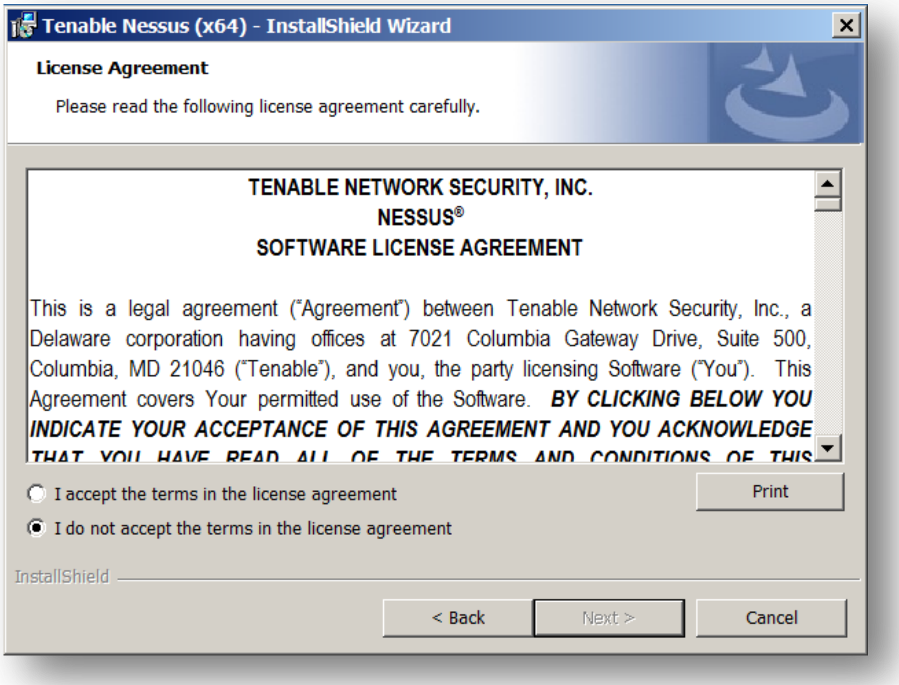


Welcome to the InstallShield Wizard for Tenable Nessus (x64)

The InstallShield(R) Wizard will install Tenable Nessus (x64) on your computer. To continue, click Next.

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

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



License Agreement

Please read the following license agreement carefully.

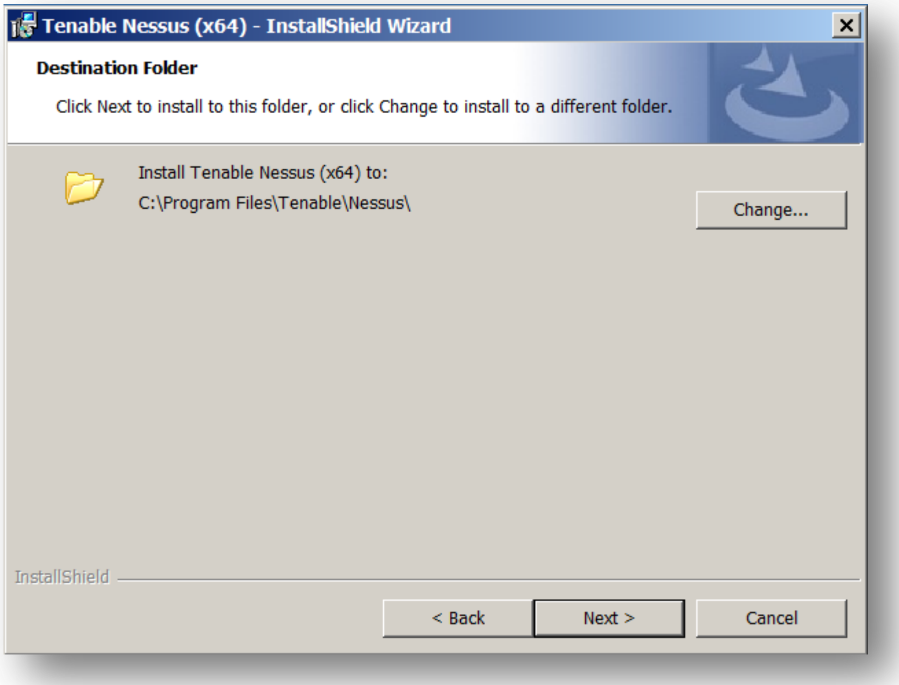
TENABLE NETWORK SECURITY, INC.
NESSUS®
SOFTWARE LICENSE AGREEMENT

This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7021 Columbia Gateway Drive, Suite 500, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers Your permitted use of the Software. ***BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS***

○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement

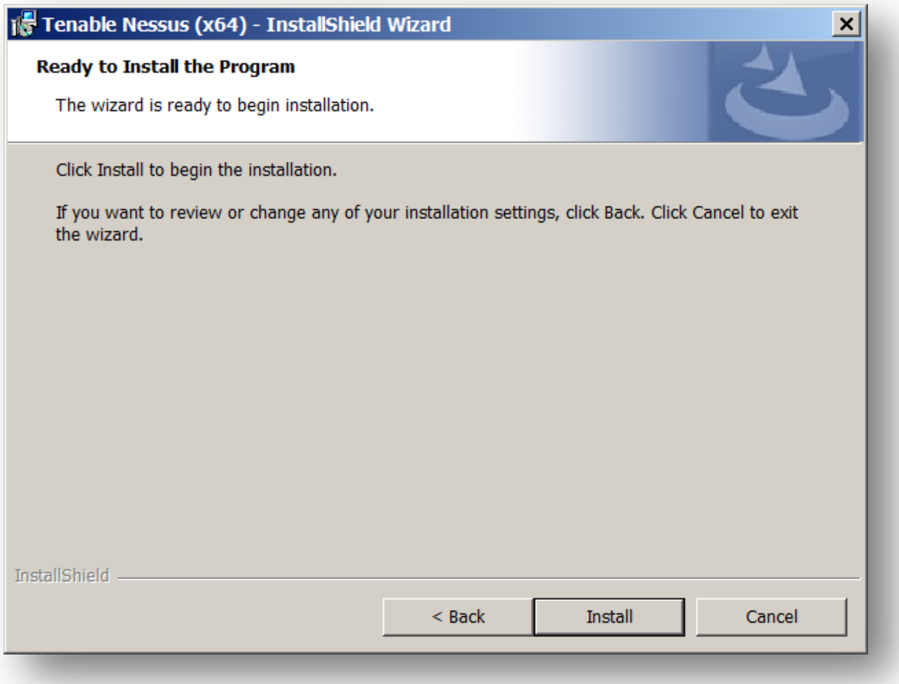
You will be prompted to confirm the installation location and then verify you want to install:



Destination Folder

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

Install Tenable Nessus (x64) to:
C:\Program Files\Tenable\Nessus\



Tenable Nessus (x64) - InstallShield Wizard

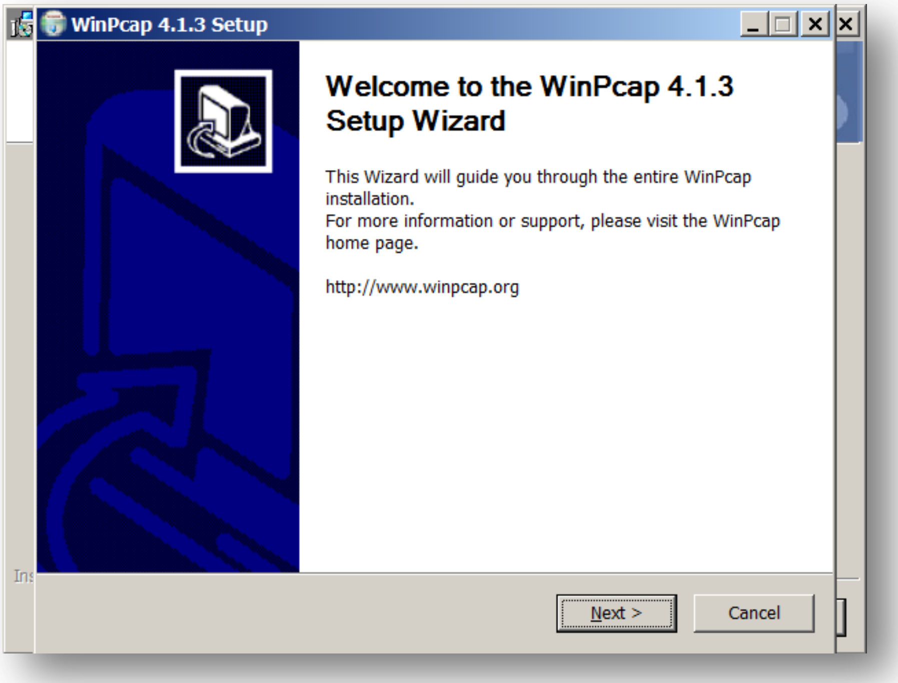
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

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

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



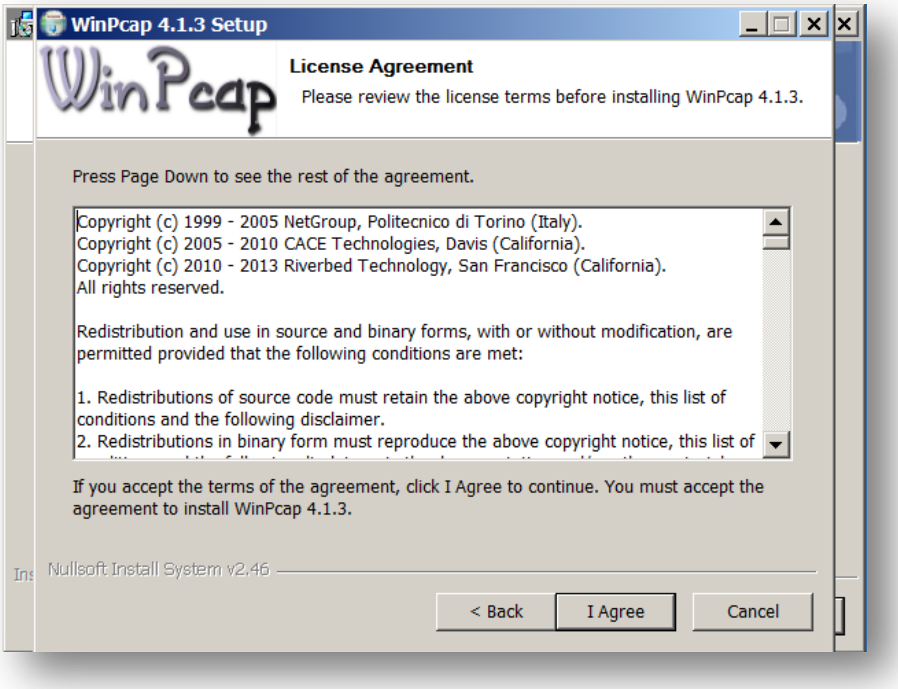
WinPcap 4.1.3 Setup

Welcome to the WinPcap 4.1.3 Setup Wizard

This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

http://www.winpcap.org

You must also agree to the WinPcap license agreement:


WinPcap 4.1.3 Setup

License Agreement

Please review the license terms before installing WinPcap 4.1.3.

Press Page Down to see the rest of the agreement.

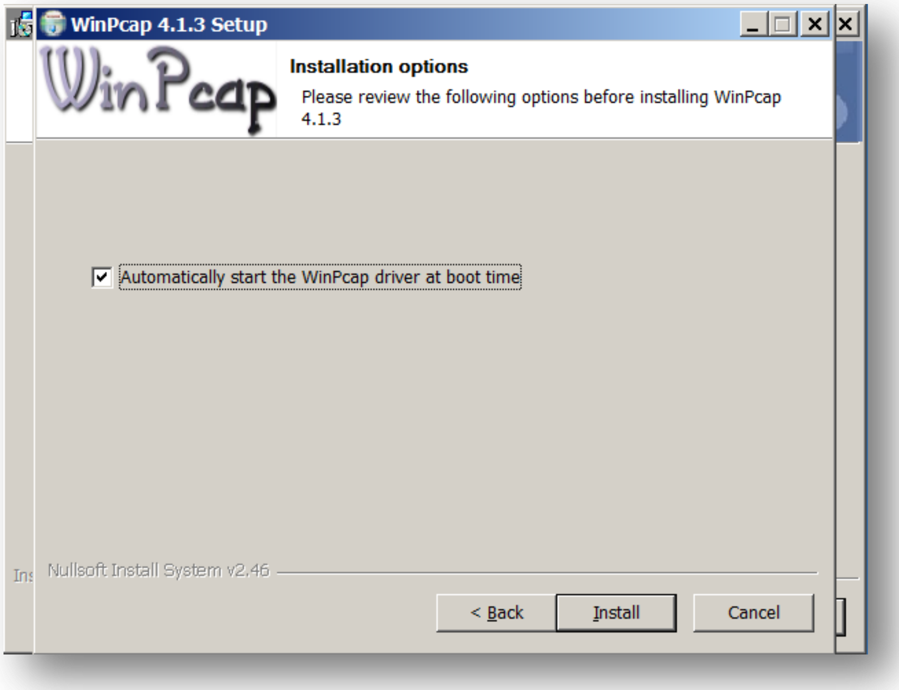
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California).
All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.3.

WinPcap will also confirm that you want to launch the driver when the system boots up. It is strongly recommended that you keep this option enabled for seamless Nessus use:

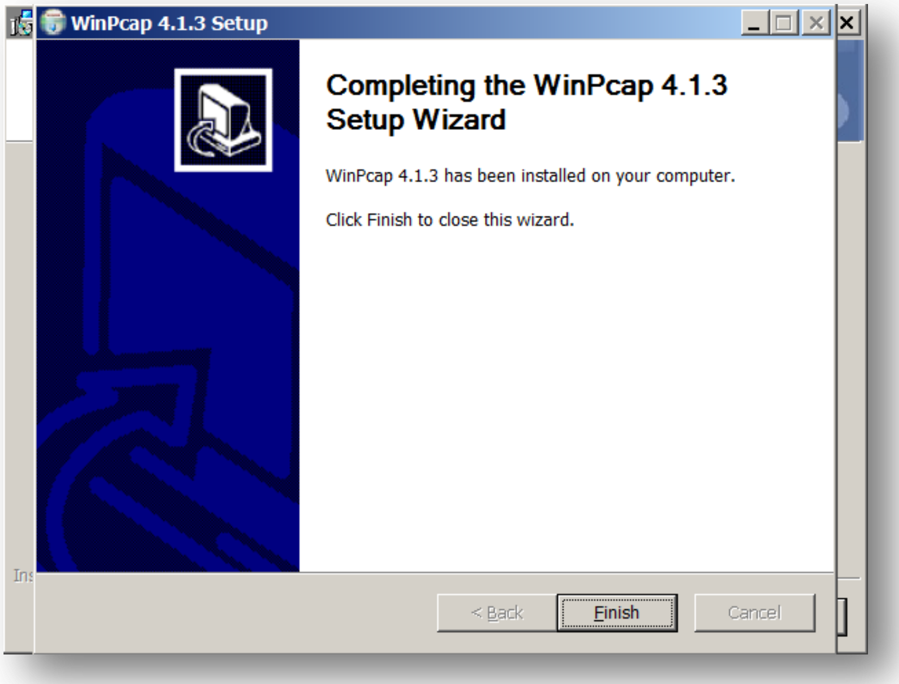

WinPcap 4.1.3 Setup

Installation options

Please review the following options before installing WinPcap 4.1.3

☑ Automatically start the WinPcap driver at boot time

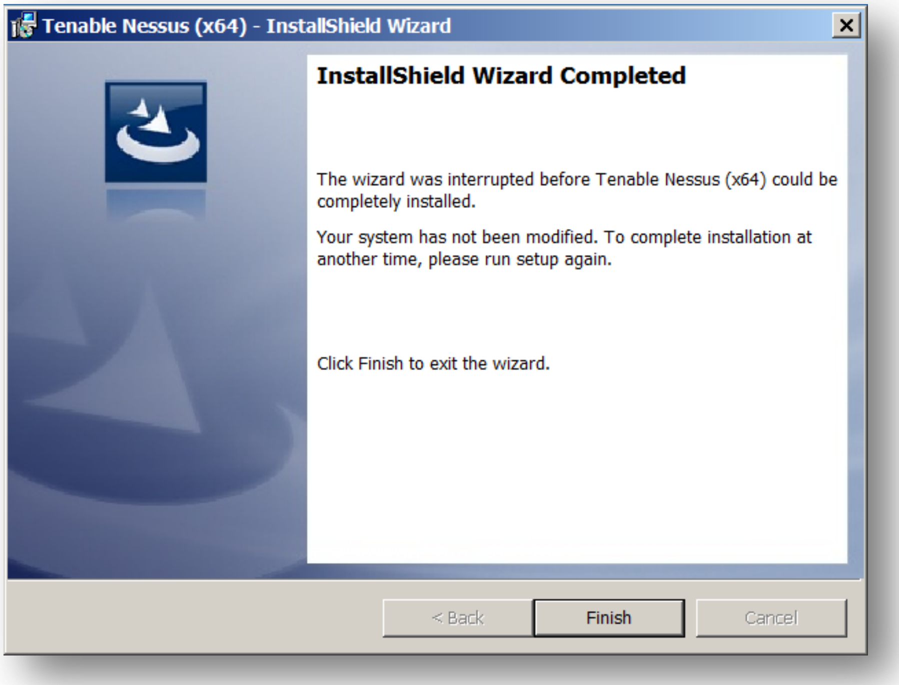
Once installation of both components is complete, click "Finish" to acknowledge each:



Completing the WinPcap 4.1.3 Setup Wizard

WinPcap 4.1.3 has been installed on your computer.

Click Finish to close this wizard.



InstallShield Wizard Completed

The wizard was interrupted before Tenable Nessus (x64) could be completely installed.

Your system has not been modified. To complete installation at another time, please run setup again.

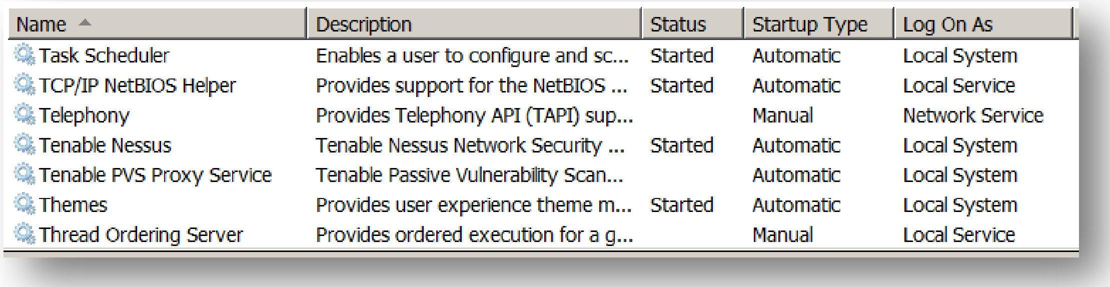
Click Finish to exit the wizard.

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

Starting and Stopping the Nessus Daemon

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

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



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

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

In addition, the Nessus service can be manipulated via the command line. For more information, consult the "Nessus Service Manipulation via Windows CLI" section in this document.

Removing Nessus

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

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

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

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

Migrating Nessus

It is not uncommon for a system administrator to have to migrate a Nessus implementation from one machine to another. To migrate a Nessus installation from one Windows system to another, follow the steps below. The steps cover copying over the critical files needed as well as correctly installing Nessus on the new system.

The important files that need to be migrated from the old installation to the new installation are:

- `C:\ProgramData\Tenable\Nessus\global.db`
- `C:\ProgramData\Tenable\Nessus\master.key`
- `C:\ProgramData\Tenable\Nessus\policies.db`

The important directories that need to be migrated from the old installation to the new installation are:

- **`C:\ProgramData\Tenable\Nessus\users`**
- **`C:\ProgramData\Tenable\Nessus\conf`**

> The migration steps works for Nessus 5 and higher. You will be able to migrate from Nessus 5.2.7 to Nessus 6, but not be able to downgrade.

The first steps are done on the original system where you have Nessus installed.

1. Run **`cmd.exe`** with "Run as…" privileges set to "Administrator".
2. At the Windows command prompt, stop the Nessus service:

   ```
   C:\> net stop "Tenable Nessus"
   ```

3. Backup the critical files in **`C:\ProgramData\Tenable\Nessus`** and the entire **`C:\ProgramData\Tenable\Nessus\conf`** directory. Given these will be copied to another system, Tenable recommends compressing the files and directories. For information on how to compress files on Windows, see http://windows.microsoft.com/en-us/windows/compress-uncompress-files-zip-files.
4. Copy over the file archive to the new server via a network share (\\computername\share) or manually depending on your environment.

On the new server, perform the following steps:

1. Install the Nessus 6.4 installation package, according to the installation instructions at the beginning of the Windows section of this document.
2. When the Nessus login page opens in your web browser, close the page or tab.
3. Run **`cmd.exe`** with "Run as…" privileges set to "Administrator".
4. At the Windows command prompt, stop the Nessus service:

   ```
   C:\> net stop "Tenable Nessus"
   ```

5. Leave this **`cmd.exe`** window open.
6. Log in to the Tenable Support Portal and reset the Nessus activation code for this installation.
7. Restore and overwrite the critical files from the older server. To do this, uncompress the archive and copy the files to the correct directory. Select yes to **Replace and Move** or **Replace and Copy**.
8. Register the activation code with this installation. This will also have Nessus fetch the latest plugins.

   ```
   C:\> cd C:\Program Files\Tenable\Nessus
   C:\> nessuscli fetch --register <activation code>
   ```

9. Re-index the Nessus plugins. This may take up to 15-20 minutes, depending on your system resources.

   ```
   C:\> cd C:\Program Files\Tenable\Nessus
   C:\> nessusd -R
   ```

10. Once Nessus completes the re-indexing process, restart the Nessus service:

```
C:\> net start "tenable nessus"
```

11. Log in to your Nessus scanner using the Nessus UI at https://yoursystem:8834/.

12. Once you confirm your new system is working correctly and all the files are migrated, go through the removal process on the original system listed in the Windows section of this document.

For backing up and/or restoring a complete Nessus installation, please contact Tenable Support if you have any questions. This will help to ensure there are no deviations from a normal installation that may prevent critical data from being maintained.

Mac OS X

Evaluation to Licensed Upgrade

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

Upgrading

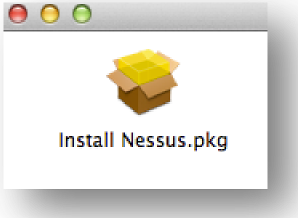
Upgrading from an older version of Nessus is the same as performing a fresh install. Download the file **`Nessus-6.4.0.dmg.gz`**, and then double-click on it to unzip it. Double click on the **`Nessus-6.4.0.dmg`** file, which will mount the disk image and make it appear under “Devices” in “Finder”. Once the volume “Nessus 6” appears in “Finder”, double click on the file Nessus 6. When the installation is complete, log in to Nessus via your browser at https://localhost:8834/.

Installation

Download the latest version of Nessus from the Nessus download page 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 product release notes. Nessus is available for Mac OS X 10.8, 10.9, and 10.10.

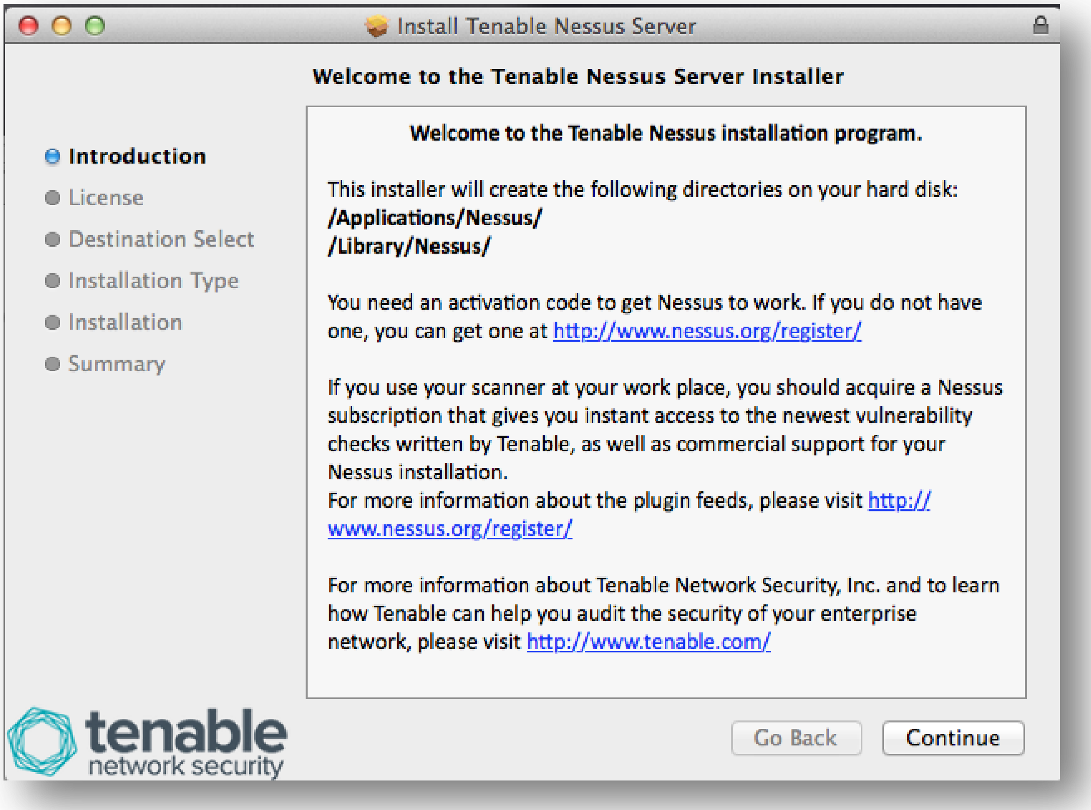
The Nessus distribution file size for Mac OS X varies slightly from release to release, but is approximately 45 MB in size.

To install Nessus on Mac OS X, you need to download the file **`Nessus-6.4.0.dmg.gz`**, and then double click on it to unzip it. Double click on the **`Nessus-6.4.0.dmg`** file, which will mount the disk image and make it appear under “Devices” in “Finder”. Once the volume “Nessus 6” appears in “Finder”, double click on the file **`Install Nessus`** package as shown below:



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

The installation will be displayed as follows:



Welcome to the Tenable Nessus Server Installer

Welcome to the Tenable Nessus installation program.

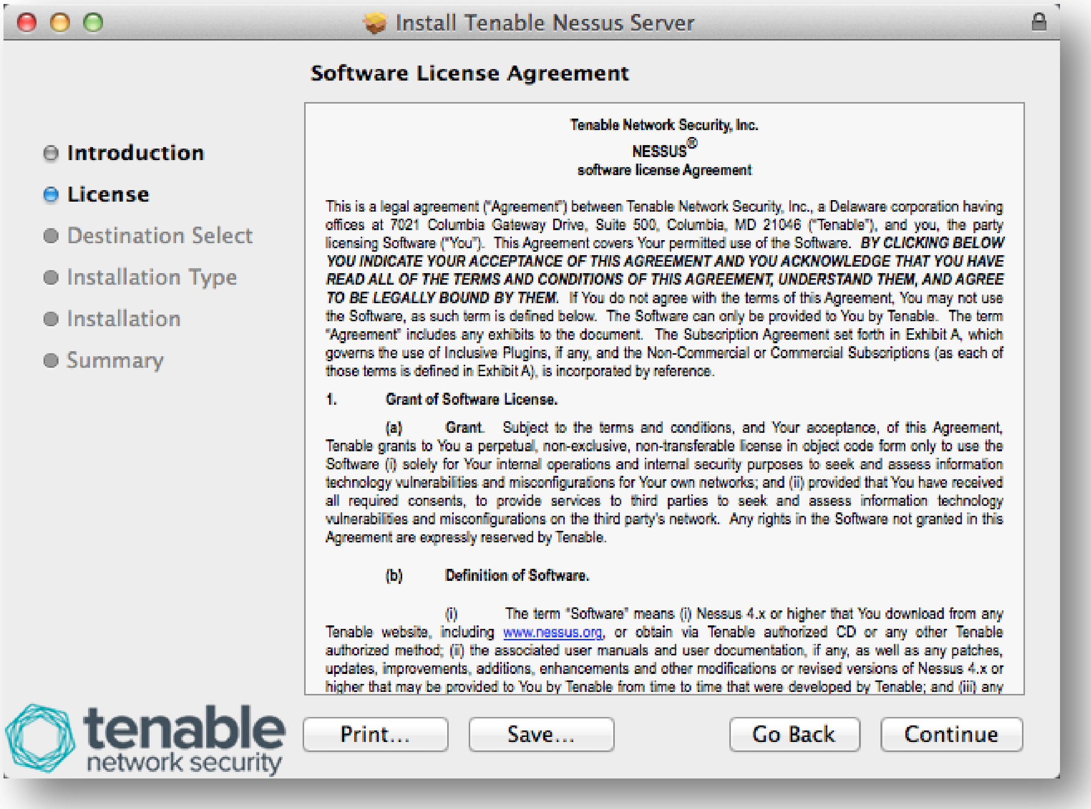
This installer will create the following directories on your hard disk:
/Applications/Nessus/
/Library/Nessus/

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

If you use your scanner at your work place, you should acquire a Nessus subscription that gives you instant access to the newest vulnerability checks written by Tenable, as well as commercial support for your Nessus installation.
For more information about the plugin feeds, please visit http://www.nessus.org/register/

For more information about Tenable Network Security, Inc. and to learn how Tenable can help you audit the security of your enterprise network, please visit http://www.tenable.com/

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:



Software License Agreement

Tenable Network Security, Inc.
NESSUS®
software license Agreement

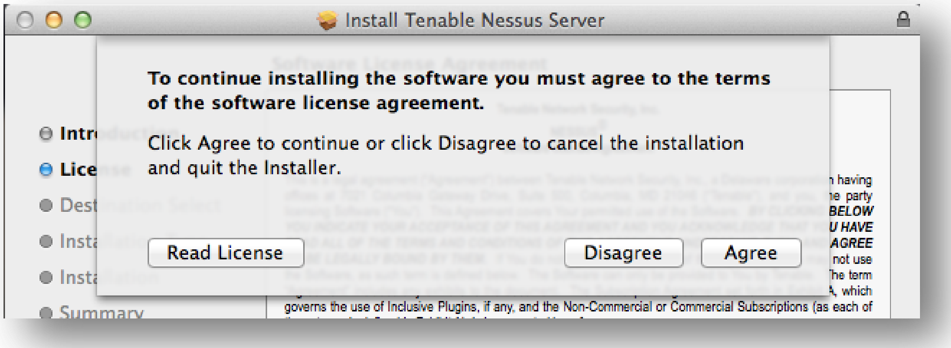
This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7021 Columbia Gateway Drive, Suite 500, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers Your permitted use of the Software. ***BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM.*** If You do not agree with the terms of this Agreement, You may not use the Software, as such term is defined below. The Software can only be provided to You by Tenable. The term "Agreement" includes any exhibits to the document. The Subscription Agreement set forth in Exhibit A, which governs the use of Inclusive Plugins, if any, and the Non-Commercial or Commercial Subscriptions (as each of those terms is defined in Exhibit A), is incorporated by reference.

1. **Grant of Software License.**

(a) Grant. Subject to the terms and conditions, and Your acceptance, of this Agreement, Tenable grants to You a perpetual, non-exclusive, non-transferable license in object code form only to use the Software (i) solely for Your internal operations and internal security purposes to seek and assess information technology vulnerabilities and misconfigurations for Your own networks; and (ii) provided that You have received all required consents, to provide services to third parties to seek and assess information technology vulnerabilities and misconfigurations on the third party's network. Any rights in the Software not granted in this Agreement are expressly reserved by Tenable.

(b) **Definition of Software.**

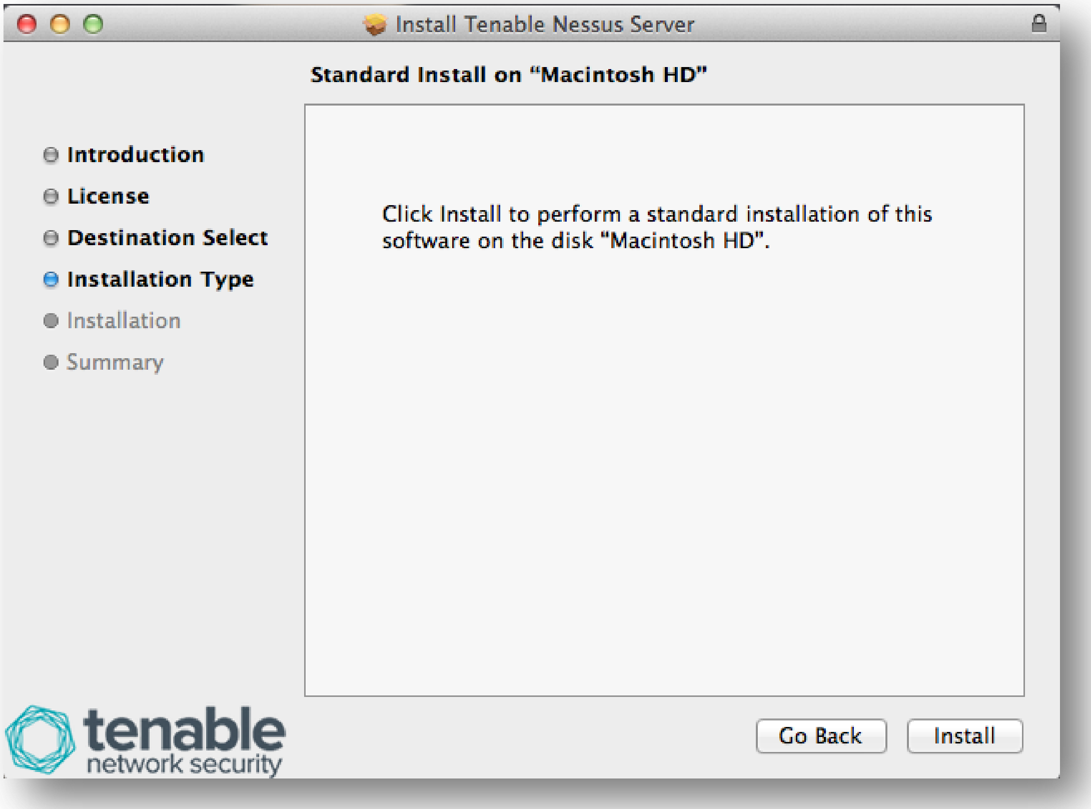
(i) The term "Software" means (i) Nessus 4.x or higher that You download from any Tenable website, including www.nessus.org, or obtain via Tenable authorized CD or any other Tenable authorized method; (ii) the associated user manuals and user documentation, if any, as well as any patches, updates, improvements, additions, enhancements and other modifications or revised versions of Nessus 4.x or higher that may be provided to You by Tenable from time to time that were developed by Tenable; and (iii) any



To continue installing the software you must agree to the terms of the software license agreement.

Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

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

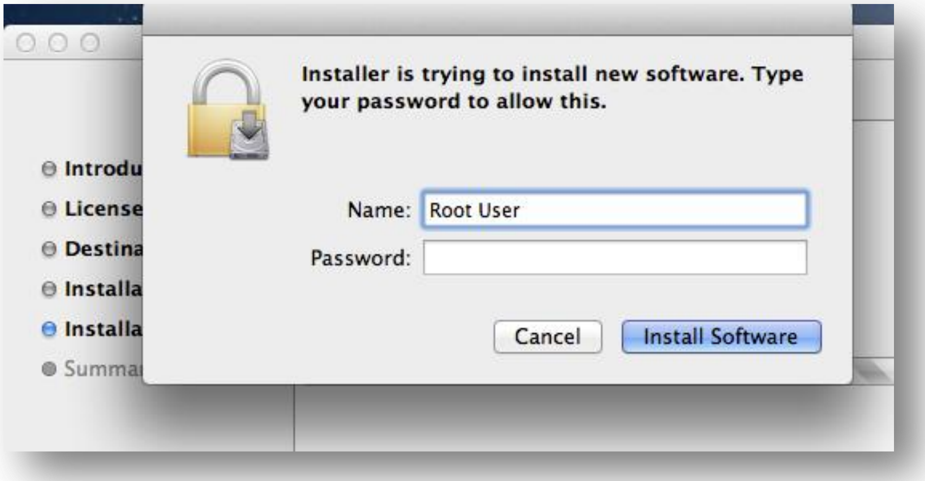


Install Tenable Nessus Server

Standard Install on "Macintosh HD"

Click Install to perform a standard installation of this software on the disk "Macintosh HD".

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

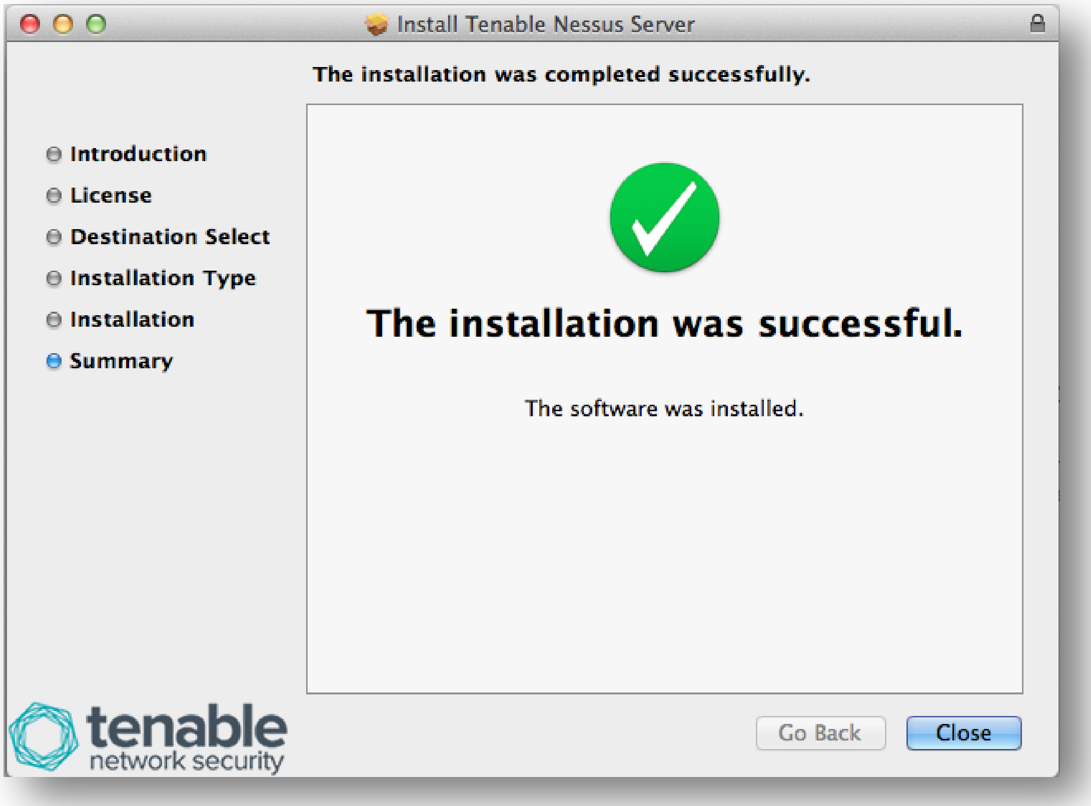


Installer is trying to install new software. Type your password to allow this.

Name: Root User

Password:

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



The installation was completed successfully.

The installation was successful.

The software was installed.

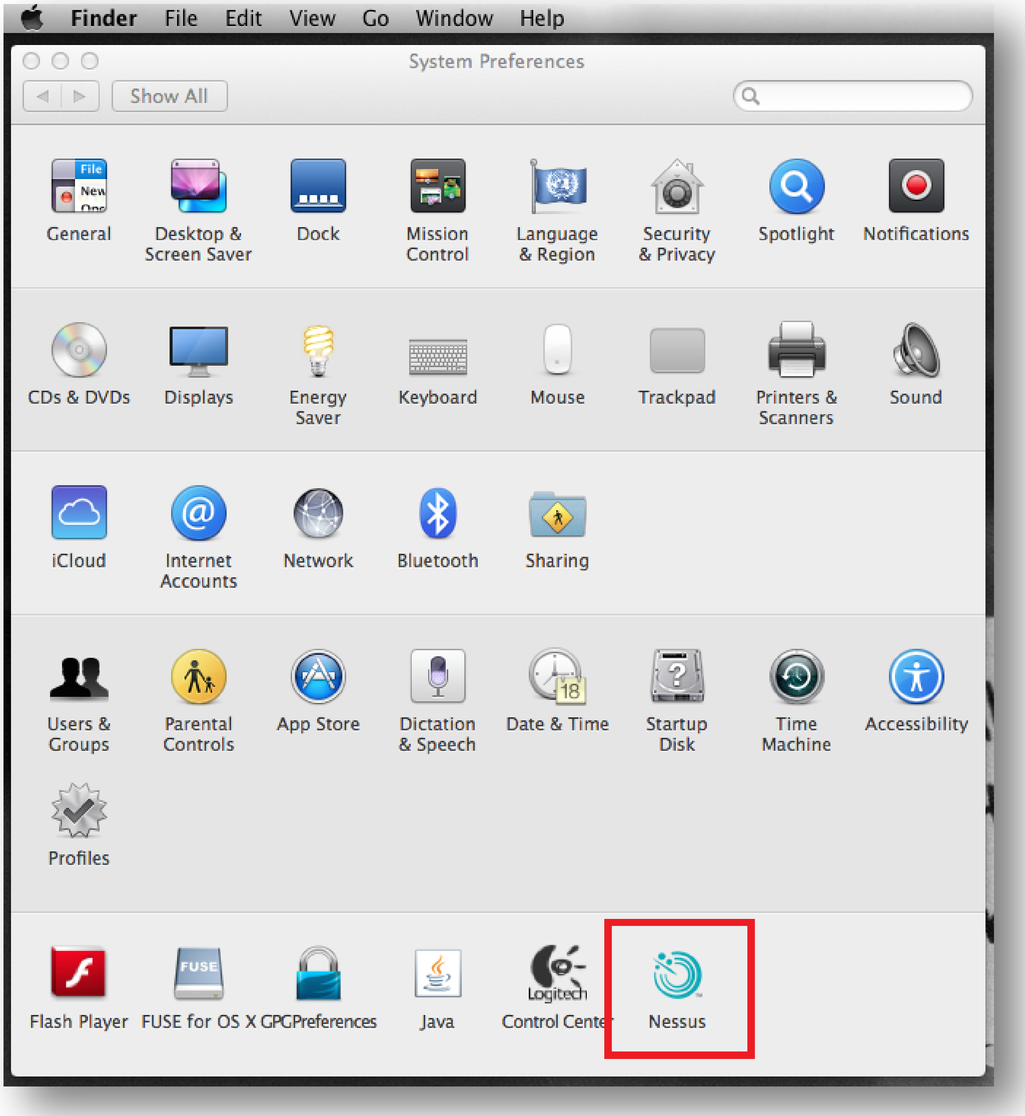
At this point, Nessus will continue by loading a page in your default web browser that will handle the initial configuration, which is discussed in the section "Feed Registration and UI Configuration".

Starting and Stopping the Nessus Service

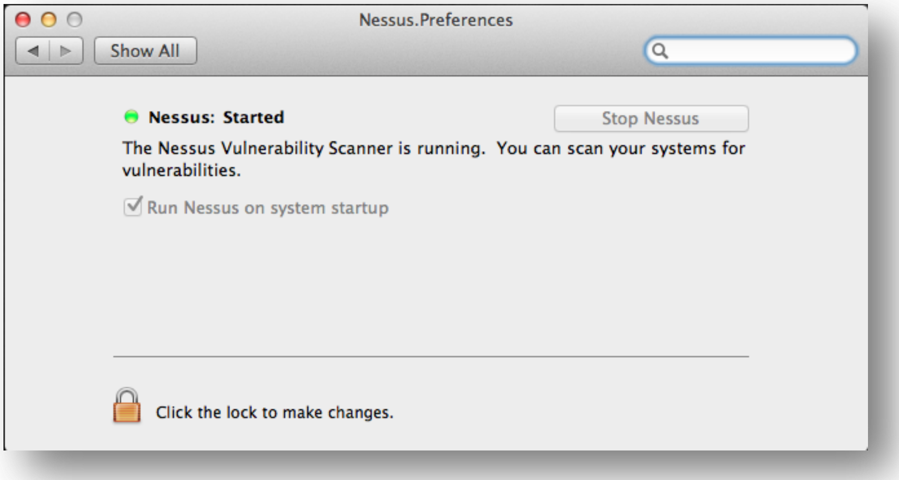
After the installation, the **nessusd** service will start. During each reboot, the service will automatically start. If there is a reason to start or stop the service, it can be done via a Terminal window (command line) or via System Preferences. If performed via the command line, it must be run as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

Action	Command to Manage **nessusd**
Start	`# launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist`
Stop	`# launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist`

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



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



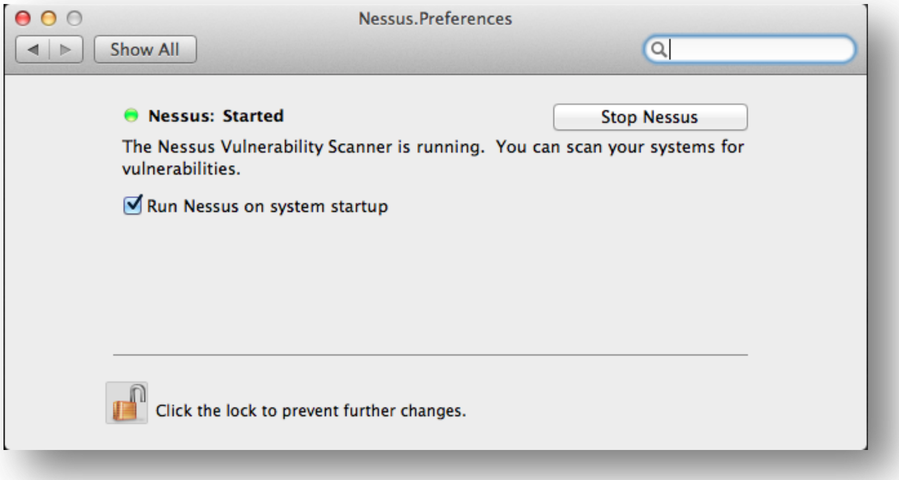
● Nessus: Started

The Nessus Vulnerability Scanner is running. You can scan your systems for vulnerabilities.

☑ Run Nessus on system startup

Click the lock to make changes.

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



● Nessus: Started

The Nessus Vulnerability Scanner is running. You can scan your systems for vulnerabilities.

☑ Run Nessus on system startup

Click the lock to prevent further changes.

Removing Nessus

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

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

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

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

Once the files are removed, disable the Nessus service. This prevents Mac OS X from trying to start a non-existing service.

To disable the Nessus service:

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

Migrating Nessus

It is not uncommon for a system administrator to have to migrate a Nessus implementation from one machine to another. To migrate a Nessus installation from one Mac OS X system to another, follow the steps below. The steps cover copying over the critical files needed as well as correctly installing Nessus on the new system.

The important files that need to be migrated from the old installation to the new installation are:

- `/Library/Nessus/run/var/nessus/global.db`
- `/Library/Nessus/run/var/nessus/master.key`
- `/Library/Nessus/run/var/nessus/policies.db`

The important directories that need to be migrated from the old installation to the new installation are:

- `/Library/Nessus/run/var/nessus/users`
- `/Library/Nessus/run/etc/nessus`

> The migration steps works for Nessus 5 and higher. You will be able to migrate from Nessus 5.2.7 to Nessus 6, but not be able to downgrade.

The first steps are done on the original system where you have Nessus installed.

1. Open a terminal window and run the **sudo** or **su** command to enable root privileges. You will be prompted for the user password:

2. Stop the Nessus service:

   ```
   # launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
   ```

3. Change to the root directory:

   ```
   # cd /
   ```

4. Backup the critical files in **/Library/Nessus/run/var/nessus** and the entire **/Library/Nessus/run/etc/nessus** directory. Given these will be copied to another system, Tenable recommends creating a tar ball of the files and directories:

   ```
   # tar -zcvf /tmp/tarOfMyNessusInstallation.tar.gz
   /Library/Nessus/run/var/nessus/global.db
   /Library/Nessus/run/var/nessus/master.key
   /Library/Nessus/run/var/nessus/policies.db
   /Library/Nessus/run/var/nessus/users
   /Library/Nessus/run/etc/nessus
   ```

   This will create a tar file in the **/tmp** directory with the name **tarOfMyNessusInstallation.tar** format.

5. Copy over the tar ball to the new server:

```
# scp /tmp/tarOfMyNessusInstallation.tar.gz mynewsystem:/tmp
```

On the new server, perform the following steps:

1. Install the Nessus 6.4 x64 DMG package, according to the installation instructions at the beginning of the Mac OS X section of this document.

2. When the Nessus login page opens in your web browser, close the page or tab.

3. Open a terminal window and run the **sudo** command. You will be prompted for the user password:

   ```
   # sudo -s
   Password:
   ```

4. Stop the Nessus service:

   ```
   # launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
   ```

5. Log in to the Tenable Support Portal and reset the Nessus activation code for this installation.

6. Restore and overwrite the critical files from the older server. To do this, untar the tar ball in the correct directory:

   ```
   # mv tmp/tarOfMyNessusInstallation.tar.gz /
   # tar -zxvf tarOfMyNessusInstallation.tar.gz
   ```

7. Register the activation code with this installation. This will also have Nessus fetch the latest plugins.

   ```
   # /Library/Nessus/run/sbin/nessuscli fetch -register <activation code>
   ```

8. Re-index Nessus plugins. This may take up to 15-20 minutes, depending on your system.

   ```
   # /Library/Nessus/run/sbin/nessus-service -R
   ```

9. Once Nessus completes the re-indexing process, restart the Nessus service:

   ```
   # launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nessusd.plist
   ```

10. Log in to your Nessus scanner using the Nessus UI at https://yoursystem:8834/.

11. Once you confirm your new system is working correctly and all the files are migrated, go through the removal process on the original system listed in the Mac OS X section of this document.

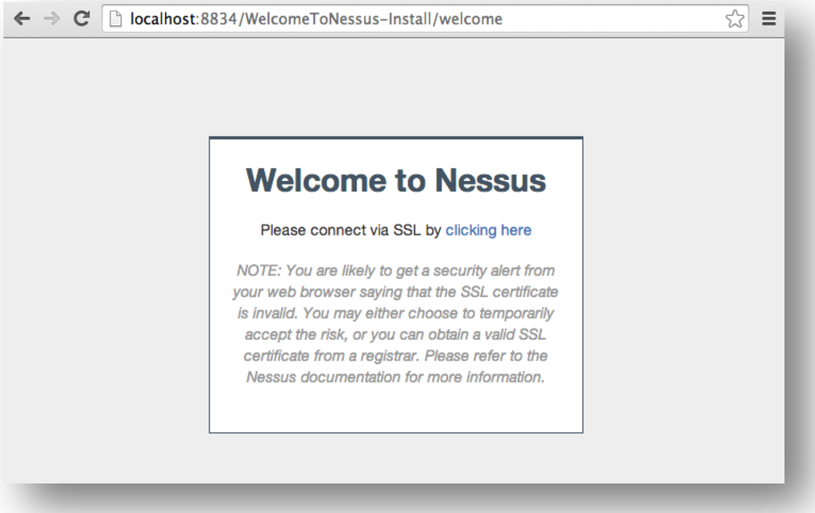
For backing up and/or restoring a complete Nessus installation, please contact Tenable Support if you have any questions. This will help to ensure there are no deviations from a normal installation that may prevent critical data from being maintained.

Feed Registration and UI Configuration

This section describes how to configure the Nessus 6 server on all platforms. 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.

If the software installation does not open your web browser to the configuration page, you can load a browser and go to https://[Nessus Server IP]:8834/WelcomeToNessus-Install/welcome (or the URL provided during the install process) to begin the process.

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 or `/etc/hosts` file, you must connect to the Nessus server using an IP address or a valid DNS name.



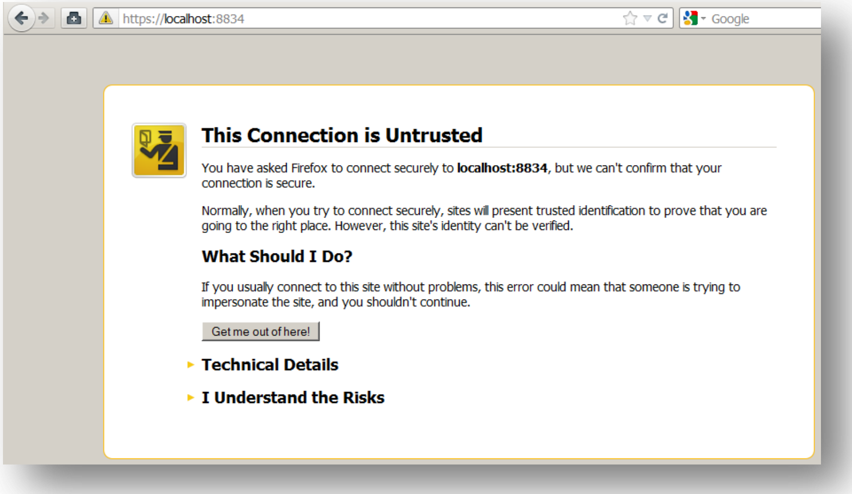
Welcome to Nessus

Please connect via SSL by clicking here

NOTE: You are likely to get a security alert from your web browser saying that the SSL certificate is invalid. You may either choose to temporarily accept the risk, or you can obtain a valid SSL certificate from a registrar. Please refer to the Nessus documentation for more information.

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

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



This Connection is Untrusted

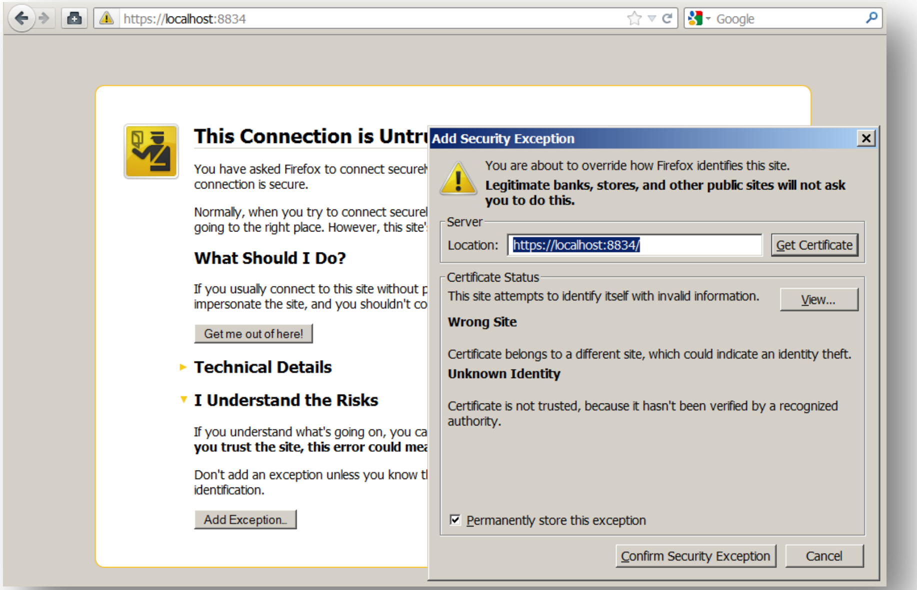
You have asked Firefox to connect securely to **localhost:8834**, but we can't confirm that your connection is secure.

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

What Should I Do?

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

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



https://localhost:8834

Google

This Connection is Untru

You have asked Firefox to connect securel
connection is secure.

Normally, when you try to connect securel
going to the right place. However, this site'

What Should I Do?

If you usually connect to this site without p
impersonate the site, and you shouldn't co

Get me out of here!

Technical Details

I Understand the Risks

If you understand what's going on, you ca
you trust the site, this error could mea

Don't add an exception unless you know t
identification.

Add Exception...

Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://localhost:8834/ Get Certificate

Certificate Status

This site attempts to identify itself with invalid information. View...

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

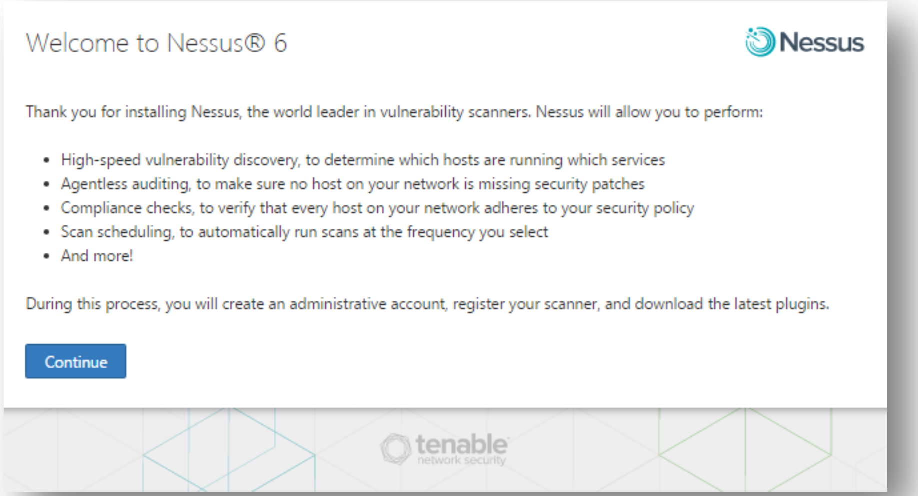
Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

Confirm Security Exception Cancel

Once accepted, you will be redirected to the initial registration screen that begins the walk-through. Click **Continue**.



Welcome to Nessus® 6

Nessus

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

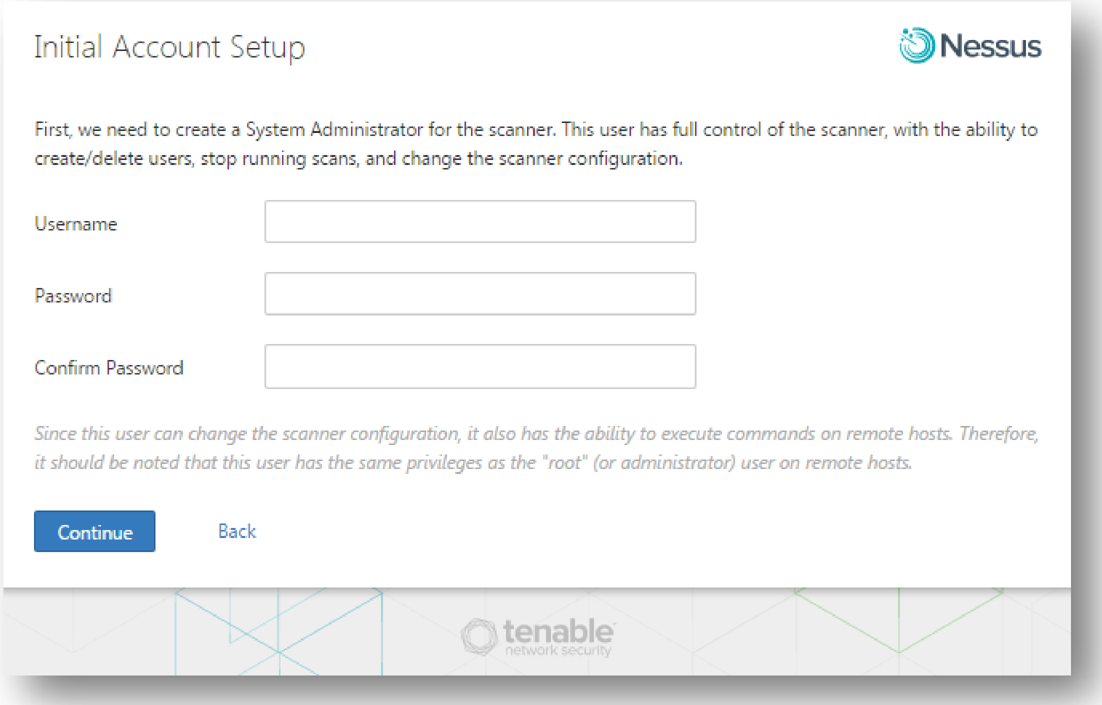
- High-speed vulnerability discovery, to determine which hosts are running which services
- Agentless auditing, to make sure no host on your network is missing security patches
- Compliance checks, to verify that every host on your network adheres to your security policy
- Scan scheduling, to automatically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

During this process, you will create an administrative account, register your scanner, and download the latest plugins.

Continue

tenable network security

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 a System Administrator for the scanner. This user has full control of the scanner, with the ability to create/delete users, stop running scans, and change the scanner configuration.

Username

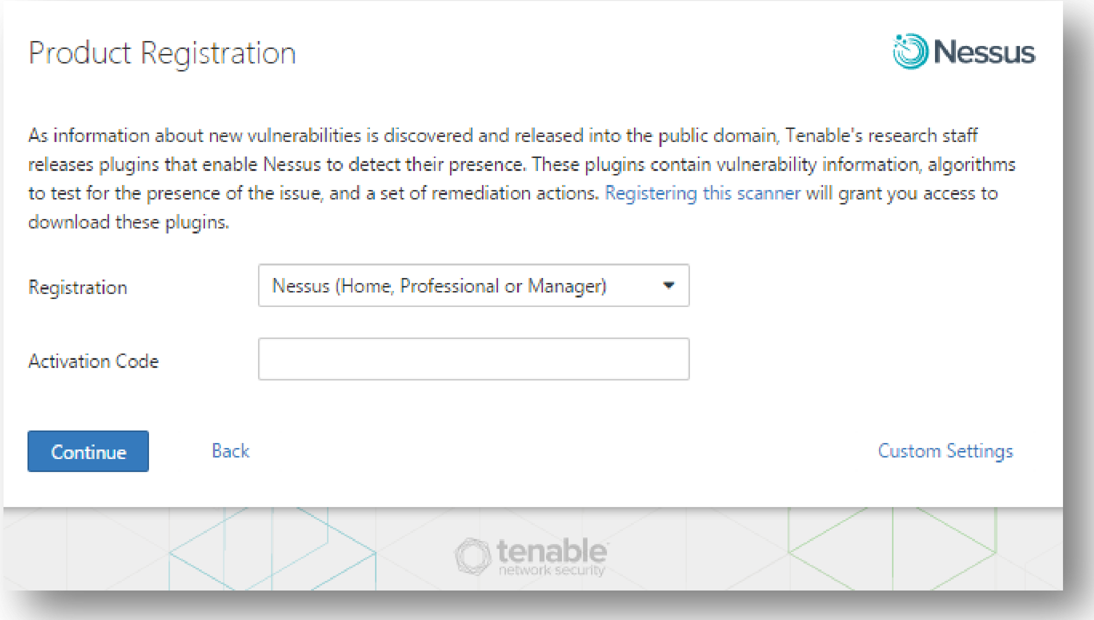
Password

Confirm Password

Since this user can change the scanner configuration, it also has the ability to execute commands on remote hosts. Therefore, it should be noted that this user has the same privileges as the "root" (or administrator) user on remote hosts.

The next screen will prompt you for which Nessus product you are installing. If you are using Nessus Manager, Nessus Professional, or Nessus Home, you will be asked for an Activation Code; you can also configure optional proxy settings. If you do not have an Activation Code, you can obtain one via the Tenable Support Portal or through your sales channel. Once registered, you will then receive an email with a link to activate the code. You must activate your code within 24 hours for Nessus to continue to operate.

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



Product Registration

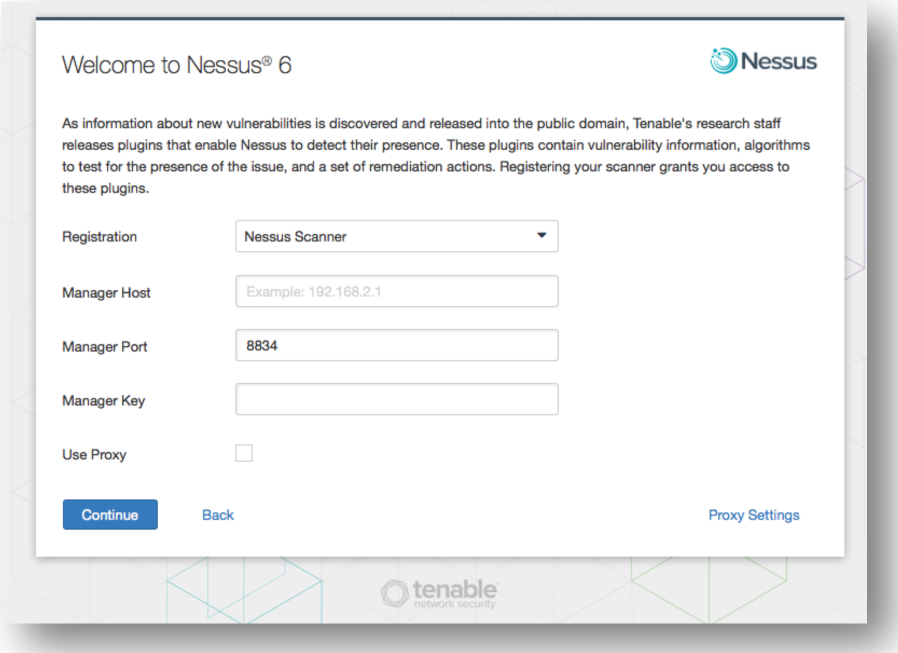
As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. Registering this scanner will grant you access to download these plugins.

Registration: Nessus (Home, Professional or Manager)

Activation Code:

If you are using Nessus Manager to manage your Nessus scanner, select “Nessus Scanner”. You will also need to input the “Manager Host” IP address, “Manager Port” number, and the “Manager Key” generated by the Nessus Manager. This will connect the Nessus scanner to the manager for plugin and engine updates, as well as receiving scans from the Manager.

> Your Nessus Manager license can only connect the amount of servers supported by your Activation Code. You cannot connect more scanners than the license allows.



Welcome to Nessus® 6

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. Registering your scanner grants you access to these plugins.

Registration: Nessus Scanner

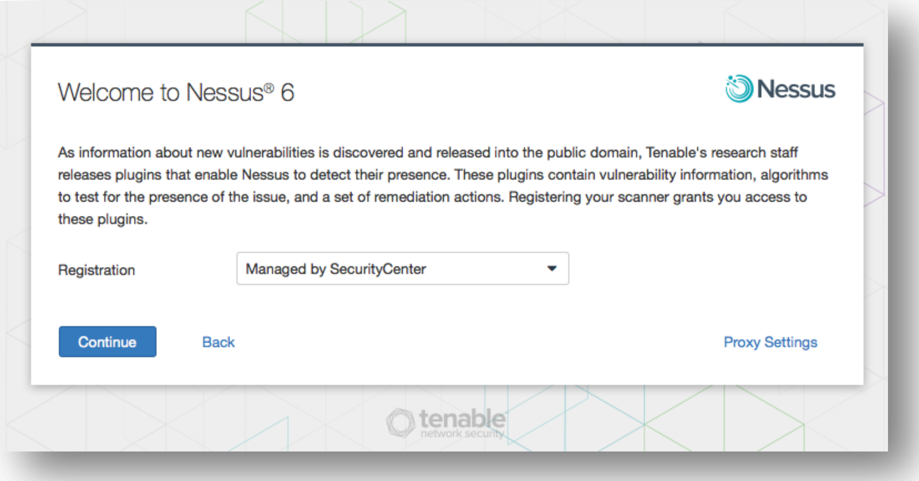
Manager Host: Example: 192.168.2.1

Manager Port: 8834

Manager Key:

Use Proxy □

If you are using Tenable's SecurityCenter to manage your Nessus scanner, 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 connect to SecurityCenter, select "Managed by SecurityCenter". 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".



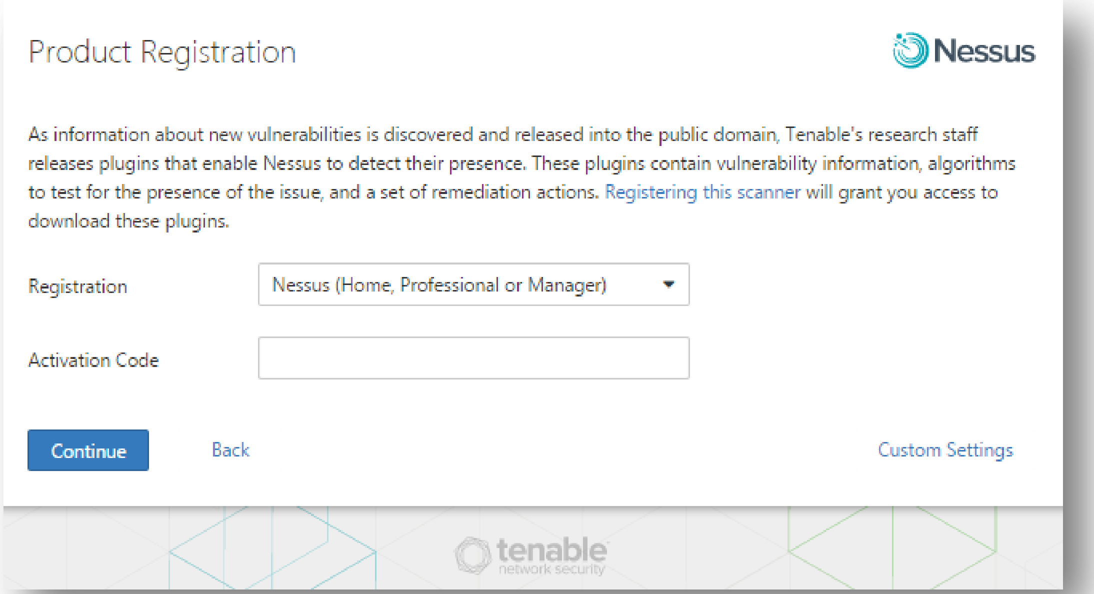
Welcome to Nessus® 6

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. Registering your scanner grants you access to these plugins.

Registration: Managed by SecurityCenter

For offline registration of plugin and engine updates, select "Offline". This option is used for Nessus implementations that do not have connectivity to the Internet (e.g., Nessus implementations in a secure data center).

Optionally, if you need to add custom settings, click on "Custom Settings" in the lower right corner:



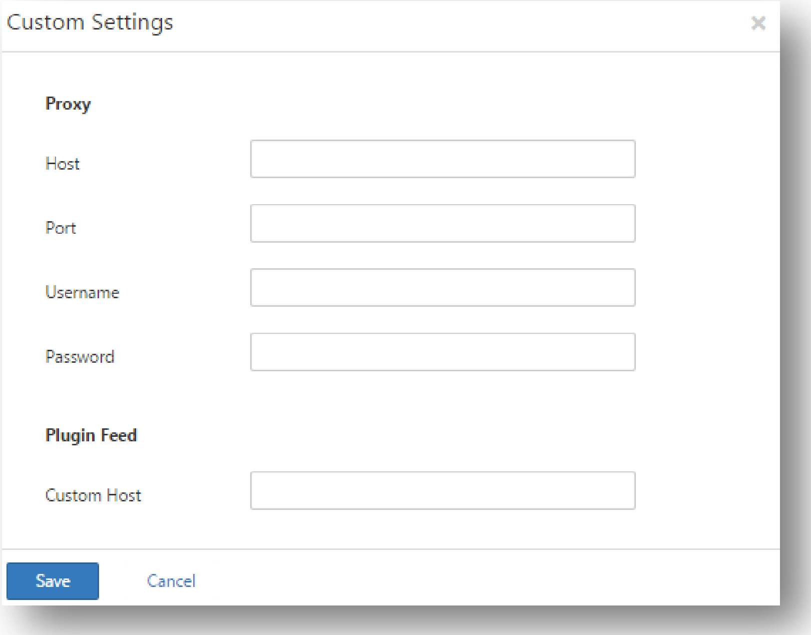
Product Registration

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. Registering this scanner will grant you access to download these plugins.

Registration: Nessus (Home, Professional or Manager)

Activation Code:

Next, type your custom settings in the fields provided.



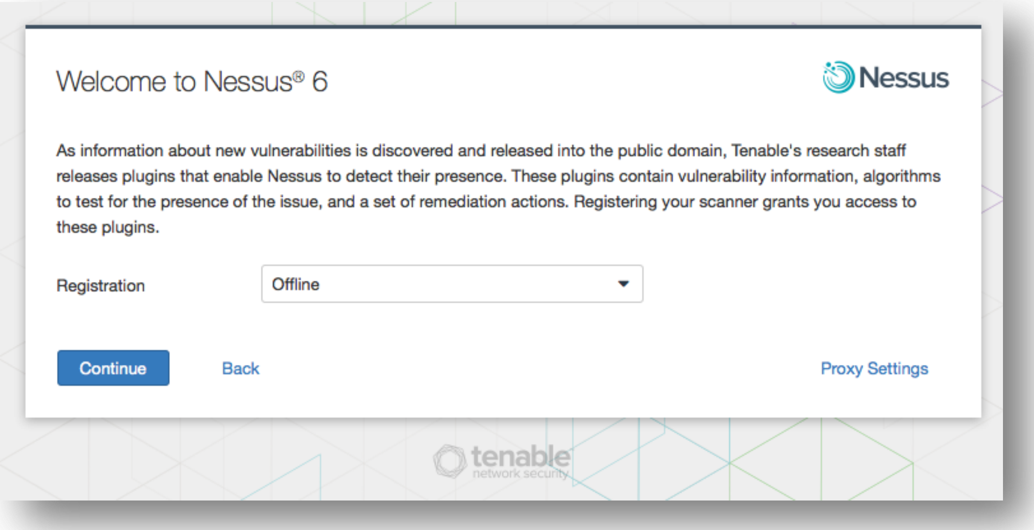
Custom Settings

Proxy

Host	
Port	
Username	
Password	

Plugin Feed

Custom Host	

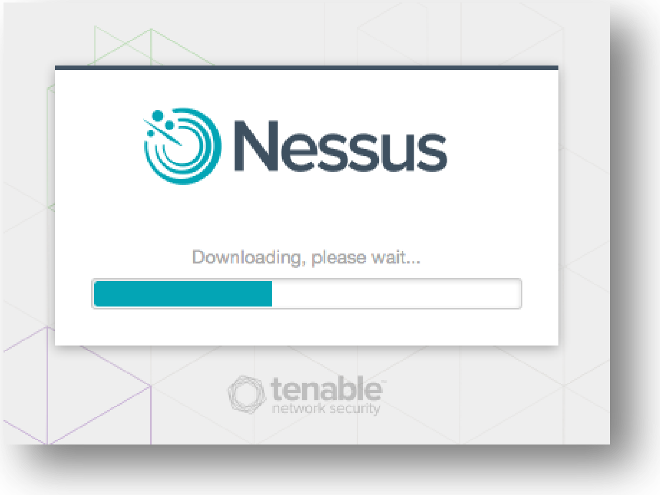


Welcome to Nessus® 6

As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff releases plugins that enable Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. Registering your scanner grants you access to these plugins.

Registration: Offline

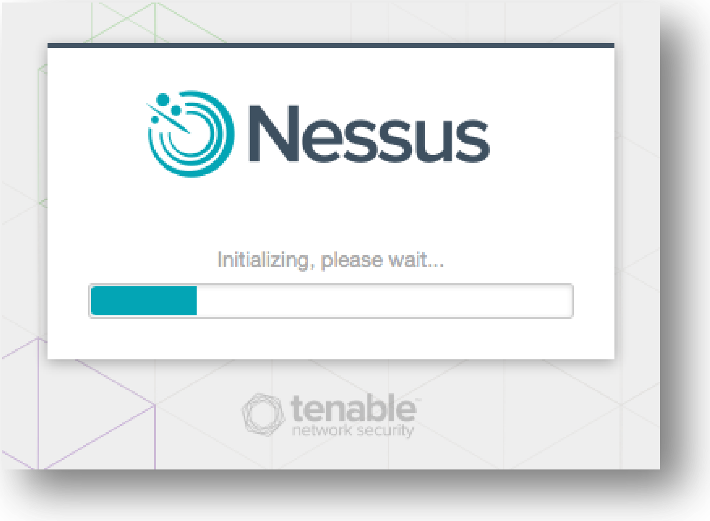
Once the Activation Code and **optional** custom setting configuration has been completed, click "**Next**" to register your scanner:



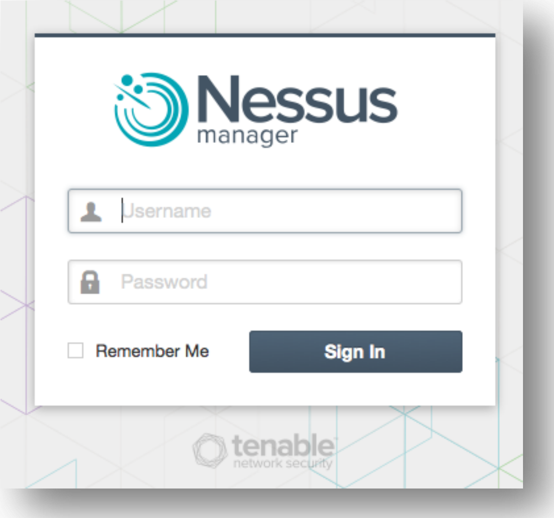
After registration, Nessus must download the plugins from Tenable. This process may take several minutes to an hour, depending on your connection speed, as it transfers a considerable amount of data to the machine, verifies file integrity, and compiles them into an internal database. Note that subsequent plugin updates are processed much more quickly.

> 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 UI will initialize and the Nessus server will start:



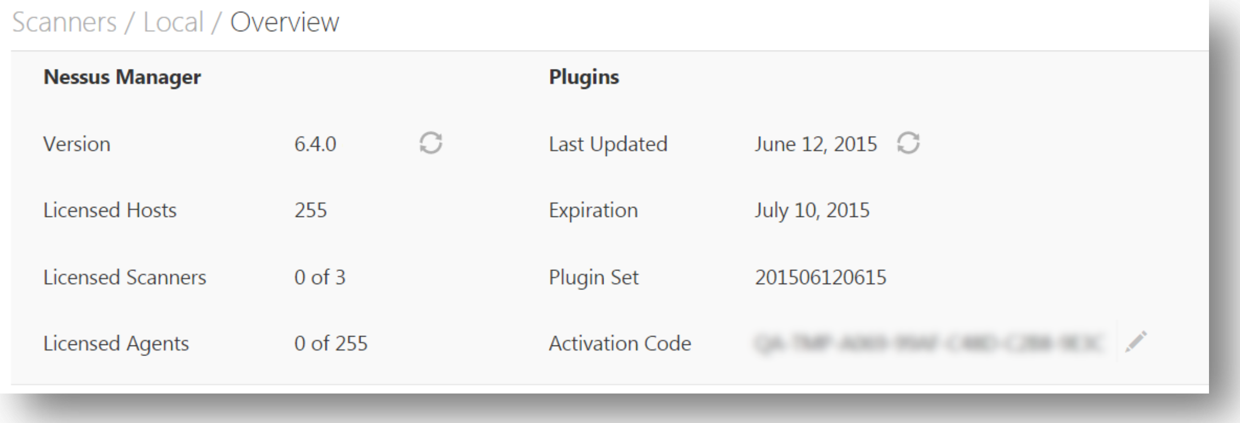
After initialization, Nessus is ready for use!



Your login screen will display the Nessus product you are connecting to via the Web UI (e.g., Professional, Scanner, Manager, and Nessus Cloud).

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

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



Scanners / Local / Overview

Nessus Manager		**Plugins**	
Version	6.4.0	Last Updated	June 12, 2015
Licensed Hosts	255	Expiration	July 10, 2015
Licensed Scanners	0 of 3	Plugin Set	201506120615
Licensed Agents	0 of 255	Activation Code	[redacted]

Nessus Cloud Prerequisites

The Nessus Cloud is an enterprise-class remote vulnerability scanning service that may be used to audit Internet-facing hosts for both network and web application vulnerabilities “from the cloud”. Subscribers who log in to Nessus scanners hosted in Tenable’s secure data center may employ the Nessus Cloud to scan any number of Internet-facing sites. This includes a wide variety of devices –enterprise servers, desktop computers, mobile laptops, iPhones – wherever is convenient and as often as needed.

The Nessus Cloud portal provides secure access to detailed vulnerability audits and remediation information hosted on Tenable’s infrastructure. The Nessus Cloud can be accessed from any computer with Internet access and a standard web browser, as well as from mobile devices including Android and iPhone/iPad, providing fixed or mobile scanner command and control, plus access to vulnerability and compliance reports from anywhere, anytime. The Nessus Cloud is supported by a world-renowned research team and has the industry's largest vulnerability knowledge base, making it suitable for even the most complex audits.

Subscription and Activation

Tenable's Nessus Cloud is available as a subscription through the Tenable Store. For pricing, please contact Tenable Sales for more information.

A Nessus Cloud subscription package includes:

- Unlimited scanning of your perimeter systems
- Web application audits
- Ability to prepare for security assessments against current PCI standards
- Up to 2 quarterly report submissions for PCI ASV validation through Tenable Network Security, Inc.
- 24/7 access to the Tenable Support Portal for Nessus knowledgebase and support ticket creation
- One user account per subscription

Upon purchase of a Nessus Cloud subscription, Tenable Product Delivery will notify the customer of product availability via email. The notification email will also include the customer's order number, product expiration date, and a product activation link. For more information, see the "Nessus Cloud User Registration" help document.

If you experience any problems with the activation process, please contact licenses@tenable.com. You must include your Customer ID with any inquiry. If you do not have a Customer ID, please include your order number to receive the proper assistance.

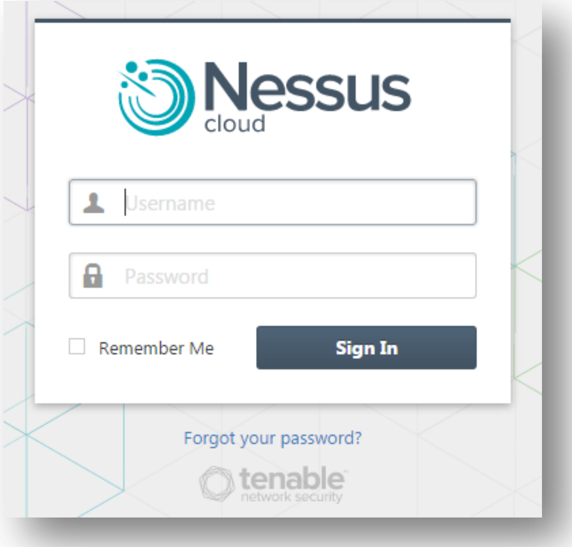
Connecting to your Nessus Cloud Account

To launch the Nessus UI, perform the following:

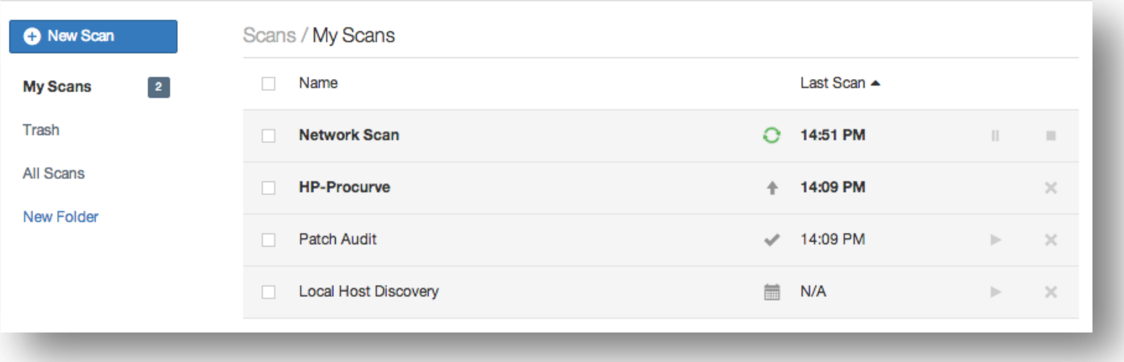
- Open a web browser of your choice.
- Enter https://cloud.tenable.com/ in the navigation bar.

> Be sure to connect to the user interface via HTTPS, as unencrypted HTTP connections are not supported.

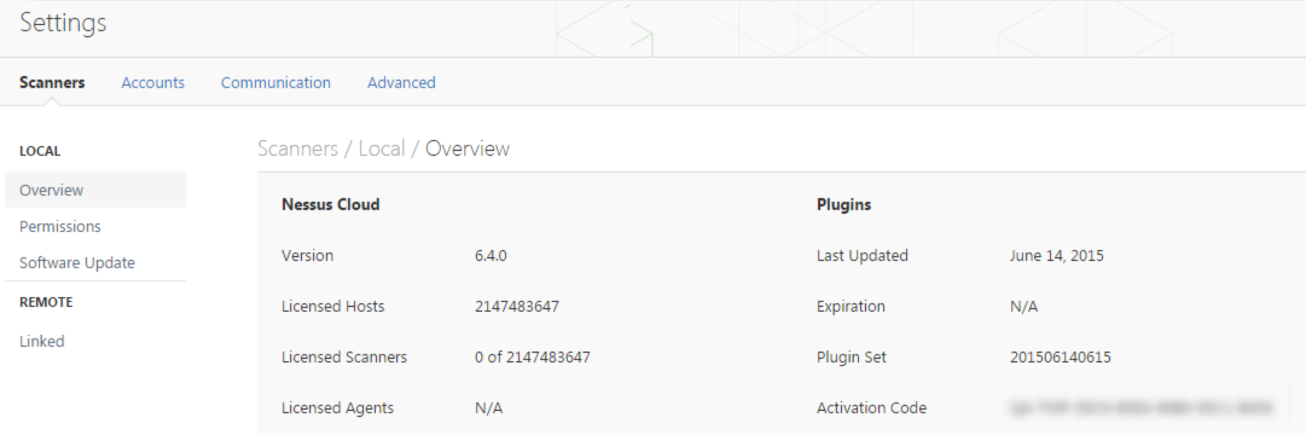
After your browser has confirmed the exception, a splash screen will be displayed as follows:



Authenticate using the administrative account and password previously created during the installation process. When logging in, you can optionally instruct your browser to remember the username on that computer. Only use this option if the computer is always in a secured location! After successful authentication, the UI will present menus to manage policies and scans. Administrative users will also see options for user management, and configuration options for the Nessus Cloud scanner:



Name	Last Scan ▲
Network Scan	14:51 PM
HP-Procurve	14:09 PM
Patch Audit	14:09 PM
Local Host Discovery	N/A



Settings

Scanners Accounts Communication Advanced

LOCAL
- Overview
- Permissions
- Software Update

REMOTE
- Linked

Scanners / Local / Overview

Nessus Cloud		Plugins	
Version	6.4.0	Last Updated	June 14, 2015
Licensed Hosts	2147483647	Expiration	N/A
Licensed Scanners	0 of 2147483647	Plugin Set	201506140615
Licensed Agents	N/A	Activation Code	[redacted]

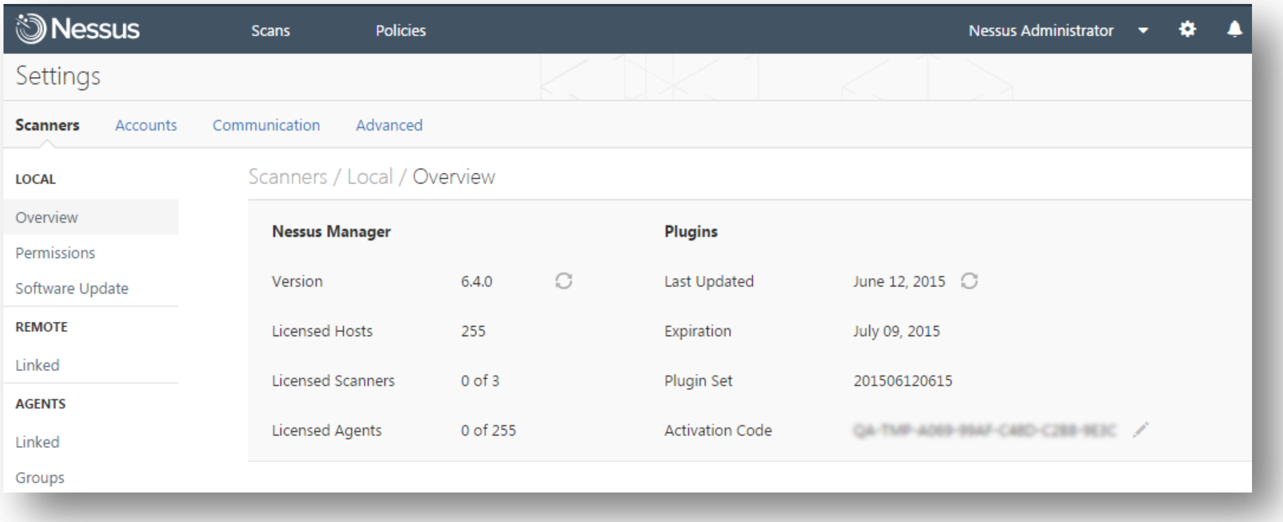
The “**Scanners**” menu shows available scanners. The multi-scanner option is already enabled; you must use the Nessus Cloud username/password authentication for connecting scanners.

The “**Accounts**” menu controls settings related to the user accounts, and can only be set by an administrator.

Configuration

Nessus Manager, Server, and Professional configuration is managed via the UI. The **`nessusd.conf`** file is deprecated. In addition, proxy settings, subscription feed registration, offline updates, mail server, and proxy server settings are managed via the UI. If you are using Nessus Manager, you will be able to also configure LDAP servers, secondary scanners, and Nessus Agents. For Nessus, you will only be able to see the Settings view. The scanner settings, including the users, can only be managed by the Manager.

Note that the configuration is divided into four sections: **Scanners**, **Accounts**, **Communication**, and **Advanced**.



Settings

Scanners Accounts Communication Advanced

LOCAL
- Overview
- Permissions
- Software Update

REMOTE
- Linked

AGENTS
- Linked
- Groups

Scanners / Local / Overview

Nessus Manager		Plugins	
Version	6.4.0	Last Updated	June 12, 2015
Licensed Hosts	255	Expiration	July 09, 2015
Licensed Scanners	0 of 3	Plugin Set	201506120615
Licensed Agents	0 of 255	Activation Code	[redacted]

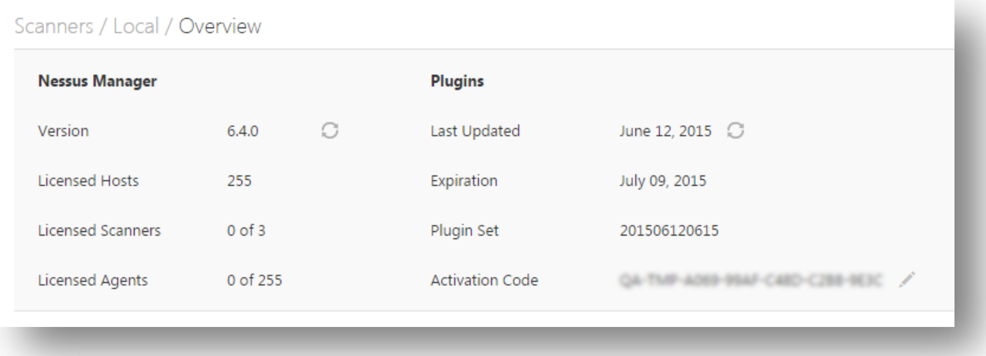
Resetting Activation Codes

If you are changing your license, you can provide an updated Activation Code both online or offline.

Resetting Activation Codes Online

After the initial Activation Code is entered during the setup process, subsequent Activation Code changes are performed through the "**Overview**" link under "**Local**". This can be accessed by clicking the pencil next to the activation code on the lower right of the UI.

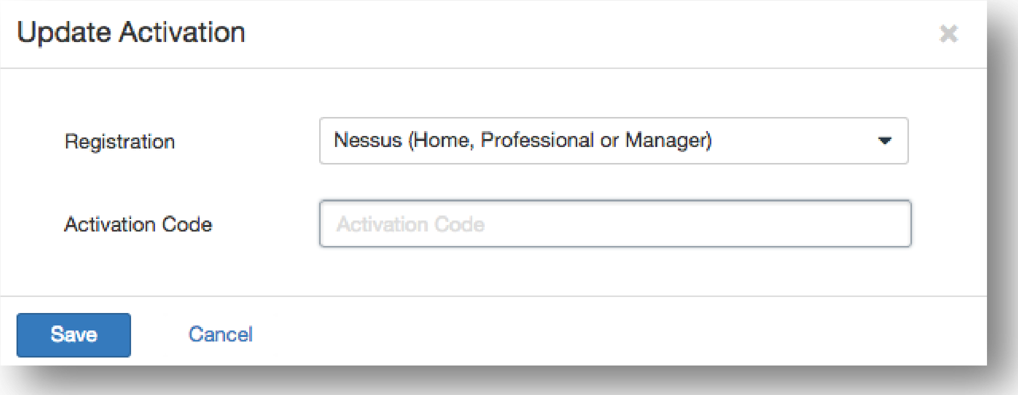
Click on the pencil next to the current Activation Code to update your code:



Scanners / Local / Overview

Nessus Manager		Plugins	
Version	6.4.0	Last Updated	June 12, 2015
Licensed Hosts	255	Expiration	July 09, 2015
Licensed Scanners	0 of 3	Plugin Set	201506120615
Licensed Agents	0 of 255	Activation Code	[redacted]

This will bring up a dialog box for inputting your new Activation Code. Inputting a new code and clicking "Save" will update the Nessus scanner with the new code (e.g., if upgrading from Nessus Home to commercial Nessus). Click "**Save**" when complete:

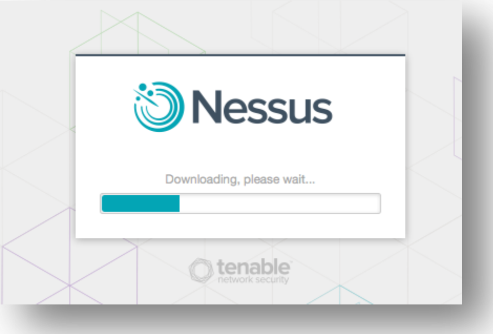


Update Activation

Registration: Nessus (Home, Professional or Manager)

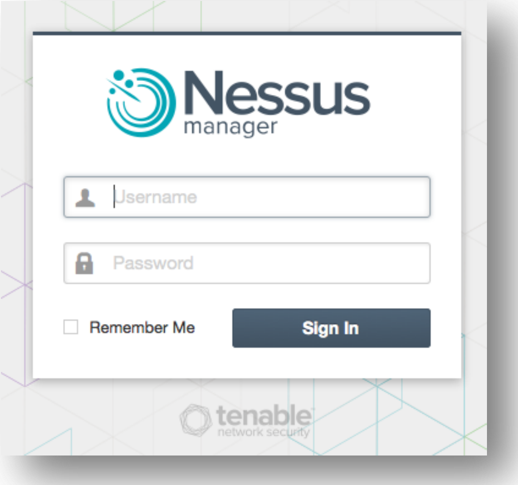
Activation Code: Activation Code

Nessus will now download the latest plugins and Nessus engine update:



Downloading, please wait...

Nessus will restart and you will need to log in again:



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

Resetting Activation Codes Offline

If your Nessus installation cannot reach the Internet directly, use the following procedure to register and update plugins:

On the system running Nessus, type the following command:

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

This will produce a string called “challenge” that looks similar to following:

```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Next, go to http://plugins.nessus.org/v2/offline.php 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 that will give you direct access to the Nessus plugins. **Save this URL because you will use it every time you update your plugins.** In addition, it will produce a file called **`nessus.license`**. Copy this file to the host running Nessus in the appropriate directory:

Platform	Directory
Linux	`# /opt/nessus/etc/nessus/`
FreeBSD	`# /usr/local/nessus/etc/nessus`
Mac OS X	`# /Library/Nessus/run/etc/nessus`
Windows	`C:\Program Files\Tenable\Nessus\conf`

Once the **`nessus.license`** file has been copied, run the **`nessuscli fetch`** command to install the file:

Platform	Directory
Linux	`# /opt/nessus/bin/nessuscli fetch --register-offline /opt/nessus/etc/nessus/nessus.license`
FreeBSD	`# /usr/local/nessus/bin/nessuscli fetch --register-offline /usr/local/nessus/etc/nessus/nessus.license`
Mac OS X	`# /Library/Nessus/run/bin/nessuscli fetch --register-offline /Library/Nessus/run/etc/nessus/nessus.license`
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe fetch --register-offline "C:\Program Files\Tenable\Nessus\conf\nessus.license"`

You can obtain the newest plugins by going to the URL that was provided in the previous step. Here, you will receive a TAR file (e.g., **`all-2.0.tar.gz`**). Copy the file to the Nessus scanner system and then type the appropriate command for your platform:

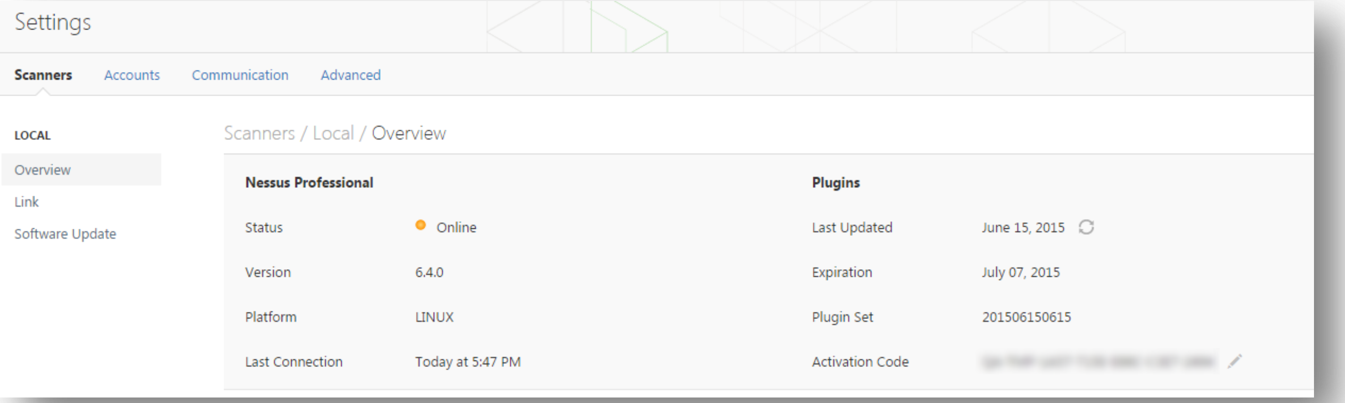
Platform	Command
Linux	`# /opt/nessus/sbin/nessuscli update all-2.0.tar.gz`
FreeBSD	`# /usr/local/nessus/sbin/nessuscli update all-2.0.tar.gz`
Mac OS X	`# /Library/Nessus/run/sbin/nessuscli update all-2.0.tar.gz`
Windows	`C:\Program Files\Tenable\Nessus>nessuscli.exe update all-2.0.tar.gz`

For more information on using **`nessuscli`** and the command line options, please see the document “Nessus 6.4 Command Line Reference”.

Local Settings

The Local section of the Settings shows the local scanner Nessus version and plugin information and software updates. In **Nessus Professional**, the options include “Overview”, “Link”, and “Software Update”.

In Nessus Manager, this also includes information on remote scanners and agents:



Settings

Scanners / Local / Overview

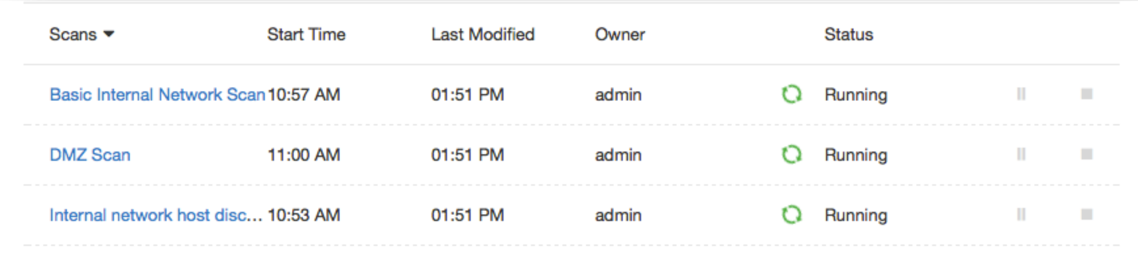
Nessus Professional		Plugins	
Status	● Online	Last Updated	June 15, 2015
Version	6.4.0	Expiration	July 07, 2015
Platform	LINUX	Plugin Set	201506150615
Last Connection	Today at 5:47 PM	Activation Code	[redacted]

The Nessus scanner shows the “**Overview**” and “**Link**”. The Nessus Manager controls the software update for the Nessus scanner.

Overview

The Overview section shows information about the Nessus configuration. This includes the Nessus product type and its version, owner, last connection, and platform. Additionally, it provides information on the plugins, including when the plugins were last updated, expiration, plugin set, and the Activation Code (if the system is running Nessus Manager or Professional).

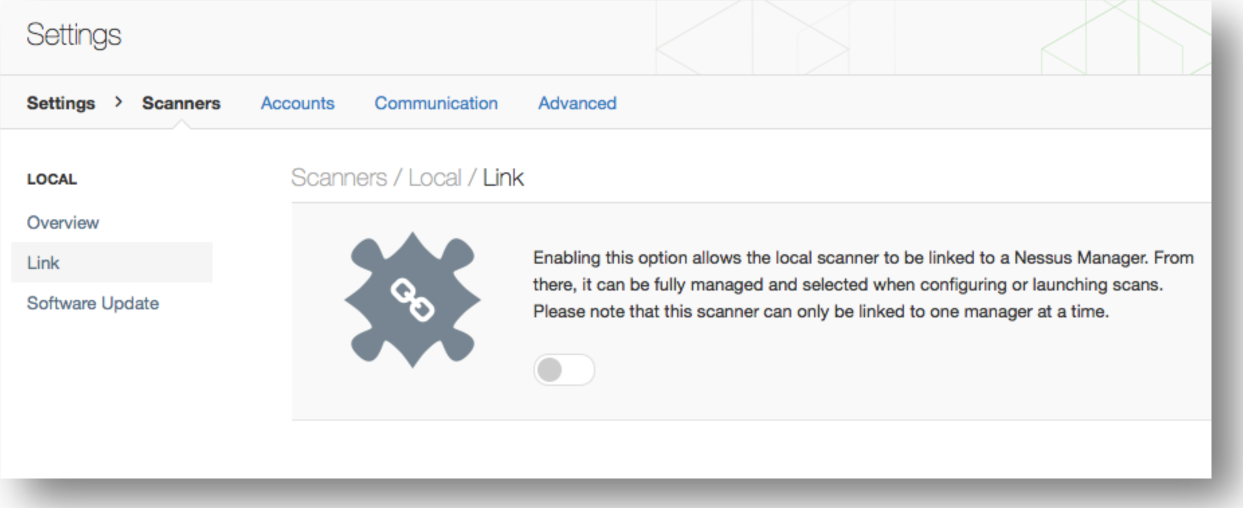
If any scans are running, they will also be displayed:



Scans ▾	Start Time	Last Modified	Owner	Status
Basic Internal Network Scan	10:57 AM	01:51 PM	admin	Running
DMZ Scan	11:00 AM	01:51 PM	admin	Running
Internal network host disc...	10:53 AM	01:51 PM	admin	Running

Link

The Link section displays a toggle switch on connecting the Nessus scanner to Nessus Manager. This is covered in detail in the “Multi-Scanner” section of this document.

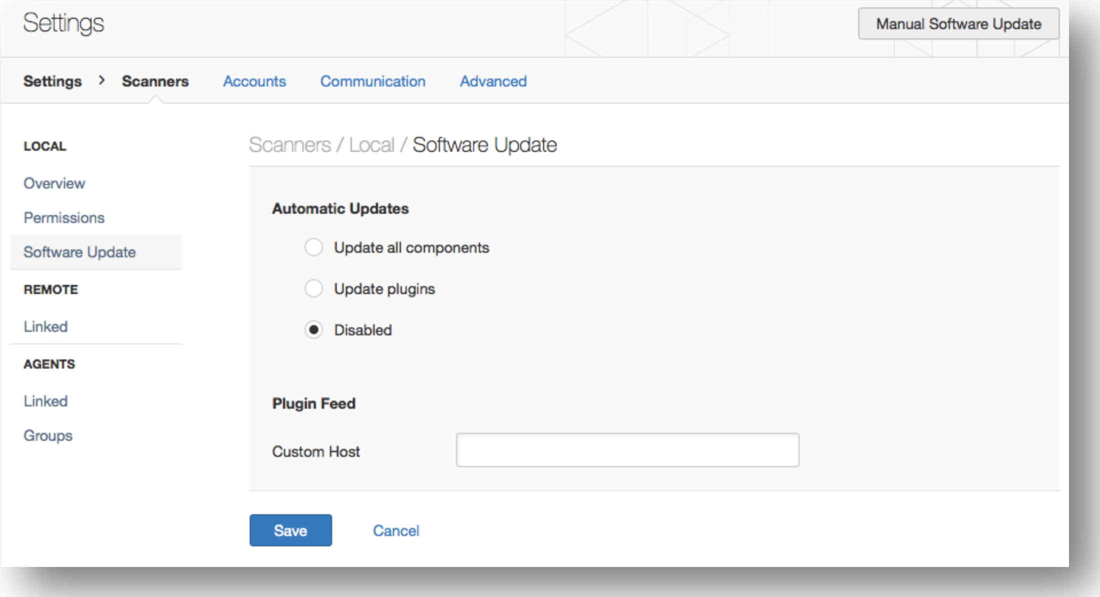


Enabling this option allows the local scanner to be linked to a Nessus Manager. From there, it can be fully managed and selected when configuring or launching scans. Please note that this scanner can only be linked to one manager at a time.

Software Update

Under the Local scanner for Nessus Manager and Nessus Professional, you can configure "**Software Update**". 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`".

Additionally, you can update the plugins or all components automatically. This is toggled through the radio buttons listed below **Automatic Updates**.



Automatic Updates

○ Update all components

○ Update plugins

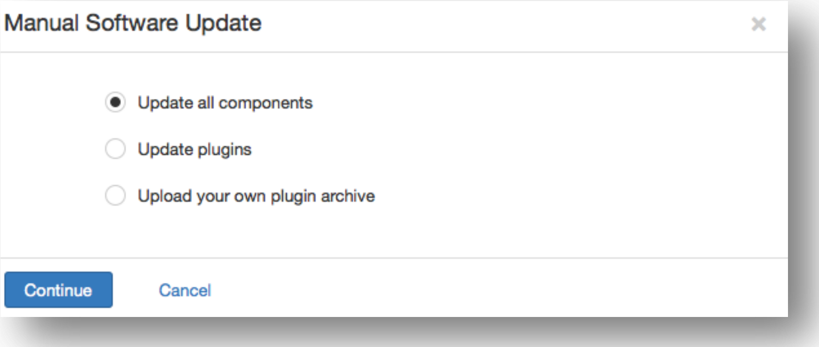
● Disabled

Plugin Feed

Custom Host

In the upper right corner of the Software Update page, there's a **Manual Software Update** button. This allows you to specify plugins for updating, update all components, or a customer plugin library for processing. This also allows you to do offline updates.

For more details on offline updating, consult the "Nessus without Internet Access" section later in this document.



Manual Software Update

● Update all components

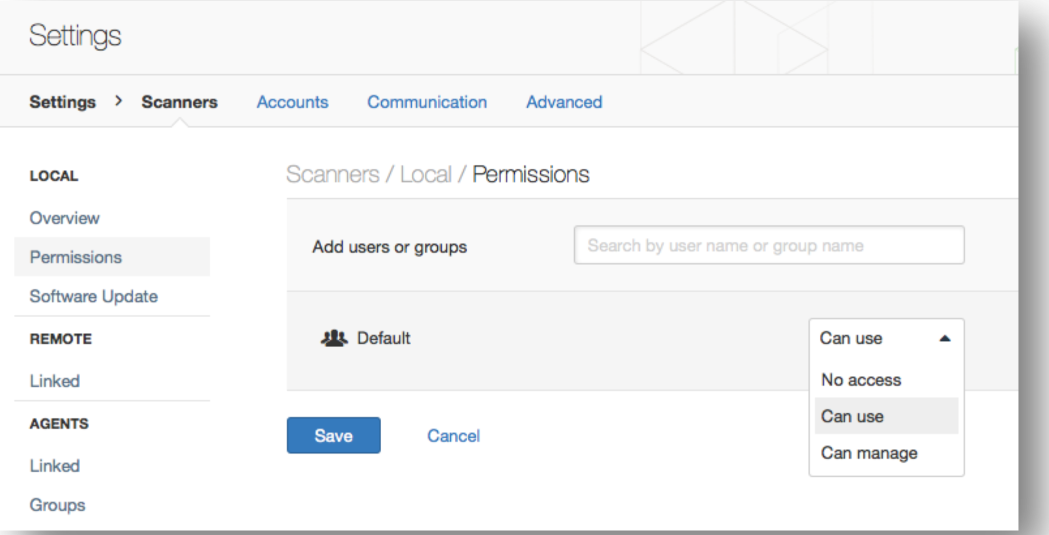
○ Update plugins

○ Upload your own plugin archive

Note that if “Update plugins” is selected, the scanner will not receive automatic updates for the Web UI and engine, which could prevent new features from working.

Permissions

In Nessus Manager, you can control the permissions of the local scanner by the username or group name:



Settings

Scanners / Local / Permissions

Add users or groups: Search by user name or group name

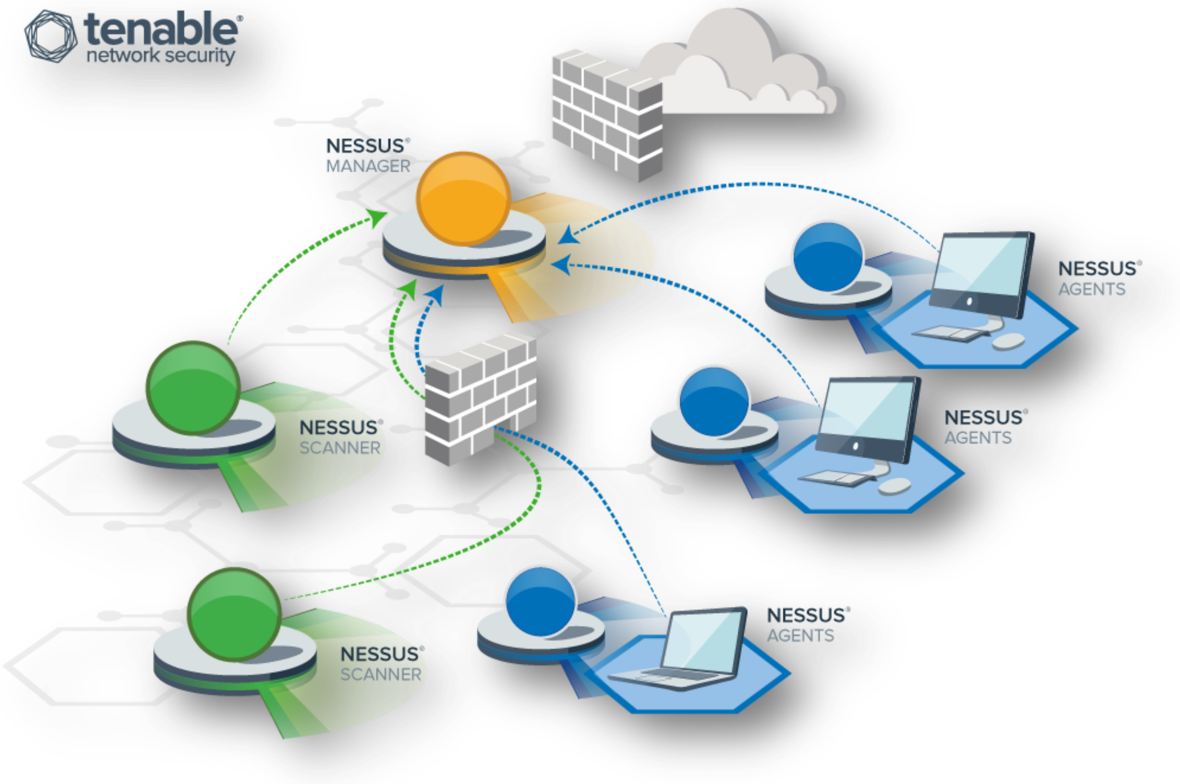
Default: Can use

Permission	Description
No Access	Any users or groups specified cannot view, use, or manage the Scanners.
Can Use	Users or groups specified here can view and use the scanner; they will not be able to make any changes.
Can Manage	Users or groups specified here can make changes to the Scanner’s settings.

Multi-Scanner

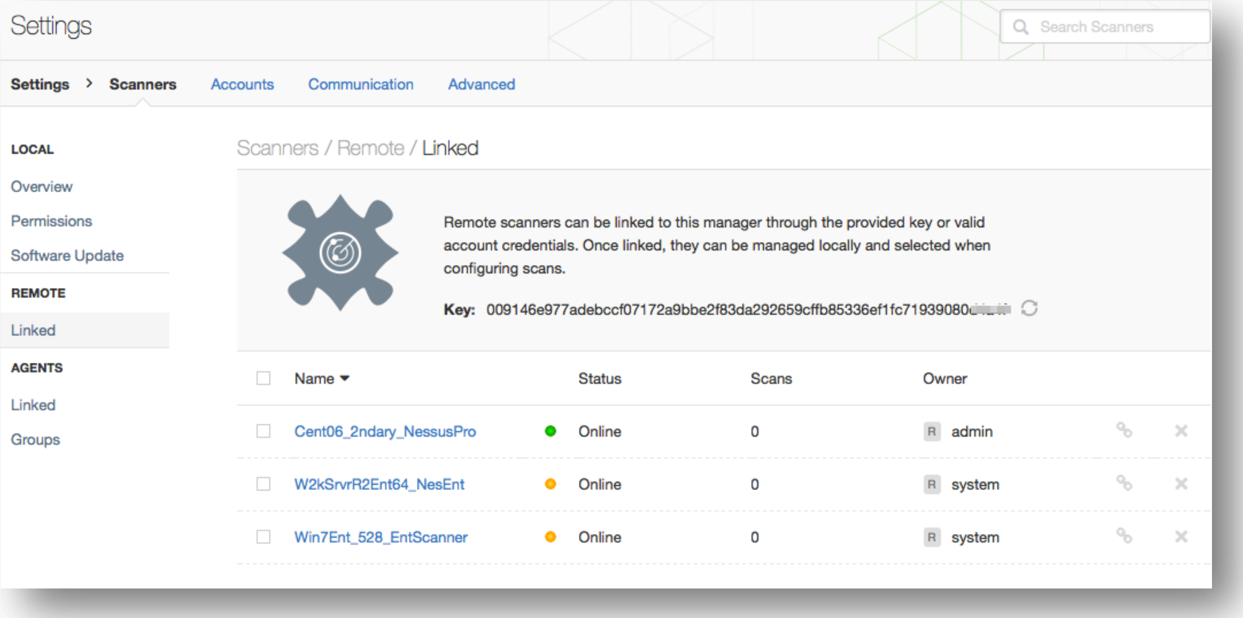
The Multi Scanner functionality gives your Nessus Manager the ability to delegate vulnerability scanning to multiple secondary servers, or be delegated to perform scans for another. This allows for consolidated reporting in a single Nessus user interface with scheduled scanning and emailing results.

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



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

Nessus scanners have limited UI functionality. Most of the functionality is managed through the Nessus Manager. They are controlled through the "Linked" section under remote in the Nessus Manager:



Scanners / Remote / Linked

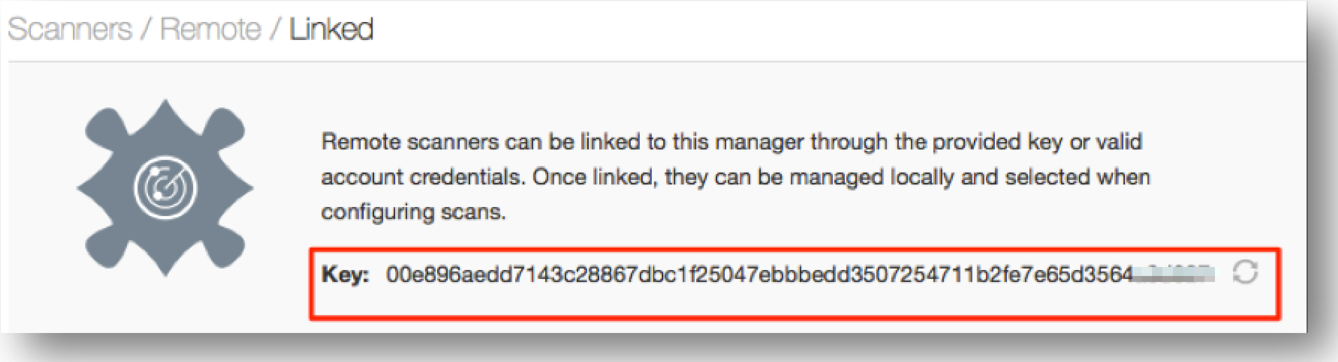
Remote scanners can be linked to this manager through the provided key or valid account credentials. Once linked, they can be managed locally and selected when configuring scans.

Key: 009146e977adebccf07172a9bbe2f83da292659cffb85336ef1fc71939080[redacted]

Name	Status	Scans	Owner
Cent06_2ndary_NessusPro	● Online	0	R admin
W2kSrvrR2Ent64_NesEnt	● Online	0	R system
Win7Ent_528_EntScanner	● Online	0	R system

Note that in addition to managing Nessus scanners, Nessus Manager can also manage Nessus Agents. Nessus Agents are covered later in this document.

Nessus Manager has the ability to designate scans to additional scanners that have been configured to be a secondary scanner. After selecting "**Settings**" under the Remote scanner section, select "**Linked**". A key will be generated that is used as a shared secret for a secondary scanner to authenticate to the primary:

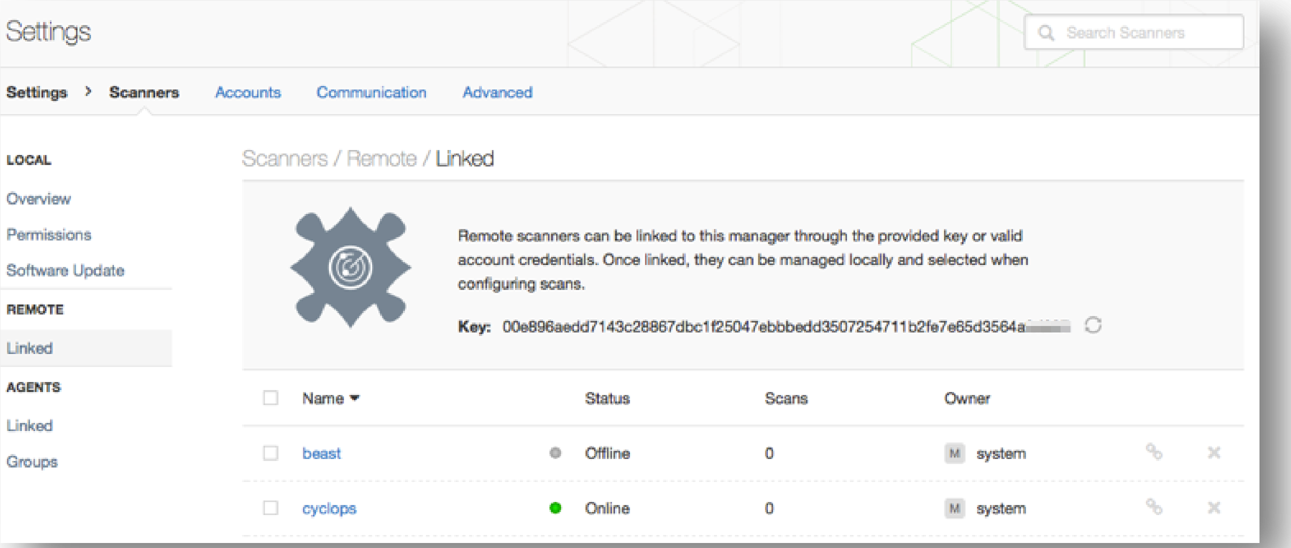


Scanners / Remote / Linked

Remote scanners can be linked to this manager through the provided key or valid account credentials. Once linked, they can be managed locally and selected when configuring scans.

Key: 00e896aedd7143c28867dbc1f25047ebbbedd3507254711b2fe7e65d3564[redacted]

If Nessus scanners are linked to Nessus Manager, they will be displayed below the key value:



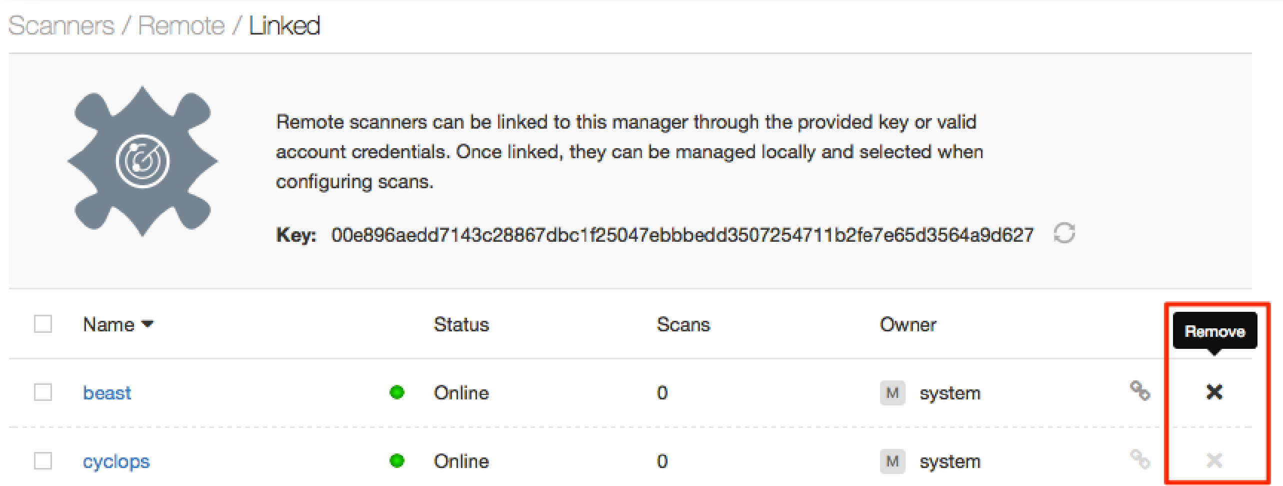
Scanners / Remote / Linked

Remote scanners can be linked to this manager through the provided key or valid account credentials. Once linked, they can be managed locally and selected when configuring scans.

Key: 00e896aedd7143c28867dbc1f25047ebbbedd3507254711b2fe7e65d3564a[redacted]

□	Name ▾		Status	Scans	Owner		
□	beast	●	Offline	0	M system		✕
□	cyclops	●	Online	0	M system		✕

This key is only used for the initial linking of the Nessus Manager and a Nessus scanner. Subsequent communication is done via a separate set of credentials. At any time, you can unlink a Nessus scanner from a Nessus Manager by clicking the “**Delete**” button after selecting the scanner.



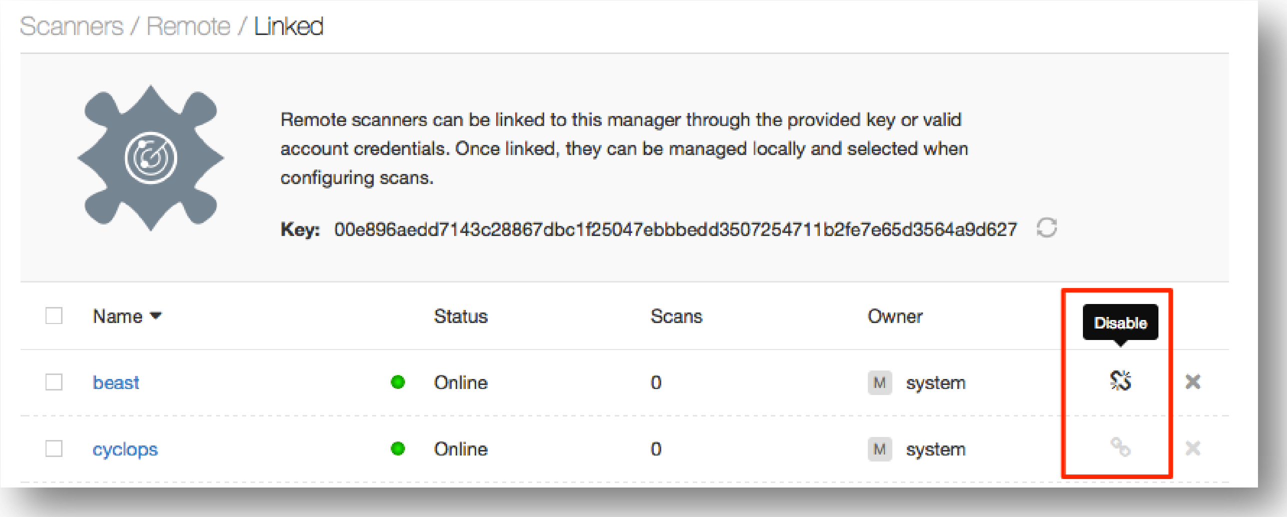
Scanners / Remote / Linked

Remote scanners can be linked to this manager through the provided key or valid account credentials. Once linked, they can be managed locally and selected when configuring scans.

Key: 00e896aedd7143c28867dbc1f25047ebbbedd3507254711b2fe7e65d3564a9d627

□	Name ▾		Status	Scans	Owner		Remove
□	beast	●	Online	0	M system		✕
□	cyclops	●	Online	0	M system		✕

You can also disable a scanner from the Nessus Manager by clicking the link:



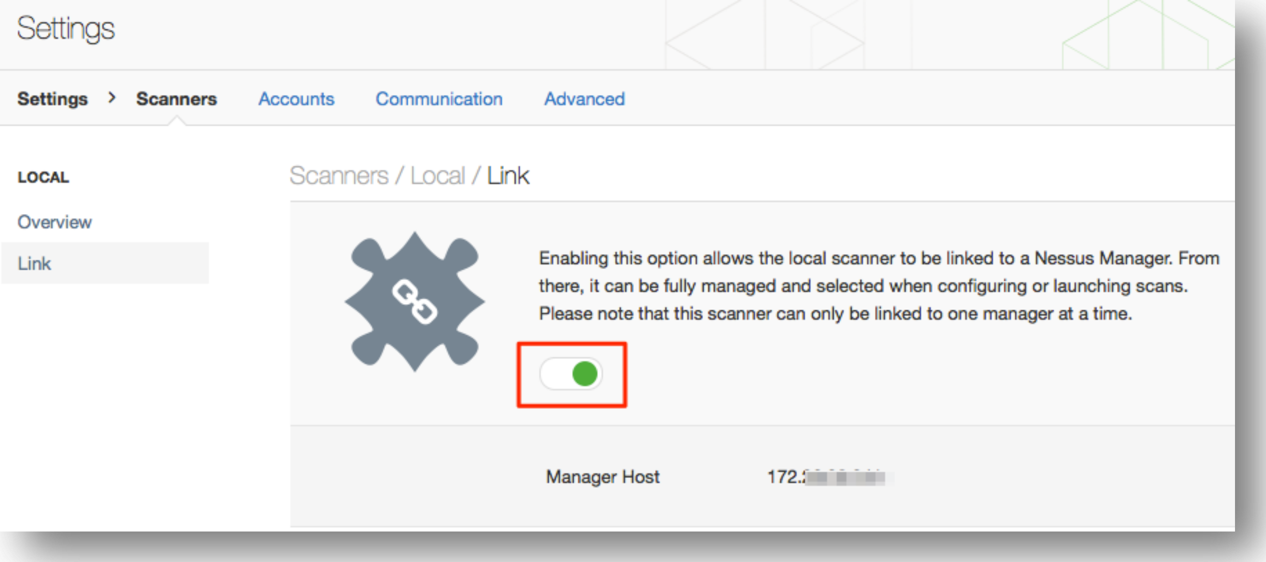
Scanners / Remote / Linked

Remote scanners can be linked to this manager through the provided key or valid account credentials. Once linked, they can be managed locally and selected when configuring scans.

Key: 00e896aedd7143c28867dbc1f25047ebbbedd3507254711b2fe7e65d3564a9d627

	Name		Status	Scans	Owner
□	beast	●	Online	0	M system
□	cyclops	●	Online	0	M system

To unlink a scanner, go to the Nessus scanner and click “**Link**” under “Local”. Toggle the switch from green to gray and click the “**Save**” button. This will clean out any previously linked scanner that is allowed to manage your local scanner.

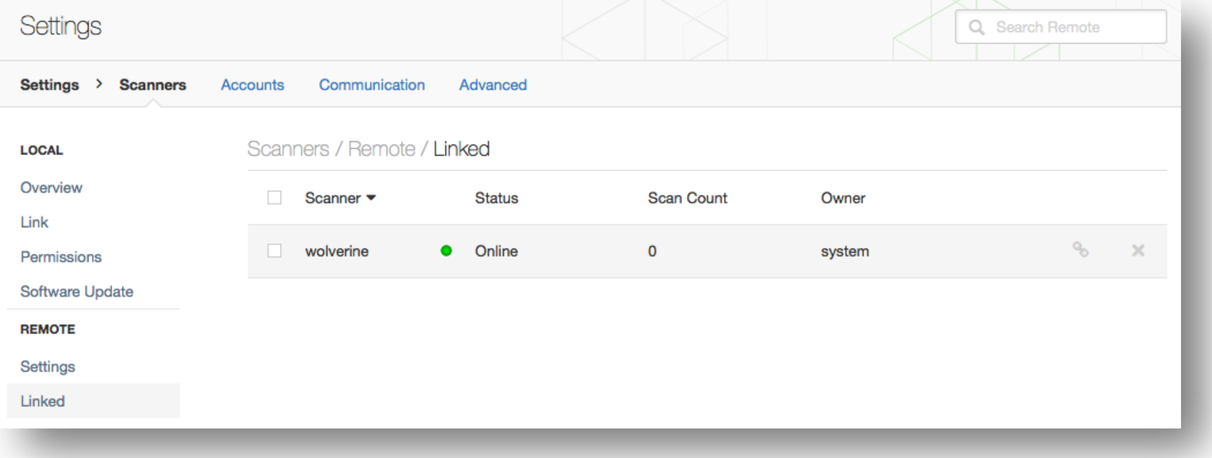


Scanners / Local / Link

Enabling this option allows the local scanner to be linked to a Nessus Manager. From there, it can be fully managed and selected when configuring or launching scans. Please note that this scanner can only be linked to one manager at a time.

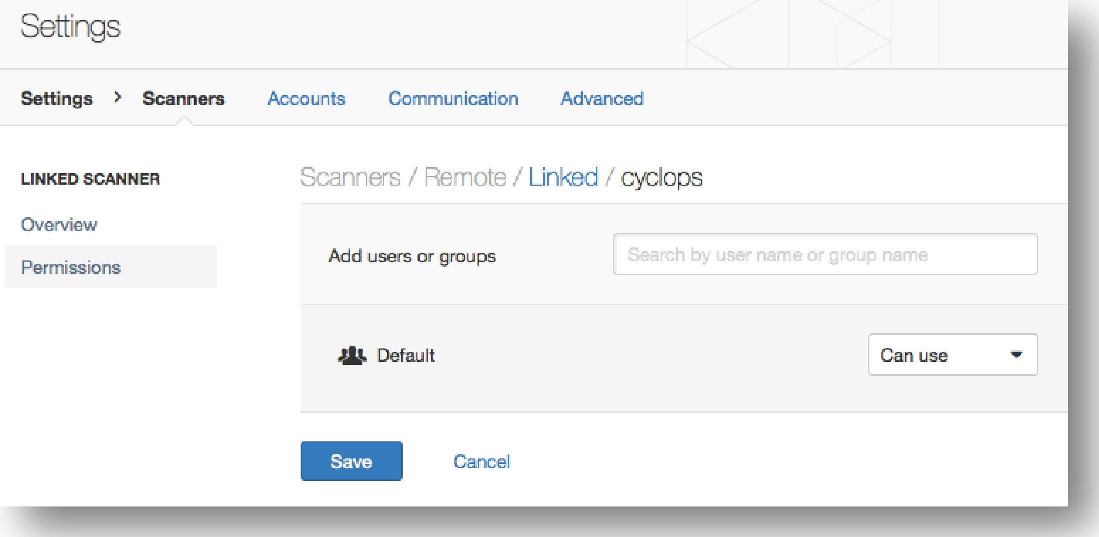
Manager Host 172.[redacted]

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



□	Scanner ▾	Status	Scan Count	Owner
□	wolverine	● Online	0	system

In Nessus Manager, you can configure the permissions of the users or groups who **Can use**, **Can manage**, or have **No access** the remote scanner:

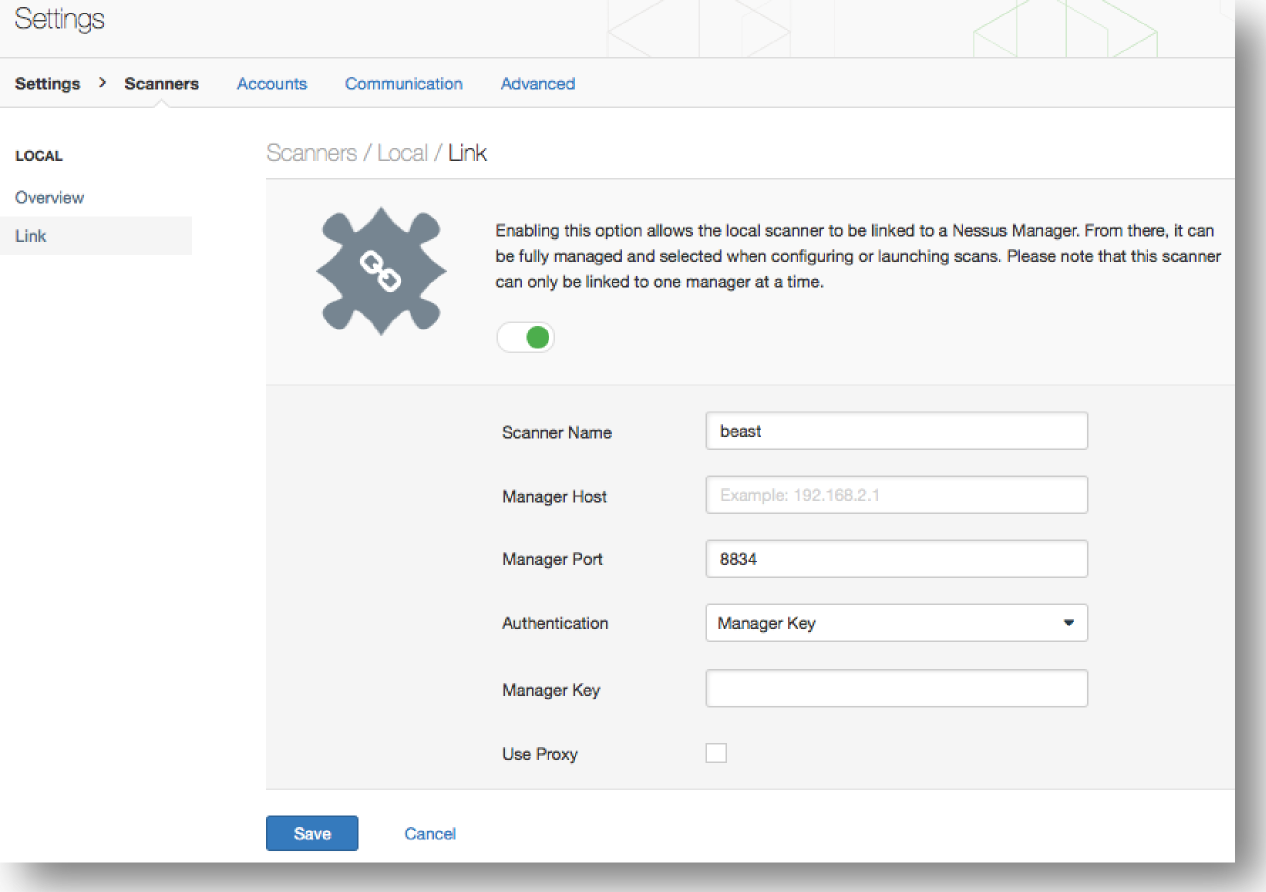


Add users or groups: Search by user name or group name

Default: Can use

Nessus scanners are configured when they are first registered to the Nessus Manager. However, if you have unlinked your Nessus scanner to the Nessus Manager and need to create a new connection, follow the next steps.

To configure your Nessus scanner, switch the toggle under the "**Link**" under the Local scanner menu item:



Enabling this option allows the local scanner to be linked to a Nessus Manager. From there, it can be fully managed and selected when configuring or launching scans. Please note that this scanner can only be linked to one manager at a time.

Scanner Name: beast

Manager Host: Example: 192.168.2.1

Manager Port: 8834

Authentication: Manager Key

Manager Key:

Use Proxy: □

Assign the scanner a unique name for easy identification, along with the key generated from the primary scanner, the primary scanner IP address, and primary scanner port. Once configured, Nessus Manager will ensure that the scanner can reach and access the primary scanner and assign it a UUID for identification.

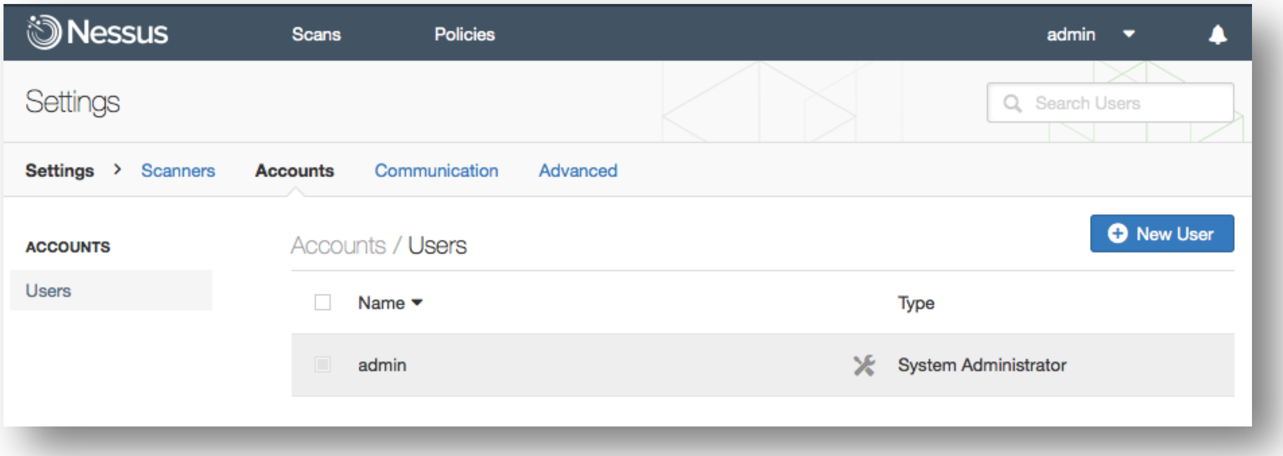
Option	Default	Description
Scanner Name	**System hostname**	Unique identifier for this Nessus scanner for the Nessus Manager
Manager Host	none	IP address of the Nessus Manager to connect
Manager Port	**8834**	Port number to connect to the Nessus Manager
Authentication	**Manager Key**	Manager Key and Username/Password are the two options available for this selection. For Nessus Manager connections, use the Nessus Manager Key. Note that authentication for the Nessus scanner must be either the primary scanner key or a username and password.
Use Proxy	disabled	If communication must be directed through a proxy, select this option. Once selected, the scanner will use the proxy configured under `Settings` > `Proxy`.

Accounts

The **Accounts** section of the Settings allows an administrator to create new user accounts and manage the accounts. In Nessus Manager, there are additional user roles and user groups that can be created.

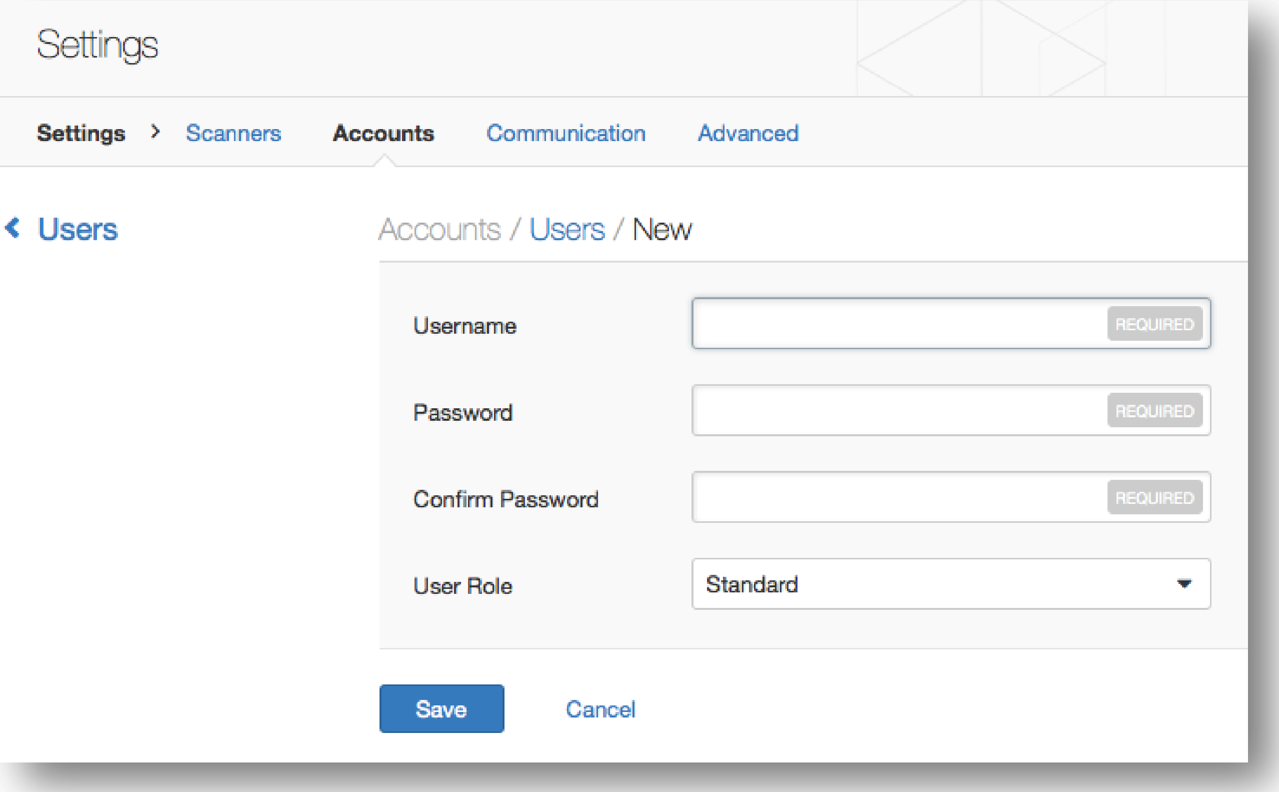
Create and Manage Nessus Users

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



Name	Type
admin	System Administrator

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



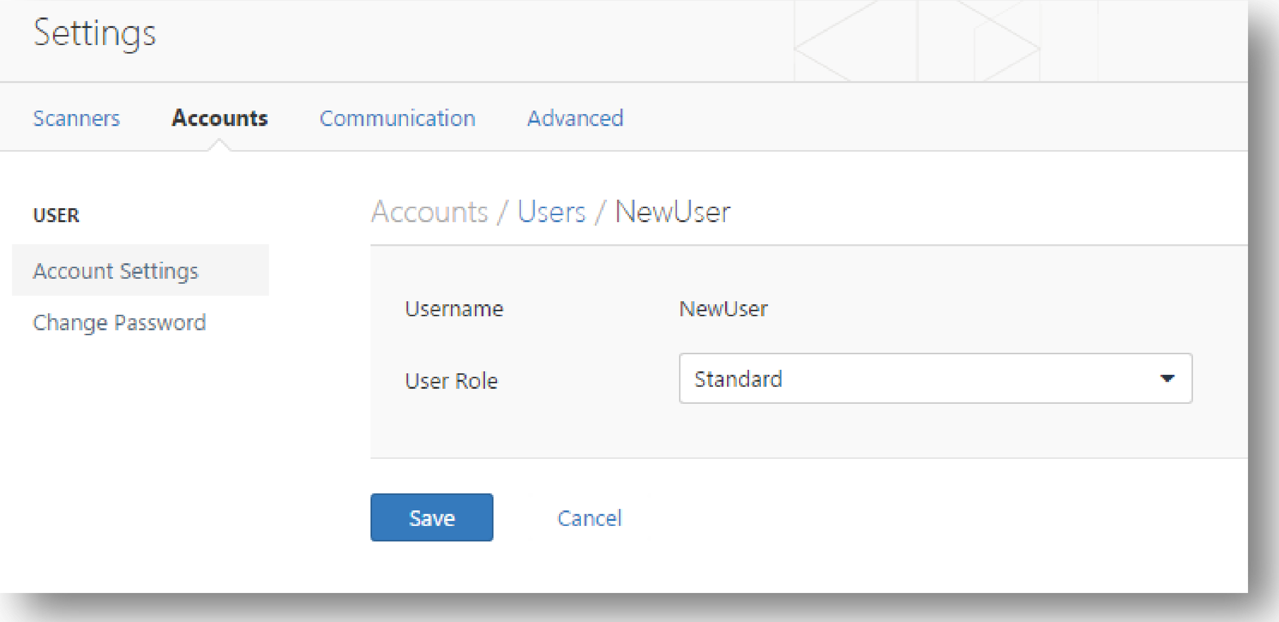
Username	REQUIRED
Password	REQUIRED
Confirm Password	REQUIRED
User Role	Standard

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

Option	Description
Username	Nessus username for new account
Password	Password for the user account being created
Confirm Password	Re-type the password for confirmation
User Role	There are two types of user roles in Nessus: standard and system administrator. System administrators can link scanners, administer user accounts and other system settings, and can configure software updates.

Nessus user roles are different in Nessus Manager. They are discussed later in the document.

If a user account needs to be modified, click on the user name. This enables you to change the user role to standard or system administrator under **Account Settings**, or **Change Password** on the selected account.


Settings

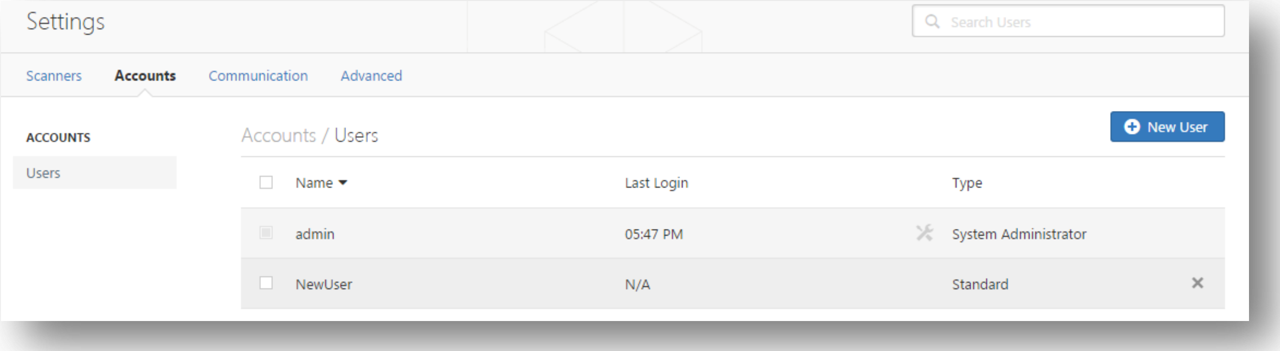
Accounts / Users / NewUser

Username: NewUser

User Role: Standard

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

To remove a user, either select the check box to the right of the account name on the list and then "**Delete**" at the top, or click the "**X**" to the right of the account name. You will be prompted for confirmation after deleting the account:

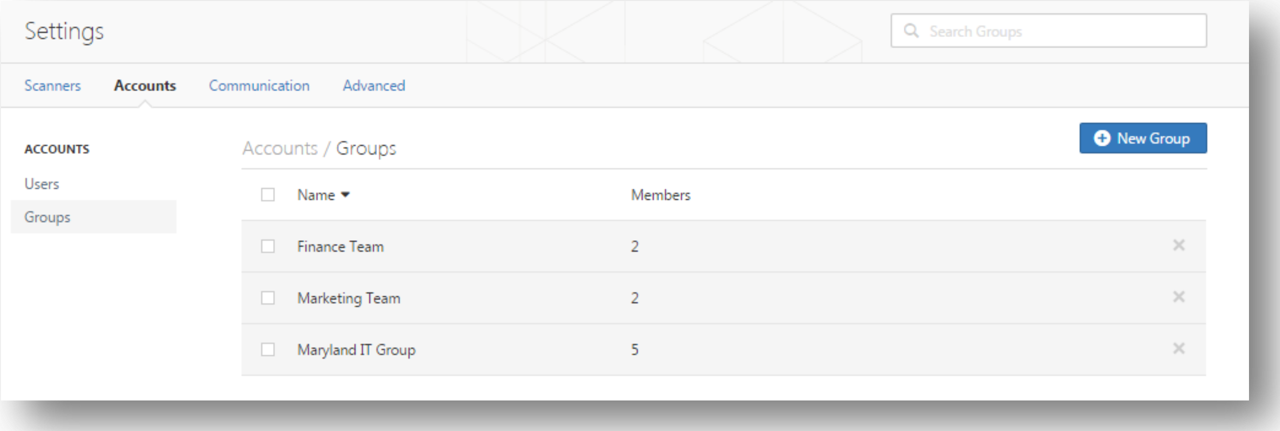


Name	Last Login	Type
admin	05:47 PM	System Administrator
NewUser	N/A	Standard

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

Create and Manage Nessus Manager User Roles and Groups

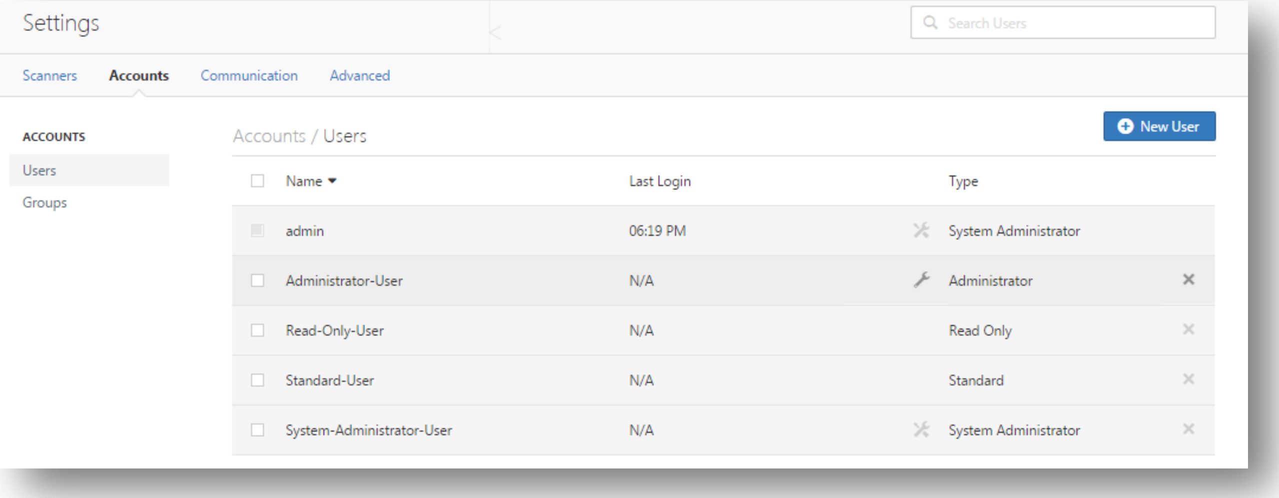
Nessus Manager has an extensive set of user and group roles that allow for granular sharing of policies, schedules, and scan results. In the **Settings** under "Accounts", you will be able to configure both users and groups.



Name	Members
Finance Team	2
Marketing Team	2
Maryland IT Group	5

Users in Nessus Manager can be managed via an LDAP server or within Nessus Manager's native users. Instructions on configuring LDAP are under the LDAP Server section of this document.

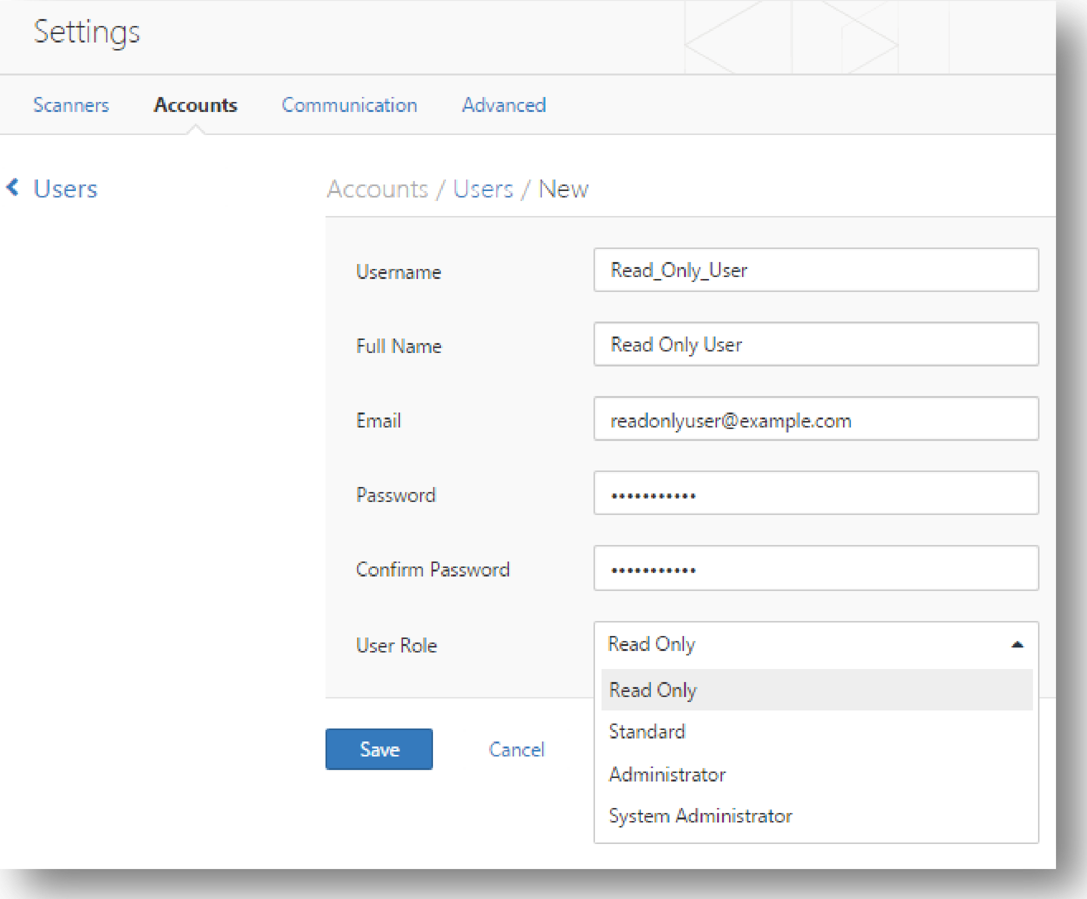
Like Nessus Professional, Nessus Manager allows you to create new users and passwords. Users in Nessus Manager have four roles available instead of the two available in Nessus Professional.



Accounts / Users

Name	Last Login	Type
admin	06:19 PM	System Administrator
Administrator-User	N/A	Administrator
Read-Only-User	N/A	Read Only
Standard-User	N/A	Standard
System-Administrator-User	N/A	System Administrator

The “**Accounts**” shows the current authenticated user as well as the user role: **Read Only**, **Standard**, **Administrator**, or **System Administrator**. The default “**admin**” account has the user role **System Administrator**.



Accounts / Users / New

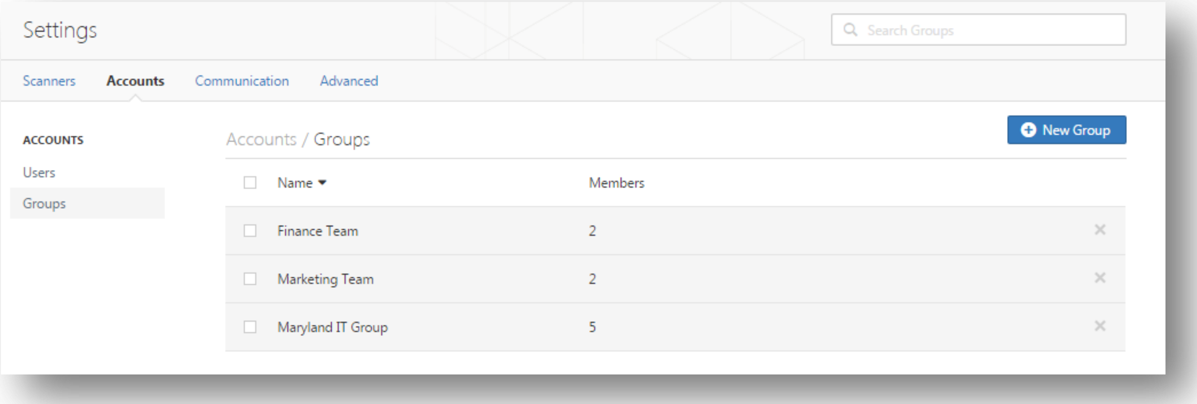
Username	Read_Only_User
Full Name	Read Only User
Email	readonlyuser@example.com
Password	•••••••••••
Confirm Password	•••••••••••
User Role	Read Only

The user roles in Nessus Manager are defined below:

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

Note that for Nessus Cloud, you must define the username as the registered email address with the Nessus Cloud service.

Additionally, users can be placed into groups depending on their function or classification (e.g., Windows Administrators, Auditors, Firewall Administrators, or Security Analysts).

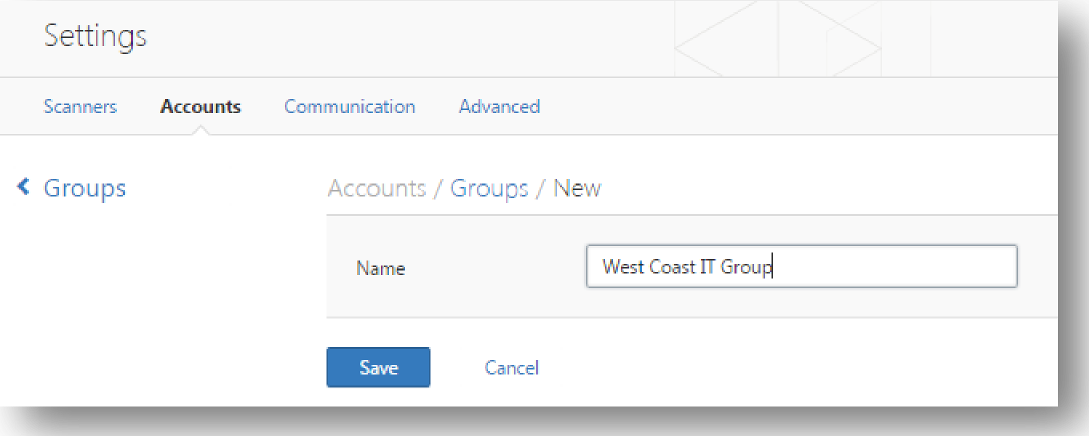


□	Name	Members
□	Finance Team	2
□	Marketing Team	2
□	Maryland IT Group	5

Click on "**Groups**" to navigate to the group view. This will list all the available groups and the list of total users in each specific group.

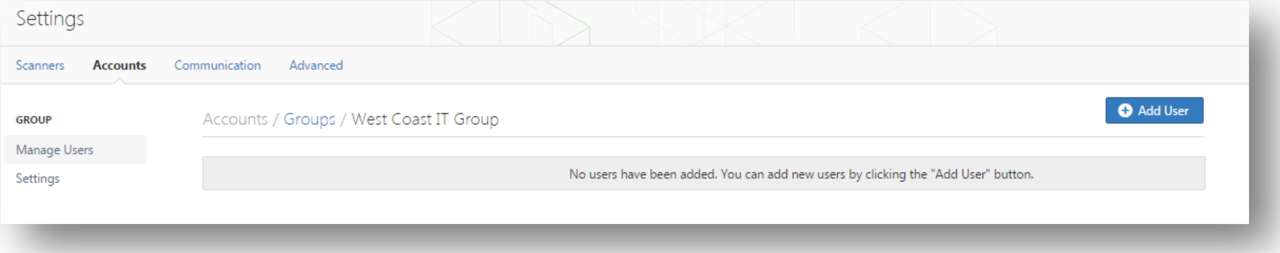
To remove a group, click on the delete button to the right of the group name.

To create a new group, click on the "**New Group**" button in the upper right. This will navigate you to the **New Group** dialog:



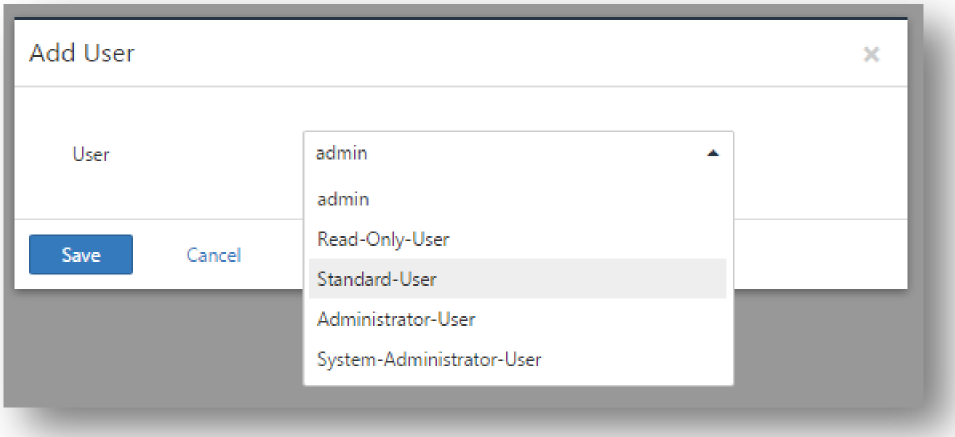
Name: West Coast IT Group

When the new group name is saved, the next page allows you to add existing users to the new group.

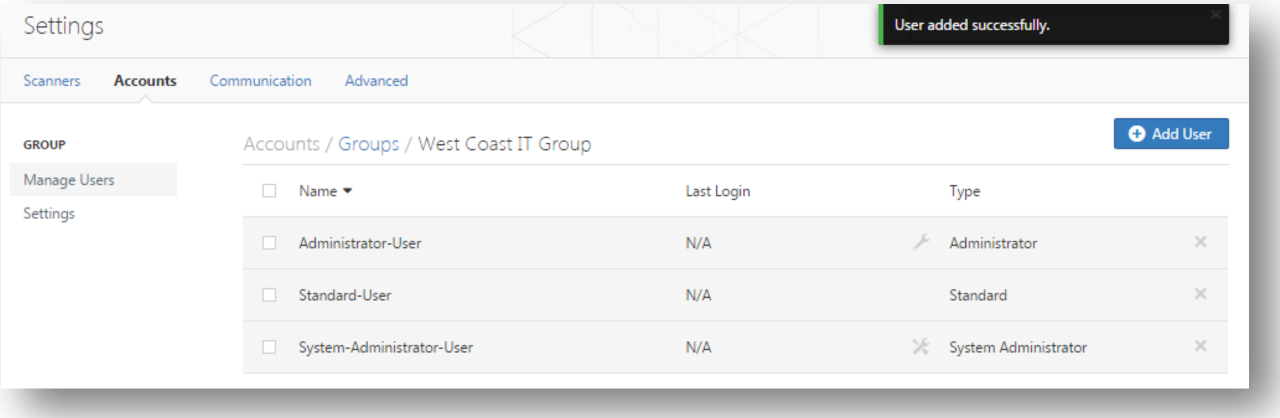


No users have been added. You can add new users by clicking the "Add User" button.

To add a user to the group, click the "**Add User**" button. This will display a new dialog:



From the drop-down, select a user to be added to the group, and then click the Save button. Continue this same process, using the Add User button to add additional users to the group.



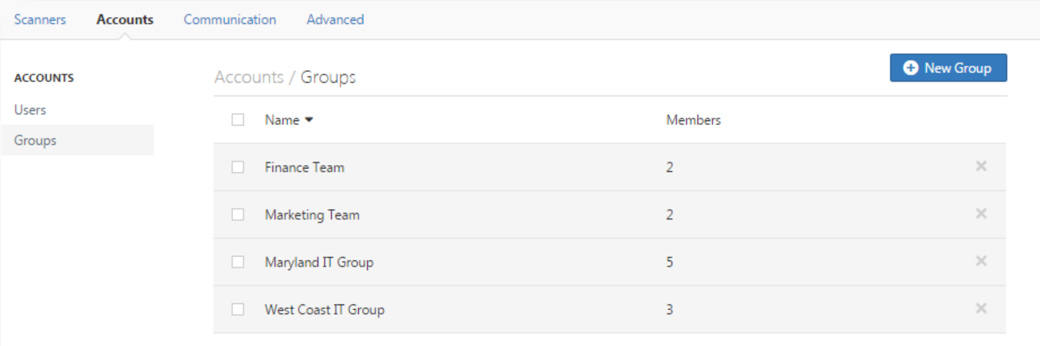
User added successfully.

Accounts / Groups / West Coast IT Group

□	Name	Last Login	Type
□	Administrator-User	N/A	Administrator
□	Standard-User	N/A	Standard
□	System-Administrator-User	N/A	System Administrator

To remove a user from the group, click on the delete button to the right of each user. If you wish to delete multiple users at a time, select the desired users and click the remove button.

To return to the Groups list, click on the Accounts link in the top navigation, and then click Groups from the left navigation.



Accounts / Groups

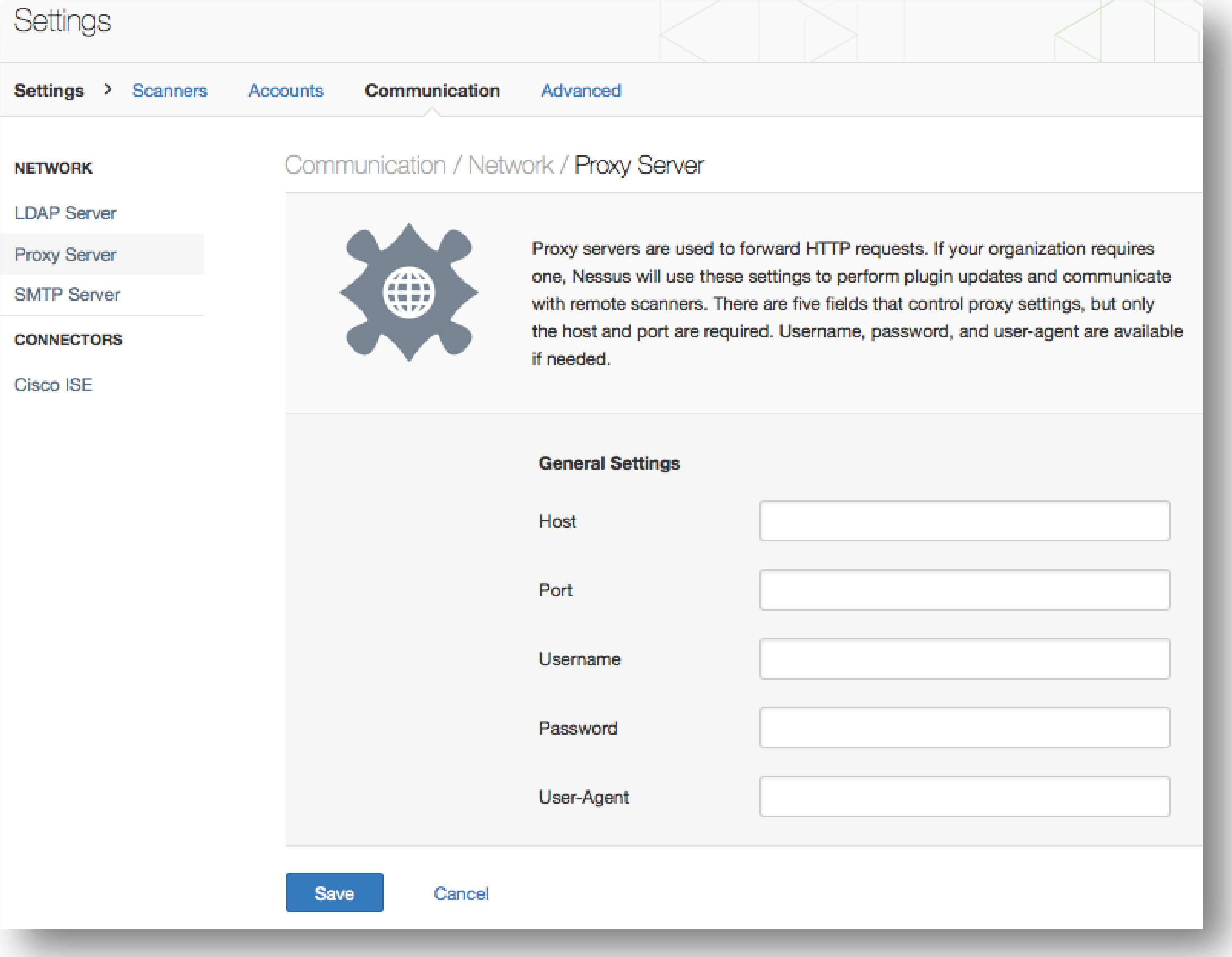
□	Name	Members
□	Finance Team	2
□	Marketing Team	2
□	Maryland IT Group	5
□	West Coast IT Group	3

Communication

The communication section covers configuring Nessus to interact with external servers. This includes the proxy server and the SMTP server. For Nessus Professional and Nessus Manager, this includes the SMTP server setting. For Nessus Manager, this also includes the LDAP server and the Cisco ISE.

Proxy Settings

For Nessus Manager and Nessus Professional you can configure the “Proxy Server” at any time. Under the “**Network**” menu via the drop-down on the top left, the “**Proxy Setting**” 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:



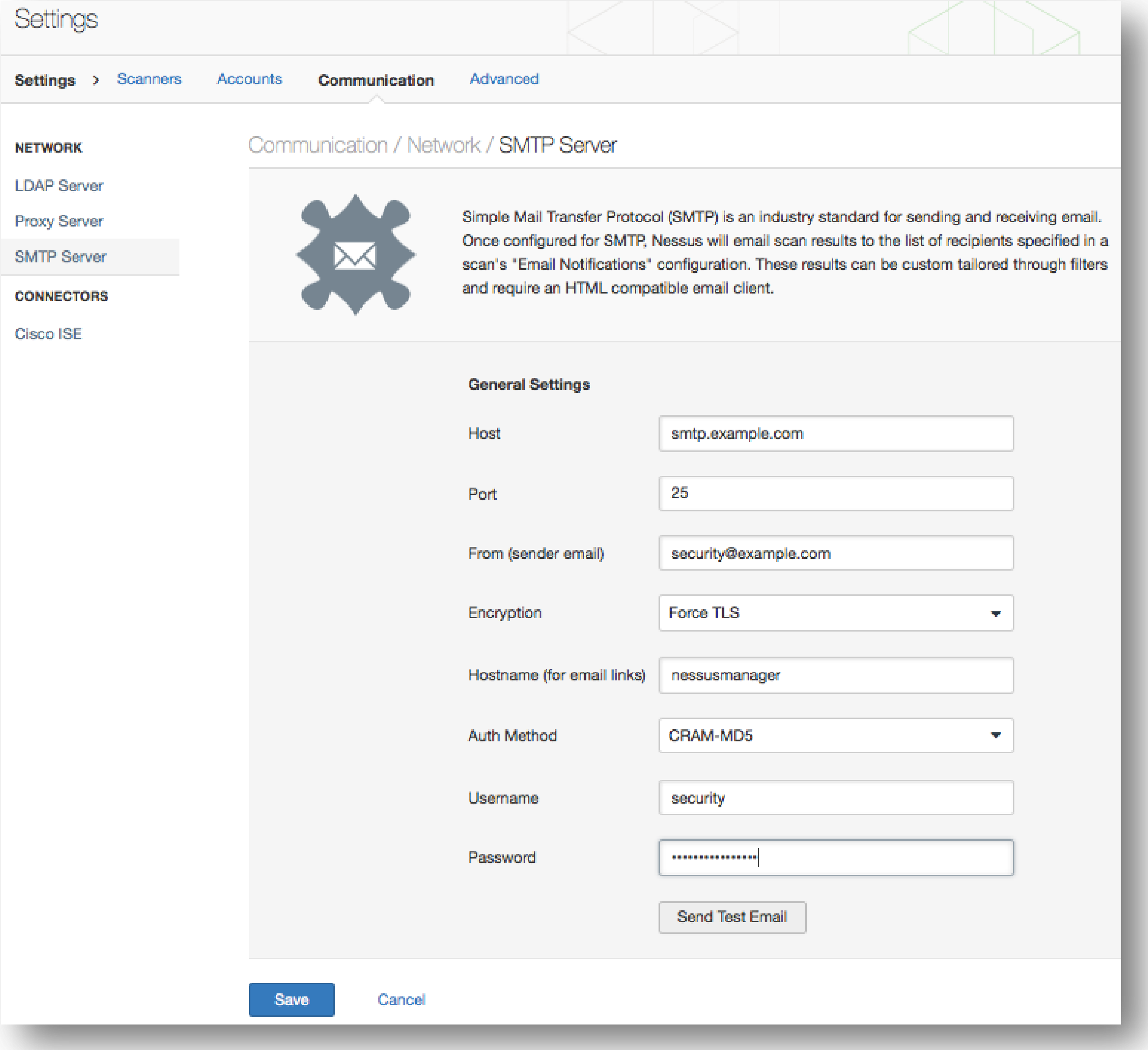
Proxy servers are used to forward HTTP requests. If your organization requires one, Nessus will use these settings to perform plugin updates and communicate with remote scanners. There are five fields that control proxy settings, but only the host and port are required. Username, password, and user-agent are available if needed.

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

Option	Description
Host	The hostname or IP of the proxy (e.g., proxy.example.com).
Port	The port of the proxy (e.g., 8080).
Username	Optional: If a username is required for proxy usage (e.g., “jdoe”).
Password	Optional: If a password is required for proxy usage (e.g., “guineapigs”).
User-Agent	Optional: If the proxy you are using filters specific HTTP user agents, a custom user-agent string can be supplied.

SMTP Server

The “**SMTP Server**” tab (under the “**Network**” menu), allows you to configure an SMTP server to notify users of scan completion via email.


Settings
Settings > Scanners Accounts Communication Advanced
NETWORK
LDAP Server
Proxy Server
SMTP Server
CONNECTORS
Cisco ISE
Communication / Network / SMTP Server

Simple Mail Transfer Protocol (SMTP) is an industry standard for sending and receiving email. Once configured for SMTP, Nessus will email scan results to the list of recipients specified in a scan's "Email Notifications" configuration. These results can be custom tailored through filters and require an HTML compatible email client.

General Settings

Host: smtp.example.com

Port: 25

From (sender email): security@example.com

Encryption: Force TLS

Hostname (for email links): nessusmanager

Auth Method: CRAM-MD5

Username: security

Password: ••••••••••••••••

Option	Description
Host	The host or IP of the SMTP server (e.g., smtp.example.com).
Port	The port of the SMTP server (e.g., 25).

From (sender email)	Who the report should appear to be from.
Nessus Server Hostname (for email links)	The IP address or hostname for the Nessus server. Note that this will only work if the Nessus host is reachable to the user reading the report.
Encryption	Specify what type of encryption should be used.
Auth Method	Method for authenticating to the SMTP server. Supported methods are None, Plain, NTLM, Login, and CRAM-MD5.
Username	The username used to authenticate to the SMTP server.
Password	The password associated with the username, provided the SMTP server requires a username and authentication.

LDAP Server

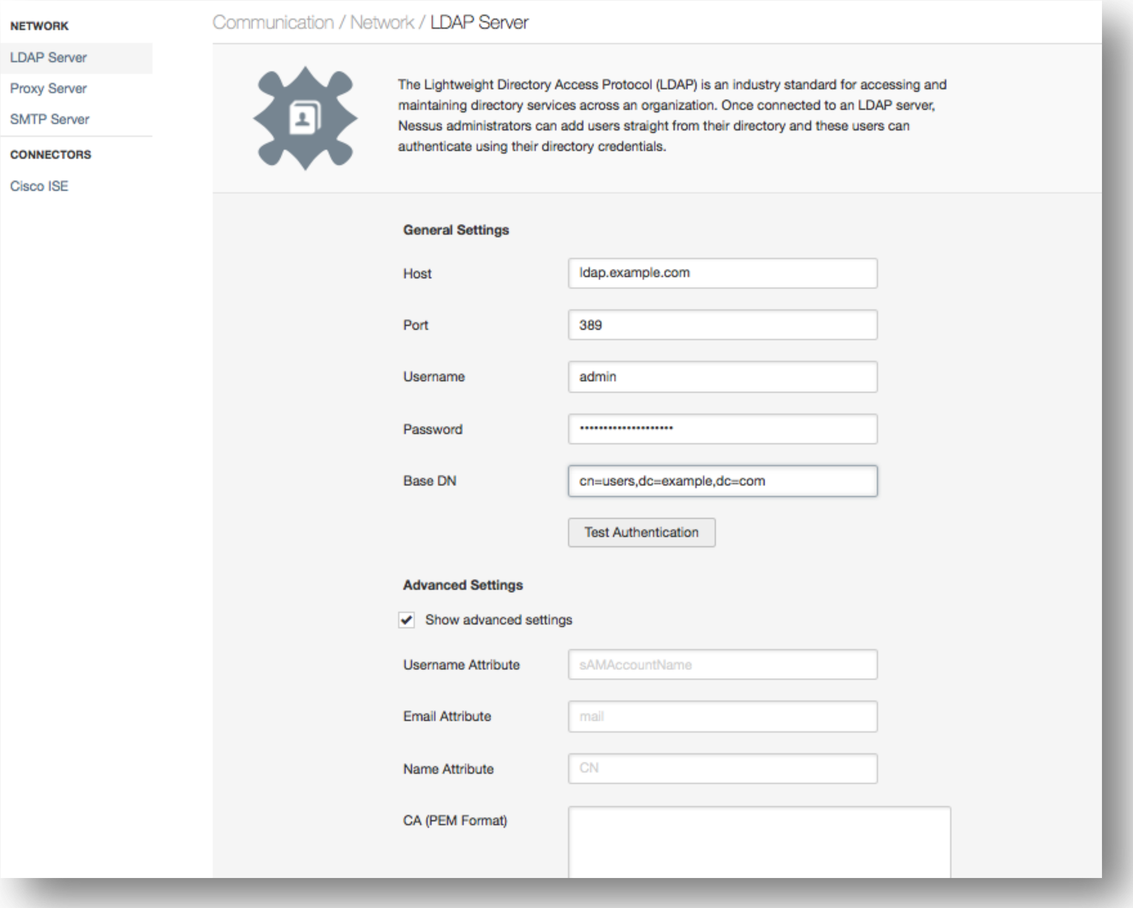
In Nessus Manager, the "**LDAP Server**" page allows you to configure an LDAP server so users can authenticate to the Nessus server using LDAP domain credentials.

Nessus auto-negotiates encryption, therefore there are no encryption options in the Nessus interface.

Nessus only accepts the following characters in the username field:

- Upper and lower case alphabetical characters (A – Z and a-z)
- Numerical characters (0 – 9)
- Period (.)
- Underscore (_)
- Dash (-)
- Plus (+)
- Ampersand (&)

If Nessus encounters characters or symbols other than specified, a 400 error will occur.



The Lightweight Directory Access Protocol (LDAP) is an industry standard for accessing and maintaining directory services across an organization. Once connected to an LDAP server, Nessus administrators can add users straight from their directory and these users can authenticate using their directory credentials.

General Settings

Host: ldap.example.com

Port: 389

Username: admin

Password: ••••••••••••••••••••

Base DN: cn=users,dc=example,dc=com

Test Authentication

Advanced Settings

☑ Show advanced settings

Username Attribute: sAMAccountName

Email Attribute: mail

Name Attribute: CN

CA (PEM Format):

Option	Description
Host	The host or IP of the LDAP server (e.g., ldap.example.com)
Port	The port of the LDAP server (e.g., 389)
Username	LDAP account with administrator access
Password	Password for the LDAP account name above
Base DN	Top level of the LDAP directory tree. Example for a common name of users in example.com is `cn=users,dc=example,dc=com`.

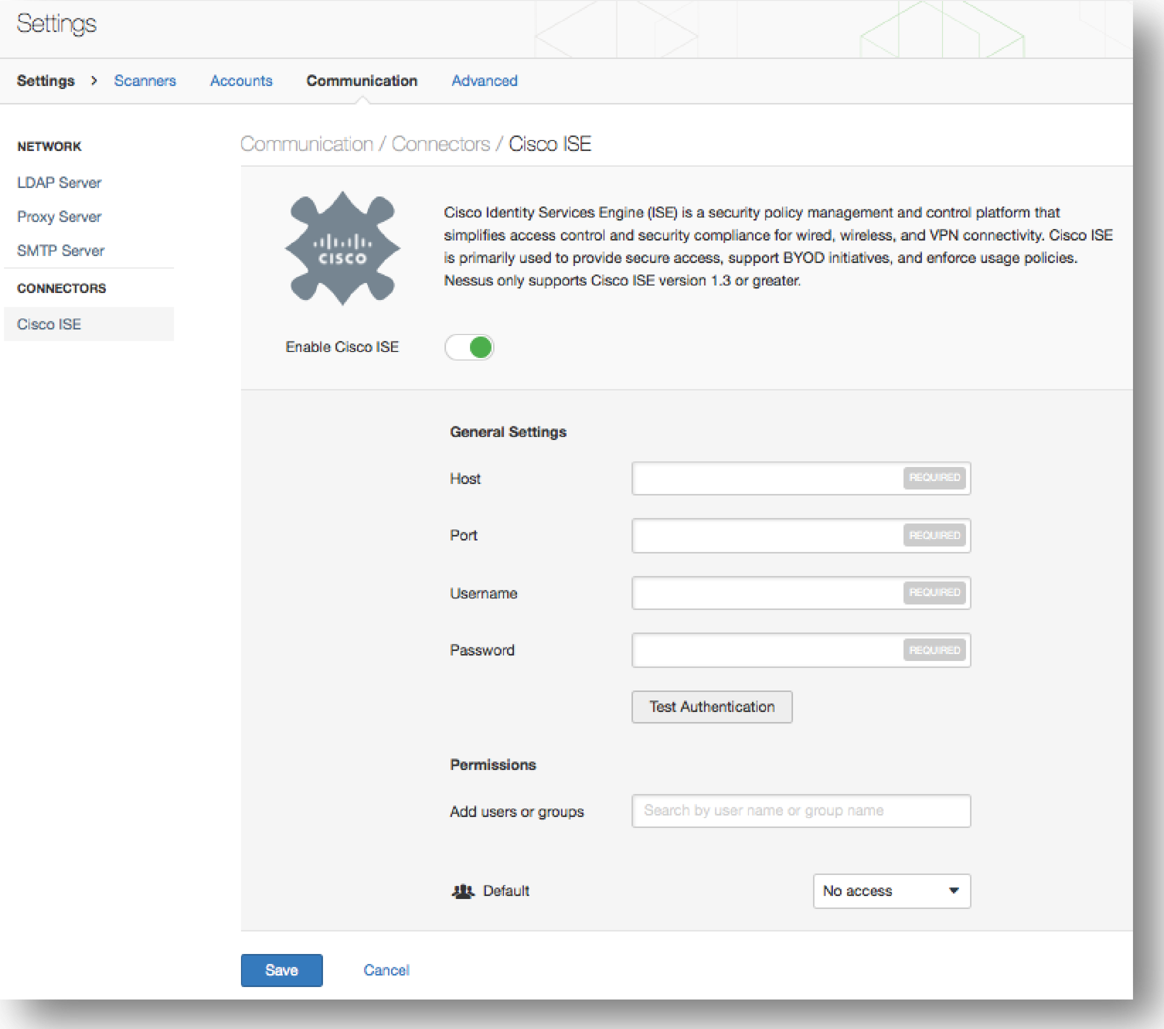
If **Show advanced settings** is enabled, the following options are available:

Option	Description
Username Attribute	Default LDAP properties used for mapping a username

Email Attribute	Default LDAP properties used for mapping an email address
Name Attribute	Default LDAP properties used for mapping a real name
CA (PEM Format)	Digital certificate of the Certificate Authority (CA) in PEM format

Cisco ISE

In Nessus Manager, the "**Cisco ISE**" setting (under the "**Connectors**" menu on the left) allows you to configure Nessus to communicate with a Cisco Identity Services Engine (ISE) server to retrieve information from the ISE and to request the ISE quarantine vulnerable devices.


Settings
Settings > Scanners Accounts Communication Advanced
NETWORK
LDAP Server
Proxy Server
SMTP Server
CONNECTORS
Cisco ISE
Communication / Connectors / Cisco ISE
cisco

Cisco Identity Services Engine (ISE) is a security policy management and control platform that simplifies access control and security compliance for wired, wireless, and VPN connectivity. Cisco ISE is primarily used to provide secure access, support BYOD initiatives, and enforce usage policies. Nessus only supports Cisco ISE version 1.3 or greater.

Enable Cisco ISE ●

General Settings

Host: REQUIRED

Port: REQUIRED

Username: REQUIRED

Password: REQUIRED

Test Authentication

Permissions

Add users or groups: Search by user name or group name

Default: No access

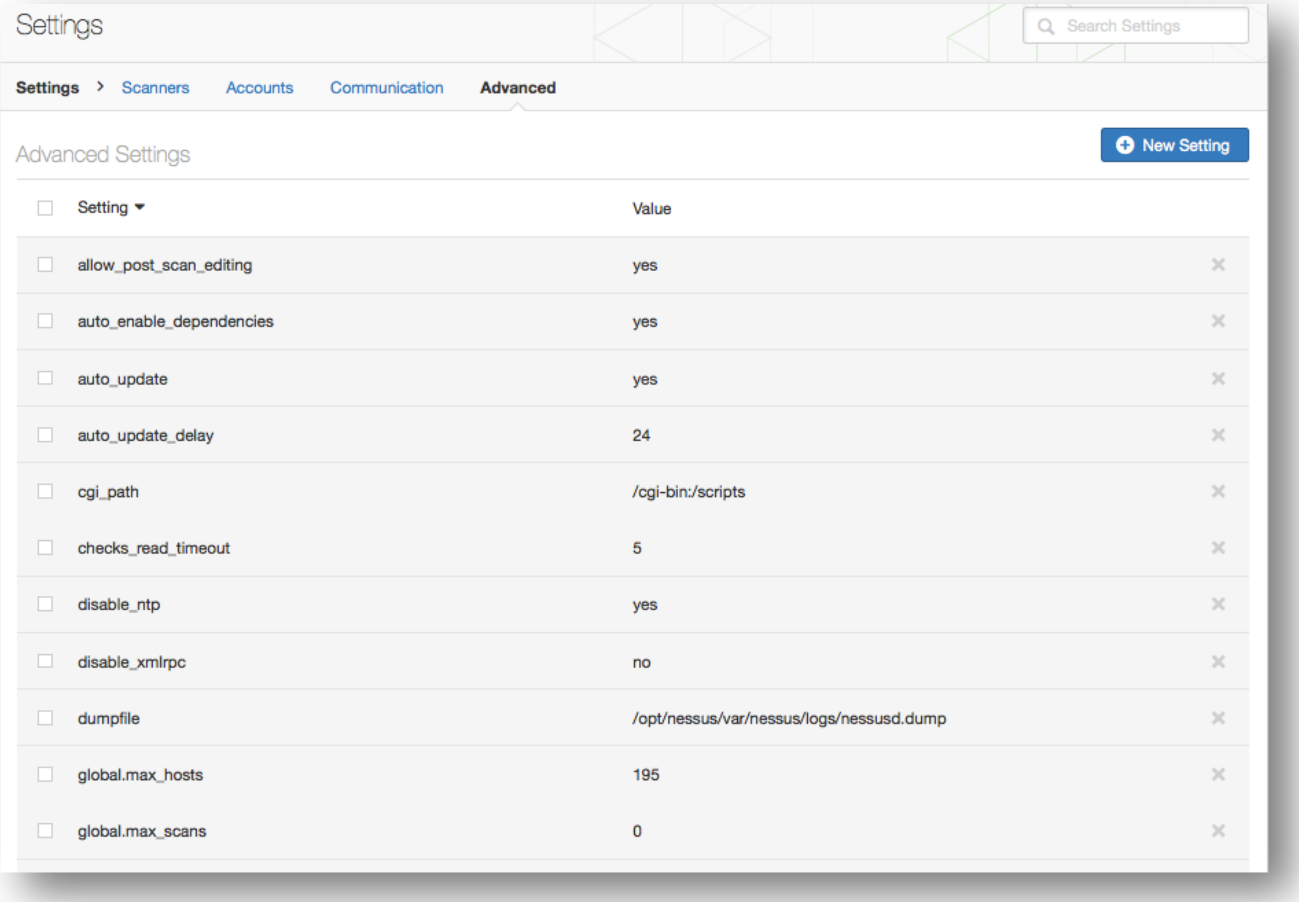
Option	Description
Host	Host name or IP address of Cisco ISE server

Port	Port for accessing Cisco ISE server (e.g., 1700)
Username	User account to access Cisco ISE
Password	Password for the user account

Advanced

In Nessus Manager and Nessus Professional, a wide variety of configuration options offer more granular control of how the scanner operates. Under the “Advanced” option on the top menu, an administrative user can manipulate these settings.

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

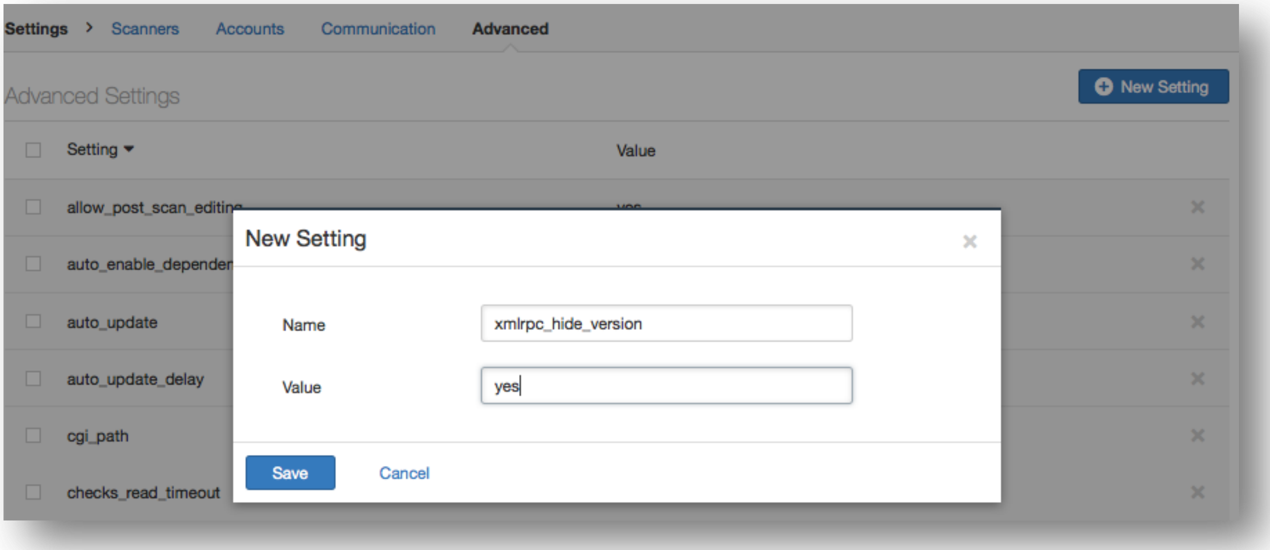


Setting	Value
allow_post_scan_editing	yes
auto_enable_dependencies	yes
auto_update	yes
auto_update_delay	24
cgi_path	/cgi-bin:/scripts
checks_read_timeout	5
disable_ntp	yes
disable_xmlrpc	no
dumpfile	/opt/nessus/var/nessus/logs/nessusd.dump
global.max_hosts	195
global.max_scans	0

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

By default, the Nessus UI operates on TCP 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 "**New Setting**" button, input the name and value, and click on "**Save**". Once a preference has been updated and saved, Nessus will process the changes within a couple of minutes.

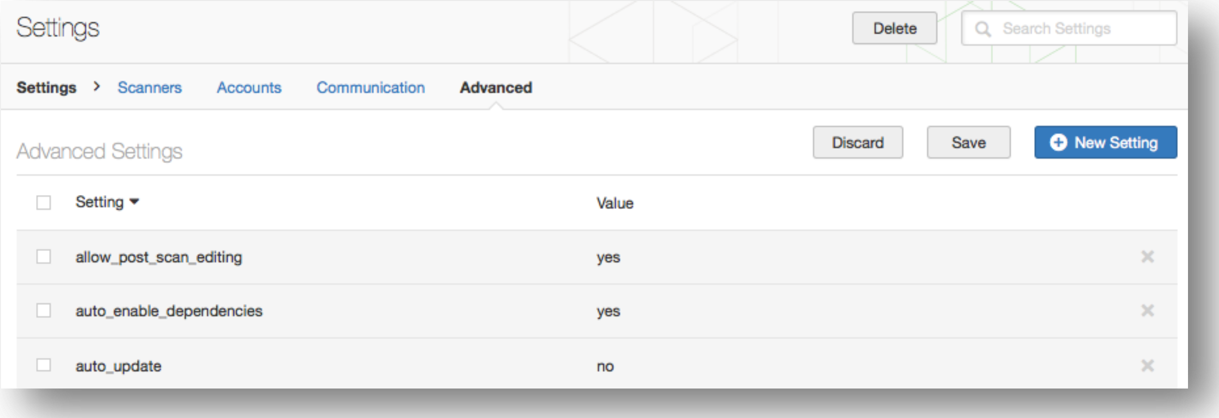


Setting	Value
allow_post_scan_editing	
auto_enable_dependen	
auto_update	
auto_update_delay	
cgi_path	
checks_read_timeout	

Name: xmlrpc_hide_version

Value: yes

After clicking "**Save**", three buttons appear on the Advanced Settings:



Setting	Value
allow_post_scan_editing	yes
auto_enable_dependencies	yes
auto_update	no

After the changes are made, you can **Save** or **Discard** them. Note that **Save** will reload the configuration with the new changes.

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

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

- Setting "`xmlrpc_hide_version`" to "`yes`" in the preferences prevents an unauthenticated user from getting the version of the Nessus engine, but will still return the UI and webserver versions.
- Setting "`user_max_login_attempt`" to a numeric value (i.e., "`3`") will lock a given account after `n` invalid login attempts. Unlocking the user requires the admin to edit the user.

Configure the Nessus Daemon (Advanced Users)

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

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

> 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 for use by SecurityCenter, it must be an admin user. SecurityCenter maintains its own user list and sets permissions for its users.

> In Nessus Manager, only a system administrator user can upload plugins to Nessus, can restart it remotely (needed after a plugin upload), and can override the **`max_hosts/max_checks`** setting in the configuration section. If the user is intended for use by SecurityCenter, it must be an admin user. SecurityCenter maintains its own user list and sets permissions for its users.

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

Option	Value
global_max_hosts	530
max_hosts	40
max_checks	5

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

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

Notes on max_hosts:

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

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

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

In addition to **`max_hosts`**, the server allows a **`global.max_hosts`** setting that controls the total hosts that can be scanned across all users at the same time. Administrators are bound by the same restrictions on both settings to avoid excessive load on the scanning server, which may have adverse effects on other users.

Notes on max_checks:

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

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

Configuration Options

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

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

enable_listen_ipv4	Directs Nessus to listen on IPv4.
enable_listen_ipv6	Directs Nessus to listen on IPv6 if the system supports IPv6 addressing.
global.max_hosts	Maximum number of simultaneous checks against each host tested.
global.max_scans	If set to non-zero, this defines the maximum number of scans that may take place in parallel. **Note**: If this option is not used, no limit is enforced.
global.max_simult_tcp_sessions	Maximum number of simultaneous TCP sessions between all scans. **Note**: If this option is not used, no limit is enforced.
global.max_web_users	If set to non-zero, this defines the maximum of (web) users who can connect in parallel. **Note**: If this option is not used, no limit is enforced.
host.max_simult_tcp_sessions	Maximum number of simultaneous TCP sessions per scanned host.
listen_address	IPv4 address to listen for incoming connections. If set to 127.0.0.1, this will restrict access to local connections only.
log_whole_attack	Log every detail of the attack? Helpful for debugging issues with the scan, but this may be disk intensive.
logfile	Location where the Nessus log file is stored.
login_banner	A text banner that will be displayed before the initial login to the Flash or HTML5 client.
max_hosts	Maximum number of hosts checked at one time during a scan.
max_checks	Maximum number of simultaneous checks against each host tested.
max_simult_tcp_sessions	Maximum number of simultaneous TCP sessions per scan.
min_password_len	Directs Nessus to enforce a policy for the length of a password for users of the scanner.
nasl_log_type	Direct the type of NASL engine output in **`nessusd.dump`**.
nasl_no_signature_check	Determines if Nessus will consider all NASL scripts as being signed. Selecting "yes" is unsafe and not recommended.
nessus_syn_scanner.global_throughput.max	Sets the max number of SYN packets that Nessus will send per second during its port scan (no matter how many hosts are scanned in parallel). Adjust this setting based on the sensitivity of the remote device to large numbers of SYN packets.
non_simult_ports	Specifies ports against which two plugins cannot not be run simultaneously.
optimize_test	Optimize the test procedure. Changing this to "no" will cause scans to take longer and typically generate more false positives.

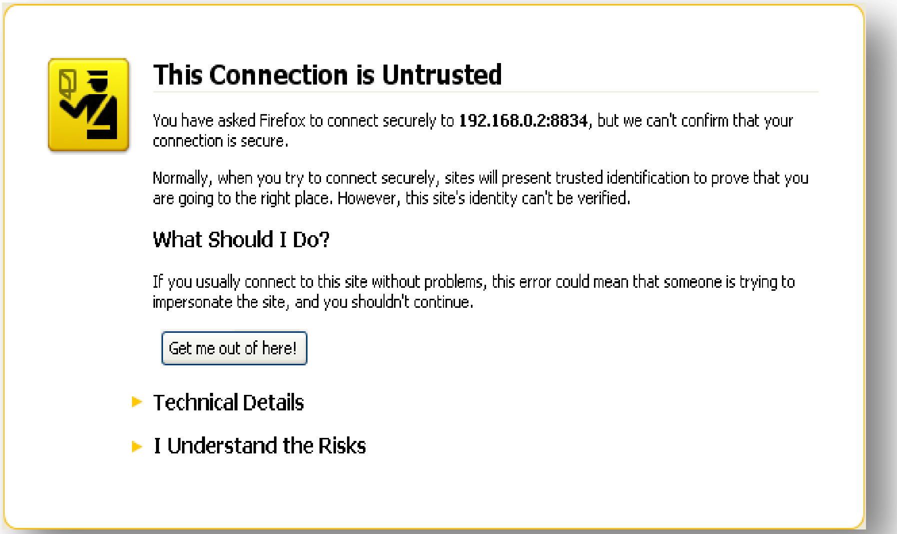
paused_scan_timeout	Kill a paused scan after the specified number of minutes (0 for no timeout).
plugin_timeout	Kill the plugin after a specified number of second (0 for no timeout).
plugin_upload	Designate if admin users may upload plugins.
plugins_timeout	Maximum lifetime of a plugin's activity (in seconds).
port_range	Range of the ports the port scanners will scan. Can use keywords "default" or "all", as well as a comma delimited list of ports or ranges of ports.
purge_plugin_db	Determines if Nessus will purge the plugin database at each update. This directs Nessus to remove, re-download, and re-build the plugin database for each update. Choosing yes will cause each update to be considerably slower.
qdb_mem_usage	Directs Nessus to use more or less memory when idle. If Nessus is running on a dedicated server, setting this to "high" will use more memory to increase performance. If Nessus is running on a shared machine, settings this to "low" will use considerably less memory, but at the price of a moderate performance impact.
reduce_connections_on_ congestion	Reduce the number of TCP sessions in parallel when the network appears to be congested.
report_crashes	Anonymously report crashes to Tenable.
rules	Location of the Nessus Rules file (`nessusd.rules`).
safe_checks	Safe checks rely on banner grabbing rather than active testing for a vulnerability.
save_knowledge_base	Save the knowledge base on disk for later use.
silent_dependencies	If enabled, the list of plugin dependencies and their output are not included in the report. A plugin may be selected as part of a policy that depends on other plugins to run. By default, Nessus will run those plugin dependencies, but will not include their output in the report. Setting this option to **no** will cause both the selected plugin, and any plugin dependencies to all appear in the report.
slice_network_addresses	If this option is set, Nessus will not scan a network incrementally (10.0.0.1, then 10.0.0.2, then 10.0.0.3, and so on) but will attempt to slice the workload throughout the whole network (e.g., it will scan 10.0.0.1, then 10.0.0.127, then 10.0.0.2, then 10.0.0.128, and so on).
source_ip	In the case of a multi-homed system with different IPs on the same subnet, this option tells the Nessus scanner which NIC/IP to use for the tests. If multiple IPs are provided, Nessus will cycle through them whenever it performs a connection.
ssl_cipher_list	Nessus only supports 'strong' SSL ciphers when connecting to port 8834.
stop_scan_on_disconnect	Stop scanning a host that seems to have been disconnected during the scan.

stop_scan_on_hang	Stop a scan that seems to be hung.
throttle_scan	Throttle scan when CPU is overloaded.
use_kernel_congestion_detection	Use Linux's TCP congestion messages to scale back scan activity as required.
www_logfile	Location where the Nessus Web Server (user interface) log is stored.
xmlrpc_idle_session_timeout	XMLRPC Idle Session Timeout in minutes. Value defaults to 30 minutes. If the value is set to zero (0), the default value of 30 minutes will still apply. ! For security purposes, if the value is set to a number greater than 30, the setting will revert back to 30.
xmlrpc_listen_port	Port for the Nessus Web Server to listen to (new XMLRPC protocol).

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

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

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

What Should I Do?

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

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

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

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

Operating System	Certificate File Locations
Linux	`/opt/nessus/com/nessus/CA/servercert.pem` `/opt/nessus/var/nessus/CA/serverkey.pem`
FreeBSD	`/usr/local/nessus/com/nessus/CA/servercert.pem` `/usr/local/nessus/var/nessus/CA/serverkey.pem`
Windows Vista and later	`C:\ProgramData\Tenable\Nessus\nessus\CA\`
Mac OS X	`/Library/Nessus/run/com/nessus/CA/servercert.pem` `/Library/Nessus/run/var/nessus/CA/serverkey.pem`

Nessus 6 supports SSL certificate chains.

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

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

Authenticating To Nessus with SSL Certificate

SSL Client Certificate Authentication

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

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

Configure Nessus for Certificates

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

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

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

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

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

   Windows Vista and later:
   ```
   C:\> copy \ProgramData\Tenable\Nessus\nessus\CA\cacert.pem
   C:\ProgramData\Tenable\Nessus\nessus\CA\ORIGcacert.pem
   ```

3. If the certificates to be used for authentication are created by a CA other than the Nessus server, the CA certificate must be installed on the Nessus server:

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

   Windows 7 and later:
   Copy the organization's CA certificate to **`C:\ProgramData\Tenable\Nessus\nessus\CA\cacert.pem`**

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

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

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

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

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

Create Nessus SSL Certificates for Login

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

1. On the Nessus server, run the **`nessuscli mkcert-client`** command.

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

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

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

```
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.

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 placed in the temporary directory in Nessus: `/opt/nessus/var/nessus/tmp/` in Linux, `/Library/Nessus/run/var/nessus/tmp/` in Mac OS X, and `C:\programdata\tenable\nessus\tmp` in Windows.

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, for example, `cert_squirrel.pem` and `key_squirrel.pem` (where "squirrel" is the hostname of the system used in this example). These files must be combined and exported into a format that may be imported into the web browser such as `.pfx`. This may be accomplished with the `openssl` program and the following command:

```
# #openssl pkcs12 -export -out combined_testkey.pfx -inkey key_testkey.pem -in
cert_testkey.pem -chain -CAfile /opt/nessus/com/nessus/CA/cacert.pem -passout
'pass:password' -name 'Nessus User Certificate for: testkey'
```

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

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

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

```
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.

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

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

Client certificates are created in a randomized temporary directory appropriate to the system. The temporary directory will be identified on the line beginning with “Your client certificates are in”. For the use of card authentication, these certificates are not needed and may be deleted.

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.

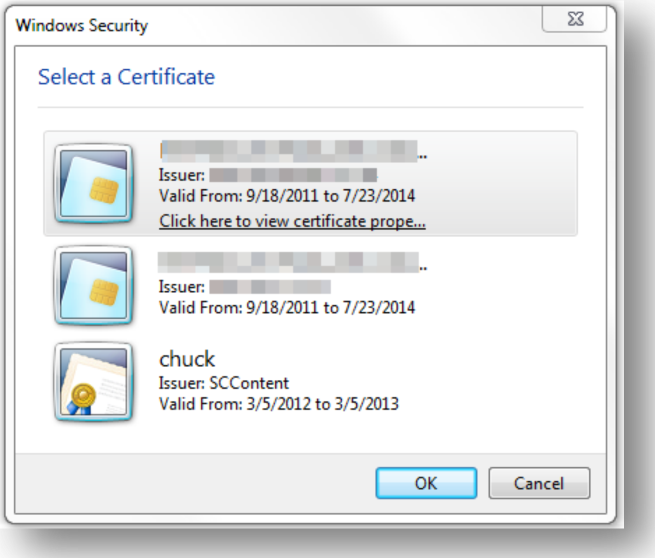
Connect with Certificate or Card Enabled Browser

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:

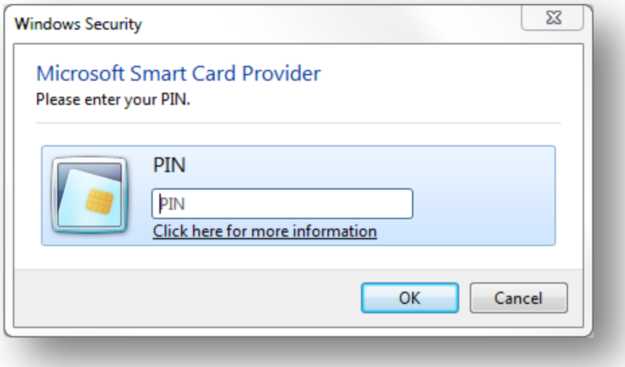


[redacted]..
Issuer: [redacted]
Valid From: 9/18/2011 to 7/23/2014
Click here to view certificate prope...

[redacted]..
Issuer: [redacted]
Valid From: 9/18/2011 to 7/23/2014

chuck
Issuer: SCContent
Valid From: 3/5/2012 to 3/5/2013

3. Once a certificate has been selected, a prompt for the PIN or password for the certificate is presented (if required) to access your certificate. When the PIN or password is successfully entered, the certificate will be available for the current session with Nessus.


Windows Security

Microsoft Smart Card Provider

Please enter your PIN.

PIN: PIN

4. Upon navigating to the Nessus web interface, the user may briefly see the username and password screen followed by an automatic login as the designated user. The Nessus user interface may be used normally.

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

Nessus without Internet Access

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

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

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

Generate a Challenge Code

You must retrieve your Activation Code from either your Tenable Support Portal account for Nessus or your Nessus Home registration email.

Note that you can only use one Activation Code per scanner. If the scanners are managed by SecurityCenter, no activation code is needed.

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

Windows:

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

Linux:

```
# /opt/nessus/sbin/nessuscli fetch --challenge
```

FreeBSD:

```
# /usr/local/nessus/bsin/nessuscli fetch --challenge
```

Mac OS X:

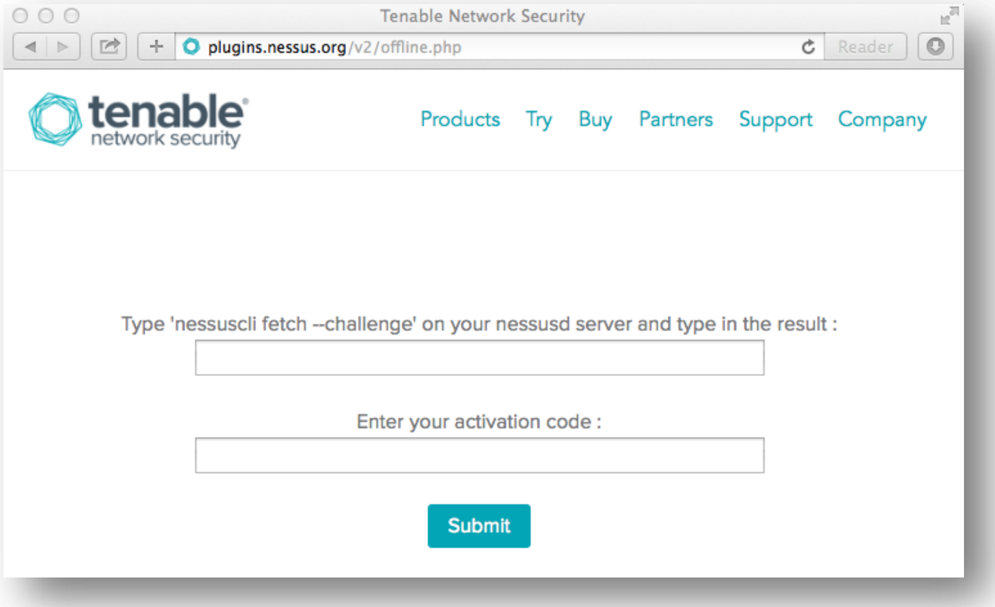
```
# /Library/Nessus/run/sbin/nessuscli fetch --challenge
```

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

```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Obtain and Install Up-to-date Plugins

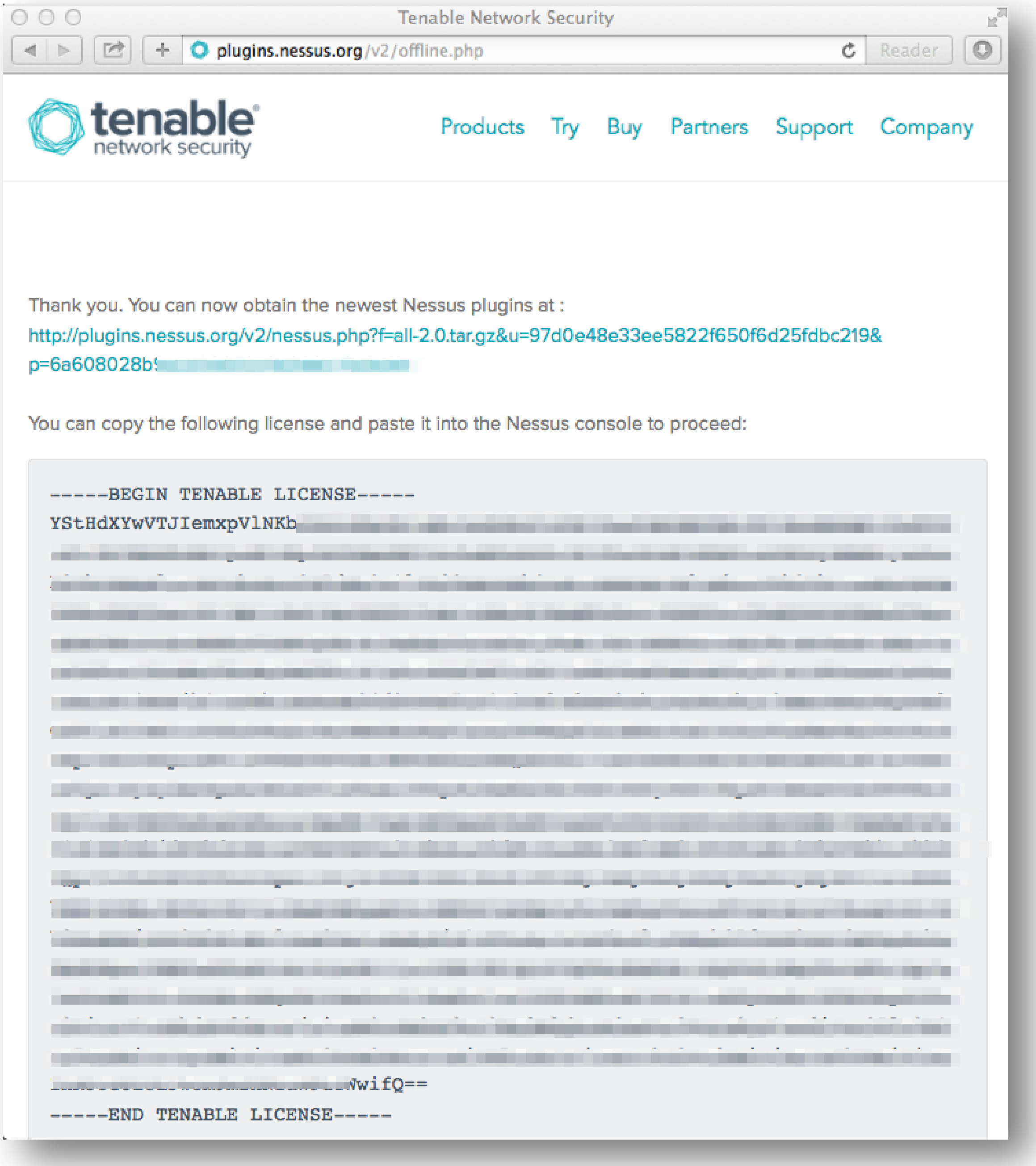
Next, go to http://plugins.nessus.org/v2/offline.php and copy and paste the “challenge” string as well as the Activation Code that you received previously into the appropriate text boxes:



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

Enter your activation code :

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



Thank you. You can now obtain the newest Nessus plugins at :
http://plugins.nessus.org/v2/nessus.php?f=all-2.0.tar.gz&u=97d0e48e33ee5822f650f6d25fdbc219&p=6a608028b[redacted]

You can copy the following license and paste it into the Nessus console to proceed:

```
-----BEGIN TENABLE LICENSE-----
YStHdXYwVTJIemxpVlNKb[redacted]
[redacted]wifQ==
-----END TENABLE LICENSE-----
```

This screen gives you access to download the latest Nessus plugin feed (**`all-2.0.tar.gz`**) along with a link to the **`nessus.license`** file at the bottom of the screen if you prefer to download the license than copy and paste it.

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

A registration code used for offline registration cannot then be used for online registration, unless the code has been reset via the Tenable Support Portal first. However, once a scanner has been registered offline, if it has access to the Internet it will also be able to update itself online without re-registration.

Next, run the following command to register Nessus offline, and install the **nessus.license** file to the Nessus directory on the host:

Windows 7/8/2008/2012:

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

Linux:

```
# /opt/nessus/sbin/nessuscli fetch --register-offline
/opt/nessus/etc/nessus/nessus.license
```

FreeBSD:

```
# /usr/local/nessus/sbin/nessuscli fetch --register-offline
/usr/local/nessus/etc/nessus/nessus.license
```

Mac OS X:

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

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> nessuscli.exe update all-2.0.tar.gz
```

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

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

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

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

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

Using and Managing Nessus from the Command Line

Nessus Major Directories

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

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

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

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

Create and Manage Nessus Users with Account Limitations

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

The following example highlights the creation of a second Nessus user with password authentication and user rules that restrict the user to scanning a class B subnet, 172.20.0.0/16. For further examples and the syntax of user rules please see the Nessus v6 Command Line Reference guide for **`nessuscli`**.

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

Please see the nessus-adduser manual for the rules syntax

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



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

`nessusd` Command Line Options

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

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

`-D`	When starting the **`nessusd`** server, this option will make the server run in the background (daemon mode).
`-v`	Display the version number and exit.
`-l`	Display the plugin feed license information and exit.
`-h`	Show a summary of the commands and exit.
`--ipv4-only`	Only listen on IPv4 socket.
`--ipv6-only`	Only listen on IPv6 socket.
`-q`	Operate in "quiet" mode, suppressing all messages to **`stdout`**.
`-R`	Force a re-processing of the plugins.
`-t`	Check the timestamp of each plugin when starting up to only compile newly updated plugins.
`-K`	Set a master password for the scanner.

If a master password is set, Nessus will encrypt all policies and 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.

On Nessus in Unix and Mac OS X, **`nessus-service`** is a wrapper for **`nessusd`**. Tenable recommends using the **`nessus-service`** on Unix and Mac OS X implementations instead of calling **`nessusd`** directly.

An example of the command line usage is shown below:

Linux:

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

FreeBSD:

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

Mac OS X:

```
# Library/Nessus/run/sbin/nessus-service [-vhD] [-c <config-file>] [-p <port-number>] [-a
<address>] [-S <ip[,ip,...]>]
```

Nessus Service Manipulation via Windows CLI

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

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


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


C:\Windows\system32>
```

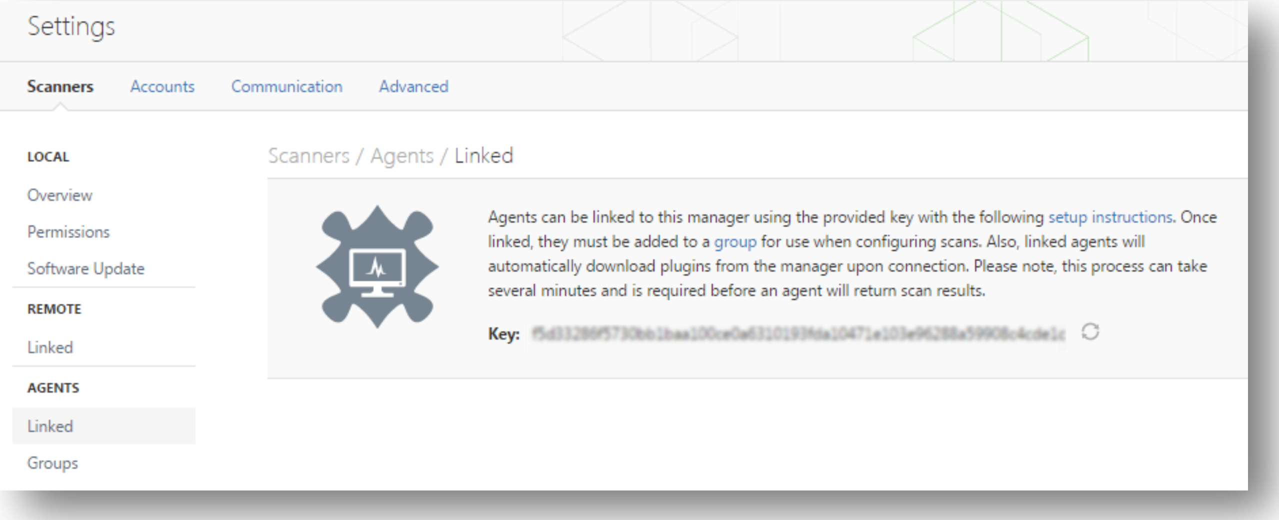
Nessus Agents

Installation

Prior to installing Nessus Agents, you must acquire the Agent Key from within Nessus.

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

Nessus Agents are linked to a Nessus Manager or Nessus Cloud similar to linking a secondary scanner. After selecting "**Agents**" under the Remote scanner section, select "**Linked**". A key will be generated that is used as a shared secret for a secondary scanner to authenticate to the primary:



Agents can be linked to this manager using the provided key with the following setup instructions. Once linked, they must be added to a group for use when configuring scans. Also, linked agents will automatically download plugins from the manager upon connection. Please note, this process can take several minutes and is required before an agent will return scan results.

Key: [redacted]

Nessus Agents are downloaded from the Tenable Support Portal, installed, and then linked to a Nessus Manager.

> Agents can be installed on your target(s) manually, via Group Policy, SCCM, or other third-party software deployment applications.

Download Nessus Agent Software

Download the latest version of the Nessus Agent through the Tenable Support Portal. Confirm the integrity of the installation package by comparing the download MD5 checksum with the one listed in the product release notes.

Nessus distribution file sizes and names vary slightly from release to release.

Unix Installation

> 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.

Platform	Installation Instructions

Red Hat, CentOS, and Oracle Linux	Use one of the appropriate commands below that corresponds to the version of Red Hat you are running:
	`# rpm -ivh NessusAgent-6.4.0-es5.i386.rpm`
	`# rpm -ivh NessusAgent-6.4.0-es5.x86_64.rpm`
	`# rpm -ivh NessusAgent-6.4.0-es6.i386.rpm`
	`# rpm -ivh NessusAgent-6.4.0-es6.x86_64.rpm`
	`# rpm -ivh NessusAgent-6.4.0-es7.x86_64.rpm`

Fedora	Use one of the appropriate commands below that corresponds to the version of Fedora you are running: `# rpm -ivh NessusAgent-6.4.0-fc20.x86_64.rpm`

After installing the agent from a command line, you will need to link it to a manager:

Example:

```
# ./nessuscli agent link
       --key=00edbg34028f795a2effb2e5be0276f232494fd74564d00d32a74548b9e92bf735
       --name=RH7_Agent --groups="All" --host=172.26.189.51 --port=8834
```

Required:
`--key`
`--host`
`--port`

Optional:
`--name`
`--groups`

After running this command, the Agent will be visible in Nessus Manager.

To unlink the agent use the following command:

```
# ./nessuscli agent unlink
```

Windows Installation

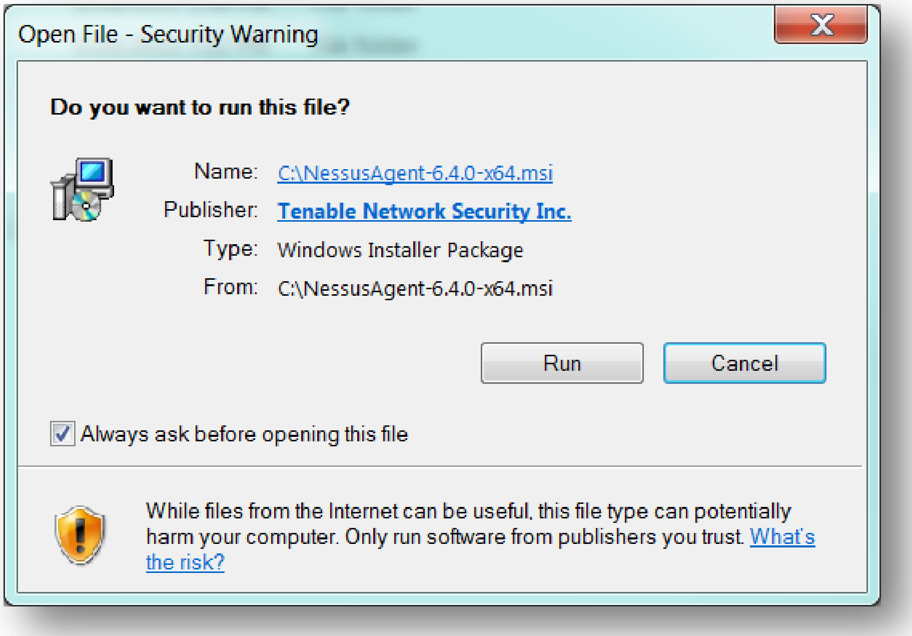
The Nessus Agents are distributed as executable installation files. Place the file on the system it is being installed on or a shared drive accessible by the system. Nessus Agents are controlled by the Nessus Manager or Nessus Cloud: They cannot run scans on their local system.

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

Installation Method	Installation Instructions
Within Windows	Navigate to the folder where the Nessus Agent **`.msi`** was downloaded to and double-click the **`.msi`** file.
Command-line Install	At a command prompt, navigate to the folder where the Nessus Agent **`.msi`** was downloaded to and run the file. Example: `C:\>`**`NessusAgent-6.4.0-x64.msi`**

Some antivirus software packages can classify Nessus products 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.

Before the installation process, the Nessus Agent will prompt you to run or cancel.



Open File - Security Warning

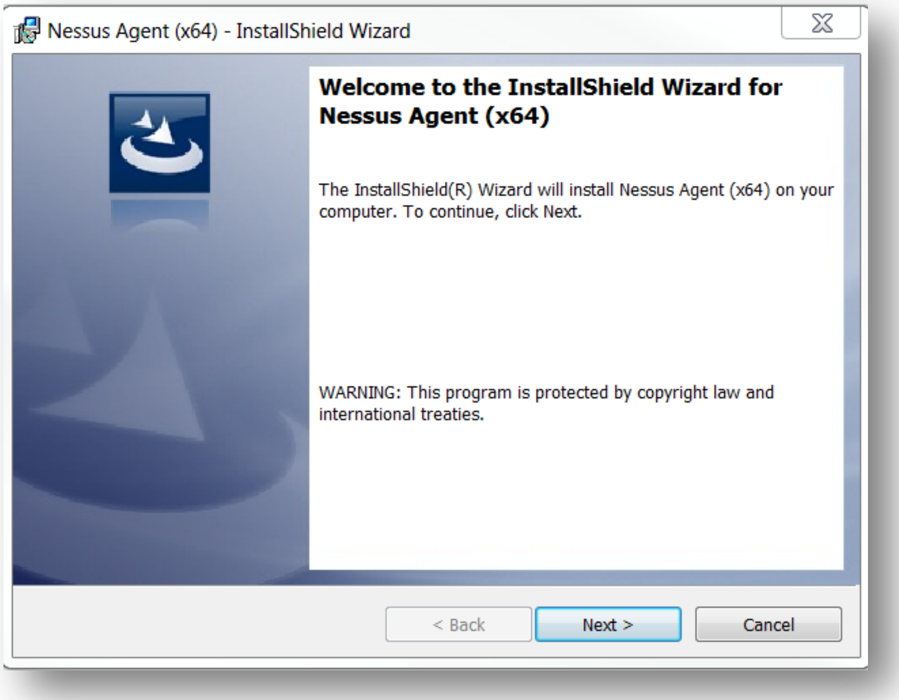
Do you want to run this file?

Name: C:\NessusAgent-6.4.0-x64.msi
Publisher: **Tenable Network Security Inc.**
Type: Windows Installer Package
From: C:\NessusAgent-6.4.0-x64.msi

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

Next, you would be presented with the InstallShield Wizard.



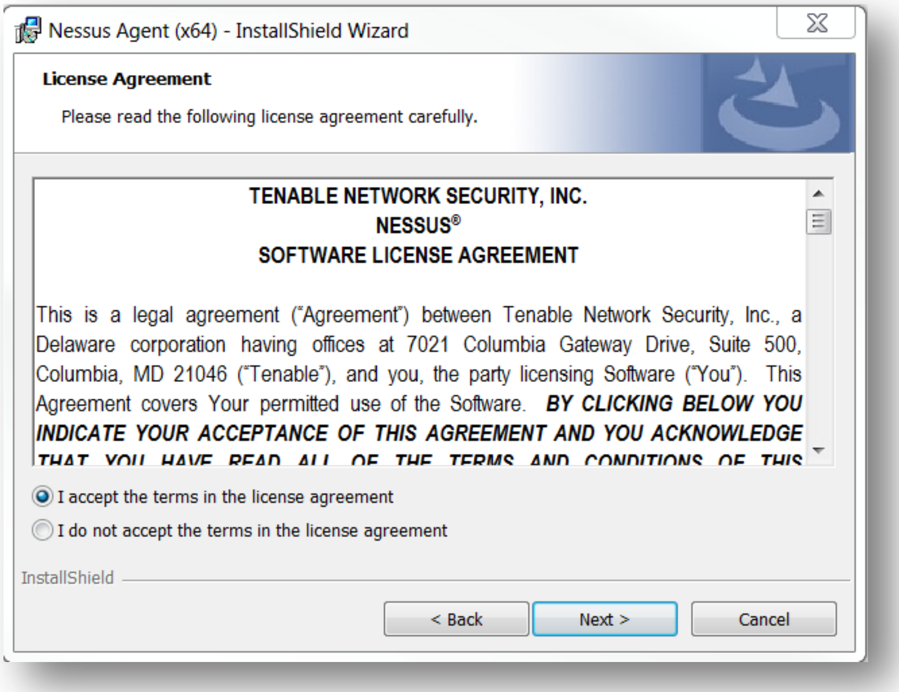
Nessus Agent (x64) - InstallShield Wizard

Welcome to the InstallShield Wizard for Nessus Agent (x64)

The InstallShield(R) Wizard will install Nessus Agent (x64) on your computer. To continue, click Next.

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

Before the actual installation begins, you must read and accept the terms in the license agreement. Click Next to proceed.



Nessus Agent (x64) - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

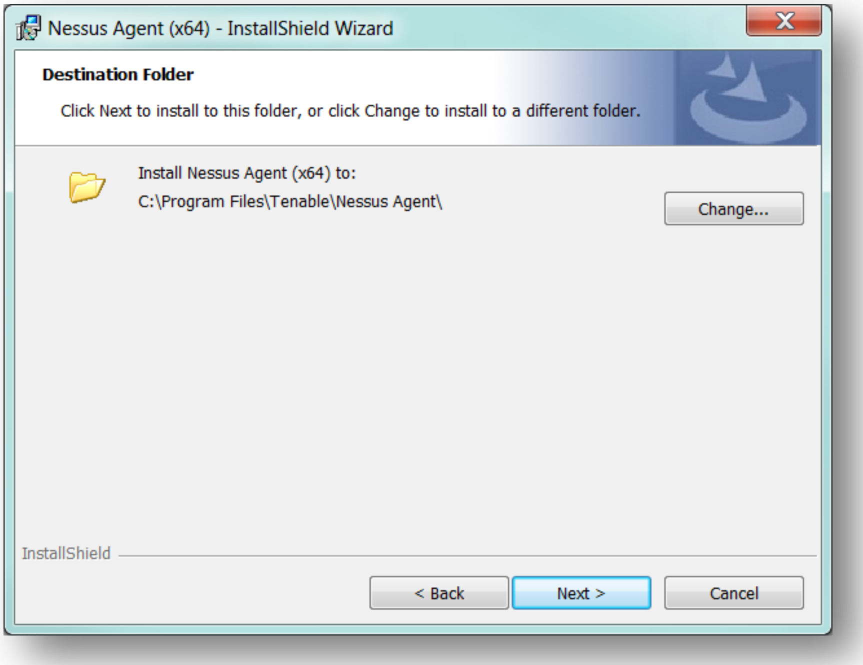
TENABLE NETWORK SECURITY, INC.
NESSUS®
SOFTWARE LICENSE AGREEMENT

This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7021 Columbia Gateway Drive, Suite 500, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers Your permitted use of the Software. ***BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS***

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

A suggested Destination Folder for the installation is displayed. You may accept the default Destination Folder of change the path.



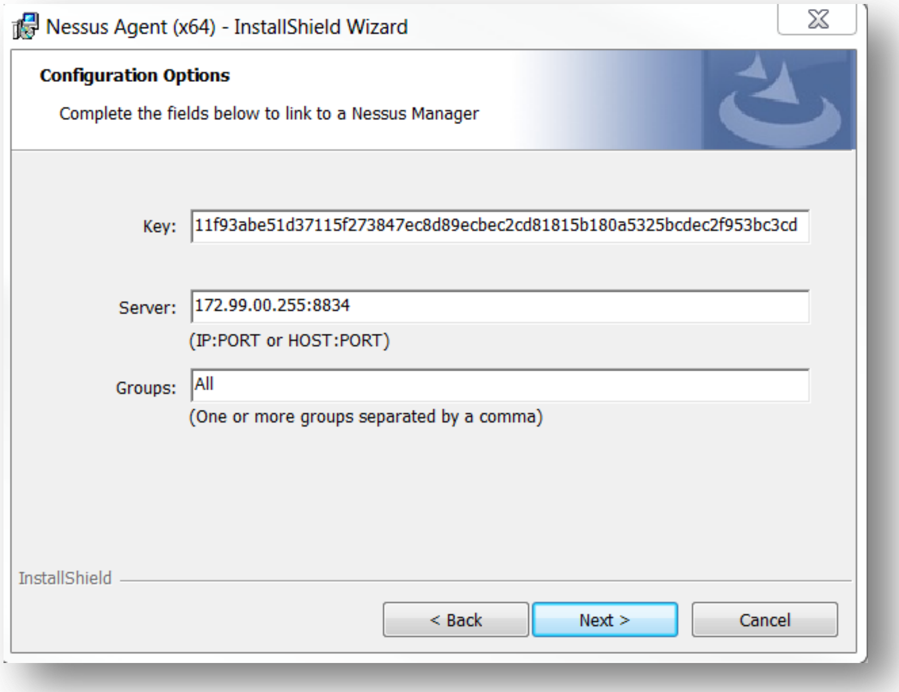
Nessus Agent (x64) - InstallShield Wizard

Destination Folder

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

Install Nessus Agent (x64) to:
C:\Program Files\Tenable\Nessus Agent\

A dialogue box will be displayed for Configuration Options. These settings allow the Nessus Agent to communicate with the Nessus Manager.



Nessus Agent (x64) - InstallShield Wizard

Configuration Options

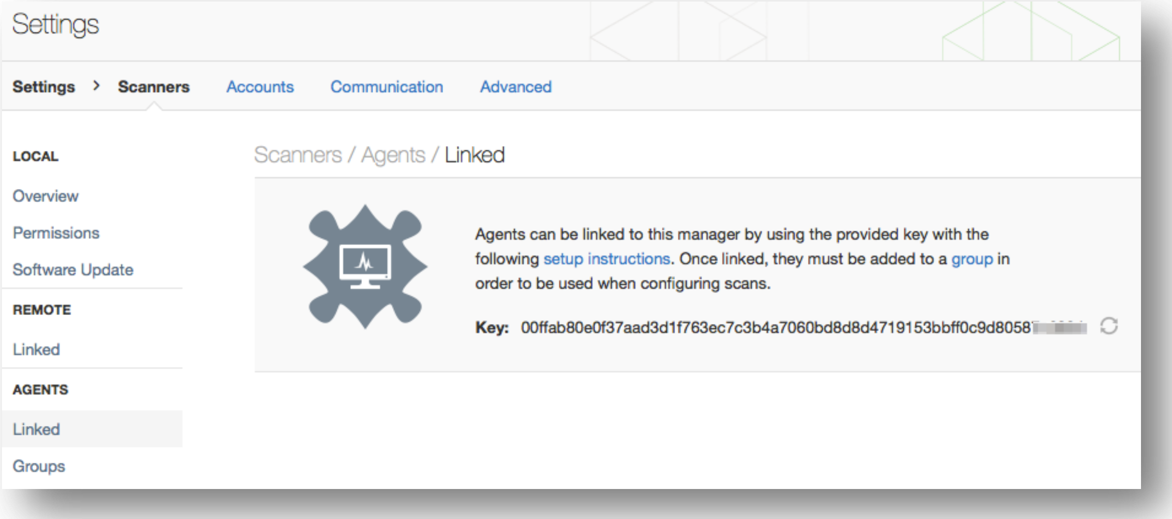
Complete the fields below to link to a Nessus Manager

Key: 11f93abe51d37115f273847ec8d89ecbec2cd81815b180a5325bcdec2f953bc3cd

Server: 172.99.00.255:8834
(IP:PORT or HOST:PORT)

Groups: All
(One or more groups separated by a comma)

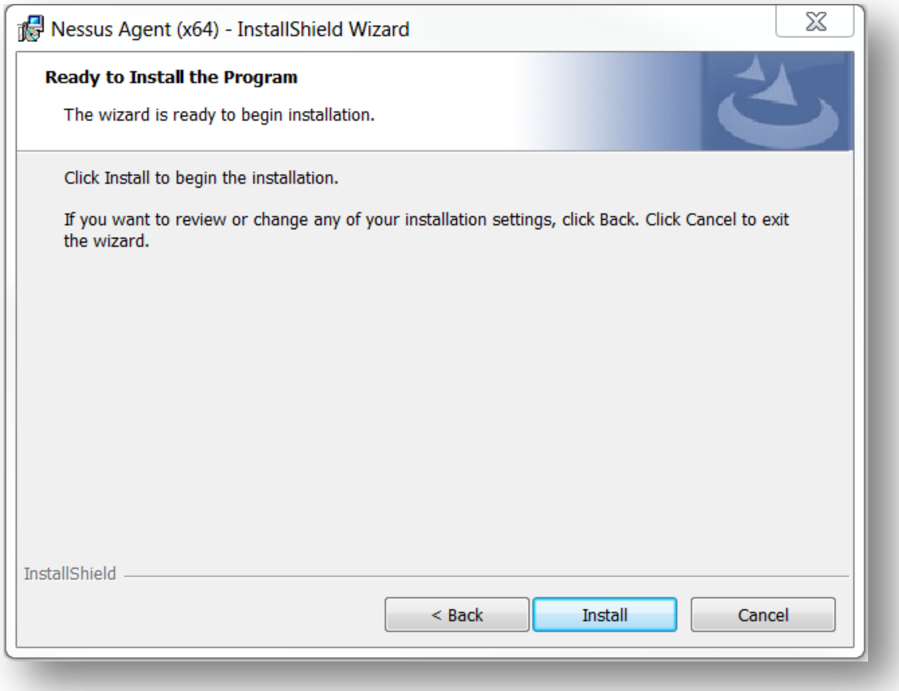
Field	Description
Key	The unique key that is generated and displayed in Nessus, which is used to link the Agent to the Manager.
Server	Enter the IP address and port number (:8834) of the Nessus Manager, or enter the hostname and port number (:8834) of the Nessus Manager. Examples: example.com:8834 127.0.0.1:8834 localhost:8834
Group	Agent groups are used to organize and manage the agents linked to your scanner. Each agent can be added to any number of groups and scans can be configured to use these groups as targets.



Agents can be linked to this manager by using the provided key with the following setup instructions. Once linked, they must be added to a group in order to be used when configuring scans.

Key: 00ffab80e0f37aad3d1f763ec7c3b4a7060bd8d8d4719153bbff0c9d8058[redacted]

After the Nessus Agent is configured, you will be prompted to run the installation:

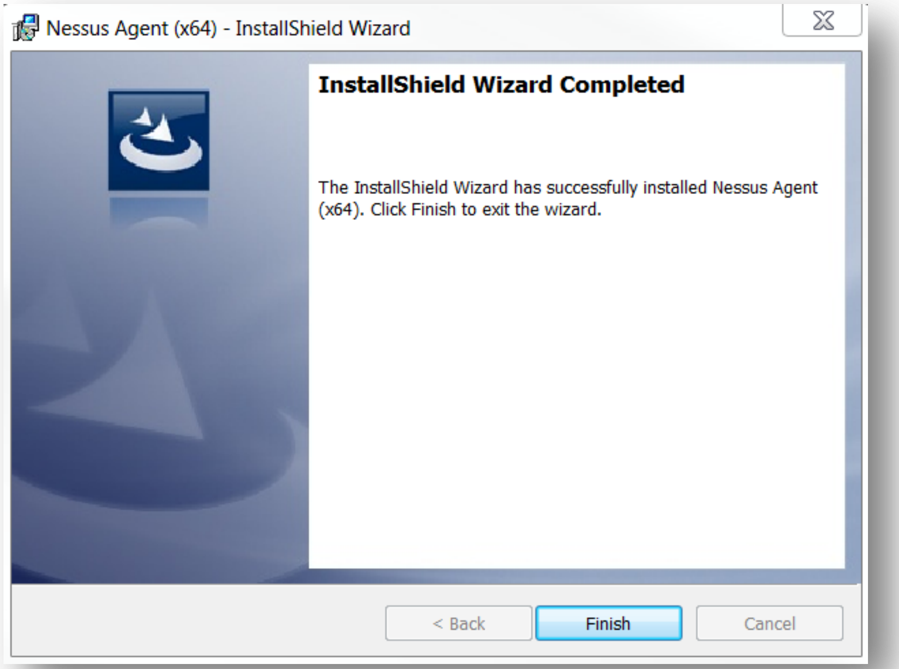

Nessus Agent (x64) - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

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


Nessus Agent (x64) - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Nessus Agent (x64). Click Finish to exit the wizard.

Finally, the Nessus Agent will register with the Nessus Manager and, if specified, added to a group. Afterwards, Nessus Agent control is handled by the Nessus Manager.

Since Nessus Agents do not run any type of remote checks, WinPCAP will not be installed.

Mac OS X Installation

To install Nessus on Mac OS X, double click **`NessusAgent-6.4.0.dmg.gz`** to unzip it. Double click on the **`NessusAgent-6.4.0.dmg`** file, which will mount the disk image and make it appear under "Devices" in "Finder". Once the volume "Nessus 6" appears in "Finder", double click on the file **`Install Nessus Agent`** package, and then follow the installation steps.

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

After installing the agent, you will need to link it to a manager from the Terminal.

Open a Terminal and run the following command.

Example:

```
# /Library/NessusAgent/run/sbin/nessuscli agent link
      --key=00edbg34028f795a2effb2e5be0276f232494fd74564d00d32a74548b9e92bf735
      --name= OSX_Agent --groups="All" --host=172.26.189.51 --port=8834
```

Required Values:
`--key`
`--host`
`--port`

Optional Values:
`--name`
`--groups`

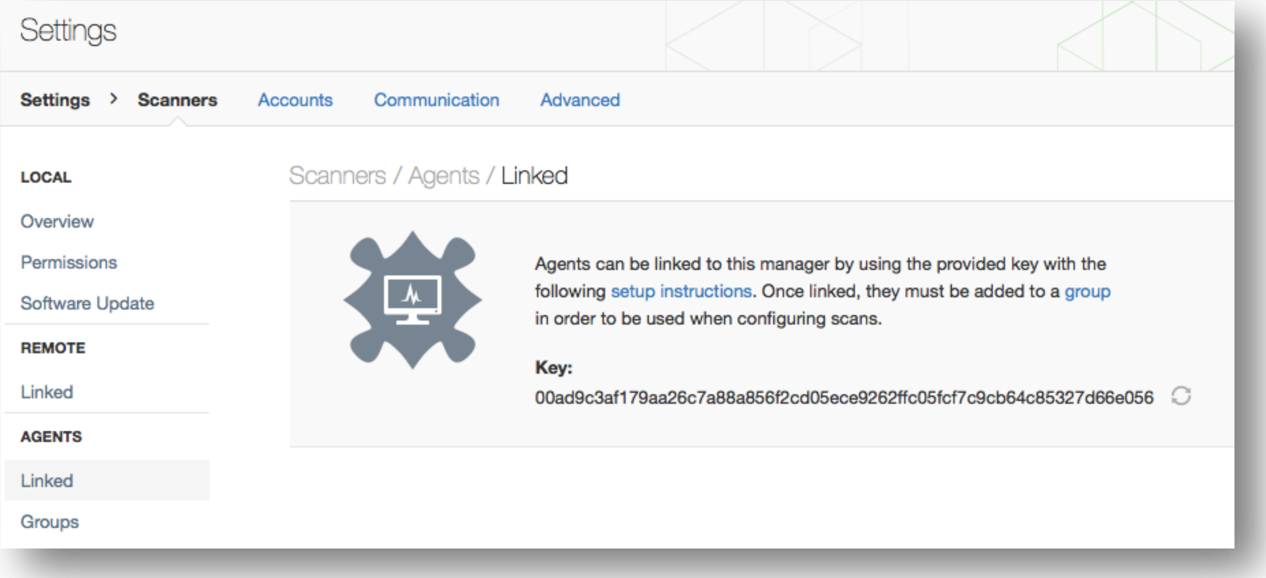
After running this command, the Agent will be visible in Nessus Manager.

To unlink the agent use the following command:

```
# /Library/NessusAgent/run/sbin/nessuscli agent unlink
```

Configuration

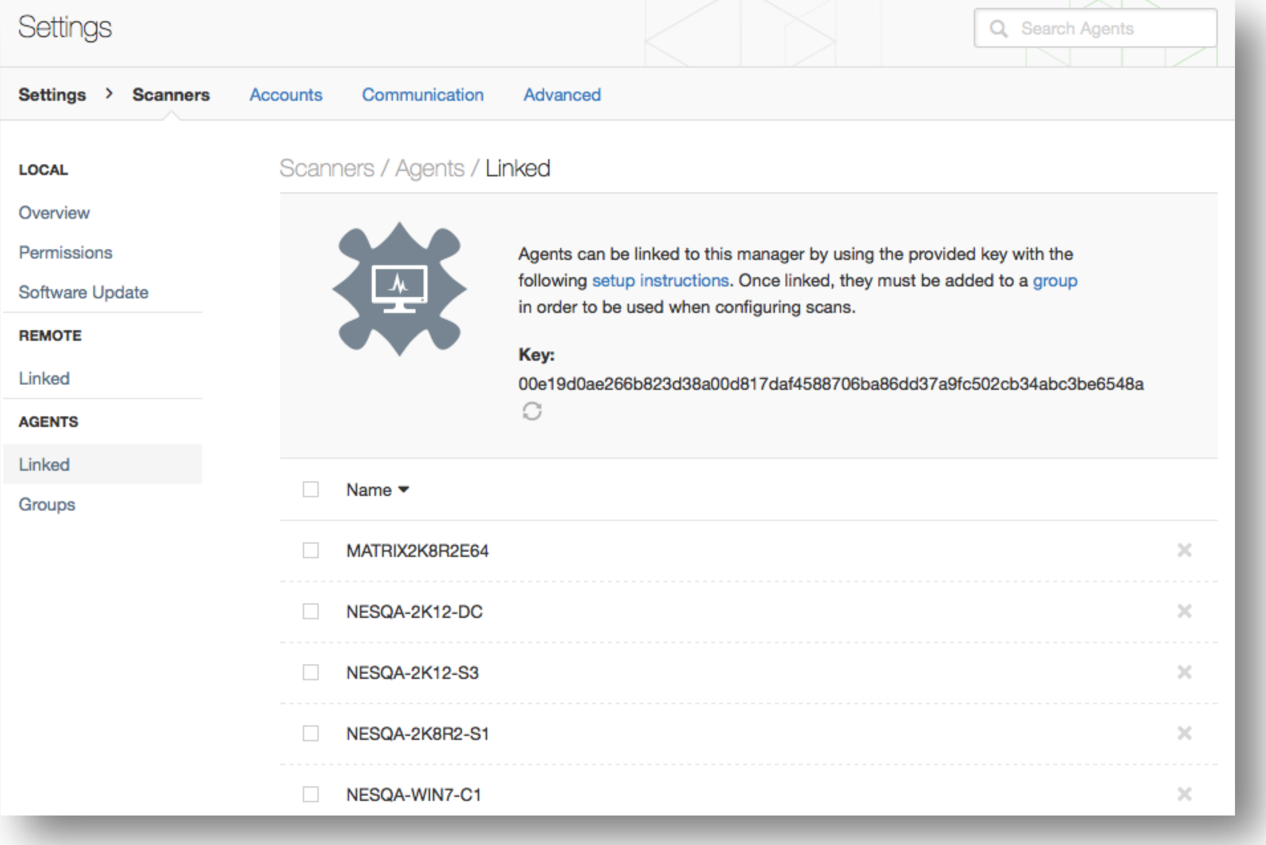
Nessus Manager and Nessus Cloud have the ability to designate scans to Nessus Agents that have been linked to it. Nessus Agents are linked to a Nessus Manager or Nessus Cloud similar to linking a secondary scanner. After selecting “**Agents**” under the Remote scanner section, select “**Linked**”. A key will be generated that is used as a shared secret for a secondary scanner to authenticate to the primary:



Agents can be linked to this manager by using the provided key with the following setup instructions. Once linked, they must be added to a group in order to be used when configuring scans.

Key:
00ad9c3af179aa26c7a88a856f2cd05ece9262ffc05fcf7c9cb64c85327d66e056

This key is only used for the initially linking the Nessus Manager or Nessus Cloud and Nessus Agent. Subsequent communication is done via a separate set of credentials. At any time, you can disable this functionality by clicking the “**Delete**” button after selecting the scanner. If there is ever concern over the shared secret becoming compromised, you can regenerate the key at any time by clicking the arrows to the right of the key. Regenerating the key will not disable any secondary scanners that are already registered. Once the secondary scanner has established communications with the primary scanner, it will display on this interface under the **Agents** scanners menu under the **Linked** menu:



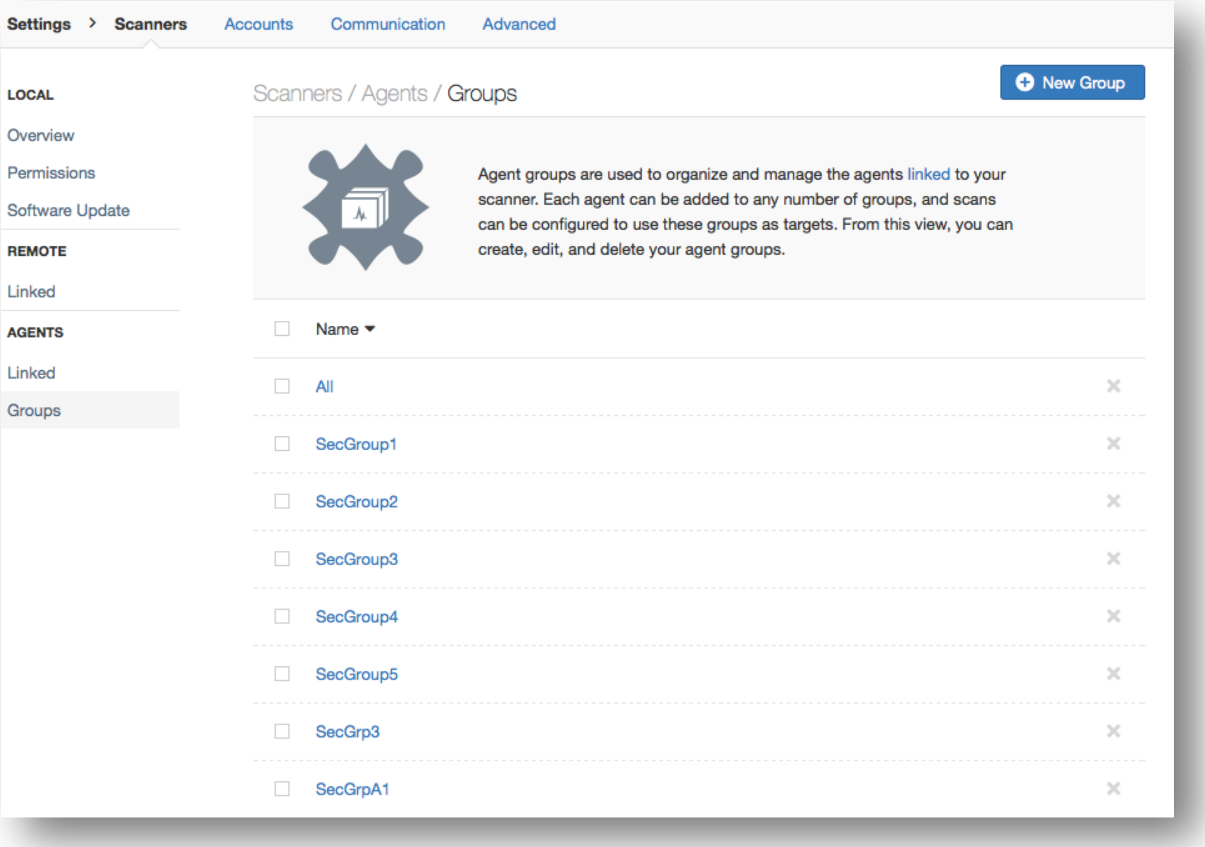
Scanners / Agents / Linked

Agents can be linked to this manager by using the provided key with the following setup instructions. Once linked, they must be added to a group in order to be used when configuring scans.

Key:
00e19d0ae266b823d38a00d817daf4588706ba86dd37a9fc502cb34abc3be6548a

□	Name ▾	
□	MATRIX2K8R2E64	✕
□	NESQA-2K12-DC	✕
□	NESQA-2K12-S3	✕
□	NESQA-2K8R2-S1	✕
□	NESQA-WIN7-C1	✕

After adding an agent, you must link it to a group. An agent will not scan unless it is part of an agent group. An agent can belong to multiple groups.

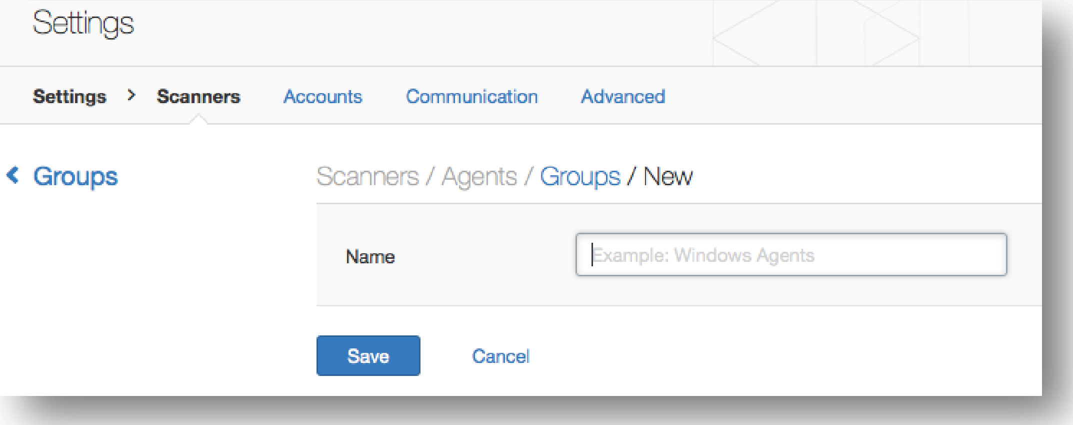


Scanners / Agents / Groups

Agent groups are used to organize and manage the agents linked to your scanner. Each agent can be added to any number of groups, and scans can be configured to use these groups as targets. From this view, you can create, edit, and delete your agent groups.

	Name ▾	
□	All	×
□	SecGroup1	×
□	SecGroup2	×
□	SecGroup3	×
□	SecGroup4	×
□	SecGroup5	×
□	SecGrp3	×
□	SecGrpA1	×

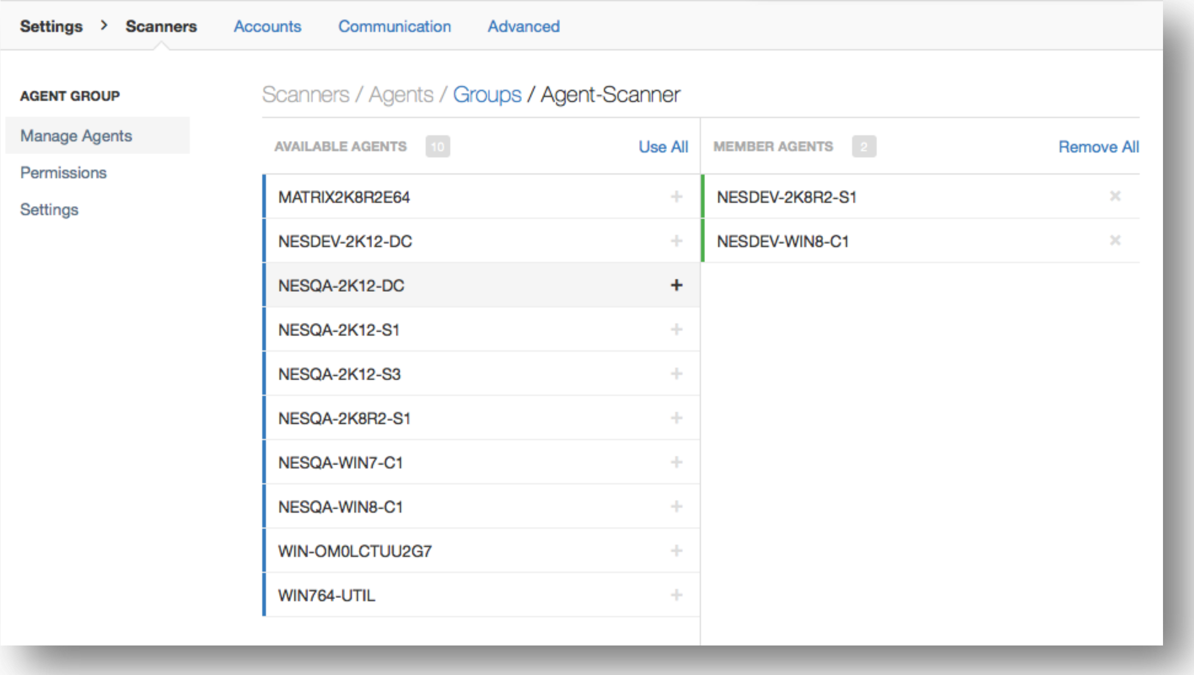
To create a new group, click the **New Group** button. This will bring up a new screen to input the unique name of the group:



Scanners / Agents / Groups / New

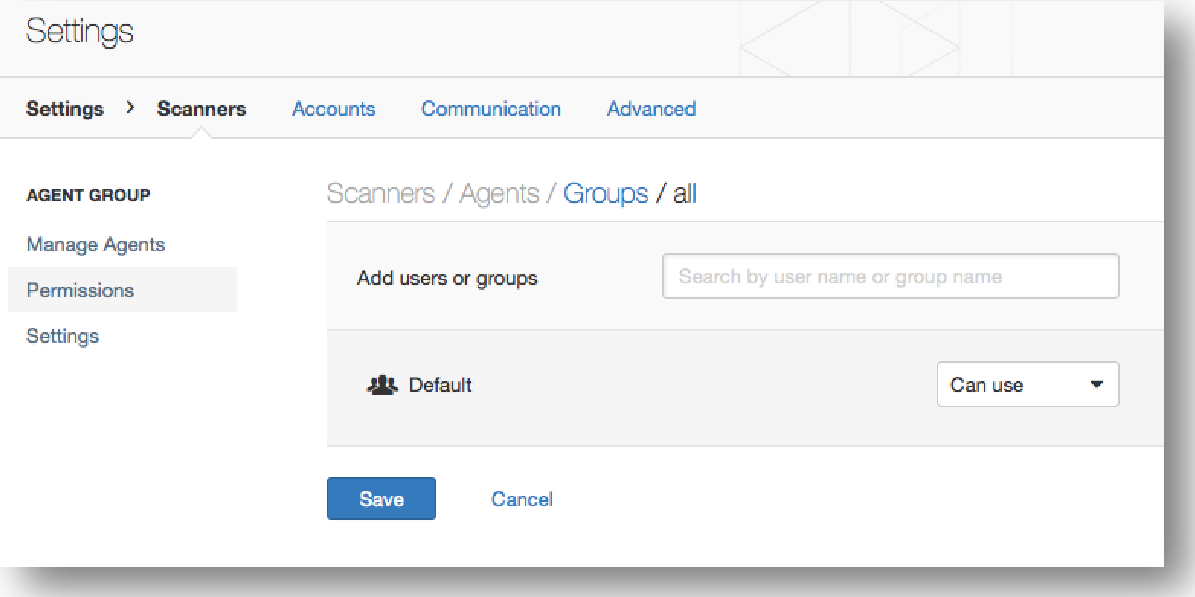
Name: Example: Windows Agents

Once a group is created, click on the group name. You will see available agents in the left column, and member agents in the right column. Member agents are members of the current group, and available agents are agents that are configured with this Nessus Manager. To move an agent from one column to another, mouse over the column and click on that agent name:



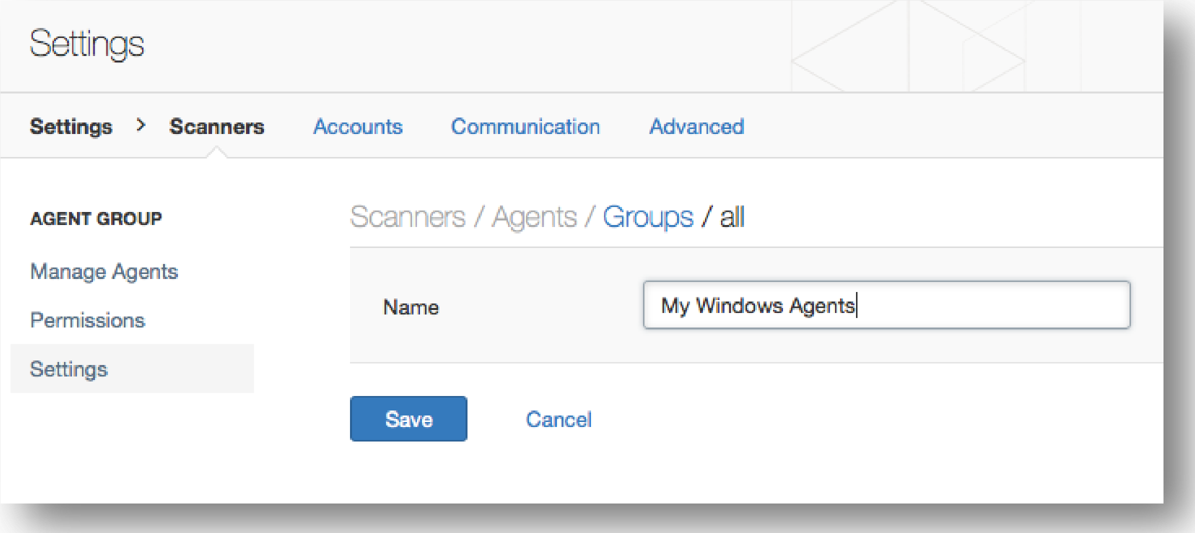
AVAILABLE AGENTS 10 Use All	MEMBER AGENTS 2 Remove All
MATRIX2K8R2E64 +	NESDEV-2K8R2-S1 ×
NESDEV-2K12-DC +	NESDEV-WIN8-C1 ×
NESQA-2K12-DC +	
NESQA-2K12-S1 +	
NESQA-2K12-S3 +	
NESQA-2K8R2-S1 +	
NESQA-WIN7-C1 +	
NESQA-WIN8-C1 +	
WIN-OM0LCTUU2G7 +	
WIN764-UTIL +	

Nessus Agents also can have permissions configured similar to Nessus scanners that are connected to the Nessus Manager. In Nessus Manager, you can configure the permissions of the users or groups who **Can use** or have **No access** the Nessus Agent group:



Copyright © 2015. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc. SecurityCenter is a trademark of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners.

If you wish to change the name of your Nessus Agent group, click on "Settings". Then replace the name in the text field:



Name: My Windows Agents

Working with SecurityCenter

SecurityCenter Overview

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

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

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

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

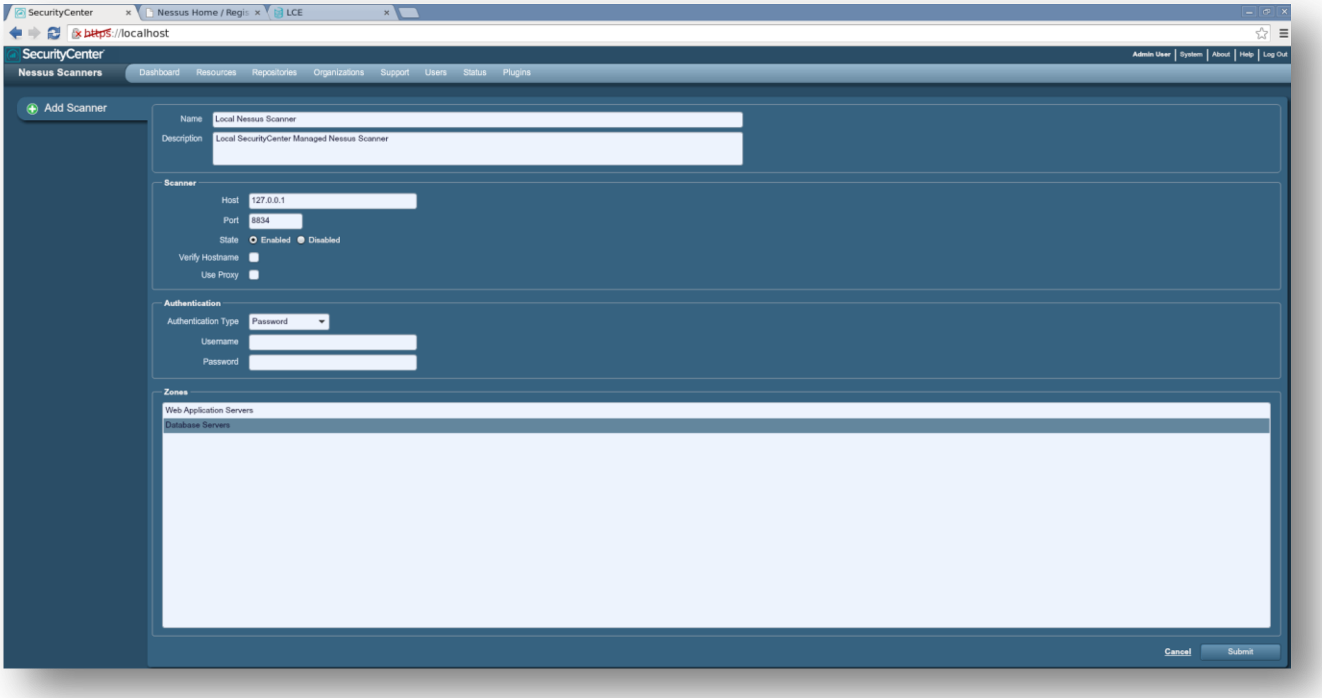
Note that if Nessus Managers administers secondary scanners, those scanners will **not** be available to SecurityCenter. Any secondary scanners will remain exclusive to Nessus Manager.

Configuring SecurityCenter to work with Nessus

The SecurityCenter administration interface is used to configure access and control of any Nessus scanner that is version 4.2.x or higher. Click the "**Resources**" tab and then click "**Nessus Scanners**". Click "**Add**" to open the "**Add Scanner**" dialog. The Nessus scanner's IP address or hostname, Nessus port (default: 8834), authentication type (created while configuring Nessus), 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, the use of a proxy may be selected, and selection of Scan Zones for the Nessus scanner to be assigned to can be selected.

An example screen capture of the SecurityCenter 4.8 "**Add Scanner**" page is shown below:



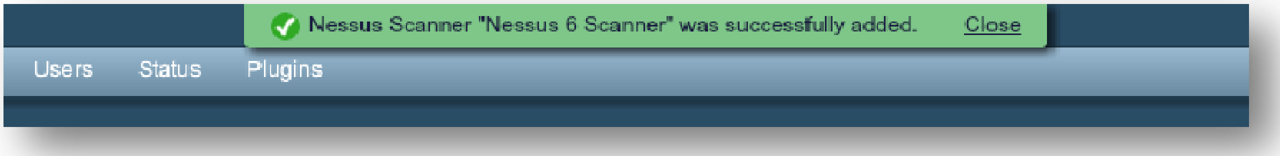
Name: Local Nessus Scanner
Description: Local SecurityCenter Managed Nessus Scanner

Scanner
Host: 127.0.0.1
Port: 8834
State: ● Enabled ○ Disabled
Verify Hostname: □
Use Proxy: □

Authentication
Authentication Type: Password
Username:
Password:

Zones
Web Application Servers
Database Servers

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



Nessus Scanner "Nessus 6 Scanner" was successfully added.

For more information on integrating Nessus scanners and SecurityCenter, please refer to the "SecurityCenter Administration Guide" available on the Tenable Support Portal.

Host-Based Firewalls

If your Nessus server is configured with a local firewall such as the default Windows firewall, or any other installed third-party firewall software, it is required that connections be opened from SecurityCenter's IP address. By default, TCP port 8834 is used to communicate with SecurityCenter. If a connection is not currently allowed for TCP port 8834 an exception will have to be made in the firewall to allow access.

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

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

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

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

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

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

Getting Support

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

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

> If you are using Nessus in conjunction with Tenable's SecurityCenter, it will automatically update your Nessus scanners without additional interaction.

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

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

Additional Resources

Tenable has produced a variety of other documents detailing Nessus' installation, deployment, configuration, user operation, and overall testing:

- Nessus 6.4 User Guide – how to configure and operate the Nessus User Interface for Nessus Professional, Nessus Manager, Nessus Cloud, and Nessus Agents
- Nessus 6.4 Command Line Reference – describes the Nessus command line tools for Nessus Professional, Nessus Manager, and Nessus Agents
- Nessus v6 SCAP Assessments – describes how to use Tenable's Nessus to generate SCAP content audits as well as view and export the scan results
- 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 and Antivirus – outlines how several popular security software packages interact with Nessus, and provides tips or workarounds to allow the software to better co-exist without compromising your security or hindering your vulnerability scanning efforts
- Comprehensive Malware Detection with SecurityCenter Continuous View and Nessus – describes how Tenable's SecurityCenter CV can detect a variety of malicious software and identify and determine the extent of malware infections
- Real-Time Compliance Monitoring – outlines how Tenable's solutions can be used to assist in meeting many different types of government and financial regulations

- Tenable Products Plugin Families – provides a description and summary of the plugin families for Nessus, Log Correlation Engine, and the Passive Vulnerability Scanner
- SecurityCenter Administration Guide

Other online resources are listed below:

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

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

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.