



Nessus 4.2 User Guide

**June 9, 2010
(Revision 9)**

The newest version of this document is available at the following URL:
http://www.nessus.org/documentation/nessus_4.2_user_guide.pdf

Table of Contents

TABLE OF CONTENTS	2
INTRODUCTION	3
NESSUS UI OVERVIEW	3
DESCRIPTION	3
SUPPORTED PLATFORMS	4
INSTALLATION	4
OPERATION	4
OVERVIEW.....	4
<i>Connect to Nessus GUI.</i>	4
POLICY OVERVIEW.....	6
CREATING A POLICY.....	7
<i>General.</i>	7
<i>Credentials.</i>	11
<i>Plugins.</i>	14
<i>Preferences.</i>	17
IMPORTING AND COPYING POLICIES.....	30
CREATING AND LAUNCHING A SCAN.....	30
REPORTS	32
<i>Browse</i>	32
<i>Report Filters</i>	35
<i>Compare</i>	38
<i>Upload & Download</i>	39
<i>.nessus File Format</i>	41
<i>Delete</i>	41
USERS.....	41
OTHER NESSUS CLIENTS	42
UNIX COMMAND LINE INTERFACE.....	42
<i>Converting a Report.</i>	43
<i>Command Line using .nessus Files</i>	44
<i>Scan Command.</i>	45
SECURITYCENTER.....	45
ABOUT TENABLE NETWORK SECURITY	47

Introduction

This document describes how to use Tenable Network Security's **Nessus user interface (UI)**. Please share your comments and suggestions with us by emailing them to support@tenablesecurity.com.

The Nessus UI is a web-based interface to the Nessus vulnerability scanner. To use the client, you must have an operational Nessus scanner deployed and be familiar with its use.

Standards and Conventions

Throughout the documentation, filenames, daemons and executables are indicated with a **courier bold** font such as `gunzip`, `httpd` and `/etc/passwd`.

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

```
# pwd
/opt/sc3/daemons
#
```



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.

Nessus UI Overview

Description

Nessus is a product developed and maintained by Tenable Network Security to provide an optimized Graphical User Interface (GUI) to the Nessus scanner. The client may be used from any system on the network to interface with deployed Nessus scanners. As of Nessus 4.2, The UI is a newly created web-based interface made up of a simple HTTP server and web client, requiring no software installation apart from the Nessus Server. As of Nessus 4, all platforms draw from the same code base eliminating most platform specific bugs and allowing for faster deployment of new features. The primary features are:

- Generates `.nessus` files that Tenable products will use as the standard for vulnerability data and scan policy.
- A policy session, list of targets and the results of several scans can all be stored in a single `.nessus` file that can be easily exported. Please refer to the [Nessus File Format guide](#) for more details.
- The GUI displays scan results in real-time so you do not have to wait for a scan to complete to view results.
- Provides unified interface to the Nessus scanner regardless of base platform. The same functionalities exist on Mac OS X, Windows and Linux.

- Scans will continue to run on the server even if you are disconnected for any reason.
- Nessus scan reports can be uploaded via the Nessus UI and compared to other reports.

Supported Platforms

Since the Nessus UI is a web-based client, it can run on any platform with a web browser.



The Nessus web-based user interface is best experienced using Microsoft Internet Explorer 7 and 8, Mozilla Firefox 3.5.x or Apple Safari.

Installation

Starting with Nessus 4.2, user management of the Nessus server is conducted through a web interface and it is no longer necessary to use a standalone NessusClient. The standalone NessusClients will still connect and operate the scanner, but they will not be updated.

Refer to the Nessus 4.2 Installation Guide for instructions on installing Nessus. No additional software installation is required.

Operation

Overview

Nessus provides a simple, yet powerful interface for managing vulnerability-scanning activity.

Connect to Nessus GUI

To launch the Nessus GUI, perform the following:

- Open a web browser of your choice.
- Enter [https://\[server IP\]:8834/](https://[server IP]:8834/) in the navigation bar.

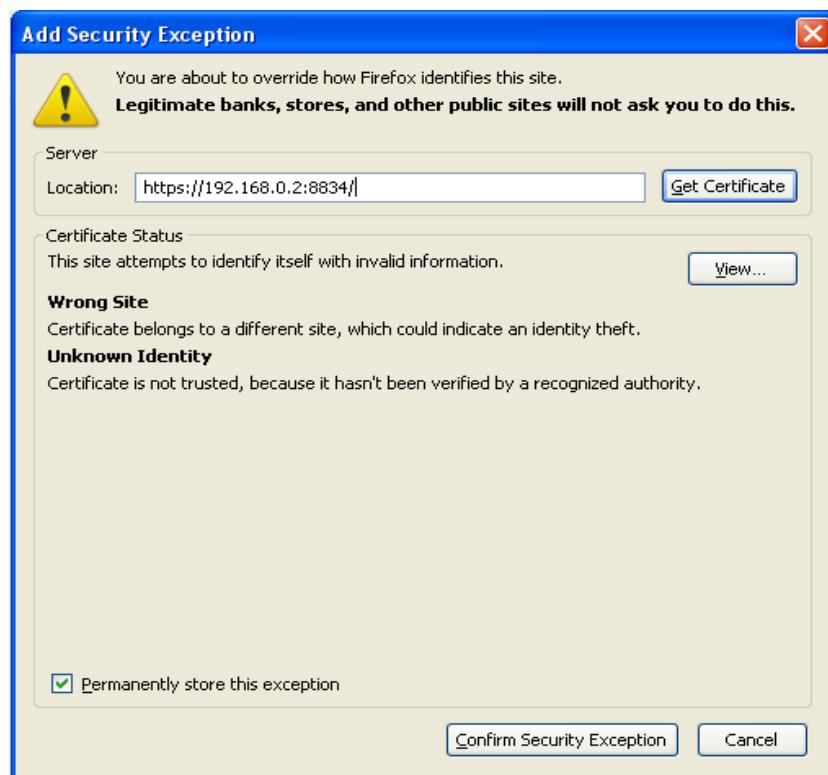


Be sure to connect to the user interface via HTTPS, as unencrypted HTTP connections are not supported.

The first time you attempt to connect to the Nessus user interface, most web browsers will display an error indicating the site is not trusted due to the self-signed SSL certificate:

The screenshot shows a browser window with two panels. The left panel has a red shield icon with a white 'X' and the text: "There is a problem with this website's security certificate." Below it, there are two error messages: "The security certificate presented by this website was not issued by a trusted certificate authority." and "The security certificate presented by this website was issued for a different website's address." A note states: "Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server." It also says: "We recommend that you close this webpage and do not continue to this website." with three options: "Click here to close this webpage.", "Continue to this website (not recommended).", and "More information". The right panel has a yellow shield icon with a person and the title "This Connection is Untrusted". It explains: "You have asked Firefox to connect securely to 192.168.0.2:8834, but we can't confirm that your connection is secure." It notes: "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." Under "What Should I Do?", it says: "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." with a "Get me out of here!" button. There are two links: "Technical Details" and "I Understand the Risks".

Users of Microsoft Internet Explorer can click on “Continue to this website (not recommended)” to load the Nessus user interface. Firefox 3.x users can click on “I Understand the Risks” and then “Add Exception...” to bring up the site exception dialog box:



Verify the “Location:” bar reflects the URL to the Nessus server and click on “**Confirm Security Exception**”. For information on installing a custom SSL certificate, consult the Nessus Installation Guide.

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



Authenticate using an account and password previously created with the server manager. After successful authentication, the UI will present menus for conducting scans:

A screenshot of the Nessus user interface in Mozilla Firefox. The title bar says "Nessus - Mozilla Firefox". The address bar shows "127.0.0.1 https://127.0.0.1:8834/". The top navigation bar includes links for Reports, Scans, Policies, and Users. The "Reports" tab is currently selected. Below the navigation is a toolbar with buttons for Browse, Compare, Upload, Download, and Delete. A table below the toolbar lists items with columns for Name, Status, and Last Updated.

Policy Overview

A screenshot of the Nessus user interface in Mozilla Firefox. The title bar says "Nessus - Mozilla Firefox". The address bar shows "127.0.0.1 https://127.0.0.1:8834/". The top navigation bar includes links for Policies, Reports, Scans, Policies, and Users. The "Policies" tab is currently selected. Below the navigation is a toolbar with buttons for Add, Import, Copy, Edit, and Delete. A table below the toolbar lists items with columns for Name, Visibility, and Owner.

A Nessus “policy” consists of configuration options related to performing a vulnerability scan. These options include, but are not limited to:

- Parameters that control technical aspects of the scan such as timeouts, number of hosts, type of port scanner and more.
- Credentials for local scans (e.g., Windows, SSH), authenticated Oracle Database scans, HTTP, FTP, POP, IMAP or Kerberos based authentication.
- Granular family or plugin based scan specifications.
- Database compliance policy checks, report verbosity, service detection scan settings, Unix compliance checks and more.

Creating a Policy

Once you have connected to a Nessus server UI, you can create a custom policy by clicking on the “**Policies**” option on the bar at the top and then “**+ Add**” button on the right. The “**Add Policy**” screen will be displayed as follows:

Note that there are four configuration tabs: **General**, **Credentials**, **Plugins** and **Preferences**. For most environments, the default settings do not need to be modified, but they provide more granular control over the Nessus scanner operation. These tabs are described below.

General

The General tab enables you to name the policy and configure scan related operations. There are six boxes of grouped options that control scanner behavior:

The “**Basic**” frame is used to define aspects of the policy itself:

Option	Description
--------	-------------

Name	Sets the name that will be displayed in the Nessus UI to identify the policy.
Visibility	Controls if the policy is <i>shared</i> with other users, or kept <i>private</i> for your use only. Only administrative users can share policies.
Description	Used to give a brief description of the scan policy, typically good to summarize the overall purpose (e.g., "Web Server scans without local checks or non HTTP services").

The “**Scan**” frame further defines options related to how the scan should behave:

Option	Description
Save Knowledge Base	The Nessus scanner can save the scan information to the Nessus server knowledge base for later use. This includes open ports, plugins that fired successfully, services discovered and more.
Safe Checks	Safe Checks will disable all plugins that may have an adverse effect on the remote host.
Silent Dependencies	If this option is checked, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, uncheck the box.
Log Scan Details to Server	Save additional details of the scan to the Nessus server log (<code>nessusd.messages</code>) including plugin launch, plugin finish or if a plugin is killed. The resulting log can be used to confirm that particular plugins were used and hosts were scanned.
Stop Host Scan on Disconnect	If checked, Nessus will stop scanning if it detects that the host has become unresponsive. This may occur if users turn off their PCs during a scan, a host has stopped responding after a denial of service plugin or a security mechanism (e.g., IDS) has begun to block traffic to a server. Continuing scans on these machines will send unnecessary traffic across the network and delay the scan.
Avoid Sequential Scans	By default, Nessus scans a list of IP addresses in sequential order. If checked, Nessus will scan the list of hosts in a random order. This is typically useful in helping to distribute the network traffic directed at a particular subnet during large scans.
Consider Unscanned Ports as Closed	If a port is not scanned with a selected port scanner (e.g., out of the range specified), Nessus will consider it closed.
Designate Hosts by their DNS Name	Use the host name rather than IP address for report output.

The “**Network**” frame gives options that better control the scan based on the target network being scanned:

Option	Description
Reduce Parallel Connections on Congestion	This enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity. If detected, Nessus will throttle the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Nessus will automatically attempt to use the available space within the network pipe again.
Use Kernel Congestion Detection (Linux Only)	Enables Nessus to monitor the CPU and other internal workings for congestion and scale back accordingly. Nessus will always attempt to use as much resource as is available. This feature is only available for Nessus scanners deployed on Linux.

The “**Port Scanners**” frame controls which methods of port scanning should be enabled for the scan:

Option	Description
TCP Scan	<p>Use Nessus’ built-in TCP scanner to identify open TCP ports on the targets. This scanner is optimized and has some self-tuning features.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  On some platforms (e.g., Windows and Mac OS X), if the operating system is causing serious performance issues using the TCP scanner, Nessus will launch the SYN scanner. </div>
UDP Scan	<p>This option engages Nessus’ built-in UDP scanner to identify open UDP ports on the targets.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  UDP is a “stateless” protocol, meaning that communication is not done with handshake dialogues. UDP based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable. </div>
SYN Scan	<p>Use Nessus’ built-in SYN scanner to identify open TCP ports on the targets. SYN scans are a popular method for conducting port scans and generally considered to be a bit less intrusive than TCP scans. The scanner sends a SYN packet to the port, waits for SYN-ACK reply and determines port state based on a reply, or lack of reply.</p>
SNMP Scan	<p>Direct Nessus to scan targets for a SNMP service. Nessus will</p>

	guess relevant SNMP settings during a scan. If the settings are provided by the user under "Preferences", this will allow Nessus to better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.
Netstat SSH Scan	This option uses <code>netstat</code> to check for open ports from the local machine. It relies on the <code>netstat</code> command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.
Netstat WMI Scan	This option uses <code>netstat</code> to check for open ports from the local machine. It relies on the <code>netstat</code> command being available via a WMI connection to the target. This scan is intended for Windows-based systems and requires authentication credentials.
Ping Host	This option enables the pinging of remote hosts on multiple ports to determine if they are alive.

The "**Port Scan Options**" frame directs the scanner to target a specific range of ports. The following values are allowed for the "Port Scan Range" option:

Value	Description
"default"	Using the keyword "default", Nessus will scan approximately 4,790 common ports.
"all"	Using the keyword "all", Nessus will scan all 65,535 ports.
Custom List	A custom range of ports can be selected by using a comma delimited list of ports or port ranges. For example, "21,23,25,80,110" or "1-1024,8080,9000-9200" are allowed. Specifying "1-65535" will scan all ports.



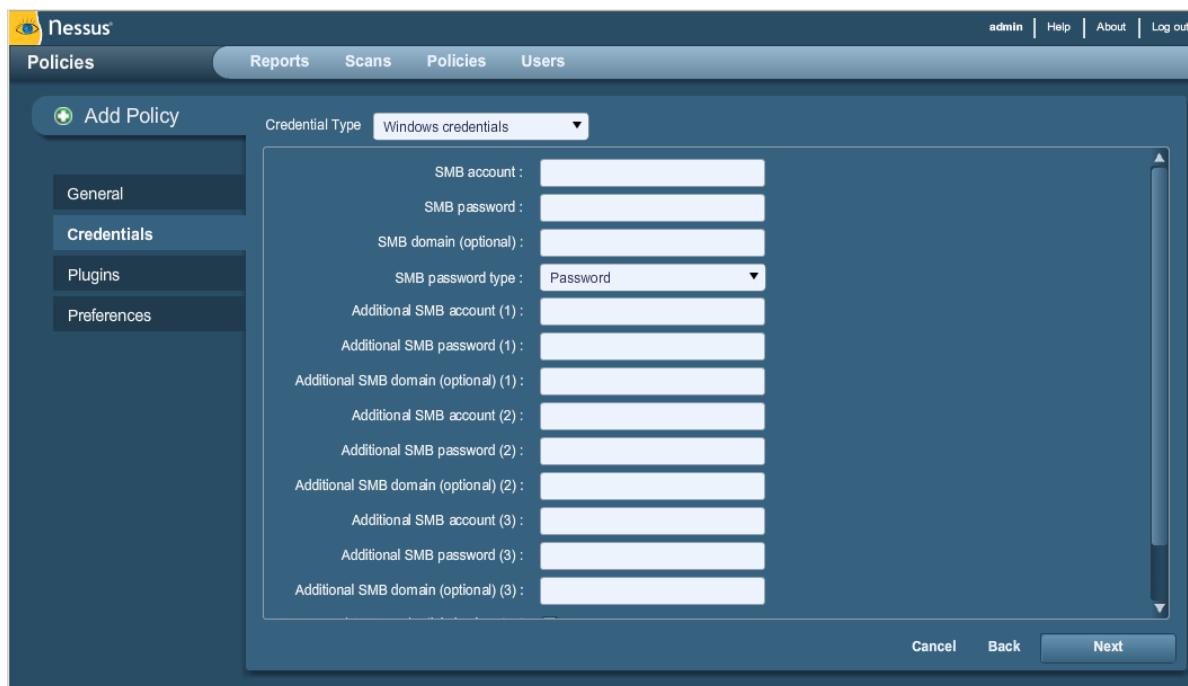
The range specified for a port scan will be applied to both TCP and UDP scans.

The "**Performance**" frame gives two options that control how many scans will be launched. These options are perhaps the most important when configuring a scan as they have the biggest impact on scan times and network activity.

Option	Description
Max Checks Per Host	This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time.
Max Hosts Per Scan	This setting limits the maximum number of hosts that a Nessus scanner will scan at the same time.
Network Receive Timeout (seconds)	Set to five seconds by default. This is the time that Nessus will wait for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.
Max Simultaneous TCP Sessions Per Host	This setting limits the maximum number of established TCP sessions for a single host.
Max Simultaneous TCP Sessions Per Scan	This setting limits the maximum number of established TCP sessions for the entire scan, regardless of the number of hosts being scanned.

Credentials

The Credentials tab, pictured below, allows you to configure the Nessus scanner to use authentication credentials during scanning. By configuring credentials, it allows Nessus to perform a wider variety of checks that result in more accurate scan results.



The “**Windows credentials**” drop-down menu item has settings to provide Nessus with information such as SMB account name, password and domain name. Server Message Block

(SMB) is a file sharing protocol that allows computers to share information transparently across the network. Providing this information to Nessus will allow it to find local information from a remote Windows host. For example, using credentials enables Nessus to determine if important security patches have been applied. It is not necessary to modify other SMB parameters from default settings.

If a maintenance SMB account is created with limited administrator privileges, Nessus can easily and securely scan multiple domains. Detailed configuration instructions are available at:

http://www.nessus.org/documentation/nessus_domain_whitepaper.pdf

Tenable recommends that network administrators consider creating specific domain accounts to facilitate testing. Nessus includes a variety of security checks for Windows NT, 2000, Server 2003, XP, Vista, Windows 7 and Windows 2008 that are more accurate if a domain account is provided. Nessus does attempt to try several checks in most cases if no account is provided.



The Windows Remote Registry service allows remote computers with credentials to access the registry of the computer being audited. If the service is not running, reading keys and values from the registry will not be possible, even with full credentials. Please see the Tenable blog post titled "[Dynamic Remote Registry Auditing - Now you see it, now you don't!](#)" for more information.

Users can select "**SSH settings**" from the drop-down menu and enter credentials for scanning Unix systems. These credentials are used to obtain local information from remote Unix systems for patch auditing or compliance checks. There is a field for entering the SSH user name for the account that will perform the checks on the target Unix system, along with either the SSH password or the SSH public key and private key pair. There is also a field for entering the Passphrase for the SSH key, if it is required.



Nessus 4 supports the **blowfish-cbc**, **aes-cbc** and **aes-ctr** cipher algorithms.

The most effective credentialed scans are those when the supplied credentials have "root" privileges. Since many sites do not permit a remote login as root, Nessus users can invoke "su" or "sudo" with a separate password for an account that has been set up to have "su" or "sudo" privileges.

Nessus can use SSH key-based access to authenticate to a remote server. If an SSH known_hosts file is available and provided as part of the scan policy, Nessus will only attempt to log into hosts in this file. This can ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a login to a system that may not be under your control. Finally, the "Preferred SSH port" can be set to direct Nessus to connect to SSH if it is running on a port other than 22.



Nessus also supports a "su+sudo" option that can be used in the event of a system not allowing privileged accounts remote login privileges.

An example screen capture of using "sudo" to elevate privileges for a scan follows. For this example, the user account is "audit", which has been added to the **/etc/sudoers** file on the

system to be scanned. The password provided is the password for the “audit” account, not the root password:

The screenshot shows the 'Add Policy' interface with the 'Credentials' tab selected. The 'Credential Type' dropdown is set to 'SSH settings'. The configuration fields include:

- SSH user name : audit
- SSH password (unsafe!) : *****
- SSH public key to use : (empty)
- SSH private key to use : (empty)
- Passphrase for SSH key : (empty)
- Elevate privileges with : sudo
- su/sudo password : *****
- SSH known_hosts file : (empty)
- Preferred SSH port : 22

There are 'Browse...' buttons next to the SSH public key, SSH private key, and SSH known_hosts file fields.

The Credentials tab also provides an option in the drop-down menu for configuring “**Oracle settings**”, specifically the Oracle SID and option to test for known default accounts in Oracle software:

The screenshot shows the 'Add Policy' interface with the 'Credentials' tab selected. The 'Credential Type' dropdown is set to 'Oracle settings'. The configuration fields include:

- Oracle SID : (empty)
- Test default accounts (slow) :

“**Kerberos configuration**” allows you to specify credentials using Kerberos keys from a remote system:

The screenshot shows the 'Add Policy' interface with 'Credentials' selected in the sidebar. The 'Credential Type' dropdown is set to 'Kerberos configuration'. The form includes fields for 'Kerberos Key Distribution Center (KDC)', 'Kerberos KDC Port' (set to 88), 'Kerberos KDC Transport' (set to udp), and 'Kerberos Realm (SSH only)'.

Finally, if a secure method of performing credentialated checks is not available, users can force Nessus to try to perform checks over insecure protocols by configuring the “**Cleartext protocol settings**” drop-down menu item. The cleartext protocols supported for this option are **telnet**, **rsh** and **rexec**.

The screenshot shows the 'Add Policy' interface with 'Credentials' selected in the sidebar. The 'Credential Type' dropdown is set to 'Cleartext protocols settings'. The form includes fields for 'User name' and 'Password (unsafe!)'. Below these are three checkboxes: 'Try to perform patch level checks over telnet', 'Try to perform patch level checks over rsh', and 'Try to perform patch level checks over rexec'.

By default, all passwords associated with the policy are encrypted. If the policy is saved to a **.nessus** file and that **.nessus** file is then copied to a different Nessus installation, all passwords in the policy will be unusable by the second Nessus scanner as it will be unable to decrypt them.

To resolve this issue, the “**Save credentials as clear text in policy**” option is provided. When selected, if the policy is saved to a **.nessus** file, all passwords will be saved to the file in clear text. The policy may then be copied to a second Nessus installation and then re-saved with the “**Save credentials**” option, thus encrypting them again.

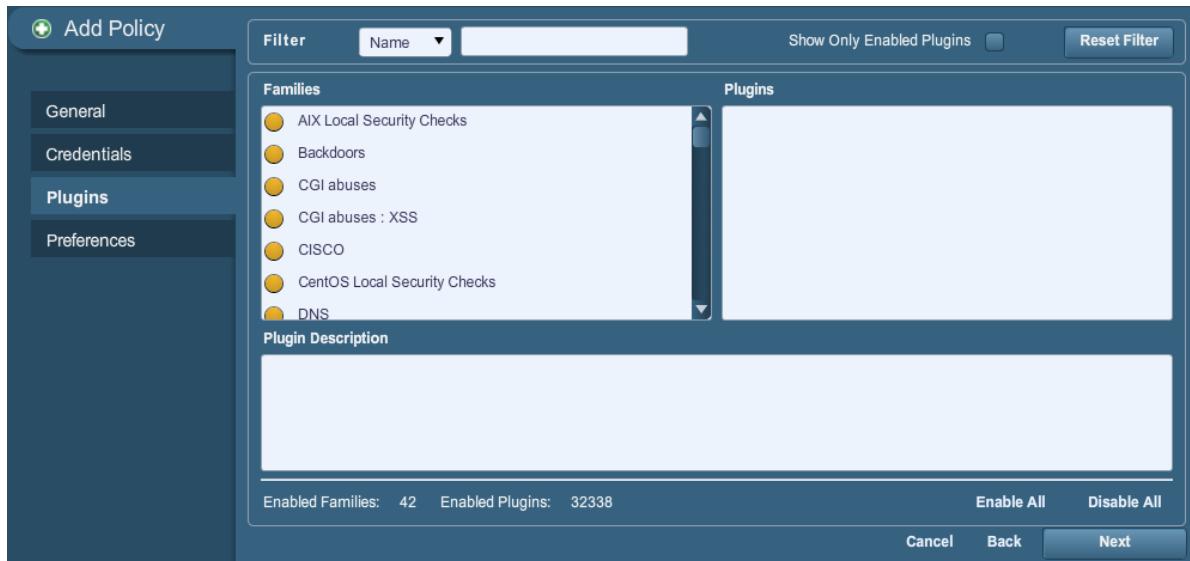
If you do not want the policy to store credentials in any manner, select the “**Do not save credentials**” option.



Using cleartext credentials in any fashion is **not** recommended! If the credentials are sent remotely, via a Nessus scan or e-mailing a policy to another administrator, the credentials could be intercepted by anyone with access to the network. Use encrypted authentication mechanisms whenever possible.

Plugins

The Plugin Selection tab enables the user to choose specific security checks by plugin family or individual checks.



Clicking on the yellow circle next to a plugin family allows you to enable or disable the entire family. Selecting a family will display the list of its plugins in the upper right pane. Individual plugins can be enabled or disabled to create very specific scan policies. As adjustments are made, the total number of families and plugins selected is displayed at the bottom. If the circle next to a plugin family is half grey and half yellow, it denotes that some of the plugins are enabled, but not all of them.

Selecting a specific plugin will display the plugin output that will be displayed as seen in a report. The synopsis and description will provide more details of the vulnerability being examined. Scrolling down in the "Plugin Description" pane will also show solution

information, additional references if available and the CVSSv2 score that provides a basic risk rating.

At the top of the plugin family tab, you can search for a specific plugin by name or ID. In the box next to “**Filter**”, type in some text to look for and hit enter:

The screenshot shows the 'Add Policy' interface with the 'Plugins' tab selected. A search bar at the top is set to 'windows'. The left sidebar shows 'General', 'Credentials', 'Plugins' (selected), and 'Preferences'. The main area displays 'Families' (DNS, Databases, Denial of Service, FTP, Gentoo Local Security Checks, Peer-To-Peer File Sharing, Policy Compliance, SMTP problems, SNMP) and 'Plugins' (34245, 10312). Below is a 'Plugin Description' section. At the bottom are buttons for 'Enabled Families: 38' and 'Enabled Plugins: 24202', and links for 'Enable All' and 'Disable All'.

When a policy is created and saved, it records all of the plugins that are initially selected. When new plugins are received via a plugin feed update, they will automatically be enabled if the family they are associated with is enabled. If the family has been disabled or partially enabled, new plugins in that family will automatically be disabled as well.



The “Denial of Service” family contains some plugins that could cause outages on a corporate network if the “Safe Checks” option is not enabled, but does contain some useful checks that will not cause any harm. The “Denial of Service” family can be used in conjunction with “Safe Checks” to ensure that any potentially dangerous plugins are not run. However, it is recommended that the “Denial of Service” family not be used on a production network.

Below the window showing the plugins you will find two options that will assist you in selecting plugins.

Option	Description
Enable all	Checks and enables all plugins and their families. This is an easy way to re-enable all plugins after creating a policy with some families or plugins disabled. Note that some plugins may require further configuration options.
Disable all	Un-checks and disables all plugins and their families. Running a scan with all plugins disabled will not produce any results.

Preferences

The “**Preferences**” tab includes means for granular control over scan settings. Selecting an item from the drop-down menu will display further configuration items for the selected category. Note that this is a dynamic list of configuration options that is dependent on the plugin feed, audit policies and additional functionality that the connected Nessus scanner has access to. A scanner with a ProfessionalFeed may have more advanced configuration options available than a scanner configured with the HomeFeed. This list may also change as plugins are added or modified.

“**Database Compliance Checks**” allow ProfessionalFeed customers to upload policy files that will be used to determine if a tested database meets the specified compliance standards. Up to five policies may be selected at one time.

The screenshot shows a software interface titled "Add Policy". On the left, there's a sidebar with tabs: General, Credentials, Plugins, and Preferences, with "Preferences" currently selected. At the top right, there are two tabs: "Plugin" and "Database settings", with "Database settings" selected. The main area contains several input fields and dropdown menus:

- Login : [text input]
- Password : [text input]
- DB Type : Oracle [dropdown menu]
- Database SID : [text input]
- Database port to use : [text input]
- Oracle auth type: NORMAL [dropdown menu]
- SQL Server auth type: Windows [dropdown menu]

The “**Database settings**” options are used to specify the type of database to be tested, relevant settings and credentials:

Option	Description
Login	The username for the database.
Password	The password for the supplied username.
DB Type	Oracle, SQL Server, MySQL, DB2, Informix/DRDA and PostgreSQL are supported.
Database SID	Database system ID to audit.
Database port to use	Port the database listens on.
Oracle auth type	NORMAL, SYSOPER and SYSDBA are supported.
SQL Server auth type	Windows or SQL are supported.

"Do not scan fragile devices" instructs the Nessus scanner not to scan printers or Novell Netware hosts if selected. Since both of these technologies are more prone to denial of service conditions, Nessus can skip scanning them. This is recommended if scanning is performed during business hours.

The screenshot shows the 'Global variable settings' configuration page. At the top, there's a 'Plugin' dropdown menu set to 'Global variable settings'. Below it is a list of configuration options:

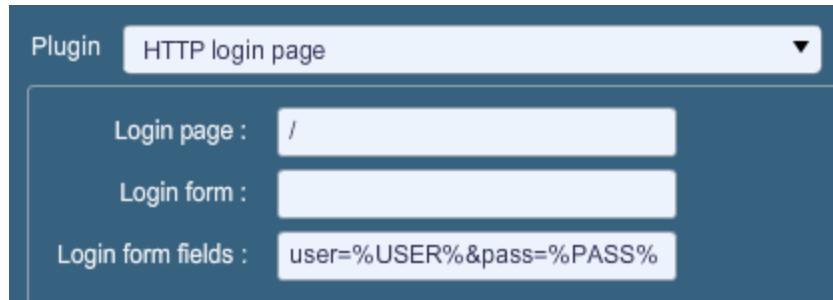
- Probe services on every port**: A checked checkbox.
- Do not log in with user accounts not specified in the policy**: An unchecked checkbox.
- Enable CGI scanning**: An unchecked checkbox.
- Network type**: A dropdown menu set to 'Mixed (use RFC 1918)'.
- Enable experimental scripts**: An unchecked checkbox.
- Thorough tests (slow)**: An unchecked checkbox.
- Report verbosity**: A dropdown menu set to 'Normal'.
- Report paranoia**: A dropdown menu set to 'Normal'.
- Debug level**: An input field containing '0'.
- HTTP User-Agent**: An input field containing 'Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)'.
- SSL certificate to use :** An input field with a 'Browse...' button.
- SSL CA to trust :** An input field with a 'Browse...' button.
- SSL key to use :** An input field with a 'Browse...' button.
- SSL password for SSL key :** An input field.

"Global variable settings" contains a wide variety of configuration options for the Nessus server.

Option	Description
Probe services on every port	Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.
Do not log in with user accounts not specified in the policy	Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.
Enable CGI scanning	Activates CGI checking. Disabling this option will tremendously speed up the audit of a local network.
Network type	Allows you to specify if you are using public routable IPs, private non-internet routable IPs or a mix of these. Select "Mixed" if you are using RFC 1918 addresses and have multiple routers within your network.

Enable experimental scripts	Causes plugins that are considered experimental to be used in the scan. Do not enable this setting while scanning a production network.
	 Tenable does not release scripts flagged "experimental" in either plugin feed.
Thorough tests (slow)	Causes various plugins to "work harder". For example, when looking through SMB file shares, a plugin can analyze 3 levels deep instead of 1. This could cause much more network traffic and analysis in some cases. Note that by being more thorough, the scan will be more intrusive and is more likely to disrupt the network, while potentially having better audit results.
Report verbosity	A higher setting will provide more or less information about plugin activity in the report.
Report paranoia	In some cases, Nessus cannot remotely determine whether a flaw is present or not. If the report paranoia is set to " Paranoid " then a flaw will be reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of " Avoid false alarm " will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. The default option (" Normal ") will be a middle ground between these two settings.
Debug level	Set this option to "1" to enable debugging information in the <code>nessusd.dump</code> log to assist with troubleshooting a Nessus scan.
HTTP User-Agent	Specifies which type of web browser Nessus will impersonate while scanning.
SSL certificate to use	Allows Nessus to use a client side SSL certificate for communicating with a remote host.
SSL CA to trust	Specifies a Certificate Authority (CA) that Nessus will trust.
SSL key to use	Specifies a local SSL key to use for communicating with the remote host.
SSL password for SSL key	The password for managing the SSL key specified.

To facilitate web application testing, Nessus can import HTTP cookies from another piece of software (e.g., web browser, web proxy, etc.) with the "**HTTP cookies import**" settings. A cookie file can be uploaded so that Nessus uses the cookies when attempting to access a web application. The cookie file must be in Netscape format.



The “**HTTP login page**” settings provide control over where authenticated testing of a custom web-based application begins.

Option	Description
Login page	The base URL to the login page of the application.
Login form	The “action” parameter for the form method. For example, the login form for <code><form method="POST" name="auth_form" action="/login.php"></code> would be “/login.php”.
Login form fields	Specify the authentication parameters (e.g., <code>login=%USER%&password=%PASS%</code>). If the keywords %USER% and %PASS% are used, they will be substituted with values supplied on the “Login configurations” drop-down menu.
Re-authenticate delay (seconds)	The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.
Check authentication on page	The URL of a protected web page that requires authentication, to better assist Nessus in determining authentication status.
Follow 30x redirections (# of levels)	If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.
Authenticated regex	A regex pattern to look for on the login page. Simply receiving a 200 response code is not always sufficient to determine session state. Nessus can attempt to match a given string such as “Authentication successful!”
Invert test (disconnected if regex matches)	A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (e.g., “Authentication failed!”)
Match regex on HTTP headers	Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to better determine authentication state.
Case insensitive regex	The regex searches are case sensitive by default. This instructs Nessus to ignore case.

The “**ICCP/COTP TSAP Addressing**” menu deals specifically with SCADA checks. It determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values. The start and stop values are set to “8” by default.

Protocol	Setting
HTTP account	
HTTP password (sent in clear)	
NNTP account	
NNTP password (sent in clear)	
FTP account	anonymous
FTP password (sent in clear)	*****
FTP writeable directory	/incoming
POP2 account	
POP2 password (sent in clear)	
POP3 account	
POP3 password (sent in clear)	
IMAP account	
IMAP password (sent in clear)	

“**Login configurations**” allows the Nessus scanner to use credentials when testing HTTP, NNTP, FTP, POP2, POP3 or IMAP. By supplying credentials, Nessus may have the ability to do more extensive checks to determine vulnerabilities. HTTP credentials supplied here will be used for Basic and Digest authentication only. For configuring credentials for a custom web application, use the “HTTP login page” pull-down menu.

The “**Modbus/TCP Coil Access**” options are available for ProfessionalFeed users. This drop-down menu item is dynamically generated by the SCADA plugins available with the ProfessionalFeed. Modbus uses a function code of 1 to read “coils” in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a “write coil” message. The defaults for this are “0” for the Start reg and “16” for the End reg.

“**Nessus SYN scanner**” and “**Nessus TCP scanner**” options allow you to better tune the native SYN scanner to detect the presence of a firewall.

Value	Description
-------	-------------

Automatic (normal)	This option can help identify if a firewall is located between the scanner and the target (default).
Disabled (softer)	Disables the Firewall detection feature.
Do not detect RST rate limitation (soft)	Disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device.
Ignore closed ports (aggressive)	Will attempt to run plugins even if the port appears to be closed. It is recommended that this option not be used on a production network.

Plugin News Server (NNTP) Information Disclosure ▾

From address :	Nessus <listme@listme.dsbl.org>
Test group name regex :	f[a-z]\.tests?
Max crosspost :	7
Local distribution	<input checked="" type="checkbox"/>
No archive	<input type="checkbox"/>

“News Server (NNTP) Information Disclosure” can be used to determine if there are news servers that are able to relay spam. Nessus will attempt to post a news message to a NNTP (Network News Transport Protocol) server(s), and can test if it is possible to post a message to upstream news servers as well.

Option	Description
From address	The address that Nessus will use as it attempts to post a message to the news server(s). This message will delete itself automatically after a short period of time.
Test group name regex	The name of the news group(s) that will receive a test message from the specified address. The name can be specified as a regular expression (regex) so that the message can be posted to multiple news groups simultaneously. For example, the default value “f[a-z]\.tests?” will broadcast a mail message to all news groups with names that begin with any letter (from “a” to “z”) and end with “.tests” (or some variation that matched the string). The question mark acts as an optional wildcard.
Max crosspost	The maximum number of news servers that will receive the test posting, regardless of the number of name matches. For example, if the Max crosspost is “7”, the test message will

	only be sent to seven news servers, even if there are 2000 news servers that match the regex in this field.
Local distribution	If this option is selected, Nessus will only attempt to post a message to the local news server(s). Otherwise, an attempt will be made to forward the message upstream.
No archive	If this option is selected, Nessus will request to not archive the test message being sent to the news server(s). Otherwise, the message will be archived like any other posting.

“PCI DSS Compliance” will have Nessus compare the scan results to current PCI DSS compliance standards. This feature is only available to ProfessionalFeed customers.

The screenshot shows the 'Ping the remote host' configuration dialog. At the top, it says 'Plugin' and 'Ping the remote host'. Below that, it says 'TCP ping destination port(s) : built-in'. There are several checkboxes with their status indicated by checked or unchecked boxes:

- Do an ARP ping:
- Do a TCP ping:
- Do an ICMP ping:
- Number of retries (ICMP):
- Do an applicative UDP ping (DNS,RPC...):
- Make the dead hosts appear in the report:
- Log live hosts in the report:
- Test the local Nessus host:
- Fast network discovery:

“Ping the remote host” options allow for granular control over Nessus’ ability to ping hosts during discovery scanning. This can be done via ARP ping, TCP ping, ICMP ping or applicative UDP ping.

Option	Description
TCP ping destination port(s)	Specifies the list of ports that will be checked via TCP ping. If you are not sure of the ports, leave this setting to the default of “built-in”.
Number of Retries (ICMP)”	Allows you to specify the number of attempts to try to ping the remote host. The default is set to 6.
Do an applicative UDP	Perform a UDP ping against specific UDP-based applications

ping (DNS, RPC...)	including DNS (port 53), RPC (port 111), NTP (port 123) and RIP (port 520).
Make the dead hosts appear in the report	If this option is selected, hosts that did not reply to the ping request will be included in the security report as dead hosts.
Log live hosts in the report	Select this option to specifically report on the ability to successfully ping a remote host.
Test the local Nessus host	This option allows you to include or exclude the local Nessus host from the scan. This is used when the Nessus host falls within the target network range for the scan.
Fast network discovery	By default, when Nessus “pings” a remote IP and receives a reply, it performs extra checks to make sure that it is not a transparent proxy or a load balancer that would return noise but no result (some devices answer to every port 1-65535 but there is no service behind). Such checks can take some time, especially if the remote host is firewalled. If the “fast network discovery” option is enabled, Nessus will not perform these checks.

“**Port scanner settings**” provide two options for further controlling port scanning activity.

Option	Description
Check open TCP ports found by local port enumerators	If a local port enumerator (e.g., WMI or netstat) finds a port, Nessus will also verify it is open remotely. This helps determine if some form of access control is being used (e.g., TCP wrappers, firewall).
Only run network port scanners if local port enumeration failed	Otherwise, rely on local port enumeration first.

“**SMB Registry: Start the Registry Service during the scan**” enables the service to facilitate some of the scanning requirements for machines that may not have the SMB Registry running all the time.

Under the “**SMB Scope**” menu, if the option “**Request information about the domain**” is set, then domain users will be queried instead of local users.

“**SMB use domain SID to enumerate users**” specifies the SID range to use to perform a reverse lookup on usernames on the domain. The default setting is recommended for most scans.

“**SMB use host SID to enumerate local users**” specifies the SID range to use to perform a reverse lookup on local usernames. The default setting is recommended.

Plugin SMTP settings

Third party domain :	example.com
From address :	nobody@example.com
To address :	postmaster@[AUTO_REPLACED_IP]

“SMTP settings” specify options for SMTP (Simple Mail Transport Protocol) tests that run on all devices within the scanned domain that are running SMTP services. Nessus will attempt to relay messages through the device to the specified “**Third party domain**”. If the message sent to the “**Third party domain**” is rejected by the address specified in the “**To address**” field, the spam attempt failed. If the message is accepted, then the SMTP server was successfully used to relay spam.

Option	Description
Third party domain	Nessus will attempt to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test might be aborted by the SMTP server.
From address	The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this field.
To address	Nessus will attempt to send messages addressed to the mail recipient listed in this field. The postmaster address is the default value since it is a valid address on most mail servers.

Plugin SNMP settings

Community name :	public
UDP port :	161
SNMPv3 user name :	
SNMPv3 authentication password :	
SNMPv3 authentication algorithm :	MD5
SNMPv3 privacy password :	
SNMPv3 privacy algorithm :	DES

“SNMP settings” allow you to configure Nessus to connect and authenticate to the SNMP service of the target. During the course of scanning, Nessus will make some attempts to

guess the community string and use it for subsequent tests. If Nessus is unable to guess the community string and/or password, it may not perform a full audit against the service.

Option	Description
Community name	The SNMP community name.
UDP port	Direct Nessus to scan a different port should SNMP be running on a port other than 161.
SNMPv3 user name	The username for a SNMPv3 based account.
SNMPv3 authentication password	The password for the username specified.
SNMPv3 authentication algorithm	Select MD5 or SHA1 based on which algorithm the remote service supports.
SNMPv3 privacy password	A password used to protect encrypted SNMP communication.
SNMPv3 privacy algorithm	The encryption algorithm to use for SNMP traffic.

“Service Detection” controls how Nessus will test SSL based services; known SSL ports (e.g., 443), all ports or none. Testing for SSL capability on all ports may be disruptive for the tested host.

“Unix Compliance Checks” allow ProfessionalFeed customers to upload Unix audit files that will be used to determine if a tested system meets the specified compliance standards. Up to five policies may be selected at one time.

The screenshot shows a configuration interface for 'Web Application Tests Settings'. At the top, there's a header bar with 'Plugin' and 'Web Application Tests Settings'. Below the header, there are several configuration options:

- Enable web applications tests:** A checkbox that is checked.
- Maximum run time (min):** A text input field containing '60'.
- Send POST requests:** A checkbox that is unchecked.
- Combinations of arguments values:** A dropdown menu set to 'one value'.
- HTTP Parameter Pollution:** A checkbox that is unchecked.
- Stop at first flaw:** A dropdown menu set to 'per port (quicker)'.
- Test embedded web servers:** A checkbox that is unchecked.
- URL for Remote File Inclusion :** A text input field containing 'http://rfi.nessus.org/rfi.txt'.

"Web Application Tests Settings" tests the arguments of the remote CGIs (Common Gateway Interface) discovered in the web mirroring process by attempting to pass common CGI programming errors such as cross-site scripting, remote file inclusion, command execution, traversal attacks or SQL injection. Enable this option by selecting the "Enable web applications tests" checkbox. These tests are dependent on the following NASL plugins:

- [11139](#) – SQL Injection (CGI abuses)
- [39465](#) – Command Execution (CGI abuses)
- [39466](#) – Cross-Site Scripting (CGI abuses: XSS)
- [39467](#) – Directory Traversal (CGI abuses)
- [39468](#) – HTTP Header Injection (CGI abuses: XSS)
- [39469](#) – Remote File Inclusion (CGI abuses)

Option	Description
Maximum run time (min)	This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given web site. Scanning the local network for web sites with small applications will typically complete in under an hour, however web sites with large applications may require a higher value.
Send POST requests	"POST requests" tests are used for enhanced web form testing. By default, the web application tests will only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required.
Combinations of arguments values	<p>This option manages the combination of argument values used in the HTTP requests. This dropdown has three options:</p> <p>one value – This tests one parameter at a time with an attack string, without trying "non-attack" variations for additional parameters. For example, Nessus would attempt "/test.php?arg1=XSS&b=1&c=1" where "b" and "c" allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated.</p> <p>All pairs (slower but efficient) – This form of testing is slightly slower but more efficient than the "one value" test. While testing multiple parameters, it will test an attack string, variations for a single variable and then use the first value for all other variables. For example, Nessus would attempt "/test.php?a=XSS&b=1&c=1&d=1" and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for "/test.php?a=XSS&b=3&c=3&d=3" when the first value of each</p>

	<p>variable is "1".</p> <p>All combinations (extremely slow) – This method of testing will do a fully exhaustive test of all possible combinations of attack strings with valid input to variables. Where "All-pairs" testing seeks to create a smaller data set as a tradeoff for speed, "all combinations" makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.</p>
HTTP Parameter Pollution	<p>When performing web application tests, attempt to bypass any filtering mechanisms by injecting content into a variable while supplying the same variable with valid content as well. For example, a normal SQL injection test may look like "/target.cgi?a=' &b=2". With HTTP Parameter Pollution (HPP) enabled, the request may look like "/target.cgi?a=' &a=1&b=2".</p>
Stop at first flaw	<p>This option determines when a new flaw is targeted. The dropdown has four options:</p> <p>per CGI – As soon as a flaw is found on a CGI by a script, Nessus switches to the next known CGI on the same server, or if there is no other CGI, to the next port/server. This is the default option.</p> <p>per port (quicker) – As soon as a flaw is found on a web server by a script, Nessus stops and switches to another web server on a different port. This applies at the script level; finding an XSS flaw will not disable searching for SQL injection or header injection, but you will have at most one report for each type on a given port, unless "thorough tests" is set. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported sometimes, if they were caught by the same attack.</p> <p>per parameter (slow) – As soon as one type of flaw is found in a parameter of a CGI (e.g., XSS), Nessus switches to the next parameter of the same CGI, or the next known CGI, or to the next port/server.</p> <p>look for all flaws (slower) – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommended in most cases.</p>
Test Embedded web servers	<p>Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.</p>

URL for Remote File Inclusion	During Remote File Inclusion (RFI) testing, this option specifies a file on a remote host to use for tests. By default, Nessus will use a safe file hosted on Tenable's web server for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing.
--------------------------------------	---

The screenshot shows the Nessus configuration interface with the 'Web mirroring' plugin selected. The configuration options are as follows:

- Number of pages to mirror: 1000
- Maximum depth: 6
- Start page: /
- Excluded items regex: /server_privileges\.php
- Follow dynamic pages:

"Web Mirroring" sets configuration parameters for Nessus' native web server content mirroring utility. Nessus will mirror web content to better analyze the contents for vulnerabilities and help minimize the impact on the server.

Option	Description
Number of pages to mirror	The maximum number of pages to mirror.
Maximum depth	Limit the number of links Nessus will follow for each start page.
Start page	The URL of the first page that will be tested. If multiple pages are required, use a colon delimiter to separate them (e.g., "/:/php4:/base").
Excluded items regex	Enable exclusion of portions of the web site from being crawled. For example, to exclude the "/manual" directory and all Perl CGI, set this field to: <code>(^/manual) (\.pl(\?.*)? \$)</code> .
Follow dynamic pages	If selected, Nessus will follow dynamic links and may exceed the parameters set above.

"Windows Compliance Checks" allow ProfessionalFeed customers to upload Microsoft Windows configuration audit files that will be used to determine if a tested system meets the specified compliance standards. Up to five policies may be selected at one time.

"Windows File Contents Compliance Checks" allows ProfessionalFeed customers to upload Windows-based audit files that search a system for a specific type of content (e.g.,

credit cards, Social Security Numbers) to help determine compliance with corporate regulations or third-party standards.

When all of the options have been configured as desired, click on “**Submit**” to save the policy and return to the Policies tab. At any time, you can click on “**Edit**” to make changes to a policy you have already created or click on “**Delete**” to remove a policy completely.

Importing and Copying Policies

The “**Import**” button on the upper right menu bar will allow you to upload previously created policies to the scanner. Using the “**Browse...**” dialog box, select the policy from your local system and click on “**Submit**”.

If you want to create a policy similar to an existing policy with minor modifications, you can select the base policy in the list and click on “**Copy**” on the upper right menu bar. This will create a copy of the original policy that can be edited to make any required modifications. This is useful for creating standard policies with minor changes as required for a given environment.

Creating and Launching a Scan

After creating a policy, you can create a new scan by clicking on the “**Scans**” option on the menu bar at the top and then click on the “**+ Add**” button on the right. The “**Add Scan**” screen will be displayed as follows:

The screenshot shows the Nessus interface with the title bar "Nessus". The menu bar includes "Scans", "Reports", "Scans", "Policies", and "Users". A modal dialog box titled "Add Scan" is open. It contains the following fields:

- Name: An input field.
- Type: A dropdown menu set to "Run Now".
- Policy: A dropdown menu set to "Please select a scan policy".
- Scan Targets: A large text area for entering target information.
- Targets File: An input field with a "Browse..." button.

There are five fields to enter the scan target:

- **Name** – Sets the name that will be displayed in the Nessus UI to identify the scan.
- **Type** – Choose between “Run Now” (immediately execute the scan after submitting) or “Template” (save as a template for repeat scanning).
- **Policy** – Select a previously created policy that the scan will use to set parameters controlling Nessus server scanning behavior.

- **Scan Targets** – Targets can be entered by single IP address (e.g., 192.168.0.1), IP range (e.g., 192.168.0.1-192.168.0.255), subnet with CIDR notation (e.g., 192.168.0.0/24) or resolvable host (e.g., www.nessus.org).
- **Targets File** – A text file with a list of hosts can be imported by clicking on “**Browse...**” and selecting a file from the local machine.



The host file must be formatted as ASCII text with one host per line and no extra spaces or lines. Unicode/UTF-8 encoding is not supported.

Example host file formats:

Individual hosts:

```
192.168.0.100
192.168.0.101
192.168.0.102
```

Host range:

```
192.168.0.100-192.168.0.102
```

Host CIDR block:

```
192.168.0.1/24
```

After you have entered the scan information, click on “**Submit**”. After submitting, the scan will begin immediately before the display is returned to the general “**Scans**” page.

Name	Owner	Status	Start Time
HR Subnet	admin	41 IPs / 509 IPs	Nov 22, 2009 21:54
Linux Boxes	admin	0 IPs / 1 IPs	Nov 22, 2009 21:55

Once a scan has launched, the Scans list will display a list of all scans currently running or paused along with basic information about the scan. After selecting a particular scan on the list, the action buttons on the top right allow you to “**Browse**” the results of the scan in progress, “**Pause**” and “**Resume**” the scan or “**Stop**” the scan completely.

When a scan has completed, it will be removed from the “**Scans**” list and be available for review on the “**Reports**” tab.

If a scan is saved as a template, it will appear in the scan list as such and wait to be launched.

Name	Owner	Status	Start Time
Payment Network	admin	Template	Never

Reports

With the release of Nessus 4.2, report stylesheets have been better integrated into the reporting system. By using the report filters and export features, users can create dynamic reports of their own choosing instead of selecting from a specific list. In addition, stylesheet support has been enhanced so that updates or the addition of a stylesheet can be performed through the plugin feed. This will allow Tenable to release additional stylesheets without requiring an upgrade or major release.

Clicking on the “**Reports**” tab on the menu bar at the top of the interface will bring up the list of running and completed scans:

Name	Status	Last Updated
Dev Subnet	Completed	Nov 3, 2009 24:35
HR Subnet	Running	Nov 3, 2009 24:38
Local Desktop	Completed	Nov 3, 2009 24:40

The “Reports” screen acts as a central point for viewing, comparing, uploading and downloading scan results.

Browse

To browse the results of a scan, select a name from the “Reports” list and click on “**Browse**”. This allows you to view results by navigating through hosts, ports and then specific vulnerabilities. The first summary screen shows each host scanned along with a breakdown of vulnerabilities and open ports:

With a host selected, the report will be segregated by port number and display associated information such as the protocol and service name, as well as a summary of vulnerabilities categorized by risk severity. As you navigate through the scan results, the user interface will maintain the list of hosts as well as a series of clickable arrows to assist in quick navigation to a specific component of the report:

Report Info		LAN Scan → 192.168.0.10					6 results
Hosts	Port	Protocol	SVC Name	Total	High	Medium	Low
192.168.0.1	0	tcp	general	7	0	0	7
192.168.0.10	0	udp	general	1	0	0	1
192.168.0.20	137	udp	netbios-ns	1	0	0	1
192.168.0.100	139	tcp	smb	1	0	0	1
	445	tcp	cifs	13	1	1	11
	2869	tcp	www	3	0	0	3

Selecting a port will display all of the vulnerability findings associated with the port and service:

LAN Scan		192.168.0.10	445 / tcp	List	Detail	13 results
Plugin ID	Name			Port	Severity	
11011	SMB Detection			cifs (445/tcp)	Low	
10785	SMB NativeLanMan			cifs (445/tcp)	Low	
10394	SMB log in			cifs (445/tcp)	Low	
10859	SMB get host SID			cifs (445/tcp)	Low	
10860	SMB use host SID to enumerate local users			cifs (445/tcp)	Low	
10395	SMB shares enumeration			cifs (445/tcp)	Low	
26919	SMB guest account for all users			cifs (445/tcp)	Medium	
10397	SMB LanMan Pipe Server browse listing			cifs (445/tcp)	Low	
10396	Microsoft Windows SMB Shares Access			cifs (445/tcp)	High	
23974	SMB Share Hosting Office Files			cifs (445/tcp)	Low	
10400	SMB accessible registry			cifs (445/tcp)	Low	
10428	SMB fully accessible registry			cifs (445/tcp)	Low	
26920	SMB NULL session			cifs (445/tcp)	Low	

In the example above, we see that host 192.168.0.10 has 13 vulnerabilities associated with TCP port 445 (CIFS or Common Internet File System). The summary of findings displays the Nessus Plugin ID, vulnerability name, port, protocol and severity. By clicking once on any column heading, the results can be sorted by the column's content. Clicking a second time will reverse sort the results:

LAN Scan		192.168.0.10	445 / tcp	List	Detail	13 results
Plugin ID	Name			Port	Severity	▼
10396	Microsoft Windows SMB Shares Access			cifs (445/tcp)	High	
26919	SMB guest account for all users			cifs (445/tcp)	Medium	
10397	SMB LanMan Pipe Server browse listing			cifs (445/tcp)	Low	
10859	SMB get host SID			cifs (445/tcp)	Low	
10860	SMB use host SID to enumerate local users			cifs (445/tcp)	Low	
10395	SMB shares enumeration			cifs (445/tcp)	Low	
11011	SMB Detection			cifs (445/tcp)	Low	
10394	SMB log in			cifs (445/tcp)	Low	
10785	SMB NativeLanMan			cifs (445/tcp)	Low	
23974	SMB Share Hosting Office Files			cifs (445/tcp)	Low	
10400	SMB accessible registry			cifs (445/tcp)	Low	
10428	SMB fully accessible registry			cifs (445/tcp)	Low	
26920	SMB NULL session			cifs (445/tcp)	Low	

Selecting a vulnerability from the list will display full details of the finding including a technical description, references, solution, detailed risk factor and any relevant output demonstrating the finding:

LAN Scan → 192.168.0.10 → 445 / tcp

Plugin ID: 10396 **Port / Service:** cifs (445/tcp) **Severity:** High

Plugin Name: Microsoft Windows SMB Shares Access

Synopsis :

It is possible to access a network share.

Description :

The remote has one or many Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read/write confidential data.

Solution :

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

Plugin Output :

The following shares can be accessed as nessus881253350738475614771646133 :

- software - (readable,writable)

← →

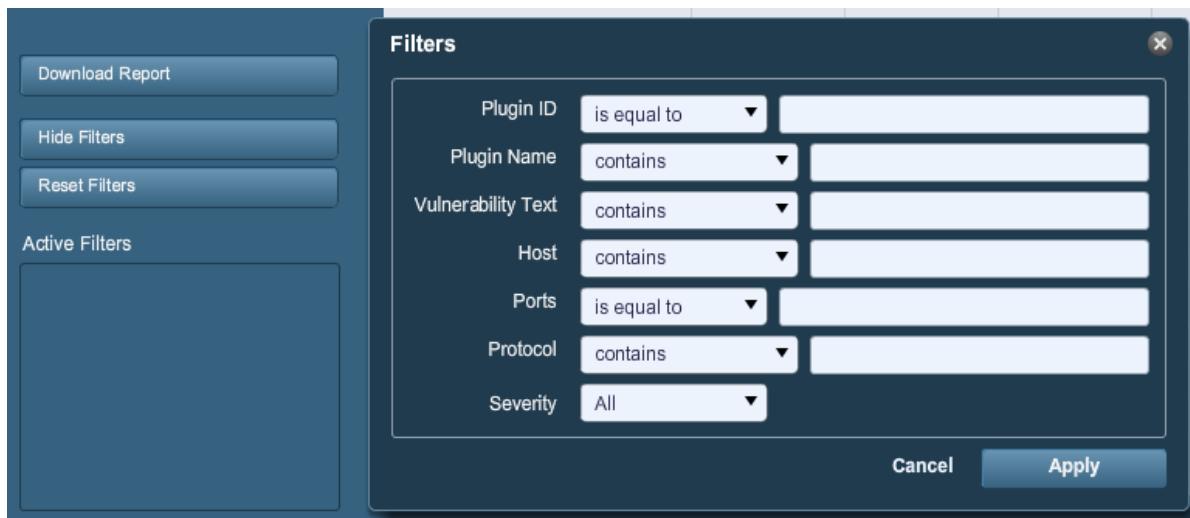
The vulnerability detail screen provides several methods for navigating around the report:

- The arrow keys at the top can be selected to jump back to a port, host or scan overview.
- The “**List**” and “**Detail**” buttons alternate between vulnerability detail and the last list view (e.g., in the example above, the vulnerabilities associated with port 445).
- The grey arrows to the left or right will cycle through the other vulnerabilities associated with the port selected.
- The bar of buttons at the bottom provides a way to jump to a specific vulnerability in the list based on risk severity. In the example above, the medium and high-risk vulnerabilities stand out.

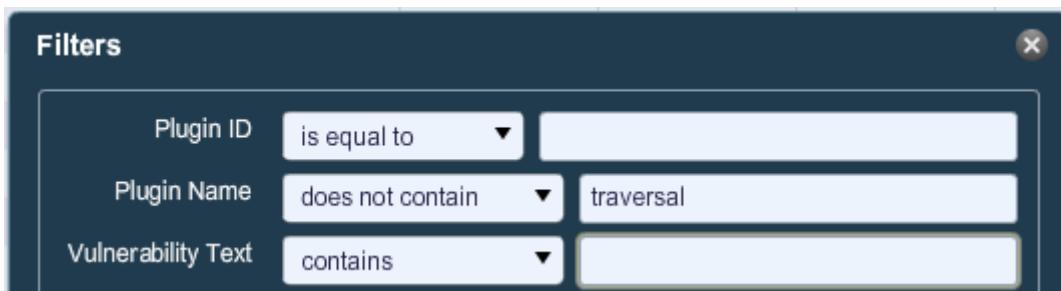
Report Filters

Nessus offers a flexible system of filters to assist in displaying specific report results. Filters can be used to display results based on any aspect of the vulnerability findings. When multiple filters are used, more detailed and customized report views can be created.

To create a filter, begin by clicking on “**Show Filters**” on the left side of the screen. Filters can be created from the report summary, host or port level breakdown screens.



A filter is created by selecting the field, a filter argument and a value to filter on:



The report filters allow for a wide variety of criteria:

Option	Description
Plugin ID	Filter results if Plugin ID “ <i>is equal to</i> ” or “ <i>is not equal to</i> ” a given number (e.g., 42111).
Plugin Name	Filter results if Plugin Name “ <i>contains</i> ”, “ <i>does not contain</i> ”, “ <i>starts with</i> ” or “ <i>does not start with</i> ” a given string (e.g., “Microsoft Windows”).
Vulnerability Text	Filter results if the plugin output “ <i>contains</i> ”, “ <i>does not contain</i> ”, “ <i>starts with</i> ” or “ <i>does not start with</i> ” a given string (e.g., “denial of service”).
Host	Filter results if the host “ <i>contains</i> ”, “ <i>does not contain</i> ”, “ <i>starts with</i> ”, “ <i>does not start with</i> ”, “ <i>is equal to</i> ” or “ <i>is not equal to</i> ” a given string (e.g., 192.168).
Ports	Filter results based on if a port “ <i>is equal to</i> ” or “ <i>is not equal to</i> ” a given number (e.g., 443).
Protocol	Filter results if a protocol “ <i>contains</i> ”, “ <i>does not contain</i> ”,

	"starts with" or "does not start with" a given string (e.g., http).
Severity	Filter results based on the risk severity: "Low", "Medium" or "High".

When using a filter, the string or numeric value can be comma delimited to filter based on multiple strings. For example, to filter results to show only web servers, you could create a "Ports" filter, select "is equal to" and input "80,443,8000,8080". This will show you results associated with those four ports.



Filter criteria are **not** case sensitive.

As filters are created, they will be listed on the left. To see the active filter details, mouse over the filter name:



As soon as a filter is created, the scan results will be updated to reflect the new filter criteria. In the example below, creating a filter to only display results with "Microsoft" in the plugin name removes most findings:

LAN Scan

4 results

Host	Total	High	Medium	Low	Open Port
192.168.0.1	17	0	1	14	2
192.168.0.10	29	1	1	24	3
192.168.0.20	29	1	1	24	3
192.168.0.100	18	0	2	14	2

Filters

Plugin ID: is equal to

Plugin Name: contains microsoft

Vulnerability Text: contains

Host: contains

Ports: is equal to

Protocol: contains

Severity: All

After the filter has been applied:

Report Info

Name: LAN Scan
Last Update: Nov 5, 2009 23:01
Status: Completed

Active Filters

Plugin Name

LAN Scan

2 results

Host	Total	High	Medium	Low	Open Port
192.168.0.10	1	1	0	0	0
192.168.0.20	1	1	0	0	0

Once the results have been filtered to provide the data set you want, you can click on “**Download Report**” to export just the filtered results.

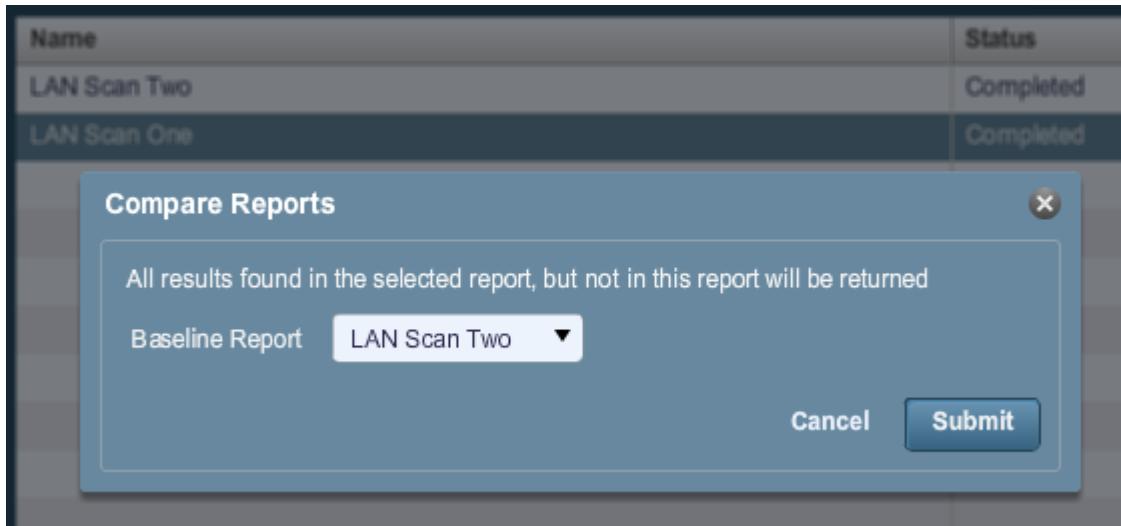
Compare



The “Compare” function is only available for ProfessionalFeed users.

With Nessus 4.2, you can compare two scan reports against each other to display differences. The ability to show scan differentials helps to point out how a given system or network has changed over time. This helps in analysis of compliance by showing how vulnerabilities are being remediated, if systems are patched as new vulnerabilities are found or how two scans may not be targeting the same hosts.

To compare reports, begin by selecting a scan from the “**Reports**” list and click on “**Compare**” from the menu bar on the right. The resulting dialog menu will give you a drop-down list of other reports to compare. Select one and click on “**Submit**”:



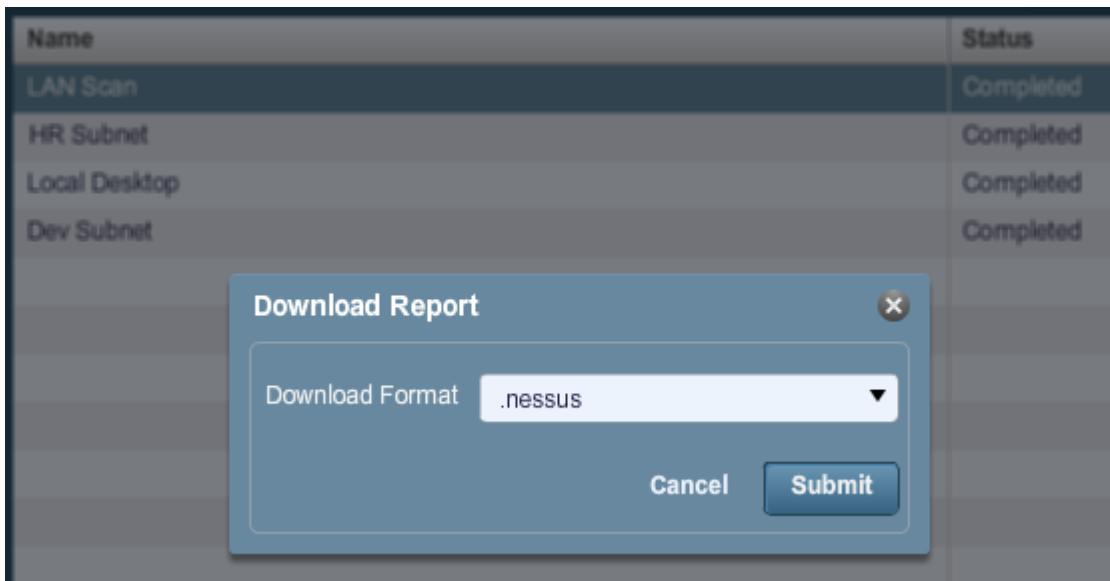
Nessus will compare the two reports and produce a list of results that are not found in both reports. These results are the scan differential and highlight what vulnerabilities have been found or remediated between the two scans. In the example above, “LAN Scan One” is a scan of the entire 192.168.0.0/24 subnet and “LAN Scan Two” is a scan of three select hosts on the 192.168.0.0/24 subnet. The “Compare” feature displays the differences, highlighting hosts that were not scanned in “LAN Scan Two”:

Report Info		Comparison Report						2 results
		Host	Total	High	Medium	Low	Open Port	
New Report	Name: LAN Scan One Last Update: Nov 12, 2009 22:57	192.168.0.2	43	0	1	31	11	
Baseline Report	Name: LAN Scan Two Last Update: Nov 12, 2009 23:05	192.168.0.100	19	0	2	15	2	

Upload & Download

Scan results can be exported from one scanner and imported to a different scanner. The “**Upload**” and “**Download**” features facilitate better scan management, report comparison, report backup and communication between groups or organizations within a company.

To export a scan, begin by selecting it from the “**Reports**” screen and clicking on “**Download**”. This will display the report download dialog box:



Reports can be downloaded in any one of four formats:

Option	Description
.nessus	An XML-based format and the de-facto standard in Nessus 4.2. This format uses an expanded set of XML tags to make extracting and parsing information more granular.
.nessus (v1)	An XML-based format used in Nessus 3.2 through 4.0.2, compatible with Nessus 4.2 and Security Center 3.
HTML export	A report generated using standard HTML, viewable in any web browser.
NBE export	A comma-separated value (CSV) based export that can be used to import into many external programs.

After selecting the format, your standard web browser “Save File” dialog will be displayed allowing you to save the scan results to the location of your choice.

To import a scan, click on the “**Upload**” button from the “**Reports**” screen:

Name	Status
LAN Scan	Completed
HR Subnet	Completed
Local Desktop	Completed
Dev Subnet	Completed

Upload Report

Report File

Using the “**Browse...**” button, select the **.nessus** scan file you want to import and click on “**Submit**”. Nessus will parse the information and make it available in the “**Reports**” interface.

.nessus File Format

Nessus uses a specific file format (**.nessus**) for scan export and import. This format has the following advantages:

- XML based, for easy forward and backward compatibility and easy implementation.
- Self-sufficient: a single **.nessus** file contains the list of targets, the policies defined by the user as well as the scan results themselves.
- Secure: Passwords are not saved in the file. Instead, a reference to a password stored in a secure location on the local host is used.

The process to create a **.nessus** file that contains the targets, policies and scan results is to first generate the policy and save it. Next, generate the list of target addresses and finally, run a scan. Once the scan is complete, all the information can be saved in a **.nessus** file by using the “**Download**” option from the “**Reports**” tab. Please see the “Nessus File Format” document for more details on **.nessus** files.

Delete

Once you are finished with scan results, you can select a scan from the “Reports” list and click on the “**Delete**” button. This will delete the scan from the user interface. **This action cannot be undone!** Use the “**Download**” feature to export your scan results before deleting.

Users

Name	Username	Role	Last Login
admin	admin	Administrator	Nov 20, 2009 24:49
figlet	figlet	User	Never Logged In

The “**Users**” tab provides an interface for Nessus scanner user management. New users can be added via the Nessus Server Manager (Mac OS X/Windows), `nessus-adduser` command (*nix) or via the user interface (all platforms). To create a new user via the Nessus user interface, click on “**Add**” on the top right menu. This will prompt you for the username, password and the option to make the user an administrator of the Nessus scanner:

Username	biscuit
Password	*****
Confirm Password	*****
Administrator	<input checked="" type="checkbox"/>

To edit or delete a user, select the username from the “**Users**” list and click on “**Edit**” or “**Delete**” on the top right menu as needed.

Other Nessus Clients

In addition to the Nessus GUI, Tenable supports two other methods for communicating with the Nessus server: the Unix command line interface and the SecurityCenter.

Unix Command Line Interface

The command line interface (CLI) is available with the Nessus server. To run a scan using command line operation, you must run the scan in batch mode using the following command syntax:

```
# /opt/nessus/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>
```

Batch mode scanning using the CLI on Windows can be done using the `nessus.exe` program.

The table below explains the various arguments used to run a scan in batch mode.

Argument	Description
----------	-------------

-q	Batch-mode. Run the Nessus scan non-interactively.
-p	Obtain a list of the plugins installed on the server.
-P	Obtain a list of the server and plugin preferences.
-s	Issue SQL output for -p and -P .
<host>	The nessusd host to connect to.
<port>	The port to which you will connect to on the remote nessusd host.
<user>	The user name to connect to nessusd with.
<password>	The password associated with user name.
<targets-file>	The name of the file containing the target machines to be scanned.
<results-file>	The name of the file where the results will be stored at the completion of the scan.

There are other options that are also available when running a scan in batch mode. These are explained in the following table.

Option	Description
-v	Make the batch mode display status messages to the screen.
-x	Do not check SSL certificates.
-v	Version. Display the version number and exit.
-h	Help. Show a summary of the commands and exit.
-T <type>	Save the data as <type> , where <type> can be "nbe", "html", "nessus" or "text".

Converting a Report

You can use Nessus to perform a conversion between report formats. Nessus can take any NBE report and change it into HTML, text or **.nessus** format.

Use the following command to convert a report:

```
# /opt/nessus/bin/nessus -i in.nbe -o out.[html|txt|nessus]
```

The option **-i** specifies the NBE file that is being converted. The option **-o** specifies the file name and type that the report will be converted to, which can be HTML, text or **.nessus** format.

Reports contained in **.nessus** files may also be converted to HTML from the command line. The syntax for this is as follows:

```
# /opt/nessus/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html
```

The **--dot-nessus** parameter indicates the **.nessus** input file is to be used. **<ReportName>** is the name of the report as it appears within the input **.nessus** file.

Command Line using **.nessus** Files

There are several arguments that may be passed to permit working with **.nessus** files as either input or output from the command line. These are detailed in the following table:

Argument	Description
--dot-nessus <file>	When used, this is always provided as the first parameter passed to the nessus binary to indicate that a .nessus file will be used. <file> is the location and name of the .nessus file to be used.
--policy-name <policy>	The name of a policy contained in the designated .nessus file. The policy parameter is provided when launching a scan from the command line. Note that the policy name provided must be the exact policy name, including single quotes, as what is displayed when using the " --list-policies " parameter (see below).
--list-policies	Provide the names of all scan policies contained in the designated .nessus file.
--list-reports	Provide the names of all reports contained in the designated .nessus file.
--target-file <file>	Over-ride the targets provided in the designated .nessus file and use those contained in the specified file.

The following command will display a list of all reports contained in the file "**scan.nessus**":

```
# /opt/nessus/bin/nessus --dot-nessus scan.nessus --list-reports
```

Following is example output:

```
List of reports contained in scan.nessus:  
- '08/03/10 11:19:55 AM - Full Safe w/ Compliance'  
- '08/03/10 01:01:01 PM - Full Safe w/ Compliance'  
- '08/03/10 01:32:10 PM - Full Safe w/ Compliance'
```

```
- '08/03/10 02:13:01 PM - Full Safe w/ Compliance'  
- '08/03/10 02:45:00 PM - Full Safe w/ Compliance'
```

The following command will display a list of all policies contained in the file "scan.nessus":

```
# /opt/nessus/bin/nessus --dot-nessus scan.nessus --list-policies
```

Sample output of this command is shown below:

```
List of policies contained in scan.nessus:  
- 'Full Safe w/ Compliance'
```

Note that when the report or policy names are to be passed as parameters to command-line Nessus, the name must be passed exactly as displayed from the above commands, including the single-quotes ('Safe w/ Compliance').

Scan Command

Assuming the policy noted in the above example exists, a scan can be launched with the following settings:

```
# /opt/nessus/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/  
Compliance' <host> <port> <user> <password> <results-file>
```

In the above example, the **<host>**, **<port>**, **<user>**, **<password>** and **<results-file>** parameters are provided as documented above. A **<targets-file>** is not required as the targets contained in the **.nessus** file are used for the scan.

The format for the report that is generated will be decided based on the file extension provided in the **nessus** command. In the command above, if the name provided for the **<results-file>** parameter was "**report.nbe**", then the report would be in **.nbe** format. Had the name been "**report.nessus**", the report would have been in **.nessus** format.

Had nothing been provided for the **<results-file>** parameter, then the report would have been added to the **scan.nessus** file.

SecurityCenter

Configuring the SecurityCenter

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

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

Add Scanner

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

Cancel **Submit**

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

Nessus Scanners

Success: Nessus Scanner "Local Scanner" was successfully added. **Close**

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

Add **Edit** **Details** **Delete**

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

About Tenable Network Security

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

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