

Nessus 6.4 User Guide

July 7, 2015

(Revision 2)

Table of Contents

Introduction	6
Standards and Conventions.....	6
Official Nessus Product Names.....	6
New in Nessus 6.4	6
Overview	7
Installation.....	7
Nessus User Interface (UI)	7
Supported Platforms.....	7
Connecting to Nessus	8
Security Warnings	8
Bypassing the SSL Warning	9
Nessus Top Navigation.....	9
User Profile Settings & Options	10
User Profile Account Settings	10
Change Password	11
Plugin Rules.....	11
API Keys	12
API Keys Warnings	12
Nessus General Settings	12
Scanners.....	13
Accounts.....	14
Communication	14
Advanced	16
Scans and Policies.....	16
Scan Library and Policy Library	16
Scanner Templates.....	17
Compliance Specific Templates	18
Mobile Device Specific Template	18
PCI Auditing Specific Templates.....	19
SCAP and OVAL Auditing Specific Template.....	19
Agent Templates	20
Scans.....	20
Scan Statuses.....	21
Create a New Scan Folder	21

Create a New Scan.....	22
Scan > Settings (Basic Network Scan Example)	22
Basic	23
Discovery	26
Assessment	33
Report	43
Advanced	45
Scan > Credentials (Basic Network Scan Example)	46
Cloud Services	48
Database	51
Host	53
Miscellaneous	68
Mobile	72
Patch Management	75
Plaintext Authentication	90
Scan > Compliance (Advanced Scan Example)	93
Example: (Upload a custom Brocade FabricOS audit file)	96
Example: TNS Brocade Fabric OS Best Practices	97
Offline Configuration Audit Policies	97
Scan > Plugins (Advanced Scan Example)	98
Manage Scans	100
Upload a Scan	101
Configure a Scan	101
Disable a Scheduled Scan	102
Copy a Scan	102
Move a Scan	103
Scan Results, Dashboards, and Reports	103
Scan Results	104
Dashboards	104
Compliance Results	111
Report Filters	112
Report Screenshots	117
Scan Knowledge Base	118
Compare the Results (Diff)	118
Managing Reports	120
HTML and PDF Customization	122



Nessus File Formats.....	123
Deleting Scan Results.....	124
Policies.....	124
Create a New Policy.....	125
Scan > Settings (Basic Network Scan Policy Example)	125
Basic	125
Shared Template Pages and Settings.....	126
Manage Policies.....	126
Upload a Policy.....	127
More Options.....	127
Download a Policy.....	128
Copy a Policy	128
Delete a Policy.....	128
Nessus Cloud & PCI ASV Validation.....	128
Submitting Scan Results for PCI Customer Review.....	130
Customer Review Interface	131
Reviewing Scan Results.....	132
Disputing Scan Results.....	134
Submitting Attachments as Evidence for a Dispute.....	135
Submitting a Scan Report for Tenable Review.....	137
PCI ASV Report Formats.....	139
Additional Resources.....	143
About Tenable Network Security	144
Appendix A – Setting up Credentialed Checks on Windows Platforms	145
Prerequisites	145
User Privileges	145
Enabling Windows Logins for Local and Remote Audits.....	145
Configuring a Local Account	145
Configuring a Domain Account for Authenticated Scanning.....	145
Step 1: Creating a Security Group.....	146
Step 2: Create Group Policy	146
Step 3: Configure the policy to add the Nessus Local Access group as Administrators.....	146
Step 4: Ensure proper ports are open in the firewall for Nessus to connect to the host	146
Allowing WMI on Windows Vista, 7, 8, 2008, 2008R2 and 2012 Windows Firewall	146
Step 5: Linking GPO.....	147
Configuring Windows 2008, Vista, and 7.....	147



Appendix B – Enabling SSH Local Security Checks on Unix and Network Devices	148
Generating SSH Public and Private Keys.....	148
Creating a User Account and Setting up the SSH Key	148
Enabling SSH Local Security Checks on Network Devices.....	150
Appendix C – Interface Shortcuts	151

Introduction

This document describes how to use Tenable Network Security's **Nessus** product. Please email any comments and suggestions to support@tenable.com.

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 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](#).

Overview

Nessus is a web-based interface to the Nessus scanner that is comprised of a simple HTTP server and web client, and requires no software installation apart from the Nessus server. The primary features are:

- Generates `.nessus` files that Tenable products 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 v2 File Format](#) guide for more details.
- Scan targets can use a variety of formats: IPv4/IPv6 addresses, hostname, and CIDR notation.
- Support for LDAP so that Nessus user interface accounts can authenticate against a remote corporate server.
- The UI 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 the UI is disconnected for any reason.
- Nessus scan reports can be uploaded via the Nessus user interface and compared to other reports.
- Scanning dashboards that display vulnerability and compliance overviews that allow you to visualize trends across your scanning history.
- A policy template to help quickly create efficient scan policies for auditing your network.
- Gives the ability to set one scanner as a primary and additional scanners secondary, allowing for a single Nessus interface to manage large-scale distributed scans.
- An extensive user and grouping system that allows for granular resource sharing including scanners, policies, schedules, and scan results.

Installation

Details for installing Nessus 6.4 are found in the [Nessus 6.4 Installation and Configuration Guide](#).

Nessus User Interface (UI)

Supported Platforms

The Nessus web-based user interface is best-experienced using the minimum version specified of the following browsers:

- Internet Explorer 9
- Firefox 32
- Chrome 37
- Safari 7.1
- Chrome 29 for Android
- Safari for iOS

Connecting to Nessus

Nessus Manager, Nessus Professional, and Nessus Home are used and managed through HTTPS on port 8834. Each user will have a unique login and password.

In a browser, type `https://[server IP]:8834`

Nessus Cloud is accessed using the URL <https://cloud.tenable.com>.

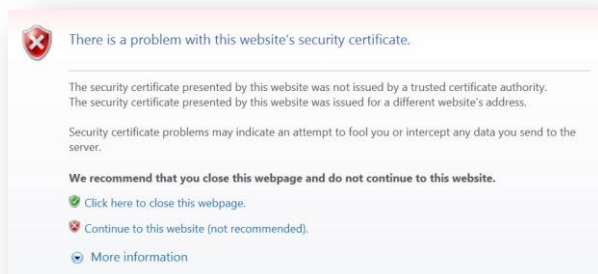
To create and configure users, refer to the [Nessus 6.4 Installation and Configuration Guide](#).

Security Warnings

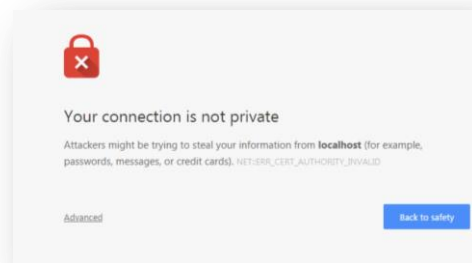
When accessing Nessus, you will encounter an error related to a security certificate issue: a connection privacy problem, an untrusted site, an unsecure connection, or similar security related error.

This is **expected and normal behavior**; Nessus is providing a **self-signed SSL certificate**.

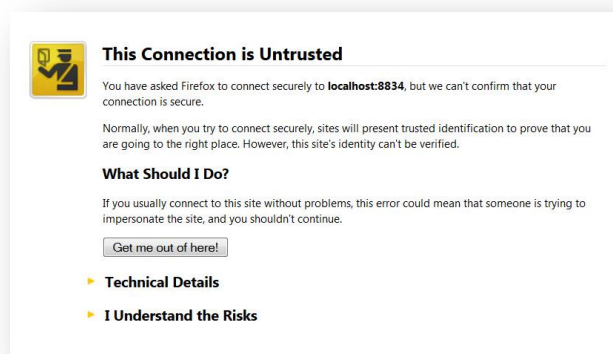
Based on the browser you are using, one of the following pages will be displayed and requires you to use the steps below to proceed to the Nessus login page.



Internet Explorer 11



Google Chrome version 43.x

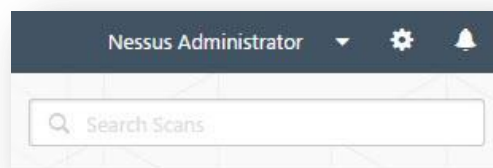





Mozilla Firefox version 32.x

Bypassing the SSL Warning

Browser	Steps
Google Chrome	Click on Advanced , and then Proceed to <i>example.com</i> (unsafe) .
Mozilla Firefox	Click on I Understand the Risks , and then click on Add Exception . Next click on Get Certificate , and finally Confirm Security Exception .
Microsoft Internet Explorer	Click on Continue to this website (not recommended) .

Nessus Top Navigation



Top Navigation Menu Options		
	User's Profile Drop-Down Menu	User Profile, Help & Support, What's New, and Sign Out
	General Settings	Depending on the version of Nessus and the permissions of the logged-in user, settings will be displayed with varying elements: Scanners , Accounts , Communication , and Advanced .
	Notifications	The bell icon displays messages related to Nessus operations.

User Profile Settings & Options

User Profile Account Settings

User Profile / Account Settings

Username

admin

Full Name

admin

Email

Example: test@test.com

User Type

System Administrator

Save

Cancel

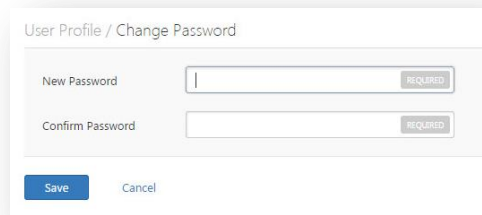
The **Account Settings** page shows the settings for the current authenticated user.



Warning: Once a username is created, it cannot be changed.

Version	Settings
Nessus Cloud	<div>Username (e-mail address)</div> <div>Full Name</div> <div>Email</div> <div>User Type</div> <div><div>!</div><div>Nessus Cloud accounts use the email address of the user for logins.</div></div>
Nessus Manager	<div>Username</div> <div>Full Name</div> <div>Email</div> <div>User Type</div>
Nessus Professional	<div>User Name</div> <div>User Type</div> <div><div>!</div><div>Nessus Professional user accounts do not have an email address associated with users.</div></div> <div><div>!</div><div>Nessus Professional only has two user types: System Administrator and Standard.</div></div>

Change Password

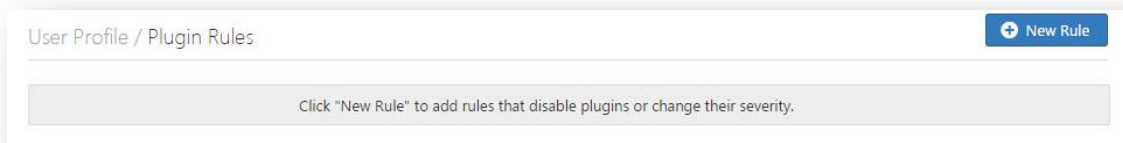
A screenshot of the 'User Profile / Change Password' form. It features two input fields: 'New Password' and 'Confirm Password'. Each field has a 'REQUIRED' label to its right. Below the input fields are two buttons: 'Save' (in blue) and 'Cancel' (in grey).

The **Change Password** option allows you to change the password, which should be done in accordance with your organization's security policy.



The current user has the ability to change their own password, and administrators have the ability to change other user's passwords by selecting the gear icon and navigating to the **Accounts / Users** page.

Plugin Rules

A screenshot of the 'User Profile / Plugin Rules' form. At the top right is a blue button with a plus icon and the text 'New Rule'. Below this is a grey rectangular box containing the text: 'Click "New Rule" to add rules that disable plugins or change their severity.'

Every audit in Nessus is coded as a plugin, which is a simple program that checks for a given flaw. Nessus uses more than 70,000+ different plugins, covering local and remote flaws.

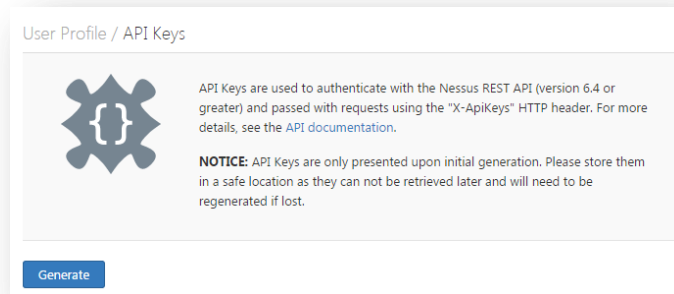
Plugin Rules allow users to create one or many rules to configure the behavior of plugins related to scans.



Information about Plugins and Plugin IDs can be found using the following links:

<http://www.tenable.com/plugins/>
<http://www.tenable.com/plugins/index.php?view=search>
<http://www.tenable.com/plugins/index.php?view=all>

API Keys



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.

Both, an **Access Key** and a **Secret Key** are created by using the **Generate** button.

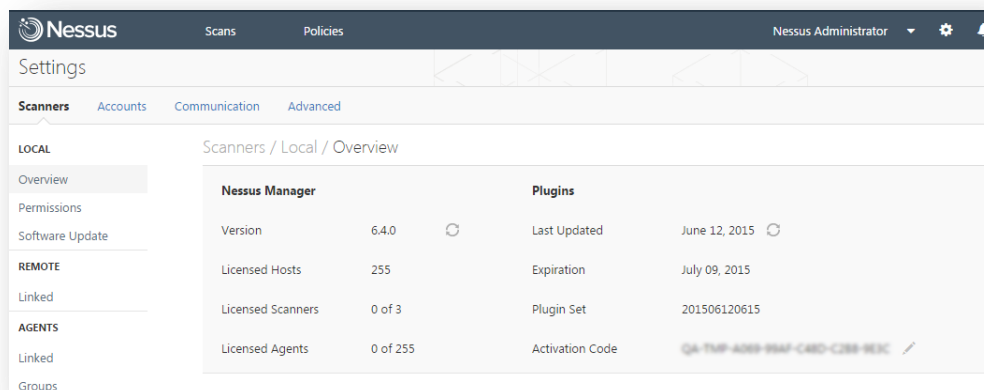
API Keys Warnings

- API Keys are only presented upon initial generation. Please store API Keys in a safe location, as they cannot be retrieved later.
- API Keys cannot be retrieved by Nessus. If lost, the API Keys must be regenerated.
- Regenerating the API Keys will immediately un-authorize any applications currently utilizing the key.

Nessus General Settings

When selected, the **Gear** icon will redirect you to the Nessus general setting page, which displays links to **Scanners**, **Accounts**, **Communication**, and **Advanced** pages.

Visibility of and access to general settings and options are determined based on User Type assigned to the user's Nessus Account.





Detailed information on Nessus general settings can be found in the [Nessus 6.4 Installation and Configuration Guide](#).

Scanners

The table below identifies general **Setting** options by product version and by user type.

Setting	Description	Product Version(s)	User Type(s)
LOCAL			
Overview	The overview page gives detailed information about the product version and plugins.	Nessus Cloud, Nessus Manager, Nessus Professional	All User Types except Read Only
Permissions	Users or groups are added to the permission page for no access, the ability to use, or the ability to manage the scanner.	Nessus Manager and Nessus Professional	System Administrator Only
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.	Nessus Professional	System Administrator Only
Software Update	Software updates can be configured for updating all components, plugins only, or disabled. The page also allows a custom host to be added for the plugin feed.	Nessus Manager and Nessus Professional	System Administrator Only
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.	Nessus Cloud, Nessus Manager, Nessus Professional	System Administrator and Administrator
AGENTS			



Setting	Description	Product Version(s)	User Type(s)
Linked	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.	Nessus Cloud and Nessus Manager	System Administrator Only
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 manage your agent groups.	Nessus Cloud and Nessus Manager	System Administrator Only

Accounts

Setting	Description	Product Version(s)	User Type(s)
ACCOUNTS			
Users	Individual Nessus Account to be used for assigning permissions.	Nessus Cloud, Nessus Manager, Nessus Professional	All User Types
Groups	Collections of users created for shared permissions.	Nessus Cloud and Nessus Manager	System Administrator Only

Communication

Setting	Description	Product Version(s)	User Type(s)
NETWORK			



LDAP Server	<p>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.</p> <p>Note: Nessus auto-negotiates encryption, therefore there are no encryption options in the Nessus interface.</p>	Nessus Cloud and Nessus Manager	System Administrator
Proxy Server	<p>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.</p>	Nessus Cloud, Nessus Manager, and Nessus Professional	System Administrator
SMTP Server	<p>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.</p>	Nessus Cloud, Nessus Manager, and Nessus Professional	System Administrator

CONNECTORS



Cisco ISE	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 1.2 or greater.	Nessus Manager	System Administrator
-----------	--	----------------	----------------------

Advanced

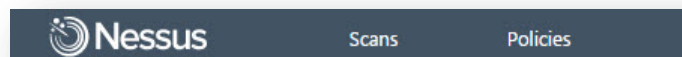
In **Nessus Manager** and **Nessus Professional**, a wide variety of configuration options offer more granular control of how the scanner operates.



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

Setting	Description	Product Version(s)	User Type(s)
Advanced Settings			
Advanced	Advanced configuration. Refer to the Nessus 6.4 Installation and Configuration Guide for in-depth information about these options and settings.	Nessus Manager and Nessus Professional	System Administrator

Scans and Policies



Type	Description
Scans	A scan is the act of Nessus assessing a host for vulnerabilities, based on defined rules.
Policies	A policy is a set of rules that defines what a scan does.

Scan Library and Policy Library

Nessus templates are used to facilitate the creation of **Scans** and **Policies**. When a new Scan or a new Policy is being created, the template library is displayed and each library contains **Scanner Templates** and **Agent Templates**.

While the templates in each library are identical, actual vulnerability scanning is performed by the creation and usage of a Scan, while the creation and usage of a policy defines the rules by which those Scans operate.

Scanner Templates



Template names may change from time-to-time based on the new policy templates to the feed. For example, when the [GHOST](#) and [Bash Shellshock](#) vulnerabilities were disclosed, policies configured to specifically detect the vulnerabilities were added to the list.

Name	Description
Advanced Scan	Scan template for users who want total control of their policy configuration.
Audit Cloud Infrastructure	Used for auditing the configuration of third-party cloud services.
Bash Shellshock Detection	Remote and credentialed checks for the Bash Shellshock vulnerability.
Basic Network Scan	For users scanning internal or external hosts.
Credentialed Patch Audit	Log in to systems and enumerate missing software updates.
GHOST (glibc) Detection	Credentialed checks for the GHOST vulnerability.
Host Discovery	Identifies live hosts and open ports.
Internal PCI Network Scan	For administrators preparing for a Payment Card Industry Data Security Standards (PCI DSS) compliance audit of their internal networks.
MDM Config Audit	Used for auditing the configuration of mobile device managers.
Mobile Device Scan	For users of Apple Profile Manager, ADSI, MobileIron, or Good MDM.
Offline Config Audit	Upload and audit the config file of a network device.
PCI Quarterly External Scan	An approved policy for quarterly external scanning required by PCI. This is offered on Nessus Cloud only.
Policy Compliance Auditing	Audit system configurations against a known baseline provided by the user.
SCAP and OVAL Compliance Auditing	Audit systems using Security Content Automation Protocol (SCAP) and OVAL definitions.
Web Application Tests	For users performing generic web application scans.
Windows Malware Scan	For users searching for malware on Windows systems.



If you are migrating from Nessus 5.x to 6.4, any changes you made to the policies will be overwritten in the policy library. User created policies will not be affected when derived from the Advanced Template.

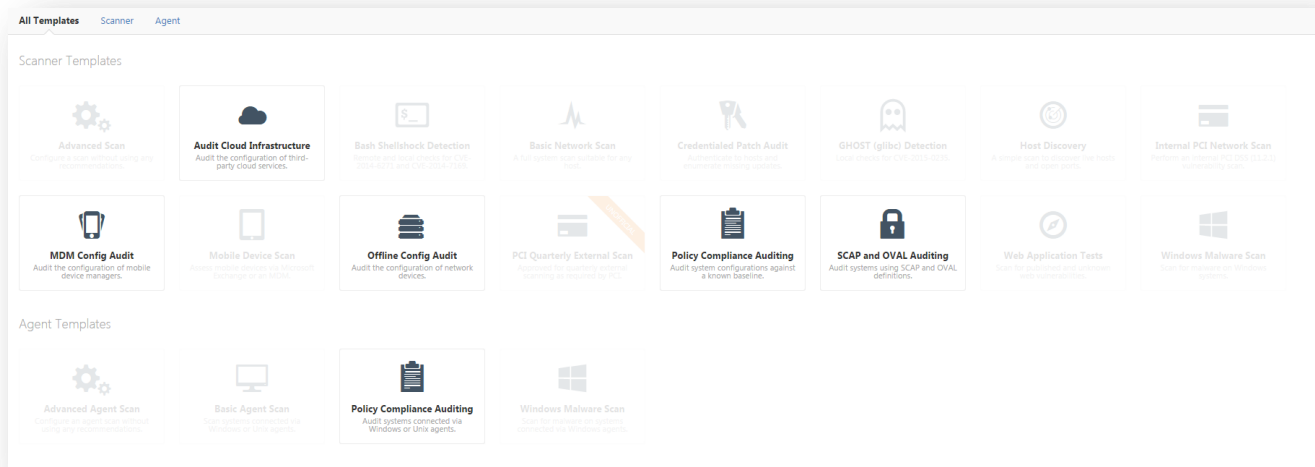


You can also search for templates using the **Search Library** box in the upper right corner.

Compliance Specific Templates

Nessus compliance auditing can be configured with the following Scanner and Agent templates:

- Audit Cloud Infrastructure
- MDM Config Audit
- Offline Config Audit
- SCAP and OVAL Auditing
- Policy Compliance Auditing



You can search for a **Compliance** using the Search Library box in the upper right corner of the page.

Mobile Device Specific Template

Mobile Device Managers (MDM)

Mobile device penetration has reached an all-time high, as both individuals and corporations become more reliant on them to conduct their affairs. An entire market has quickly evolved, centered on Bring Your Own Device (BYOD) security and integration. Like it or not, and know it or not, mobile devices are increasingly being connected to corporate networks. In some cases, such connections may seem like a harmless activity such as charging a battery. In reality, simply charging the device is often performed via USB connection, and doing so may bridge the device with the computer.

Active scanning cannot always detect mobile devices on the network directly since the devices are not always active on the network. There are several approaches that can be taken to identify mobile devices connecting to the network. One is to leverage a Mobile Device Management (MDM) console, which will contain a lot of useful information about mobile devices on the network. The drawback to this approach is the reason the issue is called Bring Your Own Device; the device is often a personal device that is not enrolled in the MDM system.

A better approach is to leverage information obtained from devices that connect to Microsoft Exchange servers. Basically, any employees who self-enroll with ActiveSync are sending their mobile OS version and other information back to the Exchange server. This provides a non-intrusive method to obtain the device type and OS version. Since Exchange is so widely deployed, the information is already available in many infrastructures. The drawback to this approach is that the information obtained is less granular than what is available on an MDM.

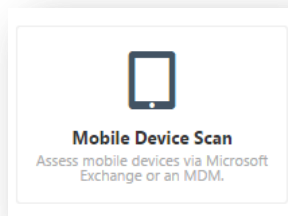
With Nessus Manager, the Nessus Mobile Devices plugin family provides the ability to obtain information from devices registered in a MDM and from Active Directory servers that contain information from MS Exchange servers. This currently includes Apple iPhone, Apple iPad, Windows Phone, and Android devices that supply version information, and have checked in to their respective servers in the last year (365 days).



The Nessus scanner must be able to reach the mobile device management (MDM) servers to query for information. You must ensure no screening devices block traffic to these systems from the Nessus scanner. In addition, Nessus must be given administrative credentials (e.g., domain administrator) to the Active Directory servers.

To scan for mobile devices, Nessus must be configured with authentication information for the management server and the mobile plugins of interest. Since Nessus authenticates directly to the management servers, a scan policy does not need to be configured to scan specific hosts.

In order to scan a mobile system, select the **Mobile Device Scan** template.



For ActiveSync scans that access data from Microsoft Exchange servers, Nessus will retrieve information from phones that have been updated in the last 365 days.

PCI Auditing Specific Templates

Tenable offers two Payment Card Industry Data Security Standard (PCI DSS) templates: one for testing internal systems and one for external scans. The external scan policy is available only via Nessus Cloud. Nessus Cloud will test for all PCI DSS external scanning requirements, including web applications. The PCI Quarterly External Scan is designed to help you meet PCI scan requirements by an Approved Scanning Vendor (ASV).

Nessus results can be used during PCI compliance assessment to demonstrate periodic and ongoing processes were maintained throughout the assessment period as required by numerous PCI DSS requirements.



In order to submit a Nessus scan for PCI attestation, the scan must be conducted and submitted by Nessus Cloud.

Nessus results can be used during PCI compliance assessment to demonstrate periodic and ongoing processes were maintained throughout the assessment period as required by numerous PCI DSS requirements.

PCI Policy	Description
PCI Quarterly External Scan	A Nessus Cloud-only option that directs Nessus to compare scan results against PCI DSS standards .
Internal PCI Network Scan	Policy for performing an internal PCI DSS vulnerability scan.

SCAP and OVAL Auditing Specific Template

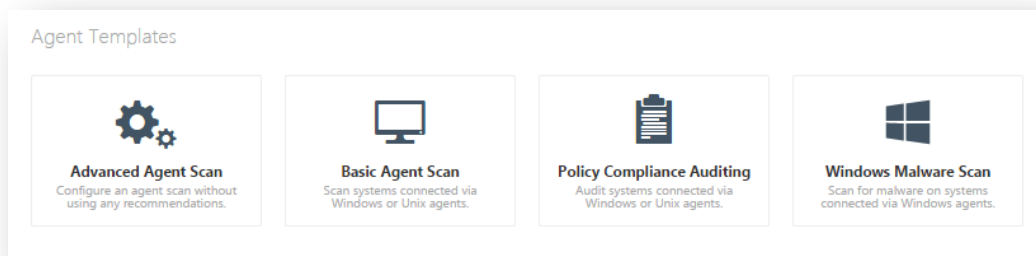
NIST's Security Content Automation Protocol (**SCAP**) is a set of policies for managing vulnerabilities and policy compliance in government agencies. It relies on multiple open standards and policies, including OVAL, CVE, CVSS, CPE, and FDCC policies. For more information on SCAP, please visit the [NIST Security Content Automation Protocol](#) site.

SCAP compliance auditing requires sending an executable to the remote host. Systems running security software (e.g., McAfee Host Intrusion Prevention), may block or quarantine the executable required for auditing. For those systems, an exception must be made for the either the host or the executable sent.

Nessus has two **SCAP** compliance templates available.

SCAP Policy	Description
Linux (SCAP)	Upload Linux SCAP zip files that will be used to determine if a tested Linux system meets the compliance standards as specified in SP 800-126.
Linux (OVAL)	Upload Linux OVAL definitions file zip format.
Windows (SCAP)	Upload Windows SCAP zip files that will be used to determine if a tested Windows system meets the compliance standards as specified in SP 800-126.
Windows (OVAL)	Upload Windows OVAL zip files that will be used to determine if a tested Windows system meets the compliance standards as specified in SP 800-126.

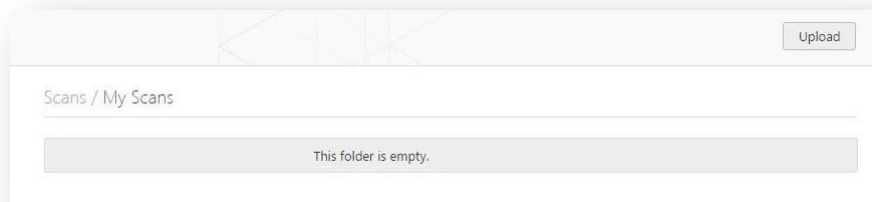
Agent Templates



Name	Description
Advanced Agent Scan	Allows you to create and manually configure an agent scan without using any recommendations.
Basic Agent Scan	Scans systems connected to Windows or Unix agents.
Policy Compliance Auditing	Used for auditing systems connected via Windows or Unix agents.
Windows Malware Scan	Scans for malware on systems connected via Windows agents.

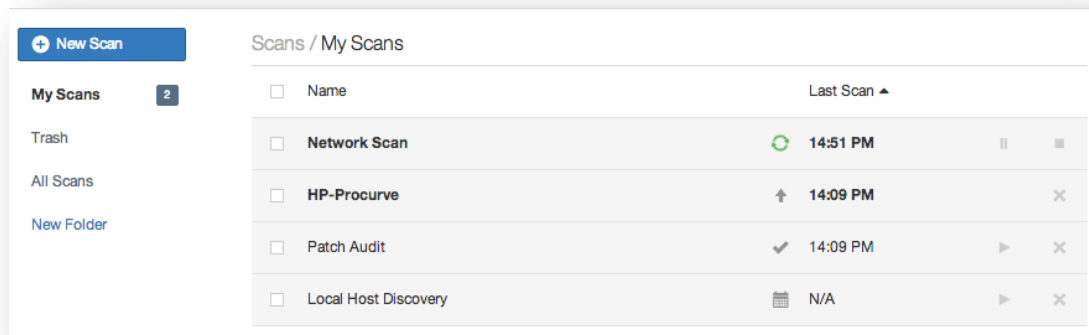
Scans

When logging into Nessus, the **Scans / My Scans** page will be displayed. This folder will remain empty until a **New Scan** is created.



Once created, **Scans** appear either the My Scans folder, or the folder designated during the creation of the Scan; using the **All Scans** link will display all **Scans** within all folders.

Scans folders also display the status of each scan. If a Scan is running, a pause and stop button will be present to allow the scan to be halted.



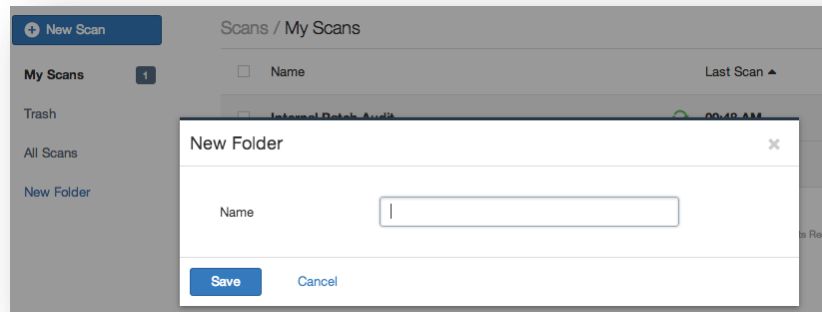
Scan Statuses

- Completed
- Aborted
- Imported
- Pending
- Running
- Resuming
- Canceling
- Cancelled
- Pausing
- Paused
- Stopping
- Stopped

Create a New Scan Folder

By default, all created **Scans** are stored in the **My Scans** folder; this is a system folder and cannot be deleted.

New folders can be created by using the **New Folder** link on the left navigation area of the **Scans / My Scans** page.



Create a New Scan

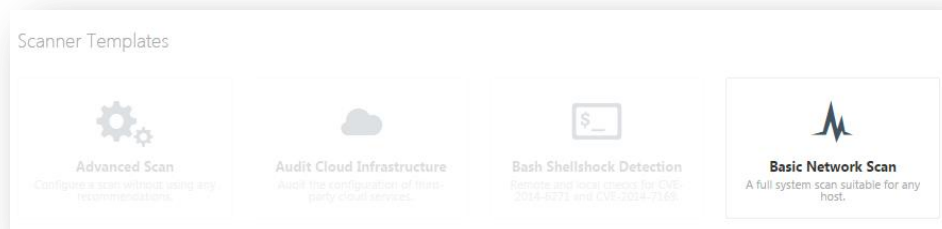
This section provides examples that demonstrate the options and settings associated **Scanner Templates**.

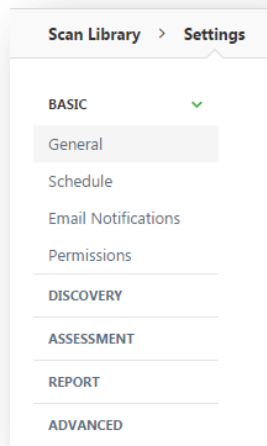
From the **Scans / My Scans** page, use the **New Scan** button to create a new scan, and you will be redirected to the **Scan Library** page.



Scan > Settings (Basic Network Scan Example)

Many of the **Scanner Templates** share the same basic settings. This example demonstrates the settings and pages as seen when using a **Basic Network Scan** template.





Basic

Settings / Basic / General

Settings / Basic / General

Name

REQUIRED

Description

Folder

My Scans

▼

Dashboard

Enabled

▼

Scanner

Local Scanner

▼

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

REQUIRED

Upload Targets

Add File

Save

Cancel

Option	Default	Description
Name	none	Sets the name that will be displayed in the Nessus user interface to identify the scan.
Description	none	Optional field for a more detailed description of the scan.
Folder	My Scans	The Nessus user interface folder to store the scan results.
Dashboard	Enabled	Enable or disable scan dashboards. Dashboards are enabled for all new scans by default. However, they are disabled on existing or imported scans unless you enable them.



Scanner	Local Scanner	Which Nessus scanner to perform the scan. This will provide multiple options if you have configured additional Nessus scanners to be secondary to this one.
Targets	none	<p>Valid Formats:</p> <ul style="list-style-type: none">• A single IP address (e.g., 192.168.0.1)• An IP range (e.g., 192.168.0.1-192.168.0.255)• A subnet with CIDR notation (e.g., 192.168.0.0/24)• A resolvable host (e.g., www.nessus.org)• A single IPv6 address (e.g., link6%eth0, fe80::2120d:17ff:fe57:333b, fe80:0000:0000:0000:0216:cbff:fe92:88d0%eth0).
Upload Targets	none	<p>A text file with a list of hosts can be imported by clicking on Add File and selecting a file from the local machine.</p> <p>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.</p>

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
```

Virtual servers:

```
www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]
```

IPv6 addresses:

```
link6
fe80::212:17ff:fe57:333b
fe80:0000:0000:0000:0216:cbff:fe92:88d0
```

IPv6 addresses with the zone index in Unix-based operating systems (e.g., Linux, FreeBSD):

```
link6%eth0
fe80::212:17ff:fe57:333b%dc0
fe80:0000:0000:0000:0216:cbff:fe92:88d0%eth0
```

IPv6 addresses with the zone index in Windows operating systems:

link6%23
fe80::212:17ff:fe57:333b%1
fe80:0000:0000:0000:0216:cbff:fe92:88d0%6



Depending on your scan settings such as **max hosts** or **max checks per host**, this may cause virtual hosts to be throttled as Nessus views them as the same IP address. On non-Windows hosts, Nessus administrators can add a custom advanced setting named **multi_scan_same_host** and set it to **yes**. This will allow the scanner to perform multiple scans against the same IP address. Note that on Windows, the PCAP driver does not allow this regardless of Nessus configuration. This functionality is available in Nessus 5.2.0 and later.

Settings / Basic / Schedule

To enable scheduling, toggle **Enable Schedule**.

Permission	Description
Once	Schedule the scan at a specific time.
Daily	Schedule the scan to occur on a daily basis, at a specific time or to repeat up to every 20 days.
Weekly	Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks.
Monthly	Schedule the scan to occur every month, by time and day or week of month, for up to 20 months.
Yearly	Schedule the scan to occur every year, by time and day, for up to 20 years.

Settings / Basic / Email Notifications

Under the **Email Notifications** tab, you can add user's email addresses to receive scan notifications. Furthermore, you may setup **Result Filters** which will define the content to be included in the notifications messages.

Settings / Basic / Email Notifications

Recipient(s)

Example: me@example.com, you@example.com

Result Filters

Match All of the following:

Plugin Description

contains

TEXT

×

Add Filter

Save

Cancel

Settings / Basic / Permissions

The **Permissions** functionality affects which users have permissions to access or configure the scan:

Settings / Basic / Permissions

Add users or groups

Search by user name or group name

Default

No access

admin

Is owner

Save

Cancel

Permission	Description
No Access	Only the user who created the policy can view, use, or edit the policy
Can View	Other users can view the scan results. They will not be able to control or configure the scan.
Can Control	Other users can control the scan (launch, pause, and stop) and view the scan results. They will not be able to configure the scan.
Can Configure	Other users can control the scan and configure the scan settings. They cannot delete the scan.

Discovery

The **Discovery** screen controls options related to discovery and port scanning including the port ranges and methods.

The options are under the headings **Host Discovery**, **Port Scanning**, and **Service Discovery**.

Settings / Discovery /Host Discovery

Settings / Discovery / Host Discovery

Ping the remote host

General Settings

☒ Test the local Nessus host

This setting specifies whether the local Nessus host should be scanned when it falls within the target range specified for the scan.

☐ Use fast network discovery

If a host responds to ping, Nessus attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. Fast network discovery

Ping Methods

☒ ARP

☒ TCP

Destination ports

built-in

☒ ICMP

☐ Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries

2

☐ UDP

Fragile Devices

☐ Scan Network Printers

☐ Scan Novell Netware hosts

Wake-on-LAN

List of MAC addresses

Add File

Boot time wait (in minutes)

5

Network Type

Network Type

Mixed (use RFC 1918)

Save

Cancel

Toggling the **Ping the remote host** switch will enable the ping options listed below.

Option	Default	Description
Ping the remote host		
	Enabled	<p>This option enables Nessus to ping remote hosts on multiple ports to determine if they are alive. When selected, this will enable other pingging options.</p> <p>To scan VMware guest systems, Ping the remote host must disabled.</p>
General Settings		
Test the local Nessus host	Enabled	<p>If Ping the remote host is enabled, this option is enabled by default for this policy. 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.</p>

Scans and Policies: Scans

27 of 151

Fast network discovery	Disabled	If Ping the remote host is enabled, you will be able to see this option. By default, this option is not enabled. 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 even when there is no service behind the device). 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.
Ping Methods		
ARP	Enabled	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.
TCP	Enabled	Ping a host using TCP.
Destination ports (TCP)	Built-in	Destination ports can be configured to use specific ports for TCP ping. This 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.
ICMP	Enabled	Ping a host using the Internet Control Message Protocol (ICMP).
Assume ICMP unreachable from the gateway means the host is down	Disabled	When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When this option is enabled, when Nessus receives an ICMP Unreachable message it will consider the targeted host dead. This is to help speed up discovery on some networks. Note that some firewalls and packet filters use this same behavior for hosts that are up but are connecting to a port or protocol that is filtered. With this option enabled, this will lead to the scan considering the host is down when it is indeed up.
Number of Retries (ICMP)	2	Allows you to specify the number of attempts to try to ping the remote host. The default is two attempts.
UDP	Disabled	Ping a host using the User Datagram Protocol (UDP). UDP is a stateless protocol, meaning that communication is not performed 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.

Option	Default	Description
Fragile devices		
	Disabled	The Fragile Devices menu offers two options that instruct the Nessus scanner not to scan hosts that have a history of being fragile, or prone to crashing when receiving unexpected input. Users can select either Scan Network Printers or Scan Novell Netware hosts to instruct Nessus to scan those particular devices. Nessus will only scan these devices if these options are checked. It is recommended that scanning of these devices be performed in a manner that allows IT staff to monitor the systems for issues.
Wake-on-LAN		
	Disabled	The Wake-on-LAN (WOL) menu controls which hosts to send WOL magic packets to before performing a scan and how long to wait (in minutes) for the systems to boot. The list of MAC addresses for WOL is entered using an uploaded text file with one host MAC

		address per line. For example: 00:11:22:33:44:55 aa:bb:cc:dd:ee:ff
Network Type		
	Mixed	Allows you to specify if you are using publicly 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.

Settings / Discovery / Port Scanning

Port scanning options define how the port scanner will behave and which ports to scan.

Settings / Discovery / Port Scanning

Ports

☐ Consider unscanned ports as closed

Port scan range:

Local Port Enumerators

☒ SSH (netstat)

☒ WMI (netstat)

☒ SNMP

☒ Only run network port scanners if local port enumeration failed

☐ Verify open TCP ports found by local port enumerators

Network Port Scanners

☒ SYN

☐ Override automatic firewall detection

☒ Use soft detection

☐ Use aggressive detection

☐ Disable detection

☐ UDP

Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP enumeration options instead if possible.

Save

Cancel

Option	Default	Description
Ports		
Consider Unscanned Ports as Closed	Disabled	If a port is not scanned with a selected port scanner (e.g., out of the range specified), Nessus will consider it closed.
Port Scan Range	default	Directs the scanner to target a specific range of ports. Options: Default , All , Custom

	default	Using the keyword default , Nessus will scan approximately 4,790 common ports. The list of ports can be found in the nessus-services file.
	all	Using the keyword all , Nessus will scan via a plugin all 65,536 ports, including port 0.
	Custom List	<p>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.</p> <p>You may also specify a split range specific to each protocol. For example, if you want to scan a different range of ports for TCP and UDP in the same policy, you would specify T:1-1024,U:300-500. You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate protocol ("1-1024,T:1024-65535,U:1025"). If you are scanning a single protocol, select only that port scanner and specify the ports normally.</p> <p>The range specified for a port scan will be applied to both TCP and UDP scans.</p>
Local Port Enumerators		
SSH (netstat)	Enabled	This option uses netstat to check for open ports from the local machine. It relies on the netstat command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.
WMI (netstat)	Enabled	<p>This option uses netstat to check for open ports from the local machine. It relies on the netstat command being available via a WMI connection to the target. This scan is intended for Windows-based systems and requires authentication credentials.</p> <p>A WMI based scan uses netstat to determine open ports, thus ignoring any port ranges specified. If any port enumerator (netstat or SNMP) is successful, the port range becomes all. However, Nessus will still honor the consider unscanned ports as closed option if selected.</p>
SNMP	Enabled	Direct Nessus to scan targets for a Simple Network Management Protocol (SNMP) service. Nessus will attempt to guess relevant SNMP settings during a scan. If the settings are provided by the user (under Credentials), 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.
Only run network port scanners if local port enumeration failed	Enabled	Rely on local port enumeration first before relying on network port scans.



Verify open TCP ports found by local port enumerators	Disabled	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).
Network Port Scanners		
TCP	Disabled	<p>Use Nessus' built-in Transmission Control Protocol (TCP) scanner to identify open TCP ports on the targets. This scanner is optimized and has some self-tuning features.</p> <p>On some platforms (e.g., Windows and Mac OS X), selecting this scanner will cause Nessus to use the SYN scanner to avoid serious performance issues native to those operating systems.</p>
SYN	Enabled	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, depending on the security monitoring device such as a firewall or Intrusion Detection System (IDS). 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.
	Use aggressive detection	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.
	Use soft detection	Disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device.
	Disable detection	Disables the Firewall detection feature.
UDP	Disabled	<p>This option engages Nessus' built-in UDP scanner to identify open UDP ports on the targets.</p> <p>Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP ports. Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enumeration options instead if possible.</p>

Settings / Discovery / Service Discovery

Settings / Discovery / Service Discovery

General Settings

☒ Probe all ports to find services

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.

Search for SSL based services

☒

Search for SSL on

Known SSL ports

Identify certificates expiring within x days

60

☒ Enumerate all SSL ciphers

When selected, Nessus ignores the list of ciphers advertised by SSL services, and enumerates them by attempting to establish connections using all possible ciphers.

☐ Enable CRL checking (connects to the Internet)

Save

Cancel



Toggling the **Search for SSL based services** switch will enable the service discovery options listed below. Otherwise, they will not be visible.

The **Service Discovery** section sets options that attempt to map each open port with the service that is running on that port.



There is a possibility that probing may disrupt servers or cause unforeseen side effects.

Settings / Discovery / Service Discovery

General Settings

☒ Probe all ports to find services

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.

Search for SSL based services

☐

Save

Cancel

Option	Default	Description
General Settings		
Probe all ports to find services	Enabled	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.
Search for SSL based services	Enabled	The Search for SSL based services controls how Nessus will test SSL based services. If selected, choose between Known SSL ports (e.g., 443) and All ports . Testing for SSL capability on all ports may be disruptive for the tested host.

If Search for SSL based services is enabled, the following options are available:

Settings / Discovery / Service Discovery

General Settings

☒ Probe all ports to find services
Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this

Search for SSL based services ☒

Search for SSL on

Identify certificates expiring within x days

☒ Enumerate all SSL ciphers
When selected, Nessus ignores the list of ciphers advertised by SSL services, and enumerates them by atte

☐ Enable CRL checking (connects to the Internet)

Option	Default	Description
Enumerate all SSL ciphers	Enabled	When Nessus performs an SSL scan, it tries to determine the SSL ciphers used by the remote server by attempting to establish a connection with each different documented SSL cipher, regardless of what the server says is available.
Enable CRL checking (connects to Internet)	Disabled	Direct Nessus to check SSL certificates against known Certificate Revocation Lists (CRL).

Assessment

The **Assessment** screen controls evaluation popular for security assessments: **General**, **Brute Force**, **SCADA**, **Web Applications**, and **Windows**.

Settings / Assessment / General

Accuracy

☐ Override normal accuracy

☒ Avoid potential false alarms

☐ Show potential false alarms

☐ Perform thorough tests (may disrupt your network or impact scan speed)

Antivirus

Antivirus definition grace period (in days):

SMTP

Third party domain:
This domain must be outside the range of the site being scanned

From address:

To address:

Option	Default	Description
Accuracy		
Override normal accuracy	Disabled	In some cases, Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to Show potential false alarms 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 potential false alarms will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. Not enabling Override normal accuracy is a middle ground between these two settings.
Perform thorough tests (may disrupt your network or impact scan speed)	Disabled	Causes various plugins to work harder. For example, when looking through SMB file shares, a plugin can analyze 3 directory 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 providing better audit results.
Antivirus		
Antivirus definition grace period (in days)	0	Configure the delay of the Antivirus software check for a set number of days (0-7). The Antivirus Software Check menu allows you to direct Nessus to allow for a specific grace time in reporting when antivirus signatures are considered out of date. By default, Nessus will consider signatures out of date regardless of how long ago an update was available (e.g., a few hours ago). This can be configured to allow for up to 7 days before reporting them out of date.



SMTP	
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 may 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.

Settings / Assessment / Brute Force

The **Brute Force** options allow for granular control of accounts for brute force scans. The **Default Accounts** options relate to how the scanner tests possible default accounts.

Settings / Assessment / Brute Force

General Settings

☒ Only use credentials provided by the user
Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.

Oracle Database

☐ Test default accounts (slow)

Save Cancel

Option	Default	Description
Only use credentials provided by the user	Enabled	In some cases, Nessus can test default accounts and known default passwords. This can cause the account to be locked out if too many consecutive invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Nessus from performing these tests.
Test default Oracle accounts (slow)	Disabled	Test for known default accounts in Oracle software.

Settings / Assessment / SCADA

The SCADA settings menu specifies options for Supervisory Control And Data Acquisition (SCADA) tests that run on all devices within the scanned domain that are running SCADA services. The Nessus vulnerability scanner performs both unauthenticated and authenticated scans of SCADA systems for a wide range of vulnerabilities for commercial customers. Settings for SCADA plugins are listed below:

Settings / Assessment / SCADA

Modbus/TCP Coil Access

Start at register

End at register

ICCP/COTP TSAP Addressing Weakness

Start COTP TSAP

Stop COTP TSAP

Option	Description
Modbus/TCP Coil Access	
	<p>The Modbus/TCP Coil Access options are available for commercial users. This drop-down menu item is dynamically generated by the SCADA plugins available with the commercial version of Nessus. 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.</p> <p>The defaults for this are 0 for the Start reg and 16 for the End reg.</p>
ICCP/COTP TSAP Addressing Weakness	
	<p>The ICCP/COTP TSAP Addressing menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values.</p> <p>The start and stop values are set to 8 by default.</p>

Settings / Assessment / Web Applications

The **Web Applications** menu 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, and SQL injection. Enable this option by selecting the Scan web applications checkbox.

Settings / Assessment / Web Applications

Web Application Settings

Scan web applications ☐

These tests are dependent on the following NASL plugins:

- [11139](#), [42424](#), [42479](#), [42426](#), [42427](#), [43160](#), [51973](#) – SQL Injection (CGI abuses)
- [39465](#), [44967](#), [51528](#) – Command Execution (CGI abuses)
- [39466](#), [47831](#), [42425](#), [46193](#), [49067](#), [51972](#), [51529](#), [52483](#), [55904](#) – Cross-Site Scripting (CGI abuses: XSS)
- [39467](#), [46195](#), [46194](#), [50494](#) – Directory Traversal (CGI abuses)
- [39468](#) – HTTP Header Injection (CGI abuses: XSS)
- [39469](#), [42056](#), [42872](#) – File Inclusion (CGI abuses)
- [42055](#) – Format String (CGI abuses)
- [42423](#), [42054](#) – Server Side Includes a.k.a. SSI (CGI abuses)
- [44136](#) – Cookie Manipulation (CGI abuses)
- [46196](#) – XML Injection (CGI abuses)
- [40406](#), [48926](#), [48927](#) – Error Messages
- [56245](#) – XPath Injection
- [47830](#), [47832](#), [47834](#), [44134](#) – Additional attacks (CGI abuses)



This list of web application related plugins is updated frequently and may not be complete. Additional plugins may be dependent on the settings in this preference option.



Toggling the **Scan web applications** switch will enable all the web application scanning options listed below. Otherwise, they will not be enabled or will be visible in the UI.

Settings / Assessment / Web Applications

Web Application Settings

Scan web applications

General Settings

☐ Use the cloud to take screenshots of public web servers

Use a custom User-Agent

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1)

Web Crawler

Start crawling from

/

Excluded pages (regex)

/server_privileges,php/logout

Maximum pages to crawl

1000

Maximum depth to crawl

6

☐ Follow dynamically generated pages

Application Test Settings

☐ Enable generic web application tests

☐ Abort web application tests if HTTP login fails
 ☐ Try all HTTP methods
 ☐ Attempt HTTP Parameter Pollution
 ☐ Test embedded web servers
 ☐ Test more than one parameter at a time per form

☒ Test random pairs of parameters
 ☐ Test all pairs of parameters (slow)
 ☐ Test random combinations of three or more parameters (slower)
 ☐ Test all combinations of parameters (slowest)

☐ Do not stop after the first flaw is found per web page

☒ Stop after one flaw is found per web server (fastest)
 ☐ Stop after one flaw is found per parameter (slow)
 ☐ Look for all flaws (slowest)

URL for Remote File Inclusion

http://rfi.nessus.org/rfi.txt

If the target(s) being scanned cannot reach the Internet, the default URL when executed.

Maximum run time (minutes)

5

This limit refers to the maximum amount of time spent attempting each

Save

Cancel

Option	Default	Description
General		
Use the cloud to take screenshots of public webservers	Disabled	<p>This option enables Nessus to take screenshots to better demonstrate some findings. This includes some services (e.g., VNC, RDP) as well as configuration specific options (e.g., web server directory indexing). The feature only works for Internet-facing hosts, as the screenshots are generated on a managed server and sent to the Nessus scanner.</p> <p>Screenshots are not exported with a Nessus scan report.</p>
Use a custom User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	Specifies which type of web browser Nessus will impersonate while scanning.

Scans and Policies: Scans

38 of 151



Web Crawler		
Start crawling from	/	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 pages (regex)	/server_privileges\.php log out	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: (^/manual) (\.pl(\?.*)?\$). Nessus supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).
Maximum pages to crawl	1000	The maximum number of pages to crawl.
Maximum depth to crawl	6	Limit the number of links Nessus will follow for each start page.
Follow dynamic pages	Disabled	If selected, Nessus will follow dynamic links and may exceed the parameters set above.
Application Test Settings		
Enable generic web application tests	Disabled	Enables the options listed below.
Abort web application tests if HTTP login fails	Disabled	If Nessus cannot login to the target via HTTP, then do not run any web application tests.
Try all HTTP methods	Disabled	This option will instruct Nessus to also use POST requests 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. When selected, Nessus will test each script/variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.
Attempt HTTP Parameter Pollution	Disabled	When performing web application tests, attempt to bypass 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.
Test embedded web servers	Disabled	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.
Test more than one parameter at a time per form	Disabled	<p>This option manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, Nessus would attempt <code>/test.php?arg1=XSS&b=1&c=1</code> 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>This drop-down has four options:</p> <p>Test random pairs of parameters – This form of testing will randomly check a combination of random pairs of parameters. This is the fastest way to test multiple parameters.</p> <p>Test all pairs of parameters (slow) – 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 <code>/test.php?a=XSS&b=1&c=1&d=1</code> 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 <code>/test.php?a=XSS&b=3&c=3&d=3</code> when the first value of each variable is 1.</p> <p>Test random combinations of three or more parameters (slower) – This form of testing will randomly check a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Note that increasing the amount of combinations by three or more increases the web application test time.</p> <p>Test all combinations of parameters (slowest) – 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</p>

		set of tests. This testing method may take a long time to complete.
Do not stop after first flaw is found per web page	Disabled	<p>This option determines when a new flaw is targeted. 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. The drop-down has four options:</p> <p>Stop after one flaw is found per web server (fastest) – 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.</p> <p>Stop after one flaw is found 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 (slowest) – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.</p>
URL for Remote File Inclusion	http://rfi.nessus.org/rfi.txt	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 by Tenable for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing.
Maximum run time (min)	5	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.

Settings / Assessment / Windows

The Windows options allow you to fine tune the scope of Windows scans.

Settings / Assessment / Windows

General Settings

☒ Request information about the SMB Domain

Enumerate Domain Users

Start UID

1000

The beginning of a range of IDs where Nessus will attempt to enumerate domain users

End UID

1200

The end of a range of IDs where Nessus will attempt to enumerate domain users

Enumerate Local Users

Start UID

1000

The beginning of a range of IDs where Nessus will attempt to enumerate local users

End UID

1200

The end of a range of IDs where Nessus will attempt to enumerate local users

Malware Files

Provide your own list of known bad MD5 hashes:

Add File

Each line in the file must begin with an MD5 hash, and can optionally be followed by a comma delimiter and a description. Blank lines and lines begin with a hash are ignored.

Provide your own list of known good MD5 hashes:

Add File

Each line in the file must begin with an MD5 hash, and can optionally be followed by a comma delimiter and a description. Blank lines and lines begin with a hash are ignored.

Hosts file whitelist

Add File

Abnormalities in a Windows system's hosts file indicate that it may have been compromised. This setting allows whitelisting entries in the hosts file that are known to be safe.

Malware Settings

☐ Disable DNS resolution

Checking this option will prevent Nessus from using the cloud to compare scan findings against known malware.

Save

Cancel

The following options affect the SMB scope for Windows targets.

Option	Default	Description
Request information about the SMB Domain		
	Enabled	If the option Request information about the domain is set, then domain users will be queried instead of local users.

Option	Description
Enumerate Domain Users	
	The Enumerate Domain Users menu specifies the SID range to use to perform a reverse lookup on usernames on the domain. The default setting is recommended for most scans. The default values are 1000 for Start UID and 1200 for End UID .
Enumerate Local Users	
	The Enumerate Local Users menu specifies the SID range to use to perform a reverse lookup on local usernames. The default setting is recommended. The default values are 1000 for Start UID and 1200 for End UID .



Malware Files	
Provide your own list of known bad MD5 hashes	<p>Additional known bad MD5 hashes can be uploaded via a text file that contains one MD5 hash per line.</p> <p>It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target and a description was provided for the hash the description will show up in the scan results. Standard hash-delimited comments (e.g., #) can optionally be used in addition to the comma-delimited ones.</p>
Provide your own list of known good MD5 hashes	<p>Additional known good MD5 hashes can be uploaded via a text file that contains one MD5 hash per line.</p> <p>It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, and a description was provided for the hash, the description will show up in the scan results. Standard hash-delimited comments (e.g., #) can optionally be used in addition to the comma-delimited ones.</p>
Hosts file whitelist	Nessus checks system hosts files for signs of a compromise (e.g., Plugin ID 23910 titled Compromised Windows System (hosts File Check). This option allows you to upload a file containing a list of hostnames that will be ignored by Nessus during a scan. Include one hostname per line in a regular text file.
Malware Settings	
Disable DNS Resolution	Checking this option will prevent Nessus from using the cloud to compare scan findings against known malware.

Report

The **Report** section affects report **Processing** and **Output**.

Settings / Report

Processing

☐ Override normal verbosity

☒ I have limited disk space. Report as little information as possible

☐ Report as much information as possible

☒ Show missing patches that have been superseded

☒ Hide results from plugins initiated as a dependency

Output

☒ Allow users to edit scan results

☐ Designate hosts by their DNS name

☐ Display hosts that respond to ping

☐ Display unreachable hosts

Save

Cancel

The **Processing** options affect the overall plugin information to be included in a report.

Option	Default	Description
Processing		
Override normal verbosity	Disabled	<p>"I have limited disk space. Report as little information as possible" will provide less information about plugin activity in the report to minimize impact on disk space.</p> <p>"Report as much information as possible" will provide more information about plugin activity in the report.</p>
Show missing patches that have been superseded	Enabled	This option allows you to configure Nessus to include or remove superseded patch information in the scan report. This option is off by default, except for policies created using the Internal PCI Network Scan template in the Policy Library.
Hide results from plugins initiated as a dependency	Enabled	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.
Output		
Allow users to edit scan results	Enabled	This feature allows users to delete items from the report when checked. When performing a scan for regulatory compliance or other types of audits, uncheck this to show that the scan was not tampered with.
Designate hosts by their DNS name	Disabled	Use the host name rather than IP address for report output.
Display hosts that respond to ping	Disabled	Select this option to specifically report on the ability to successfully ping a remote host.
Display unreachable hosts	Disabled	If this option is selected, hosts that did not reply to the ping request will be included in the security report as dead hosts.

Advanced

The **Advanced** section contains a wide variety of configuration options to offer more granular control of how the scanner operates.

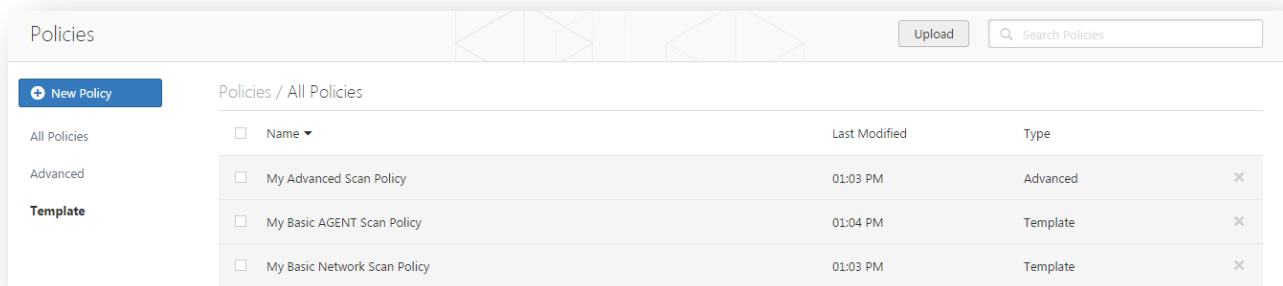
The screenshot shows the 'Settings / Advanced' window in Nessus. It is divided into three sections: General Settings, Performance Options, and Debug Settings. Under General Settings, 'Enable safe checks' is checked, while 'Stop scanning hosts that become unresponsive during the scan' and 'Scan IP addresses in a random order' are unchecked. Under Performance Options, 'Slow down the scan when network congestion is detected' is unchecked, and several numeric input fields are set to 5. Under Debug Settings, both 'Log scan details to server' and 'Enable plugin debugging' are unchecked. At the bottom are 'Save' and 'Cancel' buttons.

Settings / Advanced	
General Settings	
<input checked="" type="checkbox"/> Enable safe checks	
<input type="checkbox"/> Stop scanning hosts that become unresponsive during the scan	
<input type="checkbox"/> Scan IP addresses in a random order	
Performance Options	
<input type="checkbox"/> Slow down the scan when network congestion is detected	
Network timeout (in seconds)	5
Max simultaneous checks per host	5
Max simultaneous hosts per scan	5
Max number of concurrent TCP sessions per host	
Max number of concurrent TCP sessions per scan	
Debug Settings	
<input type="checkbox"/> Log scan details to server <small>Logs the start and finish time for each plugin used during a scan to nessusd.messages.</small>	
<input type="checkbox"/> Enable plugin debugging <small>Attaches available debug logs from plugins to the vulnerability output of this scan.</small>	
Save	Cancel

Option	Default	Description
General Settings		
Enable Safe Checks	Enabled	Enable Safe Checks disables all plugins that may have an adverse effect on the remote host.
Stop scanning hosts that become unresponsive during the scan	Disabled	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.
Scan IP addresses in a random order	Disabled	<p>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.</p> <p>Before July 2013, this option worked on a per-subnet basis. This feature has since been enhanced to randomize across the entire target IP space.</p>
Performance		
Slow down the scan when network congestion is detected	Disabled	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.
Network timeout (in seconds)	5	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 checks per host	5	This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time.
Max simultaneous hosts per scan	5	This setting limits the maximum number of hosts that a Nessus scanner will scan at the same time.
Max number of concurrent TCP sessions per host	none	This setting limits the maximum number of established TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner will eventually send (e.g., if this option is set to 15, the SYN scanner will send 1500 packets per second at most).
Max number of concurrent TCP sessions per scan	none	This setting limits the maximum number of established TCP sessions for the entire scan, regardless of the number of hosts being scanned. For Nessus scanners installed on Windows XP, Vista, 7, and 8 hosts, this value must be set to 19 or less to get accurate results.
Debug Settings		
Log scan details to server	Disabled	Logs the start and finish time for each plugin used during a scan to nessusd.messages.
Enable plugin debugging	Disabled	Attaches available debug logs from plugins to the vulnerability output of this scan

To view your policies, click on the **Policies** link from the Nessus home page.



Scan > Credentials (Basic Network Scan Example)



Agent Templates share many of same settings and options as the other **Scanner** and **Policy Templates**. However, the **Agent Templates** do not include the **Credentials** page.

By using **Credentials**, the Nessus scanner can be granted local access to scan the target system without requiring an agent. This can facilitate scanning of a very large network to determine local exposures or compliance violations. As noted, some steps of policy creation may be optional. Once created, the policy will be saved with recommended settings. You can edit the wizard options or any other aspect of the policy at any time.

There are several forms of authentication supported including but not limited to databases, SSH, Windows, network devices, patch management servers, and various plaintext authentication protocols. For example, Nessus leverages the ability to log into remote Unix hosts via Secure Shell (SSH); and with Windows hosts, Nessus leverages a variety of Microsoft authentication technologies.

Note that Nessus also uses the Simple Network Management Protocol (SNMP) to make version and information queries to routers and switches. In addition to operating system credentials, Nessus supports other forms of local authentication.

In Nessus 6.4, the following types of credentials are managed in the **Credentials** section of the policy:

- Database, which includes MongoDB, Oracle, MySQL, DB2, PostgreSQL, and SQL Server
- Rackspace, Cloud Services, which includes Amazon Web Services (AWS) and Salesforce.com
- Host, which includes Windows logins, SSH, and SNMPv3
- Mobile Device Management
- Patch Management servers
- VMware, Red Hat Enterprise Virtualization (RHEV), IBM iSeries, Palo Alto Networks PAN-OS, and directory services (ADSI and X.509)
- Plaintext authentication mechanism including FTP, HTTP, POP3, and other services



Credentialed scans can perform any operation that a local user can perform. The level of scanning is dependent on the privileges granted to the user account that Nessus is configured to use. The more privileges the scanner has via the login account (e.g., root or administrator access), the more thorough the scan results.

Nessus allows multiple credentials in the same policy. To add credentials, click the addition sign for the appropriate type of credential. Nessus will accept an unlimited number of some types of credentials; these are marked with an infinity sign ∞ . Other credential types will display a numeric value indicating the remaining number of credentials of that type that can be added to the policy.

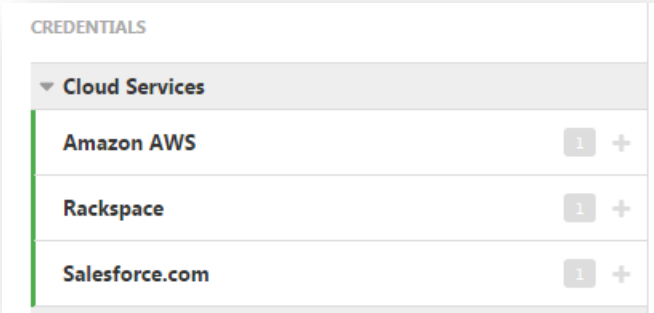
The **Credentials** tab, pictured below, allows you to configure the Nessus scanner to use authentication credentials during scanning. By configuring credentials, it allows Nessus to perform a wider variety of checks that result in more accurate scan results.



Please note that Nessus will open several concurrent authenticated connections to carry out credentialed auditing to ensure it is done in a timely fashion. Ensure that the host being audited does not have a strict account lockout policy based on concurrent sessions.

Cloud Services

Nessus supports three **Cloud Services**: Amazon AWS, Rackspace, and Salesforce.com.



Amazon AWS

Users can select **Amazon AWS** from the **Credentials** menu and enter credentials for compliance auditing an account in AWS.

A screenshot of the "Amazon AWS" credential entry form. It contains two input fields: "AWS Access Key ID" and "AWS Secret Key". Each field has a "REQUIRED" label to its right, indicating that these fields are mandatory for completion.

Option	Description
AWS Access Key ID	The AWS access key ID string.
AWS Secret Key	AWS secret key that provides the authentication for AWS Access Key ID.

Amazon AWS Global Settings

Global Settings

Regions to access

Rest of the World

Credentials for the China (Beijing) Region cannot be used to access other regions, and vice versa.

us-east-1

☐

us-west-1

☐

us-west-2

☐

eu-west-1

☐

ap-northeast-1

☐

ap-southeast-1

☐

ap-southeast-2

☐

sa-east-1

☐

us-gov-west-1

☐

HTTPS

☒

Verify SSL Certificate

☒

Option	Default	Description
Regions to access	Rest of the World	<div>In order for Nessus to audit an Amazon AWS account, you must define the regions you want to scan. Per Amazon policy, you will need different credentials to audit account configuration for the China region than you will for the Rest of the World. Choosing the Rest of the World will open the following choices:</div> <ul style="list-style-type: none">us-east-1us-west-1us-west-2eu-west-1ap-northeast-1ap-southeast-1ap-southeast-2sa-east-1us-gov-west-1
HTTPS	Enabled	Use HTTPS to access Amazon AWS.
Verify SSL Certificate	Enabled	Verify the validity of the SSL digital certificate.

Please see the [Nessus Compliance Checks](#) document, under the Amazon AWS Compliance Capability section for how to configure permissions correctly.

Rackspace

Rackspace

Username

REQUIRED

Password or API Key

REQUIRED

Authentication Method

API-Key

Global Settings

Dallas-Fort Worth (DFW)

☒

Chicago (ORD)

☒

Northern Virginia (IAD)

☒

London (LON)

☒

Sydney (SYD)

☒

Hong Kong (HKG)

☒

Option	Description
Username	Username required to log in
Password or API Keys	Password or API keys associated with the username
Authentication Method	Specify Password or API-Key from the drop-down
Global Settings	Location of Rackspace Cloud instance.

Salesforce.com

Users can select Salesforce.com from the Credentials menu. This allows Nessus to log in to Salesforce.com as the specified user to perform compliance audits.

▼ Salesforce.com

Username

REQUIRED

Password

REQUIRED

Option	Description
Username	Username required to log in to Salesforce.com
Password	Password associated with the Salesforce.com username

Database

CREDENTIALS

▼ Database

Database

∞ +

MongoDB

1 +

Nessus supports Database authentication using PostgreSQL, DB2, MySQL SQL Server, Oracle, and MongoDB.

▼ Database

Username

dba

REQUIRED

Password

Database Type

Oracle

PostgreSQL

DB2

MySQL

SQL Server

Oracle

Database Port

Auth type

SID

The **Database** credential menu is used to specify credentials, the type of database to be tested, and other relevant settings. Note that some options will appear based on your selections.

All databases will have a username and password.

Option	Description
Username	The username for the database.
Password	The password for the supplied username.
Database Type	Nessus supports Oracle, SQL Server, MySQL, DB2, Informix/DRDA, and PostgreSQL.

Oracle

Option	Default	Description
Database Port	1521	Port the database listens on.
Auth Type	SYSDBA	NORMAL, SYSOPER, and SYSDBA are supported.
SID	none	Oracle system ID that identifies a specific database.

PostgreSQL

Option	Default	Description
Database Port	5432	Port the database listens on.
Database Name	none	

DB2

Option	Default	Description
Database Port	50000	Port the database listens on.
Database Name	none	Name of the database, which is a required field.

MySQL

Option	Default	Description
Database Port	3306	Port the database listens on.

SQL Server

Option	Default	Description
Database Port	1433	Port the database listens on.
Auth Type	Windows	Windows authentication or SQL Server authentication are supported.
Instance Name	none	Name of the SQL Server instance for auditing.

MongoDB

Option	Description
Username	The username for the database.
Password	The password for the supplied username.
Database	Name of the database to audit.
Port	Port the database listens on.

Host

Nessus supports three forms of host authentication: **Windows**, **SNMPv3**, and **Secure Shell (SSH)**.

Windows

The “**Windows credentials**” menu item has settings to provide Nessus with information such as SMB account name, password, and domain name. Nessus supports several different types of authentication methods for Windows-based systems:

- The Lanman authentication method was prevalent on Windows NT and early Windows 2000 server deployments; it is retained for backward compatibility.
- The NTLM authentication method, introduced with Windows NT, provided improved security over Lanman authentication. The enhanced version, NTLMv2, is cryptographically more secure than NTLM and is the default authentication method chosen by Nessus when attempting to log into a Windows server. NTLMv2 can make use of SMB Signing.
- SMB signing is a cryptographic checksum applied to all SMB traffic to and from a Windows server. Many system administrators enable this feature on their servers to ensure that remote users are 100% authenticated and part of a domain. In addition, make sure you enforce a policy that mandates the use of strong passwords that cannot be easily broken via dictionary attacks from tools like John the Ripper and L0phtCrack. It is automatically used by Nessus if it is required by the remote Windows server. Note that there have been many different types of attacks against Windows security to illicit hashes from computers for re-use in attacking servers. SMB Signing adds a layer of security to prevent these man-in-the-middle attacks.
- The SPNEGO (Simple and Protected Negotiate) protocol provides Single Sign On (SSO) capability from a Windows client to a variety of protected resources via the users’ Windows login credentials. Nessus supports use of SPNEGO

with either NTLMSSP with LMv2 authentication or Kerberos and RC4 encryption. SPNEGO authentication happens through NTLM or Kerberos authentication; nothing needs to be configured in the Nessus policy.

- If an extended security scheme (such as Kerberos or SPNEGO) is not supported or fails, Nessus will attempt to log in via NTLMSSP/LMv2 authentication. If that fails, Nessus will then attempt to log in using NTLM authentication.
- Nessus also supports the use of Kerberos authentication in a Windows domain. To configure this, the IP address of the Kerberos Domain Controller (actually, the IP address of the Windows Active Directory Server) must be provided.

Server Message Block (SMB) is a file-sharing protocol that allows computers to share information 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.

The SMB domain field is optional and Nessus will be able to log on with domain credentials without this field. The username, password, and optional domain refer to an account that the target machine is aware of. For example, given a username of `joesmith` and a password of `my4x4mpl3`, a Windows server first looks for this username in the local system's list of users, and then determines if it is part of a domain.

Regardless of credentials used, Nessus always attempts to log into a Windows server with the following combinations:

- Administrator without a password
- A random username and password to test Guest accounts
- No username or password to test null sessions

The actual domain name is only required if an account name is different on the domain from that on the computer. It is entirely possible to have an Administrator account on a Windows server and within the domain. In this case, to log onto the local server, the username of Administrator is used with the password of that account. To log onto the domain, the Administrator username would also be used, but with the domain password and the name of the domain.



When multiple SMB accounts are configured, Nessus will try to log in with the supplied credentials sequentially. Once Nessus is able to authenticate with a set of credentials, it will check subsequent credentials supplied, but only use them if administrative privileges are granted when previous accounts provided user access.

Some versions of Windows allow you to create a new account and designate it as an administrator. These accounts are not always suitable for performing credentialed scans. Tenable recommends that the original administrative account, named Administrator be used for credentialed scanning to ensure full access is permitted. On some versions of Windows, this account may be hidden. The real administrator account can be unhidden by running a DOS prompt with administrative privileges and typing the following command:

```
C:\> net user administrator /active:yes
```

If an SMB account is created with limited administrator privileges, Nessus can easily and securely scan multiple domains. Tenable recommends that network administrators consider creating specific domain accounts to facilitate testing. Nessus includes a variety of security checks for Windows Vista, Windows 7, Windows 8, Windows 2008, Windows 2008 R2, Windows 2012, and Windows 2012 R2 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. This service must be started for a Nessus credentialed scan to fully audit a system using credentials.

Credentialed scans on Windows systems require that a full administrator level account be used. Several bulletins and software updates by Microsoft have made reading the registry to determine software patch level unreliable without administrator privileges, but not all of them. Nessus plugins will check that the provided credentials have full administrative access to ensure they execute properly. For example, full administrative access is required to perform direct reading of the file system. This allows Nessus to attach to a computer and perform direct file analysis to determine the true patch level of the systems being evaluated.

Windows

Authentication method: Password

Username: administrator REQUIRED

Password: REQUIRED

Domain:

Option	Description
Windows Authentication Methods	Options: Password, CyberArk, Kerberos, LM Hash, and NTLM Hash
Username	The target system's username.
Password	Password of the username specified.
Domain	The Windows domain of the specified user's name.

Global Settings

Global Settings

☒ Never send credentials in the clear

☒ Do not use NTLMv1 authentication

☐ Start the Remote Registry service during the scan

☐ Enable administrative shares during the scan



Option	Default	Description
Never send credentials in the clear	Enabled	For security reasons, Windows credentials are not sent in the clear by default.
Do not use NTLMv1 authentication	Enabled	If the Do not use NTLMv1 authentication option is disabled, then it is theoretically possible to trick Nessus into attempting to log into a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a hash obtained from Nessus. This hash can be potentially cracked to reveal a username or password. It may also be used to directly log into other servers. Force Nessus to use NTLMv2 by enabling the Only use NTLMv2 setting at scan time. This prevents a hostile Windows server from using NTLM and receiving a hash. Because NTLMv1 is an insecure protocol this option is enabled by default.
Start the Remote Registry service during the scan	Disabled	This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Nessus to execute some Windows local check plugins.
Enable administrative shares during the scan	Disabled	This option will allow Nessus to access certain registry entries that can be read with administrator privileges.

CyberArk

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Nessus can get credentials from CyberArk to use in a scan.

The screenshot shows a configuration window titled "Windows" with a dropdown menu set to "CyberArk Vault". The form includes the following fields and options:

- Authentication method:** CyberArk Vault (selected from a dropdown)
- Username:** administrator (text input, marked as REQUIRED)
- Domain:** (empty text input)
- Central Credential Provider Host:** vault_host.yourcompany.com (text input, marked as REQUIRED)
- Central Credential Provider Port:** 443 (text input, marked as REQUIRED)
- Vault Username (optional):** (empty text input)
- Vault Password (optional):** (empty text input)
- Safe:** (empty text input, marked as REQUIRED)
- AppId:** (empty text input, marked as REQUIRED)
- Folder:** (empty text input, marked as REQUIRED)
- PolicyId:** (empty text input)
- Use SSL:** ☒
- Verify SSL Certificate:** ☒

Option	Description
Username	The target system's username.
Domain	This is an optional field if the above username is part of a domain.
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.
Central Credential Provider Port	The port the CyberArk Central Credential Provider is listening on.
Vault Username (optional)	If the CyberArk Central Credential Provider is configured to use basic authentication you can fill in this field for authentication.
Valut Password (optional)	If the CyberArk Central Credential Provider is configured to use basic authentication you can fill in this field for authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contained the authentication information you would like to retrieve.

Appld	The Appld that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.
PolicyId	The PolicyID assigned to the credentials you would like to retrieve from the CyberArk Central Credential Provider.
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.

Kerberos

The screenshot shows a 'Windows' configuration window with the following fields and values:

- Authentication method:** Kerberos (selected from a dropdown)
- Username:** administrator (with a 'REQUIRED' label)
- Password:** (empty field with a 'REQUIRED' label)
- Key Distribution Center (KDC):** kdc.example.com (with a 'REQUIRED' label)
- KDC Port:** 88
- KDC Transport:** tcp (selected from a dropdown)
- Domain:** (empty field with a 'REQUIRED' label)

Option	Default	Description
Password	none	Like with other credentials methods, this is the user password on the target system. This is a required field.
Key Distribution Center (KDC)	none	This host supplies the session tickets for the user. This is a required field.
KDC Port	88	This option can be set to direct Nessus to connect to the KDC if it is running on a port other than 88.
KDC Transport	TCP	Note that if you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.
Domain	none	The Windows domain that the KDC administers. This is a required field.

LM Hash

▼

Windows

Authentication method

LM Hash

▼

Username

administrator

REQUIRED

Hash

REQUIRED

Domain

Option	Default	Description
Username	none	The target system's username.
Hash	none	Hash being utilized.
Domain	none	The Windows domain of the specified user's name.

NTLM Hash

▼

Windows

Authentication method

NTLM Hash

▼

Username

administrator

REQUIRED

Hash

REQUIRED

Domain

Option	Default	Description
Username	none	The target system's username.
Hash	none	Hash being utilized.
Domain	none	The Windows domain of the specified user's name.

For details on how to set up a Windows system for local checks, see [Appendix A – Setting up Credentialed Checks on Windows Platforms](#).

SNMPv3

Users can select **SNMPv3 settings** from the **Credentials** menu and enter credentials for scanning systems using an encrypted network management protocol.

These credentials are used to obtain local information from remote systems, including network devices, for patch auditing or compliance checks. There is a field for entering the SNMPv3 user name for the account that will perform the checks on the target system, along with the SNMPv3 port, security level, authentication algorithm and password, and privacy algorithm and password.

If Nessus is unable to determine the community string or password, it may not perform a full audit of the service.

▼

SNMPv3

Username

REQUIRED

Port

161

Security Level

Authentication and privacy

▼

Authentication algorithm

SHA1

▼

Authentication password

REQUIRED

Privacy algorithm

AES

▼

Privacy password

REQUIRED

Option	Description
Username	The username for a SNMPv3 based account.
Port	Direct Nessus to scan a different port if SNMP is running on a port other than 161.
Security level	Select the security level for SNMP: authentication, privacy, or both.
Authentication algorithm	Select MD5 or SHA1 based on which algorithm the remote service supports.
Authentication password	The password for the username specified.
Privacy algorithm	The encryption algorithm to use for SNMP traffic.
Privacy password	A password used to protect encrypted SNMP communication.

SSH

On Unix systems and supported network devices, Nessus uses Secure Shell (SSH) protocol version 2 based programs (e.g., OpenSSH, Solaris SSH, etc.) for host-based checks.

This mechanism encrypts the data in transit to protect it from being viewed by sniffer programs. Nessus supports five types of authentication methods for use with SSH: username and password, public/private keys, digital certificates, and Kerberos.

- Public Key

- Certificate
- CyberArk Vault
- Kerberos
- Password

Users can select **SSH settings** from the **Credentials** 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.



Non-privileged users with local access on Unix systems can determine basic security issues, such as patch levels or entries in the `/etc/passwd` file. For more comprehensive information, such as system configuration data or file permissions across the entire system, an account with root privileges is required.

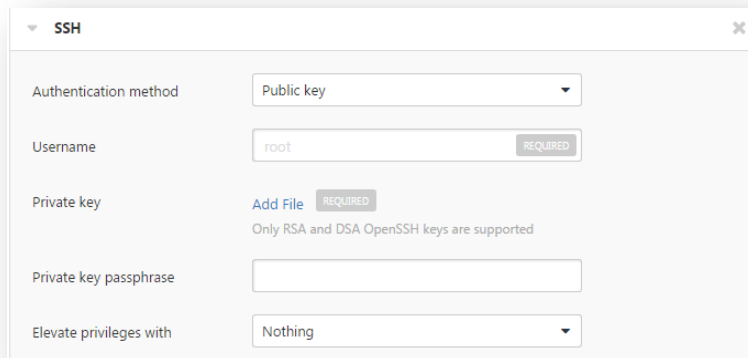
Global Settings

There are three **Global Settings** for SSH credentials that apply to all SSH Authentication methods.

The screenshot shows a 'Global Settings' dialog box. It has three sections: 'known_hosts file' with an 'Add File' link, 'Preferred port' with a text input field containing '22', and 'Client version' with a text input field containing 'OpenSSH_5.0'.

Option	Default	Description
known_hosts file	none	If an SSH known_hosts file is available and provided as part of the Global Settings of the scan policy in the known_hosts file field, 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 log into a system that may not be under your control.
Preferred port	22	This option can be set to direct Nessus to connect to SSH if it is running on a port other than 22.
Client version	OpenSSH_5.0	Specifies which type of SSH client Nessus will impersonate while scanning.

Public Key Encryption



Public Key Encryption, also referred to as asymmetric key encryption, provides a more secure authentication mechanism by the use of a public and private key pair. In asymmetric cryptography, the public key is used to encrypt data and the private key is used to decrypt it. The use of public and private keys is a more secure and flexible method for SSH authentication. Nessus supports both DSA and RSA key formats.

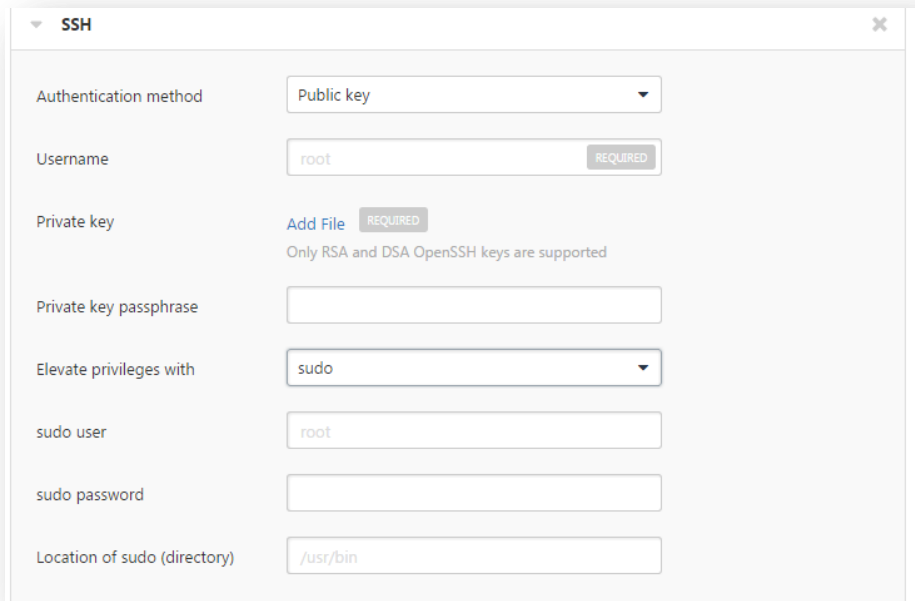
Like **Public Key Encryption**, Nessus supports RSA and DSA OpenSSH certificates. Nessus also requires the user certificate, which is signed by a Certificate Authority (CA), and the user's private key.



Nessus supports the OpenSSH SSH public key format. Formats from other SSH applications, including PuTTY and SSH Communications Security, must be converted to OpenSSH public key format.

The most effective credentialed scans are when the supplied credentials have root privileges. Since many sites do not permit a remote login as root, Nessus can invoke **su**, **sudo**, **su+sudo**, **dzdo**, **.k5login**, or **pbrun** with a separate password for an account that has been set up to have **su** or **sudo** privileges. In addition, Nessus can escalate privileges on Cisco devices by selecting **Cisco 'enable'** or **.k5login** for Kerberos logins. SSH Kerberos authentication is covered later in this section.

The figure below illustrates configuring **sudo** in conjunction with SSH keys 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 SSH keys correspond with keys generated for the audit account:

The image shows a screenshot of the 'SSH' configuration window in Nessus. The window has a title bar with a close button. Inside, there are several fields and a dropdown menu. The 'Authentication method' is set to 'Public key'. The 'Username' field contains 'root' and has a 'REQUIRED' label. The 'Private key' field has an 'Add File' button and a 'REQUIRED' label, with a note below it stating 'Only RSA and DSA OpenSSH keys are supported'. The 'Private key passphrase' field is empty. The 'Elevate privileges with' dropdown is set to 'sudo'. The 'sudo user' field contains 'root'. The 'sudo password' field is empty. The 'Location of sudo (directory)' field contains '/usr/bin'.

Nessus supports the `blowfish-cbc`, `aes-cbc`, and `aes-ctr` cipher algorithms. Some commercial variants of SSH do not have support for the blowfish algorithm, possibly for export reasons. It is also possible to configure an SSH server to only accept certain types of encryption. Check your SSH server to ensure the correct algorithm is supported.

Nessus encrypts all passwords stored in policies. However, the use of SSH keys for authentication rather than SSH passwords is recommended. This helps ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log in to a system that may not be under your control.



For supported network devices, Nessus will only support the network device's username and password for SSH connections.

If an account other than `root` must be used for privilege escalation, it can be specified under the **Escalation account** with the **Escalation password**.

Certificate

SSH

Authentication method

Certificate

Username

root

REQUIRED

User certificate

Add File

REQUIRED

Only RSA and DSA OpenSSH certificates are supported

Private key

Add File

REQUIRED

Only RSA and DSA OpenSSH keys are supported

Private key passphrase

Elevate privileges with

Nothing

Option	Description
Username	Username of the account which is being used for authentication on the host system.
User Certificate	RSA or DSA Open SSH certificate file of the user.
Private Key	RSA or DSA Open SSH key file of the user.
Private key passphrase	Passphrase of the Private Key.
Elevate privileges with	Allows for increasing privileges once authenticated.

CyberArk

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Nessus can get credentials from CyberArk to use in a scan.

SSH

Authentication method

CyberArk Vault

Username

root

REQUIRED

Central Credential Provider Host

vault_host.yourcompany.com

REQUIRED

Central Credential Provider Port

443

REQUIRED

Vault Username (optional)

Vault Password (optional)

Safe

REQUIRED

AppId

REQUIRED

Folder

REQUIRED

PolicyId

Use SSL

☒

Verify SSL Certificate

☒

Option	Description
Username	The target system's username.
Domain	This is an optional field if the above username is part of a domain.
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.
Central Credential Provider Port	The port the CyberArk Central Credential Provider is listening on.
Vault Username (optional)	If the CyberArk Central Credential Provider is configured to use basic authentication you can fill in this field for authentication.
Vault Password (optional)	If the CyberArk Central Credential Provider is configured to use basic authentication you can fill in this field for authentication.

Safe	The safe on the CyberArk Central Credential Provider server that contained the authentication information you would like to retrieve.
Appld	The Appld that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.
PolicyId	The PolicyID assigned to the credentials you would like to retrieve from the CyberArk Central Credential Provider.
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.

Kerberos

Kerberos, developed by MIT's Project Athena, is a client/server application that uses a symmetric key encryption protocol. In symmetric encryption, the key used to encrypt the data is the same as the key used to decrypt the data. Organizations deploy a KDC (Key Distribution Center) that contains all users and services that require Kerberos authentication. Users authenticate to Kerberos by requesting a TGT (Ticket Granting Ticket). Once a user is granted a TGT, it can be used to request service tickets from the KDC to be able to utilize other Kerberos based services. Kerberos uses the CBC (Cipher Block Chain) DES encryption protocol to encrypt all communications.



Note that you must already have a Kerberos environment established to use this method of authentication.

The Nessus implementation of Unix-based Kerberos authentication for SSH supports the aes-cbc and aes-ctr encryption algorithms. An overview of how Nessus interacts with Kerberos is as follows:

- End-user gives the IP of the KDC
- **nessusd** asks **sshd** if it supports Kerberos authentication
- **sshd** says yes
- **nessusd** requests a Kerberos TGT, along with login and password
- Kerberos sends a ticket back to **nessusd**
- **nessusd** gives the ticket to **sshd**
- **nessusd** is logged in



In both Windows and SSH credentials settings, you can specify credentials using Kerberos keys from a remote system. Note that there are differences in the configurations for Windows and SSH.

SSH

Authentication method

Kerberos

Username

root

REQUIRED

Password

REQUIRED

Key Distribution Center (KDC)

kdc.example.com

REQUIRED

KDC Port

88

KDC Transport

tcp

Realm

EXAMPLE.COM

REQUIRED

Elevate privileges with

Nothing

Option	Description
Username	The target system's username.
Password	Password of the username specified.
Key Distribution Center (KDC)	This host supplies the session tickets for the user.
KDC Port	This option can be set to direct Nessus to connect to the KDC if it is running on a port other than 88.
KDC Transport	The KDC uses TCP by default in Unix implementations. For UDP, change this option. Note that if you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.
Realm	The Realm is the authentication domain, usually noted as the domain name of the target (e.g., example.com).
Elevate privileges with	Allows for increasing privileges once authenticated.

If Kerberos is used, `sshd` must be configured with Kerberos support to verify the ticket with the KDC. Reverse DNS lookups must be properly configured for this to work. The Kerberos interaction method must be `gssapi-with-mic`.

Password

SSH

Authentication method

Password

Username

root

REQUIRED

Password (unsafe!)

REQUIRED

This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.

Elevate privileges with

Nothing

Option	Description
Username	The target system’s username.
Password	Password of the username specified.
Elevate privileges with	Allows for increasing privileges once authenticated.

Miscellaneous

Miscellaneous

ADSI	5	+
IBM iSeries	1	+
Palo Alto Networks PAN-OS	1	+
RHEV	1	+
VMware ESX SOAP API	1	+
VMware vCenter SOAP API	1	+
X.509	1	+

ADSI

ADSI requires the domain controller information, domain, and domain admin and password:

ADSI

Domain Controller

REQUIRED

Domain

REQUIRED

Domain Admin

REQUIRED

Domain Password

REQUIRED

“ADSI allows Nessus to query an ActiveSync server to determine if any Android or iOS-based devices are connected. Using the credentials and server information, Nessus authenticates to the domain controller (not the Exchange server) to directly query it for device information. This feature does not require any ports be specified in the scan policy. These settings are required for mobile device scanning.

Option	Description
Domain Controller	Name of the domain controller for ActiveSync
Domain	Name of the Windows domain for ActiveSync
Domain Admin	Domain admin’s username
Domain Password	Domain admin’s password



Nessus supports obtaining the mobile information from Exchange Server 2010 and 2013 only; Nessus cannot retrieve information from Exchange Server 2007.

IBM iSeries

IBM iSeries only requires an iSeries username and password:

IBM iSeries

Username

REQUIRED

Password

REQUIRED

Palo Alto Networks PAN-OS

Palo Alto Networks PAN-OS requires a PAN-OS username and password as well as the management port. Additionally, you can verify the SSL certificate:

▼ Palo Alto Networks PAN-OS

Username

REQUIRED

Password

REQUIRED

Port

443

HTTPS

Verify SSL Certificate

RHEV (Red Hat Enterprise Virtualization)

RHEV requires username, password, and network port. Additionally, you can provide verification for the SSL certificate:

▼ RHEV

Username

REQUIRED

Password

REQUIRED

Port

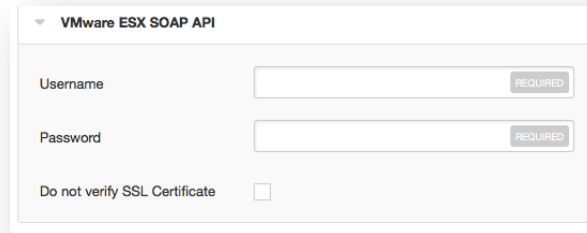
443

Verify SSL Certificate

Credential	Default	Description
Username	none	Username to login to the RHEV server. This is a required field.
Password	none	Username to the password to login to the RHEV server. This is a required field.
Port	443	Port to connect to the RHEV server.
Verify SSL Certificate	Enabled	Verify that the SSL certificate for the RHEV server is valid.

VMware ESX SOAP API

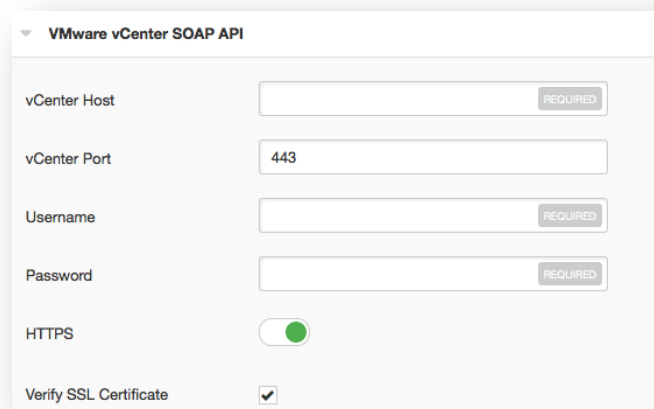
Access to VMware servers is available through its native SOAP API. VMware ESX SOAP API allows you to access the ESX and ESXi servers via username and password. Additionally, you have the option of not enabling SSL certificate verification:

A screenshot of a web form titled "VMware ESX SOAP API". It contains three input fields: "Username" and "Password", both marked as "REQUIRED" with a small button next to them. Below these is a checkbox labeled "Do not verify SSL Certificate" which is currently unchecked.

Credential	Default	Description
Username	none	Username to login to the ESXi server. This is a required field.
Password	none	Username to the password to login to the ESXi server. This is a required field.
Do not verify SSL Certificate	Disabled	Do not verify that the SSL certificate for the ESXi server is valid.

VMware vCenter SOAP API

VMware vCenter SOAP API allows you to access vCenter. This requires a username, password, vCenter hostname, and vCenter port. Additionally, you can require HTTPS and SSL certificate verification:

A screenshot of a web form titled "VMware vCenter SOAP API". It contains five input fields: "vCenter Host" (REQUIRED), "vCenter Port" (pre-filled with "443"), "Username" (REQUIRED), and "Password" (REQUIRED). Below these is a toggle switch for "HTTPS" which is currently turned on (green), and a checkbox for "Verify SSL Certificate" which is checked.

Credential	Default	Description
vCenter Host	none	Name of the vCenter host. This is a required field.
vCenter Port	443	Port to access the vCenter host.
Username	none	Username to login to the vCenter server. This is a required field.
Password	none	Username to the password to login to the vCenter server. This is a required field.
HTTPS	Enabled	Connect to the vCenter via SSL.
Verify SSL Certificate	Enabled	Verify that the SSL certificate for the ESXi server is valid.



Note that by default, local ESXi users are limited to Read-only roles. Using such an account will result in a 21745 error. Either an administrative account or one with Global -> Settings permission must be used to facilitate this audit. Credentials for the ESX SOAP API can be supplied when creating a new policy.

X.509

For X.509, you will need to supply the client certificate, client private key and its corresponding passphrase, and the trusted Certificate Authority's (CA) digital certificate:

X.509

Client certificate [Add File](#) REQUIRED

Client key [Add File](#) REQUIRED

Password for key

CA certificate to trust [Add File](#) REQUIRED

Mobile

For **Apple Profile Manager API Settings**, **AirWatch API Settings**, **Good MDM Settings**, and **MobileIron** host devices do not need to be scanned directly to obtain information about them. The Nessus scanner must be able to reach the mobile device management (MDM) server to query it for information. When either of these options is configured, the scan policy does not require a target host to scan; you can target `localhost` and the policy will still reach out to the MDM server for information.

AirWatch

AirWatch allows Nessus to query the **AirWatch** API, using the specified credentials and API key, to gather information about the mobile devices it manages. This feature does not require any ports be specified in the scan policy. Optionally, communications over SSL can be specified, as well as verifying the SSL certificate.

AirWatch

AirWatch Environment API URL REQUIRED

Port

Username REQUIRED

Password REQUIRED

API Key REQUIRED

HTTPS ☒

Verify SSL Certificate ☒

Option	Default	Description
ArWatch Environment API URL	none	This is the URL for accessing the server's API. This is a required field.
Port	443	Default port for Nessus to communicate with AirWatch.
Username	none	Username for accessing AirWatch. This is a required field.
API Key	none	API key for accessing AirWatch. This is a required field.
HTTPS	Enabled	Access AirWatch over HTTPS instead of HTTP. This will encrypt the connection.
Verify SSL Certificate	Enabled	Verify that the SSL certificate is valid.

Apple Profile Manager

“**Apple Profile Manager** allows Nessus to query an Apple Profile Manager server to enumerate Apple iOS-based devices (e.g., iPhone, iPad) on the network. Using the credentials and server information, Nessus authenticates to the Profile Manager to directly query it for device information. Optionally, communications over SSL can be specified, as well as directing the server to force a device information update (i.e., each device will update its information with the Profile Manager server).

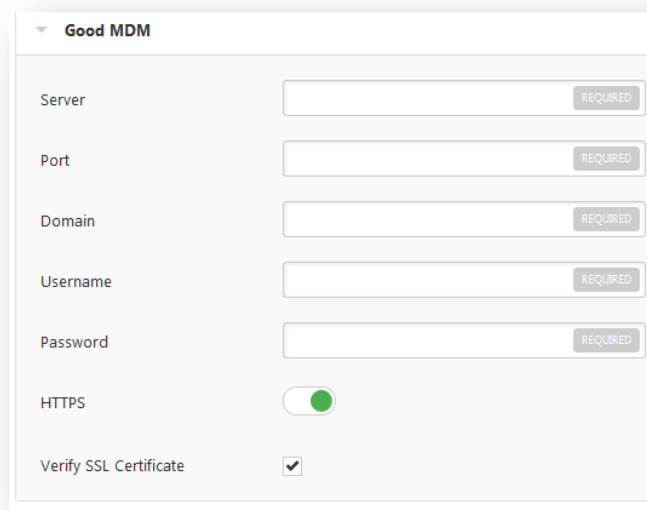
Option	Default	Description
Server	none	Name of Apple Profile Manager server. This is a required field.
Port	443	Default port for Nessus to check for Apple Profile Manager.
Username	none	Username for accessing Apple Profile Manager. This is a required field.
API Key	none	API key for accessing Apple Profile Manager. This is a required field.
HTTPS	Enabled	Access Apple Profile Manager over HTTPS instead of HTTP. This will encrypt the connection.
Verify SSL Certificate	Enabled	Verify that the SSL certificate is valid.

Global settings for the Apple Profile Manager are:

Option	Default	Description
Force Device Updates	Enabled	This forces the Apple Profile Manager to run updates.
Device update timeout (minutes)	5	This is the timeout value in minutes for the Apple Profile Manager to update.

Good MDM

“**Good MDM** allows Nessus to query a [Good](#) server to enumerate mobile devices on the network. Using the credentials and server information, Nessus authenticates to the Good server to directly query it for device information. Optionally, communications over SSL can be specified as well as strict SSL certificate verification.



Option	Default	Description
Server	none	Name of Good MDM server. This is a required field.
Port	none	Default port for Nessus to check for Good MDM.
Domain	none	Domain for Good MDM
Username	none	Username for accessing Apple Profile Manager. This is a required field.
Password	none	Password for the previously supplied username.
HTTPS	Enabled	Access Apple Profile Manager over HTTPS instead of HTTP. This will encrypt the connection.
Verify SSL Certificate	Enabled	Verify that the SSL certificate is valid.

MobileIron

“**MobileIron** allows Nessus to query a MobileIron server to enumerate any attached mobile devices (e.g., iPhone, iPad, HTC, BlackBerry, Android). Using the credentials and server information, Nessus uses authenticated API calls to query the server

for device information. Optionally, communications over SSL can be specified, as well as directing the server to verify the SSL certificate for enhanced security.

▼ MobileIron

MobileIron VSP Admin Portal URL

https://www.example.net/mifs/login.jsp

REQUIRED

MobileIron Port

443

Username

apiuser

REQUIRED

Password

REQUIRED

HTTPS

☒

Verify SSL Certificate

☒


Option	Default	Description
MobileIron VSP Admin Portal URL	none	URL for accessing the MobileIron VSP Admin Portal This is a required field.
Port	443	Default port for Nessus to check for MobileIron.
Username	none	Username for accessing MobileIron. This is a required field.
Password	none	Password for the previously supplied username.
HTTPS	Enabled	Access Apple Profile Manager over HTTPS instead of HTTP. This will encrypt the connection.
Verify SSL Certificate	Enabled	Verify that the SSL certificate is valid.

Patch Management

Nessus Manager and Nessus Cloud can leverage credentials for the Red Hat Network Satellite, IBM TEM, Dell KACE 1000, WSUS, and SCCM patch management systems to perform patch auditing on systems for which credentials may not be available to the Nessus scanner. Options for these patch management systems can be found under Credentials in their respective drop-down menus: Symantec Altiris, IBM Tivoli Endpoint Manager (BigFix), Red Hat Satellite Server, Microsoft SCCM, Dell KACE K1000, and Microsoft WSUS.



IT administrators are expected to manage the patch monitoring software and install any agents required by the patch management system on their systems.



Dell KACE K1000	1	+
IBM Tivoli Endpoint Manager (BigFix)	1	+
Microsoft SCCM	1	+
Microsoft WSUS	1	+
Red Hat Satellite Server	∞	+
Symantec Altiris	1	+

Dell KACE K1000

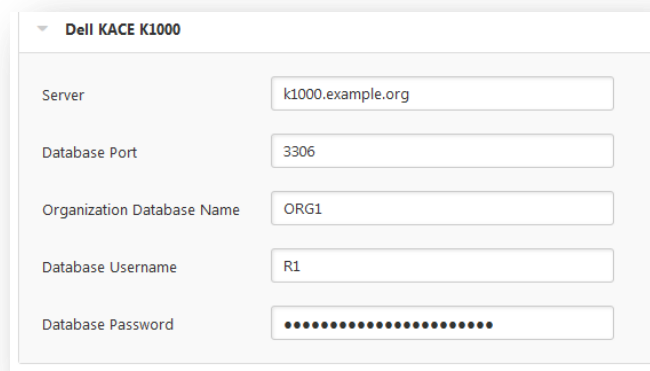
KACE K1000 is available from Dell to manage the distribution of updates and hotfixes for Linux, Windows, and Mac OS X systems. Nessus and SecurityCenter have the ability to query KACE K1000 to verify whether or not patches are installed on systems managed by KACE K1000 and display the patch information through the Nessus or SecurityCenter GUI.

- If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore KACE K1000 output.
- The data returned to Nessus by KACE K1000 is only as current as the most recent data that the KACE K1000 has obtained from its managed hosts.

KACE K1000 scanning is performed using four Nessus plugins:

- kace_k1000_get_computer_info.nbin (Plugin ID 76867)
- kace_k1000_get_missing_updates.nbin (Plugin ID 76868)
- kace_k1000_init_info.nbin (Plugin ID 76866)
- kace_k1000_report.nbin (Plugin ID 76869)

Credentials for the Dell KACE K1000 system must be provided for K1000 scanning to work properly. Under the **Credentials** tab, select **Patch Management** and then **Dell KACE K1000**:



▼ Dell KACE K1000	
Server	<input type="text" value="k1000.example.org"/>
Database Port	<input type="text" value="3306"/>
Organization Database Name	<input type="text" value="ORG1"/>
Database Username	<input type="text" value="R1"/>
Database Password	<input type="password" value="....."/>

Credential	Default	Description
Server	none	KACE K1000 IP address or system name. This is a required field.
Database Port	3306	Port the K1000 database is running on (typically TCP 3306).
Organization Database Name	ORG1	The name of the organization component for the KACE K1000 database. This component will begin with the letters ORG and end with a number that corresponds with the K1000 database username.
Database Username	none	Username required to log into the K1000 database. R1 is the default if no user is defined. The username will begin with the letter R. This username will end in the same number that represents the number of the organization to scan. This is a required field.
K1000 Database Password	none	Password required to authenticate the K1000 Database Username. This is a required field.

IBM Tivoli Endpoint Manager (BigFix)

Tivoli Endpoint Manager (TEM) is available from IBM to manage the distribution of updates and hotfixes for desktop systems. Nessus and SecurityCenter have the ability to query TEM to verify whether or not patches are installed on systems managed by TEM and display the patch information.

- If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore TEM output.
- The data returned to Nessus by TEM is only as current as the most recent data that the TEM server has obtained from its managed hosts.

TEM scanning is performed using five Nessus plugins:

- Patch Management: Tivoli Endpoint Manager Computer Info Initialization (Plugin ID 62559)
- Patch Management: Missing updates from Tivoli Endpoint Manager (Plugin ID 62560)
- Patch Management: IBM Tivoli Endpoint Manager Server Settings (Plugin ID 62558)
- Patch Management: Tivoli Endpoint Manager Report (Plugin ID 62561)
- Patch Management: Tivoli Endpoint Manager Get Installed Packages (Plugin ID 65703)

Credentials for the IBM Tivoli Endpoint Manager server must be provided for TEM scanning to work properly.

In the **Credentials** menu, select **Patch Management: IBM Tivoli Endpoint Manager Server (BigFix)** from the Plugin drop-down menu:

Credential	Default	Description
Web Reports Server	None	Name of IBM TEM Web Reports Server
Web Reports Port	none	Port that the IBM TEM Web Reports Server listens
Web Reports Username	none	Web Reports administrative username
Web Reports Password	none	Web Reports administrative username's password
HTTPS	Enabled	If the Web Reports service is using SSL
Verify SSL certificate	Enabled	Verify that the SSL certificate is valid

Package reporting is supported by RPM-based and Debian-based distributions that IBM TEM officially supports. This includes Red Hat derivatives such as RHEL, CentOS, Scientific Linux, and Oracle Linux, as well as Debian and Ubuntu. Other distributions may also work, but unless officially supported by TEM, there is no support available.

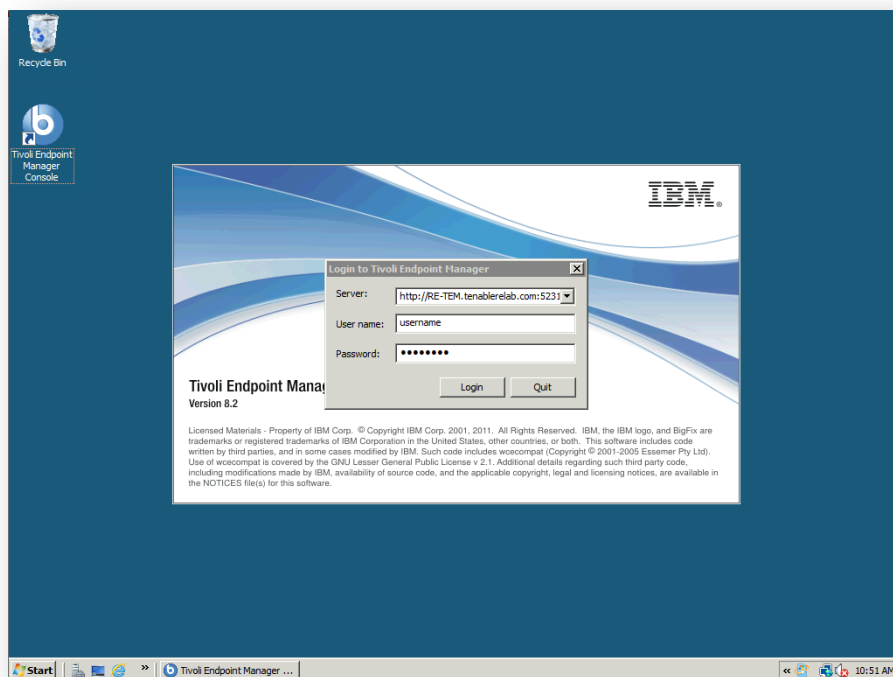
For local check plugins to trigger, only RHEL, CentOS, Scientific Linux, Oracle Linux, Debian, and Ubuntu are supported. The plugin Patch Management: Tivoli Endpoint Manager Get Installed Packages must be enabled.

In order to use these auditing features, changes must be made to the IBM TEM server. A custom Analysis must be imported into TEM so that detailed package information will be retrieved and made available to Nessus. This process is outlined below. Before beginning, the following text must be saved to a file on the TEM system, and named with a `.bes` extension:

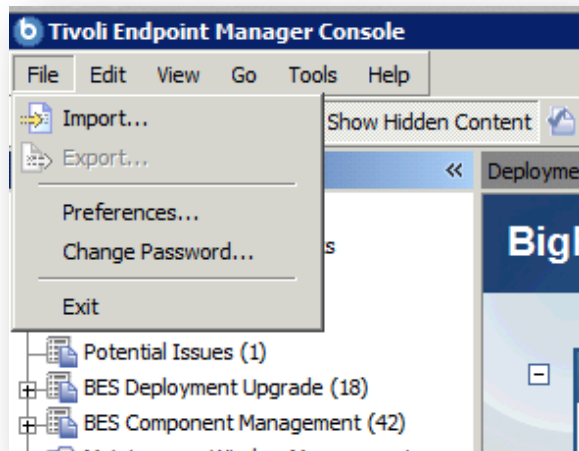
```
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="BES.xsd">
  <Analysis>
    <Title>Tenable</Title>
    <Description>This analysis provides Nessus with the data it needs for
vulnerability reporting. </Description>
    <Relevance>true</Relevance>
    <Source>Internal</Source>
    <SourceReleaseDate>2013-01-31</SourceReleaseDate>
    <MIMEField>
      <Name>x-fixlet-modification-time</Name>
      <Value>Fri, 01 Feb 2013 15:54:09 +0000</Value>
    </MIMEField>
    <Domain>BESC</Domain>
  </Analysis>
</BES>
```

```
<Property Name="Packages - With Versions (Tenable)" ID="1"><![CDATA[if
(exists true whose (if true then (exists debianpackage) else false)) then
unique values of (name of it & "|" & version of it as string & "|" & "deb" &
"|" & architecture of it & "|" & architecture of operating system) of packages
whose (exists version of it) of debianpackages else if (exists true whose (if
true then (exists rpm) else false)) then unique values of (name of it & "|" &
version of it as string & "|" & "rpm" & "|" & architecture of it & "|" &
architecture of operating system) of packages of rpm else "<unsupported>"
]]></Property>
</Analysis>
</BES>
```

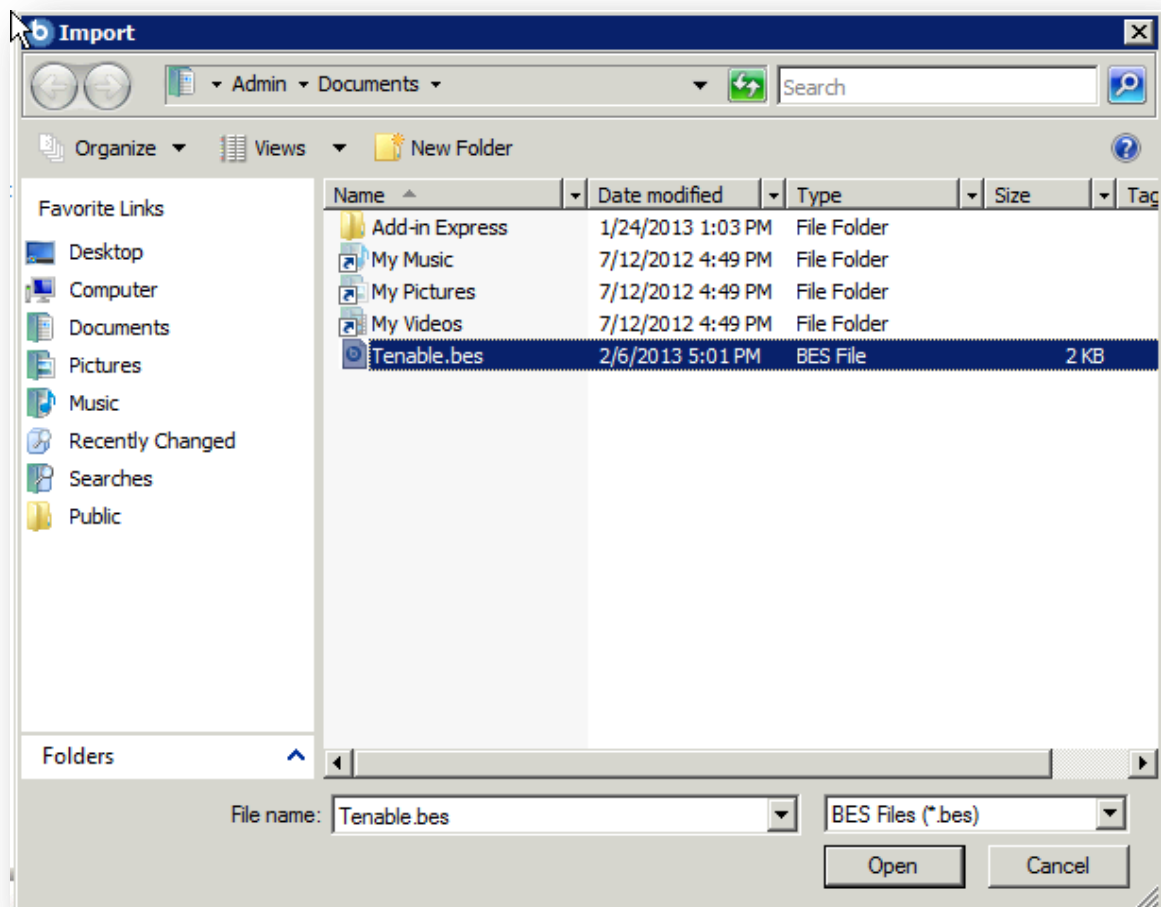
Open the TEM Console and log in:



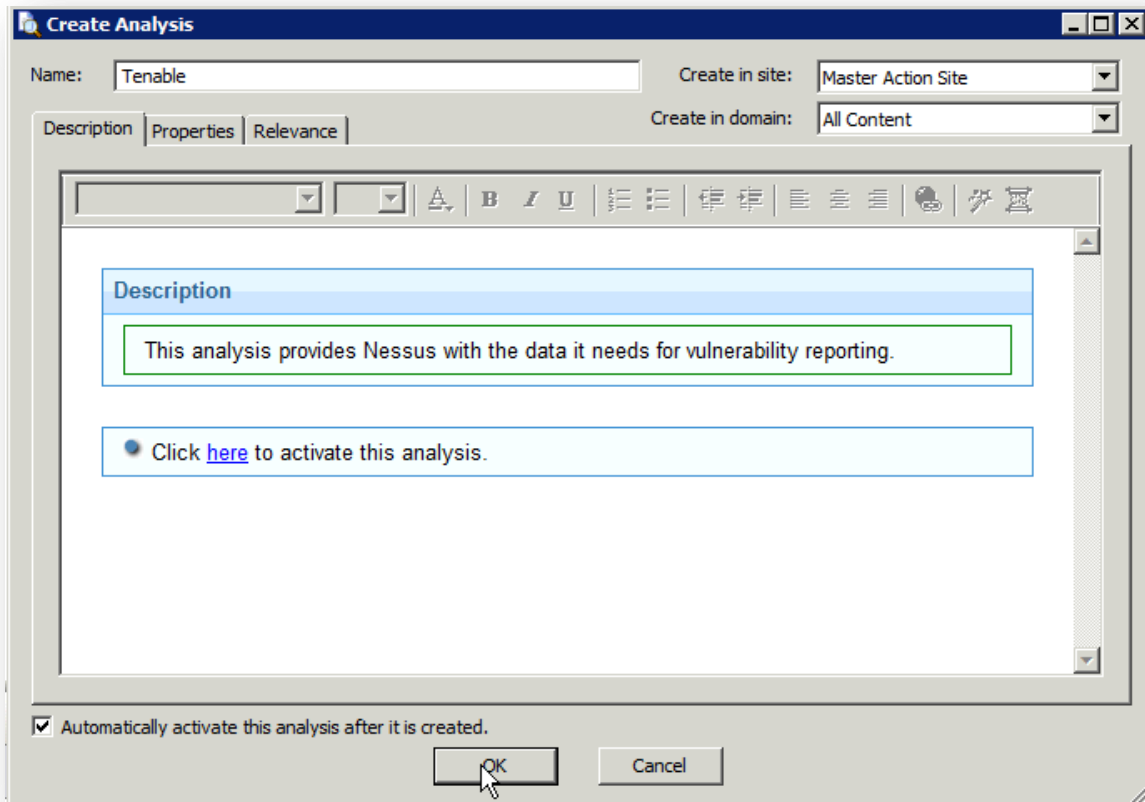
Once authenticated, click on the **File** menu item, and then **Import...**:



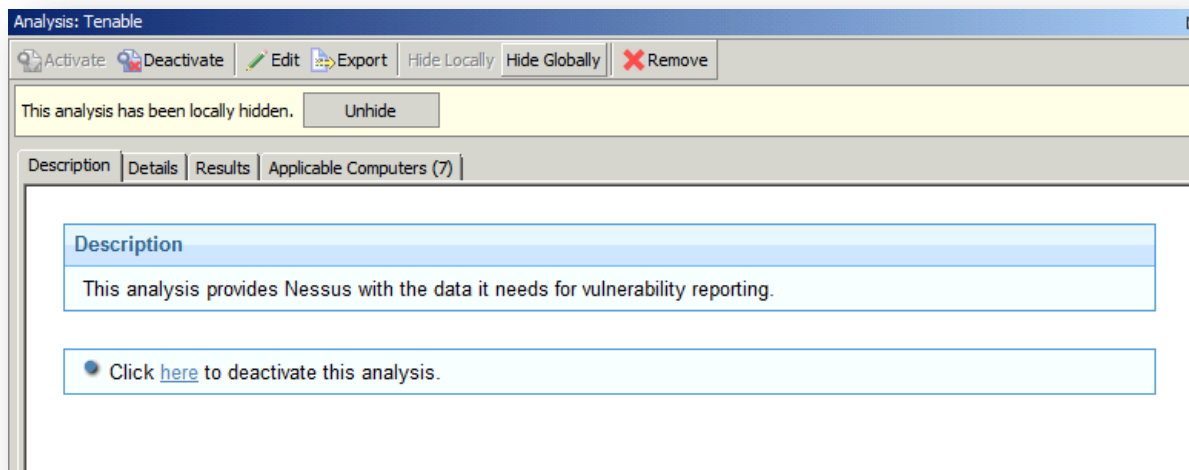
Locate the `.bes` file that contains the configuration details and click **Open**:



When the Create Analysis dialog opens, click **OK**:



Optionally, you can click Hide Locally and then Hide Globally to remove it from view, to avoid clutter:



After these steps are completed, it may take some time (depending on your network and report schedule) for the Analysis to fully populate. You can view the Applicable Computers count on the tab seen above to see how many computers have so far reported during a scan.

Microsoft SCCM

Microsoft System Center Configuration Manager (SCCM) is available to manage large groups of Windows-based systems. Nessus has the ability to query the SCCM service to verify whether or not patches are installed on systems managed by SCCM and display the patch information through the Nessus or SecurityCenter GUI.

- If the credentialed check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore SCCM output.
- The data returned by SCCM is only as current as the most recent data that the SCCM server has obtained from its managed hosts.
- Nessus connects to the server that is running the SCCM site (e.g., credentials must be valid for the SCCM **service**, meaning an admin account in SCCM with the privileges to query all the data in the SCCM MMC). This server may also run the SQL database, or the database as well as the SCCM repository can be on separate servers. When leveraging this audit, Nessus must connect to the SCCM Server, not the SQL or SCCM server if they are on a separate box.



Nessus SCCM patch management plugins support SCCM 2007 and SCCM 2012.

SCCM scanning is performed using four Nessus plugins:

- Patch Management: SCCM Server Settings (Plugin ID 57029)
- Patch Management: Missing updates from SCCM(Plugin ID 57030)
- Patch Management: SCCM Computer Info Initialization(Plugin ID 73636)
- Patch Management: SCCM Report(Plugin ID 58186)

Credentials for the SCCM system must be provided for SCCM scanning to work properly. Under the **Credentials** tab, select **Patch Management** and then **Microsoft SCCM**:

Microsoft SCCM

Server: sccm.example.org

Domain: example.org

Username: administrator

Password:

Credential	Description
Server	SCCM IP address or system name
Domain	The domain the SCCM server is a part of

Username	SCCM admin username
Password	SCCM admin password

Microsoft WSUS

Windows Server Update Services (WSUS) is available from Microsoft to manage the distribution of updates and hotfixes for Microsoft products. Nessus and SecurityCenter have the ability to query WSUS to verify whether or not patches are installed on systems managed by WSUS and display the patch information through the Nessus or SecurityCenter GUI.

- If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore WSUS output.
- The data returned to Nessus by WSUS is only as current as the most recent data that the WSUS server has obtained from its managed hosts.

WSUS scanning is performed using three Nessus plugins:

- Patch Management: WSUS Server Settings (Plugin ID 57031)
- Patch Management: Missing updates from WSUS (Plugin ID 57032)
- Patch Management: WSUS Report (Plugin ID 58133)

Credentials for the WSUS system must be provided for WSUS scanning to work properly. Under the **Credentials** tab, select **Patch Management** and then **Microsoft WSUS**:

Credential	Default	Description
Server	None	WSUS IP address or system name
Port	8530	Port WSUS is running on (typically TCP 80 or 443)
Username	none	WSUS admin username
Password	none	WSUS admin password
HTTPS	Enabled	If the WSUS service is using SSL
Verify SSL certificate	Enabled	Verify that the SSL certificate is valid

Red Hat Network Satellite

Red Hat Satellite is a systems management platform for Linux-based systems. Nessus has the ability to query Satellite to verify whether or not patches are installed on systems managed by Satellite and display the patch information.

Although not supported by Tenable, the RHN Satellite plugin will also work with Spacewalk Server, the Open Source Upstream Version of Red Hat Satellite. Spacewalk has the capability of managing distributions based on Red Hat (RHEL, CentOS, Fedora) and SUSE. Tenable supports the Satellite server for Red Hat Enterprise Linux.

- If the credential check sees a system, but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore RHN Satellite output.
- The data returned to Nessus by RHN Satellite is only as current as the most recent data that the Satellite server has obtained from its managed hosts.

Satellite scanning is performed using five Nessus plugins:

- Patch Management: Patch Schedule From Red Hat Satellite Server (Plugin ID 57066)
- Patch Management: Red Hat Satellite Server Get Installed Packages (Plugin ID 57065)
- Patch Management: Red Hat Satellite Server Get Managed Servers (57064)
- Patch Management: Red Hat Satellite Server Get System Information (Plugin ID 57067)
- Patch Management: Red Hat Satellite Server Settings (Plugin ID 57063)

Red Hat Satellite 6 Server

▼ Red Hat Satellite 6 Server

Satellite server

REQUIRED

Port

443

Username

REQUIRED

Password

REQUIRED

HTTPS

Verify SSL Certificate

☒

Credential	Default	Description
Satellite server	none	RHN Satellite IP address or system name

Port	443	Port Satellite is running on (typically TCP 80 or 443)
Username	none	Red Hat Satellite username
Password	none	Red Hat Satellite password
HTTPS	Enabled	
Verify SSL Certificate	Enabled	Verify that the SSL certificate is valid

Red Hat Satellite 5 Server

▼ Red Hat Satellite 5 Server

Satellite server

REQUIRED

Port

443

Username

REQUIRED

Password

REQUIRED

Verify SSL Certificate

☒

Credential	Default	Description
Satellite server	none	RHN Satellite IP address or system name
Port	443	Port Satellite is running on (typically TCP 80 or 443)
Username	none	Red Hat Satellite username
Password	none	Red Hat Satellite password
Verify SSL Certificate	Enabled	Verify that the SSL certificate is valid

Symantec Altiris

[Altiris](#) is available from Symantec to manage the distribution of updates and hotfixes for Linux, Windows, and Mac OS X systems. Nessus and SecurityCenter have the ability to use the Altiris API to verify whether or not patches are installed on systems managed by Altiris and display the patch information through the Nessus or SecurityCenter GUI.

- If the credential check sees a system but it is unable to authenticate against the system, it will use the data obtained from the patch management system to perform the check. If Nessus is able to connect to the target system, it will perform checks on that system and ignore Altiris output.
- The data returned to Nessus by Altiris is only as current as the most recent data that the Altiris has obtained from its managed hosts.

- Nessus connects to the Microsoft SQL server that is running on the Altiris host (e.g., credentials must be valid for the MSSQL **database**, meaning a database account with the privileges to query all the data in the Altiris MSSQL database). The database server may be run on a separate host from the Altiris deployment. When leveraging this audit, Nessus must connect to the MSSQL database, not the Altiris server if they are on a separate box.

Altiris scanning is performed using four Nessus plugins:

- symantec_altiris_get_computer_info.nbin (Plugin ID 78013)
- symantec_altiris_get_missing_updates.nbin (Plugin ID 78012)
- symantec_altiris_init_info.nbin (Plugin ID 78011)
- symantec_altiris_report.nbin (Plugin ID 78014)
- Credentials for the Altiris Microsoft SQL (MSSQL) database must be provided for Altiris scanning to work properly. Under the **Credentials** tab, select **Patch Management** and then **Symantec Altiris**:

Credential	Default	Description
Server	none	Altiris IP address or system name. This is a required field.
Database Port	5690	Port the Altiris database is running on (Typically TCP 5690)
Database Name	Symantec_CMDB	The name of the MSSQL database that manages Altiris patch information.
Database Username	None	Username required to log into the Altiris MSSQL database. This is a required field.
Database Password	none	Password required to authenticate the Altiris MSSQL database. This is a required field.
Use Windows Authentication	Disabled	Denotes whether or not to use NTLMSSP for compatibility with older Windows Servers, otherwise it will use Kerberos

To ensure Nessus can properly utilize Altiris to pull patch management information, it must be configured to do so.

Symantec Management Console Configuration Settings

Welcome to the Symantec Management Console

Step 1 - Discover
Discover Computers...
Discovered computers: 10
New in the last 5 days: 0

Step 2 - Rollout Agent
Rollout Agent...
Management Agent installed: 0
Unmanaged computers: 4
Total: 10

Step 3 - Gather Inventory
Collect Inventory...
Inventory collected: 0
No inventory collected: 4
Not collected in last 30 days: 4

Step 4 - Schedule Patch Management
Schedule Patch...

Discovered Computers:

Name	Date found
alt-suse11	9/11/2014 7:16:01 AM
RE-ALTIRIS-CMS	8/4/2014 11:32:09 AM
RE-AMS-DC	8/4/2014 1:23:57 PM
TENALTIRIS-W7	8/11/2014 8:45:01 AM
alt-cent5	9/16/2014 11:06:41 AM
alt-rhel6	9/17/2014 10:00:03 AM
RE-ALTIRIS-SMS	8/4/2014 1:23:58 PM
altiris-cent1	9/3/2014 8:45:04 AM
RE-AMS-SERVER	8/4/2014 1:23:58 PM
linux-d8x5	9/9/2014 11:15:01 AM

Total computers: 10

Discovered Computers 10
Management Agent Installed 6
Inventory Collected 6

Import Microsoft Active Directory
Import Domain Membership/WINS
Network Discovery
Automatic rollout to newly discovered computers
Collect Inventory

Solution Licensing

Solution	Version	Used/Total	Expires
Agentless Inventory	7.5.3219.0	0/20	316 days
Altiris Deployment Solution 7.5	7.5.3219.0	5/20	316 days
Altiris Patch Management Solut	7.5.3219.0	6/20	316 days
Altiris Real-Time System Mana	7.5.3219.0	1/1	316 days
Altiris Software Management S	7.5.3219.0	0/20	316 days
Inventory Solution	7.5.3251.0	6/20	316 days
pcAnywhere Solution	12.6.8556.0	0/20	316 days

Advanced Help Topics
Planning, design and implementation guide
Knowledge base
Migration guide

From the dashboard (shown above), click on **Settings** and then **Database Settings**:

Database Settings
Configure the Notification Server database.

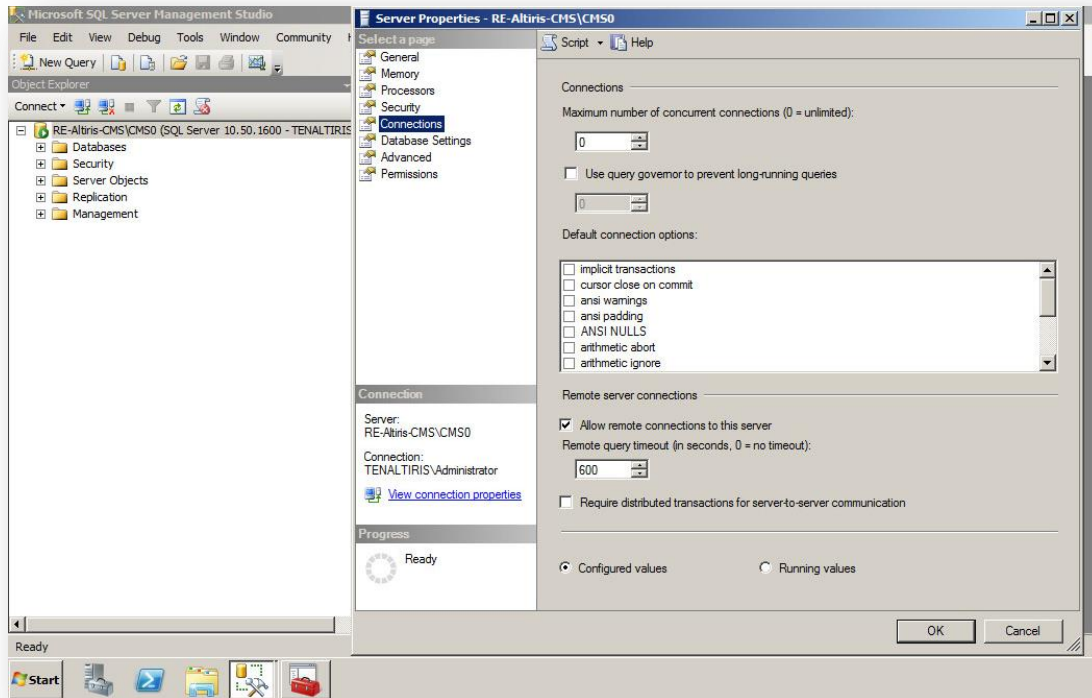
General | **Reports**

Database Server
If you did not install SQL Server as the default 'instance', then when specifying the server you need to use the following format: servername\instancename.
SQL server name: RE-ALTIRIS-CMS\CMS0

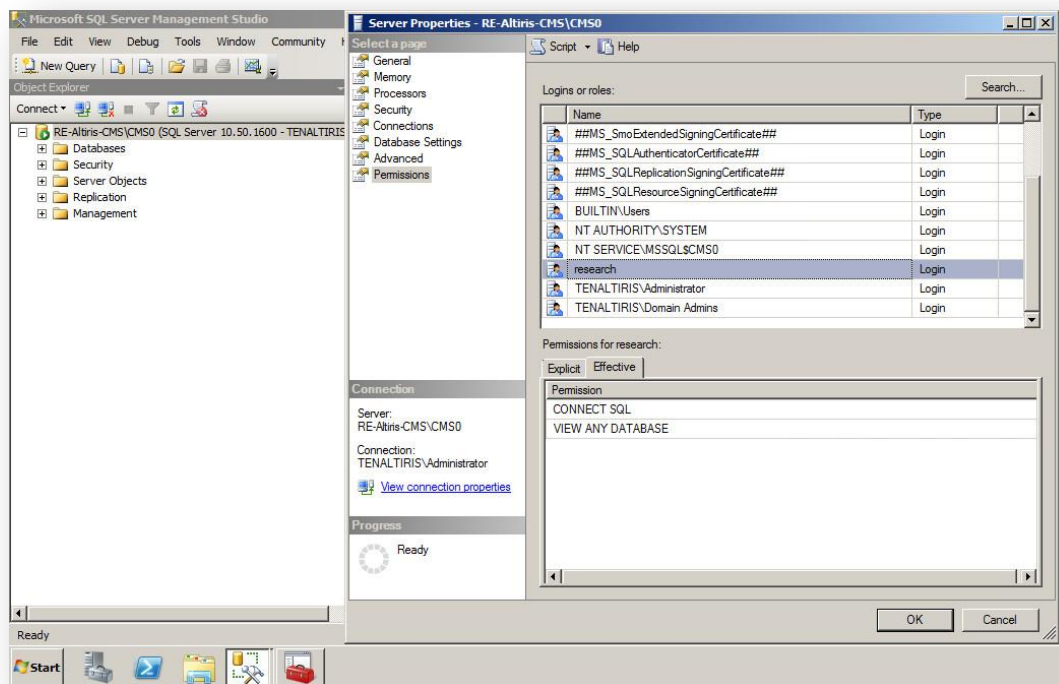
Database Credentials
☒ Use application credentials
☐ Use SQL Login
Login ID:
Password:
Confirm password:

Database Name
☒ Use existing database: Symantec_CMDB
☐ Create new database: Symantec_CMDB
Command timeout: 1600 seconds

Ensure that the SQL server name is set and that a database is selected. Next, configure the Microsoft SQL Server:



Under **Connections**, Allow remote connections to this server must be selected. Next, navigate to the **Permissions** tab:



Configure the account that Nessus will use with **CONNECT SQL** and **VIEW ANY DATABASE** credentials.

Scanning With Multiple Patch Managers

If multiple sets of credentials are supplied to Nessus for patch management tools, Nessus will use all of them. Available credentials are:

- Credentials supplied to directly authenticate to the target
- IBM TEM
- Microsoft WSUS
- Microsoft SCCM
- Red Hat Network Satellite
- Dell KACE 1000
- Altiris

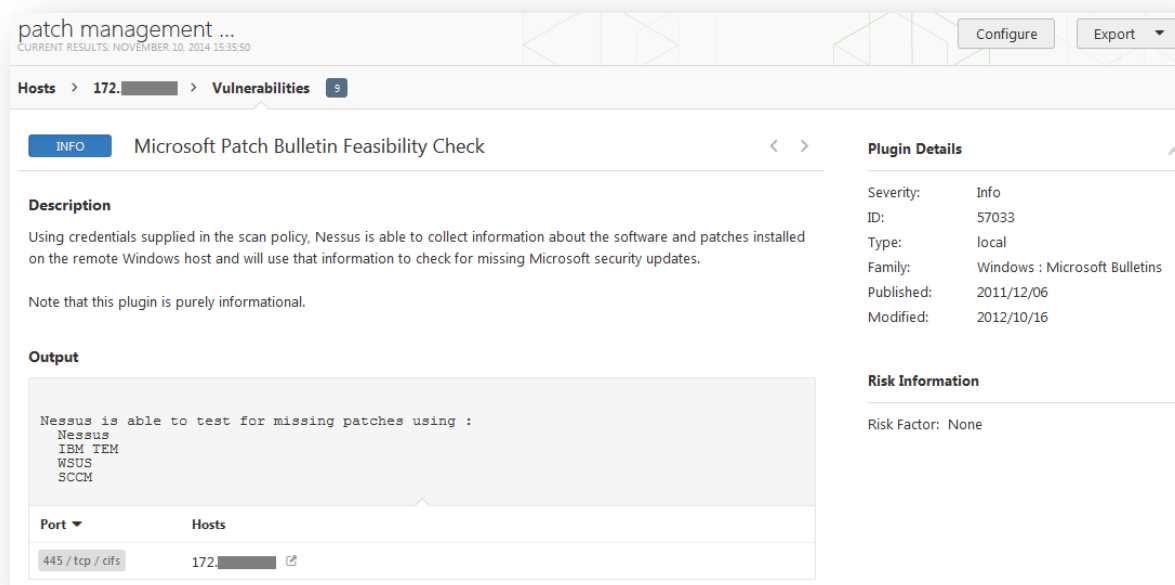
If credentials are provided for a host, as well as a patch management system, or multiple patch management systems, Nessus will compare the findings between all methods and report on conflicts or provide a satisfied finding. Using the Patch Management Windows Auditing Conflicts plugins, the patch data differences (conflicts) between the host and a patch management system will be highlighted. For example, if you provide credentials for the target host and a SCCM, IBM TEM, KACE 1000, and WSUS patch management systems, Nessus will produce the following report with a High severity rating if there are conflicts found:

The screenshot shows the Nessus interface for the 'Patch Management Windows Auditing Conflicts' plugin. The report is titled 'patch management ...' and shows 'CURRENT RESULTS: NOVEMBER 10, 2014 15:35:50'. The host is '172.17.0.1' and the vulnerability is 'Vulnerabilities 3'. The severity is 'HIGH'. The description states: 'This plugin compares vulnerabilities reported by Nessus and supplied patch management results to determine conflicts in Windows patches. The report will allow you to audit your patch management solution to determine if it is reporting properly.' The solution is: 'If conflicts exist, they should be resolved with updates.' The output shows: 'The following tools were used in this scan. IBM TEM, Nessus, SCCM, WSUS. Nessus feed : \$Date: 2005/11/08 13:18:41 \$. Nessus -> IBM TEM conflicts ms11-049 : Nessus reports vulnerable , IBM TEM is NOT reporting vulnerable'. The risk factor is 'High' and the vulnerability information is 'CPE: cpe/o:microsoft:windows'. The table at the bottom shows the host '172.17.0.1' and the port 'N/A'.

Port	Hosts
N/A	172.17.0.1

This underscores the importance of cross-referencing patches between what is on the system and what the patch management system thinks is on the system. In the above output you can see that Nessus has credentials to log in to the target system itself (indicated by the Nessus ->). Nessus is also able to pull the patch levels from SCCM (as indicated by the -> SCCM conflicts). The report for each patch and the discrepancies is displayed in the plugin output. As the first entry indicates for the host, Nessus found MS11-049 missing, but IBM TEM is reporting that patch as being applied.

This allows organizations to not only audit hosts, but to help ensure that patch management software is providing accurate information. If there are no conflicts found, Nessus will provide a Satisfied finding with an Info severity rating:



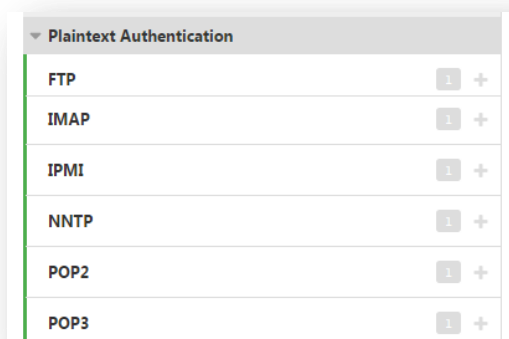
Plaintext Authentication

Finally, if a secure method of performing credentialed checks is not available, users can force Nessus to try to perform checks over insecure protocols by configuring the **Plaintext Authentication** drop-down menu item.

This menu allows the Nessus scanner to use credentials when testing HTTP, NNTP, FTP, POP2, POP3, IMAP, IPMI, SNMPv1/v2c, and telnet/rsh/rexec. 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.

Cleartext Protocols

Credentials for **FTP**, **IPMI**, **NNTP**, **POP2**, and **POP3** are username and password only.



HTTP

There are four different types of HTTP authentication: **Automatic authentication**, **Basic/Digest authentication**, **HTTP login form** for a custom web application, and **HTTP cookies import**.

HTTP Global Settings

Option	Default	Description
Login method	POST	Specify if the login action is performed via a GET or POST request.
Re-authenticate delay (seconds)	0	The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.
Follow 30x redirections (# of levels)	0	If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.
Invert authenticated regex	Disabled	A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (e.g., Authentication failed!).
Use authenticated regex on HTTP headers	Disabled	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.
Use authenticated regex on HTTP headers	Disabled	The regex searches are case sensitive by default. This instructs Nessus to ignore case.

HTTP login form

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

HTTP

Authentication method

HTTP login form

Username

admin

REQUIRED

Password

REQUIRED

Login page

/login.php

REQUIRED

Login submission page

/process_login.php

REQUIRED

Login parameters

user=%USER%&pass=%PASS%

REQUIRED

If the keywords %USER% and %PASS% are used, they will be substituted

Check authentication on page

/user/profile.php

REQUIRED

Regex to verify successful authentication

Logged in as user "[^"]+"

REQUIRED

Option	Description
Username	Login user's name.
Password	Password of the user specified.
Login page	The absolute path to the login page of the application, e.g., /login.html.
Login submission page	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 parameters	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. This field can be used to provide more than two parameters if required (e.g., a group name or some other piece of information is required for the authentication process).
Check authentication on page	The absolute path of a protected web page that requires authentication, to better assist Nessus in determining authentication status, e.g., /admin.html.
Regex to verify successful authentication	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!

HTTP cookies import

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.

HTTP

Authentication method

HTTP cookies import

Cookies file

Add File

REQUIRED

This file must be in the Netscape cookies.txt format.



Using cleartext credentials in any fashion is not recommended! If the credentials are sent remotely (e.g., via a Nessus scan), the credentials could be intercepted by anyone with access to the network.

Use encrypted authentication mechanisms whenever possible.

telnet/rsh/rexec

The **telnet/rsh/rexec** authentication section is also username and password, but there are additional Global Settings for this section that can allow you to perform patch audits using any of these three protocols.

telnet/rsh/rexec

Username

REQUIRED

Password (unsafe!)

REQUIRED

Global Settings

☐ Perform patch audits over telnet
Patch auditing will only be attempted for non-Windows targets.

☐ Perform patch audits over rsh
Patch auditing will only be attempted for non-Windows targets.

☐ Perform patch audits over rexec
Patch auditing will only be attempted for non-Windows targets.

SNMPv1/v2c

SNMPv1/v2c configuration allows you to use community strings for authentication to network devices. Up to 4 SNMP community strings can be configured.

SNMPv1/v2c

Community string

public

Global Settings

UDP port

161

Additional UDP port #1

161

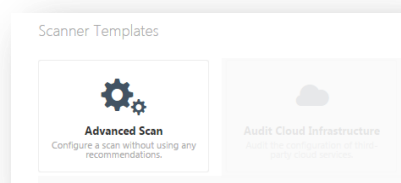
Additional UDP port #2

161

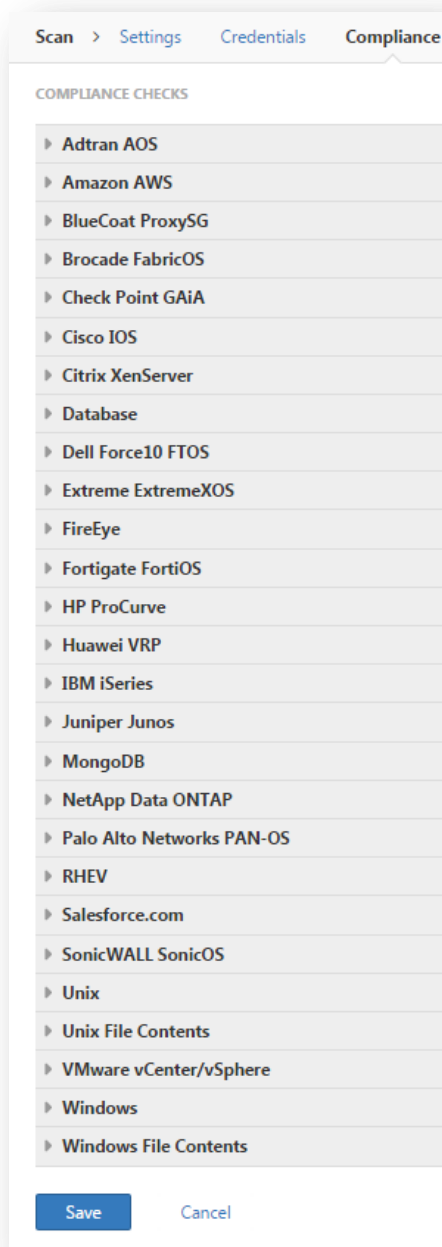
Additional UDP port #3

161

Scan > Compliance (Advanced Scan Example)



Advanced Scans share the same **Scan > Settings** and **Scan > Credentials** as does the **Basic Network Scan's** template. However, the **Advanced Scan** template includes additional **Compliance** and **Plugins** pages and settings.

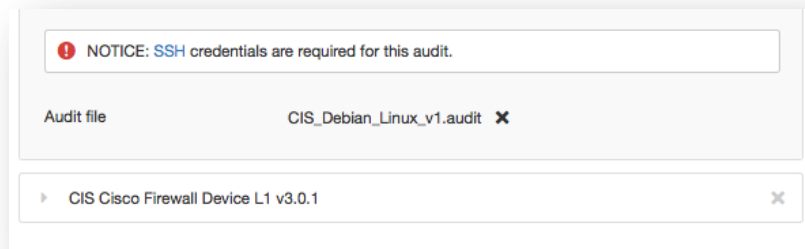


The following table provides an overview of all compliance checks.

Compliance Policy	Required Credentials	Description
Adtran AOS	SSH	An option that allows a system or policy file to be specified to test Adtran AOS based devices against compliance standards.
Amazon AWS	SSH	An option that allows a system to be specified to test the AWS account configuration against compliance standards.
Blue Coat ProxySG	SSH	An option that allows a system to be specified to test Blue Coat ProxySG devices against compliance standards.

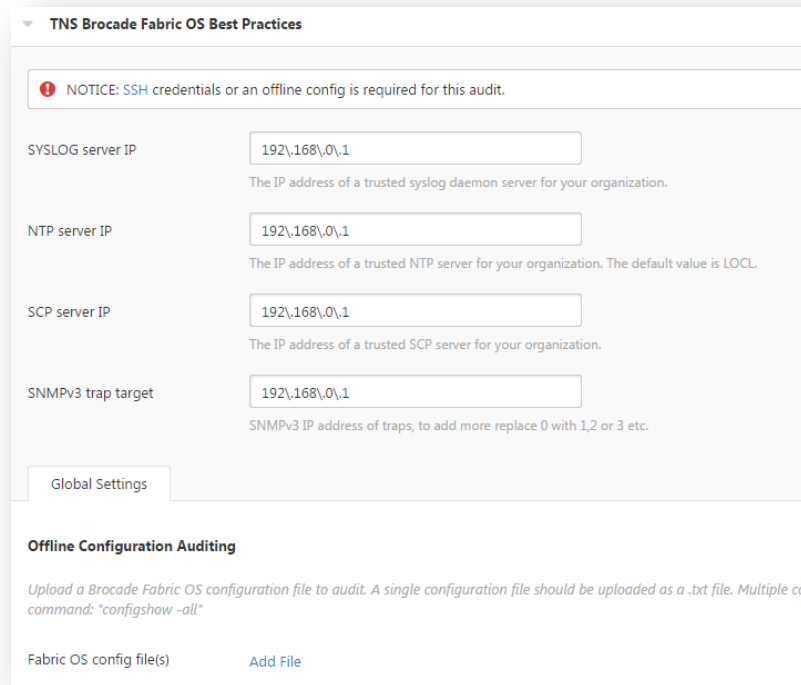
Compliance Policy	Required Credentials	Description
Brocade FabricOS		An option that allows a system or policy file to be specified to test Brocade FabricOS based devices against compliance standards.
Check Point GAIa	SSH	An option that allows a system to be specified to test Check Point GAIa based devices against compliance standards.
Cisco IOS	SSH	<p>An option that allows a device or policy file to be specified to test Cisco IOS based devices against compliance standards.</p> <p>In addition to being able to upload your own .audit files, there are also DISA STIG and other best practices files available.</p>
Citrix XenServer	SSH	A commercial option that allows a system to be specified to test Citrix XenServers against compliance standards
Database	Database credentials	An option that allows a policy file to be specified to test databases such as DB2, SQL Server, MySQL, and Oracle against compliance standards.
Dell Force10 FTOS	SSH	An option that allows a system or policy file to be specified to test Dell Force10 FTOS based devices against compliance standards.
Extreme ExtremeXOS	SSH	An option that allows a system or policy file to be specified to test Extreme ExtremeXOS based devices against compliance standards.
FireEye	SSH	An option that allows a system or policy file to be specified to test FireEye devices against compliance standards.
Fortigate FortiOS	SSH	An option that allows a system or policy file to be specified to test Fortigate FortiOS based devices against compliance standards.
HP ProCurve	SSH	An option that allows a system or policy file to be specified to test HP ProCurve devices against compliance standards.
Huawei	SSH	An option that allows a device or policy file to be specified to test Huawei VRP based devices against compliance standards.
IBM iSeries	IBM iSeries	An option that allows a policy file to be specified to test IBM iSeries systems against compliance standards.
Juniper Junos	SSH	An option that allows a device or policy file to be specified to test Juniper Junos devices against compliance standards.
MongoDB	MongoDB	An option that allows a system or policy file to be specified to test MongoDB systems against compliance standards.
NetApp Data ONTAP	SSH	An option that allows a system or policy file to be specified to test NetApp Data ONTAP devices against compliance standards.
Palo Alto Networks PAN-OS	PAN-OS	An option that allows a system to be specified to test Palo Alto Networks PAN-OS devices against compliance standards.
RHEV	RHEV	An option that allows a system to be specified to test Red Hat Enterprise Virtualization devices against compliance standards.
Salesforce.com	Salesforce SOAP API	An option that allows a system to be specified to test Salesforce applications against compliance standards.

Once a compliance policy is saved, a user can open the compliance policy and download any custom audit files. This enables a user who did not originate the policy to retrieve the audit file from the Nessus policy directly.



Example: TNS Brocade Fabric OS Best Practices

Some policies also have a best practices option, which is a pre-defined audit file where the user provides the values to their environment. In some instances, there are pre-defined DISA STIG, CIS, and PCI audit policies already available.



For more information on specific compliance policies, see the Tenable Network Security document, [Nessus Compliance Checks](#).

Offline Configuration Audit Policies

Tenable offers the ability to upload configuration policies directly to Nessus. This provides the user with the ability to upload the configuration of a critical device for auditing and not require any access to the device. This keeps the audited device online while being able to audit the configuration.

Currently supported devices for offline configuration auditing are:

- Adtran AOS
- Blue Coat ProxySG
- Brocade Fabric OS
- Cisco IOS
- Check Point GAiA
- Dell Force10 FTOS
- Extreme ExtremeXOS
- FireEye
- HP ProCurve
- Huawei VRP
- Juniper Junos
- Netapp Data ONTAP
- SonicWALL SonicOS

Scan > Plugins (Advanced Scan Example)

The **Advanced Scan** templates include **Plugin** pages and settings.

The **Plugins** menu enables you to select security checks by **Plugin Family** or individual checks.

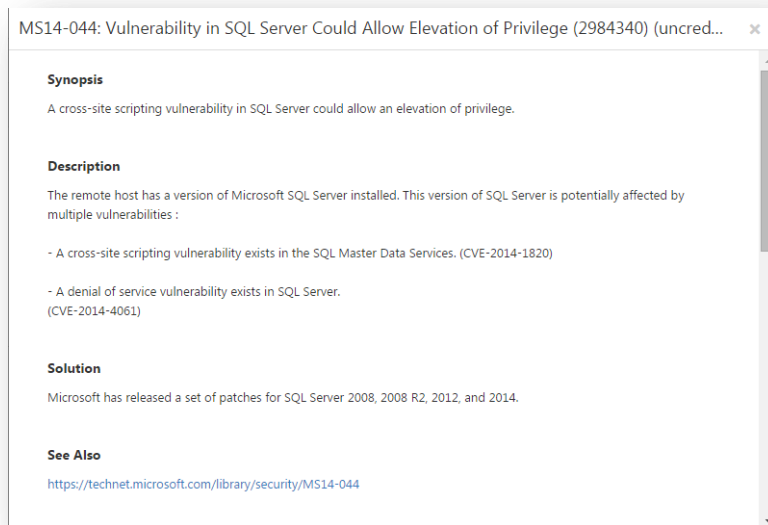
Status	Plugin Family ▼	Total
ENABLED	ADX Local Security Checks	11169
ENABLED	Amazon Linux Local Security Checks	548
ENABLED	Backdoors	102
ENABLED	CentOS Local Security Checks	1929
ENABLED	CGI abuses	3296
ENABLED	CGI abuses : XSS	604
ENABLED	CISCO	622

Status	Plugin Name	Plugin ID
	No plugin family selected.	

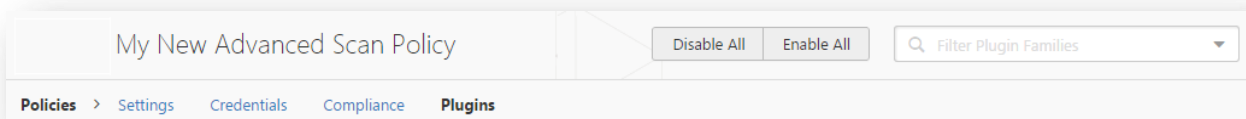
Clicking on the plugin family allows you to enable (green) or disable (grey) the entire family. Selecting a family will display the list of its plugins. Individual plugins can be enabled or disabled to create very specific scan policies.

A family with some plugins disabled will turn blue and display mixed to indicate only some plugins are enabled. Clicking on the plugin family will load the complete list of plugins, and allow for granular selection based on your scanning preferences.

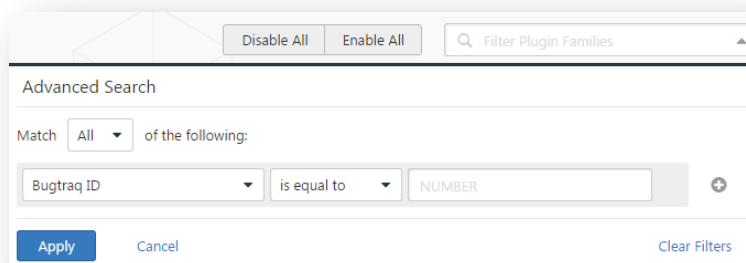
Selecting a specific plugin will display the plugin output that will be displayed as seen in a report. The synopsis and description will provide more details of the vulnerability being examined. Scrolling down in your browser will also show solution information, additional references if available, risk information; exploit information, and any vulnerability database or informational cross-references.



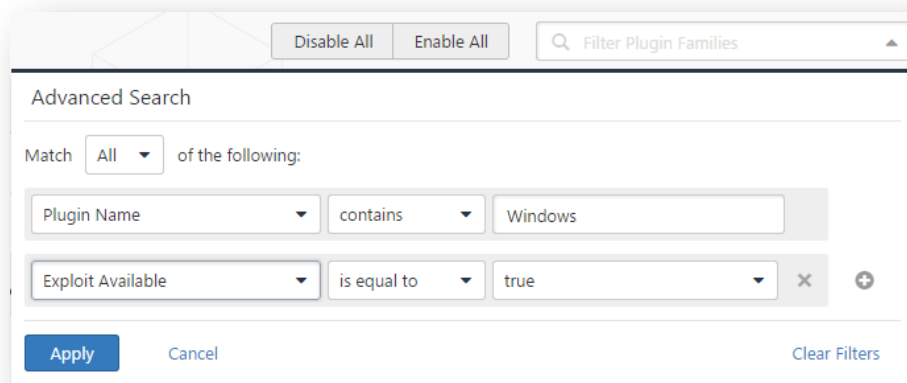
At the top of the plugin family page, you can create filters to build a list of plugins to include in the policy, as well as disable or enable all plugins. Filters allow granular control over plugin selection. Multiple filters can be set in a single policy.



To create a filter, click the Filter Plugin Families drop-down arrow.



Each filter created provides several options for refining a search. The filter criteria can be based on **Any**, where any one criteria will return matches, or **All**, where every filter criteria must be present. For example, if we want a policy that only includes plugins that have an exploit **or** can be exploited without a scripted exploit, we create two filters and select **Any** for the criteria:



Advanced Search

Match All of the following:

Plugin Name contains Windows

Exploit Available is equal to true

Apply Cancel Clear Filters

For a full list of filter criteria and details, check the [Report Filters](#) section of this document.



To use filters to create a policy, it is recommended you start by disabling all plugins. Using plugin filters, narrow down the plugins you want to be in your policy. Once completed, select each plugin family and click Enable Plugins.

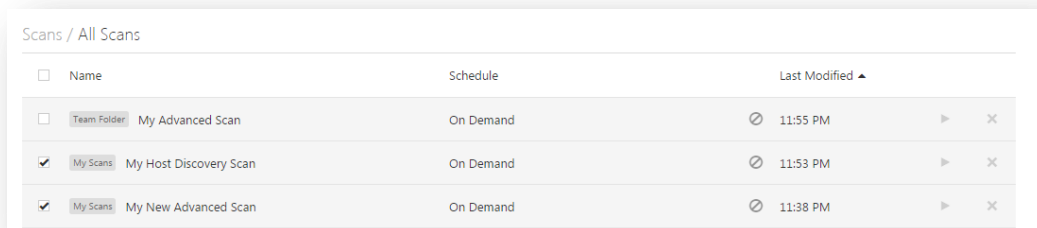
When a policy is created and saved, it records all of the plugins that are initially selected. When new plugins are received via a plugin update, they will automatically be enabled if the family they are associated with is enabled. If the family has been disabled or partially enabled, new plugins in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



The Denial of Service family contains some plugins that could cause outages on a 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 unless scheduled during a maintenance window and with staff ready to respond to any issues.

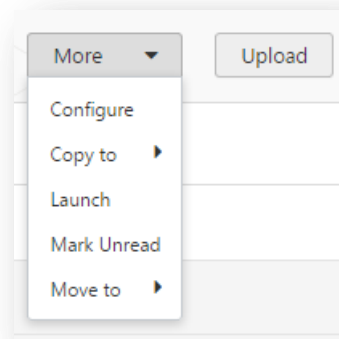
Manage Scans

Based on permissions, when a scan is selected from the list, the **More** button will appear on the page and additional options for the scan become available.



Scans / All Scans					
<input type="checkbox"/>	Name	Schedule		Last Modified	
<input type="checkbox"/>	Team Folder My Advanced Scan	On Demand		11:55 PM	
<input checked="" type="checkbox"/>	My Scans My Host Discovery Scan	On Demand		11:53 PM	
<input checked="" type="checkbox"/>	My Scans My New Advanced Scan	On Demand		11:38 PM	

- Configure
- Copy to
- Launch
- Mark Unread
- Move to



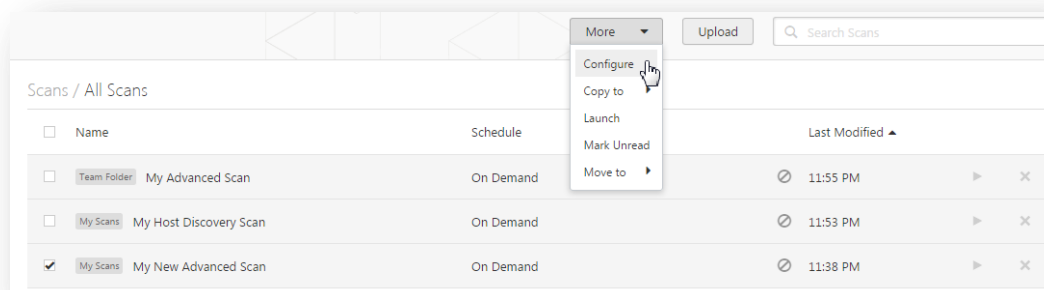
Upload a Scan

Scan reports that were previously exported may be imported using the **Upload** button. Valid file formats are **.nessus** and **.db**.

Option	Description
.nessus	<p>An XML-based format and the de-facto standard in Nessus 4.2 and later. This format uses an expanded set of XML tags to make extracting and parsing information more granular. This report does not allow chapter selection.</p> <p>If the policy is exported and saved to a .nessus file, the passwords will be stripped.</p> <p>When importing a .nessus file format, you will need to re-apply your passwords to the credentials being used.</p>
Nessus DB	<p>A proprietary encrypted database format used in Nessus 5.2 and later that contains all the information in a scan, including the audit trails and results. When exporting to this format, you will be prompted for a password to encrypt the results of the scan.</p>

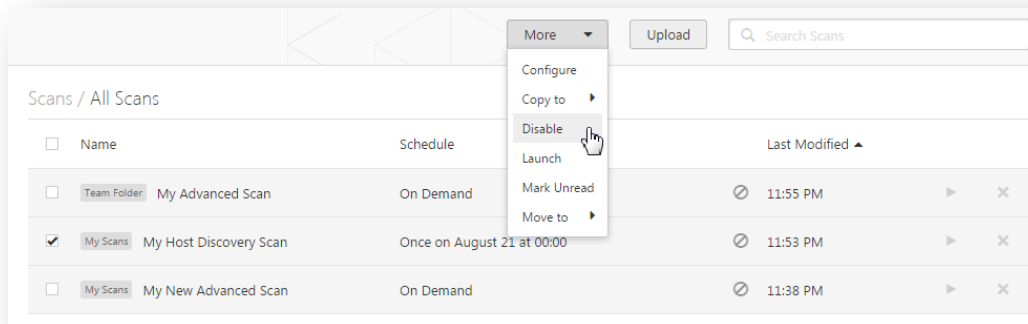
Configure a Scan

The **Configure** option allows you manage scans, including their schedules and settings, and you have the ability to update them as needed.



Disable a Scheduled Scan

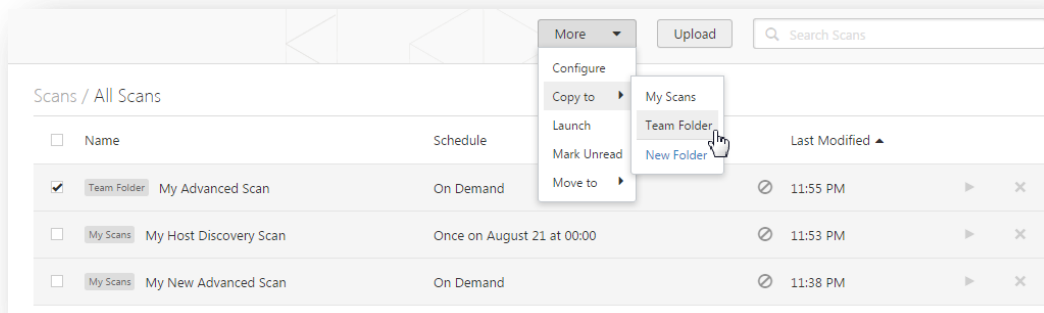
If the scan that you have selected is configured with a schedule, the **More** menu allows you to disable the schedule.



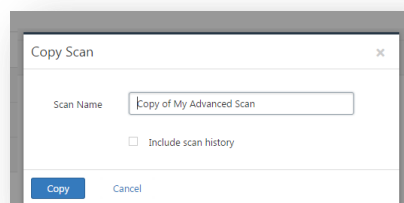
Copy a Scan

Based on permissions, you have the ability to copy existing scans.

Select the scan to be copied, and then use the **Copy to** option from the **More** drop-down menu. You may choose to copy the scan to an existing folder or create a new folder to store the copied scan.

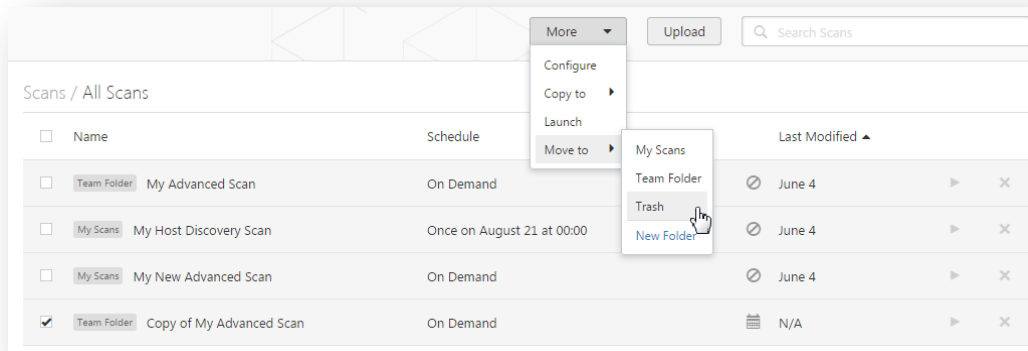


Once the **Copy to** option has been selected, create a new name for the copied scan and choose whether or not to include the original scan's history.



Move a Scan

Similar to copying a scan, the **Move to** option allows you to move a selected scan to a **New Folder**, a previously created folder, or to the **Trash** folder.



When a scan has been moved to the **Trash** folder, none of the scan's configured functions will be performed; however the scan has not been deleted; it can be deleted or it can be restored to a New Folder by selecting it from the **Trash** folder and using the **More** menu options.



Scans stored in the Trash folder will be deleted automatically after 30 days.

Scan Results, Dashboards, and Reports

Nessus has an extensive interface for viewing scan results and generating reports.

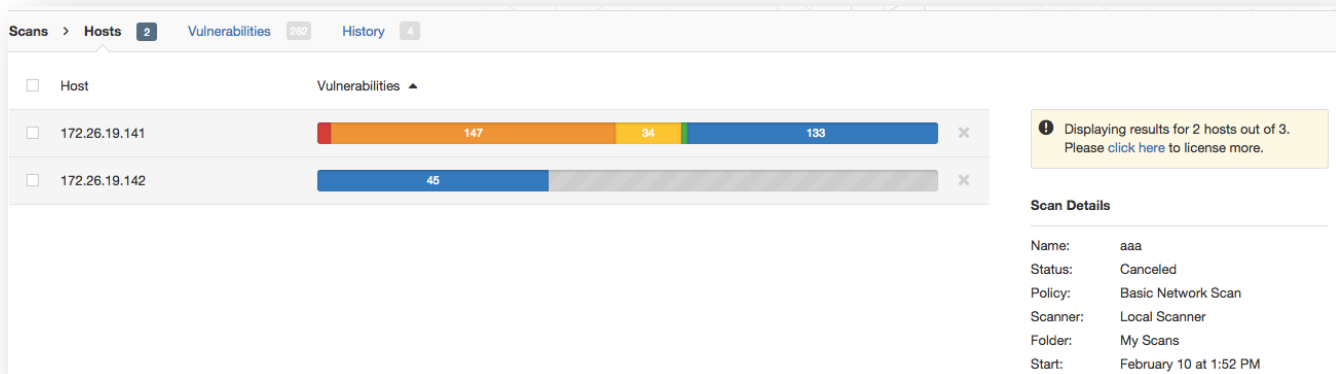
You can configure a scan, search the audit trail, launch scans, or export results while viewing the reports.

Default Network Scan
CURRENT RESULTS: NOVEMBER 10, 2014

Configure Audit Trail Launch Export

Option	Description
Configure	Navigates you back to the scan's configuration settings.
Audit Trail	Displays the audit trail dialogue.
Launch	Display two choices to launch a scan: Default and Custom . The custom option allows you to define different targets for the scan, where default will run the scan with the predefined targets.
Export	Allows you to save the scan result in one of four formats: Nessus (.nessus), HTML, CSV, or Nessus DB. Nessus DB format is an encrypted proprietary format. Note that the Nessus DB formats all the possible data about a scan, including but not limited to the results, the audit trails, and attachments.

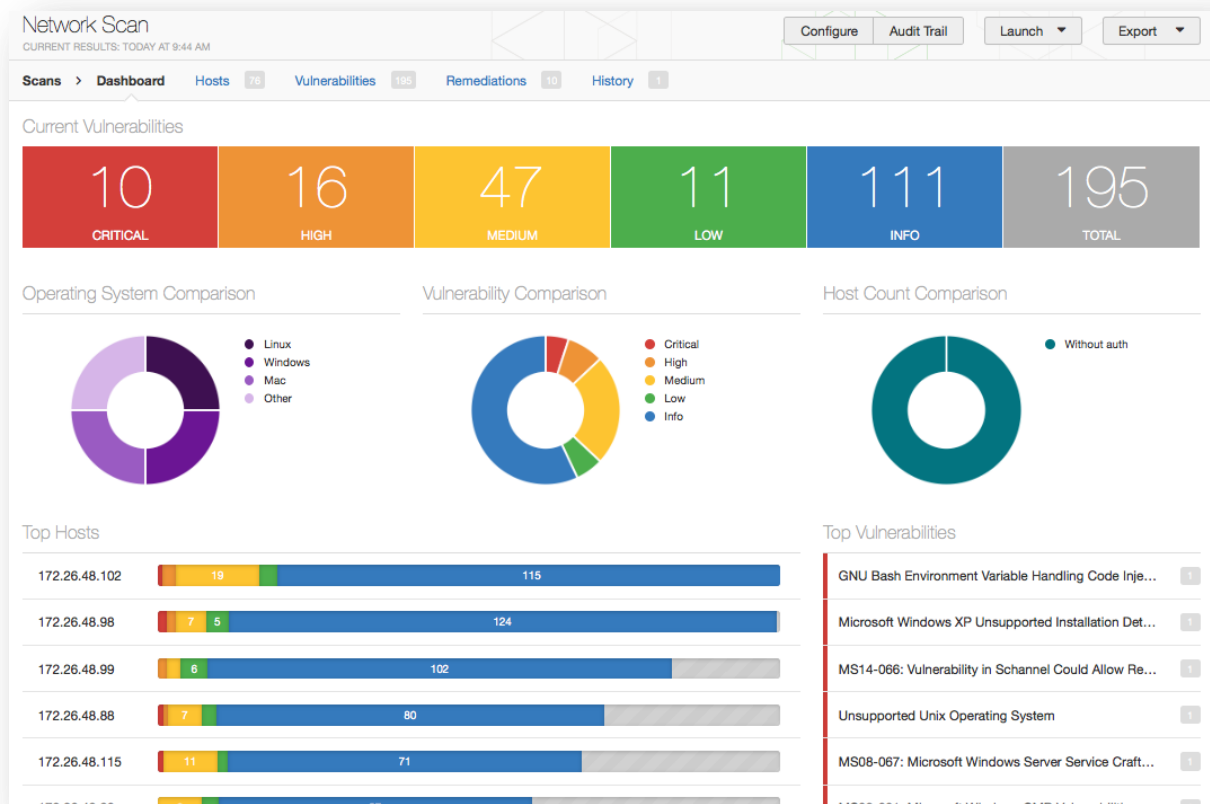
Scan Results



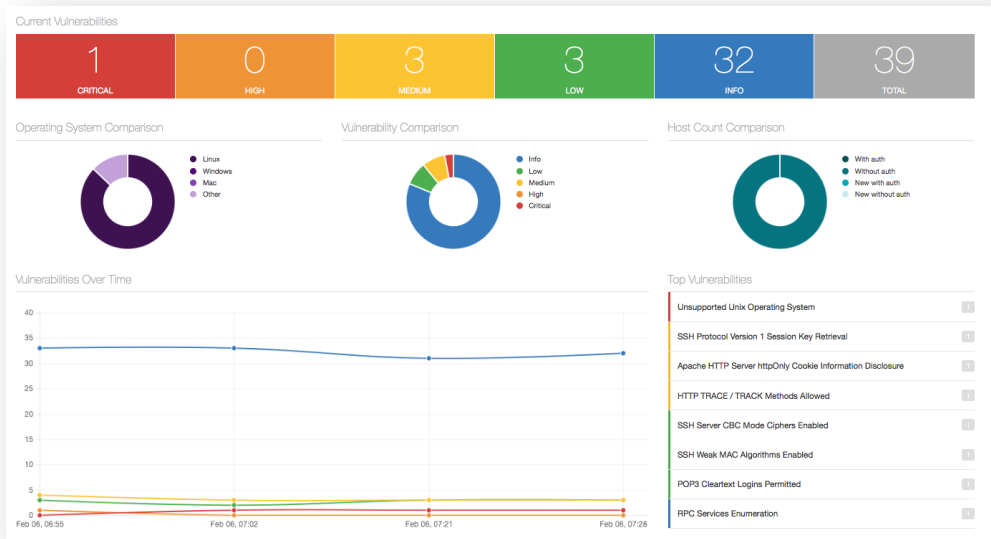
If you scan more hosts than your license allows, Nessus will display a warning directing you to contact Tenable to obtain more licenses.

Dashboards

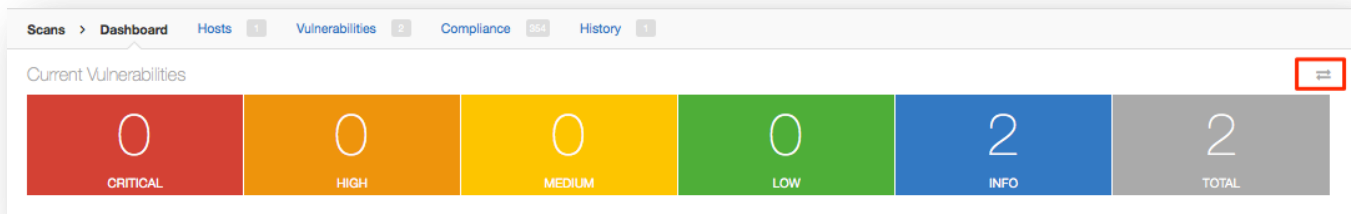
Nessus Manager and Nessus Cloud display the scan results in Scans / Dashboard.



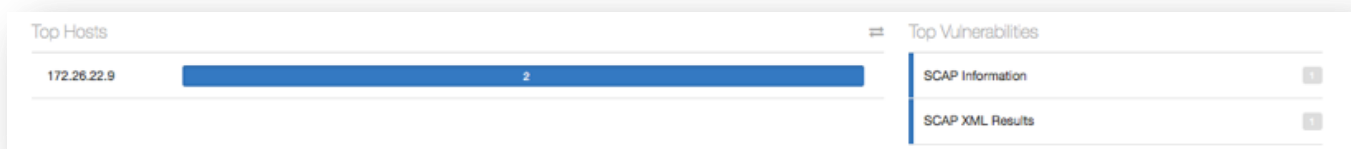
If there are multiple scan results, the **Top Hosts** chart will be replaced with **Vulnerabilities Over Time**.



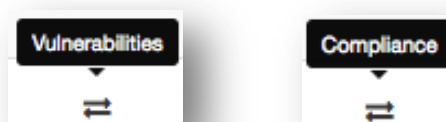
If a scan includes **Compliance** results, you will see toggle arrows above the totals.

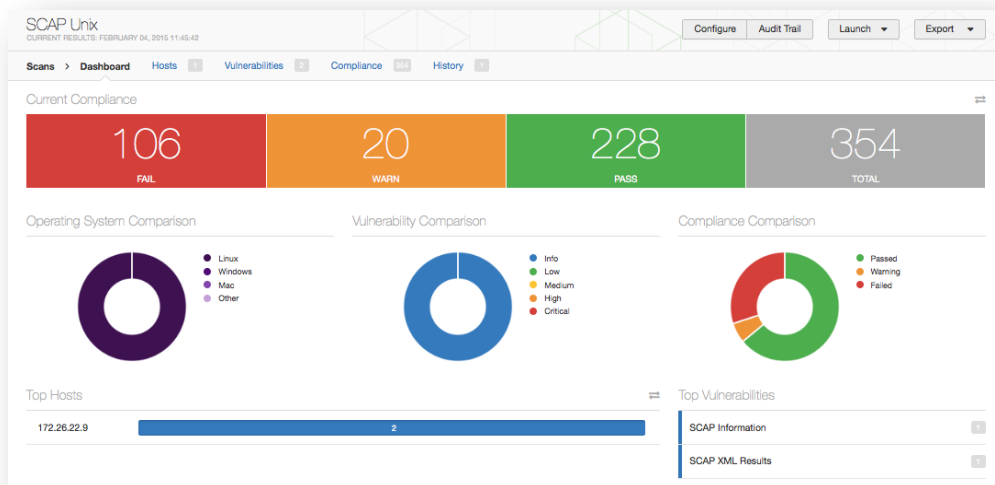


You will also see the toggle arrows next to **Top Vulnerabilities**.



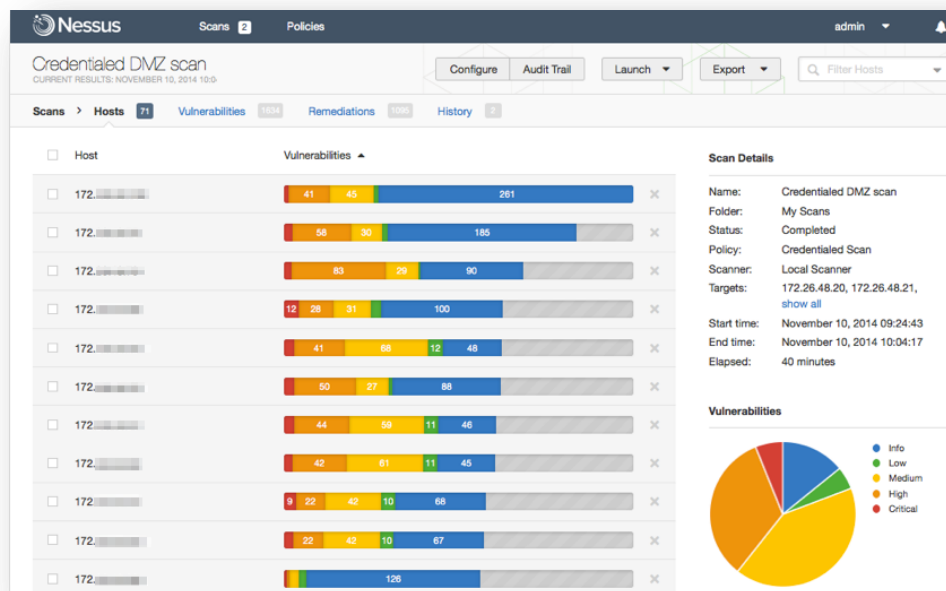
If you mouse over either set of the toggle arrows, you will see text that states that navigation will take you to vulnerability counts or compliance counts dashboard:



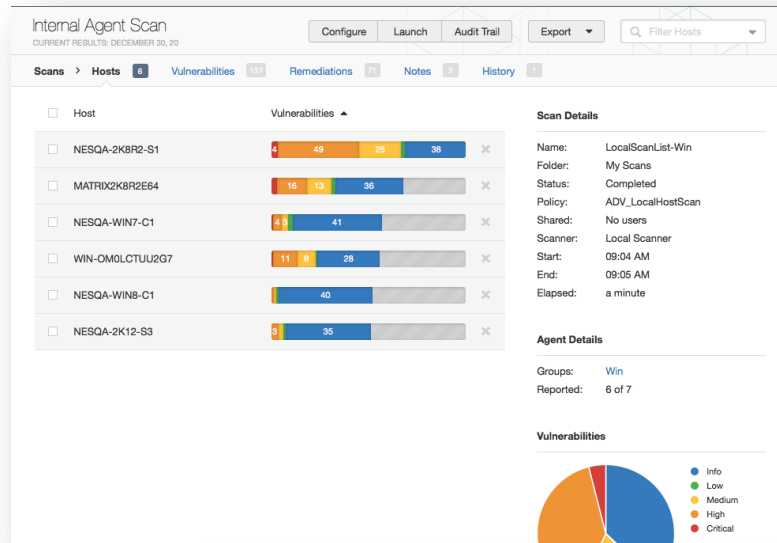


Scan dashboards only are available for completed scans. Uploaded scans do not have dashboards enabled by default.

Scan results can be navigated by vulnerabilities or hosts, displaying ports and specific vulnerability information. The default view/tab is by host summary, which shows a list of hosts with a color-coded vulnerability summary per host.

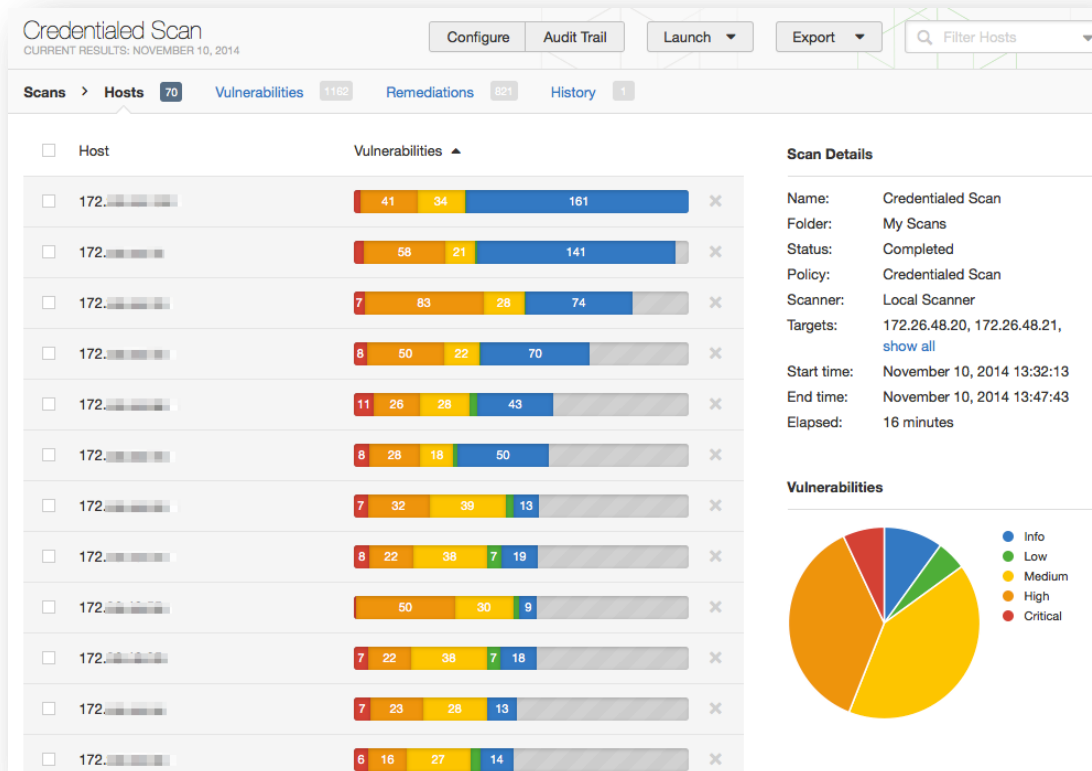


The Nessus Agent scan results can be navigated the same way as the Nessus scanners.

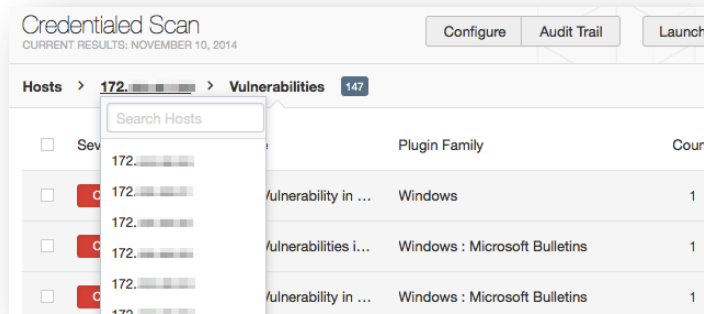


From the **Hosts** summary view, each summary will contain details about the vulnerability or informational findings, as well as **Host Details**, which provides general information about the host scanned.

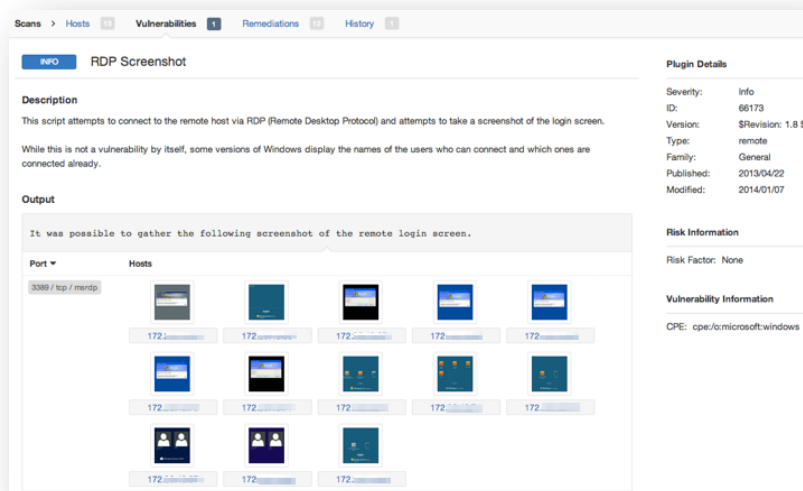
If **Allow Post-Scan Report Editing** was selected in the scan policy, a host can be deleted from the scan results by selecting the delete icon to the right of **Host Details**.



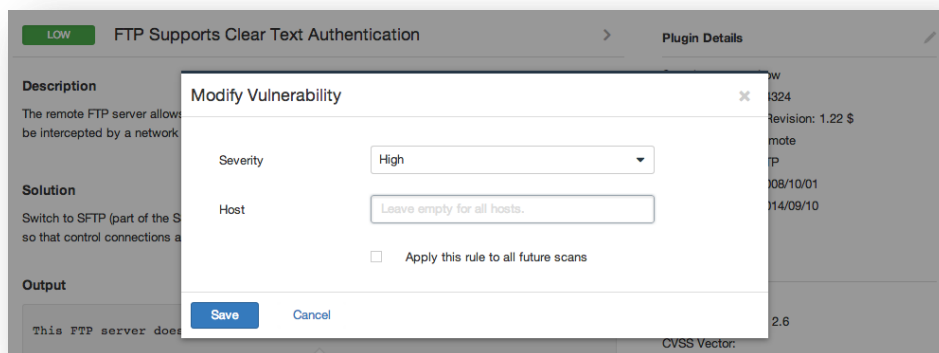
To quickly change between hosts after you have already selected one, click on the host via the navigation flow at the top to display a drop-down menu of other hosts. If there are numerous hosts, a search box will be available for quick host location:



Clicking on a vulnerability via the **Hosts** or **Vulnerabilities** tab will display vulnerability information including a description, solution, references, and any available plugin output. **Plugin Details** will be displayed on the right providing additional information about the plugin and associated vulnerability. From this screen, the pen icon to the right of **Plugin Details** can be used to modify the displayed vulnerability:



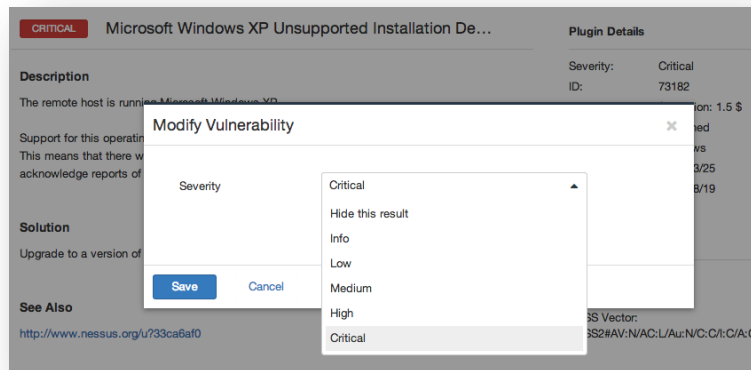
Clicking on the pen icon will display a dialog as shown below:



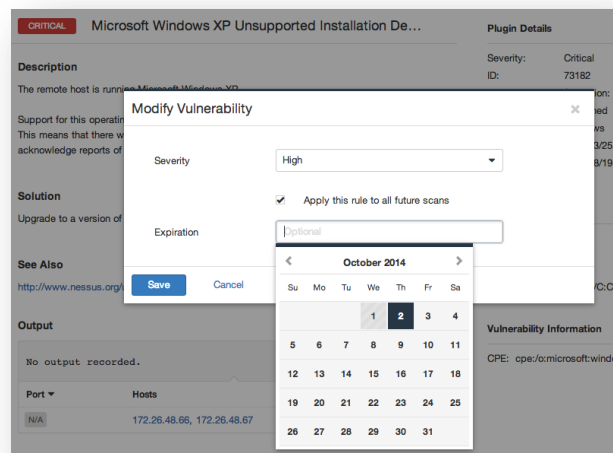


The host input in the **Modify Vulnerability** dialogue only shows when you choose to modify a vulnerability under a host, not from the vulnerability overview list.

The severity drop-down menu will enable you to re-classify the severity rating of the vulnerability in question, and also to hide it from the report:



Once the change is made, clicking **Save** will save the change and apply it to the vulnerability in question. In addition, the modification can be applied to all future reports by clicking the option. Doing so will bring up a dialog box allowing you to set an optional expiration date for the modification rule:



An expiration date can be selected using the calendar. Upon that date, the specified modification rule will no longer be applied to that finding.

Note that global rules for recasting plugin risk/severity can be established in the **User Profile -> Plugin Rules** area within Nessus.



The severity ratings are derived from the associated CVSS score, where 0 is Info, less than 4 is Low, less than 7 is Medium, less than 10 is High, and a CVSS score of 10 will be flagged Critical.

Selecting the **Vulnerabilities** tab at the top will switch to the Vulnerability View. This will sort the results by vulnerabilities rather than hosts, and include the number of hosts affected to the right. Selecting a vulnerability will provide the same information as before, but also include a list of affected hosts at the bottom, along with relevant output for each host.

The screenshot shows the 'Credentialed Scan' interface with the 'Vulnerabilities' tab selected. The main view displays the 'Unsupported Unix Operating System' vulnerability, which is marked as 'CRITICAL'. The description states that the remote Unix operating system is obsolete and no longer maintained by its vendor or provider. The solution is to upgrade to a newer version. The output section shows that CentOS release 3 support ended on 2010-10-31, and users are advised to upgrade to CentOS 7 / 6 / 5. The plugin details on the right include: Severity: Critical, ID: 33850, Version: \$Revision: 1.195 \$, Type: combined, Family: General, Published: 2008/08/08, and Modified: 2014/11/03. The risk information shows a Risk Factor of Critical, CVSS Base Score of 10.0, and CVSS Vector of CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C. At the bottom, a table lists affected hosts, showing '172.17.0.1' as the only host affected.

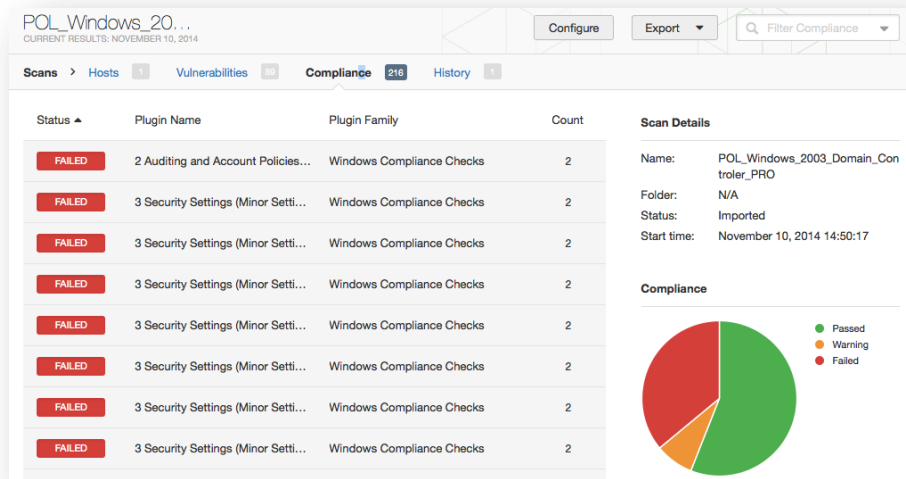
In cases where one host has multiple findings on different ports, the results will be broken down by host and further broken down by port:

The screenshot shows the 'Default Network Scan' interface with the 'Vulnerabilities' tab selected. The main view displays the 'Nessus SNMP Scanner' vulnerability, which is marked as 'INFO'. The description states that this plugin runs an SNMP scan against the remote machine to find open ports. The output section shows that Port 7/tcp was found to be open, Port 7/udp was found to be open, and Port 9/tcp was found to be open. The plugin details on the right include: Severity: Info, ID: 14274, Version: \$Revision: 1.29 \$, Type: remote, Family: Port scanners, Published: 2004/08/15, and Modified: 2011/03/11. The risk information shows a Risk Factor of None. At the bottom, a table lists affected hosts, showing '172.17.0.1' as the only host affected, with multiple findings on different ports.

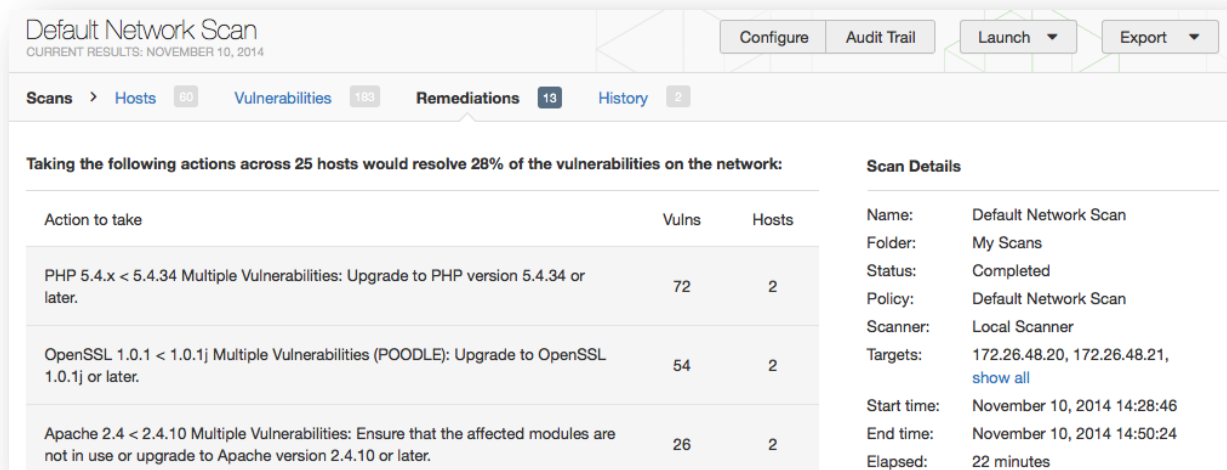
Clicking on an affected host at the bottom will load the host-based view of vulnerabilities.

Compliance Results

If a scan is initiated that uses a compliance check, the results will be found on a separate tab at the top called **Compliance**.



In addition to the **Hosts** and **Vulnerabilities** tabs, Nessus offers three additional tabs. The first is a **Remediations** tab that provides summary information to remediate major issues that have been discovered. This advice is intended to provide you with the most effective mitigation that will significantly reduce the risk posed by vulnerabilities:



The second tab is called Notes and offers advice to enhance your scan results or contains warnings:

Scans > Hosts 74 Vulnerabilities 1129 Remediations 632 **Notes 1** History 1

Scan Notes

Windows Autoruns Unique Failed
The Autoruns Unique plugin was not able to run because less than 2 systems were scanned successfully with credentials.

Scan Details

Name: Internal Patch Audit
Folder: My Scans
Status: Completed
Policy: Patch Audit
Scanner: Local Scanner
Targets: 172.26.48.20, 172.26.48.21, [show all](#)
Start time: October 01, 2014 09:48:26
End time: October 01, 2014 10:07:25
Elapsed: 19 minutes

The third tab is called **History** and it shows the scans and the list of scans by start time, end time, and status. To view an earlier scan result, select the scan in the list. The current indication will update to show the current scan result you are viewing.

Default Network Scan
CURRENT RESULTS: NOVEMBER 10, 2014

Configure Audit Trail Launch Export

Scans > Hosts 74 Vulnerabilities 1129 Remediations 632 **History 2**

<input type="checkbox"/>	Start Time	End Time	Status		
<input checked="" type="checkbox"/>	Current	Novem...	November 10, 2...	✓ Completed	✕
<input type="checkbox"/>	May 29, 2014 14...	May 29, 2014 14...	May 29, 2014 14...	✓ Completed	✕

Scan Details

Name: Default Network Scan
Folder: My Scans
Status: Completed
Policy: Default Network Scan
Scanner: Local Scanner
Targets: 172.26.48.20, 172.26.48.21, [show all](#)
Start time: November 10, 2014 14:28:46
End time: November 10, 2014 14:50:24
Elapsed: 22 minutes

Vulnerabilities

Info Low Medium High Critical

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.

The first filter type is a simple text string entered into the **Filter Vulnerabilities** box on the upper right. As you type, Nessus will immediately begin to filter the results based on your text and what it matches in the titles of the findings. The second filter type is more comprehensive and allows you to specify more details. To create this type of filter, begin by clicking on the down arrow on the right side of the **Filter Vulnerabilities** box. Filters can be created from any report tab. Multiple filters can be created with logic that allows for complex filtering. A filter is created by selecting the plugin attribute, a filter argument, and a value to filter on. When selecting multiple filters, specify the keyword Any or All accordingly. If All is selected, then only results that match **all** filters will be displayed:

Once a filter has been set, it can be removed individually by clicking on the ✕ to the right. Additionally, all filters can be removed at the same time by selecting **Clear Filters**. The report filters allow for a wide variety of criteria for granular control of results. The following filter attributes will be present if they are found in the scan results. If an attribute is not present in the scan results, Nessus will suppress them from the filters for convenience:

Option	Description
Plugin ID	Filter results if Plugin ID <i>is equal to</i> , <i>is not equal to</i> , <i>contains</i> , or <i>does not contain</i> a given string (e.g., 42111).
Plugin Description	Filter results if Plugin Description <i>contains</i> , or <i>does not contain</i> a given string (e.g., remote).
Plugin Name	Filter results if Plugin Name <i>is equal to</i> , <i>is not equal to</i> , <i>contains</i> , or <i>does not contain</i> a given string (e.g., windows).
Plugin Family	Filter results if Plugin Name <i>is equal to</i> or <i>is not equal to</i> one of the designated Nessus plugin families. The possible matches are provided via a drop-down menu.
Plugin Output	Filter results if Plugin Description <i>is equal to</i> , <i>is not equal to</i> , <i>contains</i> , or <i>does not contain</i> a given string (e.g., PHP)
Plugin Type	Filter results if Plugin Type <i>is equal to</i> or <i>is not equal to</i> one of the two types of plugins: local or remote.
Solution	Filter results if the plugin Solution <i>contains</i> or <i>does not contain</i> a given string (e.g., upgrade).
Synopsis	Filter results if the plugin Solution <i>contains</i> or <i>does not contain</i> a given string (e.g., PHP).
Hostname	Filter results if the host <i>is equal to</i> , <i>is not equal to</i> , <i>contains</i> , or <i>does not contain</i> a given string (e.g., 192.168 or lab).
Port	Filter results based on if a port <i>is equal to</i> , <i>is not equal to</i> , <i>contains</i> , or <i>does not contain</i> a given string (e.g., 80).
Protocol	Filter results if a protocol <i>is equal to</i> or <i>is not equal to</i> a given string (e.g., http).
CWE	Filter results based on Common Weakness Enumeration (CWE™) if a CVSS vector <i>is equal to</i> , <i>is not equal to</i> , <i>contains</i> , or <i>does not contain</i> a CWE reference number (e.g., 200).
CPE	Filter results based on if the Common Platform Enumeration (CPE) <i>is equal to</i> , <i>is not equal to</i> , <i>contains</i> , or <i>does not contain</i> a given string (e.g., Solaris).
CVSS Base Score	Filter results based on if a CVSS base score <i>is less than</i> , <i>is more than</i> , <i>is equal to</i> , <i>is not equal</i>



Option	Description
	<p>to, contains, or does not contain a string (e.g., 5).</p> <div><p>This filter can be used to select by risk level. The severity ratings are derived from the associated CVSS score, where 0 is Info, less than 4 is Low, less than 7 is Medium, less than 10 is High, and a CVSS score of 10 will be flagged Critical.</p></div>
CVSS Temporal Score	Filter results based on if a CVSS temporal score is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (e.g., 3.3).
CVSS Temporal Vector	Filter results based on if a CVSS temporal vector is equal to, is not equal to, contains, or does not contain a given string (e.g., E:F).
CVSS Vector	Filter results based on if a CVSS vector is equal to, is not equal to, contains, or does not contain a given string (e.g., AV:N).
Vulnerability Publication Date	Filter results based on if a vulnerability publication date <i>earlier than, later than, on, not on, contains, or does not contain</i> a string (e.g., 01/01/2012). Note: Pressing the  button next to the date will bring up a calendar interface for easier date selection.
Patch Publication Date	Filter results based on if a vulnerability <u>patch</u> publication date is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (e.g., 12/01/2011).
Plugin Publication Date	Filter results based on if a Nessus plugin publication date is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (e.g., 06/03/2011).
Plugin Modification Date	Filter results based on if a Nessus plugin modification date is less than, is more than, is equal to, is not equal to, contains, or does not contain a string (e.g., 02/14/2010).
CVE	Filter results based on if a CVE reference is equal to, is not equal to, contains, or does not contain a given string (e.g., 2011-0123).
Bugtraq ID	Filter results based on if a Bugtraq ID is equal to, is not equal to, contains, or does not contain a given string (e.g., 51300).
CERT Advisory ID	Filter results based on if a CERT Advisory ID (now called Technical Cyber Security Alert) is equal to, is not equal to, contains, or does not contain a given string (e.g., TA12-010A).
OSVDB ID	Filter results based on if an Open Source Vulnerability Database (OSVDB) ID is equal to, is not equal to, contains, or does not contain a given string (e.g., 78300).
Secunia ID	Filter results based on if a Secunia ID is equal to, is not equal to, contains, or does not contain a given string (e.g., 47650).
Exploit Database ID	Filter results based on if an Exploit Database ID (EBD-ID) reference is equal to, is not equal to, contains, or does not contain a given string (e.g., 18380).
Metasploit Name	Filter results based on if a Metasploit name is equal to, is not equal to, contains, or does not contain a given string (e.g., xslt_password_reset).
Exploited by Malware	Filter results based on if the presence of a vulnerability is exploitable by malware is equal to or is not equal to true or false.
IAVA	Filter results based on if an IAVA reference is equal to, is not equal to, contains, or does not contain a given string (e.g., 2012-A-0008).

Option	Description
IAVB	Filter results based on if an IAVB reference <i>is equal to, is not equal to, contains, or does not contain</i> a given string (e.g., 2012-A-0008).
IAVM Severity	Filter results based on the IAVM severity level (e.g., IV).
IAVT	Filter results based on if an IAVT reference <i>is equal to, is not equal to, contains, or does not contain</i> a given string (e.g., 2012-A-0008).
See Also	Filter results based on if a Nessus plugin see also reference <i>is equal to, is not equal to, contains, or does not contain</i> a given string (e.g., seclists.org).
Risk Factor	Filter results based on the risk factor of the vulnerability (e.g., Low, Medium, High, Critical).
Exploits Available	Filter results based on the vulnerability having a known public exploit.
Exploitability Ease	Filter results based on if the exploitability ease <i>is equal to or is not equal to</i> the following values: <i>Exploits are available, No exploit is required, or No known exploits are available</i> .
Metasploit Exploit Framework	Filter results based on if the presence of a vulnerability in the Metasploit Exploit Framework <i>is equal to or is not equal to</i> true or false.
CANVAS Exploit Framework	Filter results based on if the presence of an exploit in the CANVAS exploit framework <i>is equal to or is not equal to</i> true or false.
CANVAS Package	Filter results based on which CANVAS exploit framework package an exploit exists for. Options include CANVAS, D2ExploitPack, or White_Phosphorus.
CORE Exploit Framework	Filter results based on if the presence of an exploit in the CORE exploit framework <i>is equal to or is not equal to</i> true or false.
Elliot Exploit Framework	Filter results based on if the presence of an exploit in the Elliot exploit framework <i>is equal to or is not equal to</i> true or false.
Elliot Exploit Name	Filter results based on if an Elliot exploit <i>is equal to, is not equal to, contains, or does not contain</i> a given string (e.g., Typo3 FD).
ExploitHub	Filter results based on if the presence of an exploit on the ExploitHub web site <i>is equal to or is not equal to</i> true or false.

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.

If a filter option is not available, it means that the report contains nothing that meets the criteria. For example, if Microsoft Bulletin is not on the filter dropdown list, then no vulnerabilities were found that reference a Microsoft Bulletin.

As a filter is created, the scan results will be updated to reflect the new filter criteria after selecting **Apply**. The down arrow in the **Filter Vulnerabilities** box will change to a numeric representation of how many filters are currently being applied.

Once the results have been filtered to provide the data set you want, click **Export Results** to export just the filtered results. To receive a report with all of the results, remove all filters and use the export feature.

Nessus scan results provide a concise list of plugins that detected issues on the host. However, there are times where you may want to know why a plugin **did not** return results. The **Audit Trail** functionality will provide this information. Begin by clicking Audit Trail located on the upper right-hand side:

CRITICAL Samba 'AndX' Request Heap-Based Buffer Overflow

Description
The remote Samba install is prone to a heap-based buffer overflow attack.

An attacker can exploit this issue to execute arbitrary code with the privileges of the application. Failed exploit attempts will result in a denial of service condition.

Solution
Apply patches from the vendor.

See Also
<https://www.samba.org/samba/security/CVE-2012-0670.html>
<https://www.samba.org/samba/history/security.html>

Output
No output recorded.

Port	Hosts
445 / tcp / cifs	172.17.0.1

Plugin Details

Severity: Critical
ID: 58327
Version: \$Revision: 1.6 \$
Type: remote
Family: Misc.
Published: 2012/03/13
Modified: 2014/03/28

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C
CVSS Temporal Score: 7.4

Vulnerability Information

CPE: cpe:/a:samba:samba
Exploit Available: false

This will bring up the Audit Trail dialogue box. Begin by entering the ID of the plugin you want to know more about. Click **Search** and a host or list of hosts will be displayed that relates to your query. Optionally, you can supply a host IP for the initial query to limit the results to a target of interest. Once the host(s) are displayed, click on one to display information about why the plugin did not fire:

Audit Trail

Plugin ID

58327

Host

Host (Example: localhost)

Search

Failed to read a response from the Samba service listening on port 445.

Exit	Hosts
58327/1	172.16.1.1, 172.16.1.2
	172.16.1.3



Due to the resources required for the audit trail, there are cases where only a partial audit trail will be provided. For a single scanned host, the full audit trail is available. If between 2 and 512 hosts are scanned, a full audit trail is only available if the Nessus server has more than 1 CPU and 2G of RAM. Scanning over 512 hosts will always result in a partial audit trail.

The audit trail is only available for scans that originated on the host or were imported from a Nessus DB format (.db).

Report Screenshots

Nessus also has the ability to take screenshots during a vulnerability scan and include them in a report.

For example, if Nessus discovers VNC running without a password to restrict access, a screenshot will be taken to show the session and included in the report.

In the example below, a VNC was discovered where the login screen shows the administrator logged in to the system.

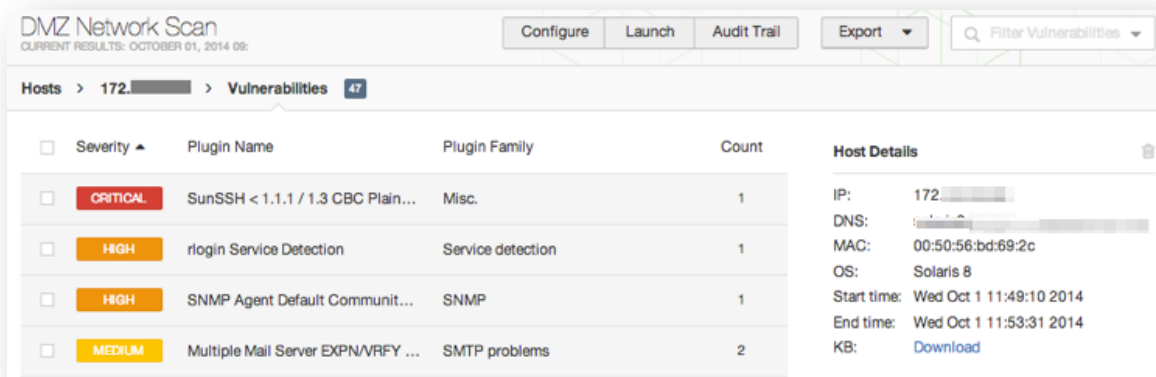


This feature must be enabled in the **Scan Web Applications** section of a scan policy, under **General**.

Scan Knowledge Base

A Knowledge Base (KB) is saved with every scan performed. This is an ASCII text file containing a log of information relevant to the scan performed and results found. A KB is often useful during cases where you need support from Tenable, as it allows Support staff to understand exactly what Nessus did, and what information was found.

To download a KB, select a report and then a specific host. To the right of the host name or IP there is link titled **Host Details**. Click on this and one of the host details is **KB** with a **Download** link:



Only scans performed on the host will have an associated KB. Imported scans do not carry the KB with them.

Compare the Results (Diff)

With Nessus, you can compare two scan reports against each other to display any differences. The ability to show scan differentials helps to point out how a given system or network has changed over time. This helps in compliance analysis 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 **Scans** list, click on **History**, check the reports you wish to compare, and select **Diff** from the upper right corner:

The screenshot shows the Nessus interface for a 'Default Network Scan'. The top navigation bar includes 'Scans', 'Hosts', 'Vulnerabilities', 'Remediations', and 'History'. The 'History' tab is active, showing a table of scan results. The table has columns for 'Start Time', 'End Time', and 'Status'. Two scans are listed: one from November 10, 2014, and another from May 29, 2014, both marked as 'Completed'. To the right of the table, the 'Scan Details' section provides information about the scan, including its name, folder, status, policy, scanner, targets, start time, end time, and elapsed time. Below the details, a 'Vulnerabilities' section features a pie chart showing the distribution of vulnerability severity levels: Info (blue), Low (green), Medium (yellow), High (orange), and Critical (red).

Start Time	End Time	Status
Novem...	November 10, 2...	Completed
May 29, 2014 14...	May 29, 2014 14...	Completed

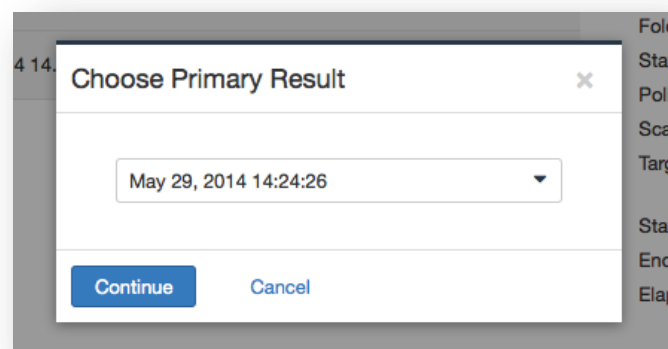
Scan Details

Name: Default Network Scan
Folder: My Scans
Status: Completed
Policy: Default Network Scan
Scanner: Local Scanner
Targets: 172.172.172.172, show all
Start time: November 10, 2014 14:28:46
End time: November 10, 2014 14:50:24
Elapsed: 22 minutes

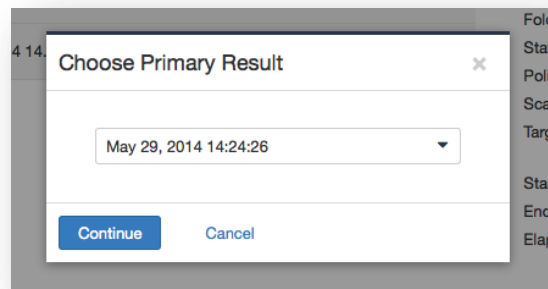
Vulnerabilities

Legend: Info (blue), Low (green), Medium (yellow), High (orange), Critical (red)

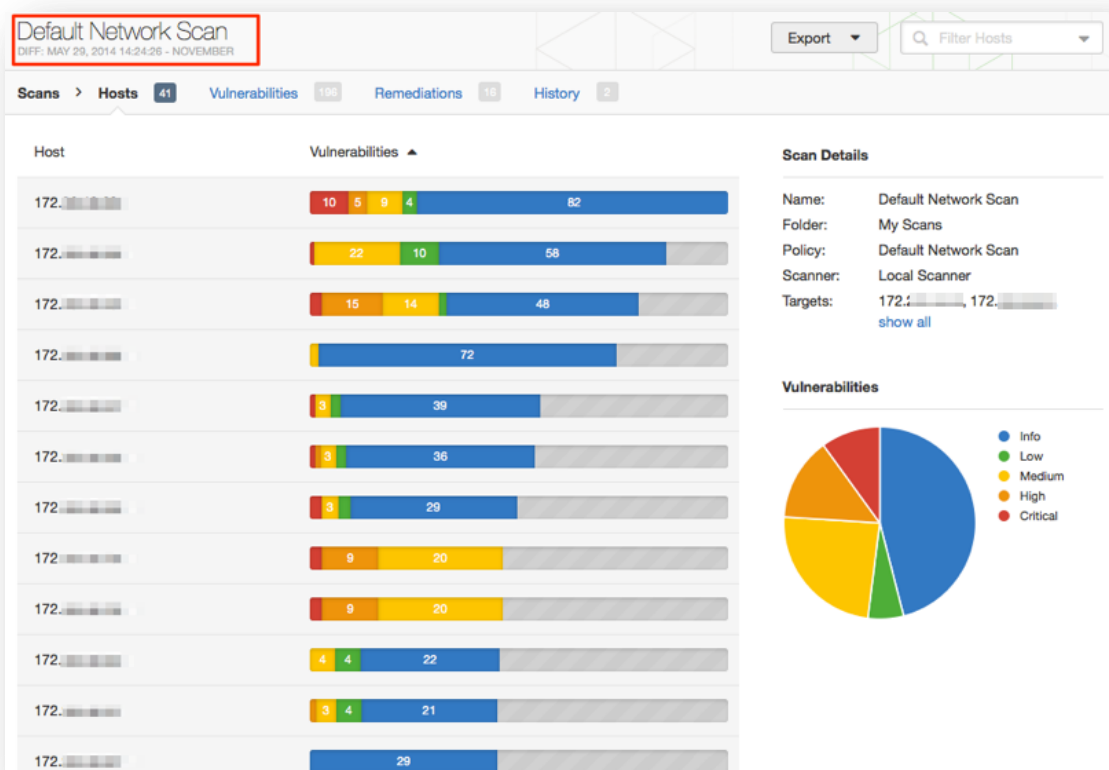
Nessus will compare the first report selected with the second and produce a list of results that are different since the first. The compare feature shows what is new since the baseline (i.e., the first report selected), not produce a differential of any two reports. This comparison highlights which vulnerabilities have been found or remediated between the two scans.



In the example above, DMZ Network Scan is an unauthenticated scan of a DMZ, performed several times.



The results display the differences and highlighting vulnerabilities that were not found in the October 1 scan with a Diff report:



Managing Reports

Nessus provides ways of managing your scan reports.

Uploading and Exporting Reports

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

Users can create their own report by chapters: Host Summary (Executive), Vulnerabilities by Host, Compliance Check (Executive), Suggested Remediations, Vulnerabilities by Plugin, or Compliance Check. The HTML format is still supported by default. For scanner hosts running Unix with Oracle Java installed, users can export reports in PDF as well as the other

supported formats: CSV, or the Nessus DB. By using the report filters and export features, users can create dynamic reports of their own choosing instead of selecting from a specific list.



Nessus DB format is an encrypted proprietary format. Note that the Nessus DB includes all the possible data about a scan, including but not limited to the results, the audit trails, and attachments.

To export a scan, begin by selecting a specific scan from the **Scans** screen, and then click on the **Export** drop-down at the top. Next, choose your file format.



Only compliance scans performed with Nessus can be exported to PDF or HTML formats with compliance chapters. Imported scans from previous versions of Nessus will not export in that manner.

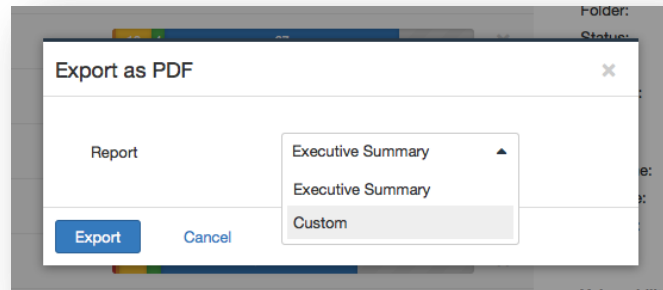
Reports can be downloaded in several formats. Note that some formats will not allow chapter selection and include all information.

Option	Description
.nessus	<p>An XML-based format and the de-facto standard in Nessus 4.2 and later. This format uses an expanded set of XML tags to make extracting and parsing information more granular. This report does not allow chapter selection.</p> <p>If the policy is exported and saved to a .nessus file, the passwords will be stripped.</p> <p>When importing a .nessus file format, you will need to re-apply your passwords to the credentials being used.</p>
Nessus DB	<p>A proprietary encrypted database format used in Nessus 5.2 and later that contains all the information in a scan, including the audit trails and results. When exporting to this format, you will be prompted for a password to encrypt the results of the scan.</p>
HTML	<p>A report generated using standard HTML that allows chapter selection. This report will open in a new tab in your browser.</p>
PDF	<p>A report generated in PDF format that allows chapter selection. Depending on the size of the report, PDF generation may take several minutes.</p> <p>Oracle Java (formerly Sun Microsystems' Java) is required for PDF report functionality on Unix based systems.</p>
CSV	<p>A comma-separated values (CSV) export that can be used to import into many external programs such as databases, spreadsheets, and more. This report does not allow chapter selection.</p>

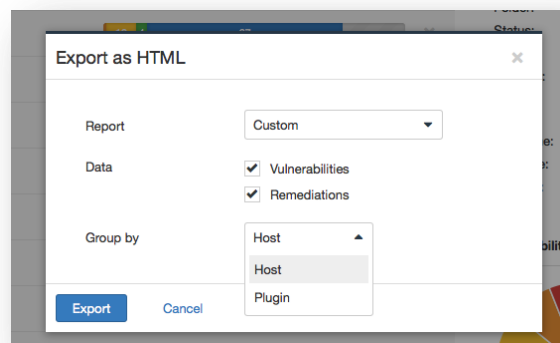
After selecting a format, your standard web browser **Save File** dialog will be displayed, allowing you to save the scan results to the location of your choice.

HTML and PDF Customization

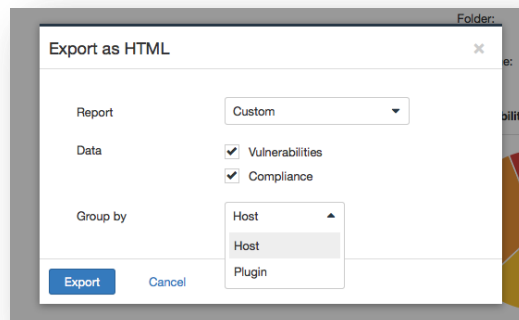
For HTML and PDF formats, Nessus will display a drop-down that will let you choose an **Executive Summary** or **Custom** report:



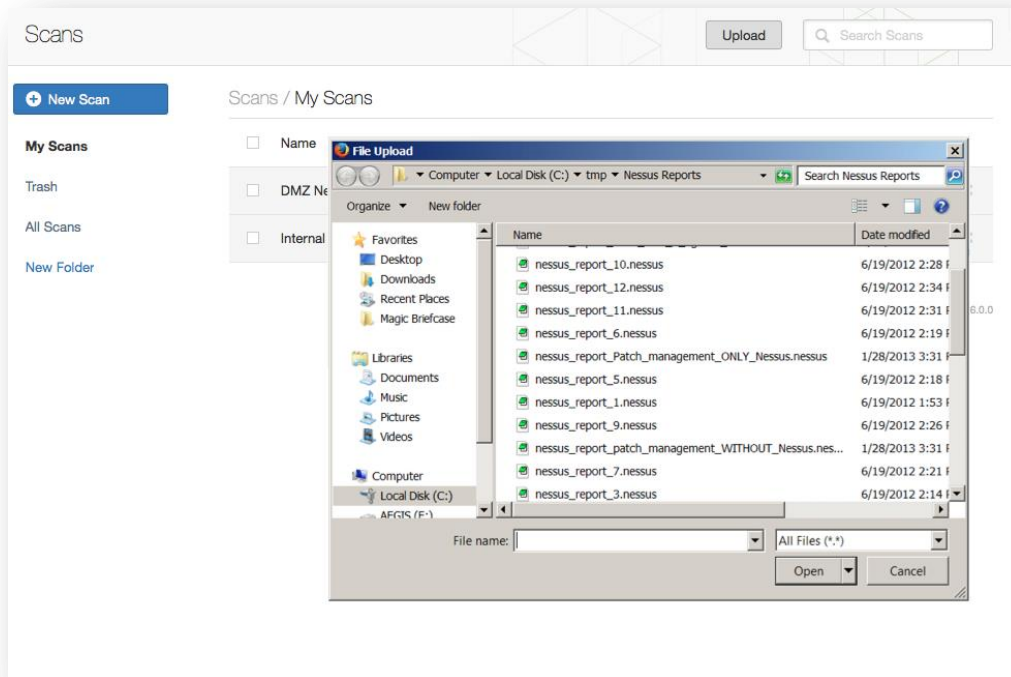
The custom drop-down allows you to specify the information to be included. This includes the vulnerabilities and remediation data, and how to group the information (by host or by plugin):



Note: The compliance scan will show different export options under a custom report:



To import a report, click on the **Upload** button on the top bar of the **Scans** screen to open a file browse window:



Select the **.nessus** scan file you want to import and click on **Open**. Nessus will parse the information and make it available in the **Scans** interface.

Nessus File Formats

Nessus uses two specific file formats (**.nessus** and **.db**) for scan export and import. The **.nessus** 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 **Export** option from the **Scans** result. Please see the [Nessus v2 File Format](#) document for more details on **.nessus** files.

The Nessus DB format (**.db**) contains all the possible data about a scan and provides a way to encrypt the file. The only way to access the file is by providing the password through a Nessus report upload.

Deleting Scan Results

Once you are finished with scan results, you can click the X to the right of the scan from the **History** tab in a scan result to move the scan to the Trash:

Scans / My Scans				
<input type="checkbox"/>	Name		Last Scan ▲	
<input type="checkbox"/>	DMZ Network Scan	✓	12:51 PM	▶ ✕
<input type="checkbox"/>	Internal Patch Audit	✓	12:51 PM	▶ ✕
<input type="checkbox"/>	POL_Windows_2003_Domain_Controller_PRO	↑	10:51 AM	▶ Trash
<input type="checkbox"/>	Home Network	↑	10:15 AM	▶ ✕

Select the **Trash** folder and you can empty the trash to permanently delete the scan.

Scans / Trash				
<input type="checkbox"/>	Name		Last Scan ▲	
<input type="checkbox"/>	Main Comp - credentialed	↑	10:50 AM	▶ ✕
<input type="checkbox"/>	Home Network	↑	10:15 AM	▶ ✕



This action cannot be undone! Use the **Export** feature to export your scan results before deleting.

Policies

A Nessus policy is a set 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.
- Offline configuration audits for network devices, allowing safe checking of network devices without needing to scan the device directly.

- Windows malware scans which compare the MD5 checksums of files, both known good and malicious files.
- Nessus 6.4 organizes policies into three categories: scanner templates, agent templates, and user-created policies. Clicking on the **New Policy** button in the Policies section brings up a list of available templates. The default policies are stored in the Policy Library. User-created policies are saved policies created from the default templates.

Create a New Policy

To create a new policy, click on **Policies** in the top navigation, and then click the **New Policy** button.

You can also search for policies using the **Search Library** box in the upper right corner.



Nessus Professional includes **Scanner Templates** only.



Depending on the template being used, settings may vary.

Policy Templates, like **Scanner Templates**, share many identical settings and configuration options.

Policy Templates do not include the following Settings, as do Scanner Templates: **Folder**, **Dashboard**, **Scanner**, **Targets**, **Schedule**, or **Email Notifications**.

In this section, settings and configuration options which only apply to **Policy Templates** will be addressed.

Scan > Settings (Basic Network Scan Policy Example)

Basic

Settings / Basic / General

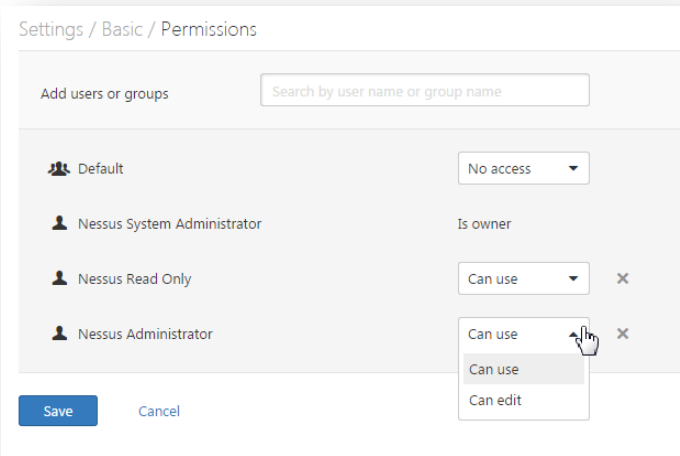
Settings / Basic / General

Name REQUIRED

Description

Save Cancel

General Option	Description
Name	Sets the name that will be displayed in the Nessus user interface to identify the Agent Scan .
Description	Provides a brief description of the scan policy, typically summarizing the overall purpose.



Permission	Description
Can Use	Users or groups specified here can view and use the policy in their scans. They will not be able to edit the policy.
Can Edit	Users or groups specified here can make changes to the policy and can use the policy.
No Access	Any users or groups specified here cannot view, use, or edit the policy.

Shared Template Pages and Settings

The following settings are shared across **Scanner Templates** and **Policy Templates**:

- [Settings > Discovery](#)
- [Settings > Assessment](#)
- [Settings > Report](#)
- [Settings > Advanced](#)
- [Credentials](#)
- [Compliance](#)
- [Plugins](#)

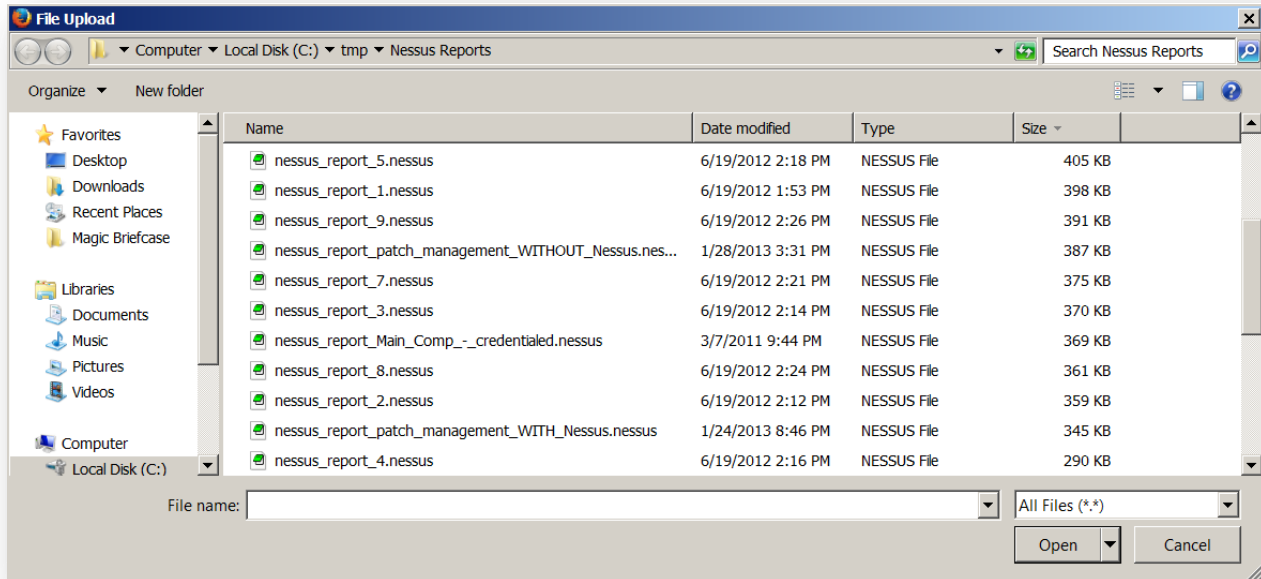
For all shared settings, refer to the [examples](#) found earlier in this document.

Manage Policies

To view your policies, click **Policies** in the top navigation of Nessus.

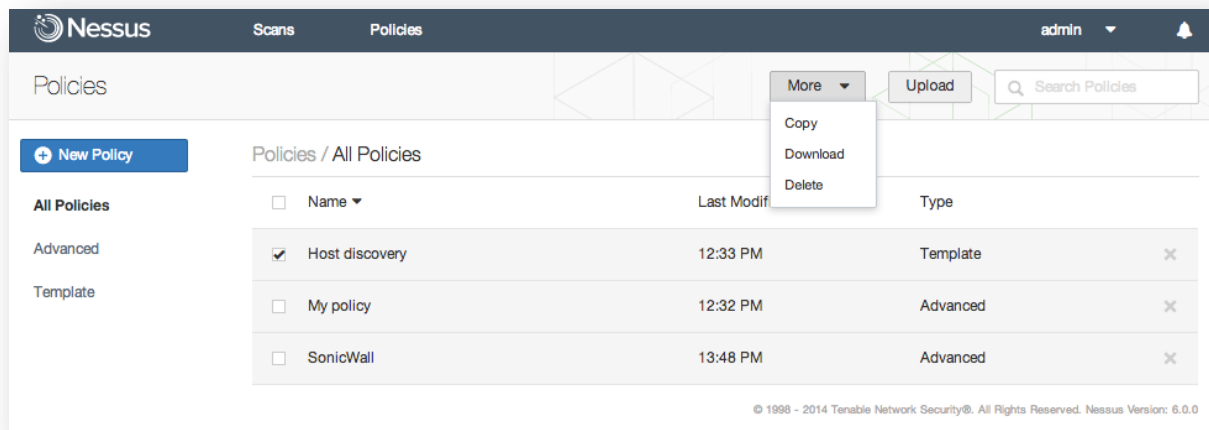
Upload a Policy

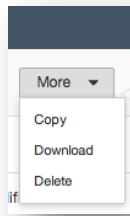
The **Upload** button on the Policies menu bar allows you to upload previously created policies to the scanner. Using the native file browser box, select the policy from your local system and click on **Open**:



More Options

When you select a policy and place a check in the box besides its name, the **More** button will appear.





Download a Policy

Clicking on **Download** will open the browser's download dialog box allows you to open the policy in an external program (e.g., text editor) or save the policy to the directory of your choice. Depending on the browser, the policy may be downloaded automatically.



Passwords and `.audit` files contained in a policy will not be exported.

Copy a Policy

To copy a policy, select a policy, then click the **More** button and choose **Copy**.

Delete a Policy

Deleting a policy is permanent; there is no folder from which the policy can be recovered.

Nessus Cloud & PCI ASV Validation

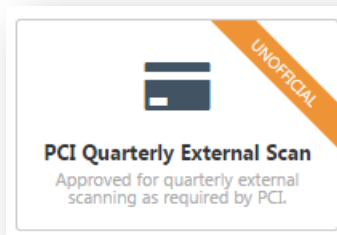
Tenable Network Security, Inc. is a PCI Approved Scanning Vendor (ASV), and is certified to validate vulnerability scans of Internet-facing systems for adherence to certain aspects of the PCI Data Security Standards (PCI DSS). Nessus Cloud includes a pre-built static PCI DSS policy that adheres to the quarterly scanning requirements of the PCI DSS v3.1. This policy may be used by merchants and providers for ongoing, continuous processes of scanning and vulnerability management. It is important to note that, while customers can use the PCI DSS scan policy to test their externally-facing systems as often as they wish, a scan must be submitted to Tenable for validation before it can be considered to qualify as a valid PCI ASV scan. Customers are allowed up to two quarterly report submissions for PCI ASV validation through Tenable Network Security, Inc.

Once logged into the service, customers have the option to select a policy titled PCI Quarterly External Scan that adheres to the requirements of the PCI ASV Program Guide v2.0 section titled ASV Scan Solution – Required Components.



To qualify as a PCI DSS ASV scan for validation through the Nessus Cloud, PCI Quarterly External Scan policy must be selected.

To create a PCI DSS ASV scan policy, go to **Policies** and click **+ New Policy**. Next, click on **PCI Quarterly External Scan**:



Settings / Basic / General

This template creates a scan that simulates an external scan (PCI DSS 11.2.2) performed by [Nessus Cloud](#) to meet PCI DSS quarterly scanning requirements. Although the results may not be submitted for validation, they may be used to see what "official" Nessus Cloud results might look like. Users that have external PCI scanning requirements should use this template in Nessus Cloud, which allows scanning unlimited times before submitting results to Tenable for validation (Nessus Cloud is a validated ASV solution).

Name REQUIRED

Description

[Save](#) [Cancel](#)

The default scan policy has been configured specifically to test for PCI compliance. There are a few additional options that you can configure as needed. From the **Policies** menu, select the policy you just created. Under the **Discovery** tab, you can opt to Scan unresponsive hosts:

Settings / Discovery / Host Discovery

☐ Scan unresponsive hosts
Enabling this setting forces Nessus to scan hosts that do not respond to any methods of ping.

[Save](#) [Cancel](#)

Under the **Advanced** tab, you can manipulate the **Scan Type**:

Settings / Advanced

Scan Type Default

Performance options:

- 20 simultaneous hosts (max)
- 4 simultaneous checks per host (max)
- 15 second network read timeout
- Slow down the scan when network congestion is detected

Save Cancel



Any policies created with the PCI Quarterly External Scan policy template cannot be edited further to ensure the required testing is performed.

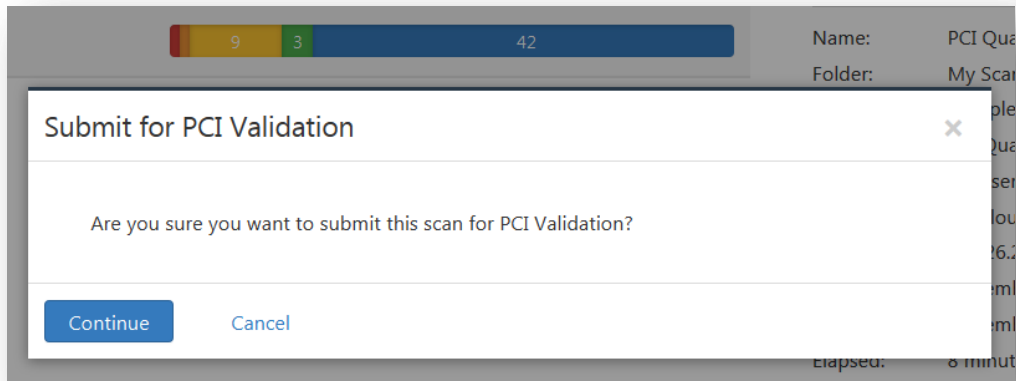
Submitting Scan Results for PCI Customer Review

Customers have the option to submit their scan results to Tenable Network Security for PCI ASV validation. By clicking Submit for PCI, the scan results will be uploaded to an administrative section of the Nessus Cloud for customer review, and the customer will be prompted to log in to the user section of the service to review the findings of the scan results from a PCI DSS perspective.

The screenshot shows the Nessus web interface. At the top, there's a navigation bar with 'Scans' (1) and 'Policies'. The main header shows 'PCI Quarterly for E...' with 'CURRENT RESULTS: NOVEMBER 20, 2014'. Below this, there are buttons for 'Configure', 'Audit Trail', 'Submit for PCI' (highlighted with a red box), and 'Export'. A search bar 'Filter Hosts' is also present. The main content area has tabs for 'Scans', 'Hosts' (1), 'Vulnerabilities' (48), 'Remediations' (1), and 'History' (1). Under the 'Hosts' tab, a host '172...' is shown with a bar chart indicating 9 vulnerabilities (red), 3 (yellow), and 42 (blue). To the right, 'Scan Details' are listed: Name: PCI Quarterly for Eval, Folder: My Scans, Status: Completed, Policy: PCI Quarterly for Eval, Shared with: No users, Scanner: US Cloud Scanner, Targets: 172..., Start time: November 20, 2014 19:41:03, End time: November 20, 2014 19:48:53, Elapsed: 8 minutes.

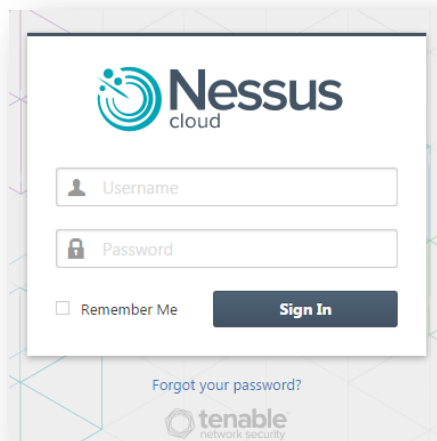


PCI-DSS ASV scans older than three months cannot be submitted for review. No Submit for PCI button will appear for those scans.



Customers are strongly urged to thoroughly review their PCI scan results before submitting their report(s) to Tenable Network Security through the Nessus Cloud. Reports with failed results are required to undergo a full PCI review cycle, of which Nessus Cloud customers are limited to two (2) per quarterly period.

Customer Review Interface



Once a customer logs into the [PCI Validation user section](#), they are presented with a list of reports that have been submitted by their unique Nessus Cloud login. The Report Filter allows reports to be filtered by Owner, Name, and Status.



Report Filter

Report Owner

Report Name

Report Status

All

Vulnerability Filters

Ticket Filters

More Filters

Apply Filters

Clear Filters

Report Filters None

List Of Reports

Show 10 entries

Search:

Name	Compliance	Status	Owner	Failed Items	Tickets	Open Tickets	Upload Time	Last Updated
PCI ASV Scan		Review Required	pciccontent@tenable.com	30	0	0	2013-05-21 16:09:35	2013-05-21 16:09:35

Showing 1 to 1 of 1 entries

Reviewing Scan Results

To pass a PCI DSS ASV assessment, all items (except for denial of service (DoS) vulnerabilities) listed as Critical, High, or Medium (or with a CVSS score of 4.0 or higher) must either be remediated or disputed by the customer, and all disputed items must either be resolved, accepted as exceptions, accepted as false positives, or mitigated through the use of compensating controls. All items listed as Critical, High, or Medium in the Nessus Cloud can be viewed in detail, and all items carry an option to dispute the item in question.

Clicking the name of the scan in the List of Reports allows the user to view a list of hosts and the number of vulnerabilities found on each host, sorted by severity.

Report Filter

Vulnerability Filters

Host Name

Plugin Id

Plugin Name

Severity

Port

Protocol

All

Vuln Filters None

More Filters None

List Of Hosts

Show 10 entries

Search:

Host Name	Host IP	Host FQDN	Low	Info	Medium	High	Disputed
72.	72.		5	78	28	9	0

Showing 1 to 1 of 1 entries

Clicking the number of Failed Items in the List of Reports will display a list of items that will need to be addressed in order to qualify for a compliant ASV report through Tenable's Nessus Cloud.



Nessus Cloud customers are responsible for reviewing all of their Failed Items before submitting a scan report to Tenable Network Security. Selecting the Failed Items in the List of Reports allows you to jump directly to the items that may affect your PCI ASV Validation compliance status.

List Of Items

Show **10** entries Search:

	Host	PluginId	Port(Proto)	SvcName	Severity	CvssScore	PluginName	Disputed
+	72.14.215.104	200012	0(tcp)	general	High	0	pcidss:expired_ssl_certificate	no
+	72.14.215.104	200001	0(tcp)	general	High	0	pcidss:directory_browsing	no
+	72.14.215.104	33929	0(tcp)	general	High	0	PCI DSS compliance	no
+	72.14.215.104	33929	443(tcp)	www	High	0	PCI DSS compliance	no
+	72.14.215.104	33929	27299(tcp)	pop3	High	0	PCI DSS compliance	no
+	72.14.215.104	56209	0(tcp)	general	Medium	0	PCI DSS compliance : Remote Access Software Has Been Detected	no
+	72.14.215.104	57792	443(tcp)	www	Medium	4.3	Apache HTTP Server httpOnly Cookie Information Disclosure	no
+	72.14.215.104	57792	80(tcp)	www	Medium	4.3	Apache HTTP Server httpOnly Cookie Information Disclosure	no
+	72.14.215.104	50600	80(tcp)	www	Medium	5	Apache Shiro URI Path Security Traversal Information Disclosure	no
+	72.14.215.104	56818	80(tcp)	www	Medium	6.4	CGI Generic Cross-Site Request Forgery Detection (potential)	no

Showing 1 to 10 of 30 entries

Use the green + button under the far left column to expand an individual entry for additional vulnerability details.

72.14.215.104 17744 22(tcp) ssh Medium 6.4 OpenSSH >= 2.3.0 AllowTcpForwarding Port Bouncing no

Dispute

Synopsis

The remote SSH server may permit anonymous port bouncing.

Description

According to its banner, the remote host is running OpenSSH, version 2.3.0 or later. Such versions of OpenSSH allow forwarding TCP connections. If the OpenSSH server is configured to allow anonymous connections (e.g. AnonCVS), remote, unauthenticated users could use the host as a proxy.

Solution

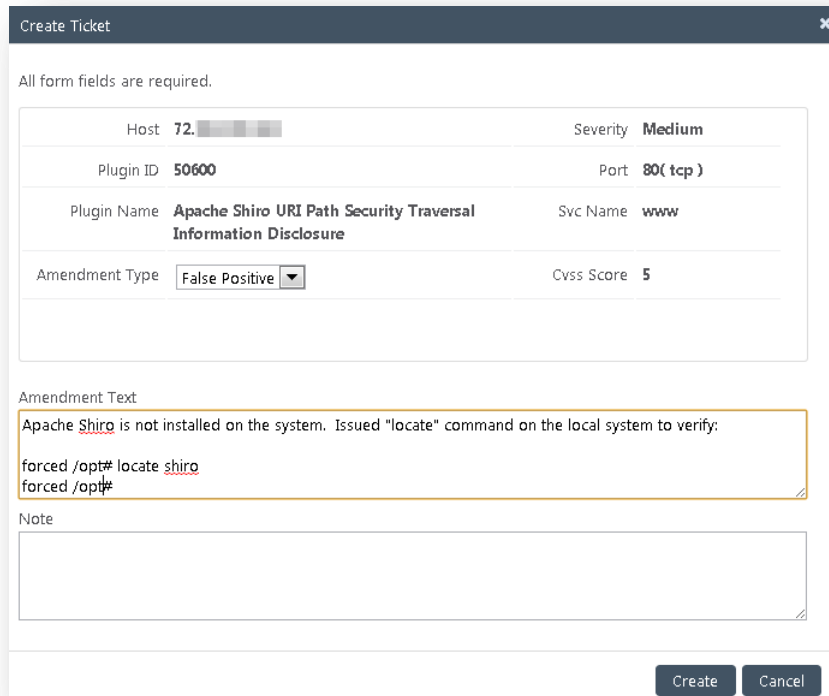
Disallow anonymous users, set AllowTcpForwarding to 'no', or use the Match directive to restrict anonymous users.

Showing 1 to 10 of 30 entries

As shown above, a Dispute button is displayed for each individual item, which allows the customer to enter additional details about vulnerability remediation, or dispute what they believe may be a false positive generated by the initial scan.

Disputing Scan Results

When an item is disputed, a ticket is created that allows for the selection of an amendment type, the addition of text to the amendment, and any other notes that the customer may want to add prior to submission for review by Tenable Network Security.



The 'Create Ticket' dialog box contains the following fields and values:

All form fields are required.	
Host	72.142.250.100
Severity	Medium
Plugin ID	50600
Port	80(tcp)
Plugin Name	Apache Shiro URI Path Security Traversal Information Disclosure
Svc Name	www
Amendment Type	False Positive
Cvss Score	5

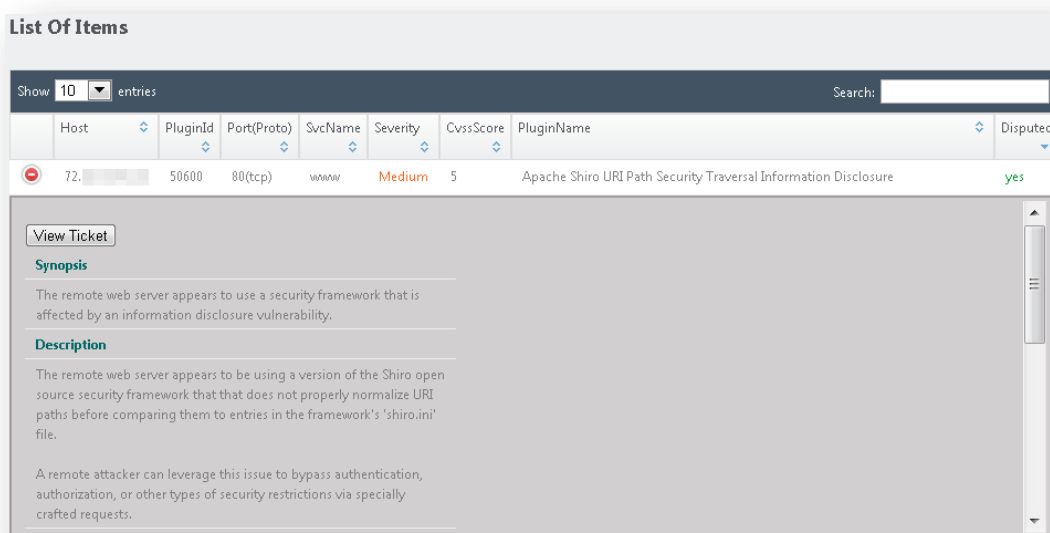
Amendment Text:

Apache Shiro is not installed on the system. Issued "locate" command on the local system to verify:
forced /opt# locate shiro
forced /opt#

Note:

Buttons: Create, Cancel

Once a ticket for a particular item has been created, the customer can view it by selecting the item in question and then selecting View Ticket.



The 'List Of Items' interface shows a table of scan results with the following columns: Host, PluginId, Port(Proto), SvcName, Severity, CvssScore, PluginName, and Disputed. The first entry is highlighted:

Host	PluginId	Port(Proto)	SvcName	Severity	CvssScore	PluginName	Disputed
72.142.250.100	50600	80(tcp)	www	Medium	5	Apache Shiro URI Path Security Traversal Information Disclosure	yes

Below the table, the 'View Ticket' button is visible. The ticket details are as follows:

Synopsis

The remote web server appears to use a security framework that is affected by an information disclosure vulnerability.

Description

The remote web server appears to be using a version of the Shiro open source security framework that does not properly normalize URI paths before comparing them to entries in the framework's 'shiro.ini' file.

A remote attacker can leverage this issue to bypass authentication, authorization, or other types of security restrictions via specially crafted requests.

Additional comments can be added by clicking the Edit button, then Add Note, and saving the note into the ticket by clicking Update.



Plugin 33929, PCI DSS Compliance, is an administrative plugin that links to the results of other plugins. If a report shows that a host is not PCI DSS compliant, resolving all failed items will then allow plugin 33929 to resolve and be replaced with plugin 33930, PCI DSS Compliance: Passed. In cases of disputes or exceptions, if all failed report items are successfully disputed or given exceptions, an exception can then be given for plugin 33929 based on the remediation of all other report issues.

Submitting Attachments as Evidence for a Dispute

Once a ticket is created, it is possible to submit supporting evidence as an attachment. After creating a ticket, click the number listed under Open Tickets to display all open tickets:

Show	10	entries	Search: <input type="text"/>							
	Name	Compliance	Status	Owner	Failed Items	Tickets	Open Tickets	Upload Time	Last Updated	
	PCI ASV Scan		Under User Review	pcicontent@tenable.com	30	1		2013-10-11 15:33:52	2013-10-11 15:35:54	<input type="button" value="Submit"/>

In the List of Tickets screen, click View:

Show 10 entries

Search:

Report Name	Host Name	Port	Plugin	Severity	Cvss Score	Status	Assigned To	Last Updated	
PCI ASV Scan	72.1.1.1	80(tcp)	50600	Medium	5	new		2013-10-11 15:35:54	View

Showing 1 to 1 of 1 entries

When the screen for the open ticket is displayed, options for Upload File and Attach are displayed:

Host	72.1.1.1	Severity	Medium
Plugin ID	50600	Port	80(tcp)
Plugin Name	Apache Shiro URI Path Security Traversal Information Disclosure	Svc Name	www
Status	new	Cvss Score	5
Assigned To	None	Attachments	None
Upload File:	<input type="button" value="Browse..."/> No file selected.	<input type="button" value="Attach"/>	
Amendment Type	False Positive		
Amendment Text	<input type="text" value="The server is not running Shiro"/>		

Click Browse... to navigate to and select the evidence file (screenshot, Word document, PDF, etc.) to be uploaded:

```
forced ~# slocate shiro
forced ~# █
```



Next, click Attach to attach the file to the ticket. When completed, the screen will display a message that the file was uploaded successfully:

Host	72.	Severity	Medium
Plugin ID	50600	Port	80(tcp)
Plugin Name	Apache Shiro URI Path Security Traversal Information Disclosure	Svc Name	www
Status	new	Cvss Score	5
Assigned To	None	Attachments	Download
Upload File:	<input type="button" value="Browse..."/> no_shiro.png	<input type="button" value="Attach"/>	The file was uploaded successfully!
Amendment Type	False Positive		
Amendment Text	The server is not running Shiro		

Clicking the Download link next to Attachments will show the names of all files attached to the ticket:

Submitting a Scan Report for Tenable Review

When tickets have been created for all outstanding report items under user review, the report can then be sent to Tenable Network Security for ASV review.

List Of Reports										
Show 10 entries		Search: <input type="text"/>								
	Name	Compliance	Status	Owner	Failed Items	Tickets	Open Tickets	Upload Time	Last Updated	
	PCI ASV Scan		Under User Review	pcicontent@tenable.com	30	30	30	2013-05-21 16:09:35	2013-05-22 08:57:44	<input type="button" value="Submit"/>
Showing 1 to 1 of 1 entries										

Before a report can be submitted for review, the customer must fill in contact information and agree to an attestation that includes mandatory text as described in the ASV Program Guide.

Report Submission

Contact Name: John Smith

Company: Tenable Network Security

Job Title: PCI Analyst

Phone: (410) 872-0555

Address: 7063 Columbia Gateway Dr

City: Columbia

State: MD

ZIP: 21046

URL: http://www.tenable.com

Next

Close

Report Submission

I attest that, this scan includes all components which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. I also acknowledges the following:

1) proper scoping of this external scan is my responsibility, and

2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of the PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

Previous

I Agree

Close

If a customer neglects to address any outstanding item for a particular scan before the report is submitted for ASV review, they will be prompted to make sure that a ticket has been created for each item. Any report with outstanding items that have not been addressed by the customer cannot be submitted to Tenable Network Security for review.

List Of Reports

Please make sure all the failed items are addressed.

Show 10 entries



Search:



	Name	Compliance	Status	Owner	Failed Items	Tickets	Open Tickets	Upload Time	Last Updated	
	PCI ASV Scan		Under User Review	pcicontent@tenable.com	30	30	30	2013-05-21 16:09:35	2013-05-22 08:57:44	Submit

When a report is finally submitted to Tenable Network Security for review, the status of the report changes from Under User Review to Under Admin Review and the Submit option is removed (greyed out) to prevent the submission of duplicate items or reports.

List Of Reports

Show entries Search:

	Name	Compliance	Status	Owner	Failed Items	Tickets	Open Tickets	Upload Time	Last Updated	
	PCI ASV Scan		Under Admin Review	pcicontent@tenable.com	30	30	30	2013-05-21 16:09:35	2013-05-22 09:18:21	<input type="button" value="Submit"/>

Showing 1 to 1 of 1 entries  








The Withdraw function within an open ticket is only available once a report has been submitted for review by Tenable's Nessus Cloud. Be careful when using the Withdraw function; withdrawing a ticket will cause the item in question to be flagged as unresolved due to having inconclusive evidence, and the report as a whole will be deemed as non-compliant.

If a Tenable Network Security staff member requests more information or if any other user action is required by the customer for a ticket, an indicator will appear in the customer's List of Reports as shown below:

List Of Reports

Show entries Search:

	Name	Compliance	Status	Owner	Failed Items	Tickets	Open Tickets	Upload Time	Last Updated	
	PCI ASV Scan		Under Admin Review	pcicontent@tenable.com	30	30	30	2013-05-21 16:09:35	2013-05-22 10:43:31	<input type="button" value="Submit"/> <div>  <div>User Action Required on 1 ticket</div> </div>

Showing 1 to 1 of 1 entries  

The ticket can then be amended by the user and resubmitted to Tenable Network Security for further review.

PCI ASV Report Formats

Once a scan report has earned compliance status by Tenable's Nessus Cloud, customers have the option of viewing reports in Attestation Report, Executive Report, or Detailed Report formats. An ASV Feedback Form is also provided to the Nessus Cloud customer. These options are available through the Download icon listed next to each report.



Download

- Attestation Report
- Executive Report
- Details Report
- ASV Feedback Form

Close

List Of Reports

Show 10 entries

	Name	Compliance	Status
	PCI ASV Scan		Resolved

Showing 1 to 1 of 1 entries

Search:

Tickets	Upload Time	Last Updated	
	2013-05-21 16:09:35	2013-05-22 11:03:46	Submit

The Attestation Report, Executive Report, and Details Report are only available to the customer in PDF format and cannot be edited.



tenable
network security

Scan Customer Information

Company: Tenable Network Security
Contact: John Smith
Title: PCI Analyst
Telephone: (410) 872-0555
Email: pcicontent@tenable.com
Business Address: 7063 Columbia Gateway Drive
City: Columbia
State: MD
ZIP: 21046
URL: http://www.tenable.com

Approved Scanning Vendor Information

Company: Tenable Network Security
Contact:
Title: Software Engineer
Telephone: 4108720555
Email: @tenable.com
Business Address: 7063 Columbia Gateway Drive, Suite 100
City: Columbia
State: MD
ZIP: 21046
URL: www.tenable.com

Scan Status

- Compliance Status: **PASSED**
- Number of unique components scanned: **1**
- Number of identified failing vulnerabilities: **30**
- Number of components* found by ASV but not scanned because scan customer confirmed components were out of scope: **0**
- Date scan completed: **Tue May 21 12:39:34 2013**
- Scan expiration date (90 days from date scan completed): **Mon Aug 19 12:39:34 2013**

Scan Customer Attestation

Tenable Network Security attests on **2013-05-22 09:18:21** that this scan includes all components* which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements

ASV Attestation



tenable
network security

This scan and report was prepared and conducted by **Tenable Network Security, Inc.** under certificate number "5049-01-02", according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide. **Tenable Network Security, Inc.** attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by sshah@tenable.com.



Scan Customer Information

Scan Customer Company: **Tenable Network Security** ASV Company: **Tenable Network Security**
Date scan was completed: **Tue May 21 12:39:34 2013** Scan expiration date: **Mon Aug 19 12:39:34 2013**

Component Compliance Summary

IP Address: **72.14.215.104** **PASSED**

Vulnerabilities Noted for each IP Address

IP Address	Plugin Name	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, Compensating Controls
72.14.215.104	Apache HTTP Server Byte Range DoS CVE-2011-3192	High	7.8	PASSED	
72.14.215.104	Apache HTTP Server Byte Range DoS CVE-2011-3192	High	7.8	PASSED	
72.14.215.104	OpenSSH < 5.7 Multiple Vulnerabilities CVE-2010-4478, CVE-2012-0814	Medium	6.8	PASSED	This issue is disputed as False Positive and its review status is accepted .

When a report name and then host name is selected within the web-based interface, a list of items pertaining to the selected report is displayed.

List Of Items

Show 10 entries

Search:

	Host	PluginId	Port(Proto)	SvcName	Severity	CvssScore	PluginName	Disputed
	72.14.215.104	17704	65001(tcp)	ssh	Medium	5	OpenSSH S/KEY Authentication Account Enumeration	yes
	72.14.215.104	17704	22(tcp)	ssh	Medium	5	OpenSSH S/KEY Authentication Account Enumeration	yes
	72.14.215.104	53841	65001(tcp)	ssh	Low	2.1	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure	no
	72.14.215.104	53841	22(tcp)	ssh	Low	2.1	Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure	no
	72.14.215.104	17703	65001(tcp)	ssh	Medium	4	OpenSSH < 5.9 Multiple DoS	no
	72.14.215.104	17703	22(tcp)	ssh	Medium	4	OpenSSH < 5.9 Multiple DoS	no
	72.14.215.104	17705	65001(tcp)	ssh	Medium	4.3	OPIE w/ OpenSSH Account Enumeration	yes
	72.14.215.104	17705	22(tcp)	ssh	Medium	4.3	OPIE w/ OpenSSH Account Enumeration	yes
	72.14.215.104	44081	65001(tcp)	ssh	Medium	6.8	OpenSSH < 5.7 Multiple Vulnerabilities	yes
	72.14.215.104	44081	22(tcp)	ssh	Medium	6.8	OpenSSH < 5.7 Multiple Vulnerabilities	yes

Additional Resources

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

- [Nessus 6.4 Installation and Configuration Guide](#) – step by step walk through of installation and configuration 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.

Appendix A – Setting up Credentialed Checks on Windows Platforms

Prerequisites

User Privileges

A very common mistake is to create a local account that does not have enough privileges to log on remotely and do anything useful. By default, Windows will assign new local accounts Guest privileges if they are logged into remotely. This prevents remote vulnerability audits from succeeding. Another common mistake is to increase the amount of access that the Guest users obtain. This reduces the security of your Windows server.

Enabling Windows Logins for Local and Remote Audits

The most important aspect about Windows credentials is that the account used to perform the checks should have privileges to access all required files and registry entries, and in many cases this means administrative privileges. If Nessus is not provided the credentials for an administrative account, at best it can be used to perform registry checks for the patches. While this is still a valid method to determine if a patch is installed, it is incompatible with some third party patch management tools that may neglect to set the key in the policy. If Nessus has administrative privileges, then it will actually check the version of the dynamic-link library (.dll) on the remote host, which is considerably more accurate.

Configuring a Local Account

To configure a stand-alone Windows server with credentials to be used that is not part of a domain, simply create a unique account as an administrator.

Make sure that the configuration of this account is not set with a typical default of Guest only: local users authenticate as guest. Instead, switch this to Classic: local users authenticate as themselves.

To configure the server to allow logins from a domain account, the Classic security model should be invoked. To do this, follow these steps:

1. Open Group Policy by clicking on start, click Run, type `gpedit.msc` and then click OK.
2. Select Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
3. From the list of policies open Network access: Sharing and security model for local accounts.
4. In this dialog, select Classic – local users authenticate as themselves and click OK to save this.

This will cause users local to the domain to authenticate as themselves, even though they are actually not really physically local on the particular server. Without doing this, all remote users, even real users in the domain, will actually authenticate as a Guest and will likely not have enough credentials to perform a remote audit.

Note that the `gpedit.msc` tool is not available on some version such as Windows 7 Home, which is not supported by Tenable.

Configuring a Domain Account for Authenticated Scanning

To create a domain account for remote host-based auditing of a Windows server, the server must first be Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Windows 7, and Windows 8 and be part of a domain. There are five general steps that should be performed to facilitate this scanning while keeping security in mind.

Step 1: Creating a Security Group

First, create a security group called **Nessus Local Access**:

- Log onto a Domain Controller, open Active Directory Users and Computers.
- Create a security Group from **Menu select Action -> New -> Group**.
- Name the group **Nessus Local Access**. Make sure it has a Scope of **Global** and a Type of **Security**.
- Add the account you will use to perform Nessus Windows Authenticated Scans to the **Nessus Local Access** group.

Step 2: Create Group Policy

Next, you need to create a group policy called **Local Admin GPO**.

- Open the **Group Policy Management Console**.
- Right click on **Group Policy Objects** and select **New**.
- Type the name of the policy **Nessus Scan GPO**.

Step 3: Configure the policy to add the Nessus Local Access group as Administrators

Here you will add the **Nessus Local Access** group to the **Nessus Scan GPO** policy and put them in the groups you wish them to use.

- Right click **Nessus Scan GPO** Policy then select **Edit**.
- Expand **Computer configuration\Policies\Windows Settings\Security Settings\Restricted Groups**.
- In the Left pane on **Restricted Groups**, right click and select **Add Group**.
- In the **Add Group** dialog box, select browse and type **Nessus Local Access** and then click **Check Names**.
- Click **OK** twice to close the dialog box.
- Click **Add** under **This group is a member of:**
- Add the **Administrators** Group.
- Click **OK** twice.

Step 4: Ensure proper ports are open in the firewall for Nessus to connect to the host

Nessus uses SMB (Server Message Block) and WMI (Windows Management Instrumentation) for this we need to make sure that the Windows Firewall will allow access to the system.

Allowing WMI on Windows Vista, 7, 8, 2008, 2008R2 and 2012 Windows Firewall

- Right click **Nessus Scan GPO** Policy then select **Edit**.
- Expand **Computer configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Inbound Rules**
- Right-click in the working area and choose **New Rule...**
- Choose the **Predefined** option, and select **Windows Management Instrumentation (WMI)** from the drop-down list.

- Click on **Next**.
- Select the Checkboxes for:
 - Windows Management Instrumentation (ASync-In)
 - Windows Management Instrumentation (WMI-In)
 - Windows Management Instrumentation (DCOM-In)
- Click on **Next**
- Click on **Finish**
- **Note:** You can later edit the predefined rule created and limit the connection to the ports by IP Address and Domain User so as to reduce any risk for abuse of WMI.

Step 5: Linking GPO

- In Group policy management console, right click on the domain or the OU and select Link an Existing GPO
- Select the Nessus Scan GPO

Configuring Windows 2008, Vista, and 7

When performing authenticated scans against Windows 2008, Vista or 7 systems, there are several configuration options that must be enabled:

1. Under **Windows Firewall -> Windows Firewall Settings**, **File and Printer Sharing** must be enabled.
2. Using the `gpedit.msc` tool (via the Run.. prompt), invoke the **Group Policy Object Editor**. Navigate to **Local Computer Policy -> Administrative Templates -> Network -> Network Connections -> Windows Firewall -> Standard Profile -> Windows Firewall : Allow inbound file and printer exception**, and enable it.
3. While in the **Group Policy Object Editor**, navigate to **Local Computer Policy -> Administrative Templates -> Network -> Network Connections -> Prohibit use of Internet connection firewall on your DNS domain** and ensure it is set to either Disabled or Not Configured.
4. The Remote Registry service must be enabled (it is disabled by default). It can be enabled manually for continuing audits, either by an administrator or by Nessus. Using plugin IDs [42897](#) and [42898](#), Nessus can enable the service just for the duration of the scan.



Enabling this option grants Nessus permission to enable and disable the Remote Registry service—even if you have explicitly set it to 'Disabled'.



Windows User Account Control (UAC) can be disabled alternatively, but that is not recommended. To turn off UAC completely, open the Control Panel, select User Accounts and then set Turn User Account Control to off. Alternatively, you can add a new registry key named `LocalAccountTokenFilterPolicy` and set its value to 1. This key must be created in the registry at the following location: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy`. For more information on this registry setting, consult the [MSDN 766945 KB](#). In Windows 7 and 8, if UAC is disabled, then `EnableLUA` must be set to 0 in `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System` as well.

Appendix B – Enabling SSH Local Security Checks on Unix and Network Devices

This section is intended to provide a high-level procedure for enabling SSH between the systems involved in the Nessus credentialed checks. It is not intended to be an in-depth tutorial on SSH. It is assumed the reader has the prerequisite knowledge of Unix system commands.

Generating SSH Public and Private Keys

The first step is to generate a private/public key pair for the Nessus scanner to use. This key pair can be generated from any of your Unix systems, using any user account. However, it is important that the keys be owned by the defined Nessus user.

To generate the key pair, use **ssh-keygen** and save the key in a safe place. In the following example the keys are generated on a Red Hat ES 3 installation.

```
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/test/.ssh/id_dsa):
    /home/test/Nessus/ssh_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
/home/test/Nessus/ssh_key.
Your public key has been saved in
/home/test/Nessus/ssh_key.pub.
The key fingerprint is:
06:4a:fd:76:ee:0f:d4:e6:4b:74:84:9a:99:e6:12:ea
#
```

Do not transfer the private key to any system other than the one running the Nessus server. When **ssh-keygen** asks you for a passphrase, enter a strong passphrase or hit the Return key twice (i.e., do not set any passphrase). If a passphrase is specified, it must be specified in the Policies -> Credentials -> SSH settings options in order for Nessus to use key-based authentication.

Nessus Windows users may wish to copy both keys to the main Nessus application directory on the system running Nessus (C:\Program Files\Tenable\Nessus by default), and then copy the public key to the target systems as needed. This makes it easier to manage the public and private key files.

Creating a User Account and Setting up the SSH Key

On every target system to be scanned using local security checks, create a new user account dedicated to Nessus. This user account must have exactly the same name on all systems. For this document, we will call the user **nessus**, but you can use any name.

Once the account is created for the user, make sure that the account has no valid password set. On Linux systems, new user accounts are locked by default, unless an initial password was explicitly set. If you are using an account where a password had been set, use the **passwd -l** command to lock the account.

You must also create the directory under this new account's home directory to hold the public key. For this exercise, the directory will be **/home/nessus/.ssh**. An example for Linux systems is provided below:


```
# passwd -l nessus
# cd /home/nessus
# mkdir .ssh
#
```

For Solaris 10 systems, Sun has enhanced the **passwd(1)** command to distinguish between locked and non-login accounts. This is to ensure that a user account that has been locked may not be used to execute commands (e.g., cron jobs). Non-login accounts are used only to execute commands and do not support an interactive login session. These accounts have the NP token in the password field of **/etc/shadow**. To set a non-login account and create the SSH public key directory in Solaris 10, run the following commands:

```
# passwd -N nessus

# grep nessus /etc/shadow
nessus:NP:13579:::::::
# cd /export/home/nessus
# mkdir .ssh
#
```

Now that the user account is created, you must transfer the key to the system, place it in the appropriate directory and set the correct permissions.

From the system containing the keys, secure copy the public key to system that will be scanned for host checks as shown below. 192.1.1.44 is an example remote system that will be tested with the host-based checks.

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
#
```

You can also copy the file from the system on which Nessus is installed using the secure FTP command, **sftp**. Note that the file on the target system must be named **authorized_keys**.



Do not use the **no-pty** option in your **authorized_keys** file for SSH authentication. This can impact the SSH credentialed scans.


Return to the System Housing the Public Key

Set the permissions on both the **/home/nessus/.ssh** directory, as well as the **authorized_keys** file.

```
# chown -R nessus:nessus ~nessus/.ssh/
# chmod 0600 ~nessus/.ssh/authorized_keys
# chmod 0700 ~nessus/.ssh/
#
```

Repeat this process on all systems that will be tested for SSH checks (starting at Creating a User Account and Setting up the SSH Key above).

Test to make sure that the accounts and networks are configured correctly. Using the simple Unix command **id**, from the Nessus scanner, run the following command:



```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

If it successfully returns information about the `nessus` user, the key exchange was successful.

Enabling SSH Local Security Checks on Network Devices

In addition to using SSH for local security checks, Nessus also supports local security checks on various network devices. Those network devices currently include Cisco IOS devices, F5 networks devices, Huawei devices, Junos devices, and Palo Alto Networks devices.

Network devices that support SSH require both a username and password. Currently, Nessus does not support any other forms of authentication to network devices.

See your appropriate network device manual for configuring SSH support.

Appendix C – Interface Shortcuts

Page	Hot Key	Description
Home		
	R	Scans
	P	Policies
	U	Users
	G	Groups (Nessus Manager and Nessus Cloud)
	M	User Profile
	Shift + R OR N	New Scan
	Shift + F	New Folder (Scan view only)
Policies		
	N	New Policy
Accounts / Users		
	N	New User
Accounts / Groups		
	N	New User Group (Nessus Manager and Nessus Cloud)
Settings / Advanced		
	N	New Setting