



# Tenable Nessus and Thycotic Integration Guide

Last Revised: July 15, 2025



## Table of Contents

<b>Introduction</b> .....	<b>3</b>
<b>Integration Requirements</b> .....	<b>4</b>
<b>Integrate with Thycotic Secret Server</b> .....	<b>5</b>
Configure Windows Credentials .....	5
Configure Linux Credentials .....	10
<b>Troubleshooting</b> .....	<b>18</b>



# Introduction

---

This document describes how to deploy Tenable™ Nessus® for integration with Thycotic Secret Server. Please email any comments and suggestions to Tenable Support.

Security administrators know that conducting network vulnerability assessments means getting access to and navigating an ever-changing sea of usernames, passwords, and privileges. By integrating Thycotic Secret Server with Nessus, administrators now have even more choice and flexibility for reducing the credentials headache.

The Tenable® integration with Thycotic Secret Server delivers a comprehensive authenticated scanning solution that provides security teams better vulnerability insight in order to further protect privileged accounts. This integration supports the storage of privileged credentials in Thycotic Secret Server and their automatic retrieval at scan time by Tenable. This ensures that sensitive passwords are safely stored, controlled, auditable and easily changed without manual intervention.

By integrating Nessus with Thycotic Secret Server, you can:

- Store credentials in Thycotic Secret Server instead of managing and updating the credentials directly within a Tenable solution.
- Reduce the time and effort needed to document credential storage within the organizational environment.
- Automatically enforce security policies within specific departments or for specific business unit requirements, simplifying your compliance process.
- Reduce the risk of unsecured privileged accounts and credentials across the enterprise.



## Integration Requirements

You must meet the following minimum version requirements to integrate Tenable Nessus with Thycotic Secret Server:

- Thycotic Secret Server version 8.9 or later
- Nessus Manager version 6.7 or later

**Note:** Tenable does not support the Thycotic Cloud product. For more information, contact your Tenable representative.

**Note:** The integration requires enabling the Thycotic Secret Server web services API, which is available in Secret Server Professional and the hosted version of Secret Server.



# Integrate with Thycotic Secret Server

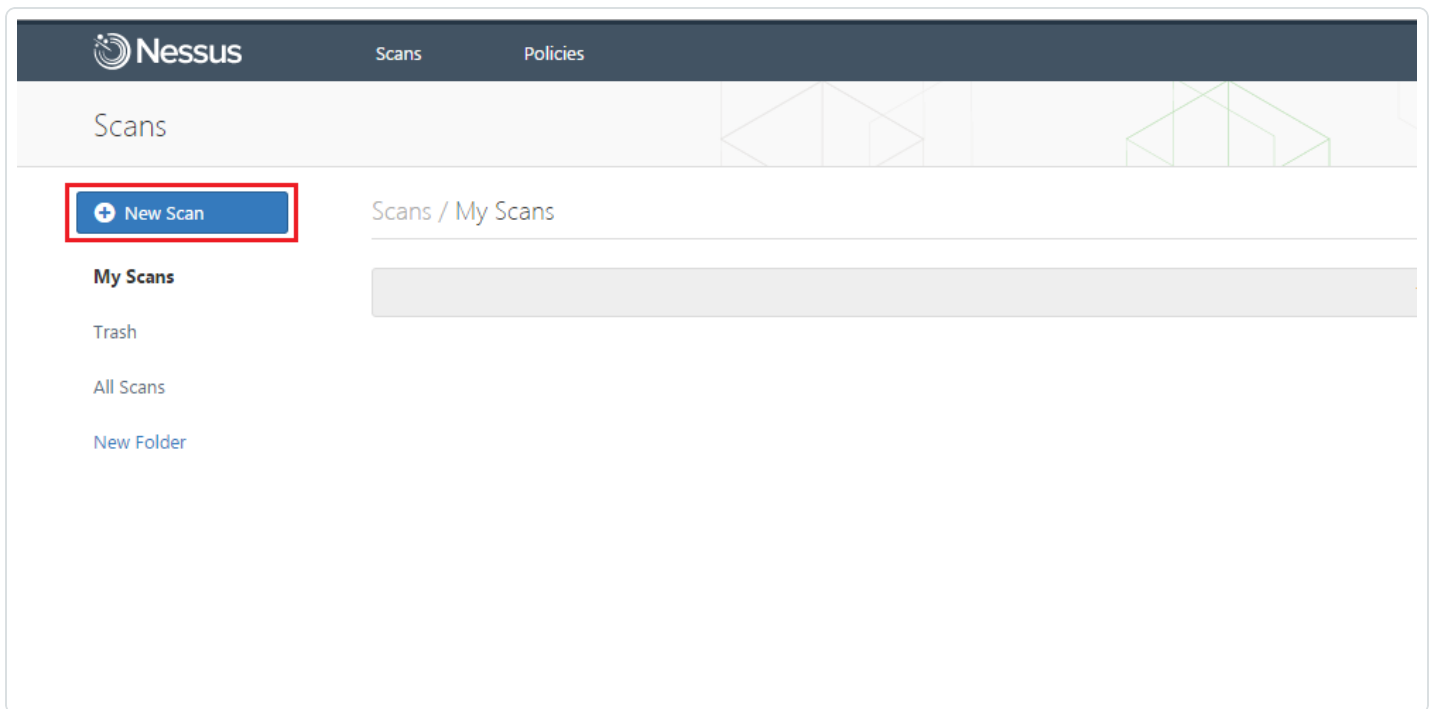
You can configure Nessus Manager to perform credentialed network scans of Windows and Linux systems using Thycotic's password management solution. Credentials are configured similarly to other credentialed network scans.

[Configure Windows Credentials](#)

[Configure Linux Credentials](#)

## Configure Windows Credentials

Log in to Nessus Manager and click the **+ New Scan** button to configure Nessus Manager for credentialed scans of Windows systems using Thycotic's password management solution.



Select a "Scanner Template" for the scan type required for your scan. For demonstration purposes, the "Advanced Scan" template will be used.



**Nessus**

ScansPolicies

Scan Library

All TemplatesScannerAgent

Scanner Templates

**Advanced Scan**  
Configure a scan without using any recommendations.

**Audit Cloud Infrastructure**  
Audit the configuration of third-party cloud services.

**Badlock Detection**  
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

**Bash Shellshock Detection**  
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

**Basic Network Scan**  
A full system scan suitable for any host.

**Internal PCI Network Scan**  
Perform an internal PCI DSS (11.2.1) vulnerability scan.

**Malware Scan**  
Scan for malware on Windows and Unix systems.

**MDM Config Audit**  
Audit the configuration of mobile device managers.

**Mobile Device Scan**  
Assess mobile devices via Microsoft Exchange or an MDM.

**Offline Config Audit**  
Audit the configuration of network devices.

**Web Application Tests**  
Scan for published and unknown web vulnerabilities.

To configure a credentialed scan for Windows systems using Thycotic's password management solution, enter a descriptive **Name** and enter the IP address(es) or hostname(s) of the scan **Targets**.

New Scan / Advanced Scan

Scan Library > Settings Credentials Compliance Plugins

BASIC

General

Schedule

Notifications

Permissions

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Settings / Basic / General

Name

Thycotic - Windows

Description

Folder

My Scans

Dashboard

Enabled

Targets

172.1.2.3/24

Upload Targets

Add File

Save

Cancel

Once the “Name” and “Targets” have been configured, click on **Credentials** and then select **Windows** from the left-hand menu.

Nessus

Scans Policies

New Scan / Advanced Scan

Scan Library > Settings Credentials Compliance Plugins

CREDENTIALS

Cloud Services

Database

Host

SNMPv3

SSH

Windows

Miscellaneous

Mobile

Patch Management

Plaintext Authentication

ACTIVE CREDENTIALS

Add credentials from the adjacent list

Save

Cancel



Click the **Authentication method** drop-down and select **Thycotic Secret Server**.

The screenshot shows the Nessus interface for configuring a scan. The 'Credentials' tab is active, and the 'Host' section is expanded. The 'Windows' credential type is selected. The 'Authentication method' dropdown menu is open, showing options: Password, CyberArk, Kerberos, LM Hash, NTLM Hash, Password, and Thycotic Secret Server. The 'Thycotic Secret Server' option is highlighted with a red box. Below the dropdown, there are checkboxes for 'Never send credentials in the clear', 'Do not use NTLMv1 authentication', 'Start the Remote Registry service during the scan', and 'Enable administrative shares during the scan'. The 'Save' button is visible at the bottom left.

Configure each field for Windows authentication. Refer to “Table 1 - Thycotic Windows Credentials” below for a description of each field. Once the Windows credentials have been configured, click **Save** to finalize the changes.



Nessus
Scans
Policies

### Thycotic - Windows / Configuration

POLICY: ADVANCED SCAN

Scan > Settings
**Credentials**
Compliance
Plugins

CREDENTIALS

- Cloud Services
- Database
- Host
- SNMPv3**
- SSH**
- Windows**
- Miscellaneous
- Mobile
- Patch Management
- Plaintext Authentication

ACTIVE CREDENTIALS

Windows
Domain: domain.com, User: user, Auth ...

Authentication method

Thycotic Secret Server

Username

System\_user

Domain

Thycoticdomain.com

Thycotic Secret Name

\*\*\*\*\*

Thycotic Secret Server URL

https://<targetaddress>/SecretServer

Thycotic Login Name

Thycotic\_Login\_Name

Thycotic Password

\*\*\*\*\*

Thycotic Organization (optional)

Org1

Thycotic Domain (optional)

Verify SSL Certificate

☒

Global Settings

☒

Never send credentials in the clear

☒

Do not use NTLMv1 authentication

☐

Start the Remote Registry service during the scan

*Table 1 - Thycotic Windows Credentials*

Option	Description
Username	The target system(s) username
Domain	This is an optional field if the above username is part of a domain
Thycotic Secret Name	The value (“Secret Name”) that the secret is stored as on the Thycotic server
Thycotic Secret Server URL	URL of the Thycotic Secret Server, which sets the transfer method, target, and target directory. This information can be found in Admin > Configuration > Application Settings > Secret Server URL on the Thycotic server.
Thycotic Login Name	The username used to authenticate to the Thycotic server
Thycotic Password	The password associated with the Thycotic Login Name



Thycotic Organization (optional)	This is an optional value used in cloud instances of Thycotic to define which organization should be queried
Thycotic Domain (optional)	This is an optional value set if the domain value is set for the Thycotic server
Verify SSL Certificate	Use the Custom_CA setup method to validate SSL server certificates

To verify the integration is working, click the **Launch button** to initiate an on-demand scan.

The screenshot shows the Nessus interface with the 'Scans' tab selected. On the left, there's a sidebar with 'New Scan', 'My Scans', 'Trash', 'All Scans', and 'New Folder'. The main area shows a table of scans. The first scan is 'Thycotic - Windows' with a status of 'On Demand'. A red box highlights the 'Launch' button next to this scan.

Once the scan has completed, select the completed scan and look for “Plugin ID 10394” (shown below), which validates that authentication was successful. If the authentication is not successful, refer to the “Troubleshooting” section of this document.

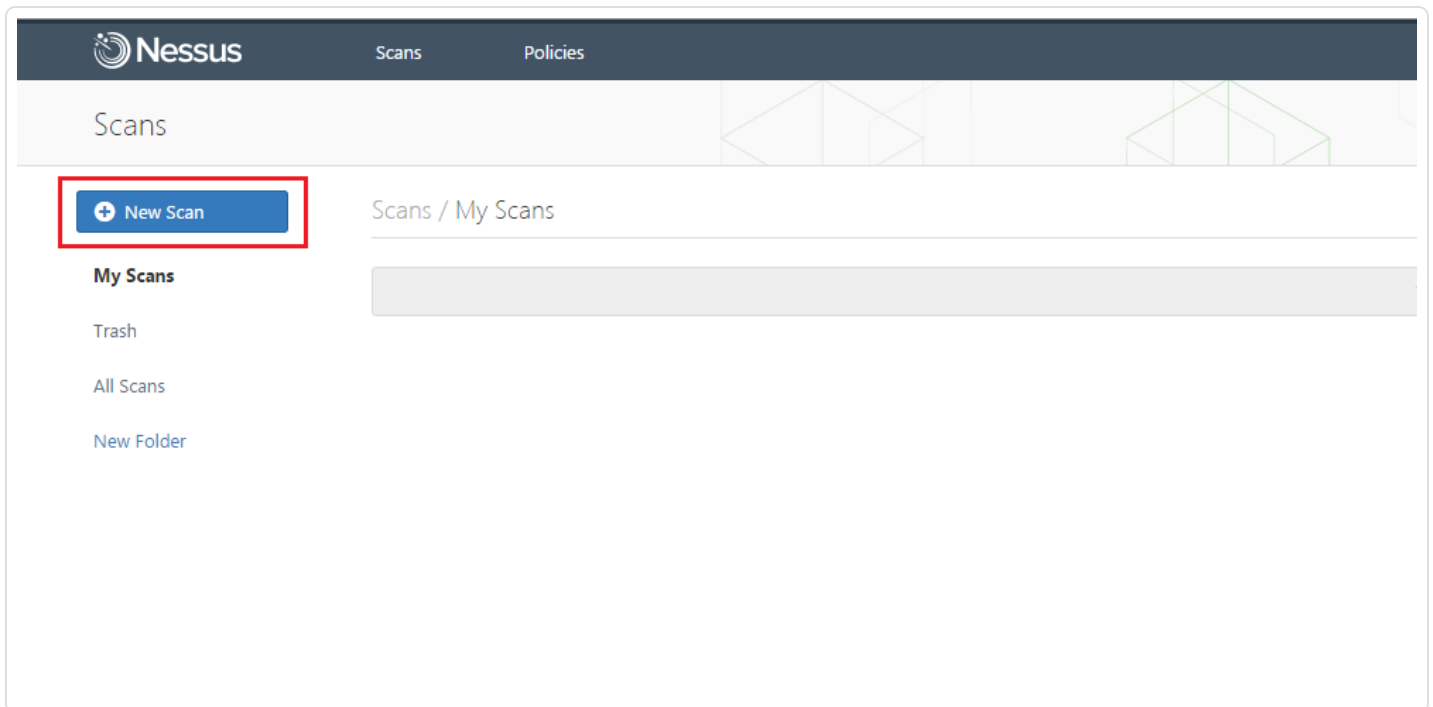
The screenshot shows the Nessus interface with the 'Vulnerabilities' tab selected. The breadcrumb trail is 'Hosts > [Host Name] > Vulnerabilities'. The main area shows a table of vulnerabilities. The first vulnerability is 'Microsoft Windows SMB Log In Possible' with a severity of 'INFO'. A red box highlights the 'Launch' button next to this vulnerability.

## Configure Linux Credentials



Configuring Linux credentialed scans follows the same basic steps as Windows credentialed scans with only a few minor differences.

Log in to Nessus Manager and click the **+ New Scan** button to begin the Linux credentialed scan configuration.



Select a “Scanner Template” for the scan type required for your scan. For demonstration purposes, the “Advanced Scan” template will be used.



**Nessus**

ScansPolicies

Scan Library

All TemplatesScannerAgent

Scanner Templates

**Advanced Scan**  
Configure a scan without using any recommendations.

**Audit Cloud Infrastructure**  
Audit the configuration of third-party cloud services.

**Badlock Detection**  
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

**Bash Shellshock Detection**  
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

**Basic Network Scan**  
A full system scan suitable for any host.

**Internal PCI Network Scan**  
Perform an internal PCI DSS (11.2.1) vulnerability scan.

**Malware Scan**  
Scan for malware on Windows and Unix systems.

**MDM Config Audit**  
Audit the configuration of mobile device managers.

**Mobile Device Scan**  
Assess mobile devices via Microsoft Exchange or an MDM.

**Offline Config Audit**  
Audit the configuration of network devices.

**Web Application Tests**  
Scan for published and unknown web vulnerabilities.

To configure a credentialed scan for Linux systems using Thycotic's password management solution, enter a descriptive **Name** and enter the IP address(es) or hostname(s) of the scan **Targets**.

Nessus

ScansPolicies

Thycotic - Linux / Configuration

POLICY: ADVANCED SCAN

Scan > SettingsCredentialsCompliancePlugins

BASIC

General

Schedule

Notifications

Permissions

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Settings / Basic / General

Name

Thycotic - Linux

Description

Folder

My Scans

Dashboard

Enabled

Targets

172.1.2.3/24


Upload Targets

Add File

Save

Cancel

Once the “Name” and “Targets” have been configured, click on **Credentials** and then select **SSH** from the left-hand menu.



Scans Policies

## New Scan / Advanced Scan

Scan Library > Settings **Credentials** Compliance Plugins

**CREDENTIALS**

- Cloud Services
- Database
- Host
  - SNMPv3
  - SSH**
  - Windows
- Miscellaneous
- Mobile
- Patch Management
- Plaintext Authentication


**ACTIVE CREDENTIALS**

Add credentials from the adjacent list

Save

Cancel

In the **Authentication method** drop-down box, select **Thycotic Secret Server**.



Scans Policies

## Thycotic - Linux / Configuration

POLICY: ADVANCED SCAN

Scan > Settings **Credentials** Compliance Plugins

**CREDENTIALS**

- Cloud Services
- Database
- Host
  - SNMPv3
  - SSH
  - Windows
- Miscellaneous
- Mobile
- Patch Management
- Plaintext Authentication

**ACTIVE CREDENTIALS**

- Windows
- SSH**

Authentication method

Public key  
Certificate  
CyberArk  
Kerberos  
Password  
Public key  
**Thycotic Secret Server**

Username

Private key

Private key passphrase

Elevate privileges with

Nothing

Global Settings

known\_hosts file

Add File

Preferred port

22

Client version

OpenSSH\_5.0

Save

Cancel



Configure each field for SSH authentication. Refer to “Table 2 - Thycotic SSH Credentials” below for a description of each field. Once the SSH credentials have been configured, click **Save** to finalize the changes.

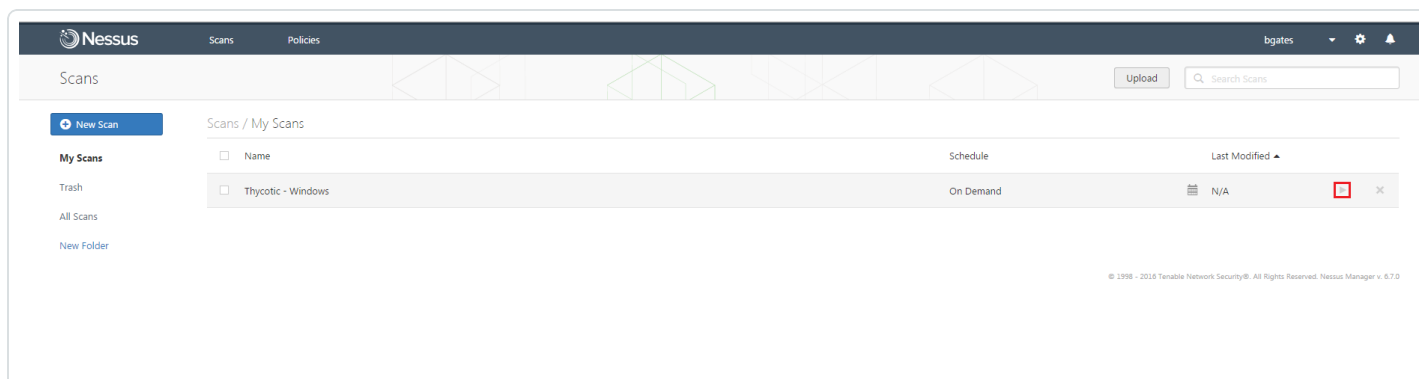
*Table 2 - Thycotic SSH Credentials*

Option	Description
Username	The username that is used to authenticate via ssh to the system.
Thycotic Secret Name	This is the value that the secret is stored as on the Thycotic server. It is referred to as the “Secret Name” on the Thycotic server.
Thycotic Secret Server URL	This is used to set the transfer method, target , and target directory for the scanner. The value can be found in <b>Admin &gt; Configuration &gt; Application Settings &gt; Secret Server URL</b> on the Thycotic server. For example consider the following address



	https://pw.mydomain.com/SecretServer/. We will parse this to know that https defines it is a ssl connection, pw.mydomain.com is the target address, /SecretServer/ is the root directory.
Thycotic Login Name	The username used to authenticate to the Thycotic server.
Thycotic Password	The password associated with the <b>Thycotic Login Name</b> .
Thycotic Organization (optional)	This value is used in cloud instances of Thycotic to define which organization your query should hit.
Thycotic Domain (optional)	This is an optional value set if the domain value is set for the Thycotic server.
Use Private Key	Use key based authentication for SSH connections instead of a password.
Verify SSL Certificate	Verify if the SSL Certificate on the server is signed by a trusted CA.
Thycotic elevate privileges with	<p>The privilege escalation method you want to use to increase the user's privileges after initial authentication. Multiple options for privilege escalation are supported, including su, su+sudo and sudo. Your selection determines the specific options you must configure.</p> <div><b>Note:</b> For additional information about all of the supported privilege escalation types and their accompanying fields, see <a href="#">SSH</a> in the Tenable Nessus User Guide.</div>

To verify the integration is working, click the **Launch button** to initiate an on-demand scan.







Once the scan has completed, select the completed scan and look for “Plugin ID 12634”, which validates that authentication was successful. If the authentication is not successful, refer to the “Troubleshooting” section of this document.



# Troubleshooting

Nessus Manager 6.7 offers the ability to enable plugin debugging, which will allow for easier troubleshooting and resolution should issues arise. Enabling plugin debugging attaches available debug logs from plugins to the vulnerability output of the scan it is enabled on.

To enable plugin debugging, navigate to scan **Settings** and click **Advanced** in the left-hand menu.

The screenshot shows the Nessus Manager interface for configuring a scan named 'Thycotic - Windows'. The left-hand menu is expanded, and the 'ADVANCED' option is highlighted with a red box. The main content area displays the 'Settings / Basic / General' configuration page. The fields are as follows:

Field	Value
Name	Thycotic - Windows
Description	
Folder	My Scans
Dashboard	Enabled
Targets	172.1.2.3/24

At the bottom of the configuration area, there are links for 'Upload Targets' and 'Add File'. At the very bottom, there are 'Save' and 'Cancel' buttons.

Select the **Enable plugin debugging** checkbox and click **Save** to finalize the change.



## Thycotic - Windows / Configuration

POLICY: ADVANCED SCAN

Scan > **Settings** Credentials Compliance Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

### Settings / Advanced

#### General Settings

- ☒ Enable safe checks
- ☐ Stop scanning hosts that become unresponsive during the scan
- ☐ Scan IP addresses in a random order

#### Performance Options

- ☐ Slow down the scan when network congestion is detected
- ☐ Use Linux kernel congestion detection

Network timeout (in seconds)

Max simultaneous checks per host

Max simultaneous hosts per scan

Max number of concurrent TCP sessions per host

Max number of concurrent TCP sessions per scan

#### Debug Settings

- ☐ Log scan details to server  
Logs the start and finish time for each plugin used during a scan to nessusd.messages.

- ☒ Enable plugin debugging  
Attaches available debug logs from plugins to the vulnerability output of this scan.

Save

Cancel