



## **Tenable Nessus for Thycotic Integration Guide**

---

Last Revised: March 15, 2018

---

# 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 .....	6
Configure Linux Credentials .....	12
<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 [support@tenable.com](mailto:support@tenable.com).

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, customers are now granted even more choice and flexibility for reducing the credentials headache.

The combined Tenable-Thycotic solution works when a Nessus Manager scan policy is configured to query a Thycotic Secret Server for privileged credentials. At the time of the scan, Nessus Manager sends a request to Thycotic to request the privileged account credentials to be used. Thycotic then provides the privileged account credentials back to Nessus Manager, and the provided credentials are then used to log in to the target system to identify vulnerabilities and misconfigurations.

Benefits of integrating Nessus with Thycotic Secret Server include:

- Credentials stored in Thycotic Secret Server no longer need to be managed and updated directly within a Tenable solution
- Reduce the time and effort needed to document where credentials are stored within the entire organizational environment
- Automatically enforce security policies within specific departments or for specific business unit requirements, which simplifies compliance
- Reduce the risk of unsecured privileged accounts and credentials across the enterprise

---

## Integration Requirements

---

The following are required in order to integrate Tenable Nessus with Thycotic Secret Server:

- Thycotic Secret Sever version 8.9 or higher
- Nessus Manager version 6.7 or higher

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

---

## Integrate with Thycotic Secret Server

---

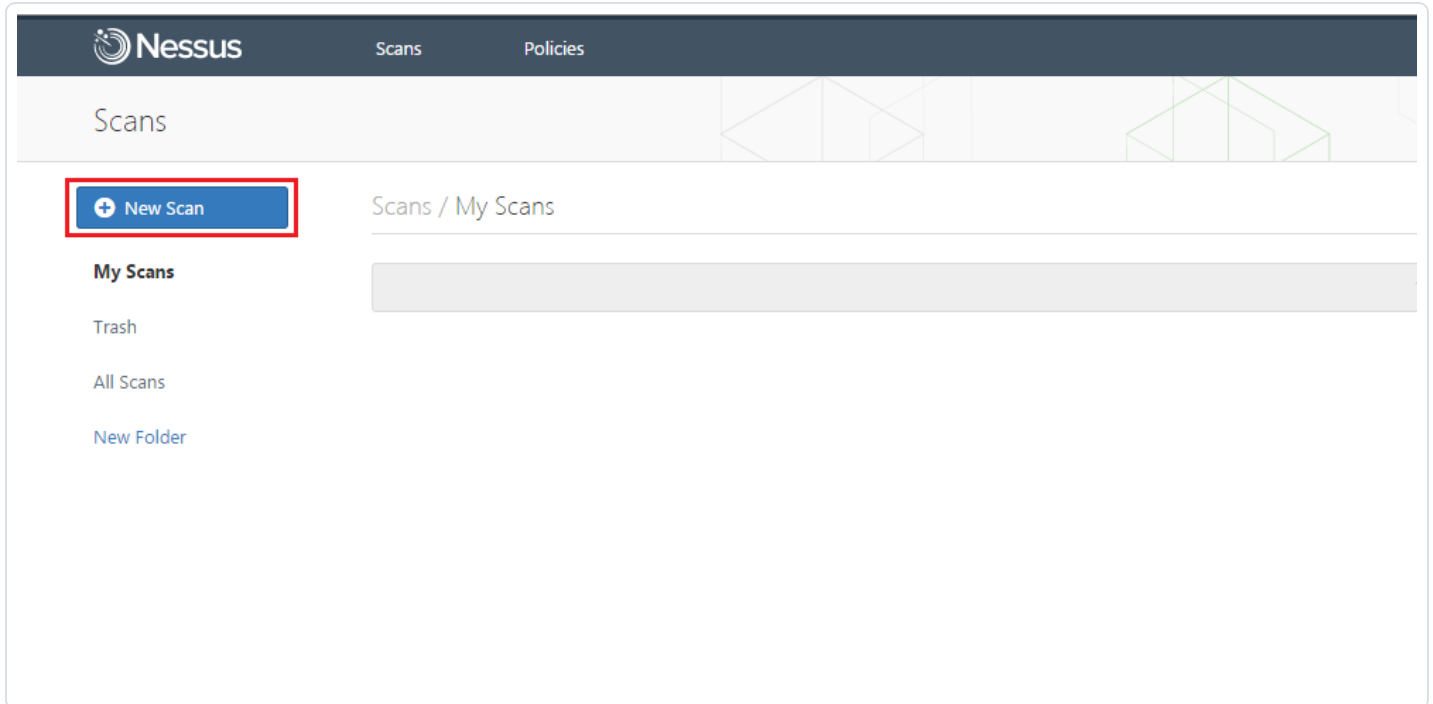
Nessus Manager can be configured to perform credentialed network scans of both Windows and Linux systems using Thycotic's password management solution. Thycotic's integration with Nessus Manager is seamless, so credentials are configured similarly to other credentialed network scans.

[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.

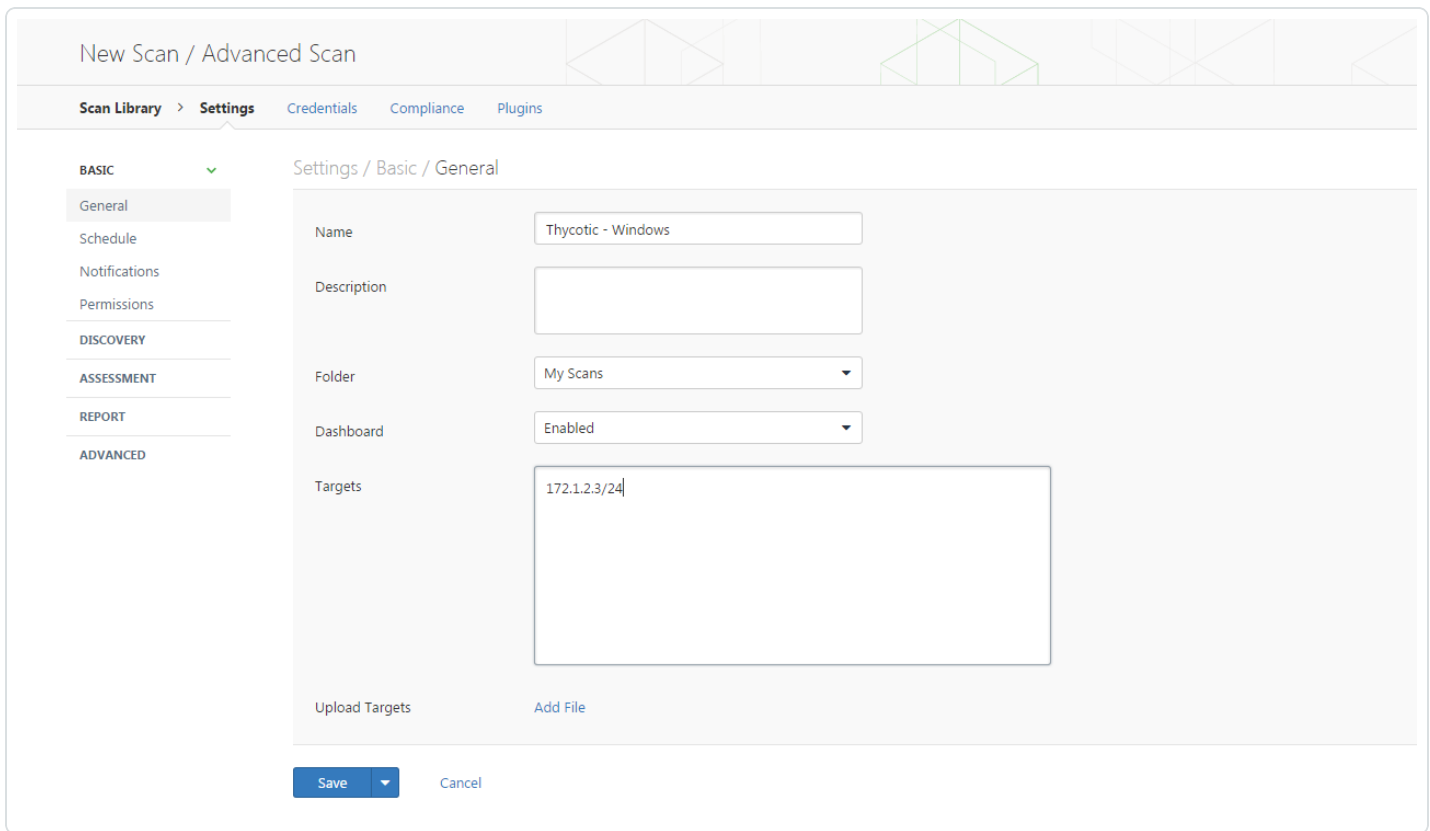


Select a “Scanner Template” for the scan type required for your scan. For demonstration purposes, the “Advanced Scan” template will be used.

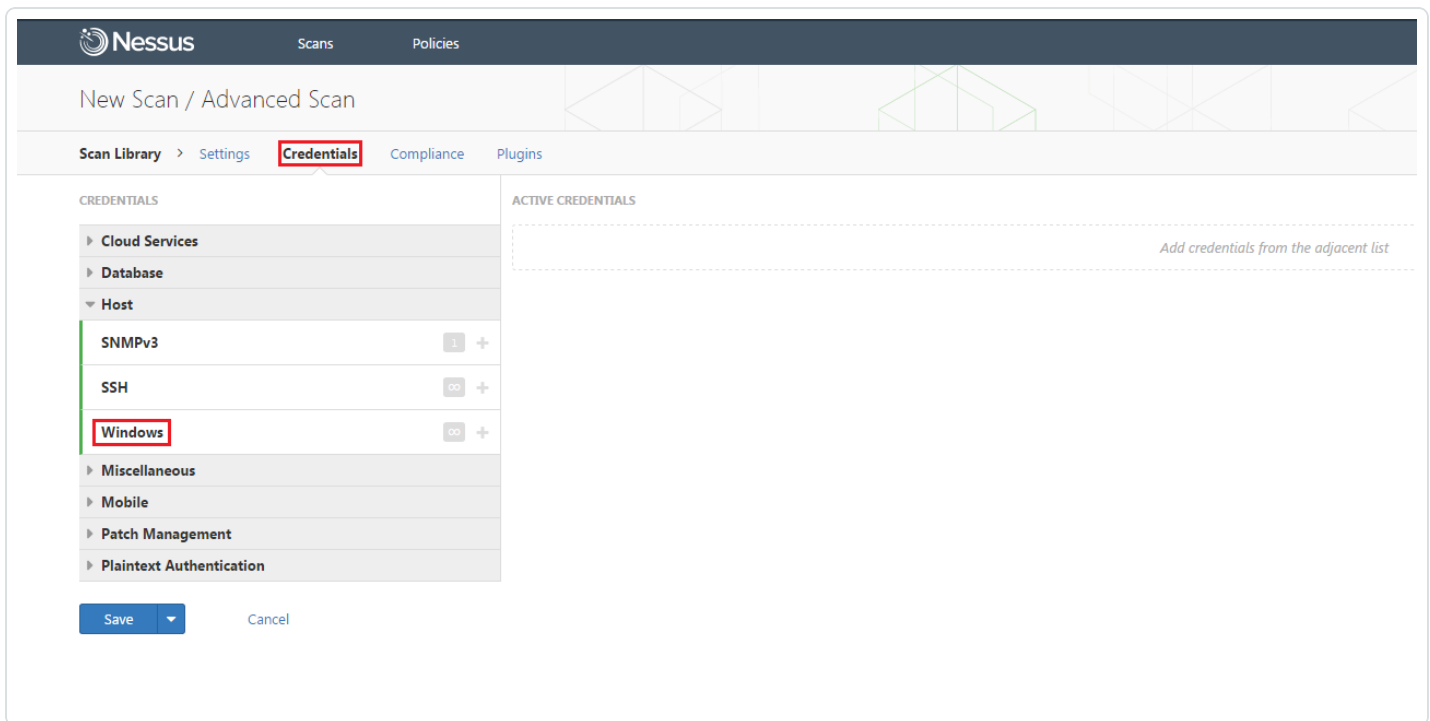
The screenshot displays the Nessus Scan Library interface. At the top, there is a dark blue header with the Nessus logo and navigation links for 'Scans' and 'Policies'. Below the header, the page is titled 'Scan Library' and includes tabs for 'All Templates', 'Scanner', and 'Agent'. The main content area is labeled 'Scanner Templates' and features a grid of ten template cards, each with an icon, a title, and a brief description:

- 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**.

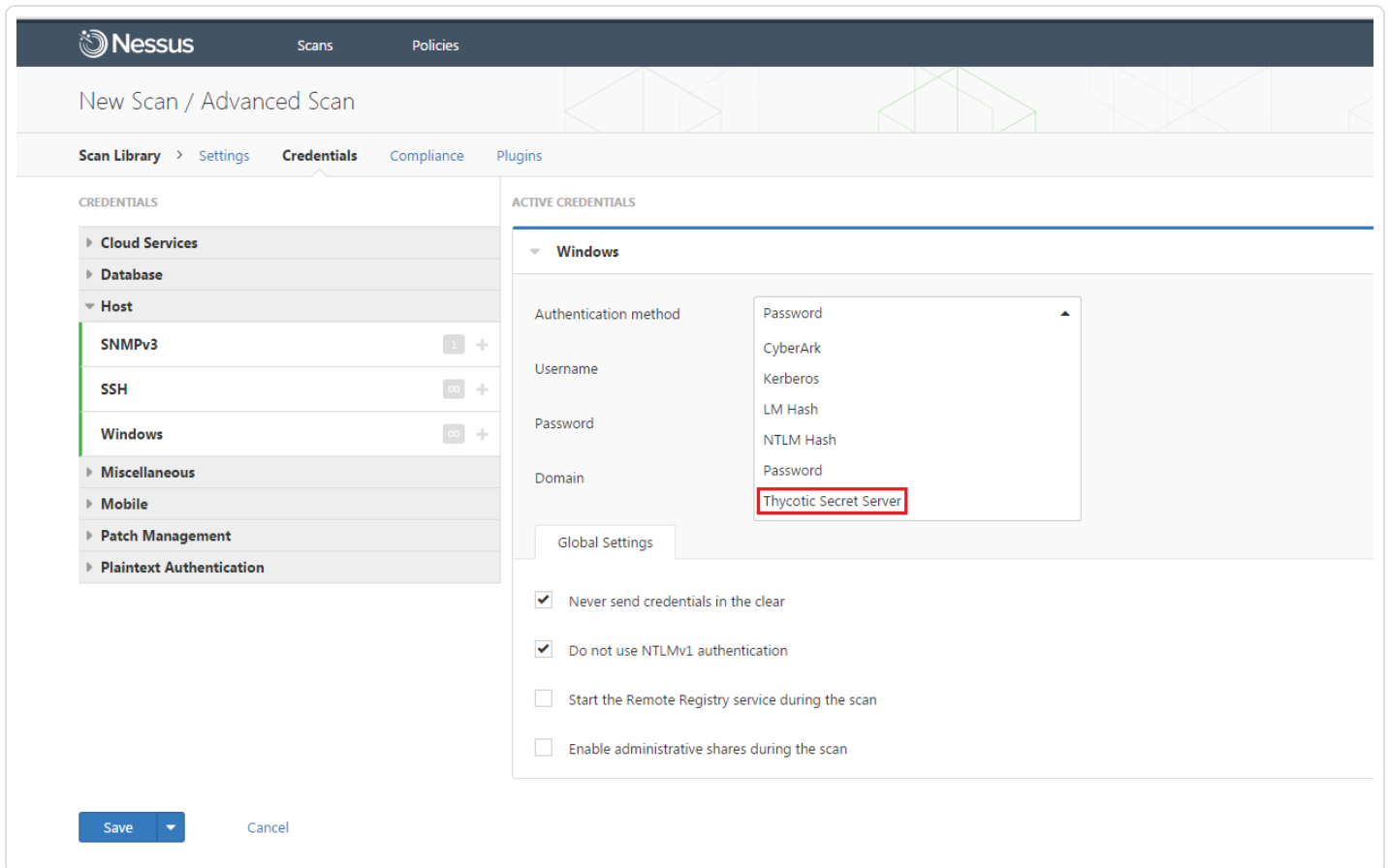


Once the “Name” and “Targets” have been configured, click on **Credentials** and then select **Windows** from the left-hand menu.





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



The screenshot shows the Nessus interface for configuring credentials. The top navigation bar includes 'Scans' and 'Policies'. The main header reads 'New Scan / Advanced Scan'. Below this, there are tabs for 'Scan Library', 'Settings', 'Credentials', 'Compliance', and 'Plugins'. The 'Credentials' section is active, showing a list of credential types on the left: Cloud Services, Database, Host, SNMPv3, SSH, Windows, Miscellaneous, Mobile, Patch Management, and Plaintext Authentication. The 'Windows' credential type is selected. On the right, the 'ACTIVE CREDENTIALS' section shows the configuration for 'Windows'. The 'Authentication method' dropdown is open, displaying a list of 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 fields for 'Username', 'Password', and 'Domain'. A 'Global Settings' tab is also visible. At the bottom, 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'. A 'Save' button and a 'Cancel' link are located 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.

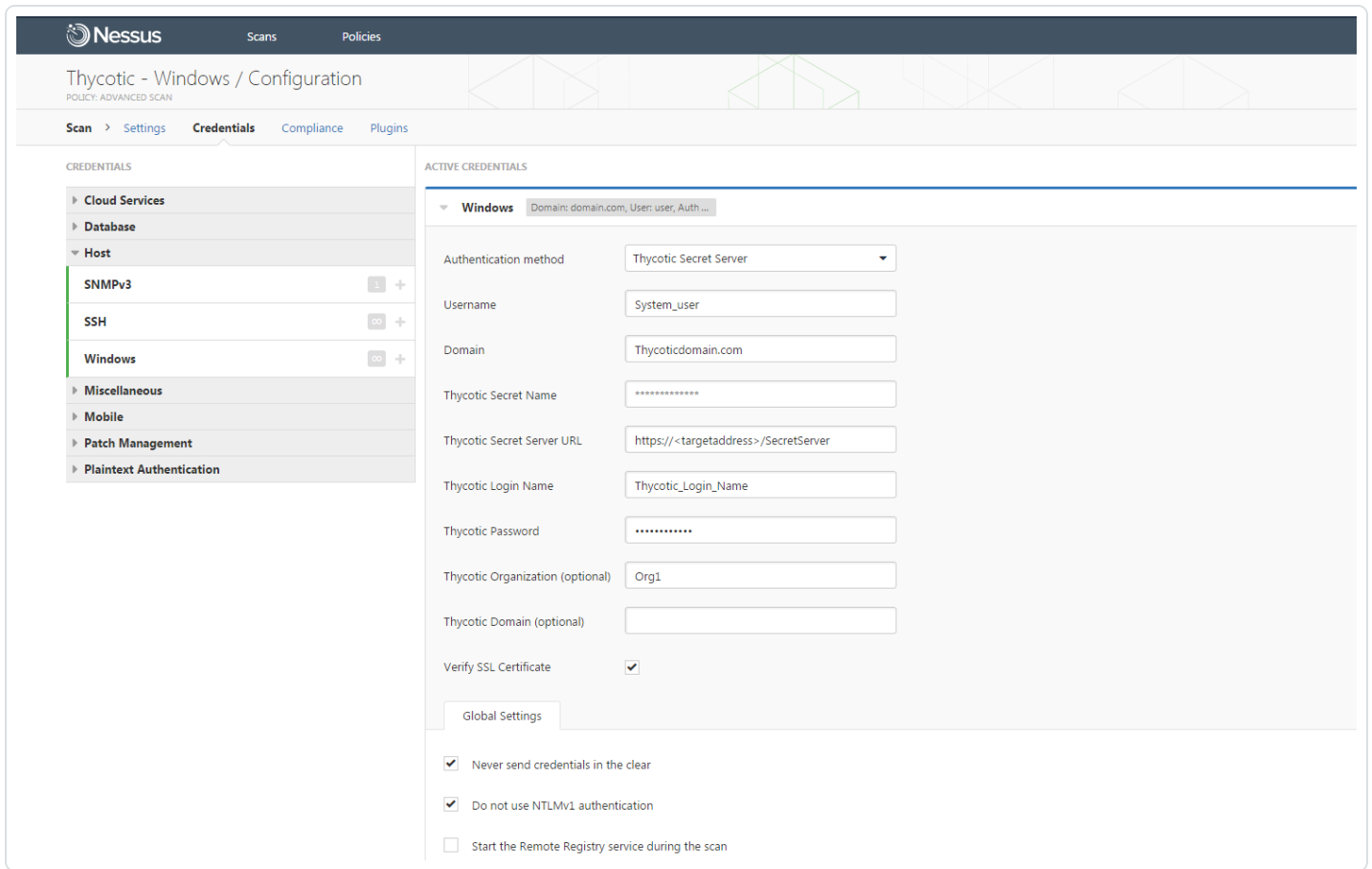
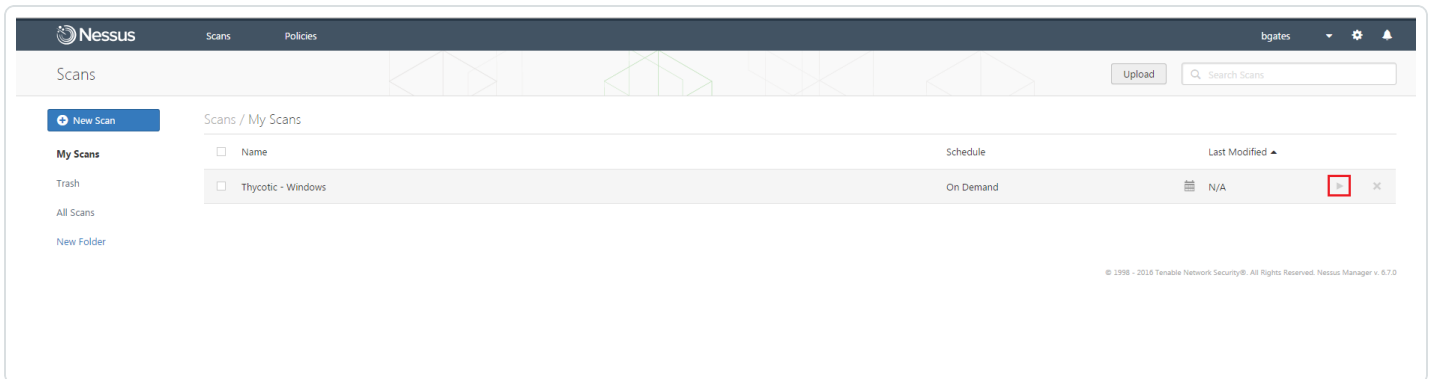


Table 1 – Thycotic Windows Credentials

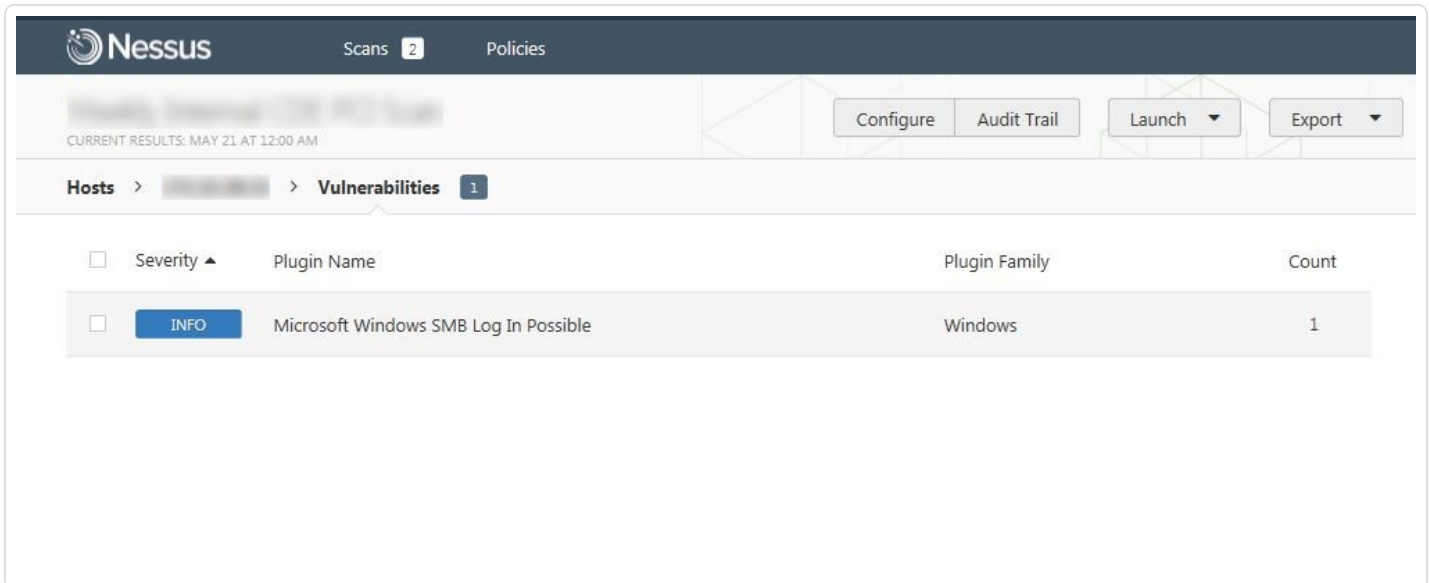
Option	Description
Username	The target system(s) username
Domain	This is an optional field if the above username is part of a domain
Thycotic Secret Name	The value (“Secret Name”) that the secret is stored as on the Thycotic server
Thycotic Secret Server URL	URL of the Thycotic Secret Server, which sets 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	This is an optional value used in cloud instances of Thycotic to

(optional)	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.



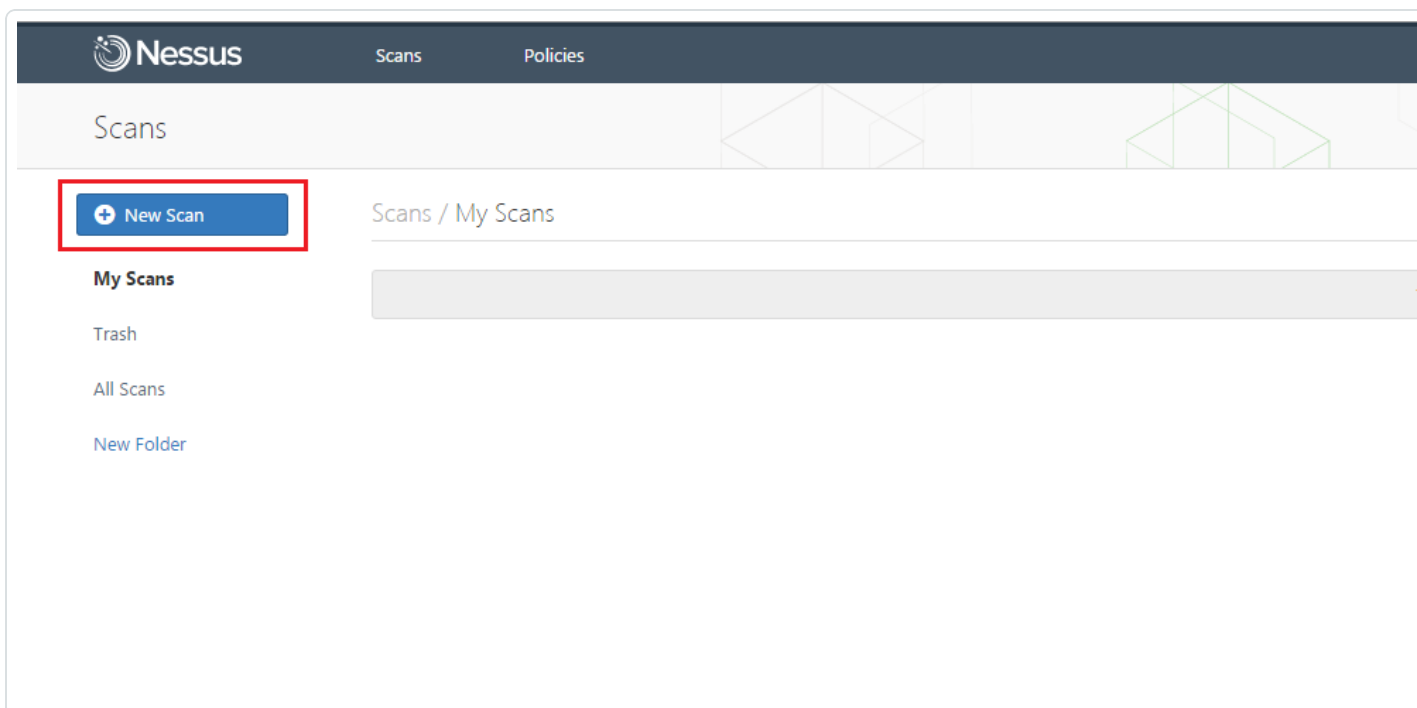
Once the scan has completed, select the completed scan and look for “Plugin ID 10394” (shown below), which validates that authentication was successful. If the authentication is not successful, refer to the “Troubleshooting” section of this document.



# 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.

The screenshot displays the Nessus Scan Library interface. At the top, there is a dark header with the Nessus logo and navigation links for 'Scans' and 'Policies'. Below the header, the page is titled 'Scan Library' and has tabs for 'All Templates', 'Scanner', and 'Agent'. The main content area is titled 'Scanner Templates' and contains ten cards, each representing a different scan type with an icon, title, and brief description:

- 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.

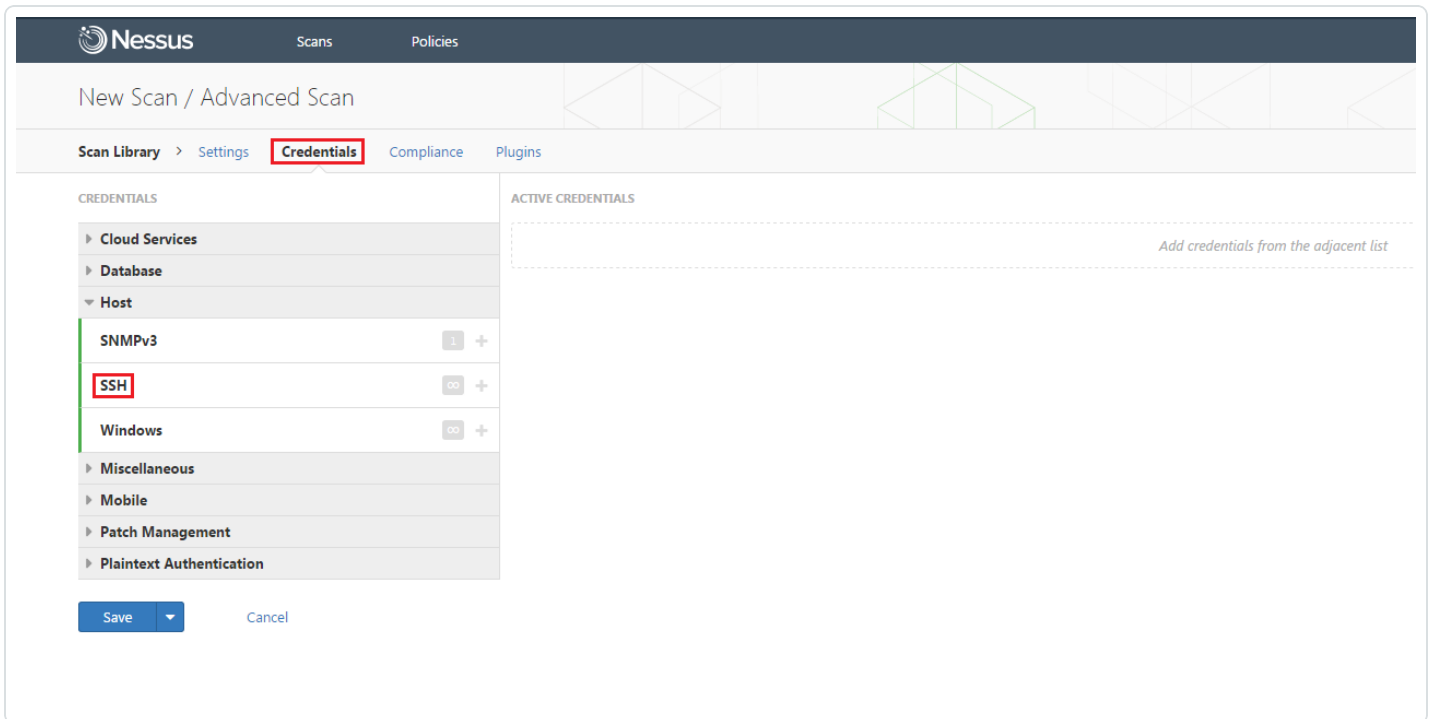
To configure a credentialed scan for Linux systems using Thycotic’s password management solution, enter a descriptive **Name** and enter the IP address(es) or hostname(s) of the scan **Targets**.

The screenshot shows the Nessus configuration interface for a scan named "Thycotic - Linux". The page is titled "Thycotic - Linux / Configuration" and has a policy of "ADVANCED SCAN". The navigation menu includes "Scan", "Settings", "Credentials", "Compliance", and "Plugins". The "Settings" section is expanded to show "BASIC" settings, with a sub-menu for "General". The "General" settings are as follows:

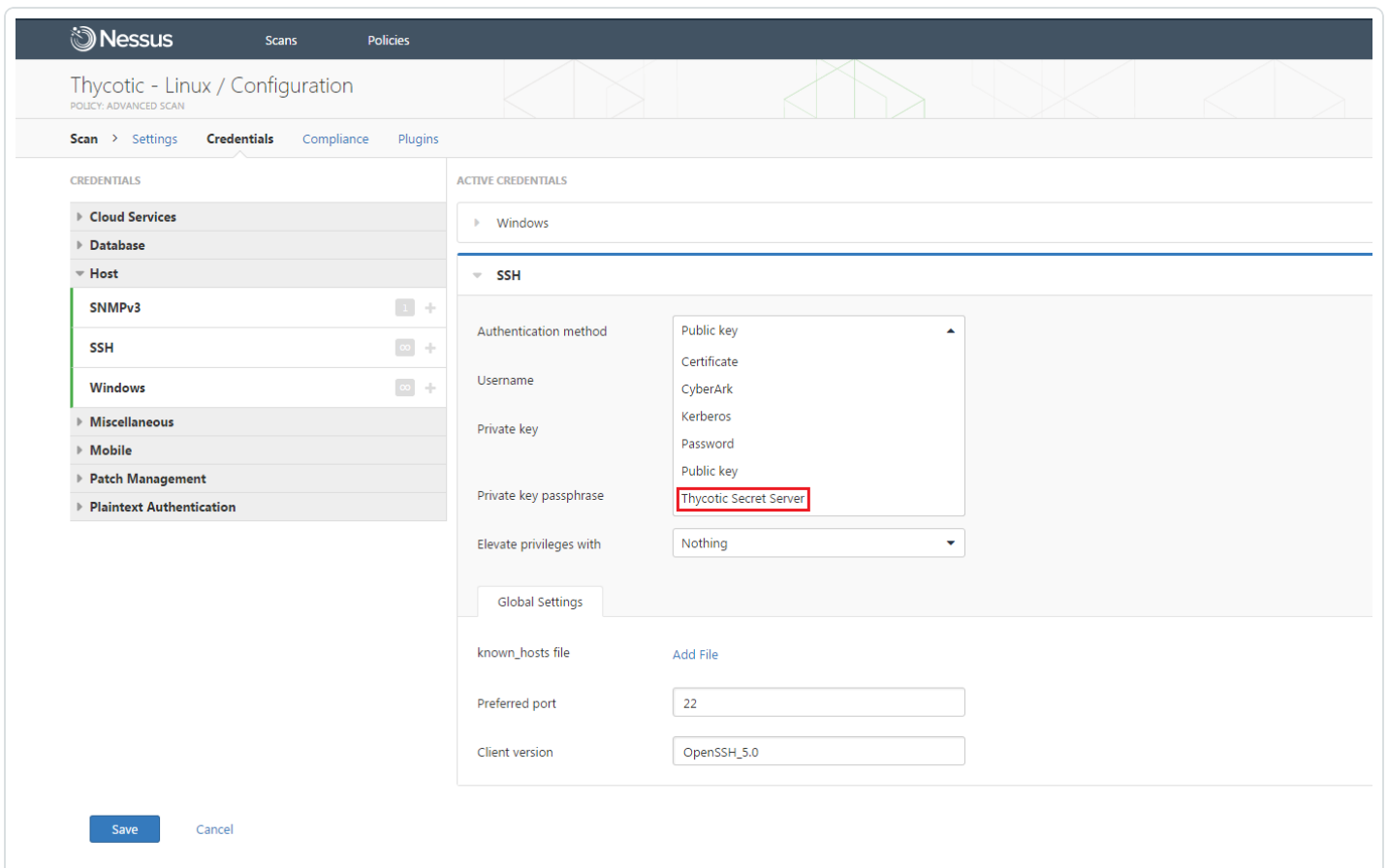
Field	Value
Name	Thycotic - Linux
Description	
Folder	My Scans
Dashboard	Enabled
Targets	172.1.2.3/24

At the bottom of the configuration area, there are "Upload Targets" and "Add File" options. Below the configuration area are "Save" and "Cancel" buttons.

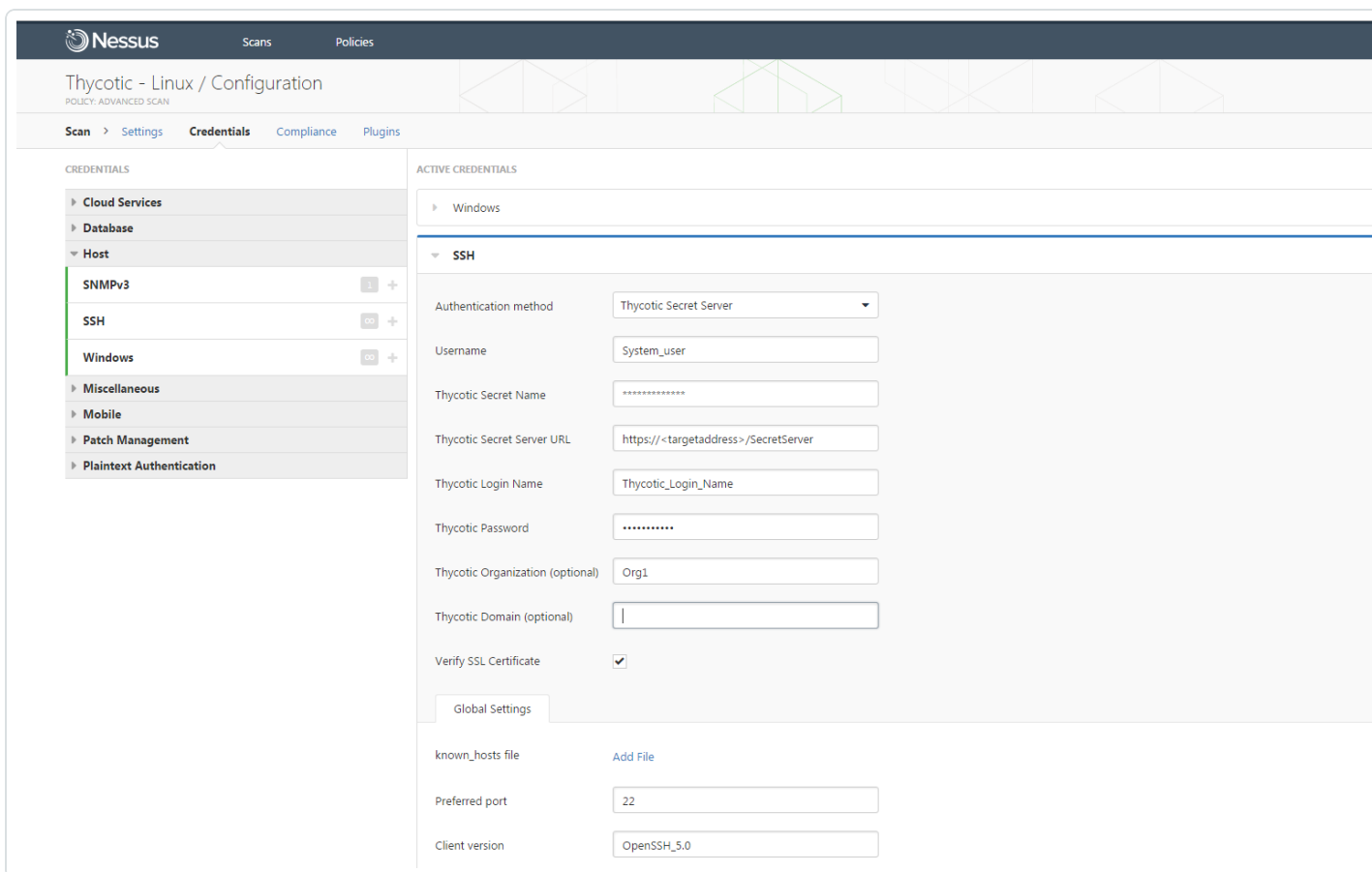
Once the “Name” and “Targets” have been configured, click on **Credentials** and then select **SSH** from the left-hand menu.



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



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.



The screenshot shows the Nessus configuration page for Thycotic SSH credentials. The left sidebar lists various credential categories, with 'SSH' selected. The main configuration area includes the following fields:

- Authentication method:** Thycotic Secret Server
- Username:** System\_user
- Thycotic Secret Name:** [Redacted]
- Thycotic Secret Server URL:** https://<targetaddress>/SecretServer
- Thycotic Login Name:** Thycotic\_Login\_Name
- Thycotic Password:** [Redacted]
- Thycotic Organization (optional):** Org1
- Thycotic Domain (optional):** [Empty]
- Verify SSL Certificate:**
- Global Settings:** [Tab]
- known\_hosts file:** Add File
- Preferred port:** 22
- Client version:** OpenSSH\_5.0

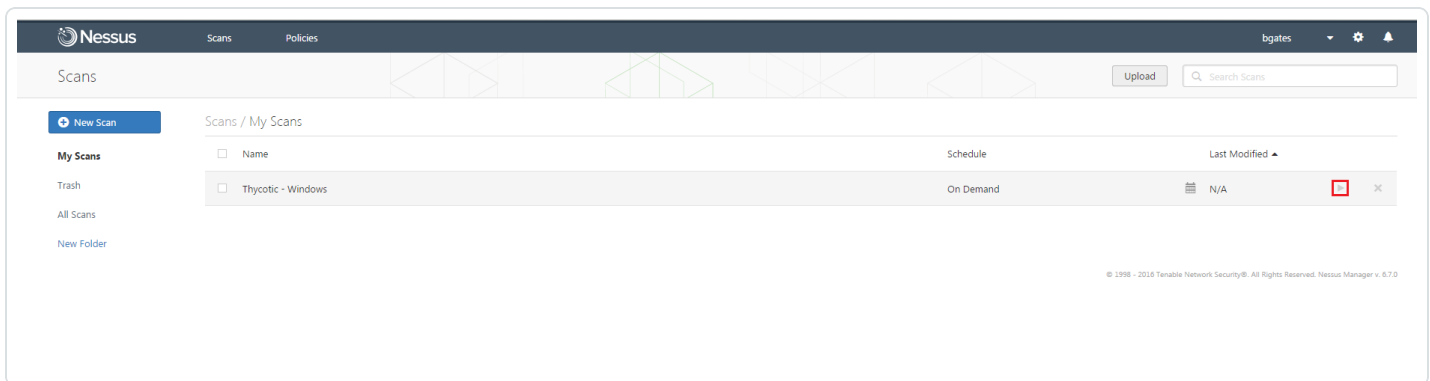
Table 2 – Thycotic SSH Credentials

Option	Description
Username	The target system(s) username
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.

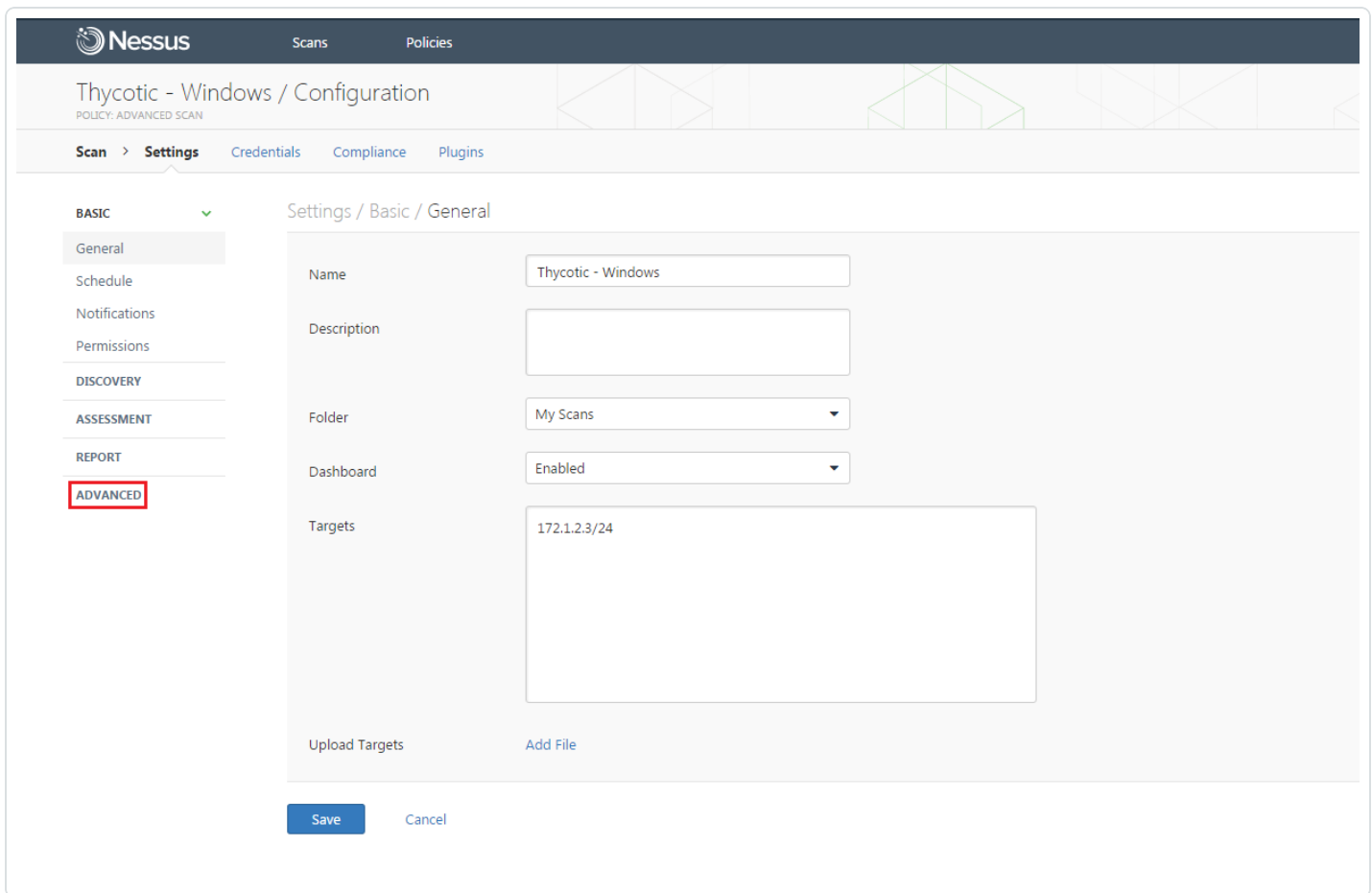


Once the scan has completed, select the completed scan and look for “Plugin ID 12634”, which validates that authentication was successful. If the authentication is not successful, refer to the “Troubleshooting” section of this document.

# 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 displays the Nessus Manager interface for configuring a scan. The top navigation bar includes 'Nessus', 'Scans', and 'Policies'. The main header shows 'Thycotic - Windows / Configuration' with a sub-header 'POLICY: ADVANCED SCAN'. Below this, a breadcrumb trail reads 'Scan > Settings > Credentials > Compliance > Plugins'. The left-hand menu is organized into sections: 'BASIC' (with a dropdown arrow), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED' (highlighted with a red box). Under 'BASIC', the 'General' sub-tab is selected. The main content area is titled 'Settings / Basic / General' and contains the following fields:

- Name:** Thycotic - Windows
- Description:** (empty text box)
- Folder:** My Scans (dropdown menu)
- Dashboard:** Enabled (dropdown menu)
- Targets:** 172.1.2.3/24 (text area)

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.

- 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.