



Tenable and Thycotic Integration Guide

Last Revised: April 01, 2026



Table of Contents

Introduction	3
Tenable Nessus with Thycotic Secret Server	4
Integration Requirements	4
Integrate with Thycotic Secret Server	4
Configure Windows Credentials	4
Configure Linux Credentials	10
Troubleshooting	16
Tenable Security Center with Thycotic Secret Server	18
Integration Requirements	18
Integrate with Thycotic Secret Server	18
Configure Windows Credentials	18
Configure SSH/Linux Credentials	20
Configure a Credentialed Scan	25
Verify Integration	28
Tenable Vulnerability Management with Thycotic Secret Server	30
Integration Requirements	30
Integrate with Thycotic Secret Server	30
Configure Windows Credentials	30
Configure Linux Credentials	35
Troubleshooting	39



Introduction

This document describes how to deploy Tenable Vulnerability Management 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 Tenable Vulnerability Management, 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 Tenable Vulnerability Management 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.



Tenable Nessus with Thycotic Secret Server

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

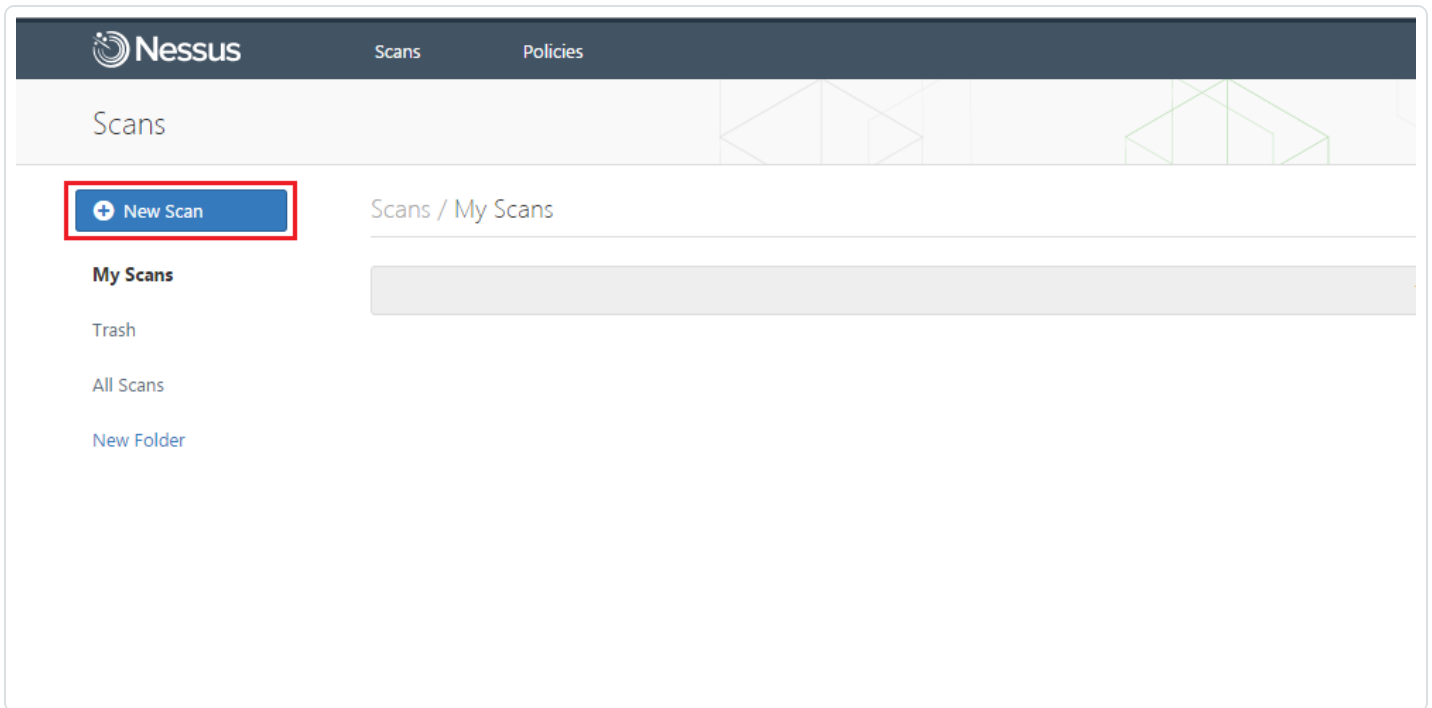
You can configure Nessus Manager to perform credentialed network scans of Windows and Linux systems using Thycotic's password management solution. Credentials are configured similarly to other credentialed network scans.

[Configure Windows Credentials](#)

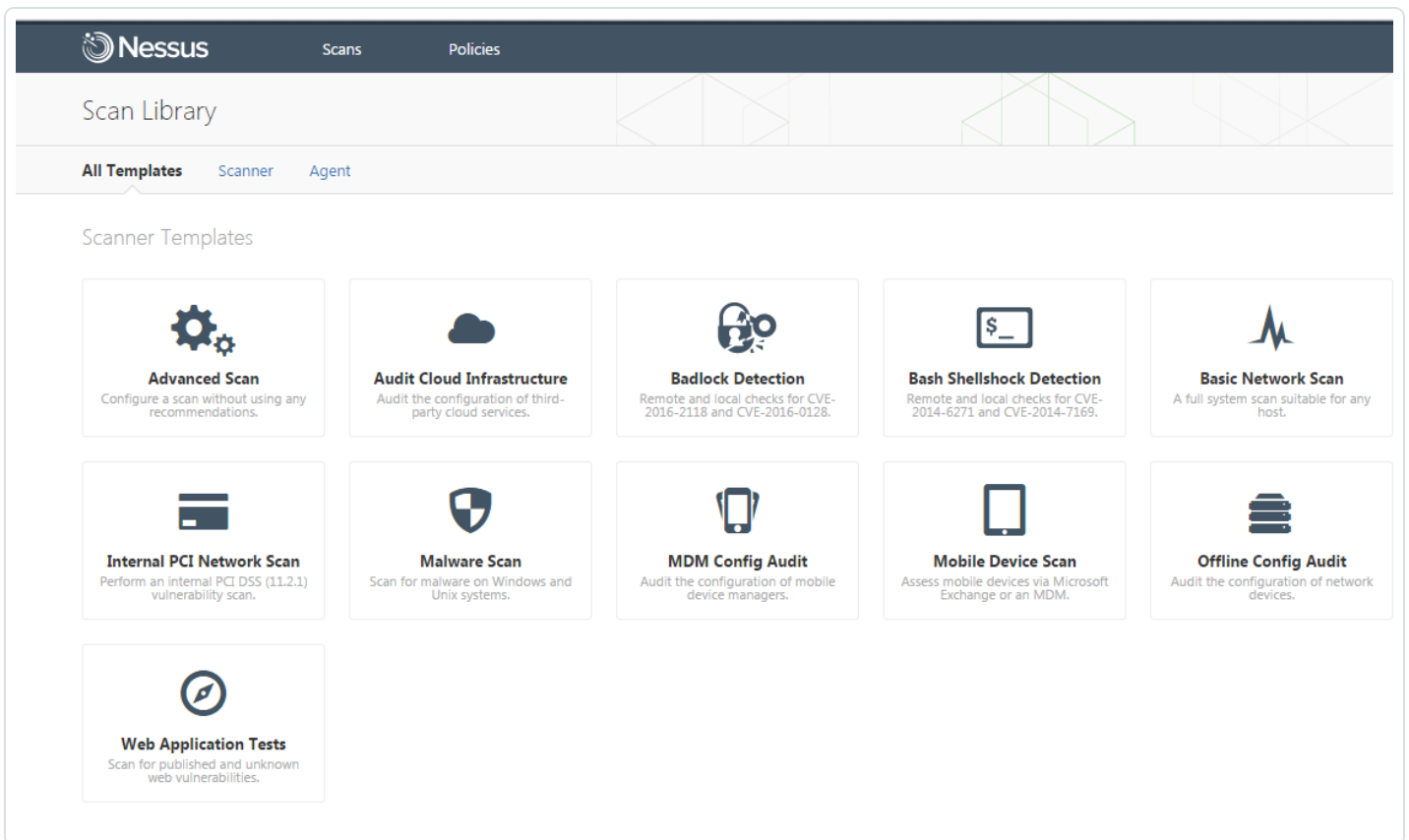
[Configure Linux Credentials](#)

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.





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

CREREDENTIALS

- Cloud Services
- Database
- Host
 - SNMPv3 1 +
 - 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**.

Nessus Scans Policies

New Scan / Advanced Scan

Scan Library > Settings **Credentials** Compliance Plugins

CREREDENTIALS

- Cloud Services
- Database
- Host
 - SNMPv3 1 +
 - SSH ∞ +
 - Windows** ∞ +
- Miscellaneous
- Mobile
- Patch Management
- Plaintext Authentication

ACTIVE CREDENTIALS

Windows

Authentication method Password

Username CyberArk

Password Kerberos

Domain LM Hash

NTLM Hash

Password

Thycotic Secret Server

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

Save Cancel



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.

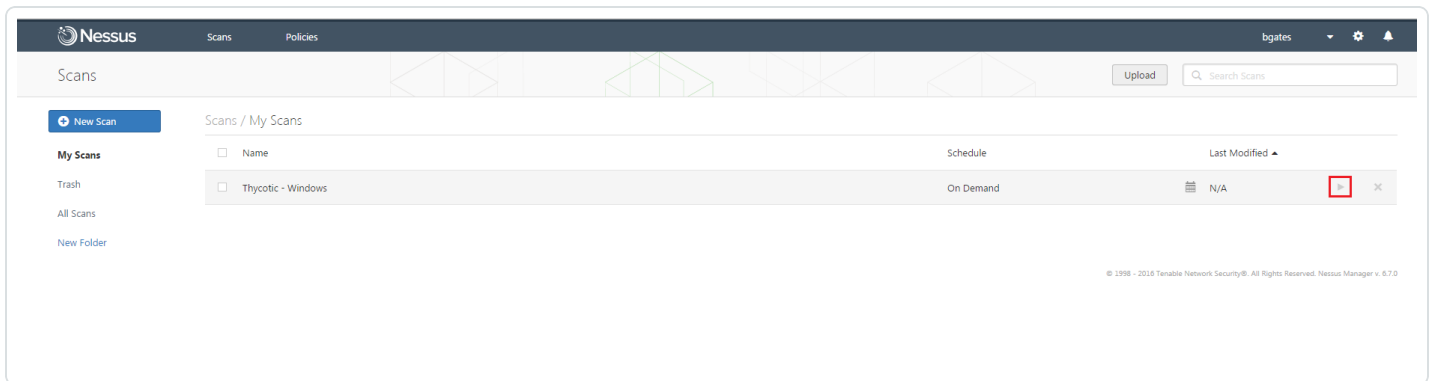
Table 1 - Thycotic Windows Credentials

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 (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 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 a dark header containing the Nessus logo, 'Scans 2', and 'Policies'. Below the header, there are navigation buttons: 'Configure', 'Audit Trail', 'Launch', and 'Export'. The main content area shows a breadcrumb trail: 'Hosts > [redacted] > Vulnerabilities 1'. Below this is a table with the following columns: 'Severity', 'Plugin Name', 'Plugin Family', and 'Count'. The table contains one entry: a blue 'INFO' severity level, the plugin name 'Microsoft Windows SMB Log In Possible', the plugin family 'Windows', and a count of '1'.

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.

The screenshot shows the Nessus interface with a dark header containing the Nessus logo, 'Scans', and 'Policies'. Below the header, the word 'Scans' is displayed. On the left side, there is a sidebar with a blue button labeled '+ New Scan' which is highlighted with a red rectangle. Below this button are the following menu items: 'My Scans', 'Trash', 'All Scans', and 'New Folder'. The main content area on the right is titled 'Scans / My Scans' and contains a large, empty grey rectangular area.



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 tabs for "Scans" and "Policies". Below the header, the page is titled "Scan Library" and includes a breadcrumb trail: "All Templates" (selected), "Scanner", and "Agent". The main content area is titled "Scanner Templates" and features a grid of ten template cards. Each card contains 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 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 web interface. At the top, there is a dark blue header with the Nessus logo and navigation links for 'Scans' and 'Policies'. Below this, the page title is 'Thycotic - Linux / Configuration' with a sub-label 'POLICY: ADVANCED SCAN'. A secondary navigation bar includes 'Scan', 'Settings', 'Credentials', 'Compliance', and 'Plugins'. On the left, a sidebar menu is organized into sections: 'BASIC' (with a green checkmark), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. Under 'BASIC', the 'General' option is selected and highlighted. The main content area is titled 'Settings / Basic / General' and contains several configuration fields: 'Name' (text input with 'Thycotic - Linux'), 'Description' (empty text input), 'Folder' (dropdown menu with 'My Scans'), 'Dashboard' (dropdown menu with 'Enabled'), and 'Targets' (text area with '172.1.2.3/24'). At the bottom of the main area, there are links for 'Upload Targets' and 'Add File'. At the very bottom, there 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.

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

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

Nessus 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

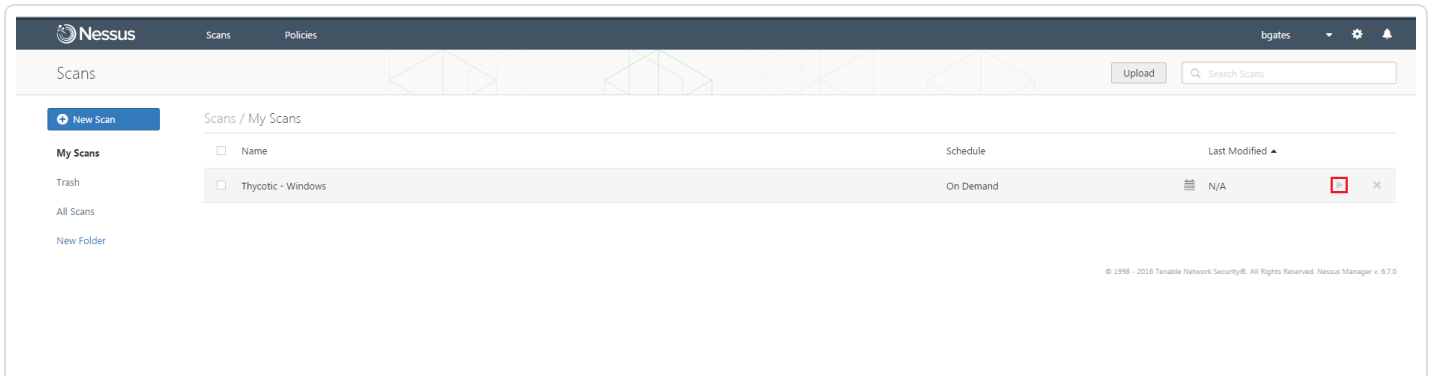
Option	Description
Username	The username that is used to authenticate via ssh to the system.
Thycotic Secret Name	This is the value that the secret is stored as on the Thycotic server. It is referred to as the “Secret Name” on the Thycotic server.
Thycotic Secret Server URL	This is used to set the transfer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



	<p>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.</p>
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 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	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.

Note: For additional information about all of the supported privilege escalation types and their accompanying fields, see [SSH](#) in the Tenable Nessus User Guide.

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

Tenable Nessus 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 configuration interface for a scan named "Thycotic - Windows". The page title is "Thycotic - Windows / Configuration" with a sub-header "POLICY: ADVANCED SCAN". The navigation menu includes "Scan", "Settings", "Credentials", "Compliance", and "Plugins". The left-hand menu is expanded to show "BASIC" (with a dropdown arrow), "General", "Schedule", "Notifications", "Permissions", "DISCOVERY", "ASSESSMENT", "REPORT", and "ADVANCED" (highlighted with a red box). 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 bottom right, 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.

Save

Cancel



Tenable Security Center with Thycotic Secret Server

Integration Requirements

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

- Thycotic Secret Server version 8.9 or later
- Tenable Security Center 5.3.2 or later

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 Tenable Security Center 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](#)

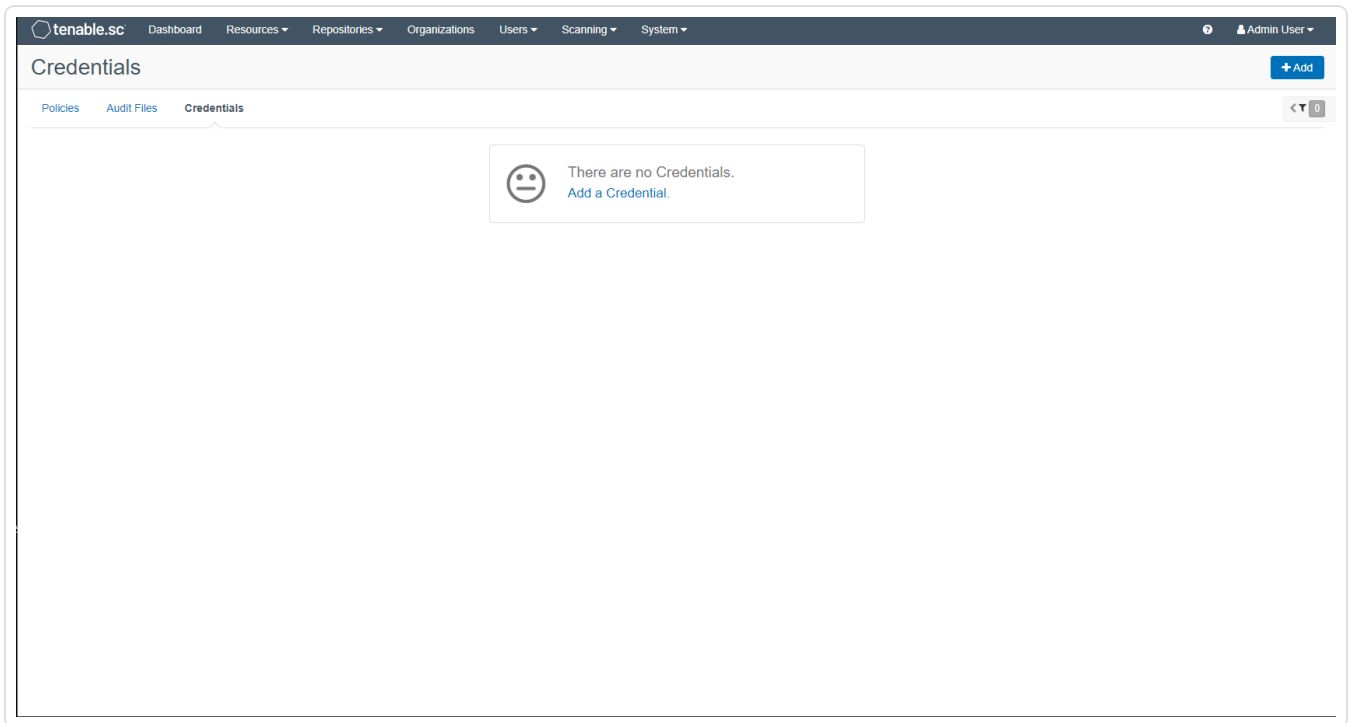
[Configure SSH/Linux Credentials](#)

[Configure a Credentialed Scan](#)

Configure Windows Credentials

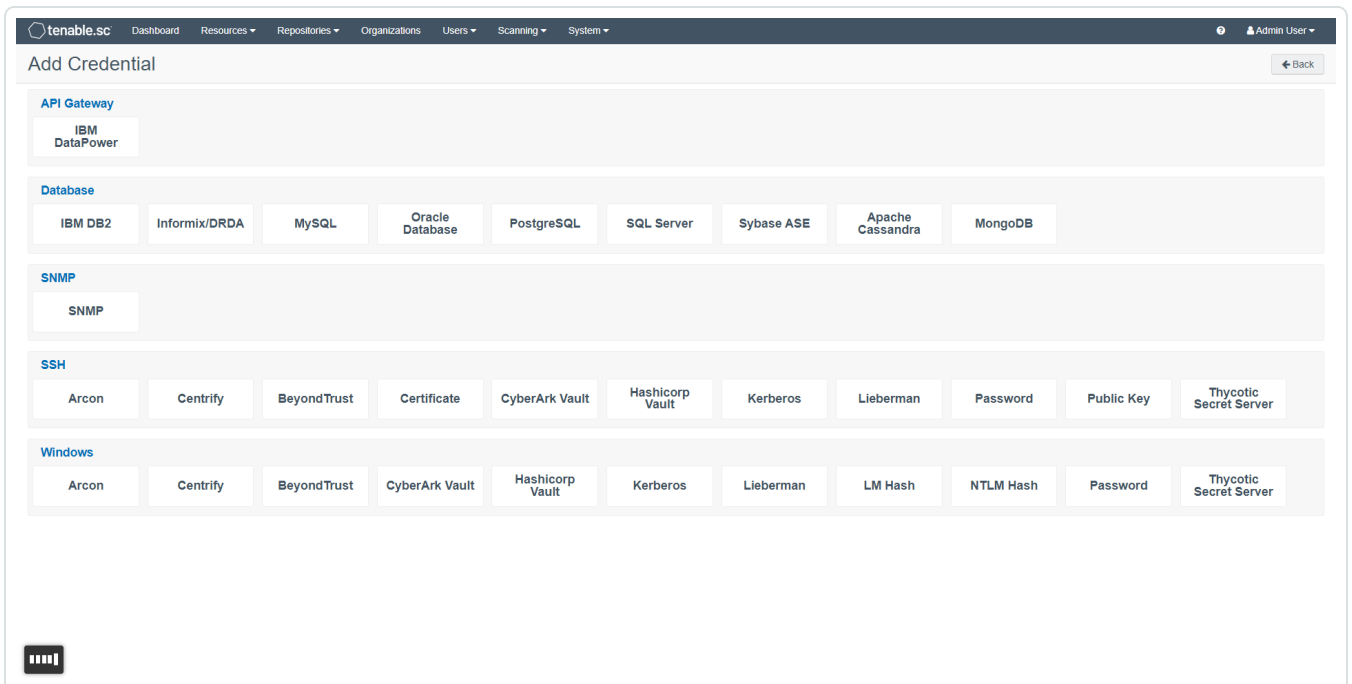
1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scanning > Credentials** (administrator users) or **Scans > Credentials** (organizational users).

The **Credentials** page appears.



3. Click **Add**.

The **Add Credential** page appears.



4. Select **Thycotic Secret Server**.



The configuration page appears.

5. Configure each field for Windows authentication. For more information, see Thycotic Secret Server Options in the [Tenable Security Center User Guide](#),
6. Click **Submit**.

Configure SSH/Linux Credentials

1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scanning > Credentials** (administrator users) or **Scans > Credentials** (organizational users).

The Credentials page appears.

Name	Tag	Type	Group	Owner	Last Modified
Thycotic - Linux		SSH	Full Access		1 minute ago
Thycotic - Windows		Windows	Full Access		1 hour ago



3. Click **Add**.

The Add Credential page appears.

SecurityCenter SC™ Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾

Add Credential ← Back

General

Name*

Description

Tag

Credential

Type

Authentication Method


Username*


Password*

Domain

4. In the **General** section, type a **Name** and **Description** for the credentials.

5. (Optional) Select a **Tag**.



SecurityCenter  Dashboard ▾ Analysis ▾ Scans ▾ Reporting ▾ Assets Workflow ▾ Users ▾ User Profile ▾

Add Credential ← Back

General

Name*

Description

Tag

6. In the **Credential** section, in the **Type** drop-down box, select **SSH**.

Credential

Type

Authentication Method

Username*

Private Key*

Passphrase

Privilege Escalation



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

Credential

Type

Authentication Method

Username*

Thycotic Secret Name*

Thycotic Secret Server URL*

Thycotic Login Name*

Thycotic Password*

Thycotic Organization (optional)

Thycotic Domain (optional)

Verify SSL Certificate

Use Private Key

8. Configure each option for SSH configuration. Refer to [Thycotic Secret Server SSH Options](#) for a description of each option.

9. Click **Submit** to finalize the changes.

Thycotic Secret Server SSH Options

The following table describes the options to configure when using Thycotic Secret Server as the **Authentication Method** for 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	The value you want Tenable Security Center to use when setting



URL	<p>the transfer method, target, and target directory for the scanner. Find the value on the Thycotic server, in Admin > Configuration > Application Settings > Secret Server URL.</p> <p>For example, if you type <i>https://pw.mydomain.com/SecretServer</i>, Tenable Security Center determines it is an SSL connection, that <i>pw.mydomain.com</i> is the target address, and that <i>/SecretServer</i> is the root directory.</p>
Thycotic Login Name	The username used to authenticate to the Thycotic server.
Thycotic Password	The password associated with the Thycotic Login Name you provided.
Thycotic Organization (optional)	In cloud instances of Thycotic, the value that identifies which organization the Tenable Security Center query should target.
Thycotic Domain (optional)	This is an optional value set if the domain value is set for the Thycotic server.
Use Private Key	If enabled, Tenable Security Center uses key-based authentication for SSH connections instead of password authentication.
Verify SSL Certificate	If enabled, Tenable Security Center verifies the SSL Certificate on the Thycotic server.
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 style="border: 1px solid blue; padding: 5px;"><p>Note: For additional information about all of the supported privilege escalation types and their accompanying fields, see SSH in the Tenable Nessus User Guide.</p></div>

Configure a Credentialed Scan



1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scans > Active Scans**.

The Active Scans page appears.

3. Click **Add**.

The Add Active Scan page appears.

SecurityCenter SC Dashboard Analysis Scans Reporting Assets Workflow Users

Add Active Scan

← Back

- General
- Settings
- Targets
- Credentials
- Post Scan

General

Name*

Description

Policy* Select a Policy

Schedule

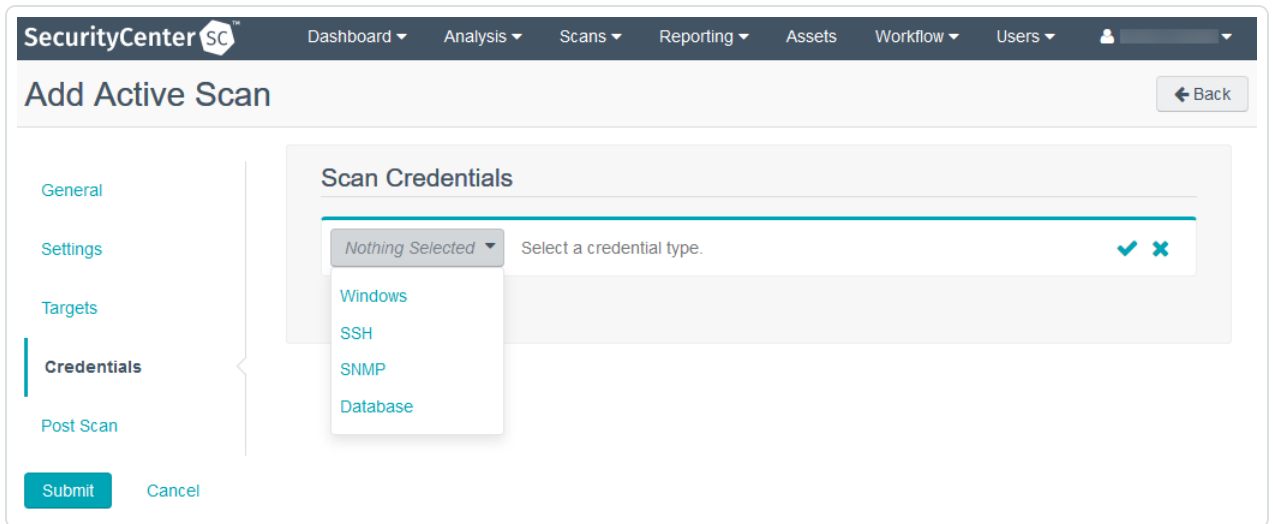
Schedule On Demand [✎](#)

4. In the **General** section:
 1. Type a **Name** for the scan.
 2. (Optional) Type a **Description** for the scan.
 3. Select a **Policy** for the scan.
 4. (Optional) Select a **Schedule** for the scan.
5. In the **Settings** section:
 1. If prompted, select a **Scan Zone** for the scan.
 2. Select an **Import Repository** for the scan.
 3. Select a **Scan Timeout Action** for the scan.

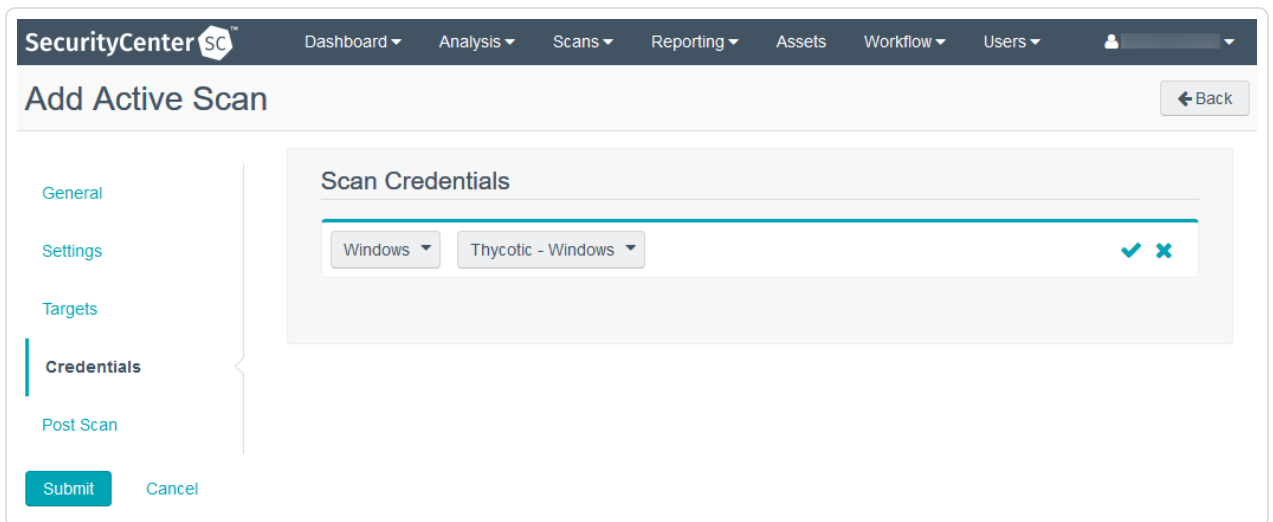


4. Select a **Rollover Schedule** for the scan.
5. Enable or disable the **Advanced** options.
6. In the **Targets** section:
 1. Select a **Target Type** for the scan.

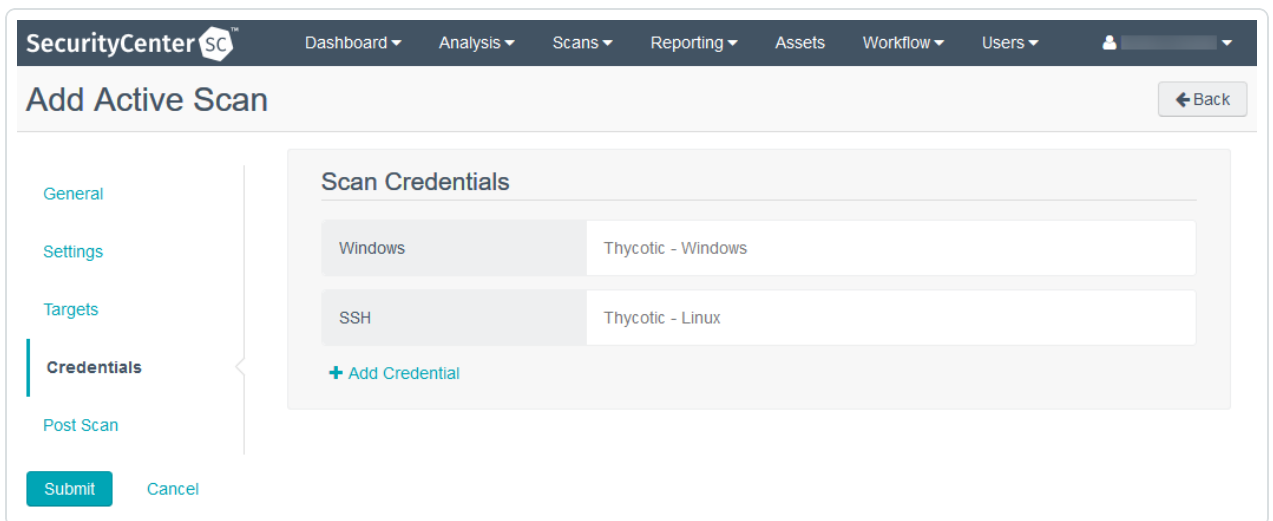
The page updates to show the required options for that target type.
 2. Select one or more **Assets** and/or **IPs / DNS Names** for the scan.
7. In the **Credentials** section, to configure credentialed scanning using your Thycotic credentials, click **Add Credential**.
 1. In the drop-down box, select **Windows** to use Windows credentials or **SSH** to use Linux credentials.



2. In the drop-down box that appears to the right of the drop-down box in the previous step, select the name of the Thycotic credentials configured in step 4 of [Configure Windows Credentials](#) or step 4 of [Configure SSH/Linux Credentials](#).



3. Click the check mark to save the credentials.
4. (Optional) Repeat step 7 to configure additional credentials.



8. In the **Post Scan** section:
 1. (Optional) If you previously added an email address to your account profile and you want to configure email notifications, enable or disable **E-Mail Me on Launch** or **E-Mail Me on Completion**.
 2. (Optional) If you want to configure automatic report generation, click Add Report. For more information, see [Add a Report to a Scan](#).
9. Click **Submit**.

Verify Integration



To verify the integration succeeded, you can initiate a scan using a custom policy containing only plugins that validate access to Windows and Linux targets. This policy is known as a Quick Credential Debug (QCD) scan. QCD enables administrators to perform quick credential tests without performing a full a vulnerability scan.

A QCD scan policy for Windows and Linux includes the following plugins (plugin ID numbers are in parentheses):

- (10394) Microsoft Windows SMB Log In Possible
- (12634) Authenticated Check: OS Name and Installed Package Enumeration
- (21745) Authentication Failure - Local Checks Not Run

Plugin 10394 verifies authentication to Windows targets, plugin 12634 verifies authentication to Linux targets by attempting to authenticate via SSH and enumerate a list of installed packages, and plugin 21745 reports authentication failures along with an audit trail useful for debugging.

Refer to the [Tenable Security Center User Guide](#) for information on how to create a custom scan policy containing only these three plugins.

- [Add a Scan Policy](#)
- [Configure Plugin Options](#)
- [Start or Pause a Scan](#)



Tenable Vulnerability Management with Thycotic Secret Server

Integration Requirements

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

- Thycotic Secret Server version 8.9 or later
- Tenable Vulnerability Management, Tenable's cloud platform for vulnerability management

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

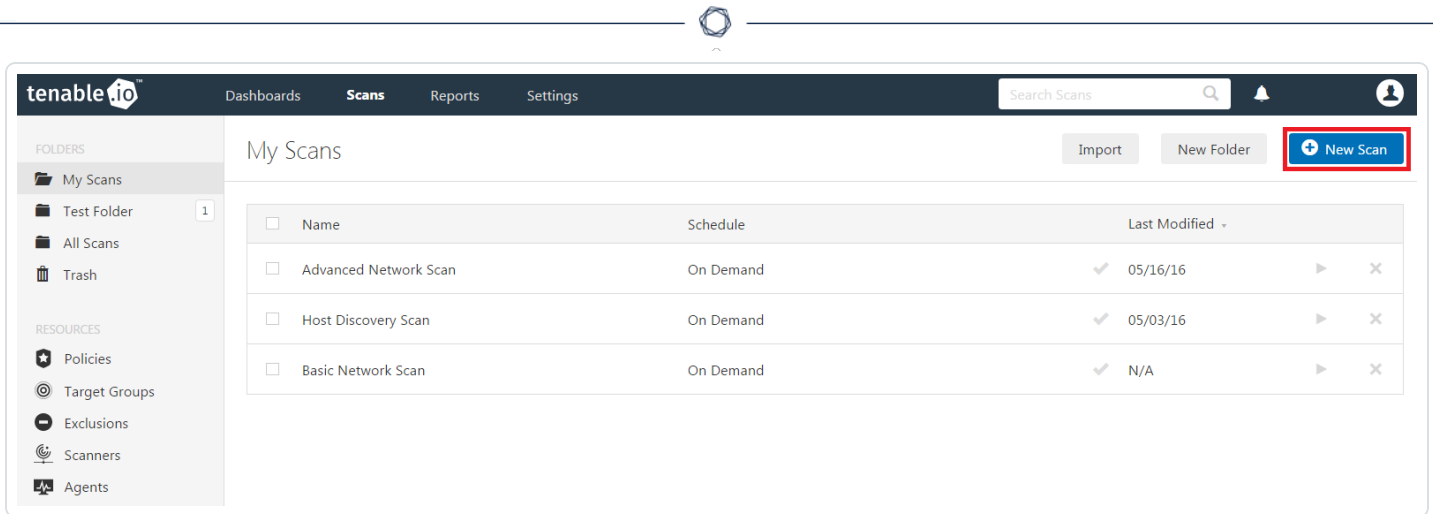
You can configure Tenable Vulnerability Management to perform credentialed network scans of Windows and Linux systems using Thycotic's password management solution. Credentials are configured similarly to other credentialed network scans.

[Configure Windows Credentials](#)

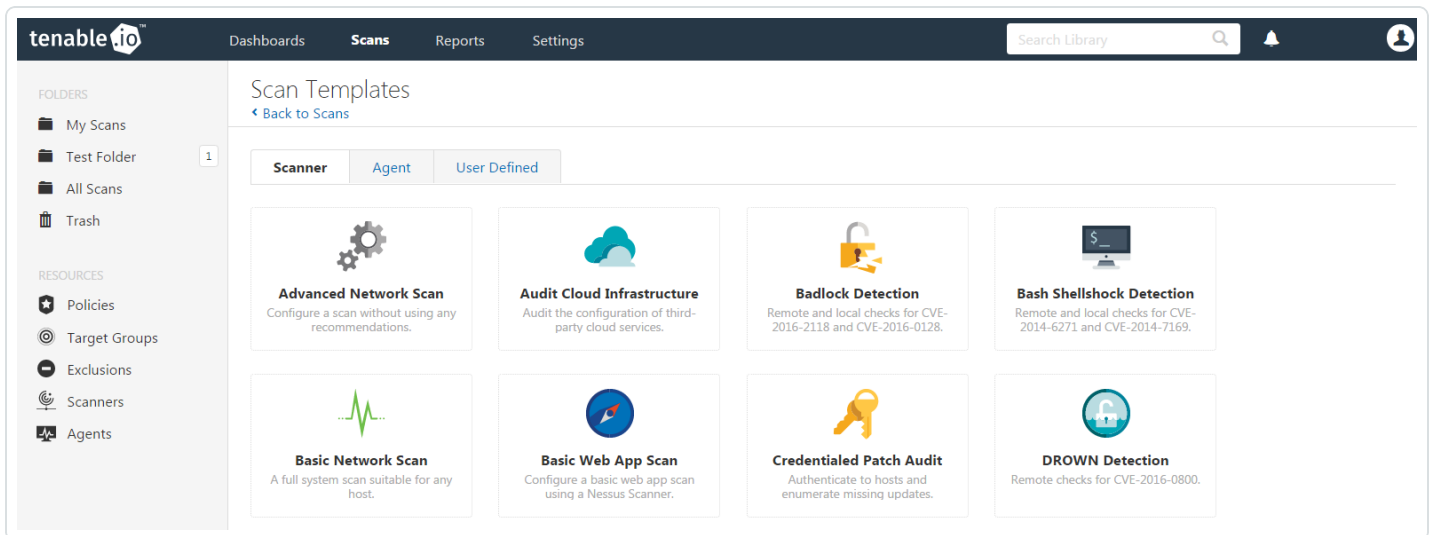
[Configure Linux Credentials](#)

Configure Windows Credentials

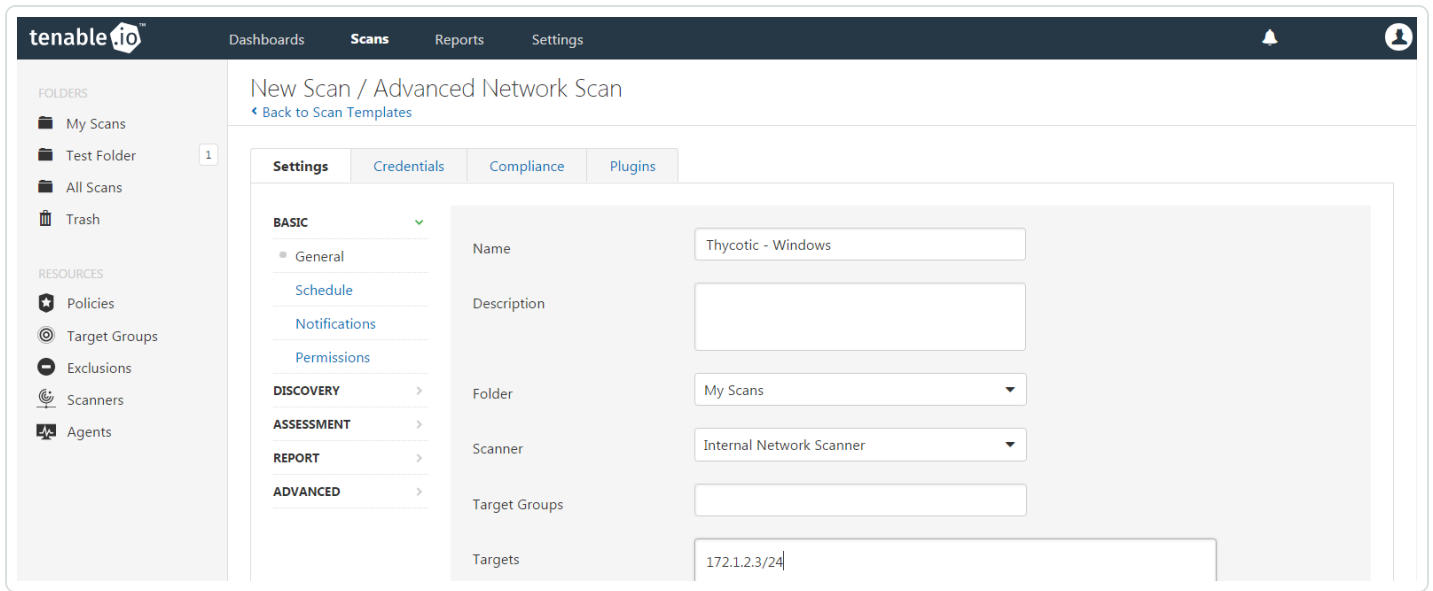
Log in to Tenable Vulnerability Management and click **Scans** and then the **+ New Scan** button to configure Tenable Vulnerability Management for credentialed scans of Windows systems using Thycotic's password management solution.



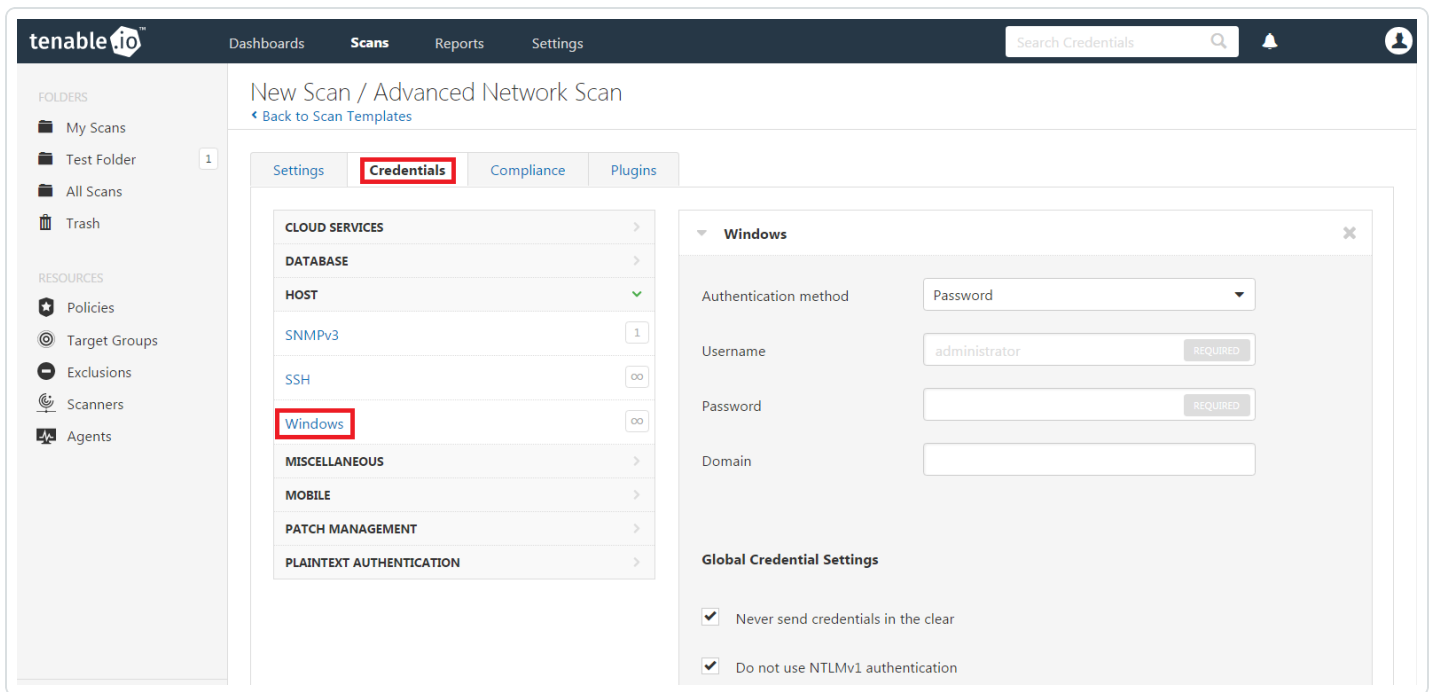
Select a “Scan Template” for the scan type required for your scan. For demonstration purposes, the “Advanced Network Scan” template will be used.



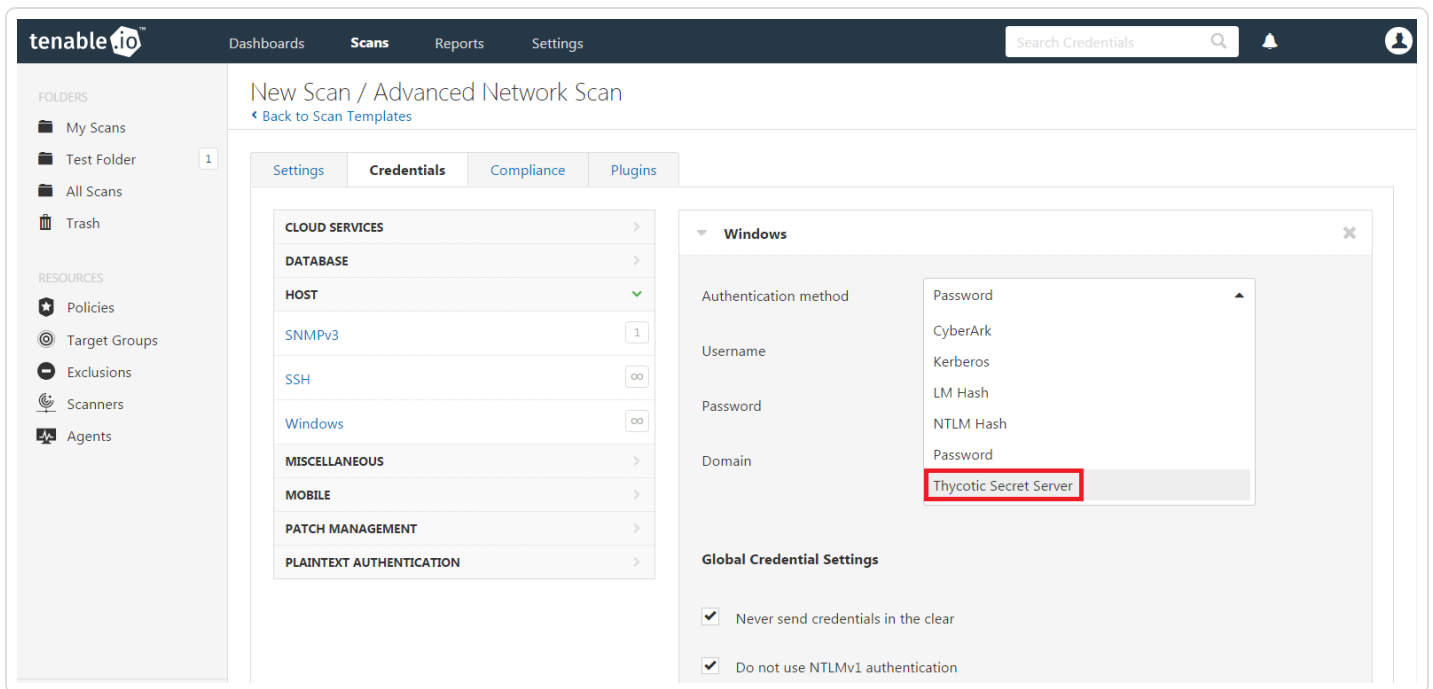
To configure a credentialed scan for Windows systems using Thycotic’s password management solution, enter a descriptive **Name** and enter the IP address(es) or hostname(s) of the scan **Targets**.



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**.



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.

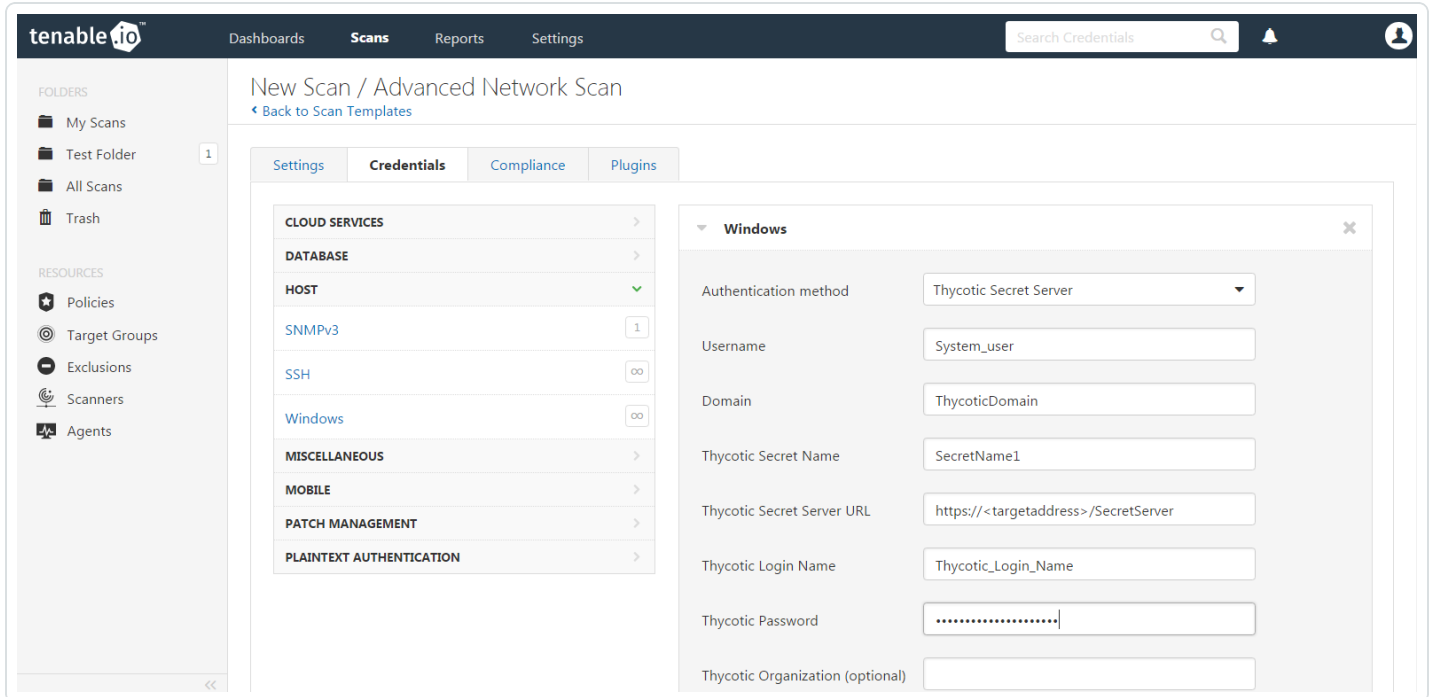
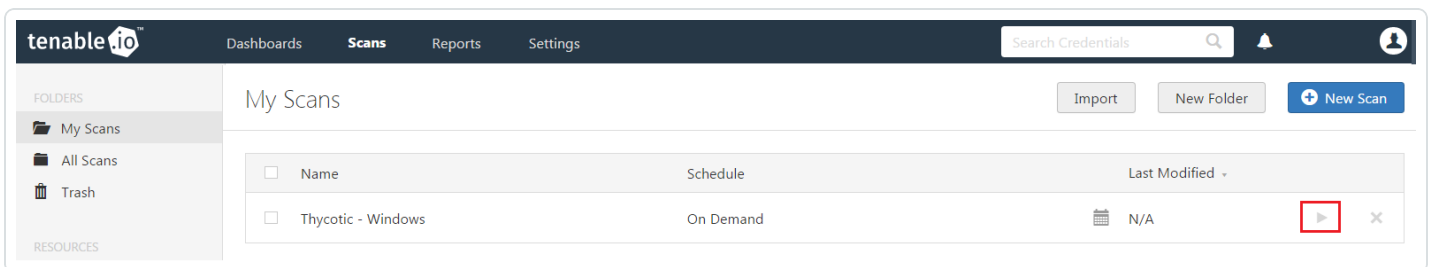


Table 1 - Thycotic Windows Credentials



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 (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 10394” (shown below), which validates that authentication was successful. If the authentication is not successful, refer to the [Troubleshooting](#) section of this document.

tenable.io | Dashboards | Scans | Reports | Settings | Search Credentials

192.168.1.106
[Back to Windows 10](#) | [Configure](#) | [Export](#)

Vulnerabilities 1

Sev	Name	Family	Count
●	Microsoft Windows SMB Log In Possible	Windows	1

Host Details

IP: 192.168.1.106
 MAC: 0c:8b:fd:52:05:1c
 OS: Microsoft Windows 10 Home
 Start: January 3 at 10:44 AM
 End: January 3 at 10:50 AM
 Elapsed: 6 minutes

Configure Linux Credentials

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

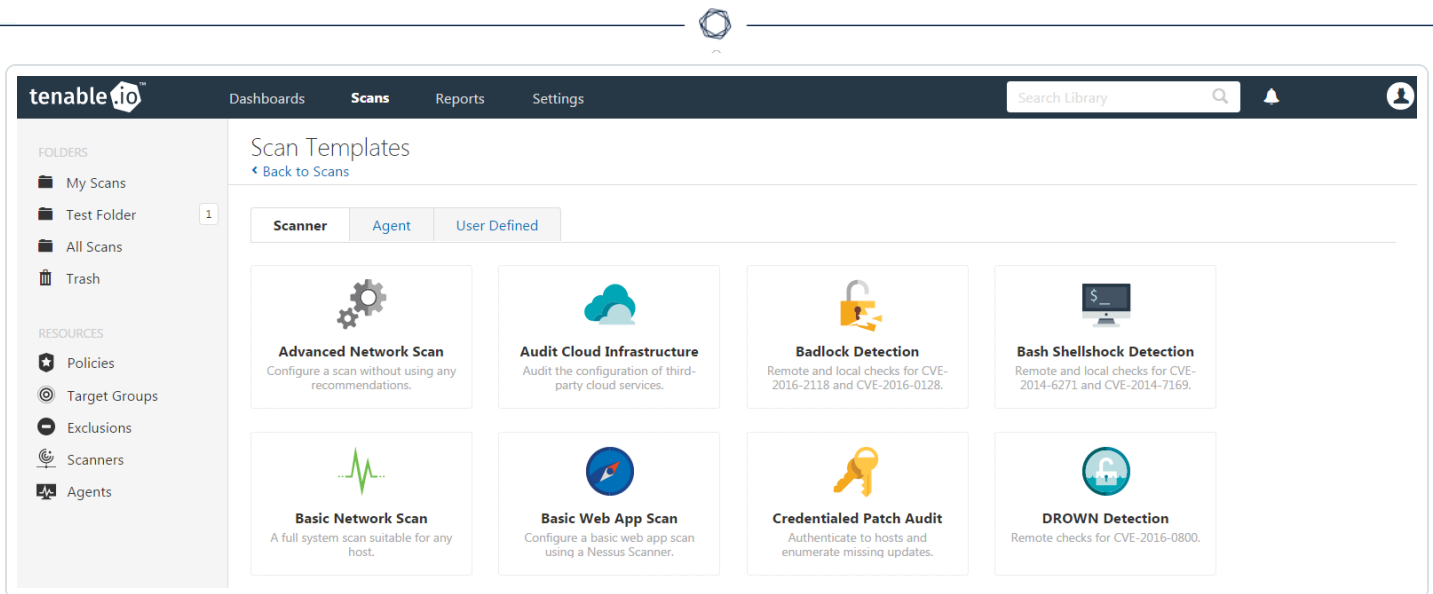
Log in to Tenable Vulnerability Management and click **Scans** and then the **+ New Scan** button to begin the Linux credentialed scan configuration.

tenable.io | Dashboards | Scans | Reports | Settings | Search Scans

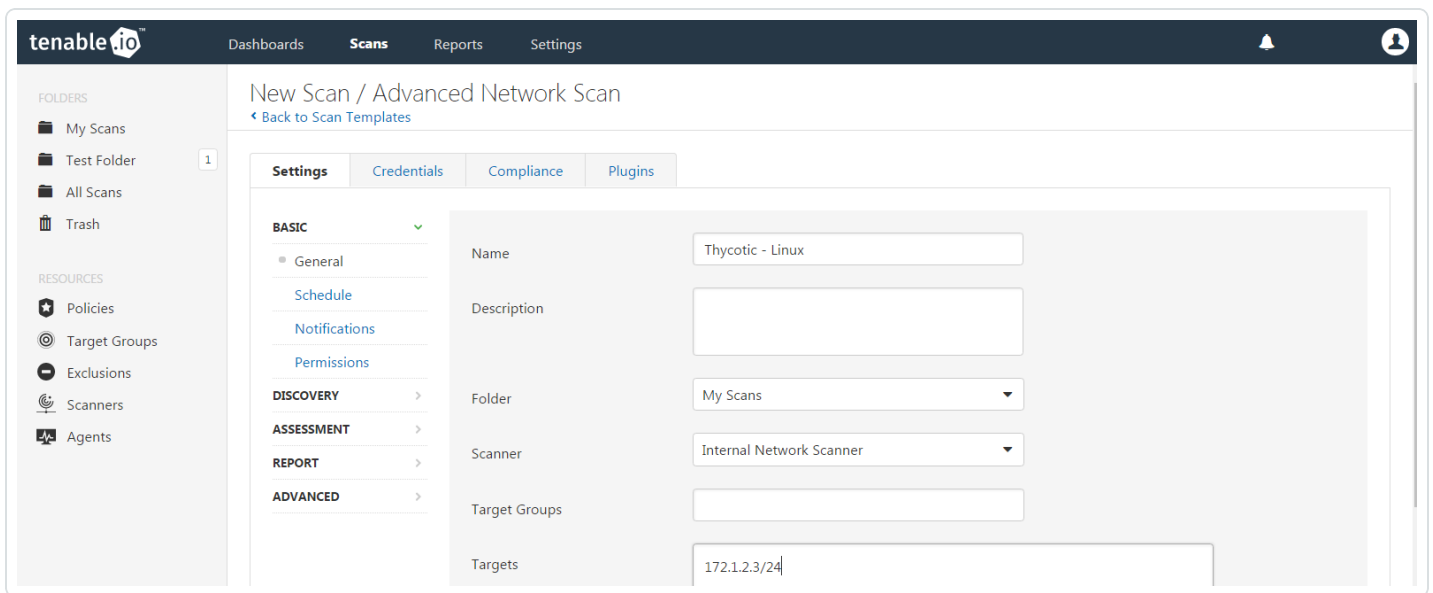
My Scans | [Import](#) | [New Folder](#) | [+ New Scan](#)

Name	Schedule	Last Modified
Advanced Network Scan	On Demand	05/16/16
Host Discovery Scan	On Demand	05/03/16
Basic Network Scan	On Demand	N/A

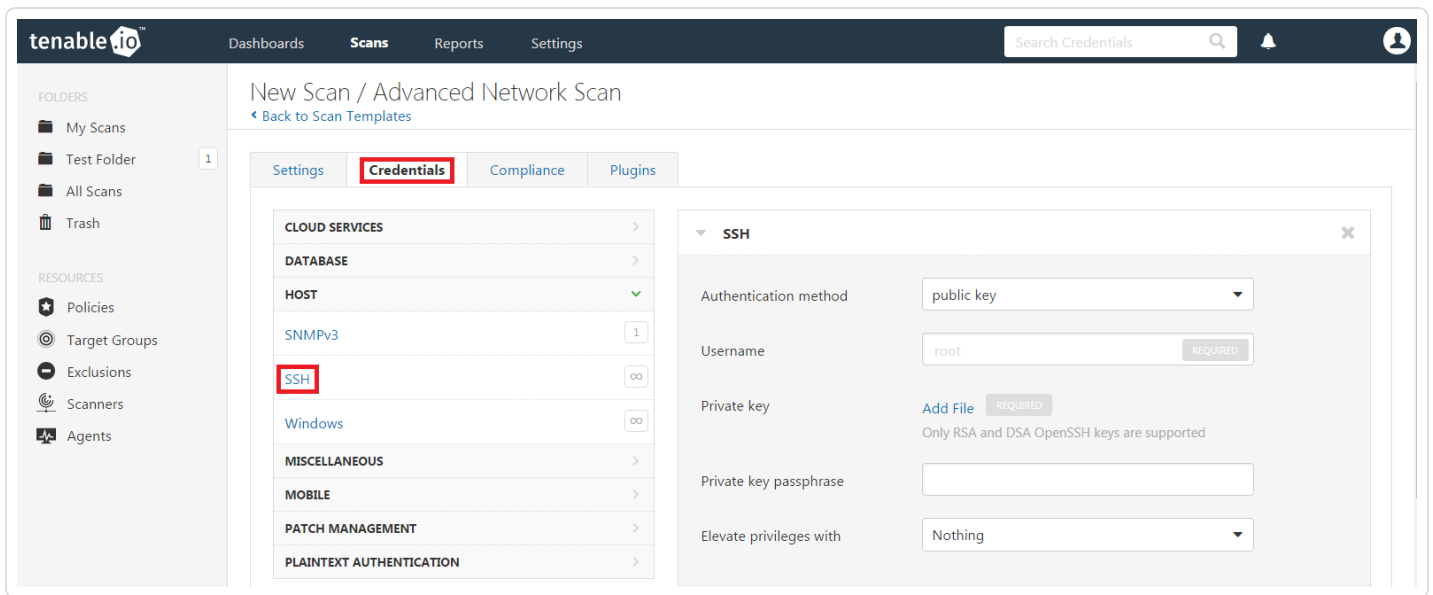
Select a “Scan Template” for the scan type required for your scan. For demonstration purposes, the “Advanced Scan” template will be used.



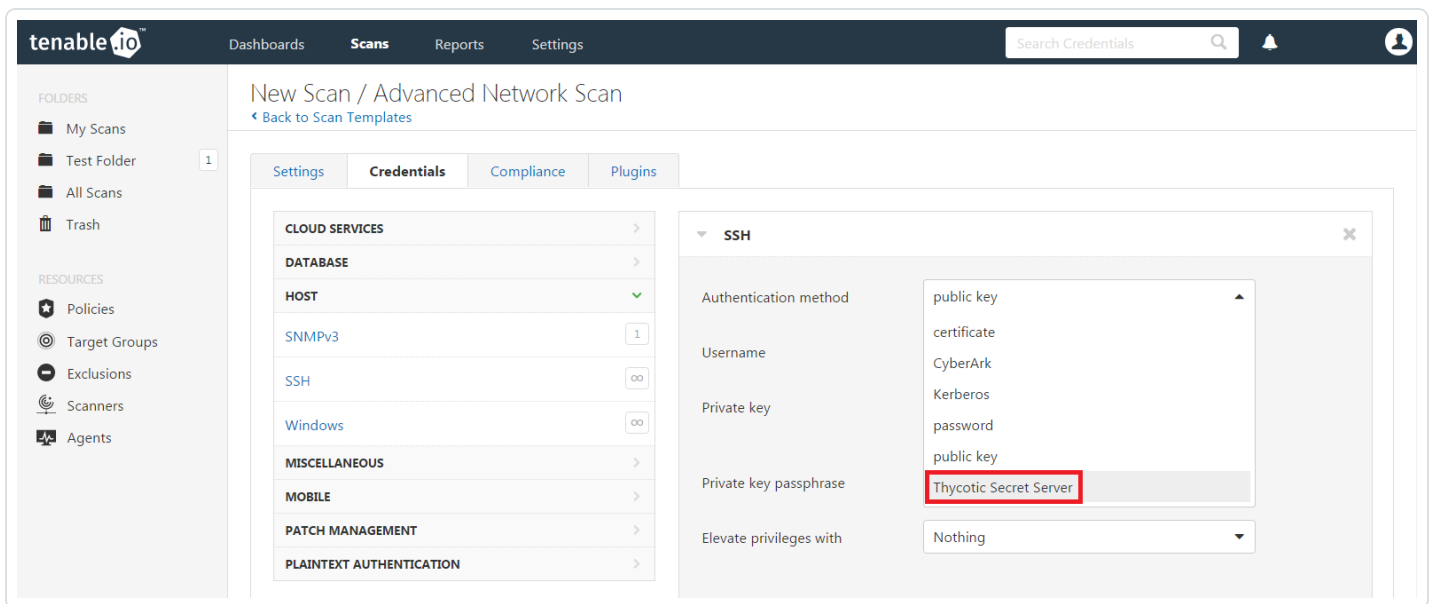
To configure a credentialed scan for Linux systems using Thycotic’s password management solution, enter a descriptive **Name** and enter the IP address(es) or hostname(s) of the scan **Targets**.



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



In the **Authentication method** drop-down box, 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.

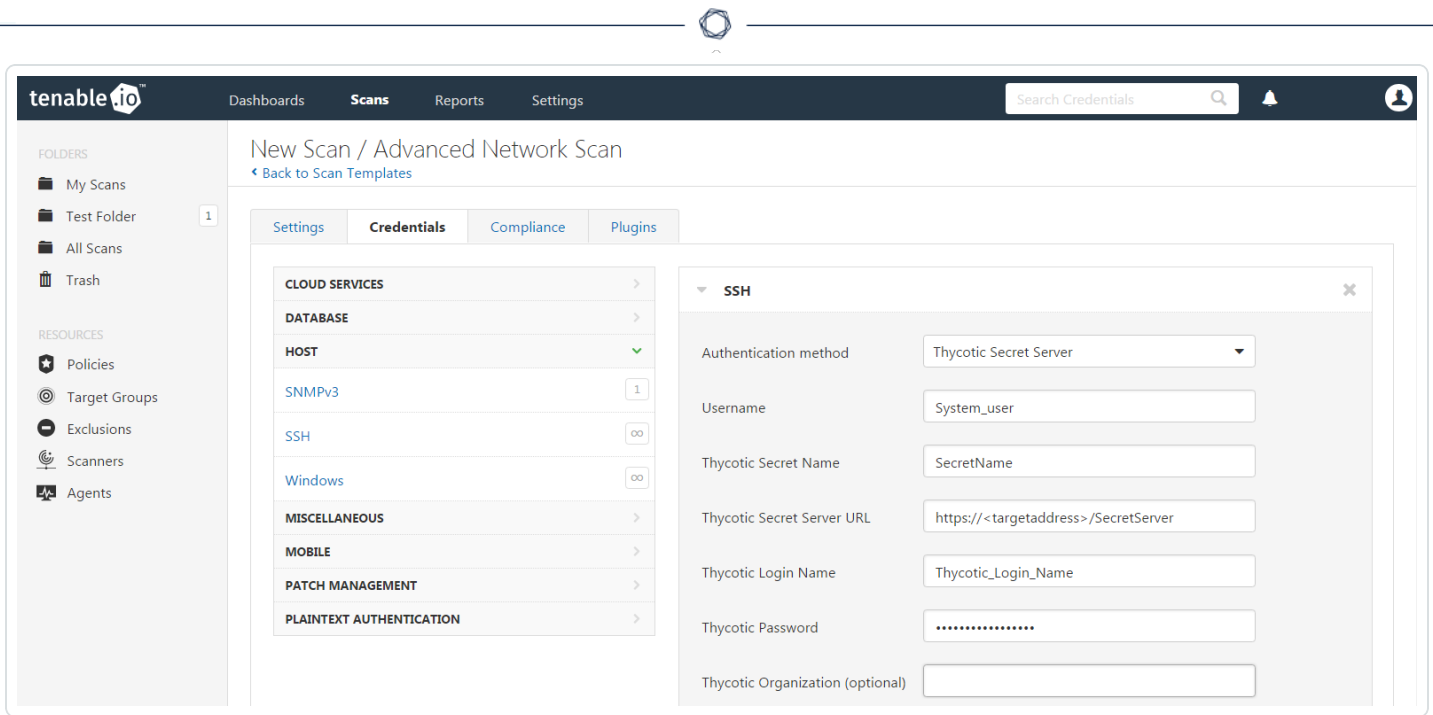


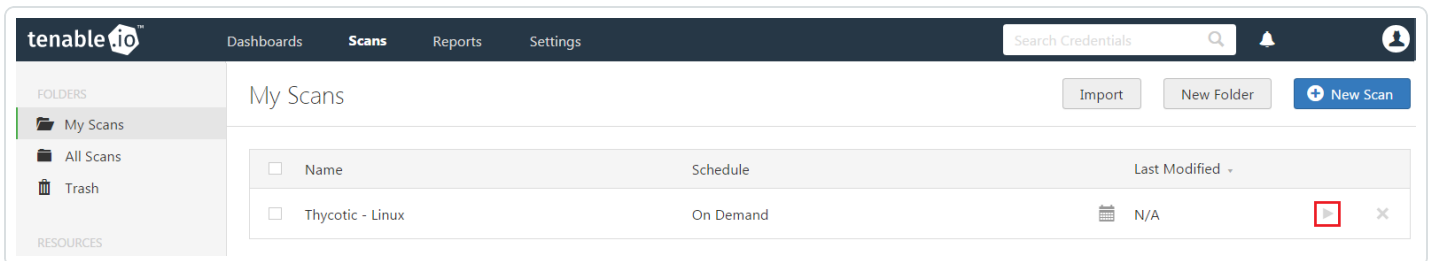
Table 2 - Thycotic SSH Credentials

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 Admin > Configuration > Application Settings > Secret Server URL on the Thycotic server. For example consider the following address <code>https://pw.mydomain.com/SecretServer/</code> . 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 Thycotic Login Name .
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	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. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">Note: For additional information about all of the supported privilege escalation types and their accompanying fields, see Host in the Tenable Vulnerability Management 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

Tenable Vulnerability Management 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.

tenable.io Dashboards Scans Reports Settings

New Scan / Advanced Network Scan
[← Back to Scan Templates](#)

Settings Credentials Compliance Plugins

BASIC ▼

- General
- Schedule
- Notifications
- Permissions

DISCOVERY ▶

ASSESSMENT ▶

REPORT ▶

ADVANCED ▶

Name: Thycotic - Windows

Description: |

Folder: My Scans

Scanner: Internal Network Scanner

Target Groups:

Targets: 172.1.2.3/24

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

tenable.io Dashboards Scans Reports Settings

Performance Options

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

Network timeout (in seconds): 5

Max simultaneous checks per host: 5

Max simultaneous hosts per scan: 100

Max number of concurrent TCP sessions per host:

Max number of concurrent TCP sessions per scan:

Debug Settings

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

Save Cancel