



Tenable Vulnerability Management and Thycotic Integration Guide

Last Revised: July 15, 2025



Table of Contents

Introduction	3
Integration Requirements	4
Integrate with Thycotic Secret Server	5
Configure Windows Credentials	5
Configure Linux Credentials	9
Troubleshooting	15



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.



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](#)

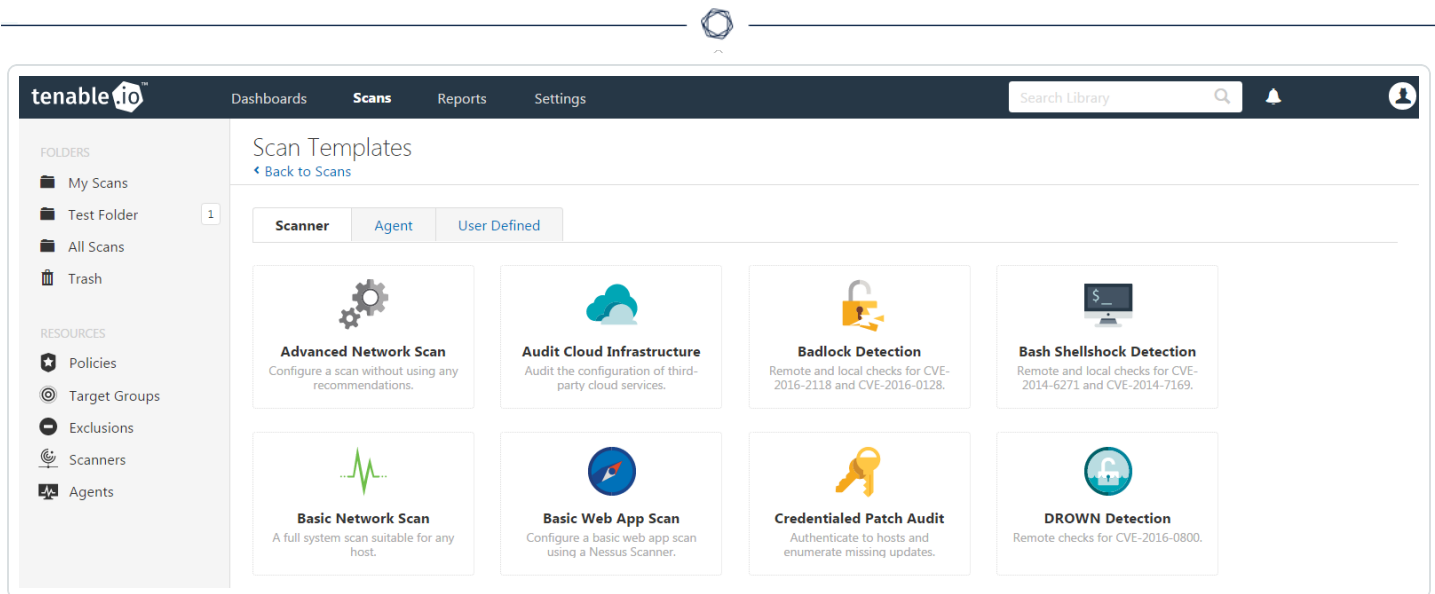
Configure Windows Credentials

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.

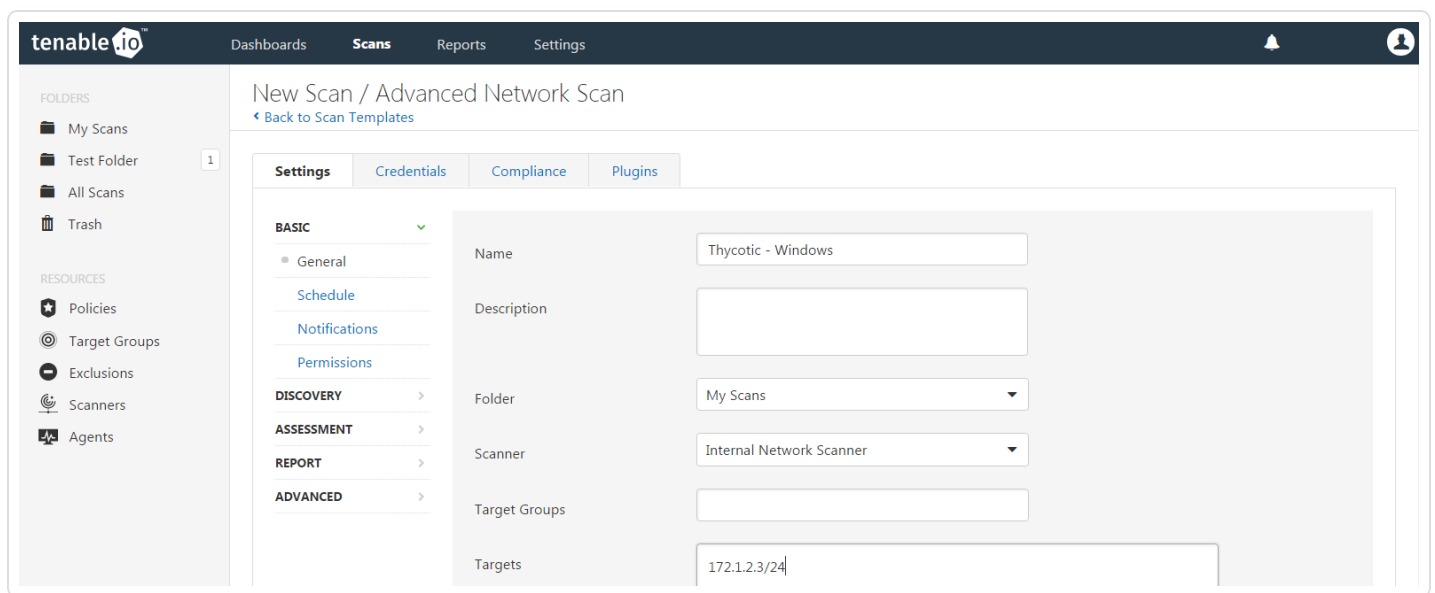
The screenshot shows the Tenable.io interface. The top navigation bar includes 'Dashboards', 'Scans', 'Reports', and 'Settings'. A search bar for 'Search Scans' is on the right. The left sidebar shows 'FOLDERS' (My Scans, Test Folder, All Scans, Trash) and 'RESOURCES' (Policies, Target Groups, Exclusions, Scanners, Agents). The main content area is titled 'My Scans' and contains a table of scans. The '+ New Scan' button is highlighted with a red box.

<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	Advanced Network Scan	On Demand	✓ 05/16/16	▶	✕
<input type="checkbox"/>	Host Discovery Scan	On Demand	✓ 05/03/16	▶	✕
<input type="checkbox"/>	Basic Network Scan	On Demand	✓ N/A	▶	✕

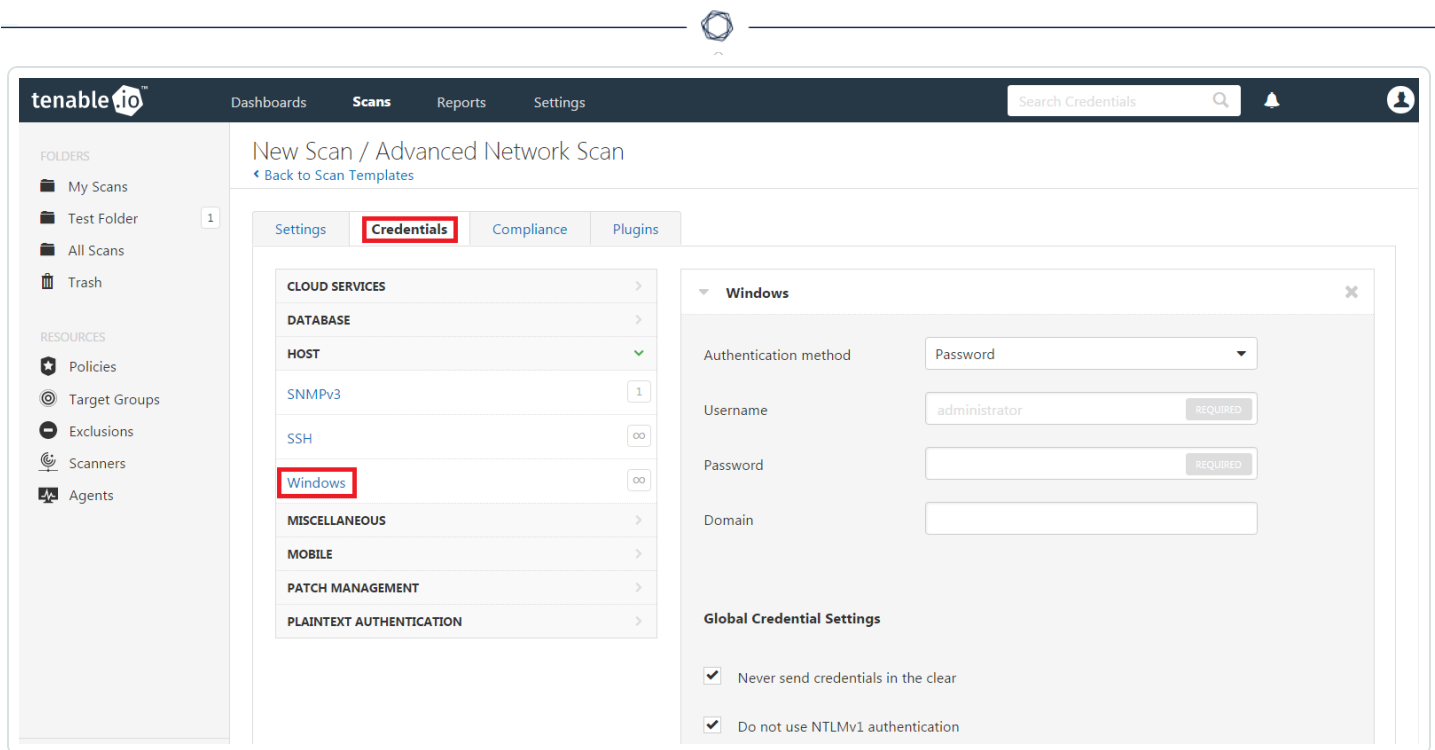
Select a "Scan Template" for the scan type required for your scan. For demonstration purposes, the "Advanced Network Scan" template will be used.



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.



tenable.io Dashboards Scans Reports Settings Search Credentials

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

Settings **Credentials** Compliance Plugins

CLOUD SERVICES >
 DATABASE >
 HOST >
 SNMPv3 1
 SSH ∞
Windows ∞
 MISCELLANEOUS >
 MOBILE >
 PATCH MANAGEMENT >
 PLAINTEXT AUTHENTICATION >

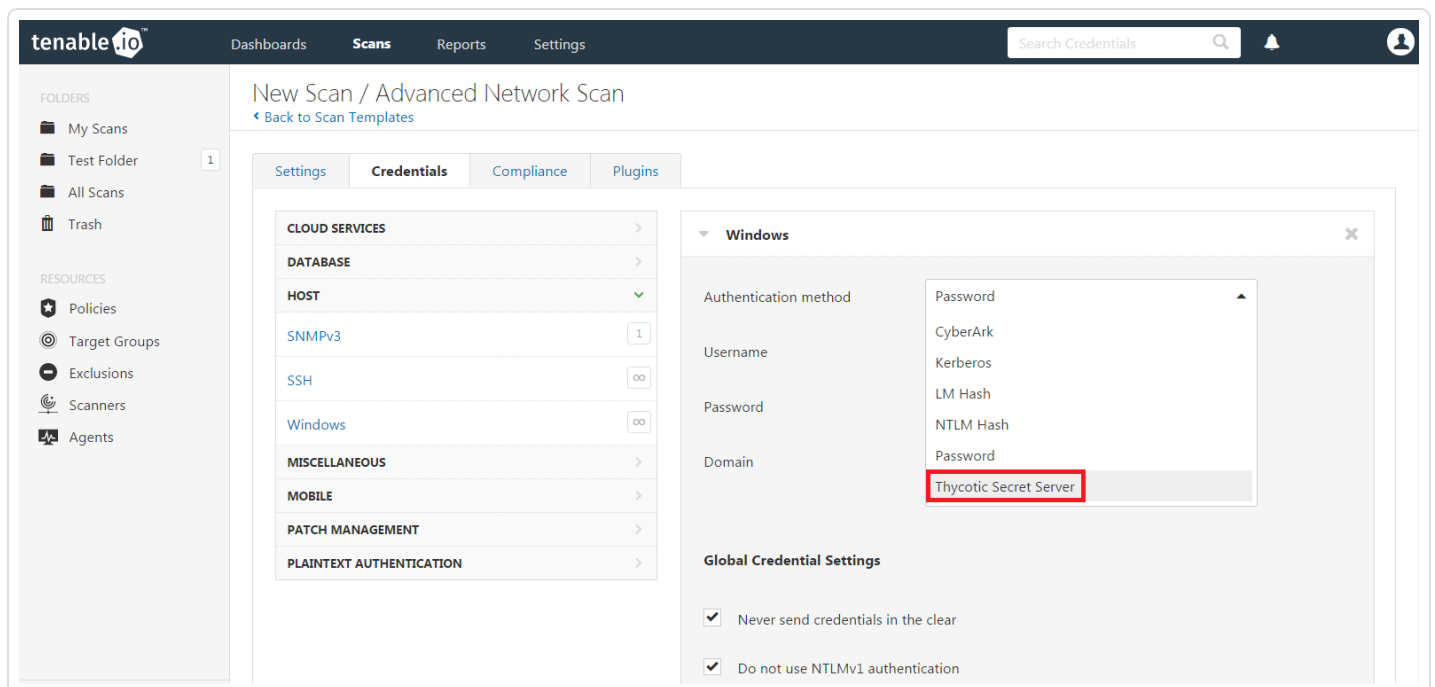
Windows

Authentication method Password
 Username administrator REQUIRED
 Password REQUIRED
 Domain

Global Credential Settings

☒ Never send credentials in the clear
☒ Do not use NTLMv1 authentication

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



tenable.io Dashboards Scans Reports Settings Search Credentials

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

Settings **Credentials** Compliance Plugins

CLOUD SERVICES >
 DATABASE >
 HOST >
 SNMPv3 1
 SSH ∞
 Windows ∞
 MISCELLANEOUS >
 MOBILE >
 PATCH MANAGEMENT >
 PLAINTEXT AUTHENTICATION >

Windows

Authentication method Password
 Username administrator
 Password
 Domain

Global Credential Settings

☒ Never send credentials in the clear
☒ Do not use NTLMv1 authentication

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.

The screenshot shows the Tenable.io 'New Scan / Advanced Network Scan' configuration page. The 'Credentials' tab is selected, and a 'Windows' configuration window is open. The window contains the following fields:

- Authentication method: Thycotic Secret Server (dropdown)
- Username: System_user (text input)
- Domain: ThycoticDomain (text input)
- Thycotic Secret Name: SecretName1 (text input)
- Thycotic Secret Server URL: https://<targetaddress>/SecretServer (text input)
- Thycotic Login Name: Thycotic_Login_Name (text input)
- Thycotic Password: [masked] (password input)
- Thycotic Organization (optional): (text input)

The left sidebar shows a navigation menu with 'FOLDERS' (My Scans, Test Folder, All Scans, Trash) and 'RESOURCES' (Policies, Target Groups, Exclusions, Scanners, Agents).

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	This is an optional value set if the domain value is set for the



(optional)	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 Tenable.io interface. The top navigation bar includes 'Dashboards', 'Scans', 'Reports', and 'Settings'. A search bar for 'Search Credentials' is on the right. The left sidebar shows 'FOLDERS' with 'My Scans', 'All Scans', and 'Trash', and 'RESOURCES' with 'Policies', 'Asset Lists', 'Exclusions', 'Scanners', and 'Agents'. The main area is titled 'My Scans' and contains a table with columns: Name, Schedule, and Last Modified. A single scan is listed: 'Thycotic - Windows' with a schedule of 'On Demand' and 'Last Modified' as 'N/A'. A red box highlights a play button icon in the 'Last Modified' column, which is the 'Launch' button.

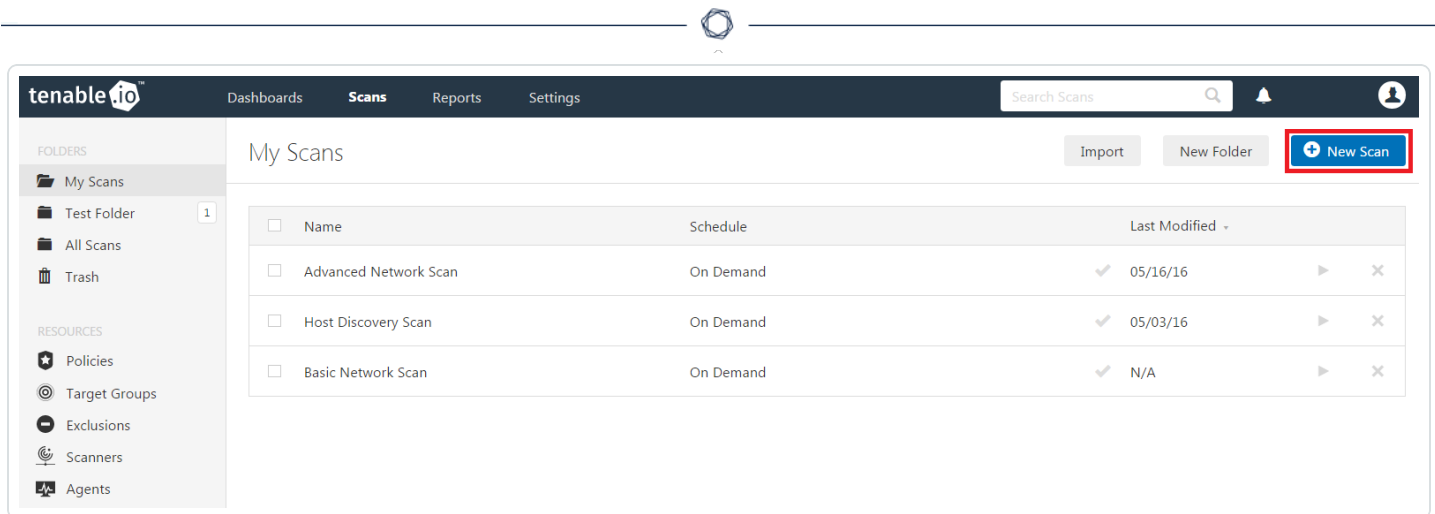
Once the scan has completed, select the completed scan and look for “Plugin ID 10394” (shown below), which validates that authentication was successful. If the authentication is not successful, refer to the [Troubleshooting](#) section of this document.

The screenshot shows the Tenable.io interface for a specific host. The top navigation bar is the same. The left sidebar is the same. The main area is titled '192.168.1.106' with a link 'Back to Windows 10'. There are 'Configure' and 'Export' buttons. Below this is a 'Vulnerabilities' section with a count of 1. A table lists the vulnerability: 'Microsoft Windows SMB Log In Possible' with a severity of 'High' (indicated by a blue dot) and a count of 1. To the right of the table is a 'Host Details' section with the following information: IP: 192.168.1.106, MAC: 0c8b: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.

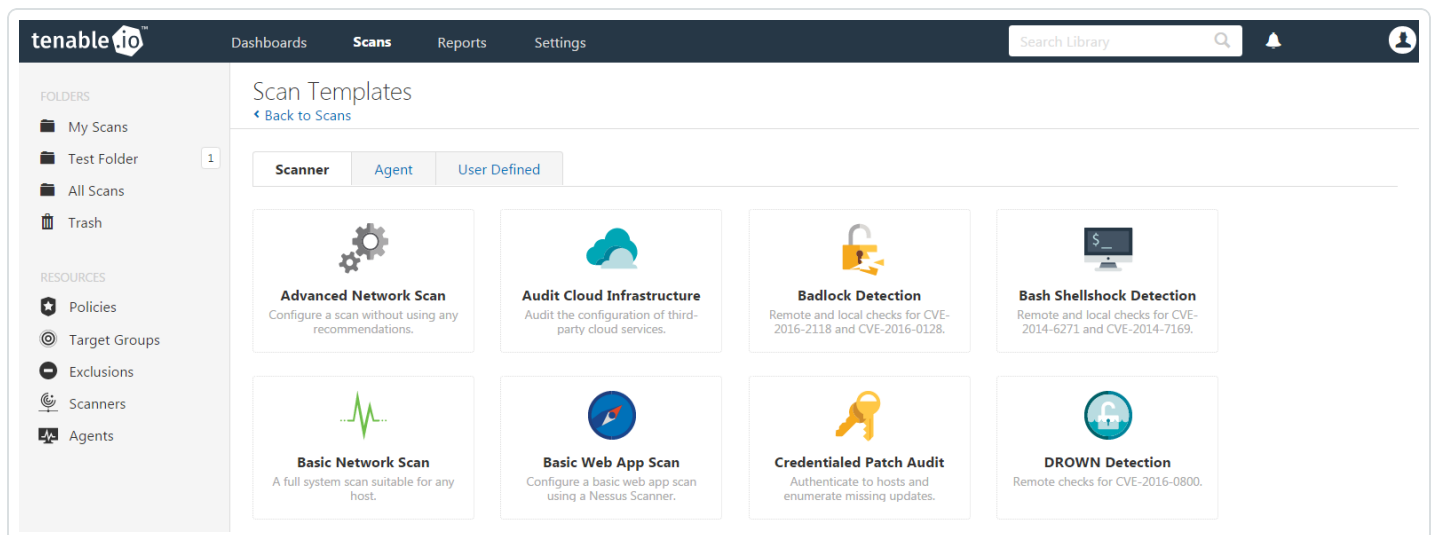


The screenshot shows the Tenable.io interface. The top navigation bar includes 'Dashboards', 'Scans', 'Reports', and 'Settings'. A search bar labeled 'Search Scans' is on the right. The left sidebar shows 'FOLDERS' (My Scans, Test Folder, All Scans, Trash) and 'RESOURCES' (Policies, Target Groups, Exclusions, Scanners, Agents). The main content area is titled 'My Scans' and contains a table of scans:

<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	Advanced Network Scan	On Demand	✓ 05/16/16	▶	✕
<input type="checkbox"/>	Host Discovery Scan	On Demand	✓ 05/03/16	▶	✕
<input type="checkbox"/>	Basic Network Scan	On Demand	✓ N/A	▶	✕

Buttons for 'Import', 'New Folder', and 'New Scan' (highlighted with a red box) are located at the top right of the main content area.

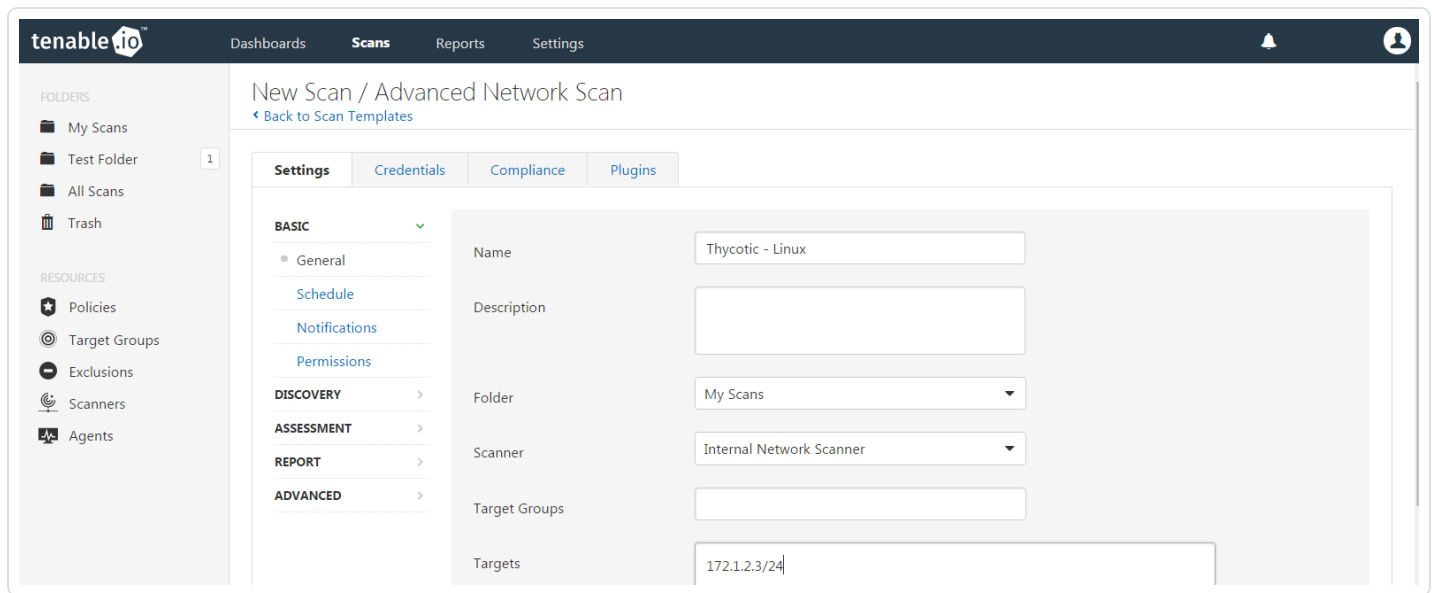
Select a “Scan Template” for the scan type required for your scan. For demonstration purposes, the “Advanced Scan” template will be used.



The screenshot shows the Tenable.io 'Scan Templates' page. The top navigation bar is the same as the previous screenshot. The left sidebar is also the same. The main content area is titled 'Scan Templates' and has a 'Back to Scans' link. Below the title are tabs for 'Scanner', 'Agent', and 'User Defined'. The 'Scanner' tab is selected, displaying a grid of scan templates:

- Advanced Network 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.
- Basic Web App Scan**: Configure a basic web app scan using a Nessus Scanner.
- Credentialed Patch Audit**: Authenticate to hosts and enumerate missing updates.
- DROWN Detection**: Remote checks for CVE-2016-0800.

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**.



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 - Linux

Description:

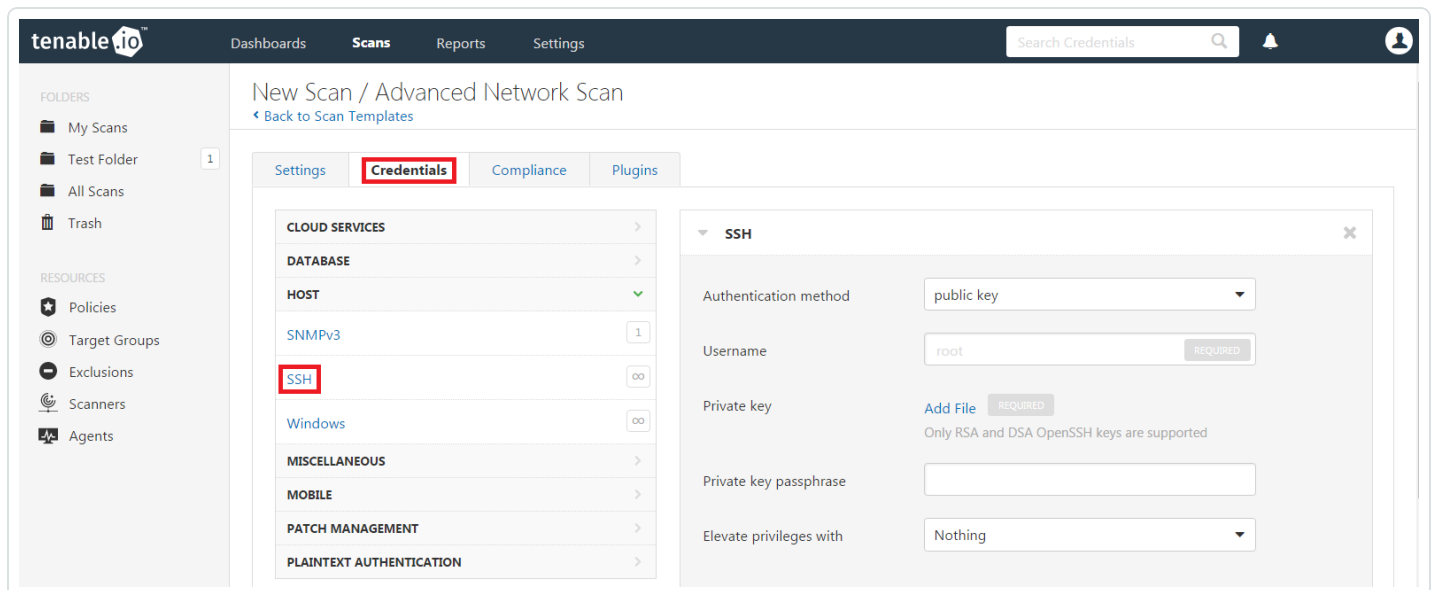
Folder: My Scans

Scanner: Internal Network Scanner

Target Groups:

Targets: 172.1.2.3/24

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



tenable.io Dashboards **Scans** Reports Settings

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

Settings **Credentials** Compliance Plugins

CLOUD SERVICES >

DATABASE >

HOST ✓

SNMPv3 1

SSH ∞

Windows ∞

MISCELLANEOUS >

MOBILE >

PATCH MANAGEMENT >

PLAINTEXT AUTHENTICATION >

SSH

Authentication method: public key

Username: root REQUIRED

Private key: Add File REQUIRED
 Only RSA and DSA OpenSSH keys are supported

Private key passphrase:

Elevate privileges with: Nothing

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

The screenshot shows the Tenable.io 'New Scan / Advanced Network Scan' configuration page. The left sidebar contains 'FOLDERS' (My Scans, Test Folder, All Scans, Trash) and 'RESOURCES' (Policies, Target Groups, Exclusions, Scanners, Agents). The main content area has tabs for 'Settings', 'Credentials', 'Compliance', and 'Plugins'. The 'SSH' tab is active, displaying a configuration form. The 'Authentication method' dropdown is open, showing options: 'public key', 'certificate', 'CyberArk', 'Kerberos', 'password', 'public key', and 'Thycotic Secret Server' (highlighted with a red box). Other fields include 'Username', 'Private key', 'Private key passphrase', and 'Elevate privileges with' (set to 'Nothing').

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 Tenable.io 'New Scan / Advanced Network Scan' configuration page with the 'SSH' tab selected. The 'Authentication method' is set to 'Thycotic Secret Server'. The form fields are as follows: 'Username' (System_user), 'Thycotic Secret Name' (SecretName), 'Thycotic Secret Server URL' (https://<targetaddress>/SecretServer), 'Thycotic Login Name' (Thycotic_Login_Name), 'Thycotic Password' (masked with dots), and 'Thycotic Organization (optional)' (empty).

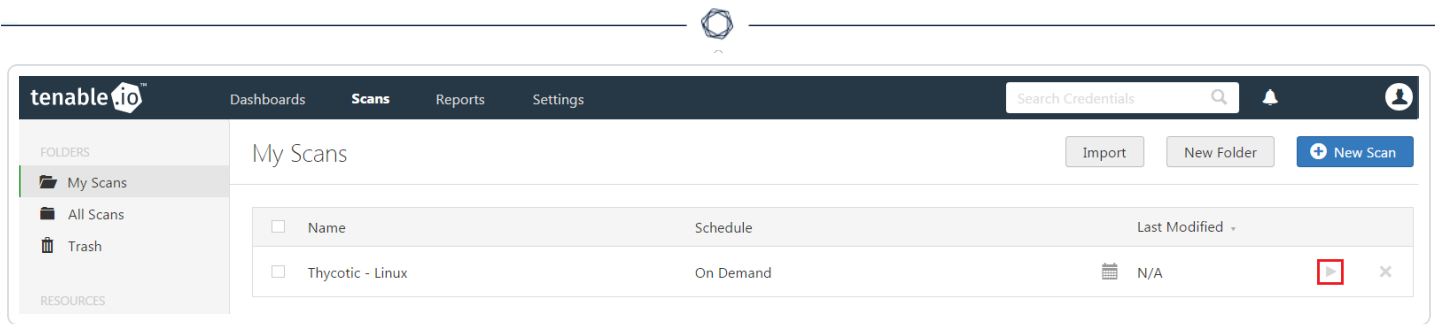
Table 2 - Thycotic SSH Credentials

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 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 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	<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>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.

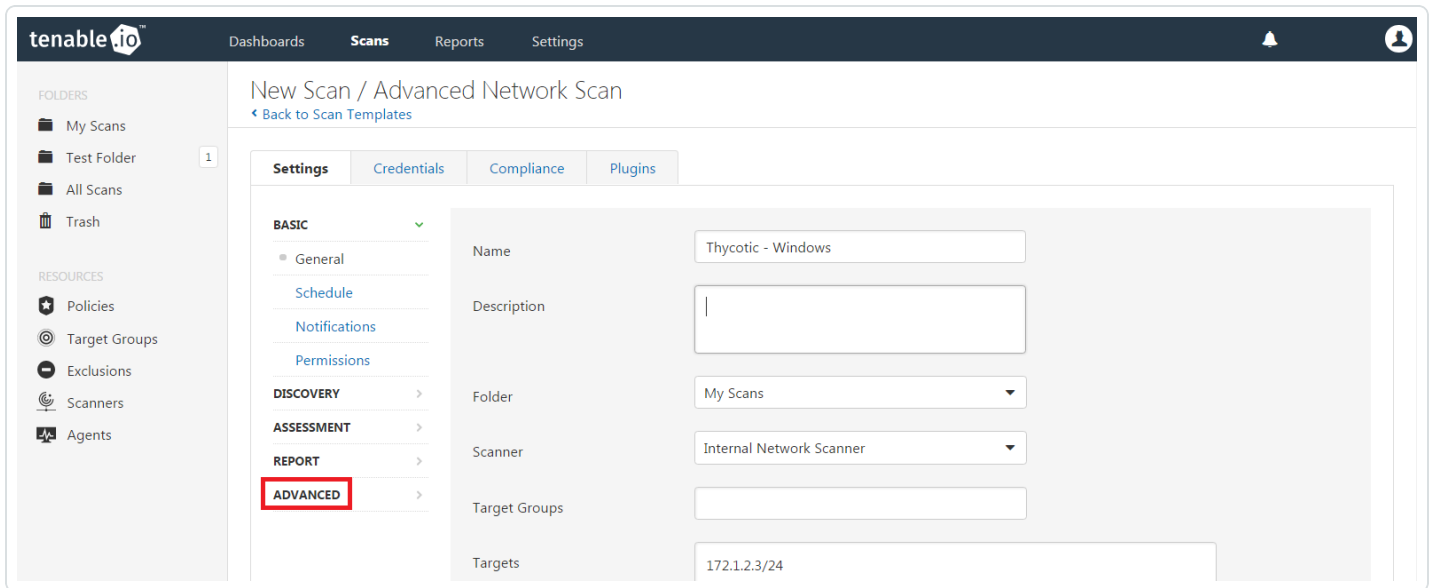


Once the scan has completed, select the completed scan and look for “Plugin ID 12634”, which validates that authentication was successful. If the authentication is not successful, refer to the “Troubleshooting” section of this document.

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

FOLDERS

- My Scans
- Test Folder 1
- All Scans
- Trash

RESOURCES

- Policies
- Target Groups
- Exclusions
- Scanners
- Agents

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

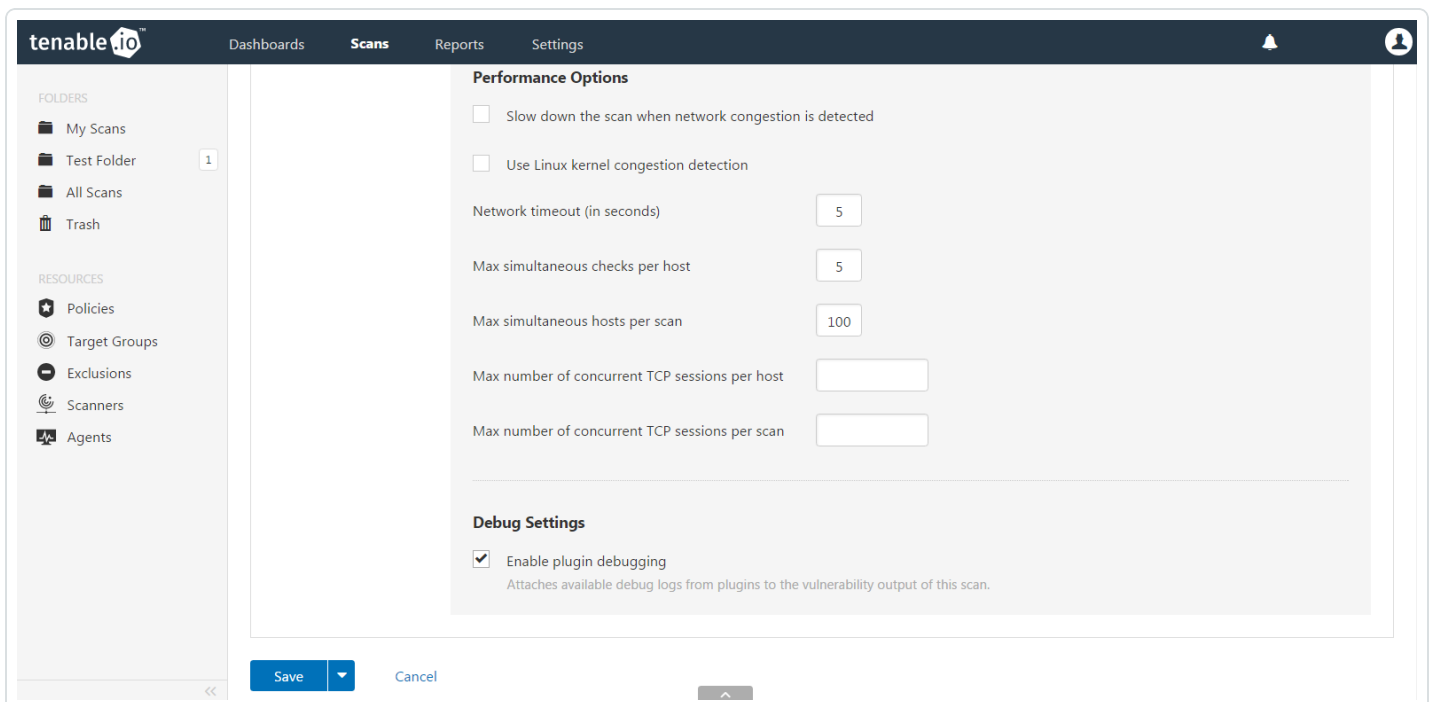
Folder My Scans

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

FOLDERS

- My Scans
- Test Folder 1
- All Scans
- Trash

RESOURCES

- Policies
- Target Groups
- Exclusions
- Scanners
- Agents

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