Tenable Vulnerability Management and Thycotic Integration Guide

Last Revised: April 09, 2025

Copyright © 2025 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

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

- Ø

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 Sever 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.

tenable .io	Dashboards Scans Reports Settings		Search Scans Q 🌲
	My Scans		Import New Folder 🗲 New Scan
🖆 My Scans	-		
Test Folder 1	Name	Schedule	Last Modified +
All Scans			
🛍 Trash	Advanced Network Scan	On Demand	✓ 05/16/16
	Host Discovery Scan	On Demand	✓ 05/03/16 ► ×
Policies	Basic Network Scan	On Demand	✓ N/A ► ×
Target Groups			
Exclusions			
Scanners			
🙅 Agents			

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**.

tenable		Dashboards	Scans Rej	ports Settings			٨	2
FOLDERS My Scans		New Scan Scan T	/ Advance ^{Templates}	ed Network S	can			
Test Folder	1	Settings	Credentials	Compliance	Plugins			
All Scans		BASIC	~					
		 General 		Name		Thycotic - Windows		
RESOURCES		Schedule	1	Description				
Target Groups		Notificati	ions	Description				
Exclusions		Permissio	ons					
Scanners		DISCOVERY	>	Folder		My Scans 👻		
Agents		ASSESSMENT	>			Internal Network Scappor		
		REPORT	>	Scanner				
		ADVANCED	>	Target Groups				
				Targets		172.1.2.3/24		

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	Q,	A	2		
FOLDERS My Scans Test Folder 1	New Sc Sections	New Scan / Advanced Network Scan < Back to Scan Templates										
All ScansTrash	CLOUD	SERVICES		mplance		 Windows 			×			
RESOURCES Policies	HOST	ASE			> •	Authentication method	Password	-				
 Target Groups Exclusions Scanners 	SSH	SSH			Username Password		REQUIRED					
Agents	MISCE	MISCELLANEOUS MOBILE			>	Domain						
	PATCH	MANAGEMENT	ITION			Global Credential Settings						
						 Never send credentials in the Do not use NTLMv1 authen 	ne clear ttication					

 \sim

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

tenable 🚺	Dashboards Sca	ans Report	s Settings			Search Credentials	۹. 👃	2	
FOLDERS My Scans	New Scan /	Advanced	Network So	can					
Test FolderAll Scans	Settings	Credentials	Compliance	Plugins					
🛍 Trash	CLOUD SERVIC	ES			▼ Windows			×	
RESOURCES	DATABASE			> ~	Authentication method	Password	•		
Target Groups	Policies Target Groups SNMPv3				Username	CyberArk Kerberos			
 Exclusions Scanners 	SSH	SSH		00	Password	LM Hash			
Agents	MISCELLANEO	US		>	NTLM Hash Domain Password				
	MOBILE				Thycotic Secret Server				
	PATCH MANAG	GEMENT							
	PLAINTEXT AU	ITHENTICATION			Global Credential Settings				
					✓ Never send credentials in th	ne clear			
					Do not use NTLMv1 authen	tication			

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.

								- Ø					
tenable .io	Das	shboards	Scans	Reports	Settings	;			Search Credentials Q			2	
FOLDERS		New Scar [•] Back to Scan	n / Advai _{Templates}	nced I	Network S	can							
Test FolderAll Scans		Settings	Credenti	als	Compliance	Plugin	ns						
🛍 Trash		CLOUD SE	RVICES					- Windows			×		
RESOURCES Policies		DATABAS	E			> ~		Authentication method	Thycotic Secret Server	•			
Target GroupsExclusions			SNMPv3						Username	System_user			
Scanners				Windows	Windows			0	~	Domain	ThycoticDomain		
The right of		MISCELLA	NEOUS					Thycotic Secret Name	SecretName1				
		MOBILE PATCH MANAGEMENT						Thycotic Secret Server URL	https:// <targetaddress>/SecretServer</targetaddress>				
		PLAINTEX	T AUTHENTICA	TION				Thycotic Login Name	Thycotic_Login_Name				
								Thycotic Password					
	<							Thycotic Organization (optional)					

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.

tenable 🕡	Dashboards Scans Reports	Settings	Search Credentials Q	2
	My Scans		Import New Folder	+ New Scan
🖆 My Scans				
All Scans	Name	Schedule	Last Modified 🗸	
III Hash	Thycotic - Windows	On Demand	m N/A	► ×

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 <u>Troubleshooting</u> section of this document.

tenable	Dashboards Scans Reports Settings		Search C	Credentials Q	3
FOLDERS	192.168.1.106			Configure	oort 🔻
All ScansTrash	Vulnerabilities 1				
	Sev - Name	Family 👻	Count 🔺	Host Details	Ť
Policies	 Microsoft Windows SMB Log In Possible 	Windows	1 I	IP: 192.168.1.106	
🔳 Asset Lists				MAC: 0c:8b:td:52:05:1c OS: Microsoft Windows 10 Home	
Exclusions			2	Start: January 3 at 10:44 AM	
Scanners			E	End: January 3 at 10:50 AM	
Agents			E	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	Da	ashboards Scans Reports Settings		Search Scans Q A
FOLDERS		My Scans		Import New Folder • New Scan
Test Folder All Scans	1	□ Name	Schedule	Last Modified +
🛍 Trash		Advanced Network Scan	On Demand	✓ 05/16/16
		Host Discovery Scan	On Demand	05/03/16 🕨 🗙
 Policies Target Groups 		Basic Network Scan	On Demand	✓ N/A ► ×
Exclusions				
🖤 Scanners				

n

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**.

					~		
tenable 🔞	Dashboards	Scans Rep	oorts Settings			Å	2
FOLDERS My Scans	New Scan	n / Advance Templates	ed Network S	can			
Test Folder 1	Settings	Credentials	Compliance	Plugins			
Trash	BASIC	~			Thursday Linux		
	 General 		Name		Thýcotic - Linux		
Policies	Schedule	e	Description				
Target Groups	Notificat	tions					
Exclusions	Permissi	ons					
Scanners	DISCOVERY	>	Folder		My Scans 👻		
Agents	ASSESSMENT	r >					
	REPORT	>	Scanner		Internal Network Scanner		
	ADVANCED	>	Target Groups				
			Targets		172.1.2.3/24		

0 -

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

tenable , io	Dashboards Sca	ans Reports	Settings		Search Credentials	
FOLDERS My Scans Test Folder All Scans	New Scan /	Advanced Ne nplates Credentials Co	mpliance Plugins			
🛍 Trash	CLOUD SERVIC	ES		▼ SSH	×	
	DATABASE	DATABASE				
Policies	HOST		*	Authentication method	public key 🔹	
Target Groups	SNMPv3		1	Username root		
Exclusions	SSH		\sim			
🗳 Scanners 🗛 Agents	Windows	Windows		Private key	Add File REQUIRED Only RSA and DSA OpenSSH keys are supported	
	MISCELLANEO	US				
	MOBILE	MOBILE		Private key passphrase		
	PATCH MANA	GEMENT		Elevate privileges with	Nothing	
	PLAINTEXT AU	JTHENTICATION				

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

enable 🥡 🛛 🛛	ashboards Scans Repo	rts Settings			Search Credentials	۹ 🔺				
OLDERS My Scans	New Scan / Advanced Network Scan < Back to Scan Templates									
Test Folder 1	Settings Credentials	Compliance	Plugins							
Trash	CLOUD SERVICES			▼ SSH			×			
	DATABASE									
Policies	HOST		~	Authentication method Username	public key					
Target Groups	SNMPv3		1		certificate					
Exclusions	SSH		00		CyberArk					
Scanners				Private key	Kerberos					
Agents	Windows				password					
	MISCELLANEOUS			Private key passphrase						
	MOBILE			i mute key pusspinuse	Inycotic Secret Server					
	PATCH MANAGEMENT			Elevate privileges with	Nothing	-				
	PLAINTEXT AUTHENTICATION									

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.

tenable io		Dashboards	Scans	Reports	Settings			Search Credentials Q	A	2	
FOLDERS		New Scan / Advanced Network Scan ^c Back to Scan Templates									
Test FolderAll Scans	1	Settings Credentials Compliance Plugins									
🛍 Trash		CLOUD SERVICES				▼ SSH	X	£			
RESOURCES		DATAE	DATABASE HOST			>	Authentication method	Thycotic Secret Server	•		
 Foncies Target Groups 		SNMP	v3			1	Username	System_user			
 Exclusions Scanners 		SSH	SSH Windows MISCELLANEOUS			©	Thycotic Secret Name	SecretName			
🛧 Agents		MISCE					Thycotic Secret Server URL	https:// <targetaddress>/SecretServer</targetaddress>			
		MOBILE PATCH MANAGEMENT					Thycotic Login Name	Thycotic_Login_Name			
		PLAIN	PLAINTEXT AUTHENTICATION				Thycotic Password	••••••			
							Thycotic Organization (optional)				

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	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 <u>Host</u> in the Tenable Vulnerability Management User Guide.

- Ø -

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

tenable , io	Dashboards Scans Reports Set	tings	Search Credentials Q 🔺 主
FOLDERS	My Scans		Import New Folder 😌 New Scan
All Scans Trash	Name	Schedule	Last Modified +
RESOURCES	Thycotic - Linux	On Demand	₩ N/A

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 🕡		Dashboards	Scans Rep	oorts Settings	5			٨	2													
FOLDERS My Scans Test Folder	1	New Scan / Advanced Network Scan < Back to Scan Templates Settings Credentials Compliance Plugins																				
 All Scans Trash 															BASIC	~						
RESOURCES												 General Schedule 		Name Description		Thycotic - Windows						
Target GroupsExclusions																Notificati Permissic	ons					
🗳 Scanners			DISCOVERY	>	Folder		My Scans															
		REPORT ADVANCED	>	Scanner Target Groups																		
				Targets		172.1.2.3/24																

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

tenable .io	Dashboard	ls Scans	Reports	Settings	•	2
FOLDERS My Scans Test Folder All Scans Trash RESOURCES Policies Target Groups Exclusions Scanners Agents	1		Perf Netw Max Max Max	Formance Options Slow down the scan when network congestion is detected Use Linux kernel congestion detection vork timeout (in seconds) 5 simultaneous checks per host 5 simultaneous hosts per scan 100 number of concurrent TCP sessions per host number of concurrent TCP sessions per scan		
	< Save	e 🔽 Car	Deb v	ug Settings Enable plugin debugging Attaches available debug logs from plugins to the vulnerability output of this scan.		