

Tenable and Delinea Integration Guide

Last Revised: February 26, 2024

Table of Contents

Welcome to Tenable for Delinea	3
Delinea Integrations	4
Database Integration	5
SSH Integration	7
Windows Integration	2

- Ø

Welcome to Tenable for Delinea

This document provides information and steps for integrating Tenable Vulnerability Management, Tenable Nessus, or Tenable Security Center with Delinea Privileged Access Management (PAM).

The Tenable® integration with Delinea delivers a comprehensive authenticated scanning solution that provides security teams better vulnerability insight in order to protect privileged accounts. This integration supports the storage of privileged credentials in Delinea 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.

For more information about each product integration, see *Delinea* in the <u>Tenable Nessus</u>, <u>Tenable</u> <u>Vulnerability Management</u>, and <u>Tenable Security Center</u> user guides.

Delinea Integrations

View one of the following options for Delinea integration steps:

Ø

- Database Integration
- <u>SSH Integration</u>
- <u>Windows Integration</u>

Database Integration

Tenable provides full database support for Delinea.

Requirements

- Tenable Vulnerability Management or Tenable Nessus account
- Delinea account

Required User Role: Standard, Scan Manager, or Administrator

To configure Tenable for Delinea database:

- 1. Log in to your Tenable user interface.
- 2. Click Scans.

The My Scans page appears.

3. Click + New Scan.

The Scan Templates page appears.

4. Select a scan template.

The scan configuration page appears.

- 5. In the Name box, type a name for the scan.
- 6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
- 7. (Optional) Add a description, folder location, scanner location, and specify target groups.
- 8. Click the Credentials tab.

The Credentials pane appears.

9. Click the Database option.

The **Database** options appear.

10. In the Database Type drop-down box, select Cassandra, Oracle, DB2, MongoDB, PostgreSQL, MySQL, SQL Server, or Sybase ASE.

11. In the Auth Type drop-down box, click Delinea Secret Server.

The Delinea Secret Server options appear.

12. Configure each option for the **Database** authentication.

Option	Description	Required
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled Secret Name on the Delinea server.	yes
Delinea Host	The Delinea Secret Server IP address or DNS address.	yes
Delinea Port	The port on which Delinea Secret Server listens.	yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, credentials are selected.	yes
Delinea Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API key	The API key provided by Delinea Secret Server.	yes
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL certificate	If enabled, verifies the SSL Certificate on the Delinea server.	no

0 -

13. Click Save.

SSH Integration

To configure Tenable with Delinea using SSH integration:

- 1. Log in to your Tenable user interface.
- 2. Click Scans.
- 3. Click + New Scan.

The My Scans page appears.

= 🔿 tenable.io Vulnerab	ility Management > Scans				Quick Actions 🧔 🔑 온
Scans					Create Scan
☐ Folders ⊕	Search	,			
Search ,0	NAME	SCHEDULE	LAST RUN 🗸	STATUS	
🗀 My Scans	NNM-540 User Scan	On Demand	N/A	Empty	
All Scans	central-region-assets User Scan	On Demand	N/A	Empty	
Trash 6	re-test2 User Scan	On Demand	N/A	Empty	
	re-test2 User Scan	On Demand	N/A	Empty	
	re-test2 User Scan	On Demand	N/A	Empty	
	re-test User Scan	On Demand	N/A	Empty	
	Test Shared	On Demand	N/A	Empty	
	re-test2 User Scan	On Demand	N/A	Empty	
	re-test2 User Scan	On Demand	N/A	Empty	
	re-test User Scan	On Demand	N/A	Empty	
	Temp_3 Shared	On Demand	N/A	Empty	

O

4. Select a scan template.

The Scan Templates page appears.

= 🔿 tenable.io Vulnerability Management > Scans > Select a Scan Ter	nplate		⊙Quick Actions 🧔 🦀 გ
Select a Scan Template			Î
Scanner Agent User Defined			
Search ,0 25 Results			
Vulnerability Scans (Common)			
Advanced Network Scan Configure a scan without using any recommendations.	Multiple - Masic Network Scan A full system scan suitable for any host.	Credentialed Patch Audit Authensicate to hosts and enumerate missing updates.	Host Discovery A simple scan to discover live hosts and open ports.
Perform an internal PCI DSS (11.2.1) vulnerability scan.	Legacy Web App Scan Legacy Web App Scan Scan for published and unknown web vulnerabilities using Nessus Scanner.	Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.	PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI.
Configuration Scans			
Audit Cloud Infrastructure Audit the configuration of third party cloud services.	MDM Config Audit Audt the configuration of mobile device managers.	Offline Config Audit Audit the configuration of network devices.	Policy Compliance Auditing Audit system configurations against a known baseline.
SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.			
Tactical Scans			
2020 Threat Landscape Retrospective (TLR) A scan to detect vulnerabilities featured in our End of Year report.	Active Directory Starter Scan Look for misconfigurations in Active Directory.	CHOST (glibc) Detection Local checks for CVE-2015-0235.	Intel AMT Security Bypass Remote and local checks for CVE-2017:5689.
Scan for malware on Windows and Unix systems.	PrintNightmare Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler	ProxyLogon : MS Exchange Bernote and local checks to ideact Exchange vulnerabilities targeted by HAFNIUM.	Ripple20 Remote Scan

The scan configuration page appears.

Basic		
General		
NAME		SCAN RESULTS
	REQUIRED	Show in dashboard
DESCRIPTION		FOLDER
		My Scans ~
SCANNER		TAGS
Auto-Select	~	Select
Requires scanner groups configured for scan routing (linked scanners only)		Select one or more tags to scan all assets that have any of the specified tags applied. To see a list of assets identified by the specified tags, click View
NETWORK		A5365.
Default	~	
TARGET GROUPS		
Select	۲	
TARGETS		
Example: 192.168.1.1-192.168.1.255, 192.168.2.0/24, host.domain.com		REQUIRED
UPLOAD TARGETS		
Adume		
Schedule		
Notifications		
EMAIL RECIPENT(S)		SMS REUPENIES
cxample. megexample.com, yougexample.com		Exempte: (302) 333-1212, 144 /70 0300 461

- 5. In the **Name** box, type a name for the scan.
- 6. In the Targets box, type an IP address, hostname, or range of IP addresses.
- 7. (Optional) Add a description, folder location, scanner location, and specify target groups.
- 8. Click the Credentials tab.

The Credentials options appear.

ate a Scan -	Advanced Network Scan	Select Credenti	al Type
35	Credentials	Search	,P 46 Cr
lasic		MANAGED CREDENTIALS	
sessment	Add Credentials	API GATEWAY	
eport		CLOUD SERVICES	
ials	All Added Credentials	DATABASE	
ce		HOST	
		MISCELLANEOUS	
		MOBILE	
		PATCH MANAGEMENT	

R

- 9. In the Select a Credential menu, select the Host drop-down.
- 10. Select SSH.

The **Delinea** field options appear.

11. Configure each field for **SSH** authentication.

Option	Description	Required
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, Credentials is selected.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the API Key	yes

	Ø	
	authentication method is selected.	
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled Secret Name on the Delinea server.	yes
Delinea Host	The Delinea Secret Server host to pull the secrets from.	yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	yes
Use Private Key	If enabled, uses key-based authentication for SSH connections instead of password authentication.	no
Checkout Duration	The duration Tenable should check out the password from Delinea. Duration time is in hours and should be longer than the scan time.	yes
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL Certificate	If enabled, verifies the SSL Certificate on the Delinea server.	no
Elevate privileges with	The privilege escalation method you want to use to increase users' 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.	no
Custom password prompt	Some devices are configured to prompt for a password with a non-standard string (for example, "secret-passcode"). This setting allows recognition of these prompts. Leave this blank for most standard password prompts.	no

	^	
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list.	no
	Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use Targets To Prioritize Credentials , you configure the scan to use the successful credential first, which allows the scan to access the target faster.	

- 0

12. Click Save.

Windows Integration

To configure Tenable with Delinea using Windows integration:

- 1. Log in to Tenable Vulnerability Management.
- 2. In the upper-left corner, click the \equiv button.

The left navigation plane appears.

3. In the left navigation plane, click **Settings**.

The **Settings** page appears.

4. Click the Credentials widget.

The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

5. Click the \oplus button next to the **Credentials** title.

The credential form plane appears.

6. In the Host section, click Windows.

The selected credential options appear.

7. In the Authentication Method drop-down, select Delinea.

The **Delinea** options appear.

8. Configure the **Delinea** credentials.

Option	Description	Required
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, Credentials is selected.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the API Key authentication method is selected.	yes
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled Secret Name on the Delinea server.	yes
Delinea Host	The Delinea Secret Server IP address for API requests.	yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Checkout Duration	The duration Tenable should check out the password from Delinea. Duration time is in hours and should be longer than the scan time.	yes
Use SSL	Enable if the Delinea Secret Server is configured to	no

O

	Õ	
	support SSL.	
Verify SSL Certificate	If enabled. verifies the SSL Certificate on the Delinea server.	no

9. Click Save.