

Tenable and Senhasegura Integration Guide

Last Revised: February 07, 2024

Table of Contents

Welcome to Tenable for Senhasegura	3
Senhasegura Integrations	4
Database Integration	5
SSH Integration	.10
Windows Integration	.15

- Ø

Welcome to Tenable for Senhasegura

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

Senhasegura is a privileged access management software solution that stores, manages, and monitors all credentials, such as passwords, SSH keys, and digital certificates in a secure digital vault. Using encryption mechanisms, the password vault offers users the ability to use only one password to access a series of credentials registered in the solution. Additionally, Senhasegura can be used to access all network resources through SSH and RDP protocols, storing all records of their use for audit and compliance analysis purposes. Its intelligence allows for real-time analysis of actions taken by users and alert generation to identify fraud or inappropriate action.

Senhasegura Integrations

View one of the following options for Senhasegura integration steps:

O

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

Database Integration

To configure database integration:

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

The My Scans page appears.

= ()tenable.io Vulnerabi	ility Management > Scans				🗢 Quick Actions 🧔 🥬 S
Scans					Create Scan
☐ Folders ⊕	Search	,P 29 Results			
Search ,P	□ 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	
C Trash 6	re-test2 User Scan	On Demand	N/A	Empty	
	re-test2 User Scan	On Demand	N/A	Empty	
	re-test2 UserScan	On Demand	N/A	Empty	
	re-test User Scan	On Demand	N/A	Empty	
	Test Shared	On Demand	N/A	Empty	
	re-test2 UserScan	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	

Ø

3. Click + New Scan.

The Select a Scan Template page appears.

			O Build's Lations 🖉 🥼 🔒
	mpiate		C Quick Actions 💝 💝 3
Select a Scan Template			
Scanner Agent User Defined			
Search ,0 25 Results			
Vulnerability Scans (Common)			
Advanced Network Scan Configure a scan without using any recommendations.		Credentialed Patch Audit Authencicate to hosts and enumerate missing updates.	Host Discovery A simple scan to discover live hosts and open ports.
Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan.	Conception Conceptin Conception Conception Conception Conception Conception C	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 Audit 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.	GHOST (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 Remote and local checks to detect Exchange vulnerabilities targeted by HARHUM.	Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the ne

4. Select a scan template. For demonstration, the Advanced Network Scan template is used.

O

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 Assets
NETWORK		
Default	~	
TARGET GROUPS		
Select	۲	
TARGETS		
Example: 192.168.1.1-192.168.1.255, 192.168.2.0/24, host.domain.com		REQUIRED
Add File		
Schedule		
Notifications		
EMAIL RECIPIENTIS)		SMS RECIPIENTIS)
Example: me@example.com, you@example.com		Example: (302) 555-1212, +44 770 0900 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.

≡ ()tenable.io vu	Inerability Management > Scans > Select a Scan Template > Create a Scan		Quick Actions 🧔 🤌 :
Create a Scan - /	Advanced Network Scan		
Settings Basic	Credentials		
Discovery Assessment Report	Add Credentials 🛞		
Advanced Credentials		All Added Credoritals	
Compliance Plugins			
			Save & Launch Save Cancel

R

The Credentials pane appears.

⊖tenable.io ∣v	Inerability Management + Scans - Select a Scan Template - Create a Scan		
eate a Scan -	Advanced Network Scan	Select Credential Type	э
ngs	Credentials	Search ,C 46 Cr	Ired
Basic Discovery		MANAGED CREDENTIALS	
port	Add Credentials 🛞	CLOUD SERVICES	
wanced		DATABASE	
tials		HOST	
nce		MISCELLANEOUS	
		MOBILE	
		PATCH MANAGEMENT	
		PLAINTEXT AUTHENTICATION	

9. Click the **Database** option.

The **Database** options appear.

ate a Scan - A	Advanced Network Scan			
ğs.	Credentials		Search	,0 46 Cred
iscovery			MANAGED CREDENTIALS	
sessment	Add Credentials 🛞		API GATEWAY	
ort anced			CLOUD SERVICES	
als		All Added Credentials	DATABASE	
e			HOST	
			MISCELLANEOUS	
			PATCH MANAGEMENT	
			PLAINTEXT ALITHENTICATION	

ð

10. From the **Database Type** drop-down, select **Oracle**.

≡ ()tenable.io v	Inerability Management > Scans > Soixct a Scan Template > Create a Scan		×
Create a Scan -	Advanced Network Scan	Select Credenti	al Type
Settings	Credentials	Search	,0 46 Credentials
Basic		MANAGED CREDENTIALS	
Assessment	Add Condensity (a)	API GATEWAY	
Report	Au Creanuas 🐨	CLOUD SERVICES	
Credentials	All Added Credentials	DATABASE	
Compliance		HOST	
Divelop		MISCELLANEOUS	
Plognis		MOBILE	
		PATCH MANAGEMENT	
		PLAINTEXT AUTHENTICATION	

11. From the Auth Type drop-down, select Senhasegura.

The Senhasegura field options appear.

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

Option	Description	Required
Senhasegura Host	The IP address or URL for the Senhasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Tenable uses 443.	yes
Senhasegura API Client ID	The Client ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Secret ID	The Secret ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura Credential ID or Identifier	The credential ID or identifier for the credential you are requesting to retrieve.	yes
Private Key File	e Key File The Private Key used to decrypt Required if y encrypted sensitive data from A2A. enabled enc	
	Note: You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, you must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Senhasegura.	sensitive data in A2A Application Authorizations.
HTTPS	This is enabled by default.	yes
Verify SSL Certificate	This is disabled by default.	no

- Ø -

13. Click Save.

SSH Integration

To configure SSH integration:

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

The My Scans page appears.

= 🔿 tenable.io Vulnerab	ility Management > Scans				ି Quick Actions 🧔 🦺 ଥ
Scans					⊕ Create Scan 🕺 Tools
☐ Folders ⊕	Search	,A 29 Results			
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	
C Remediation Scans 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.

= Otenable.io Vulnerability Management > Scans > Select a Scan Ter	nplate		S Quick Actions 🧔 🦺 8
Select a Scan Template			1
Scanner Agent User Defined			
Search ,0 25 Results			
Vulnerability Scans (Common)			
Advanced Network Scan Configure a scan without using any recommendations.		Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	Host Discovery A simple scan to discover live hosts and open ports.
Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan.	C 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 Audit 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 Reatured in our End of Year report.	Active Directory Starter Scan Look for misconfigurations in Active Directory.	GHOST (glibc) Detection Local checks for CVE-2015-0235.	Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.
Malware Scan Scan for malware on Windows and Unix systems.	PrintNightmare Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler	ProxyLogon : MS Exchange Remote and local checks to detect Exchange vulnerabilities targeted by HARNUM.	Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the ne

The scan configuration page appears.

Basic		
Ground		
General		SCAN DESI II TS
	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 Assets
NETWORK		
Default	~	
TARGET GROUPS		
Select	۲	
TARGETS		
Example: 192.168.1.1-192.168.1.255, 192.168.2.0/24, host.domain.com		REQUIRED
Add File		
Schedule		
Notifications		
EMAIL RECIPIENT(S)		SMS RECIPENT(S)
Example: megexample.com, yougexample.com		Example: (302) 333-1212, 444 770 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.

Contraction by Punchasting Withing punch is view is well is well in the point of the point	Oteratio in Lu		^		
r set	eate a Scan -	Jinerability Management > Scans > Sect a Scan Template > Create a Scan	Se	lect Credential	Туре
MADC OCCODENTS AND CONCENTS AND CONCENTS	ngs	Credentials		irch	,9 46 Crea
second part Ad Cadentals • Ad Cadentals • Cond Simulary of Cadentas • Cond Simulary of Cadentals •	asic iscovery		MA MA	NAGED CREDENTIALS	
ord Close Strekes anded Dataset inter- Not not Not N	sessment	Add Credentials	AP	GATEWAY	
ANA CONTRACTOR OF CONTRACTON OF CONTRACTOR O	port vanced		а.	JUD SERVICES	
re Not Miclaweous Model Mode Model Model M	als		All Added Gredentials DA	ABASE	
MCLUAROS MOLE RENTOT AUTOMICATION RAINOT AUTOMICATION	ce		HO	ST	
MOLE INCOLAMAGEMENT PAINEDTAURISTICATION			M	CELLANEOUS	
			M	BILE	
			PAL	CH MANAGEMENT	

ð

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

The Senhasegura field options appear.

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

Option	Description	Required
Senhasegura Host	The IP address or url for the Senhasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Tenable uses 443.	yes
Senhasegura API Client ID	The Client ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Secret ID	The Secret ID for the applicable Senhasegura A2A Application for	yes

Option	Description	Required
	Oauth 2.0 API authentication.	
Senhasegura Credential ID or Identifier	The credential ID or identifier for the credential the you are requesting to retrieve.	yes
Use SSH Key for Target Authentication	The user can select this option to retrieve the SSH Key to authenticate to the target if the configuration is applicable in Senhasegura.	Required if authenticating to target with SSH Key.
Private Key File	The private key used to decrypt encrypted sensitive data from A2A.	Required if you have enabled encryption
	Note: You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, you must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Senhasegura.	of sensitive data in A2A Application Authorizations.
Escalate Privileges with	Use the drop-down menu to select the privilege elevation method, or select Nothing to skip privilege elevation.	Required if you wish to escalate privileges.
	Note: Tenable supports multiple options for privilege escalation, including su, su+sudo and sudo. For example, if you select sudo, more fields for sudo user, Escalation Account Name, and Location of su and sudo (directory) are provided and can be completed to support authentication and privilege escalation through Senhasegura. The Escalation Account Name field is then required to complete	

- Ø

Option	Description	Required
	your privilege escalation.	
	Note: For more information about supported privilege escalation types and their accompanying fields, see the <u>Nessus User Guide</u> , the <u>Tenable</u> <u>Vulnerability Management User Guide</u> , or the <u>Tenable Security Center User Guide</u> .	
Escalation account credential ID or identifier	If the escalation account has a different username or password from the least privileged user, enter the credential ID or identifier for the escalation account credential here.	no
HTTPS	This is enabled by default.	yes
Verify SSL Certificate	This is disabled by default.	no

- Ø

12. Click Save.

Windows Integration

To configure Tenable with Senhasegura 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 Senhasegura.

The Senhasegura options appear.

8. Configure the **Senhasegura** credentials.

Option	Description	Required
Senhasegura Host	The IP address or URL for the Senhasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Tenable uses 443.	yes
Senhasegura API Client ID	The Client ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Secret ID	The Secret ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Domain	The domain to which the username belongs.	no
Senhasegura Credential ID or Identifier	The credential ID or identifier for the credential the you are requesting to retrieve.	yes
Private Key File	The Private Key used to decrypt encrypted sensitive data from A2A.	Required if you have enabled encryption of
	Note: You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, the user must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Senhasegura.	Application Authorizations.
HTTPS	This is enabled by default.	yes

Ø

Option	Description	Required
Verify SSL Certificate	This is disabled by default.	no

0

9. Click Save.