

Tenable and Senhasegura Integration Guide

Last Revised: July 14, 2023

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
- SSH Integration
- <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.

Folders Search Search Search Search NM4544 NM5544 NM5544 NM554 Miscans Control In Tran 6 Tran 6 Control In Control Control Control In Control	egion-assets User Scan User Scan	SCHEDULE On Demand On Demand On Demand	LAST RIM NUA NUA	status Empty Empty Empty
My Scans NNM-54 All Scans central-re Remediation Scans re-test2 Trash 6 re-test2	egion-assets User Scan User Scan	On Demand On Demand On Demand	N/A N/A	Empty Empty
All Scans central-re Remediation Scans re-test2 Trash 6 re-test2	egion-assets User Scan User Scan	On Demand On Demand	N/A N/A	Empty
Remediation Stans re-test2 re-test2	User Scan	On Demand	N/A	
Trash 6 re-test2				Empty
re-test2	User Scan	On Demand		
re-test2			N/A	Empty
	User Scan	On Demand	N/A	Empty
re-test l	User Scan	On Demand	N/A	Empty
 Test Sha 	ared	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

O

3. Click + New Scan.

The **Select a Scan Template** page appears.

lect a Scan Template			
nner Agent User Defined			
rch ,O 25 Results			
erability 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.
Perform an internal PCI DSS (11.2.1) vulnerability 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.
iguration 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.			
ical 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.
Malware Scan Scan for malware on Windows and Unix systems.	PrintNightmare Local checks to detect the PrintNightmare Vulnerability in Windows Print Socier	ProxyLogon : MS Exchange Remote and local checks to detect Exchange vulnerabilities traveleted by HARMUM.	Ripple20 Remote Scan NHM 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.

The scan configuration page appears.

Basic		
DdSIC		
General		
NAME		SCAN RESULTS
NV/RL	REQUIRED	Show in dashboard
DESCRIPTION		FOLDER
		My Scans V
		my stana .
SCANNER		TAGS
Auto-Select		IRUS Select
Requires scanner groups configured for scan routing (linked scanners only)	-	Leter on 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		Assets.
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		
Add File		
Schedule		
Schedule		
Notifications		
EMAIL RECIPIENT(S)		SMS RECIPIENT(S)
Example: me@example.com, you@example.com		Example: (302) 555-1212, +44 770 0900 461

 \bigcirc

- 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 vul	Inerability Management > Scans > Select a Scan Template > Create a Scan		ි Quick Actions 🧔 🦺 පි
Create a Scan - A	Advanced Network Scan		
Settings Basic	Credentials		
Discovery Assessment Report	Add Credentials 🛞		
Advanced Credentials		All Added Credentials	
Compliance Plugins			
			Save & Launch Save Cancel

 \bigcirc

The **Credentials** pane appears.

ate a sean	- Advanced Network Scan	Select Credential	Тур
35	Credentials	Search	<u>,</u> р 4
asic	Credentials	MANAGED CREDENTIALS	
covery iessment		YAL CALENNA,	
port	Add Credentials 🛞	CLOUD SERVICES	
anced		All Added Gredentials DMTMBASE	
als		HOST	
ce		MISCELLANEOUS	
		BLIBOM	
		PATCH MANAGEMENT	
		PLAINTERT AUTHENTICATION	

9. Click the **Database** option.

The **Database** options appear.

ate a Scan - I	Advanced Network Scan			ect Credentia	
gs	Credentials		Sear	rch	,오 46 Cred
iscovery			MAN	AGED CREDENTIALS	
sessment	Add Credentials 🛞			GATEWAY	
ort anced				UD SERVICES	
als		All Added Credentials		ABASE	
ie .			HOS		
				CELLANEOUS	
			MOR	SILE CH MANAGEMENT	

ð

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

⊖tenable.io v	Inerability Management > Scors > Select a Scan Template > Create a Scan				
eate a Scan -	dvanced Network Scan Select Crede				
ngs	Credentials	Search	,0 46 Creder		
Basic Discovery		MANAGED CREDENTIALS			
Assessment	Add Credentials 🛞	API GATEWAY			
eport dvanced		CLOUD SERVICES			
itials	All Added Credentais	DATABASE			
nce		HOST			
		MISCELLANEOUS			
		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 Sen- hasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Ten- able uses 443.	yes
Senhasegura API Cli- ent ID	The Client ID for the applicable Sen- hasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Secret ID	The Secret ID for the applicable Sen- hasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura Cre- dential ID or Identifier	The credential ID or identifier for the credential 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 Applic- ation Authorizations. If enabled, you must provide a private key file in the scan credentials. This can be down- loaded from the applicable A2A application in Senhasegura.	sensitive data in A2A Application Author- izations.
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.

ans					⊕ Create Scan 🛛 🕅 Tools
] Folders 🐵	Search	D 29 Results			
sarch ,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	
Remediation Scans	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.

lect a Scan Template			
nner Agent User Defined			
arch ,P 25 Results			
nerability Scans (Common)			
Advanced Network Scan Configure a scan without using any recommendations.	→ Basic Network Scan A full system scan suitable for any host.	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.	Conception with the second sec	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.
figuration 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.			
ical 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.
Malware Scan Scan for malware on Windows and Unix systems.	PrintNightmare Local checks to detect the PrintNightmare Vulnerability in	ProxyLogon : MS Exchange Remote and local checks to detect Exchange vulnerabilities	Ripple20 Remote Scan

The scan configuration page appears.

Basic		
DdSIC		
General		
NAME		SCAN RESULTS
NV/RL	REQUIRED	Show in dashboard
DESCRIPTION		FOLDER
		My Scans V
		my stana .
SCANNER		TAGS
Auto-Select		IRUS Select
Requires scanner groups configured for scan routing (linked scanners only)	-	Leter on 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		Assets.
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		
Add File		
Schedule		
Schedule		
Notifications		
EMAIL RECIPIENT(S)		SMS RECIPIENT(S)
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.

The Credentials options appear.

credentials Image: service and servi	credentials feach p evy MARCEO CREDENTIALS MARCEO CREDENTIALS and credentials Add Credentials Add Credentials add Add Credentials Conserved add Credentials Conserved Conserved add Credentials Add Credentials Conserved add Credentials Conserved Conserved add Credentials Conserved Conserved add Credentials Conserved		Inerability Management > Scans > Select a Scan Template > Create a Scan		Select Credential Type
redentials www.septement Ad Credentials Ad Credentials Add Credentials	Credentials MAACD CREDENTALS evy Ad Credentials @ Ad Credentials @ Ad Credentials @ add Credentials @ Ad Added Ordentials add Credentials @ Added Ordentials	ate a Scan -	Advanced Network Scan		Select credential type
ey and Co Celebrius and Celebr	ey and Credential and Credentia and Credential and Credential and Credential and Credential and	gs	Credentials		Search ,P 46 Cn
Add Credentials Add Credentials Add C	Add Credentials Add Credentials Add C	ilc covery			MANAGED CREDENTIALS
Code Strategy Constraints Code Strategy Code Strateg	Codo Structs Codo Structs Codo Structs DRAME Adatad Creations ROT HOT ROT Koll Landon ROT	sessment	Add Credentials		API GATEWAY
A Adadd Criefrain Danae Da Danae Danae Da Danae Danae Dana Danae Danae	A Additio Credentians AA Additio Credentians	port vanced			CLOUD SERVICES
MSCELAREOUS MODILE RATCH MANAGEMENT	MICELIAROUS MORLE PRIDI MARGARINT	ials		All Added Gredentials	DATABASE
MOBLE ROTH MANAGABENT	MOBLE PRICH MANAGEMENT	nce			HOST
PROMAMANT	HOTO HAMAGADOT				
PLAINED AUTHORITORION	PLAINTEXT AUTHORITICATION				

R

- 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 Sen- hasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Ten- able uses 443.	yes
Senhasegura API Cli- ent ID	The Client ID for the applicable Sen- hasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Secret ID	The Secret ID for the applicable Sen- hasegura A2A Application for Oauth	yes

Option	Description	Required
	2.0 API authentication.	
Senhasegura Cre- dential ID or Identifier	The credential ID or identifier for the credential the you are requesting to retrieve.	yes
Use SSH Key for Tar- get Authentication	The user can select this option to retrieve the SSH Key to authenticate to the target if configuration is applic- able in Senhasegura.	Required if authen- ticating 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	The Private Key used to decrypt encrypted sensitive data from A2A.	Required if you wish to escalate priv-
	Note: Tenable supports multiple options for privilege escalation, includ- ing 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 sup- port authentication and privilege escal- ation through Senhasegura. The Escalation Account Name field is then required to complete your privilege escalation.	ileges.

Ø

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

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 Sen- hasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Ten- able uses 443.	yes
Senhasegura API Cli- ent ID	The Client ID for the applicable Sen- hasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Secret ID	The Secret ID for the applicable Sen- hasegura A2A Application for Oauth 2.0 API authentication.	yes
Domain	The domain to which the username belongs.	no
Senhasegura Cre- dential ID or Identifier	The credential ID or identifier for the credential the you are request- ing 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 Applic- ation 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.	sensitive data in A2A Application Author- izations.
HTTPS	This is enabled by default.	yes

Ø

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

 \cap

9. Click Save.