Tenable and Senhasegura Integration Guide

Last Revised: July 14, 2023

Table of Contents

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:

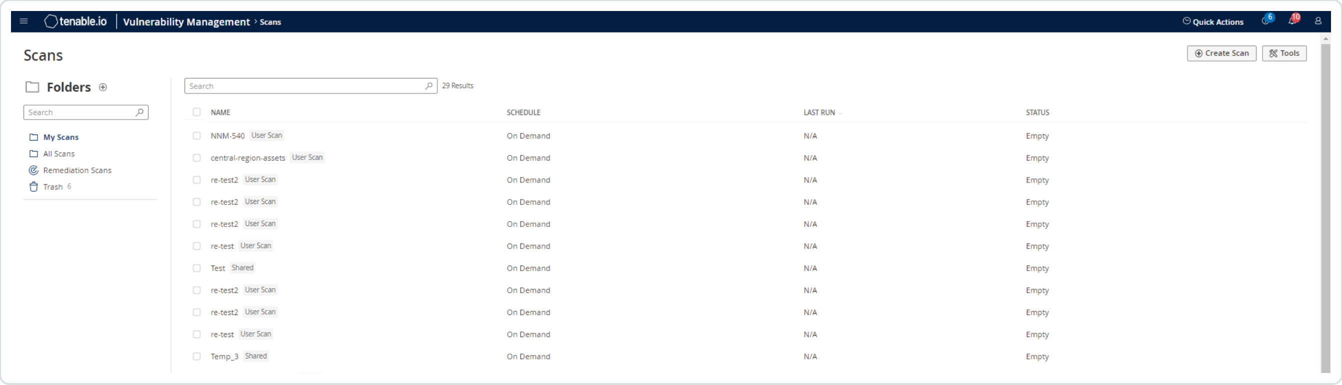
- Database Integration
- SSH Integration
- Windows Integration

Database Integration

To configure database integration:

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

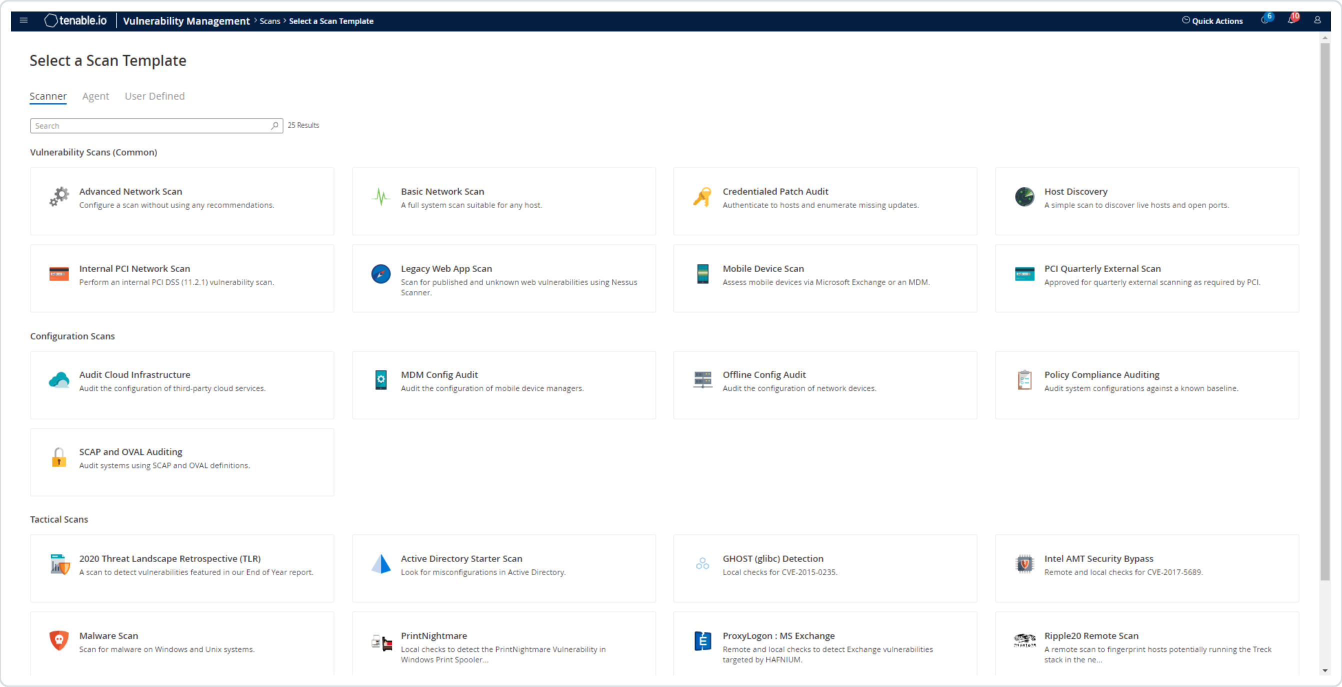
   The **My Scans** page appears.



NAME	SCHEDULE	LAST RUN	STATUS
NNM-540 User Scan	On Demand	N/A	Empty
central-region-assets 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-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

3. Click **+ New Scan.**

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



Vulnerability 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.

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 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.

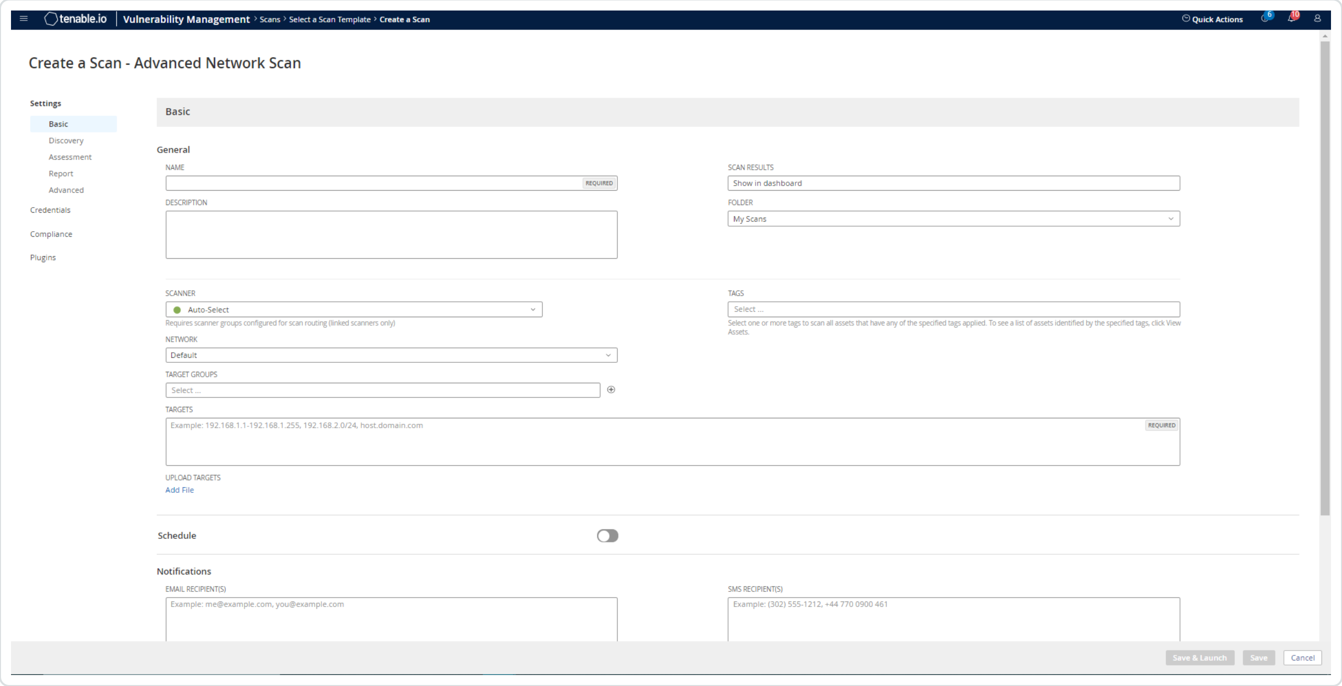
PrintNightmare
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler...

ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

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.

The scan configuration page appears.



Create a Scan - Advanced Network Scan

Basic

General

NAME: REQUIRED

DESCRIPTION:

SCAN RESULTS: Show in dashboard

FOLDER: My Scans

SCANNER: Auto-Select

Requires scanner groups configured for scan routing (linked scanners only)

TAGS: Select ...

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 ...

TARGETS: Example: 192.168.1.1-192.168.1.255, 192.168.2.0/24, host.domain.com REQUIRED

UPLOAD TARGETS: Add File

Schedule

Notifications

EMAIL RECIPIENT(S): Example: me@example.com, you@example.com

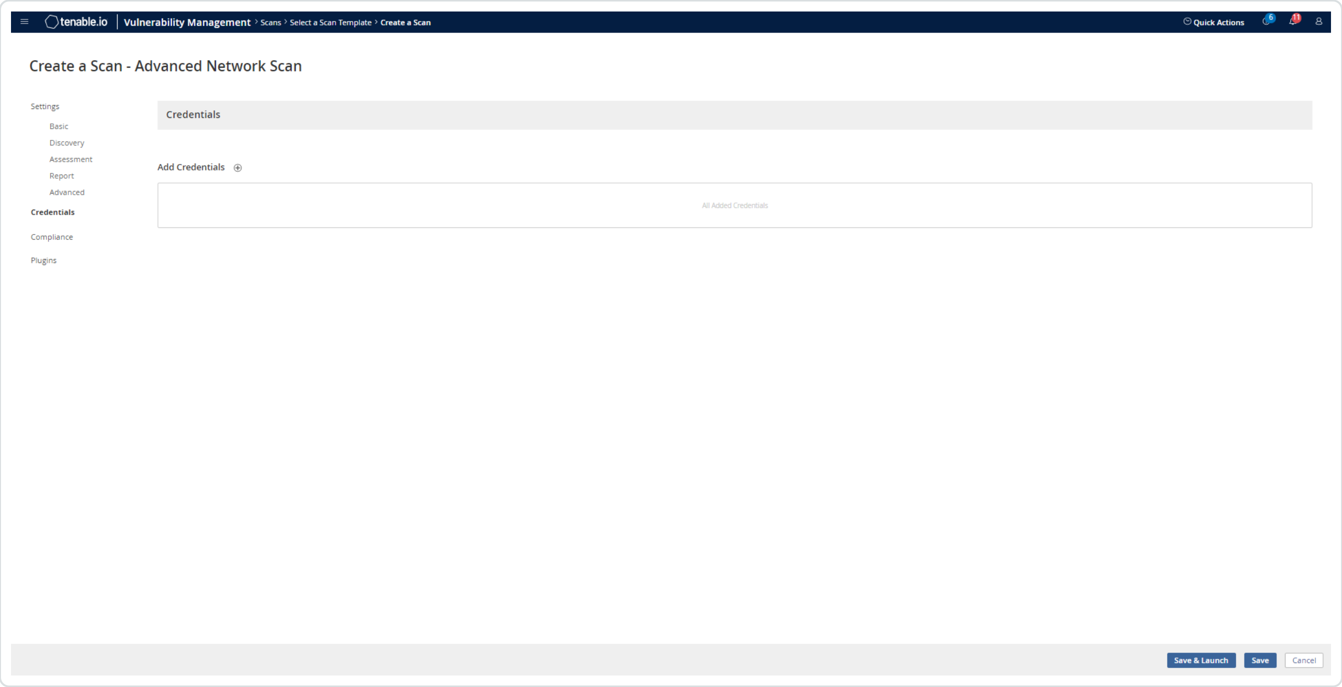
SMS RECIPIENT(S): Example: (302) 555-1212, +44 770 0900 461

5. In the **Name** box, type a name for the scan.

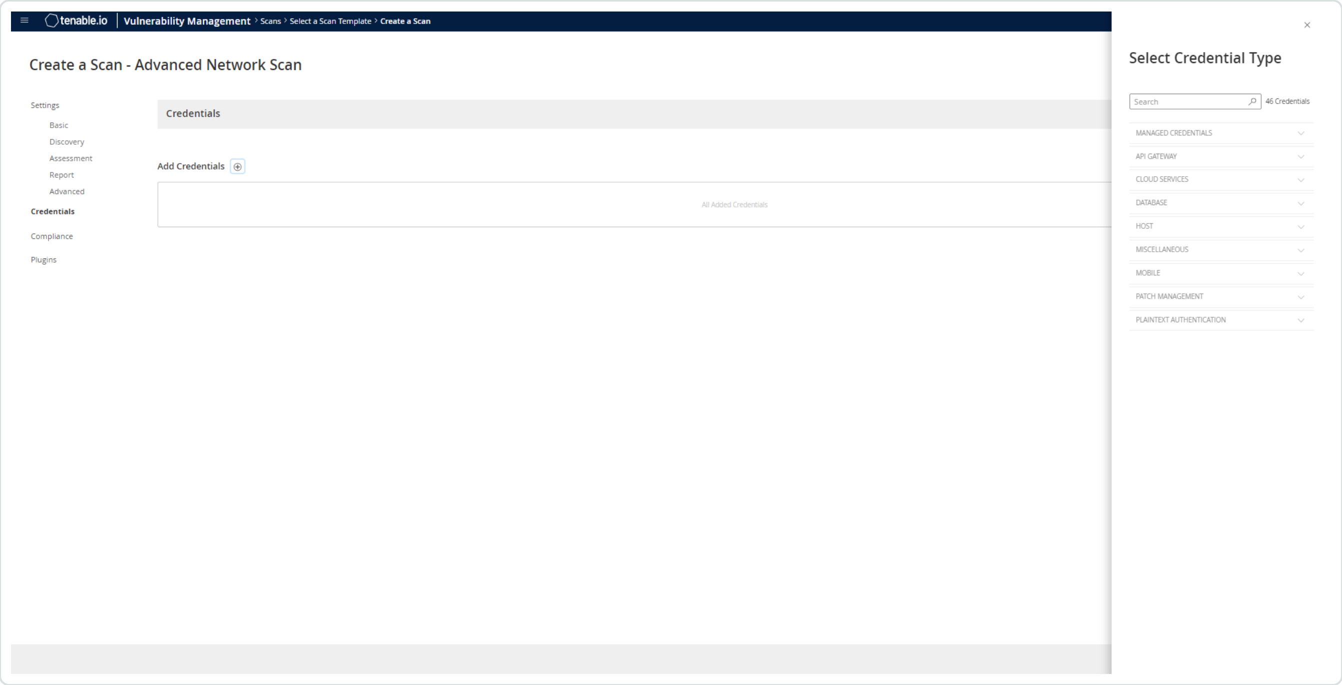
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.

7. (Optional) Add a description, folder location, scanner location, and specify target groups.

8. Click the **Credentials** tab.

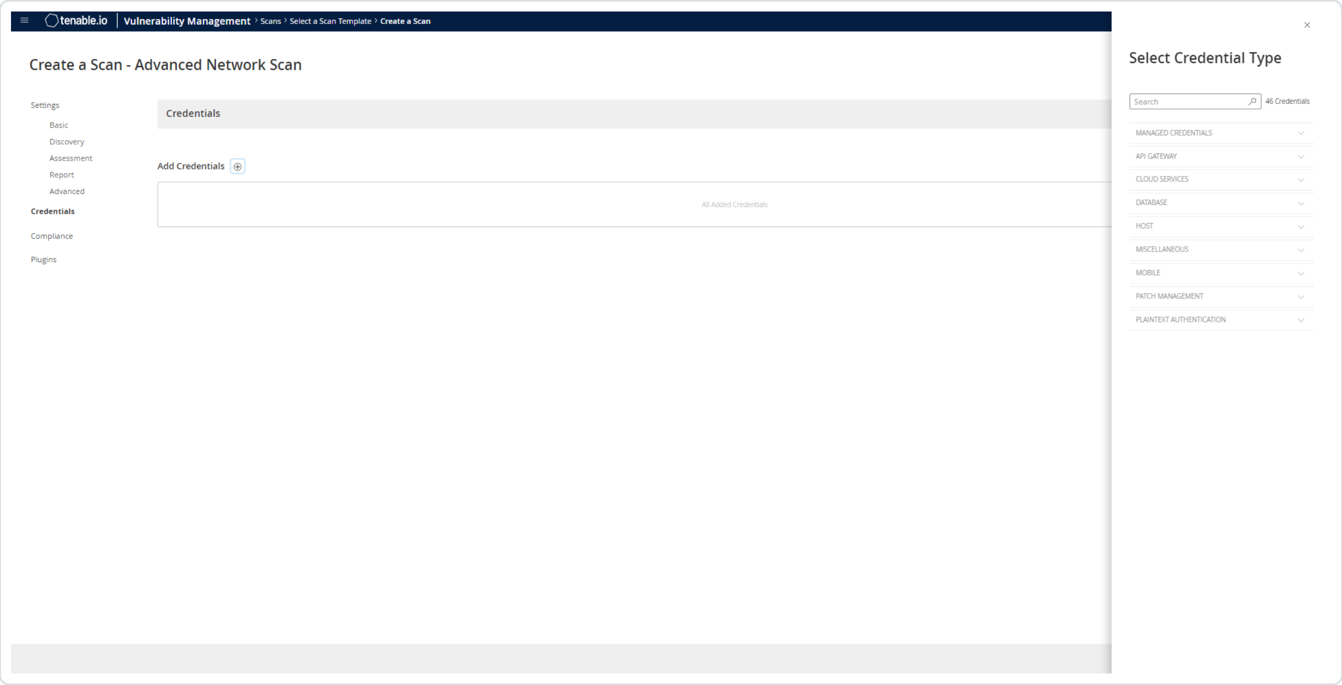


The **Credentials** pane appears.

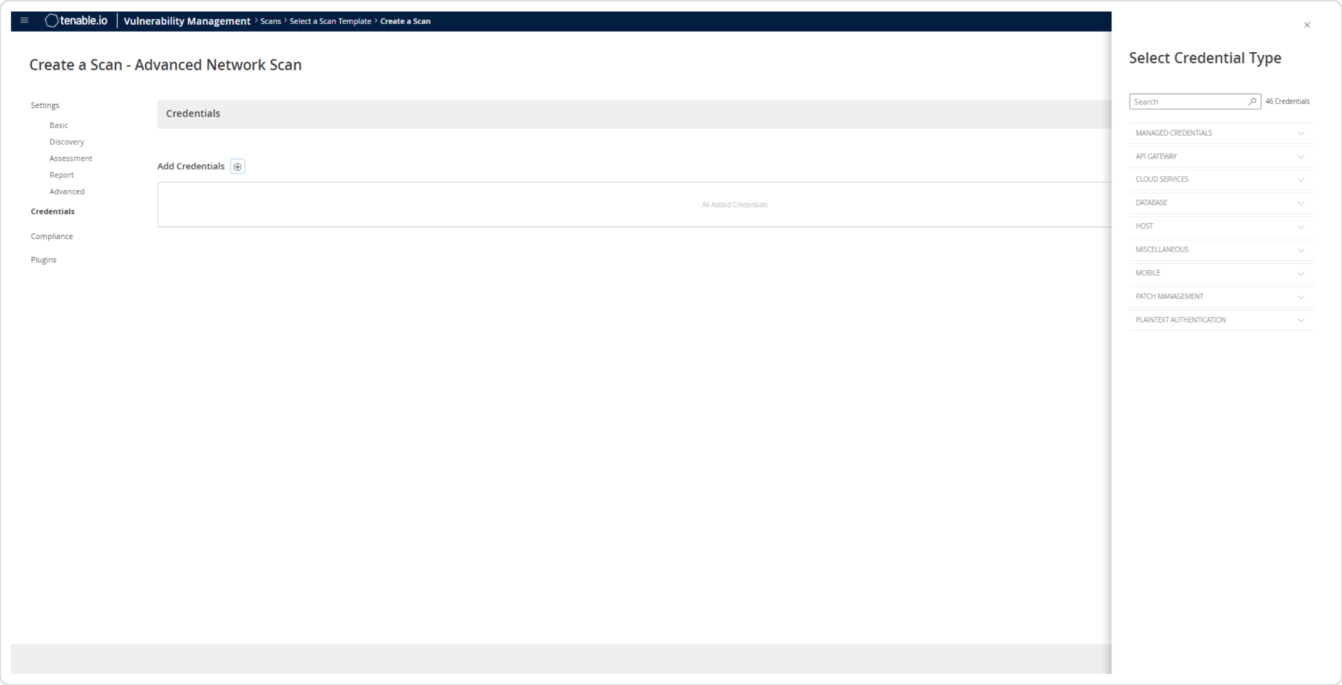


9. Click the **Database** option.

   The **Database** options appear.



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



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	The Private Key used to decrypt encrypted sensitive data from A2A. **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.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
HTTPS	This is enabled by default.	yes
Verify SSL Certificate	This is disabled by default.	no

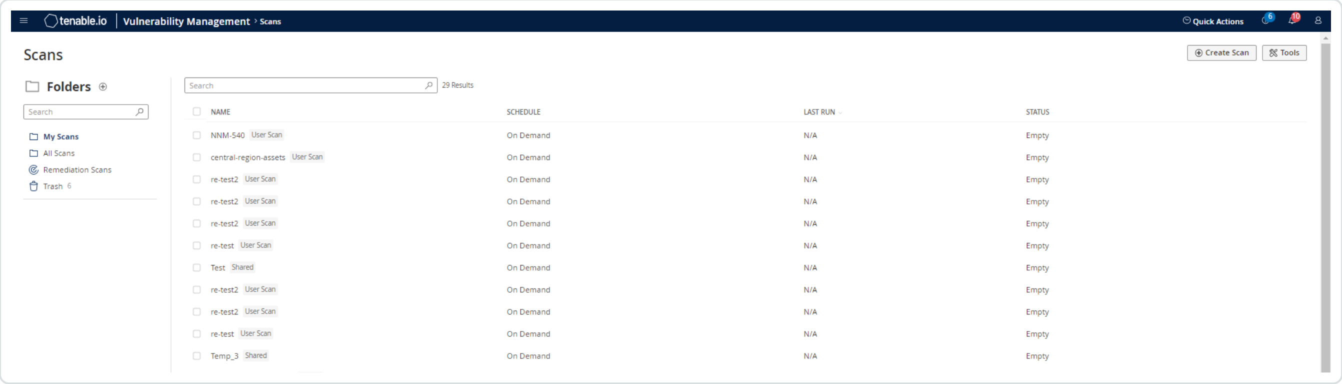
13. Click **Save**.

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.



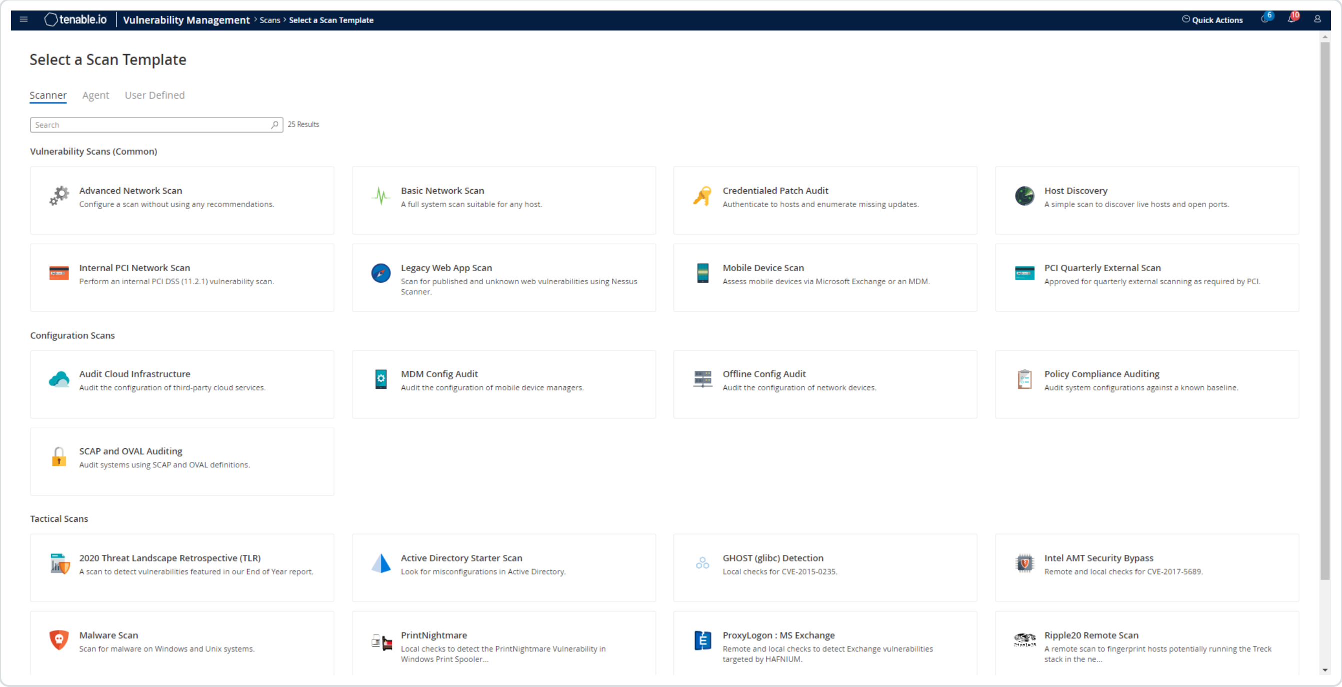
Scans

29 Results

NAME	SCHEDULE	LAST RUN	STATUS
NNM-540 User Scan	On Demand	N/A	Empty
central-region-assets 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-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

4. Select a scan template.

   The **Scan Templates** page appears.



Select a Scan Template

25 Results

Vulnerability 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.

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 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.

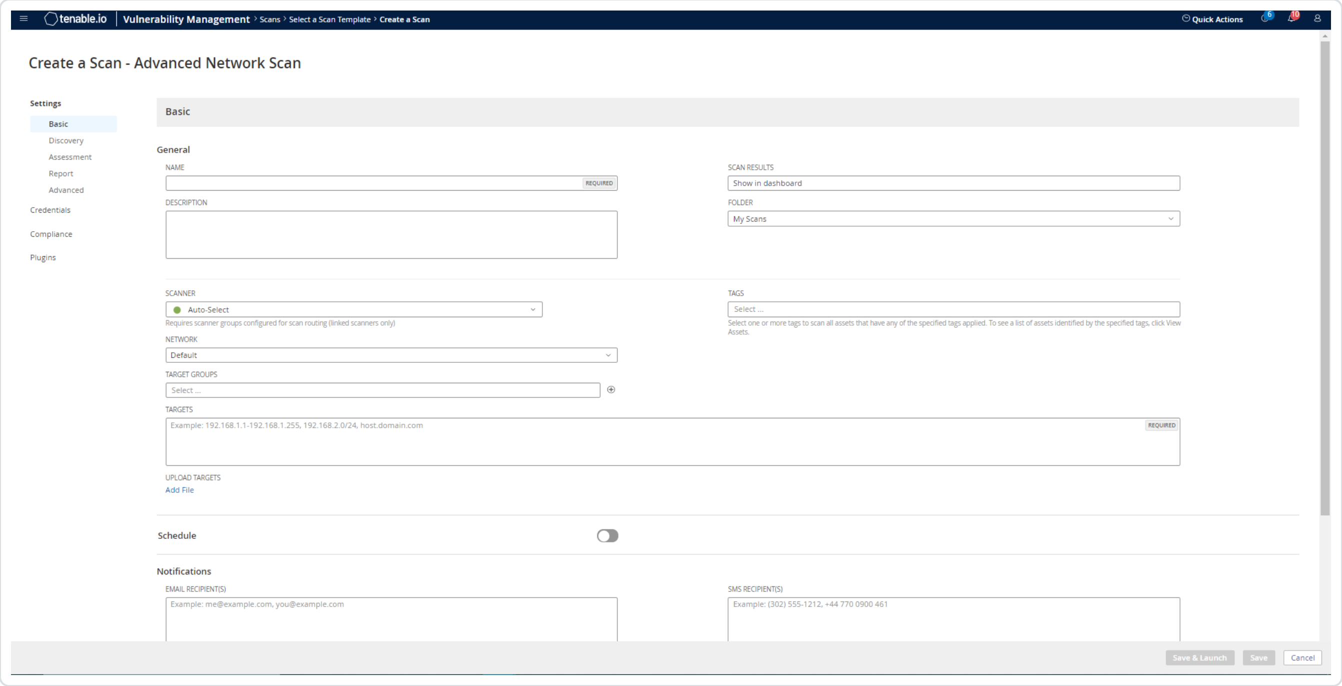
Malware Scan
Scan for malware on Windows and Unix systems.

PrintNightmare
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler...

ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the ne...

The scan configuration page appears.



Create a Scan - Advanced Network Scan

Basic

General

NAME REQUIRED

DESCRIPTION

SCAN RESULTS: Show in dashboard

FOLDER: My Scans

SCANNER: Auto-Select

Requires scanner groups configured for scan routing (linked scanners only)

TAGS: Select ...

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 ...

TARGETS: Example: 192.168.1.1-192.168.1.255, 192.168.2.0/24, host.domain.com REQUIRED

UPLOAD TARGETS: Add File

Schedule

Notifications

EMAIL RECIPIENT(S): Example: me@example.com, you@example.com

SMS RECIPIENT(S): Example: (302) 555-1212, +44 770 0900 461

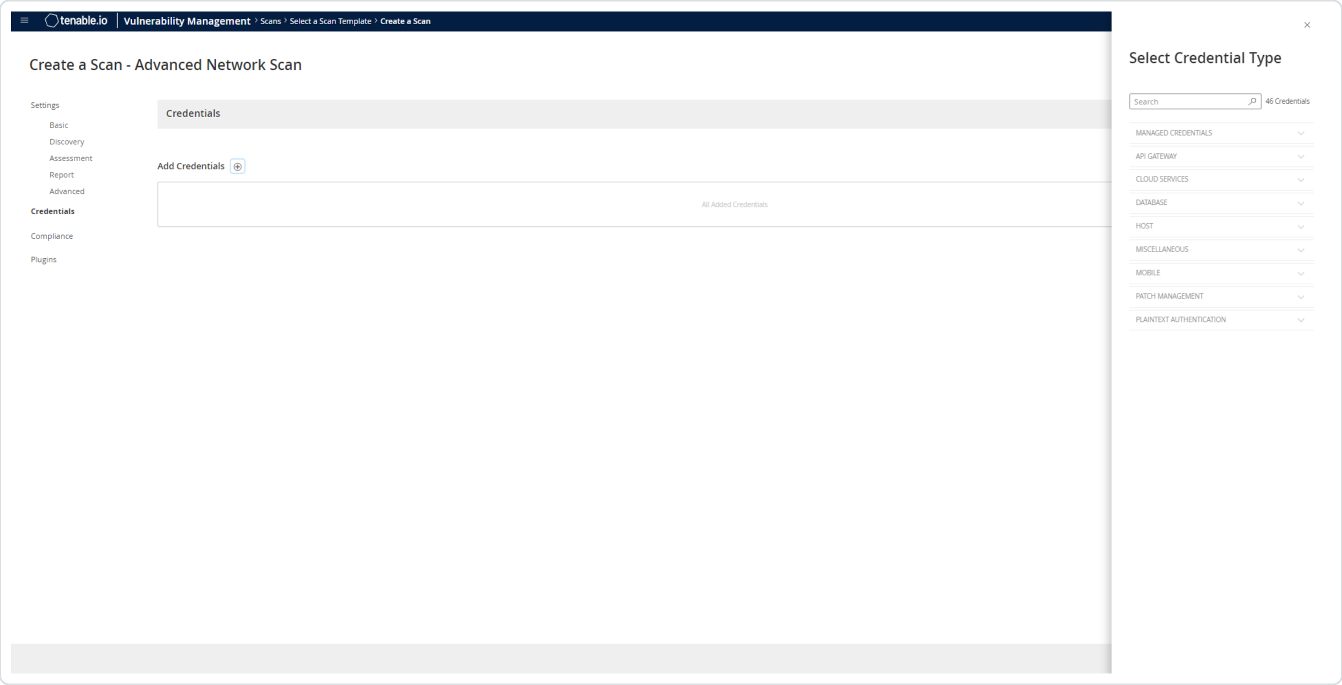
5. In the **Name** box, type a name for the scan.

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.



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 Oauth	yes

Option	Description	Required
	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 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. **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.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
Escalate Privileges with	The Private Key used to decrypt encrypted sensitive data from A2A. **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 your privilege escalation.	Required if you wish to escalate privileges.

Option	Description	Required
	Note: For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide, the Tenable Vulnerability Management User Guide, or the Tenable Security Center User Guide.	
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

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 ≡ 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 ⊕ 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. **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.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
HTTPS	This is enabled by default.	yes

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

9. Click **Save**.