



# Tenable and Senhasegura Integration Guide

---

Last Revised: March 07, 2023



## Table of Contents

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



---

## Welcome to Tenable for Senhasegura

---

This document provides information and steps for integrating Tenable.io and Nessus 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](#)

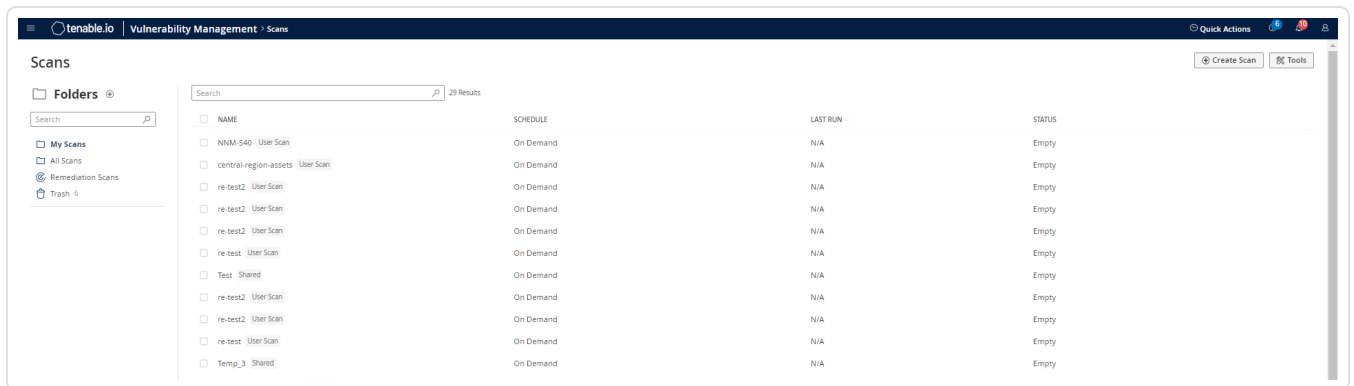


# Database Integration

To configure database integration:

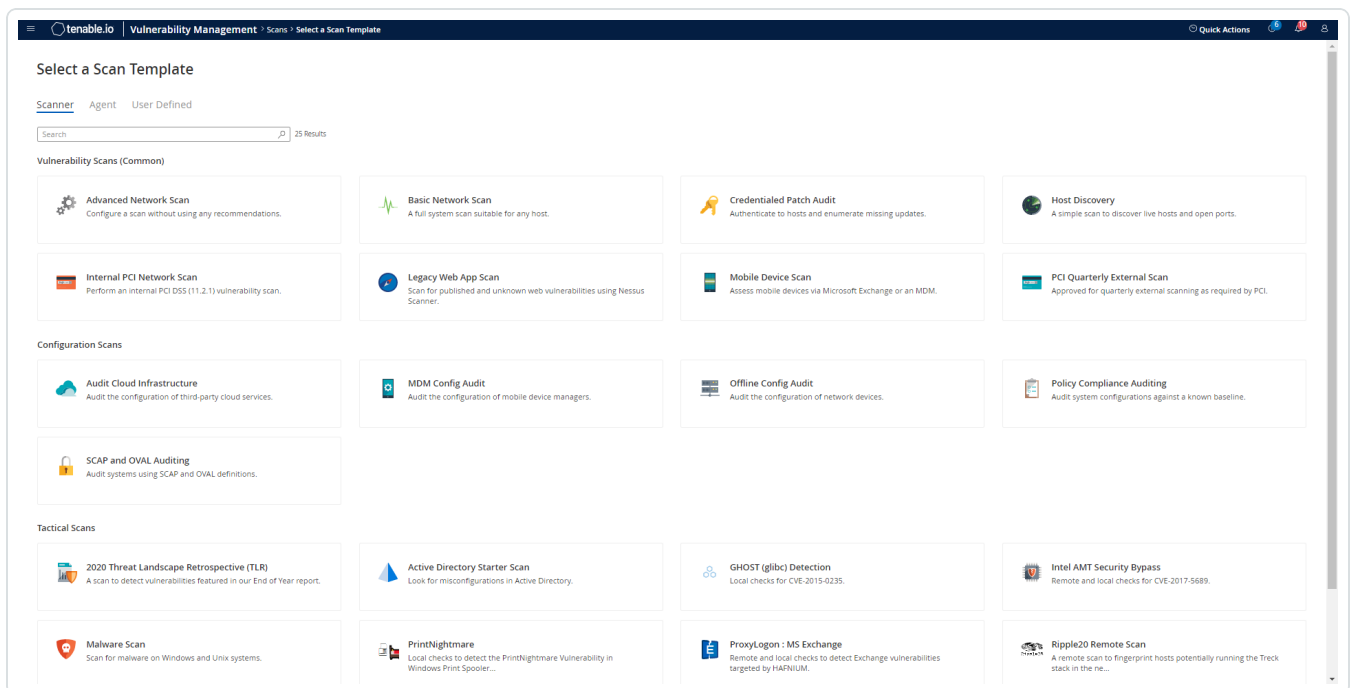
1. Log in to the Tenable user interface.
2. Click **Scans**.

The **My Scans** page appears.



3. Click **+ New Scan**.

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



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



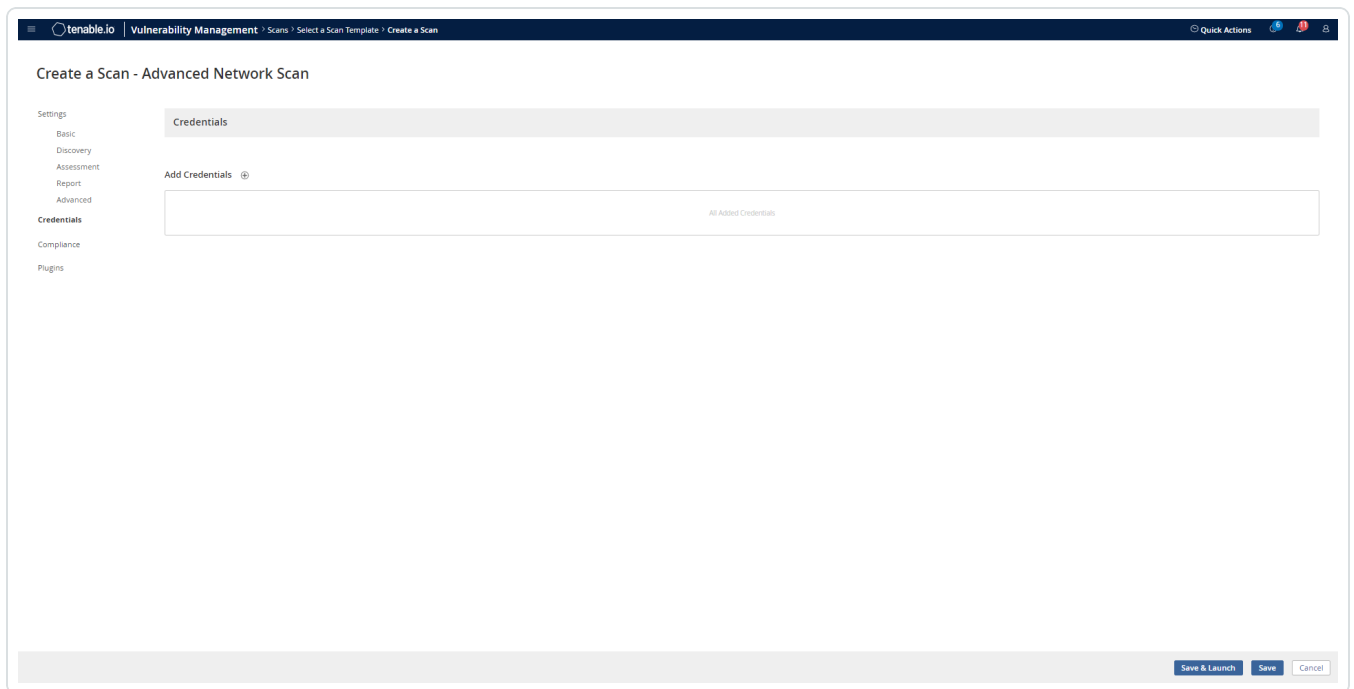
The scan configuration page appears.

The screenshot shows the 'Create a Scan - Advanced Network Scan' configuration page in Tenable.io. The page is divided into several sections:

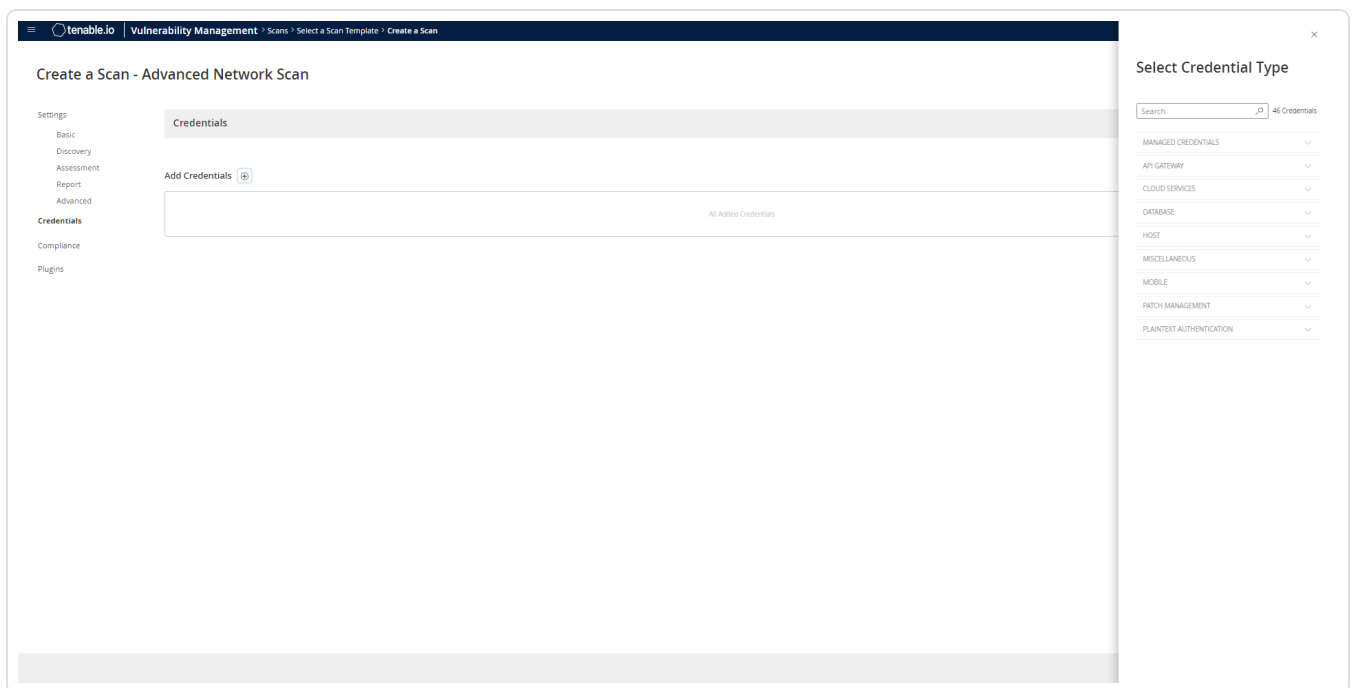
- Settings:** A sidebar on the left with tabs for Basic, Discovery, Assessment, Report, Advanced, Credentials, Compliance, and Plugins. 'Basic' is selected.
- General:**
  - NAME:** A text input field with a 'REQUIRED' label.
  - DESCRIPTION:** A text input field.
  - SCANNER:** A dropdown menu set to 'Auto-Select'.
  - NETWORK:** A dropdown menu set to 'Default'.
  - TARGET GROUPS:** A dropdown menu with a plus icon.
  - TARGETS:** A text input field with an example: '192.168.1.1-192.168.1.255, 192.168.2.0/24, host.domain.com' and a 'REQUIRED' label.
  - UPLOAD TARGETS:** A link labeled 'Add File'.
- Schedule:** A toggle switch.
- Notifications:**
  - EMAIL RECIPIENTS:** A text input field with an example: 'me@example.com, you@example.com'.
  - SMS RECIPIENTS:** A text input field with an example: '(302) 555-1212, +44 770 0900 461'.
- SCAN RESULTS:** A dropdown menu set to 'Show in dashboard'.
- FOLDER:** A dropdown menu set to 'My Scans'.
- TAGS:** A dropdown menu set to 'Select...'.

At the bottom right, there are three buttons: 'Save & Launch', 'Save', and 'Cancel'.

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.

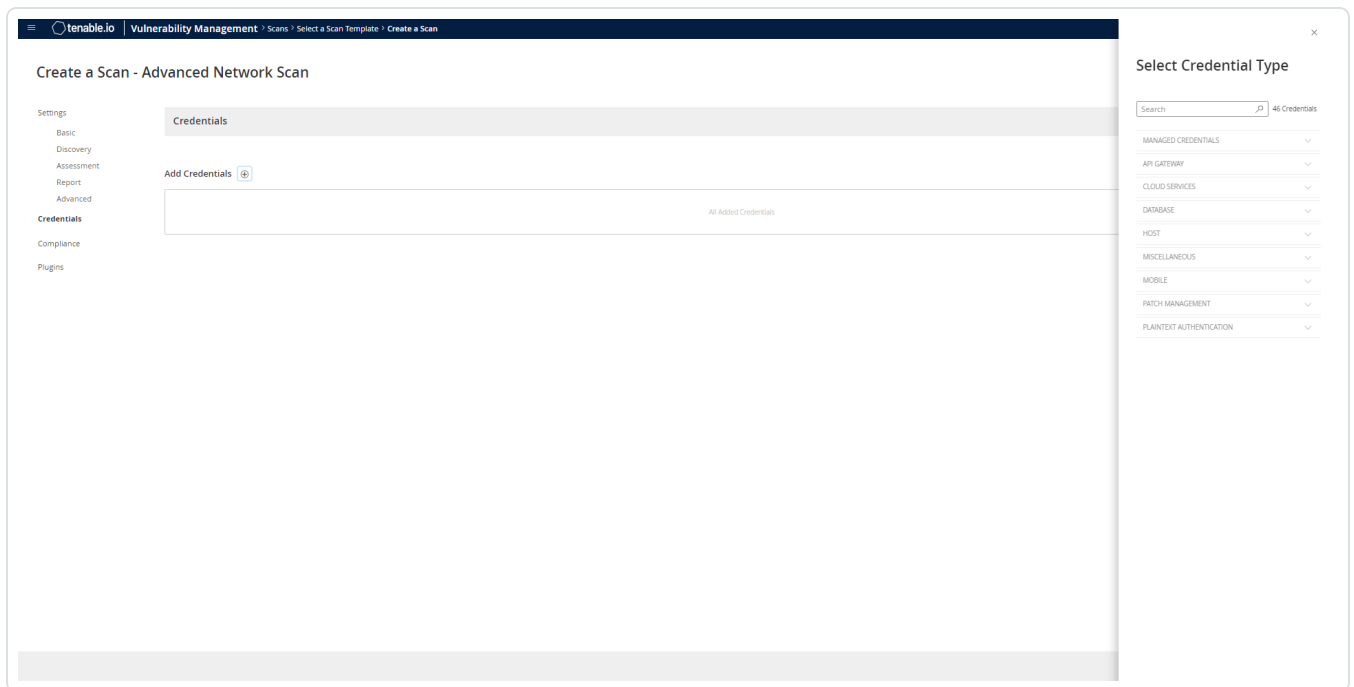


The **Credentials** pane appears.

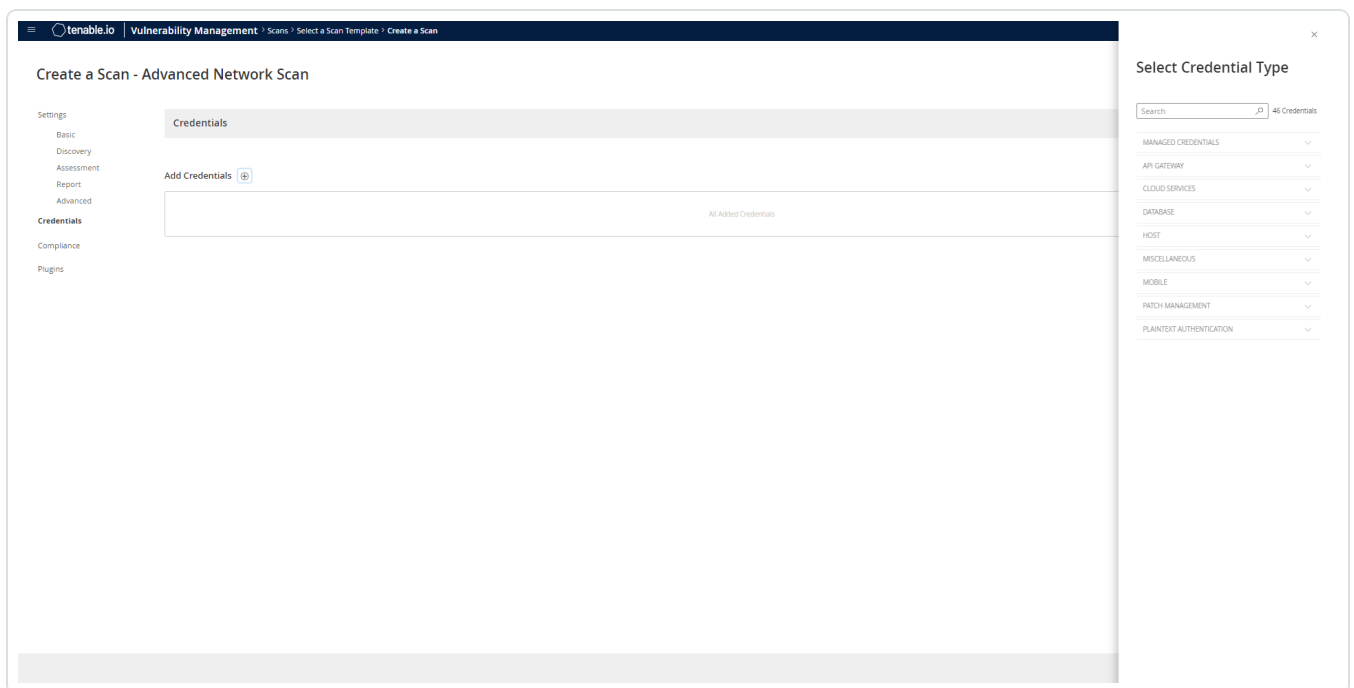


9. Click the **Database** option.

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. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"><b>Note:</b> 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.</div>	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**.

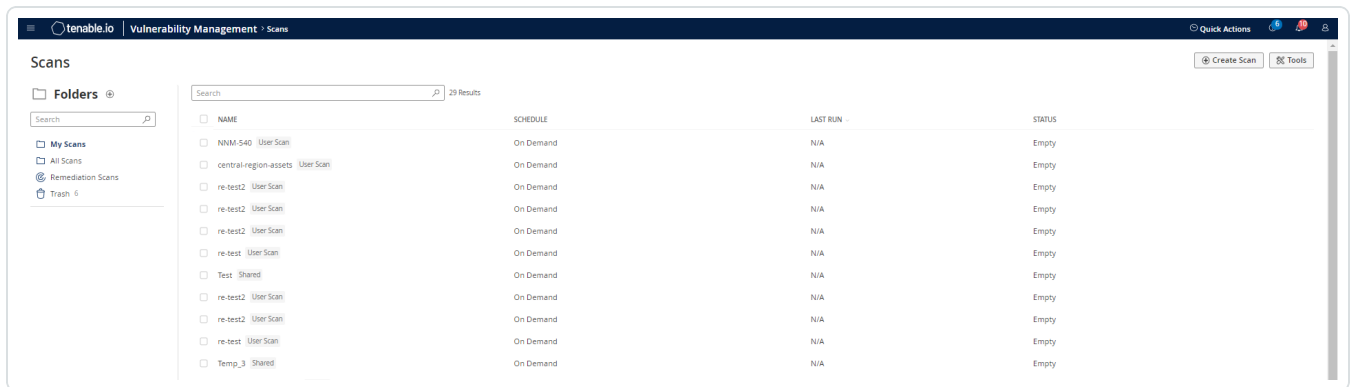


# SSH Integration

To configure SSH integration:

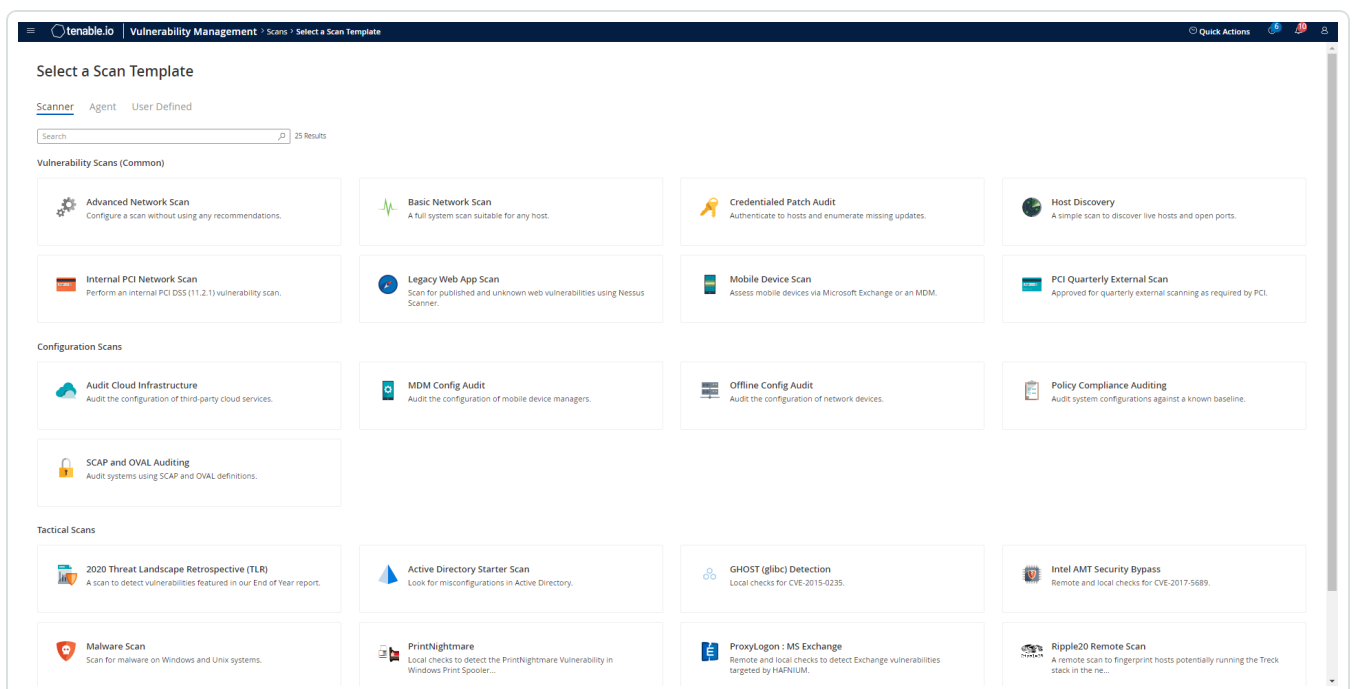
1. Log in to the Tenable user interface.
2. Click **Scans**.
3. Click **+ New Scan**.

The **My Scans** page appears.



4. Select a scan template.

The **Scan Templates** page appears.

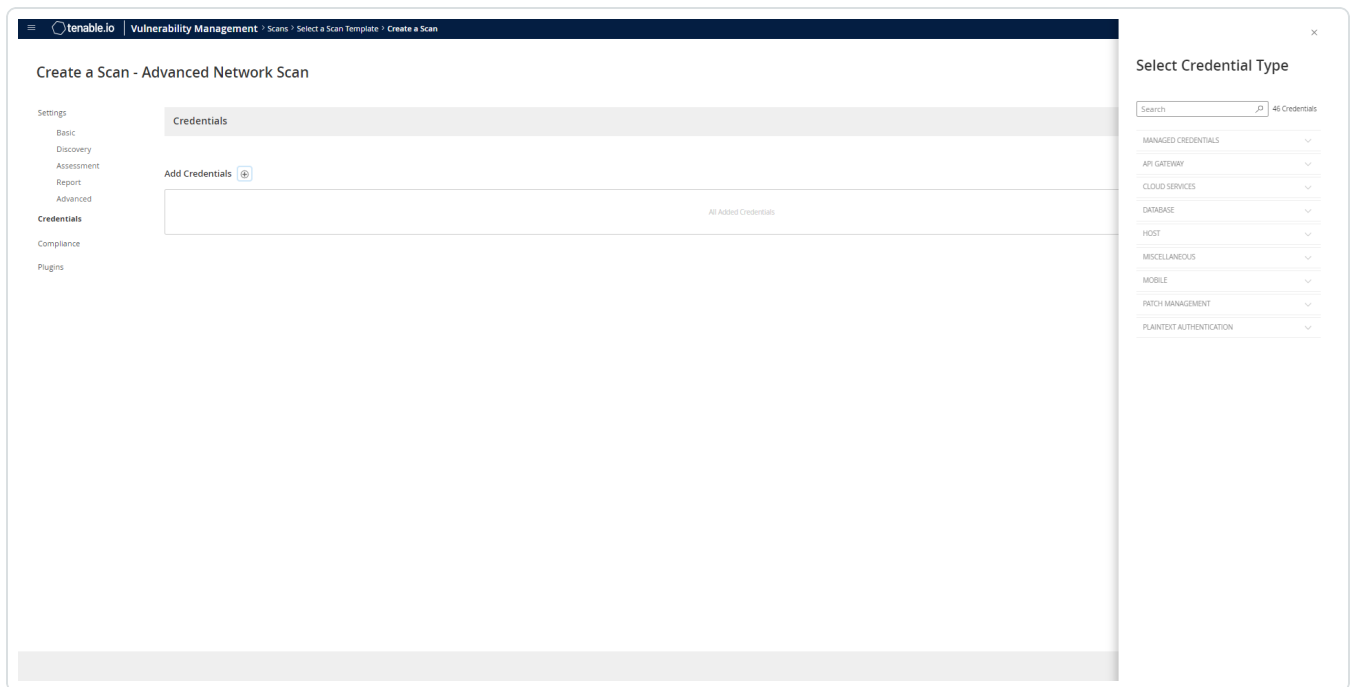




The scan configuration page appears.

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 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	<p>The Private Key used to decrypt encrypted sensitive data from A2A.</p> <div style="border: 1px solid blue; padding: 5px;"><p><b>Note:</b> 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.</p></div>	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
Escalate Privileges with	<p>The Private Key used to decrypt encrypted sensitive data from A2A.</p> <div style="border: 1px solid blue; padding: 5px;"><p><b>Note:</b> 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.</p></div>	Required if you wish to escalate privileges.



Option	Description	Required
	<b>Note:</b> For more information about supported privilege escalation types and their accompanying fields, see the <a href="#">Nessus User Guide</a> and the <a href="#">Tenable.io User Guide</a> .	
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.io.
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. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"><b>Note:</b> 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.</div>	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**.