Tenable and WALLIX Bastion Integration Guide

Last Revised: May 05, 2022

Table of Contents

Welcome to Tenable for WALLIX Bastion PAM

This document provides information and steps for integrating Tenable.io or Nessus Manager with WALLIX Bastion Privileged Access Management (PAM).

Easy to use and easy to deploy, the WALLIX Bastion PAM solution delivers robust security and oversight over privileged access to critical IT infrastructure. Reduce the attack surface and meet regulatory compliance requirements with simplified PAM. By integrating WALLIX Bastion PAM with Tenable products, customers have more choice and flexibility.

The benefits of integrating Tenable with WALLIX Bastion PAM include:

- Credential updates directly in Tenable.io or Nessus Manager
- Enforced credential complexity to ensure that critical systems' credentials meet strict password criteria
- Routine and automated rotation of passwords by account or domain to stop breaches related to shared or hijacked passwords
- Eliminate generic admin and root passwords shared and used by anyone

For more information on WALLIX Bastion PAM, see the WALLIX Bastion documentation.

For information on Tenable.io functions or installing and/or launching Tenable.io, see the Tenable User Guide.

For information on Nessus Manager functions or installing and/or launching Nessus, see the Nessus User Guide.

Windows Integration

Tenable provides full database support for WALLIX Bastion integrations. Complete the following steps to configure Windows credentials for scans with WALLIX Bastion.

For more information on Tenable scans, see the Nessus User Guide. and the Tenable.io User Guide.

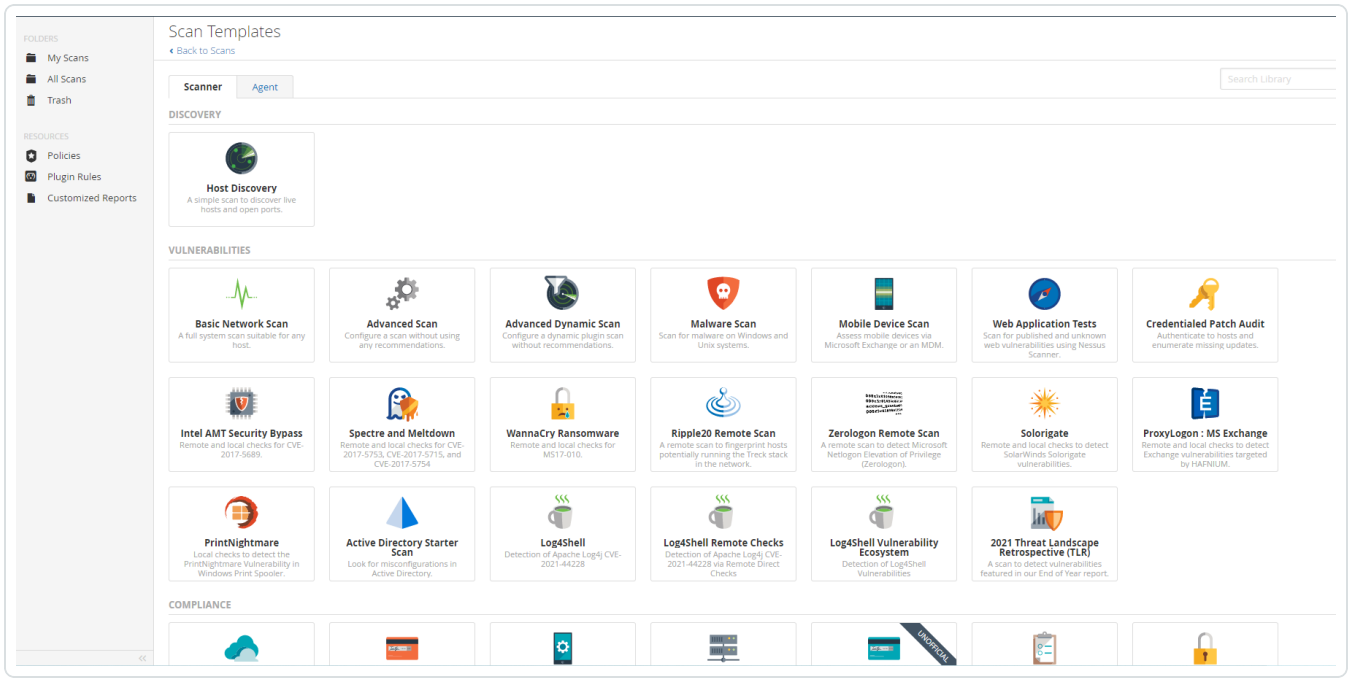
Requirements:

- WALLIX Bastion account
- Tenable.io or Nessus Manager account

To configure WALLIX Bastion using Windows integration:

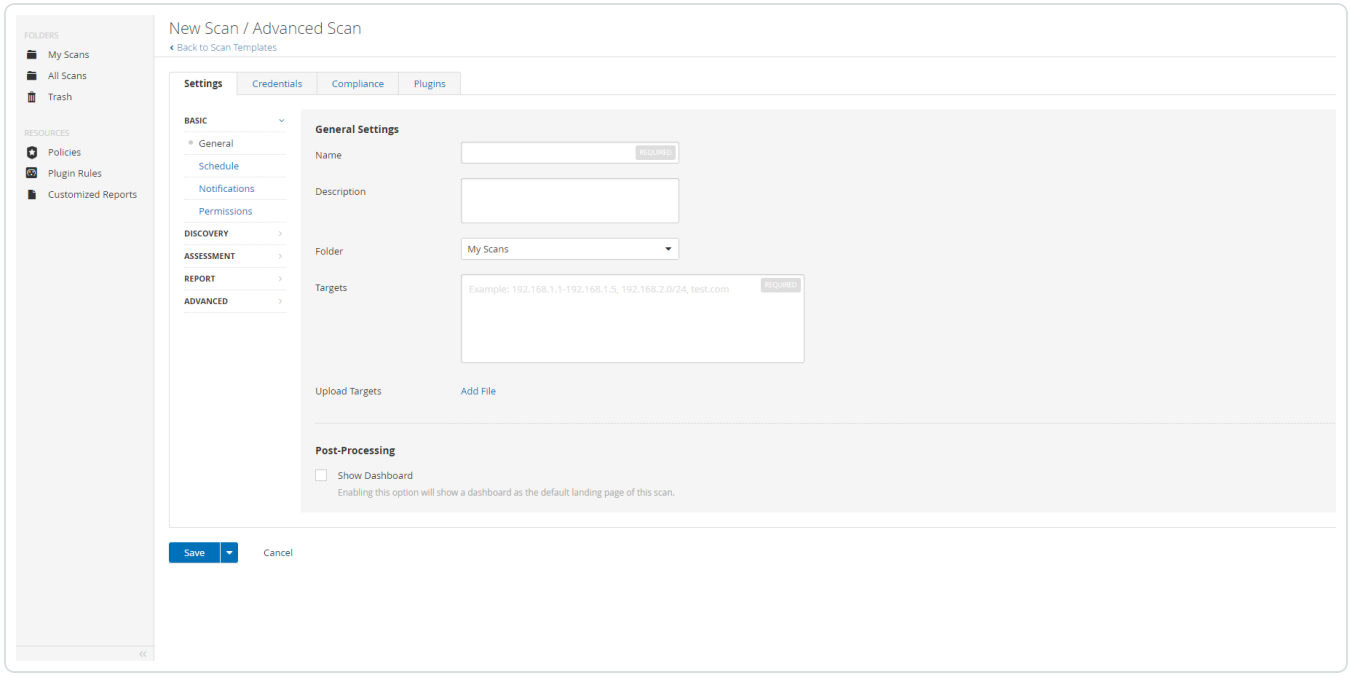
1. Log in to your Tenable user interface.
2. Click **Scans**.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.



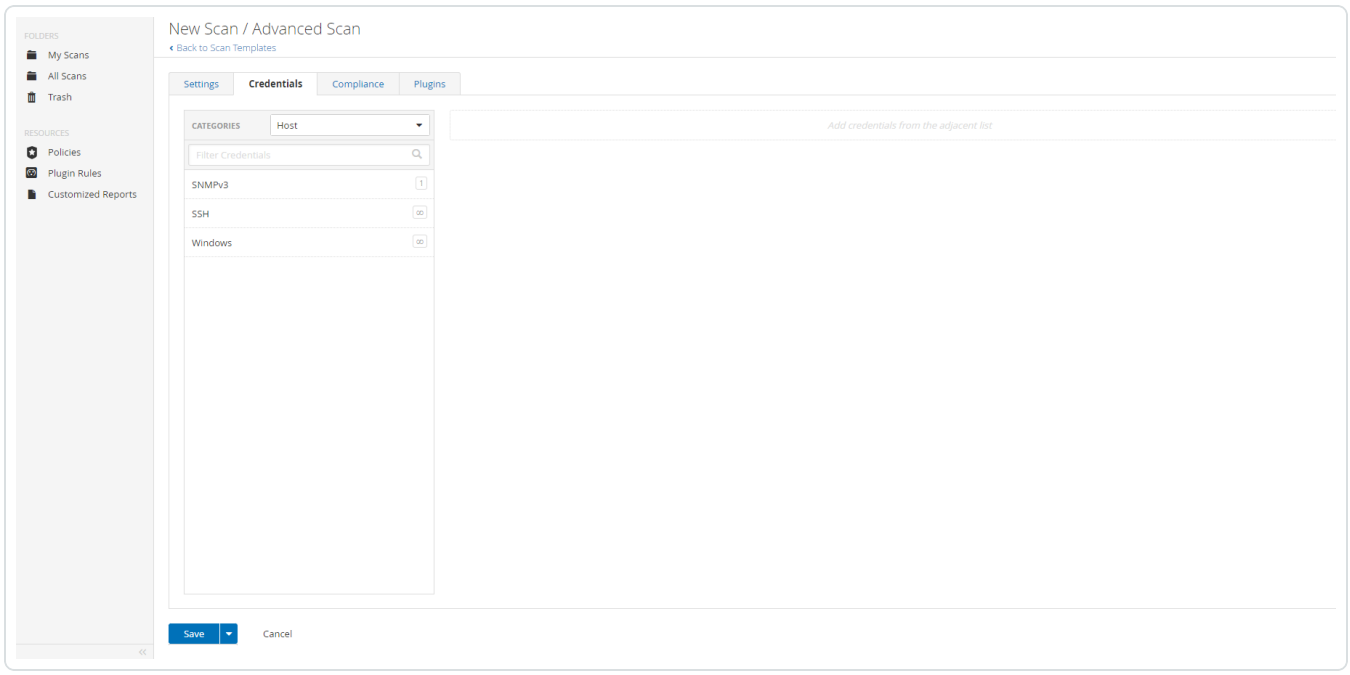
4. Select **Advanced Scan**.

The selected scan template appears.



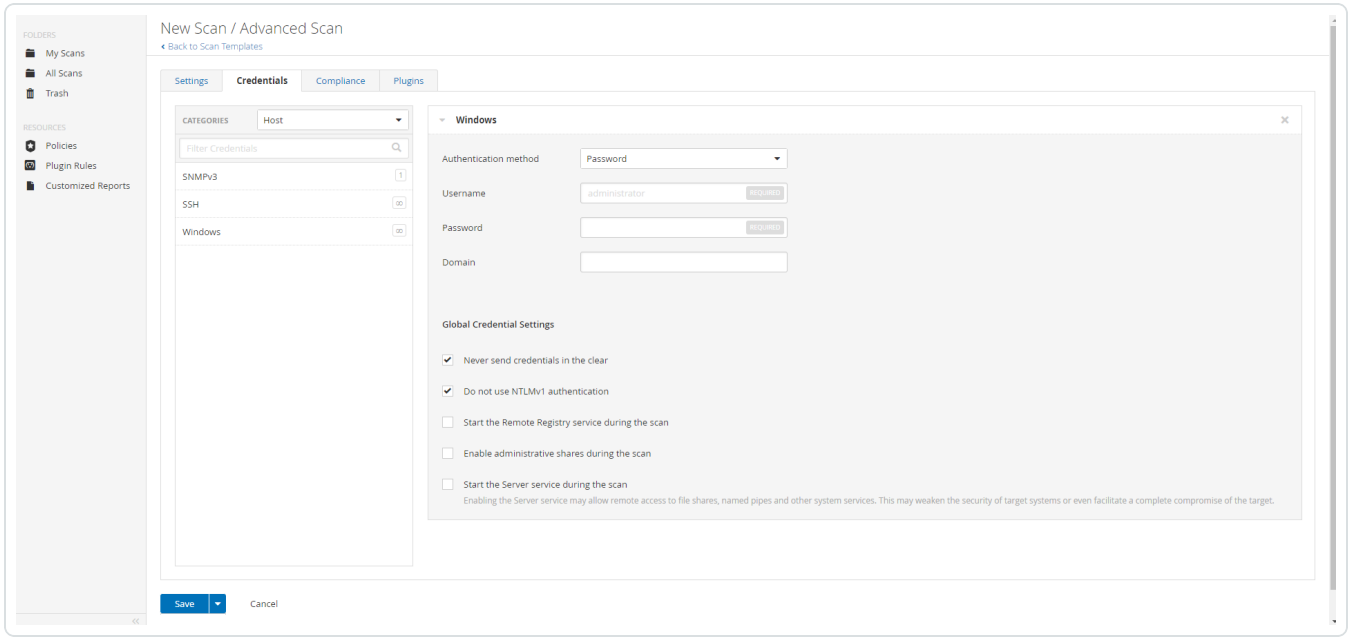
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   The Credentials options appear.



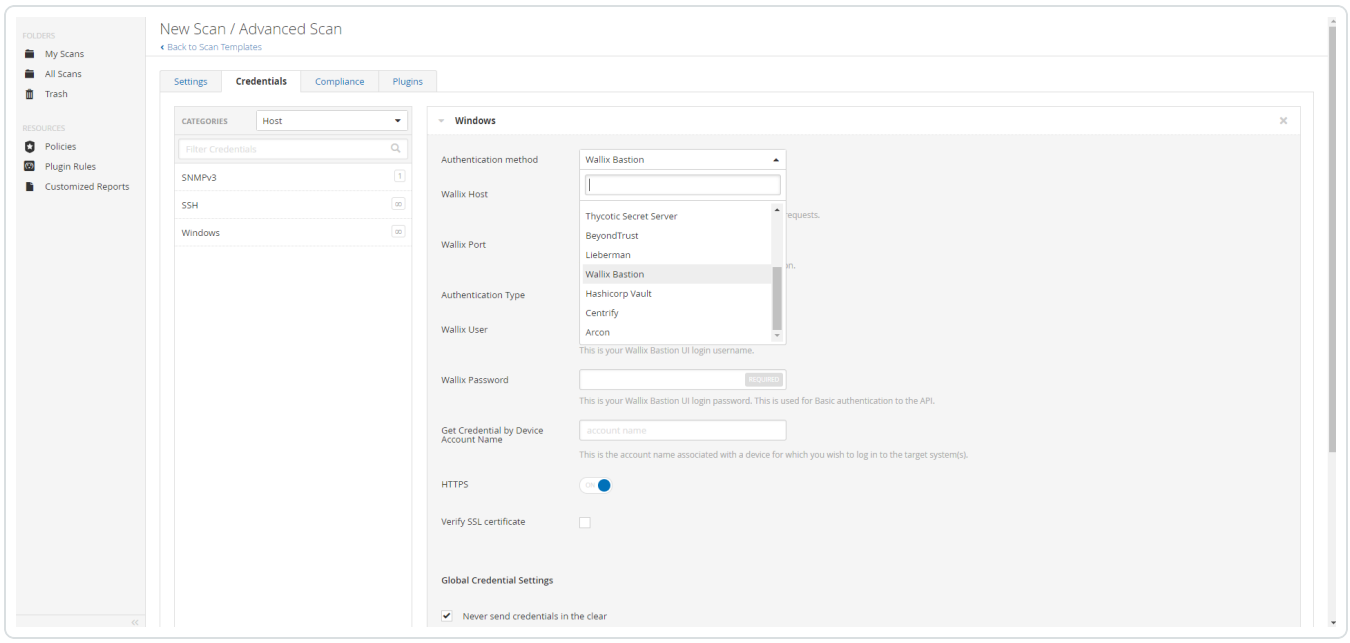
9. In the **Host** section, click **Windows**.

   The selected credential options appear.



10. In the **Authentication Method** drop-down box, select **Wallix Bastion**.

    The **Wallix Bastion** options appear.



11. Configure the **Wallix Bastion** credentials.

Option	Description	Required
Wallix Host	The IP address for the WALLIX Bastion host.	yes
Wallix Port	The port on which the WALLIX Bastion API communicates. By default, Nessus Manager uses 443.	yes
Authentication Type	**Basic** authentication (with WALLIX Bastion user interface username and Password requirements) or **API Key** authentication (with username and WALLIX Bastion-generated API key requirements).	yes
Wallix User	Your WALLIX Bastion user interface login username.	yes
Wallix Password	Your WALLIX Bastion user interface	yes

Option	Description	Required
	login password. Used for **Basic** authentication to the API.	
Wallix API Key	The API key generated in the WALLIX Bastion user interface. Used for **API Key** authentication to the API.	yes
Get Credential by Device Account Name	The account name associated with a **Device** you want to log in to the target systems with. **Note:** If the device has more than one account, you must enter the specific device name for the account you want to retrieve credentials for. Failure to do this may result in credentials for the wrong account returned by the system.	Required only if you have a target and/or device with multiple accounts.
HTTPS	This is enabled by default. **Caution:** The integration fails if you disable **HTTPS**.	yes
Verify SSL Certificate	This is disabled by default and unsupported in WALLIX Bastion PAM integrations.	no

12. Click **Save**.

Verification

1. Click the arrow next to the **Save** button to drop down the launch button.
2. To verify the integration is working, click the **Launch** button to initiate an on-demand scan.
3. After the scan completes, click the scan to view the results.

SSH Integration with Privilege Escalation option

Tenable provides full SSH support for WALLIX Bastion, including optional Privilege Access Management (PAM). Complete the following steps to configure SSH credentials for scans with WALLIX Bastion.

For more information on Tenable scans, see the Nessus User Guide and the Tenable.io User Guide.

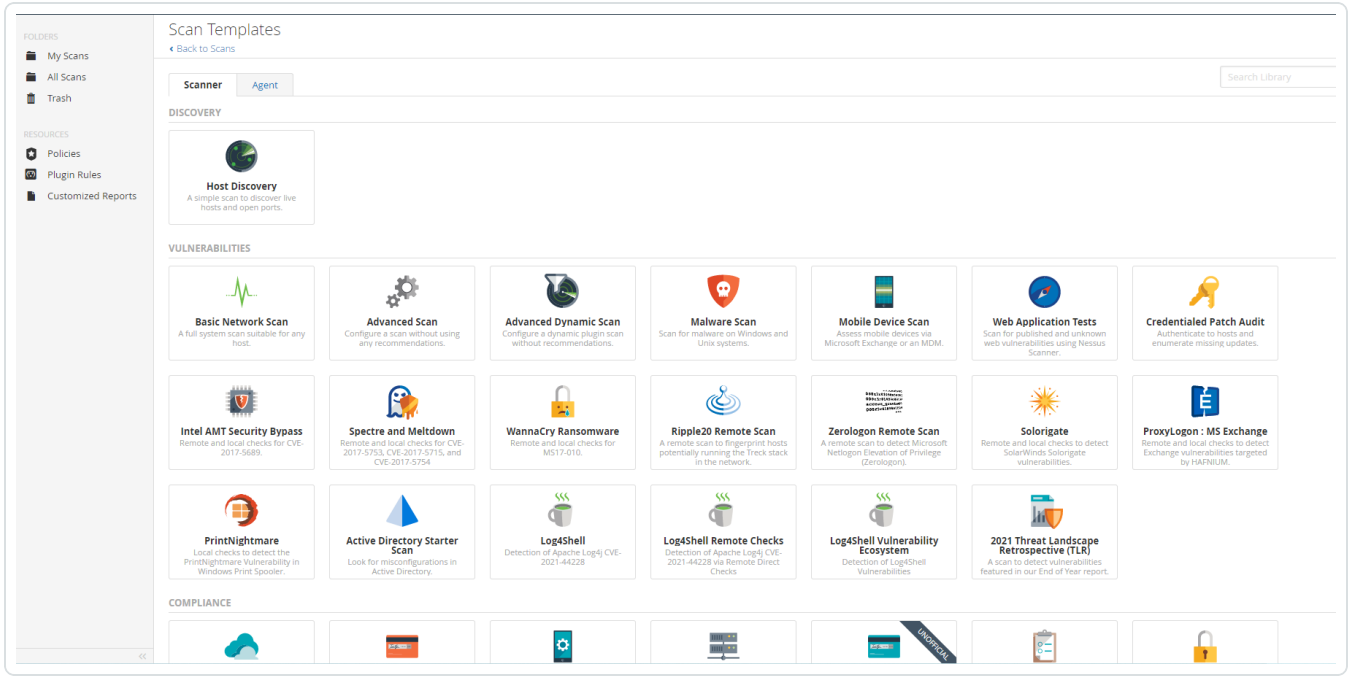
Requirements:

- WALLIX Bastion account
- Tenable.io or Nessus Manager account

To configure SSH integration:

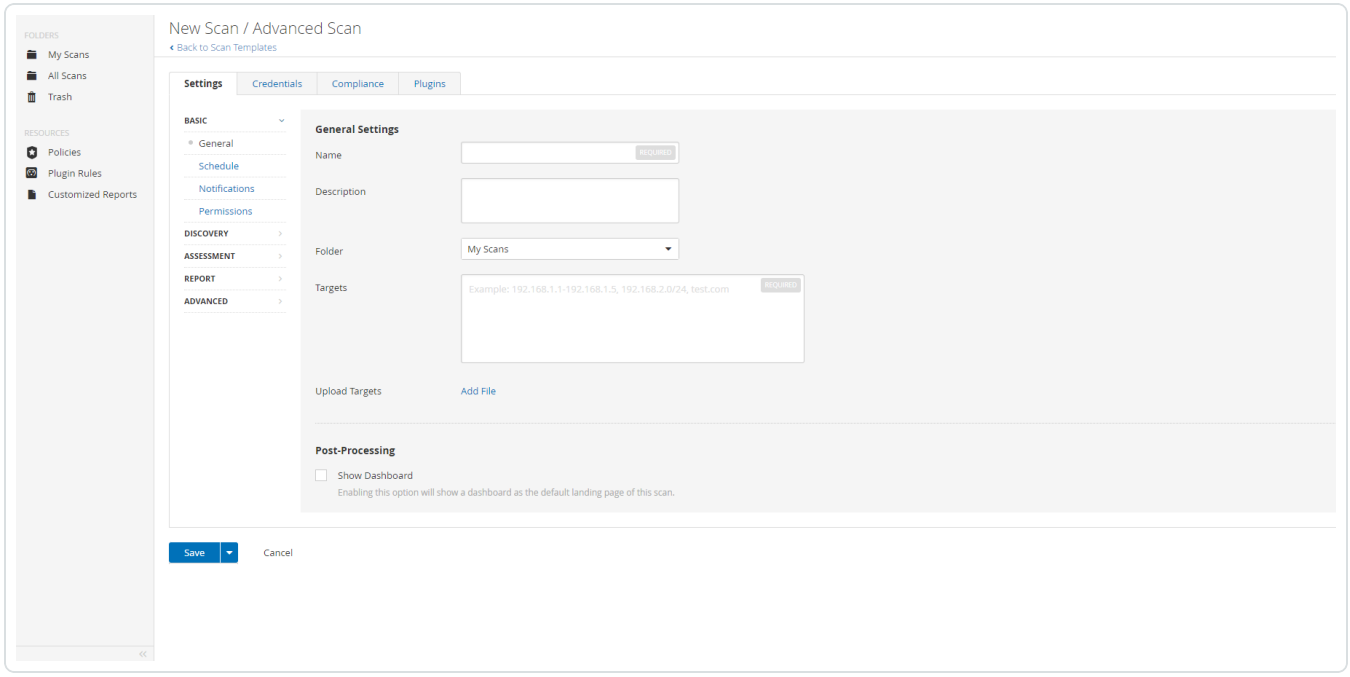
1. Log in to your Tenable user interface.
2. Click **Scans**.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.



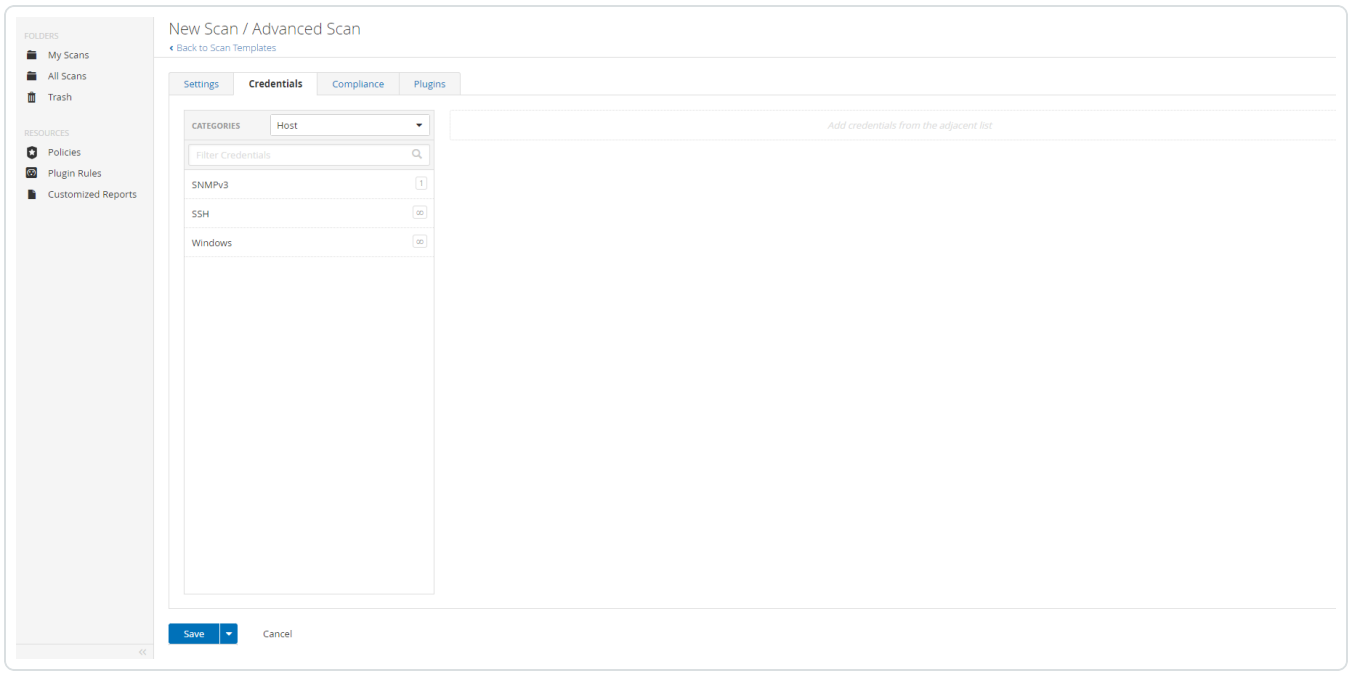
4. Select **Advanced Scan**.

The selected scan template appears.



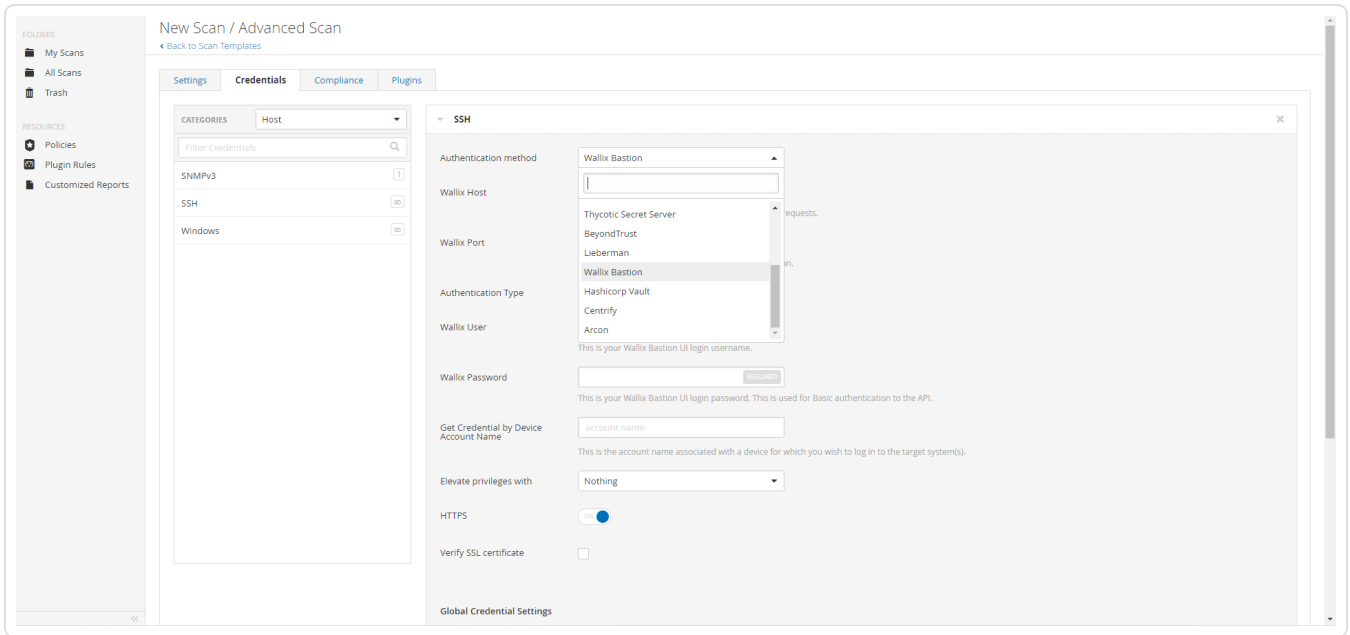
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   The Credentials options appear.



9. In the left-hand menu, select **SSH**.
10. Click **Authentication method**.
11. Select **Wallix Bastion** in the drop-down box.

    The **Wallix Bastion SSH** options appear.



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

Option	Description	Required
Wallix Host	The IP address for the WALLIX Bastion host.	yes
Wallix Port	The port on which the WALLIX Bastion API communicates. By default, Nessus Manager uses 443.	yes
Authentication Type	**Basic** authentication (with WALLIX Bastion user interface username and Password requirements) or **API Key** authentication (with username and WALLIX Bastion-generated API key requirements).	yes
Wallix User	Your WALLIX Bastion user interface login username.	yes
Wallix Password	Your WALLIX Bastion user interface login password. Used for **Basic** authentication to the API.	yes
Wallix API Key	The API Key generated in the WALLIX Bastion user interface. Used for **API Key** authentication to the API.	yes
Get Credential by Device Account Name	The account name associated with a **Device** you want to log in to the target systems with. **Note:** If your device has more than one account, you must enter the specific device name for the account you want to retrieve credentials for. Failure to do this may result in credentials for the wrong account returned by the system.	Required only if you have a target and/or device with multiple accounts.

Option	Description	Required
Elevate privileges with	This enables WALLIX Bastion Privileged Access Management (PAM). Use the drop-down menu to select the privilege elevation method. To bypass this function, leave this field set to **Nothing**. **Caution:** In your WALLIX Bastion account, the WALLIX Bastion super admin must have enabled "credential recovery" on your account for PAM to be enabled. Otherwise, your scan may not return any results. For more information, see your WALLIX Bastion documentation. **Note:** Multiple options for privilege escalation are supported, 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 WALLIX Bastion PAM. The **Escalation Account Name** field is then required to complete your privilege escalation. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide and the Tenable.io User Guide.	Required if you wish to escalate privileges.
HTTPS	This is enabled by default. **Caution:** The integration fails if you disable **HTTPS**.	yes

Option	Description	Required
Verify SSL Certificate	This is disabled by default and unsupported in WALLIX Bastion PAM integrations.	no

13. Click **Save**.

Verification

1. Click the arrow next to the **Save** button to drop down the launch button.
2. To verify the integration is working, click the **Launch** button to initiate an on-demand scan.
3. After the scan completes, click the scan to view the results.

Database Integration

Tenable provides full database support for WALLIX Bastion integrations. Complete the following steps to configure database credentials for scans with WALLIX Bastion.

For more information on Tenable scans, see the Nessus User Guide and the Tenable.io User Guide.

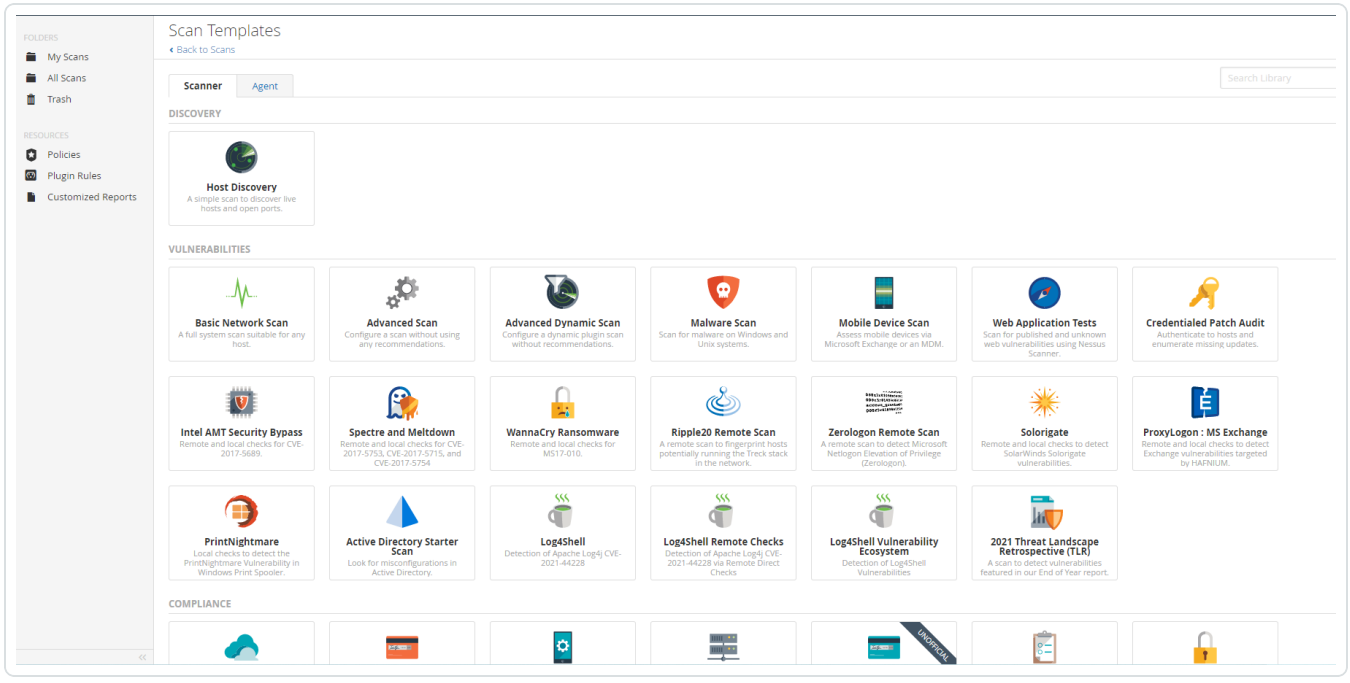
Requirements:

- WALLIX Bastion account
- Tenable.io or Nessus Manager account

To configure Database integration:

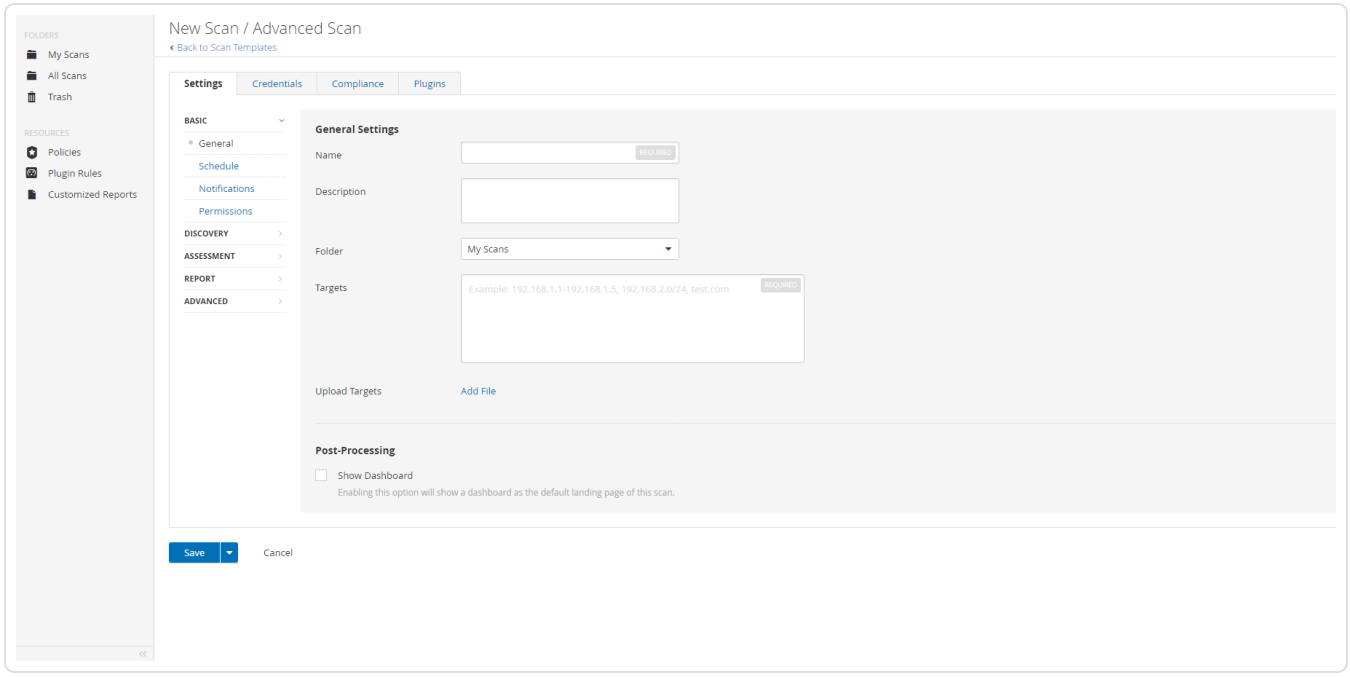
1. Log in to your Tenable user interface.
2. Click **Scans**.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.



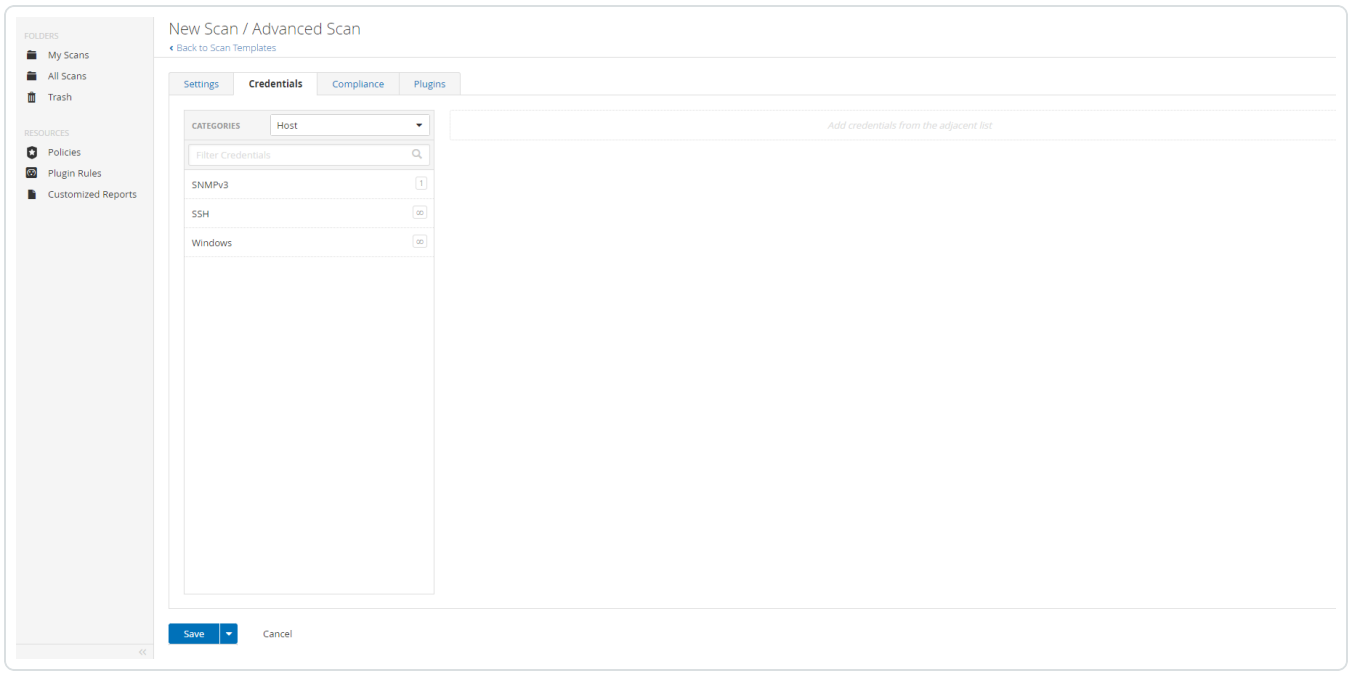
4. Select **Advanced Scan**.

The selected scan template appears.



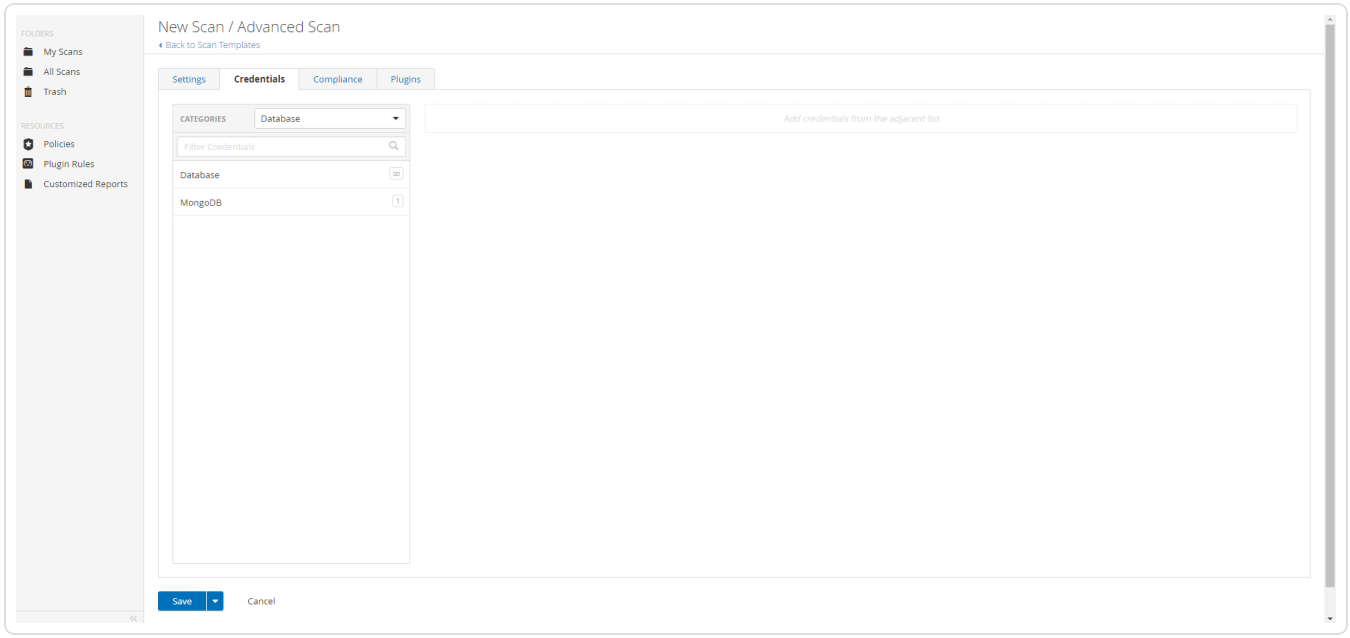
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   The **Credentials** options appear.



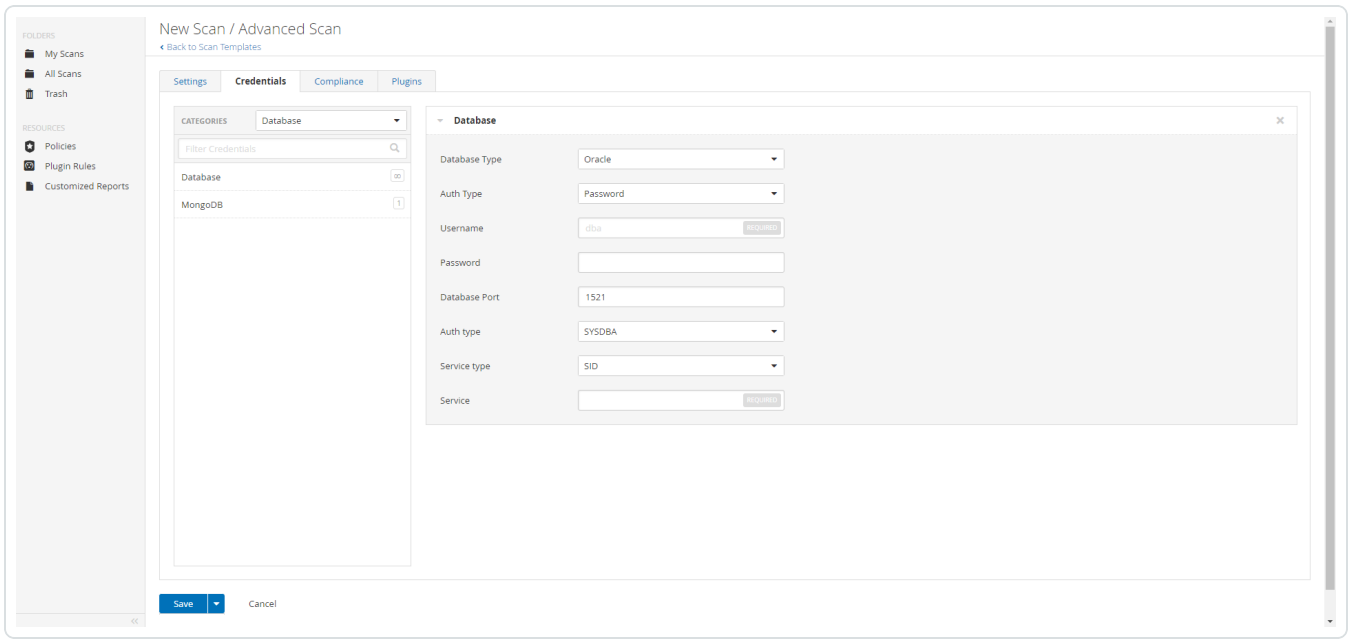
9. In the **Categories** drop-down box, select **Database**.

   The **Database** options appear.



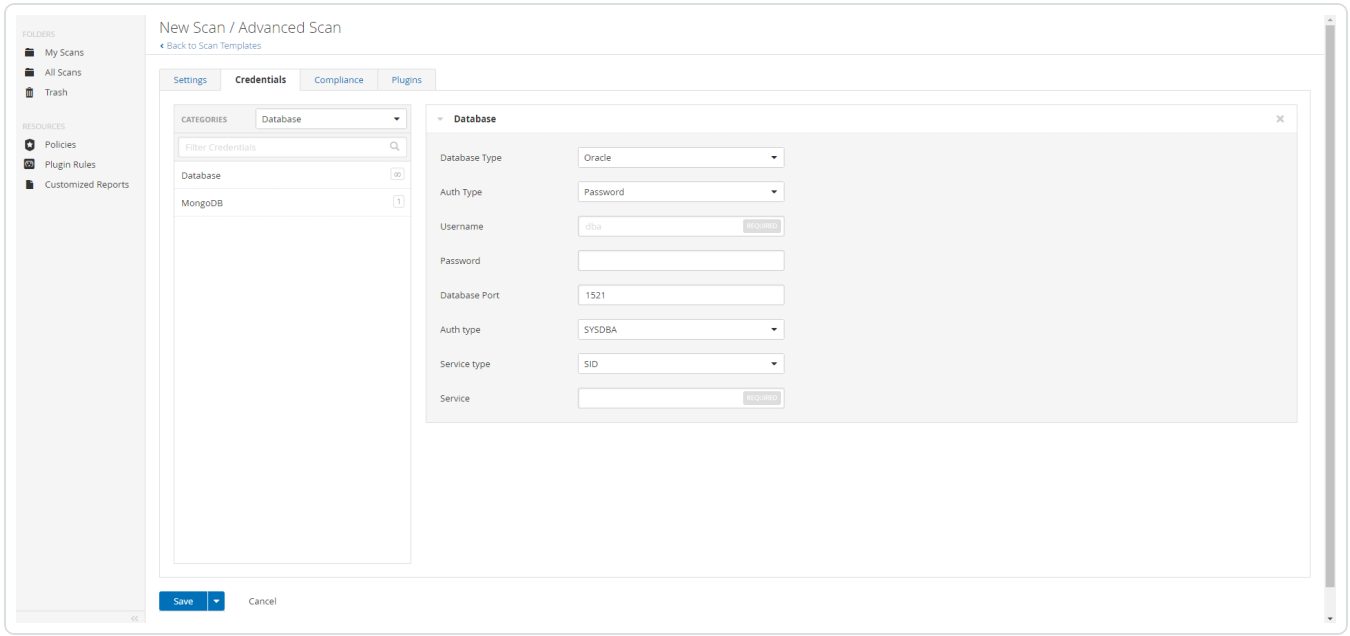
10. Click **Database**.

    The **Database** options appear.

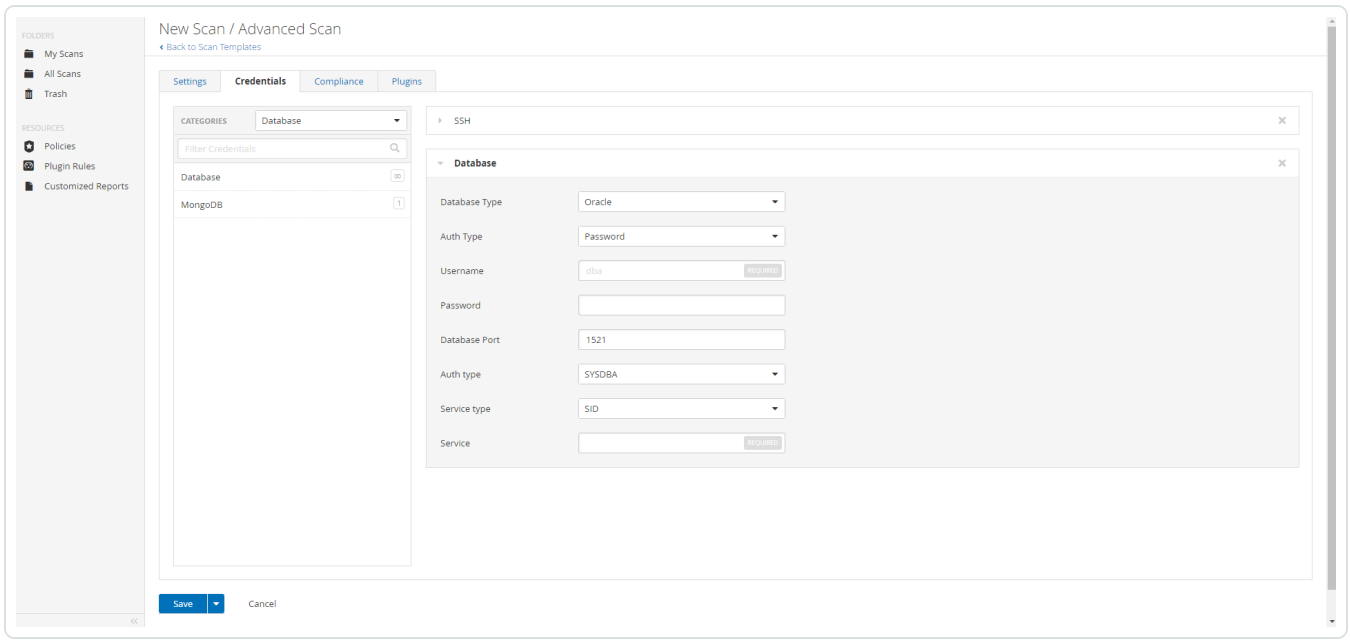


11. Click the **Database Type** drop-down box.

    The **Database** field options appear.

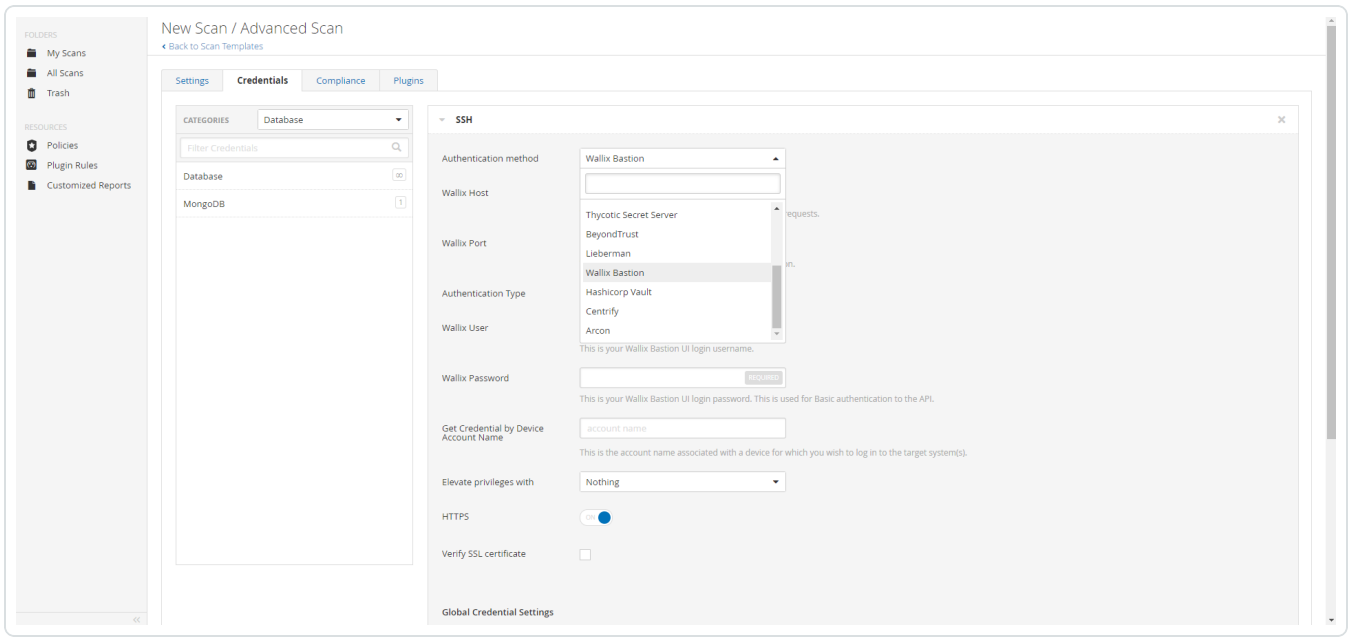


12. From the **Database Type** drop-down box, select **Oracle**.



13. From the **Auth Type** drop-down box, select **Wallix Bastion**.

    The **Wallix Bastion** field options appear.



14. Configure each field for **Database** authentication.

Option	Description	Required
Wallix Host	The IP address for the WALLIX Bastion host.	yes
Wallix Port	The port on which the WALLIX Bastion API communicates. By default, Tenable uses 443.	yes
Authentication Type	**Basic** authentication (with WALLIX Bastion user interface username and Password requirements) or **API Key** authentication (with username and WALLIX Bastion-generated API key requirements).	no
Wallix User	Your WALLIX Bastion user interface login username.	yes
Wallix Password	Your WALLIX Bastion user interface login password. Used for **Basic** authentication to the API.	yes
Wallix API Key	The API key generated in the WALLIX Bastion user interface. Used for **API Key** authentication to the API.	yes
Get Credential by Device Account Name	The account name associated with a **Device** you want to log in to the target systems with. **Note:** If your device has more than one account you must enter the specific device name for the account you want to retrieve credentials for. Failure to do this may result in credentials for the wrong account returned by the system.	Required only if you have a target and/or device with multiple accounts.

Option	Description	Required
HTTPS	This is enabled by default. **Caution:** The integration fails if you disable **HTTPS**.	yes
Verify SSL Certificate	This is disabled by default and is not supported in WALLIX Bastion PAM integrations.	no
Database Port	The TCP port that the Oracle database instance listens on for communications from. The default is port 1521.	no
Auth Type	The type of account you want Tenable to use to access the database instance: • **SYSDBA** • **SYSOPER** • **NORMAL**	no
Service Type	The Oracle parameter you want to use to specify the database instance: **SID** or **SERVICE_NAME**.	no
Service	The SID value or SERVICE_NAME value for your database instance. The **Service** value you enter must match your parameter selection for the **Service Type** option.	yes

15. Click **Save**.

Verification

1. Click the arrow next to the **Save** button to drop down the launch button.
2. To verify the integration is working, click the **Launch** button to initiate an on-demand scan.
3. After the scan completes, click the scan to view the results.