



Tenable and WALLIX Bastion Integration Guide

Last Revised: October 06, 2023



Table of Contents

Welcome to Tenable for WALLIX Bastion PAM	3
Windows Integration	4
SSH Integration with Privilege Escalation option	9
Database Integration	15



Welcome to Tenable for WALLIX Bastion PAM

This document provides information and steps for integrating Tenable Vulnerability Management, Tenable Nessus Manager, or Tenable Security Center 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 Vulnerability Management or Tenable 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 Vulnerability Management functions or installing and/or launching Tenable Vulnerability Management, see the [Tenable Vulnerability Management User Guide](#).

For information on Tenable Nessus Manager functions or installing and/or launching Tenable Nessus, see the [Tenable Nessus User Guide](#).

For information on Tenable Security Center functions or installing and/or launching Tenable Security Center, see the [Tenable Security Center 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 Vulnerability Management User Guide](#).

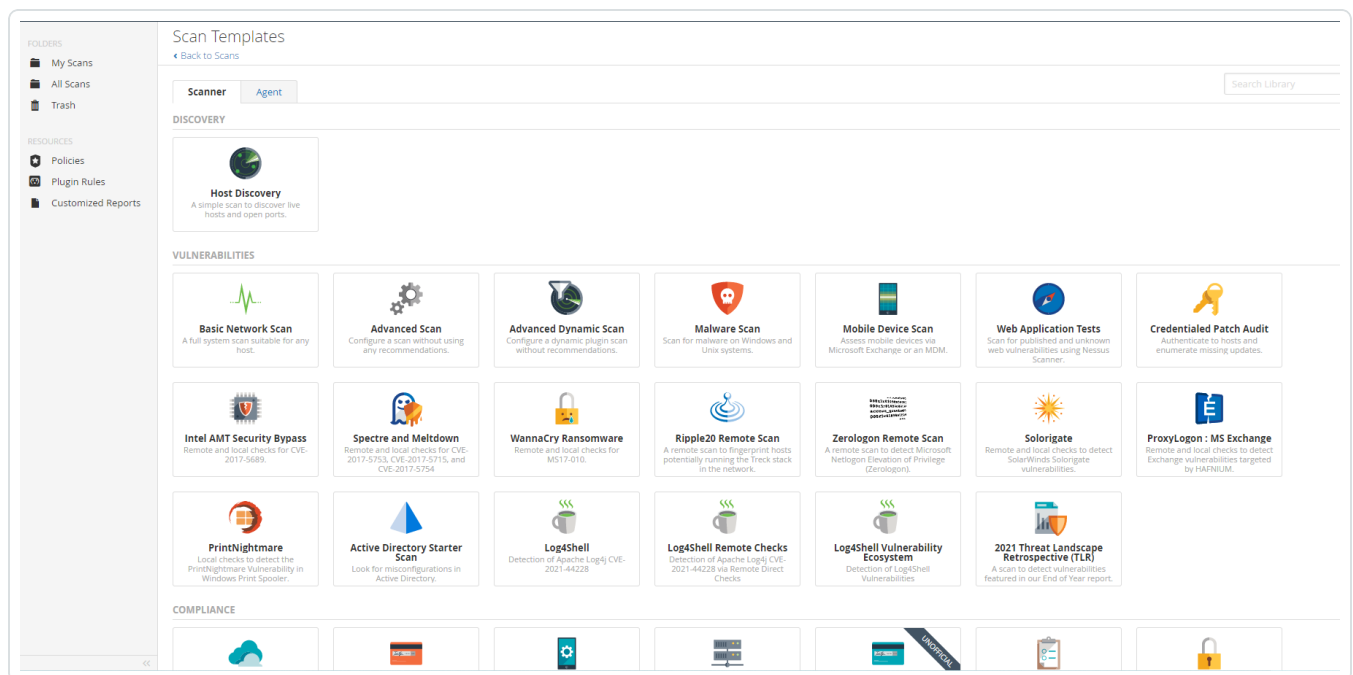
Requirements:

- WALLIX Bastion account
- Tenable Vulnerability Management or Tenable 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.



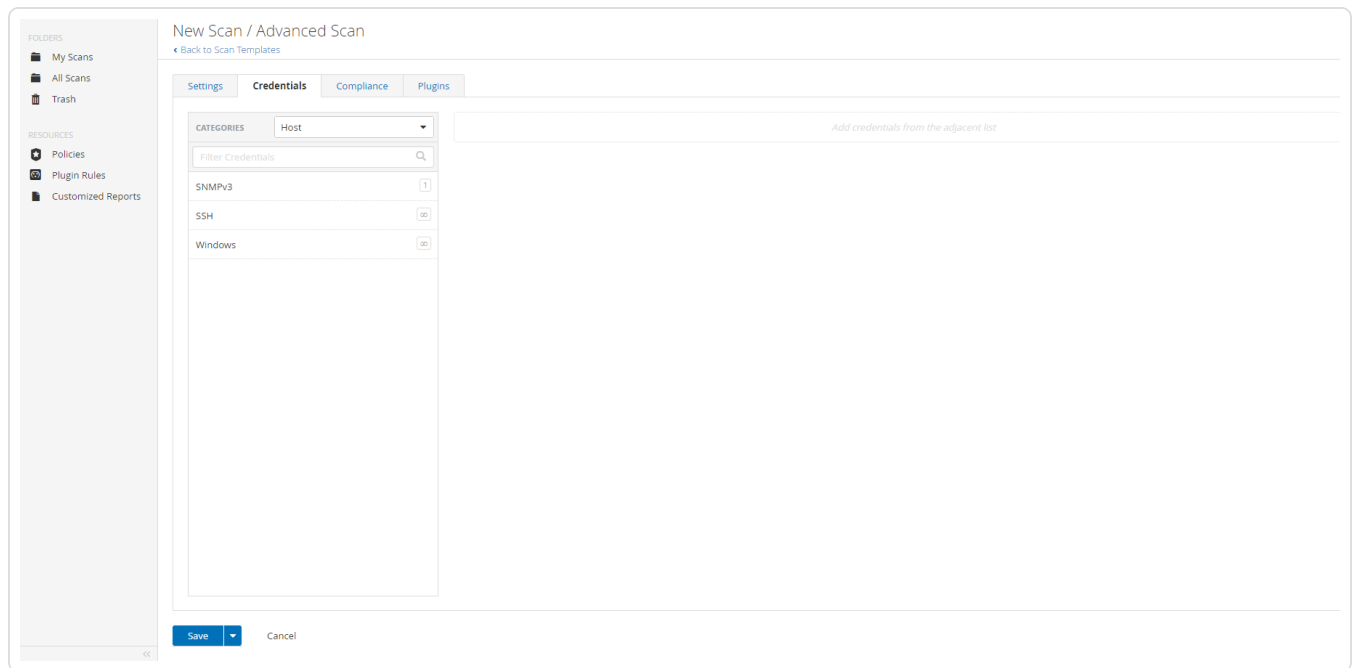
4. Select **Advanced Scan**.



The selected scan template appears.

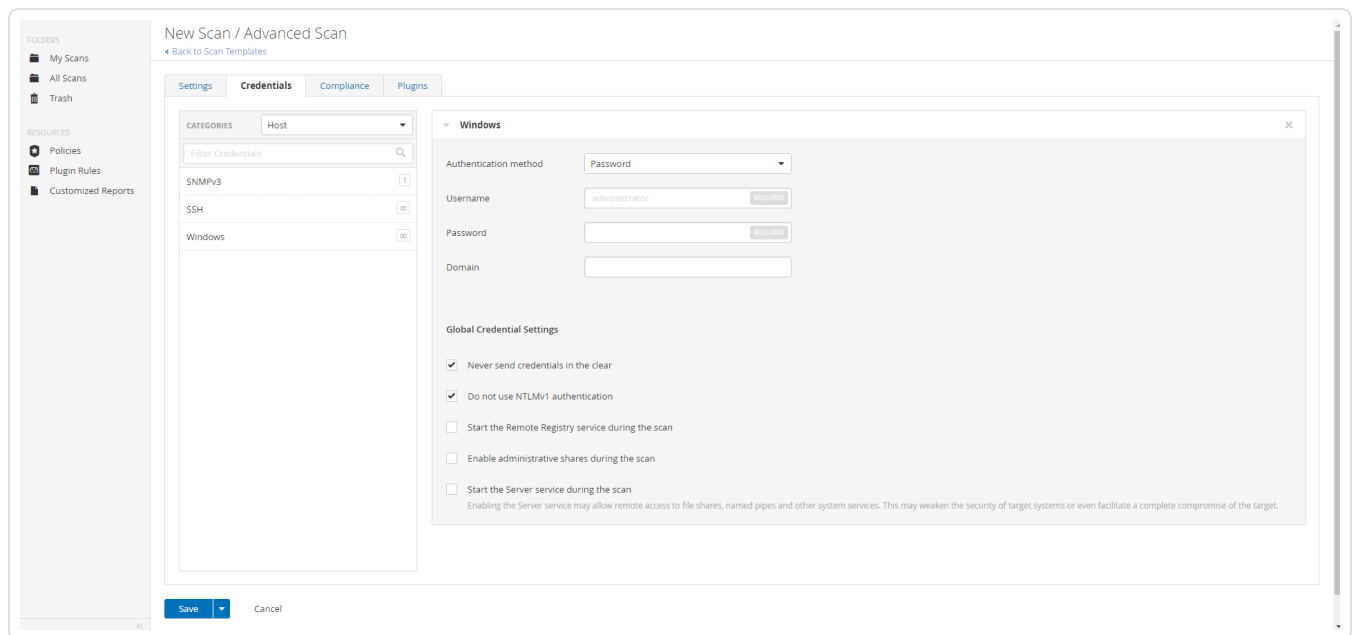
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

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.

New Scan / Advanced Scan
 < Back to Scan Templates

Settings **Credentials** Compliance Plugins

CATEGORIES Host

Filter Credentials

SNMPv3 1

SSH 10

Windows 10

Windows

Authentication method: Wallix Bastion

Wallix Host: [text input]

Wallix Port: [text input]

Authentication Type: [dropdown menu]

Wallix User: [text input]

Wallix Password: [text input]

Get Credential by Device Account Name: [text input]

HTTPS: ☒

Verify SSL certificate: ☐

Global Credential Settings

☒ Never send credentials in the clear

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, Tenable 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	yes



Option	Description	Required
	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	<p>The account name associated with a Device you want to log in to the target systems with.</p> <div>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.</div>	Required only if you have a target and/or device with multiple accounts.
HTTPS	<p>This is enabled by default.</p> <div>Caution: The integration fails if you disable HTTPS.</div>	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](#), the [Tenable Vulnerability Management User Guide](#), or the [Tenable Security Center User Guide](#).

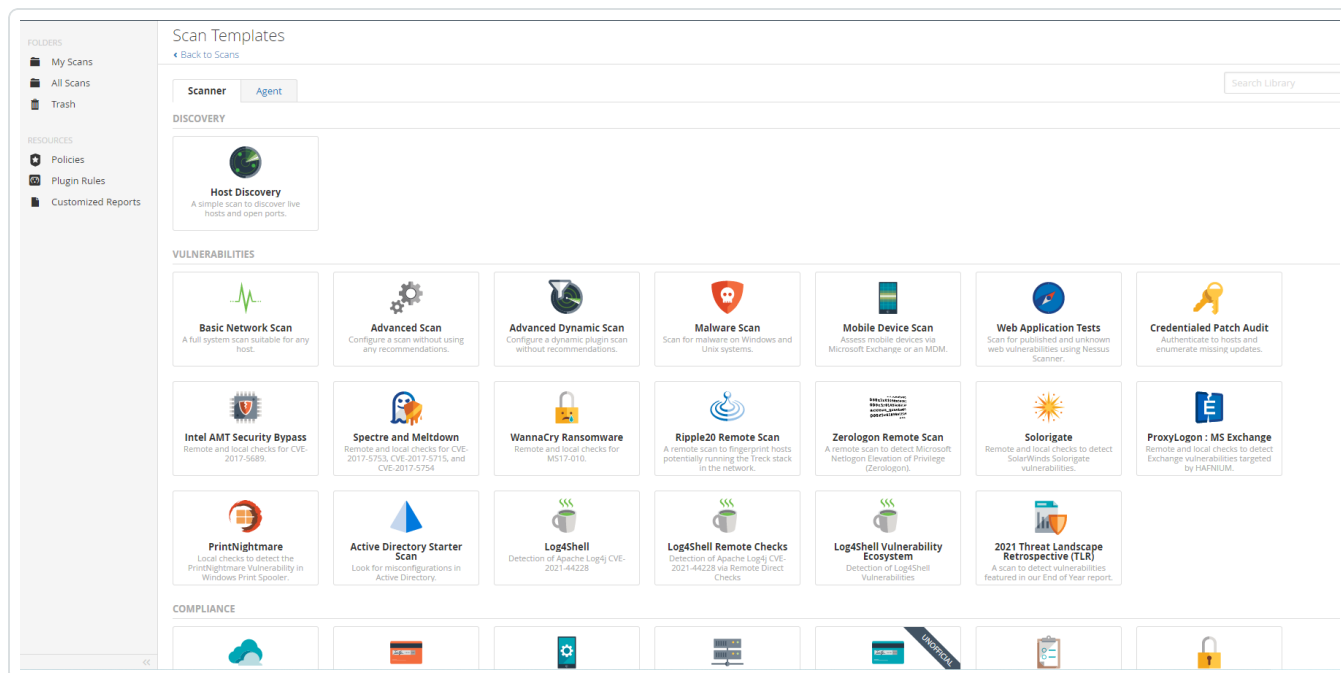
Requirements:

- WALLIX Bastion account
- Tenable Vulnerability Management or Tenable 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.



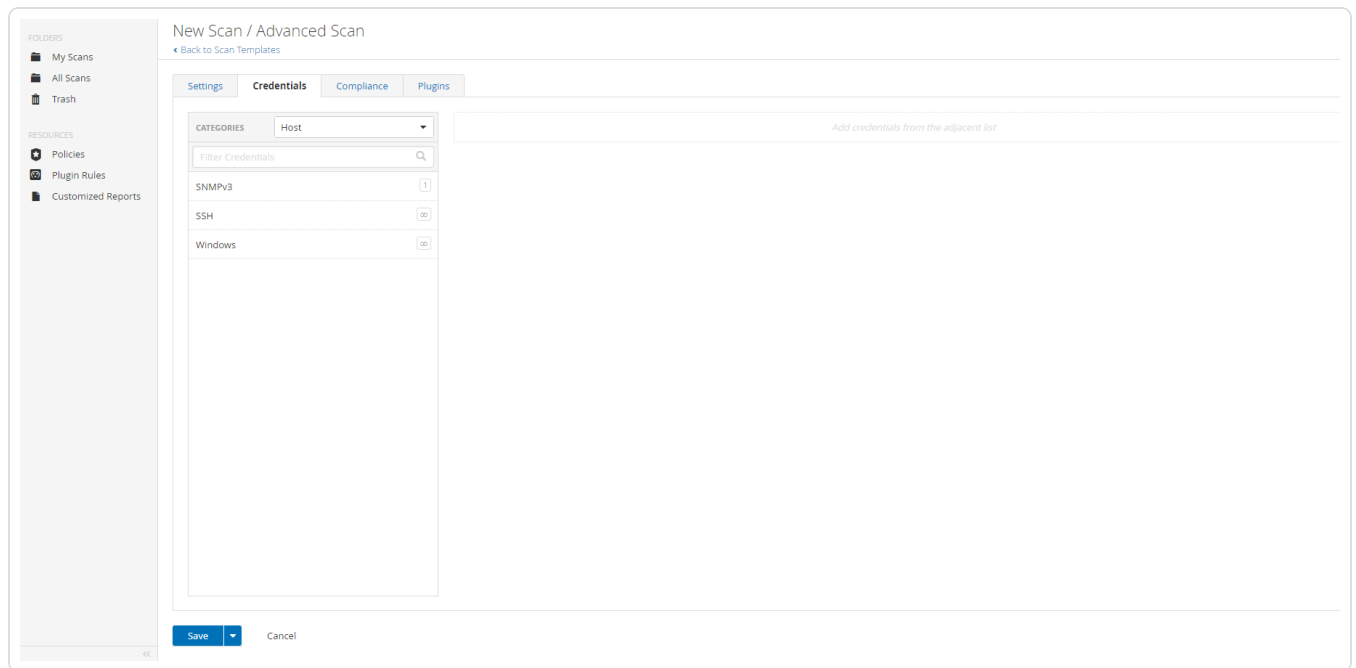
4. Select **Advanced Scan**.



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.

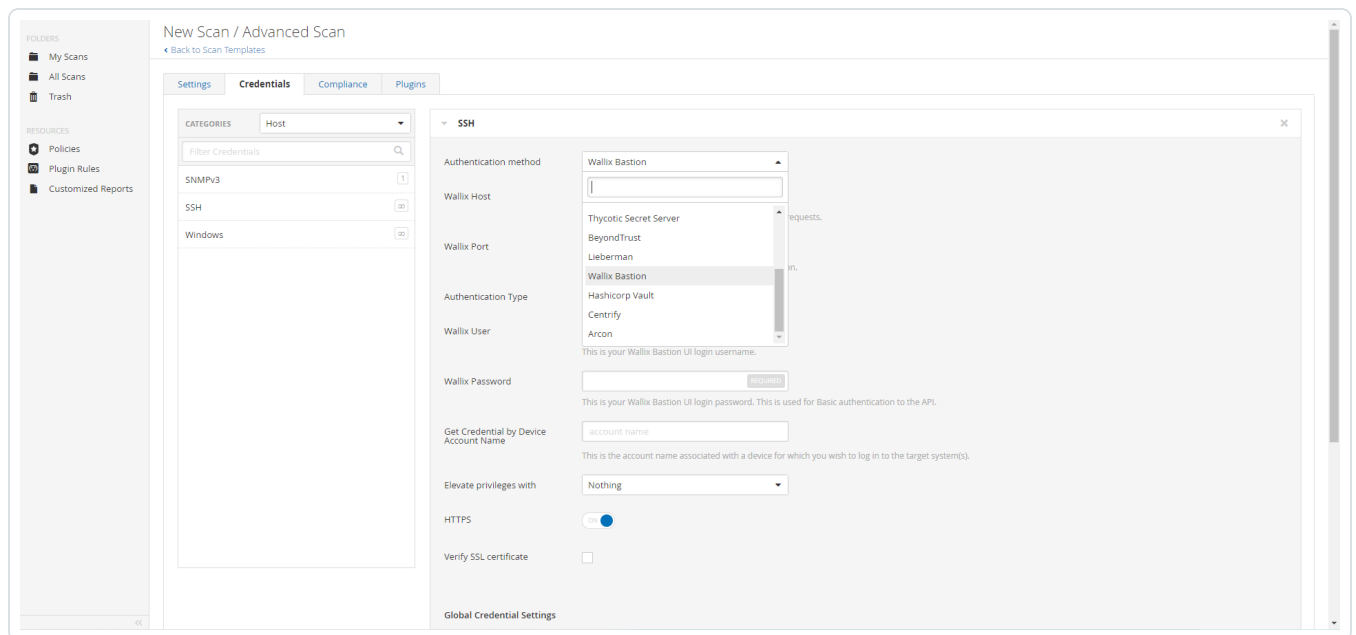


9. In the left-hand menu, select **SSH**.

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, Tenable 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	<p>The account name associated with a Device you want to log in to the target systems with.</p> <div>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.</div>	Required only if you have a target and/or device with multiple accounts.
Elevate privileges	This enables WALLIX Bastion Privileged	Required if you



Option	Description	Required
with	<p>Access Management (PAM). Use the drop-down menu to select the privilege elevation method. To bypass this function, leave this field set to Nothing.</p> <div>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.</div> <div>Note: Multiple options for privilege escalation are supported, including <i>su</i>, <i>su+sudo</i> and <i>sudo</i>. 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.</div> <div>Note: For more information about supported privilege escalation types and their accompanying fields, see the Tenable Nessus User Guide, Tenable Vulnerability Management User Guide, or the Tenable Security Center User Guide.</div>	wish to escalate privileges.
HTTPS	<p>This is enabled by default.</p> <div>Caution: The integration fails if you disable HTTPS.</div>	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 Vulnerability Management User Guide](#).

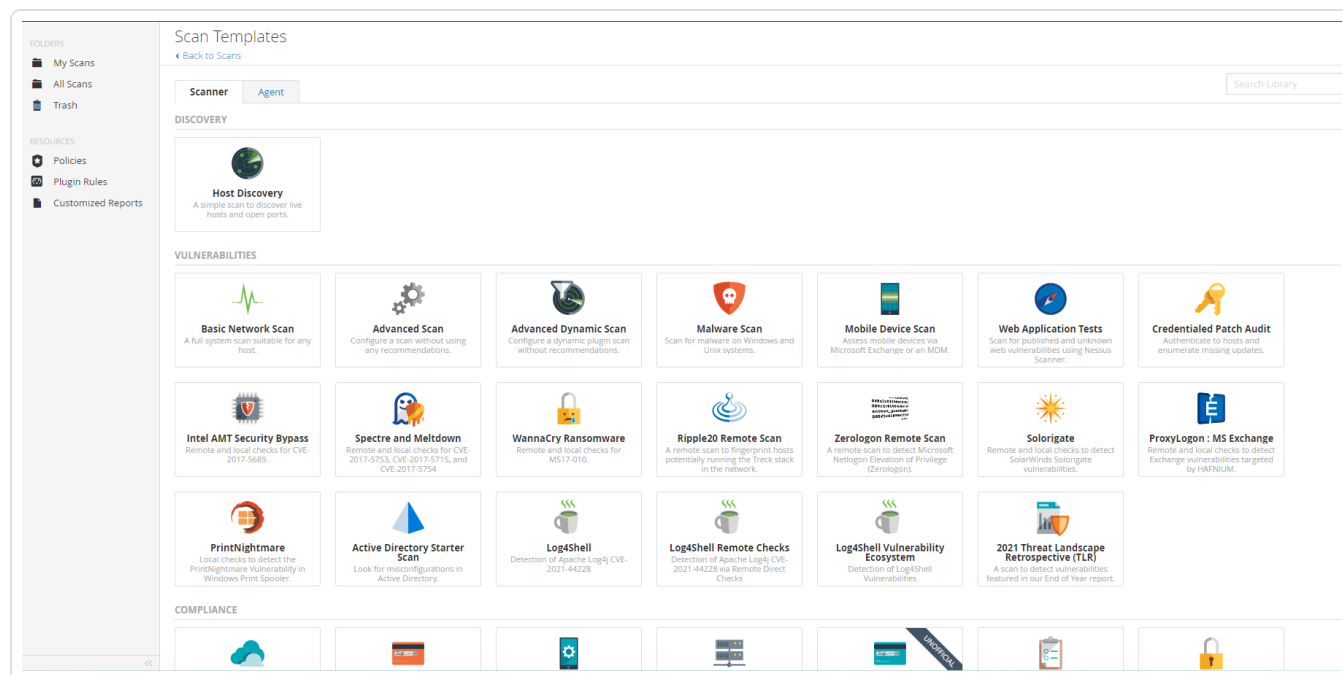
Requirements:

- WALLIX Bastion account
- Tenable Vulnerability Management or Tenable 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.



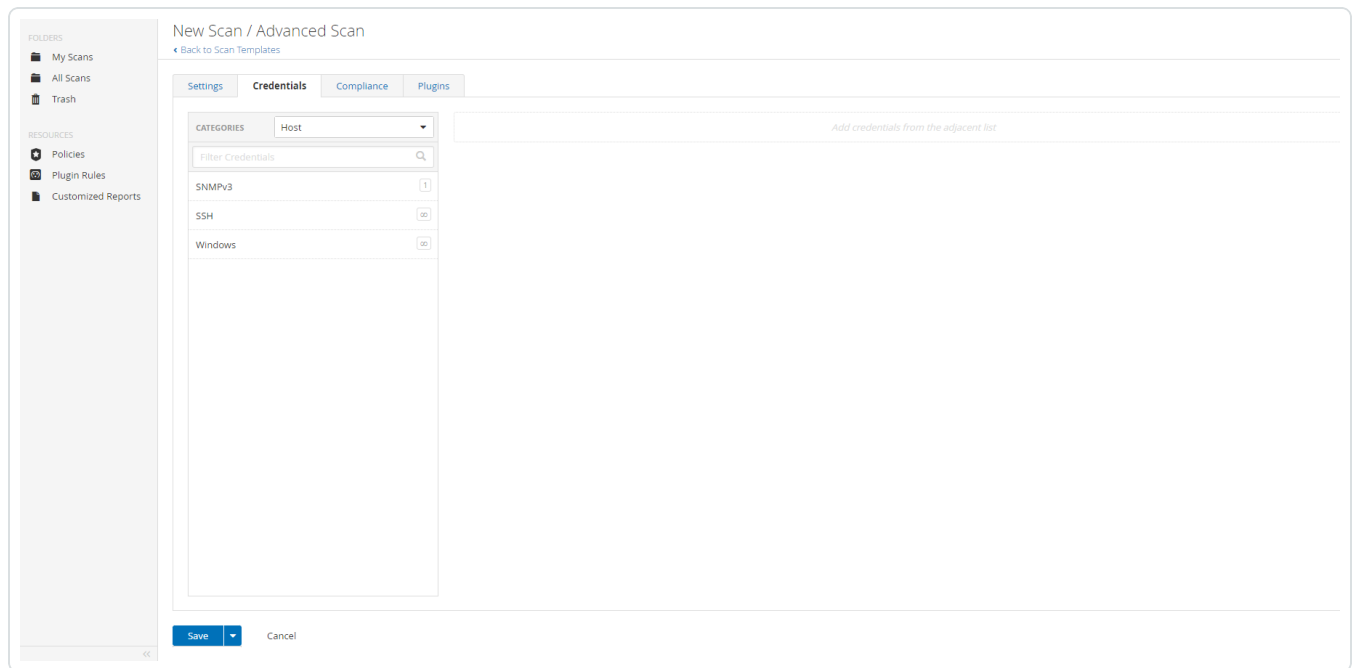
4. Select **Advanced Scan**.



The selected scan template appears.

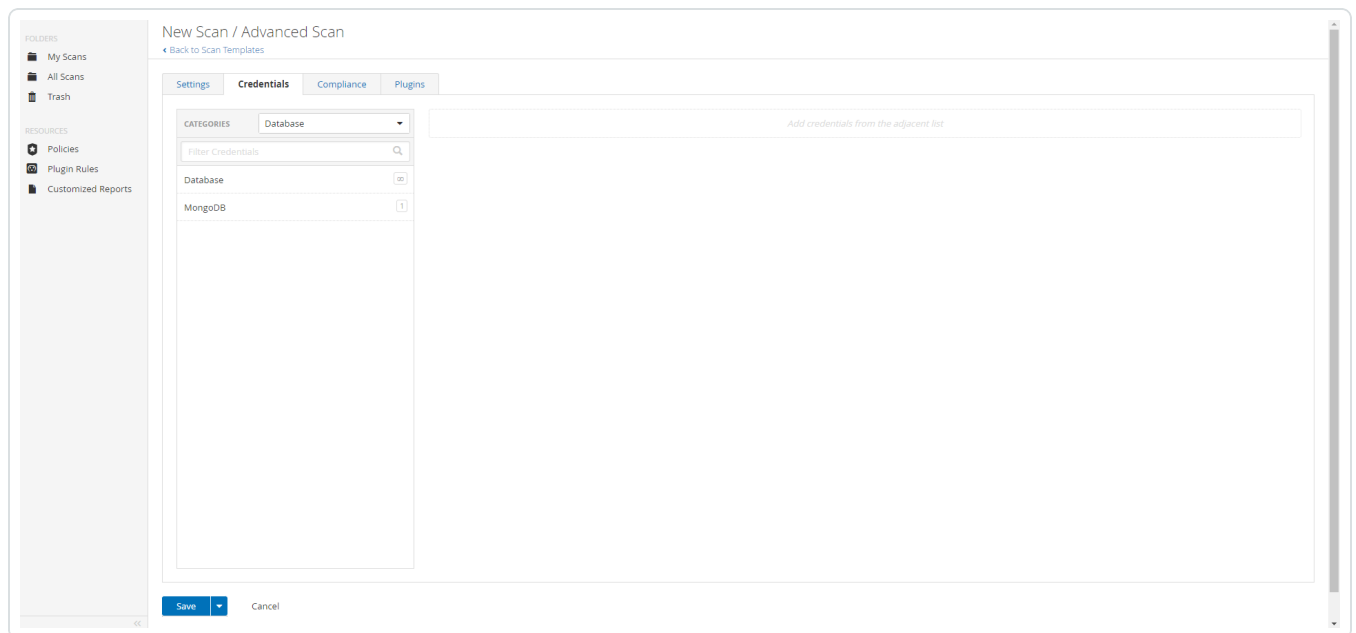
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

The **Credentials** options appear.



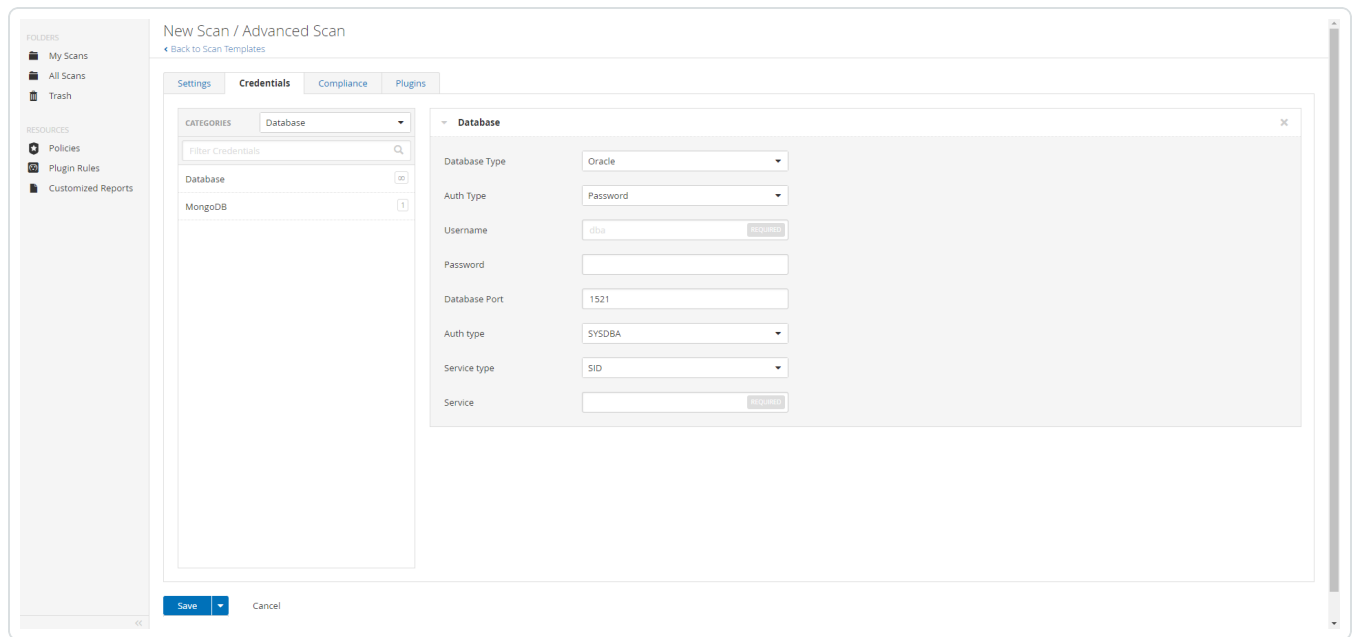
9. In the **Categories** drop-down box, select **Database**.

The **Database** options appear.



10. Click **Database**.

The **Database** options appear.



The screenshot shows the 'New Scan / Advanced Scan' interface. On the left is a sidebar with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports). The main area has tabs for 'Settings', 'Credentials', 'Compliance', and 'Plugins'. The 'Database' configuration window is open, showing a list of categories on the left with 'Database' selected. The 'Database' field is highlighted. The right pane shows the configuration for the selected database type, which is currently set to 'Oracle'.

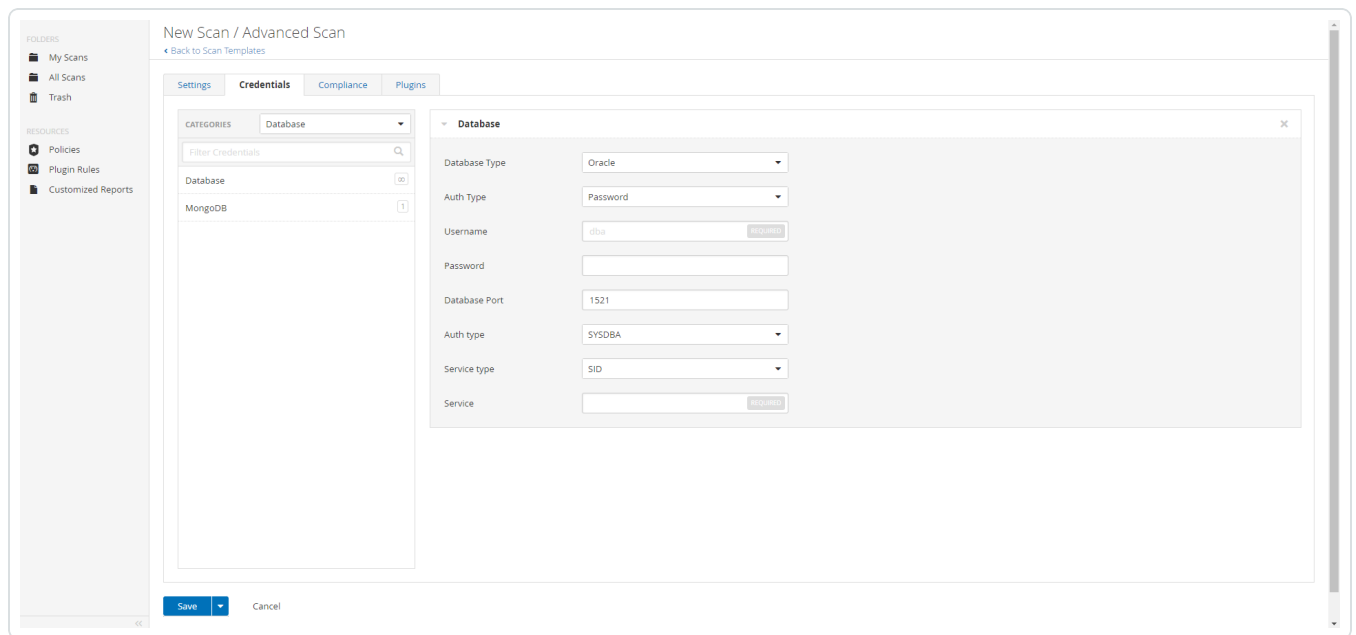
Database Configuration Fields:

- Database Type: Oracle
- Auth Type: Password
- Username: dba
- Password:
- Database Port: 1521
- Auth type: SYSDBA
- Service type: SID
- Service:

Buttons: Save, Cancel

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

The **Database** field options appear.



This screenshot is identical to the previous one, showing the 'Database' configuration window. The 'Database Type' is set to 'Oracle'. The 'Database' field is highlighted in the left pane, and the right pane shows the configuration for the selected database type.

Database Configuration Fields:

- Database Type: Oracle
- Auth Type: Password
- Username: dba
- Password:
- Database Port: 1521
- Auth type: SYSDBA
- Service type: SID
- Service:

Buttons: Save, Cancel

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

NEW Scan / Advanced Scan

← Back to Scan Templates

Settings Credentials Compliance Plugins

CATEGORIES Database

Filter Credentials

Database

MongoDB

SSH

Database

Database Type Oracle

Auth Type Password

Username dba

Password

Database Port 1521

Auth type SYSDBA

Service type SID

Service

Save Cancel

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

The **Wallix Bastion** field options appear.

NEW Scan / Advanced Scan

← Back to Scan Templates

Settings Credentials Compliance Plugins

CATEGORIES Database

Filter Credentials

Database

MongoDB

SSH

Authentication method Wallix Bastion

Wallix Host

Wallix Port

Authentication Type

Wallix User

Wallix Password

Get Credential by Device Account Name

Elevate privileges with Nothing

HTTPS

Verify SSL certificate

Global Credential Settings

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

Option	Description	Required
Wallix Host	The IP address for the WALLIX Bastion	yes



Option	Description	Required
	host.	
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	<p>The account name associated with a Device you want to log in to the target systems with.</p> <div>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.</div>	Required only if you have a target and/or device with multiple accounts.
HTTPS	This is enabled by default.	yes



Option	Description	Required
	Caution: The integration fails if you disable HTTPS .	
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: <ul style="list-style-type: none">• 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.