

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

- Ø

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 <u>Tenable Vulnerability Management User Guide</u>.

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

For information on Tenable Security Center functions or installing and/or launching Tenable Security Center, see the <u>Tenable Security Center User Guide</u>.

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 <u>Nessus User Guide</u>. and the <u>Tenable Vulnerability</u> <u>Management User Guide</u>.

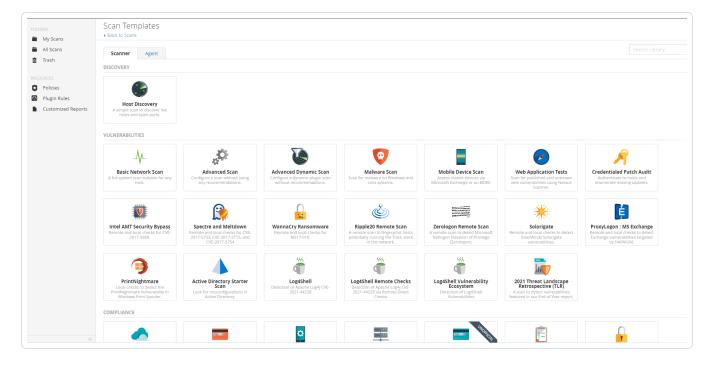
Requirements:

- 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.

All Scans	Settings	Credentials	Compliance Plugins	
Trash	BASIC	~	General Settings	
Policies	 General Schedule 		Name	(RQUIRD)
Plugin Rules Customized Reports	Notificatio		Description	
	Permissio	ns		
	ASSESSMENT		Folder	My Scans 💌
	REPORT		Targets	Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
			Upload Targets	Add File
			Post-Processing Show Dashboard Enabling this option will show	v a dashboard as the default landing page of this scan.
	Save 🔻	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 options appear.

	New Scan / Advanced Scan « Back to Scan Templates								
All Scans Trash	Settings Credentials Compliance Pluging	5							
	CATEGORIES Host -								
olicies	Filter Credentials Q								
lugin Rules Sustomized Reports	SNMPv3								
	SSH								
	Windows								

2

9. In the Host section, click Windows.

The selected credential options appear.

h	Settings Credentials Compliance Plugin	5
	CATEGORIES Host •	 Windows
les	Filter Credentials Q	Authentication method Password
n Rules omized Reports	SNMPv3	Username administrator
	SSH	
	Windows	Password request
		Domain
		Global Credential Settings
		Never send credentials in the clear
		O not use NTUM/1 authentication
		Start the Remote Registry service during the scan
		Enable administrative shares during the scan
		Start the Server service during the scan Enabling the Server service may allow remote access to file shares, named pipes and other system services. This may weaken the security of target systems or even facilitate a complete compromise of the target.
		ставий по восто по тај вали селаке воски на напоч напов раск ила нако тик тај новен на сокиј от ведо фолти и со пошаке а опфиси опфицио и не ведо

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

The Wallix Bastion options appear.

				- 0
FOLDERS	New Scan / Advanced Scan < Back to Scan Templates			
 All Scans Trash 	Settings Credentials Complia	nce Plugins		
	CATEGORIES Host	•	- Windows	x
Policies Plugin Rules		٩	Authentication method	Wallix Bastion
Customized Reports	SNMPv3 SSH		Wallix Host	
	Windows		Wallix Port	Thycotic Server equests. BeyondTrust Lieberman
			Authentication Type	Wallix Bastion P. Hashicory Vault Centrify
			Wallix User	Arcon This is your Wallix Bastion UI login username.
			Wallix Password	This is your Walk Bastion UI login password. This is used for Basic authentication to the API.
			Get Credential by Device Account Name	account name This is the account name associated with a device for which you wish to log in to the target system(s).
			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	The account name associated with a Device you want to log in to the target systems with.	Required only if you have a target and/or device 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.	multiple accounts.
HTTPS	This is enabled by default.	yes
	Caution: The integration fails if you disable HTTPS .	
Verify SSL Certificate	This is disabled by default and unsupported in WALLIX Bastion PAM integrations.	no

O

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 <u>Nessus User Guide</u>, the <u>Tenable Vulnerability</u> Management User Guide, or the <u>Tenable Security Center User Guide</u>.

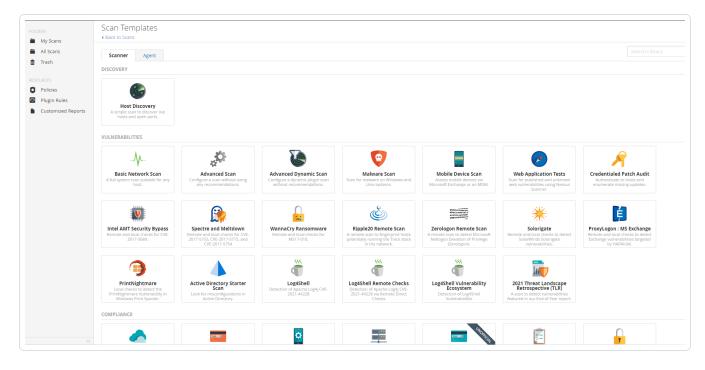
Requirements:

- 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.

My Scans All Scans	Back to Scan Templates Settings Credenti	ials Compliance Plugin	ns
Trash	BASIC	General Settings	
Policies Plugin Rules	General Schedule	Name	more the second s
Customized Reports	Notifications Permissions	Description	
	DISCOVERY >	Folder	My Scans 👻
	REPORT >	Targets	Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
		Upload Targets	Add File
		Post-Processing Show Dashboard Enabling this option will s	show a dashboard as the default landing page of this scan.
	Save 🔻 Cance	21	

0

- 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.

RS My Scans	New Scan / Advanced Scan « Back to Scan Templates	
All Scans Trash	Settings Credentials Compliance Plugins	
	CATEGORIES Host 👻	
Policies	Filter Credentials Q	
Plugin Rules Customized Reports	SNMPv3	
	SSH @	
	Windows	

n

- 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.

My Scans	< Back to Scan					
All Scans Trash	Settings	Credentials	Compliance	Plugins		
	CATEGORIE	s Host		-	✓ SSH	×
Policies					5511	n
Plugin Rules				Q	Authentication method	Wallix Bastion
Customized Reports	SNMPv3				Wallix Host	
	SSH			00	Wallix Host	Thycotic Secret Server equests.
	Windows			8	Malla David	Beyond Trust
					Wallix Port	Liebermanin.
						Wallix Bastion
					Authentication Type	Hashicorp Vault Centrify
					Wallix User	Arcon
						This is your Wallix Bastion UI login username.
					Wallix Password	REQ.(IND)
						This is your Wallix Bastion UI login password. This is used for Basic authentication to the API.
					Get Credential by Device Account Name	
					Account Name	This is the account name associated with a device for which you wish to log in to the target system(s).
					Elevate privileges with	Nothing
					HTTPS	
					Verify SSL certificate	

12. Configure each field for $\ensuremath{\textbf{SSH}}$ 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	The account name associated with a Device you want to log in to the target systems with.	Required only if you have a target and/or
	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.	device with multiple accounts.
Elevate privileges	This enables WALLIX Bastion Privileged	Required if you

- Ø -

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

	O	
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 <u>Nessus User Guide</u> and the <u>Tenable Vulnerability</u> <u>Management User Guide</u>.

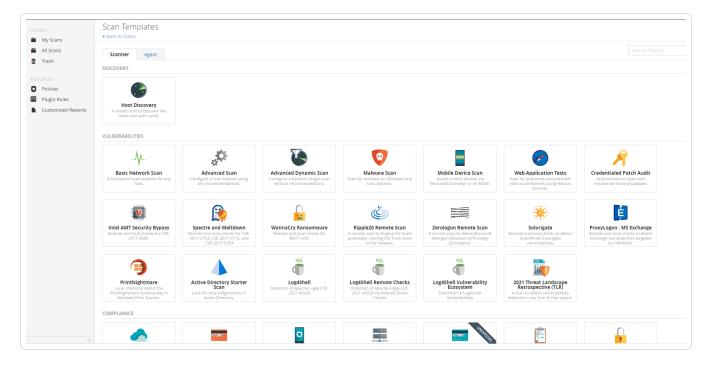
Requirements:

- 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.

All Scans Trash	Settings	Credentials	Compliance Plugins	
	BASIC	~	Convert Contriner	
JRCES Policies	General		General Settings	
Plugin Rules	Schedule		Name	
Customized Reports	Notificati	ons	Description	
	Permissio	ons		
	DISCOVERY		Falila	My Scans 💌
	ASSESSMENT		Folder	Ny Julis
	ADVANCED		Targets	Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
			Upload Targets	Add File
			Post-Processing Show Dashboard Enabling this option will sho	ow a dashboard as the default landing page of this scan.
	Save 🔻	Cancel		

0

- 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.

/ Scans	New Scan / Advanced Scan « Back to Scan Templates	
Scans	Settings Credentials Compliance Plugins	
	CATEGORIES Host •	
licies	Filter Credentials	
igin Rules stomized Reports	SNMPv3	
	SSH	
	Windows	

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

The **Database** options appear.

Settings Cre	dentials Compliance	Plugins	
CATEGORIES	Database	•	
		Q	
Database			
MongoDB			

10. Click Database.

The Database options appear.

icans	Settings Credentials Compliance	Plugin			
h :	CATEGORIES Database	-	- Database		
ies		Q	Database Type	Oracle •	
in Rules omized Reports	Database				
connector responde	MongoDB		Auth Type	Password •	
			Username	dba Retrained	
			Password		
			Database Port	1521	
			Auth type	SYSDBA	
			Service type	SID ·	
			Service	accura	

m

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

The **Database** field options appear.

l Scans ash	Settings	Credentials	Compliance	Plugins				
	CATEGORIE	Database	2	•	 Database 			×
icies gin Rules				Q,	Database Type	Oracle		
tomized Reports	Database			00	Auth Type	Password	•	
	MongoDB							
					Username		REQUIRED	
					Password			
					Database Port	1521		
					Auth type	SYSDBA	•	
					Service type	SID	v	
					Service		REQUIRED	

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

cans							
1	Settings C	redentials	Compliance	Plugins			
	CATEGORIES	Database		•	> SSH		
ies n Rules				Q,	- Database		
omized Reports	Database			00			
	MongoDB				Database Type	Oracle 🔹	
					Auth Type	Password •	
					Username		
					Password		
					Database Port	1521	
					Auth type	SYSDBA 🗸	
					Service type	SID •	
					Service		

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

The Wallix Bastion field options appear.

My Scans All Scans	< Back to Scan T Settings	Credentials	Compliance	Plugins		
📋 Trash	Secongs	credentiuis	compliance	riugins		
	CATEGORIE	5 Database		•	- SSH	x
Policies				Q	Authentication method	Wallix Bastion
Plugin Rules Customized Reports	Database			00	Autoritication method	
Customized Reports	MongoDB				Wallix Host	
					Wallix Port	Thycotic Server expension BeyondTrust Lieberman
						Wallix Bastion
					Authentication Type	Hashicorp Vault
					Wallix User	Centrify Arcon
						This is your Wallix Bastion UI login username.
					Wallix Password	REQUISID
						This is your Wallix Bastion UI login password. This is used for Basic authentication to the API.
					Get Credential by Device Account Name	
						This is the account name associated with a device for which you wish to log in to the target system(s).
					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	The account name associated with a Device you want to log in to the target systems with.	Required only if you have a target and/or device 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.	multiple accounts.	
HTTPS	This is enabled by default.	yes	

- 0

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: • 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

O

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.