Tenable and HashiCorp Vault Integration Guide

Last Revised: January 10, 2024

Copyright © 2024 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to Tenable for HashiCorp Vault

This document provides information and steps for integrating Tenable applications with HashiCorp Vault.

Integrating Tenable applications with HashiCorp Vault provides security administrators with options to secure and tightly control access to tokens, passwords, certificates, and encryption keys for protecting machines, applications and sensitive data using the user interface, CLI, or HTTP API.

You can integrate HashiCorp Vault with Tenable Vulnerability Management, Tenable Nessus, or Tenable Security Center.

The benefits of integrating Tenable applications with HashiCorp Vault include:

- Central management of secrets to reduce secrets sprawl
- Access management to secrets in a multi-cloud world
- A streamline of the lifecycle of secrets making them easier to consume through various strategies

For additional information about HashiCorp Vault, see the Hashicorp website.

Requirements

To properly integrate Tenable with HashiCorp Vault you must meet the following requirements.

Tenable Product

You must have an active account for at least one of the following Tenable products to integrate with HashiCorp Vault: Tenable Vulnerability Management, Tenable Security Center, or Tenable Nessus Manager.

Tenable Role

You must have the appropriate role for your Tenable account as listed below.

Tenable Vulnerability Management - Standard, Scan Manager, Administrator, or System Administrator

Tenable Security Center - Any

Tenable Nessus Manager - Standard, Administrator, or System Administrator

HashiCorp Vault Requirements

You must have an active HashiCorp Vault account. To create a HashiCorp Vault account, use the following steps.

1. Install HashiCorp Vault.
2. Start your HashiCorp Vault server.
3. Create a Secret.
4. Authenticate HashiCorp Vault.
5. Deploy HashiCorp Vault.

API Requirements

Required User Role: Standard, Scan Manager, or Administrator

Hashicorp requires API URLs to be formatted in a specific way. The URL must start with `/v1/` and not end with a `/`.

Refer to the following table for examples.

URL Type	Description	Required
KV1 Engine URL	(KV1) The URL HashiCorp Vault uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL HashiCorp Vault uses to access the KV2 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL HashiCorp Vault uses to access the active directory engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the AD **Vault Type**

Nessus for HashiCorp Vault

View the corresponding section to configure your Tenable Nessus application with Hashicorp Vault.

Configure Tenable Nessus Manager with HashiCorp Vault (Windows and SSH)

Configure Tenable Nessus Manager with HashiCorp Vault (Database)

Configure Tenable Nessus Manager with IBM DataPower Gateway

Configure Tenable Nessus Manager with HashiCorp Vault (Windows and SSH)

Required User Role: Standard, Scan Manager, or Administrator

In Tenable Nessus Manager, you can integrate with HashiCorp Vault using Windows or SSH credentials. Complete the following steps to configure Tenable Nessus Manager with HashiCorp Vault using these credentials.

Before you begin:

- Ensure you have both a Tenable Nessus Manager and HashiCorp Vault account.

To integrate Tenable Nessus Manager with HashiCorp Vault using Windows or SSH credentials:

1. Log in to Tenable Nessus Manager.
2. Click **Scans**.

   The **My Scans** page appears.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.
4. Select a scan template.

   The selected scan template **Settings** 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. By default, the **Categories** drop-down box displays **Host**.
9. In the **Categories** drop-down, click **Host**.
10. In the **Categories** list, click your preferred **Host** configuration: **Windows** or **SSH**.

The selected configuration options appear.

11. In the selected configuration window, click the **Authentication method** drop-down box.

    The **Authentication method** options appear.

12. Select **HashiCorp Vault**.

    The **HashiCorp Vault** options for Windows or SSH appear.

13. Configure the credentials.

Windows and SSH Credentials		
Option	Description	Required
Hashicorp Vault host	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Hashicorp Vault port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate**(Required) and **Hashicorp Client Certificate Private Key** (Required) appear. Select the appropriate files for the client certificate and private key.	yes
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault	yes

	when you configured your App Role.	
Authentication URL	The path/subdirectory to the authentication endpoint. This is not the full URL. For example: `/v1/auth/approle/login`	yes
Namespace	The name of a specified team in a multi-team environment.	no
Vault Type	The HashiCorp Vault version: KV1, KV2, AD, or LDAP. For additional information about HashiCorp Vault versions, see the HashiCorp Vault documentation.	yes
KV1 Engine URL	(KV1) The URL HashiCorp Vault uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL HashiCorp Vault uses to access the KV2 engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL HashiCorp Vault uses to access the Active Directory engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the AD **Vault Type**
LDAP Engine URL	(LDAP) The URL HashiCorp Vault uses to access the LDAP engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the LDAP **Vault Type**

Username Source	(KV1 and KV2) A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(KV1 and KV2) The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	(KV1 and KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Domain Key (Windows)	(Required if Kerberos Target Authentication is enabled.) The key name that the domain is stored under in the secret.	yes
Secret Name	(KV1, KV2, and AD) The key secret you want to retrieve values for.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled.) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Domain (Windows)	(Required if Kerberos Target Authentication	yes

	is enabled.) The domain to which Kerberos Target Authentication belongs, if applicable.	
Realm (SSH)	(Required if Kerberos Target Authentication is enabled.) The Realm is the authentication domain, usually noted as the domain name of the target (for example, example.com).	yes
Use SSL	If enabled, Tenable Nessus Manager uses SSL for secure communications. Configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, validates the SSL certificate. Configure SSL in Hashicorp Vault before enabling this option.	no
Enable for HashiCorp Vault	Enables/disables IBM DataPower Gateway use with HashiCorp Vault.	yes
Elevate privileges with (SSH)	Use a privilege escalation method such as su or sudo to use extra privileges when scanning. **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 secret name, and Location of sudo (directory) are provided and can be completed to support authentication and privilege escalation through HashiCorp Vault. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Nessus User	Required if you wish to escalate privileges.

	Guide and the Tenable Vulnerability Management User Guide.	
Escalation account secret name (SSH)	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

14. Click **Save**.

    Tenable Nessus Manager saves the credential.

    The **My Scans** page appears.

What to do next:

Verify the integration is working.

To verify the integration is working:

1. On the **My Scans** page, click the **Launch** button to initiate an on-demand scan.
2. Once the scan completes, select the completed scan and look for the following message:
    - For Windows: *Microsoft Windows SMB Log In Possible: 10394*. This result validates that authentication was successful.
    - For SSH: *Plugin ID 97993 It was possible to log into the remote host via SSH using 'password' authentication*.

Configure Tenable Nessus Manager with HashiCorp Vault (Database)

In Tenable Nessus Manager, you can integrate with HashiCorp Vault using database credentials. Complete the following steps to configure Tenable Nessus Manager with HashiCorp Vault for database credentials. You can Enable Database Plugins in the scanner to display them in the output.

Requirements

Required User Role: Standard, Administrator, or System Administrator

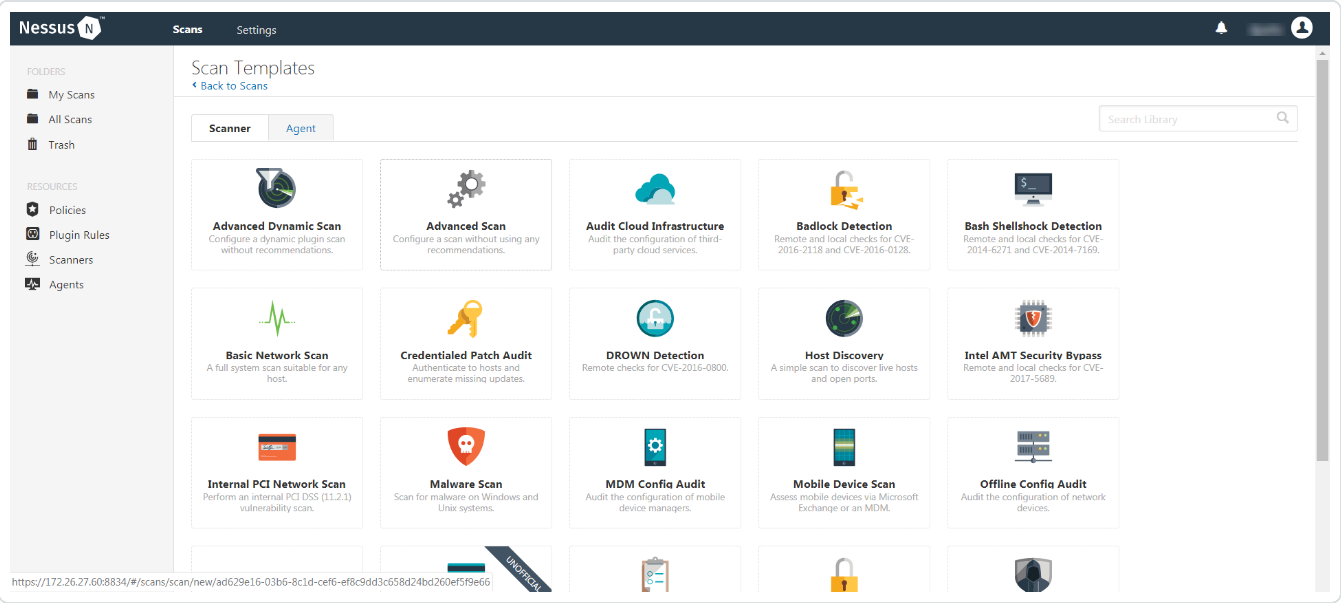
- Tenable Nessus Manager account
- HashiCorp Vault account

To integrate Tenable Nessus Manager with HashiCorp Vault using database credentials:

1. Log in to Tenable Nessus Manager.
2. Click **Scans**.

   The **My Scans** page appears.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.



Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Advanced Scan
Configure a scan without using any recommendations.

Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan
A full system scan suitable for any host.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

DROWN Detection
Remote checks for CVE-2016-0800.

Host Discovery
A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan
Scan for malware on Windows and Unix systems.

MDM Config Audit
Audit the configuration of mobile device managers.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit
Audit the configuration of network devices.

https://172.26.27.60:8834/#/scans/scan/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66

4. Select a scan template.

   The selected scan template **Settings** 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. By default, the **Categories** drop-down box displays **Host**.

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

   The **Database** options appear below.

10. In the **Categories** list, click **Database**.

    The **Database** options appear.

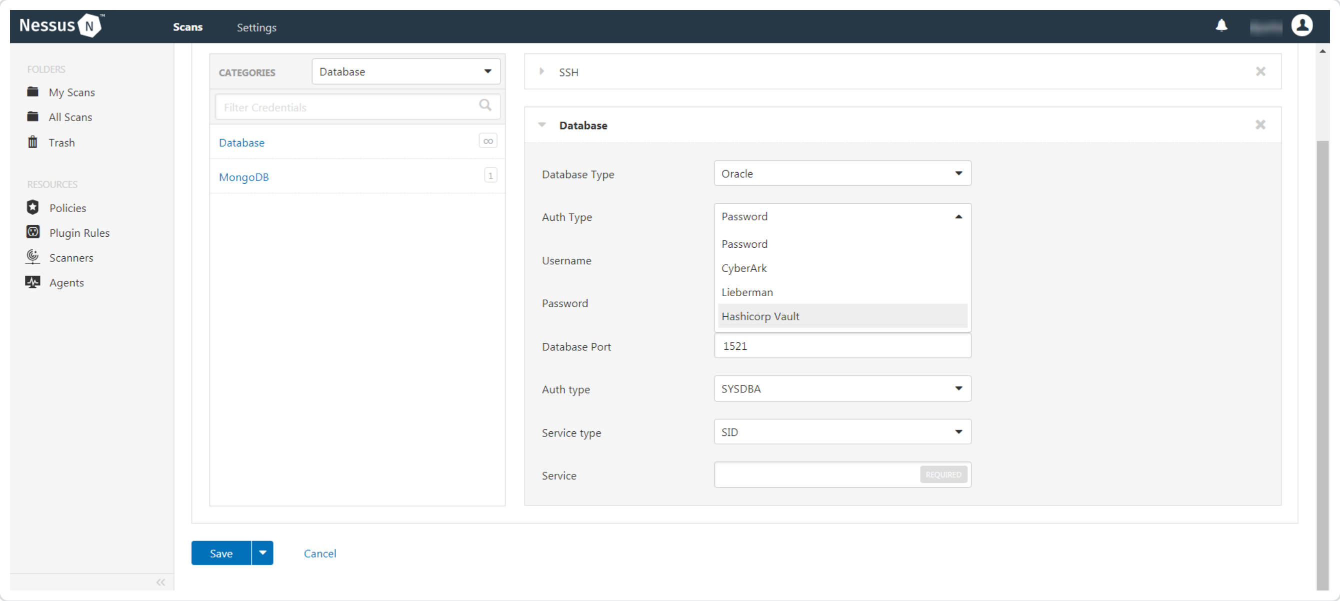
11. In the Database section, click the **Database Type** drop-down box.

    The **Database** options appear.

12. In the **Database Type** drop-down box, click your preferred database: **PostgreSQL**, **DB2**, **MySQL**, **SQL Server**, **Oracle**, or **Sybase ASE**.

The selected **Database** options appear.

13. In the **Auth Type** drop-down box, click **Hashicorp**.



CATEGORIES: Database

Database

Database Type: Oracle

Auth Type: Password
- Password
- CyberArk
- Lieberman
- Hashicorp Vault

Username

Password

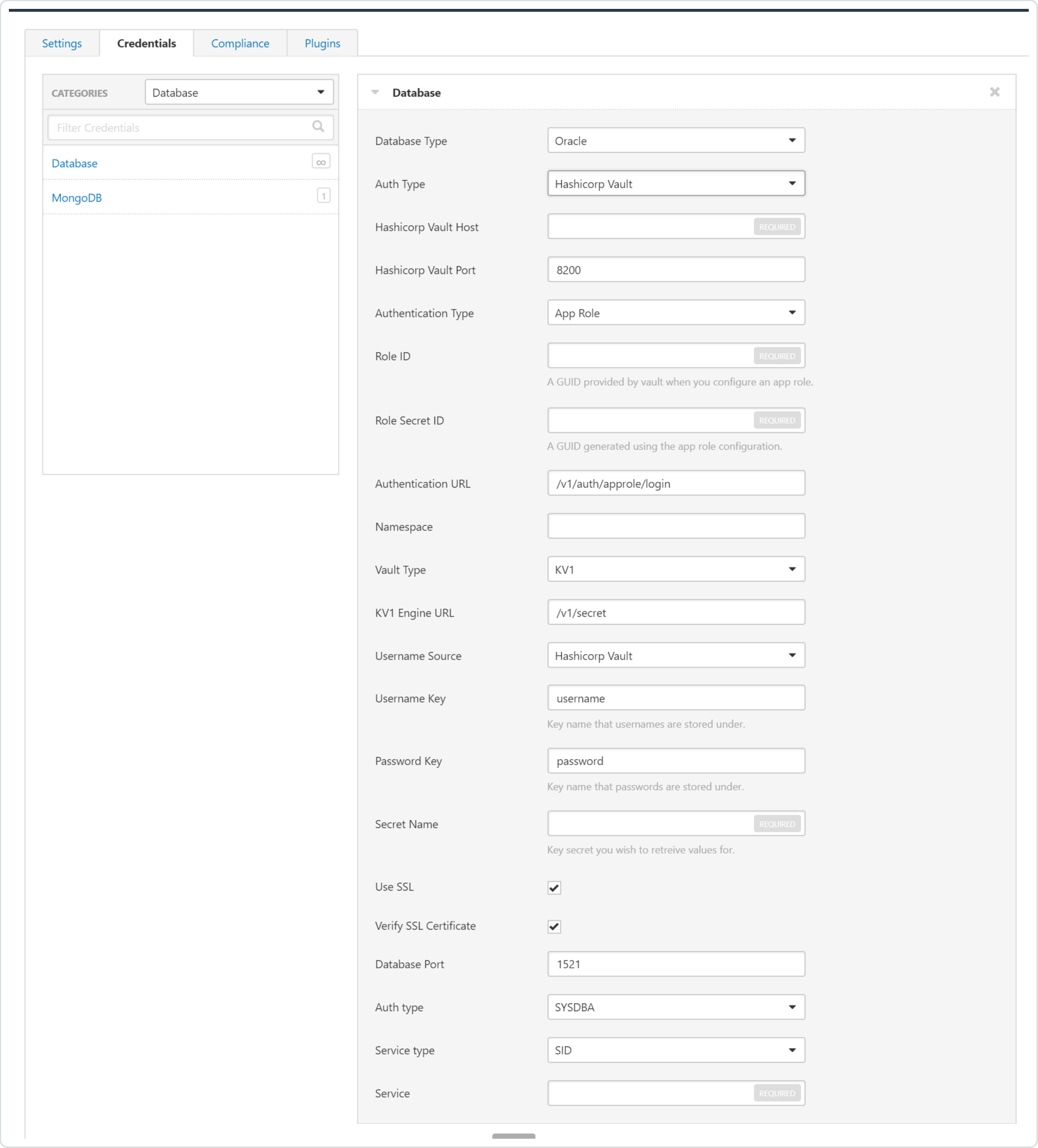
Database Port: 1521

Auth type: SYSDBA

Service type: SID

Service: REQUIRED

The HashiCorp Vault options appear.



Database Type	Oracle
Auth Type	Hashicorp Vault
Hashicorp Vault Host	REQUIRED
Hashicorp Vault Port	8200
Authentication Type	App Role
Role ID	REQUIRED A GUID provided by vault when you configure an app role.
Role Secret ID	REQUIRED A GUID generated using the app role configuration.
Authentication URL	/v1/auth/approle/login
Namespace	
Vault Type	KV1
KV1 Engine URL	/v1/secret
Username Source	Hashicorp Vault
Username Key	username Key name that usernames are stored under.
Password Key	password Key name that passwords are stored under.
Secret Name	REQUIRED Key secret you wish to retreive values for.
Use SSL	☑
Verify SSL Certificate	☑
Database Port	1521
Auth type	SYSDBA
Service type	SID
Service	REQUIRED

14. Configure the **Database** credentials.

Option	Description	Required

Hashicorp Vault host	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Hashicorp Vault port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate** and **Hashicorp Client Certificate Private Key** appear. Select the appropriate files for the client certificate and private key.	yes
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The path/subdirectory to the authentication endpoint. This is not the full URL. For example: `/v1/auth/approle/login`	yes
Namespace	The name of a specified team in a multi-team environment.	no
Vault Type	The HashiCorp Vault version: KV1, KV2, AD, or LDAP. For additional information about HashiCorp Vault versions, see the	yes

	HashiCorp Vault documentation.	
KV1 Engine URL	(KV1) The URL HashiCorp Vault uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL HashiCorp Vault uses to access the KV2 engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL HashiCorp Vault uses to access the active directory engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the AD **Vault Type**
LDAP Engine URL	(LDAP) The URL HashiCorp Vault uses to access the LDAP engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the LDAP **Vault Type**
Username Source	(KV1 and KV2) A drop-down box to specify whether the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(KV1 and KV2) The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	(KV1 and KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	(KV1, KV2, and AD) The key secret you want to retrieve values for.	yes

Use SSL	If enabled, Tenable Nessus Manager uses SSL for secure communications. Configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no
Database Port	The port on which Tenable Nessus Manager communicates with the database.	yes
Auth Type	The authentication method for the database credentials. Oracle values include: • SYSDBA • SYSOPER • NORMAL	yes
Service Type	(Oracle databases only) Valid values include: SID and SERVICE_NAME.	yes
Service	(Oracle database only) A specific field for the configuration for the database.	yes

15. Click **Save**.

Enable Database Plugins

To enable database plugins:

1. In the scan where you configured the Hashicorp credentials, click the **Plugins** tab.

   The **Plugins** section appears.

2. Click the **Status** button.

3. Click **Save**.

   See the chart for database plugin types and corresponding IDs.

Plugin Type	Plugin ID
MSSQL	91827
Oracle	91825
MySQL	91823
PostgresSQL	91826

Configure Tenable Nessus Manager with IBM DataPower Gateway

In Tenable Nessus Manager, you can integrate with HashiCorp Vault using IBM DataPower Gateway credentials. Complete the following steps to configure Tenable Nessus Manager with HashiCorp Vault using these credentials.

Required User Role: Standard, Scan Manager, or Administrator

Before you begin:

- Ensure you have both a Tenable Nessus Manager and HashiCorp Vault account.

To integrate Tenable Nessus Manager with HashiCorp Vault using IBM DataPower Gateway credentials:

1. Log in to Tenable Nessus Manager.
2. Click **Scans**.

   The **My Scans** page appears.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.
4. Select a scan template.

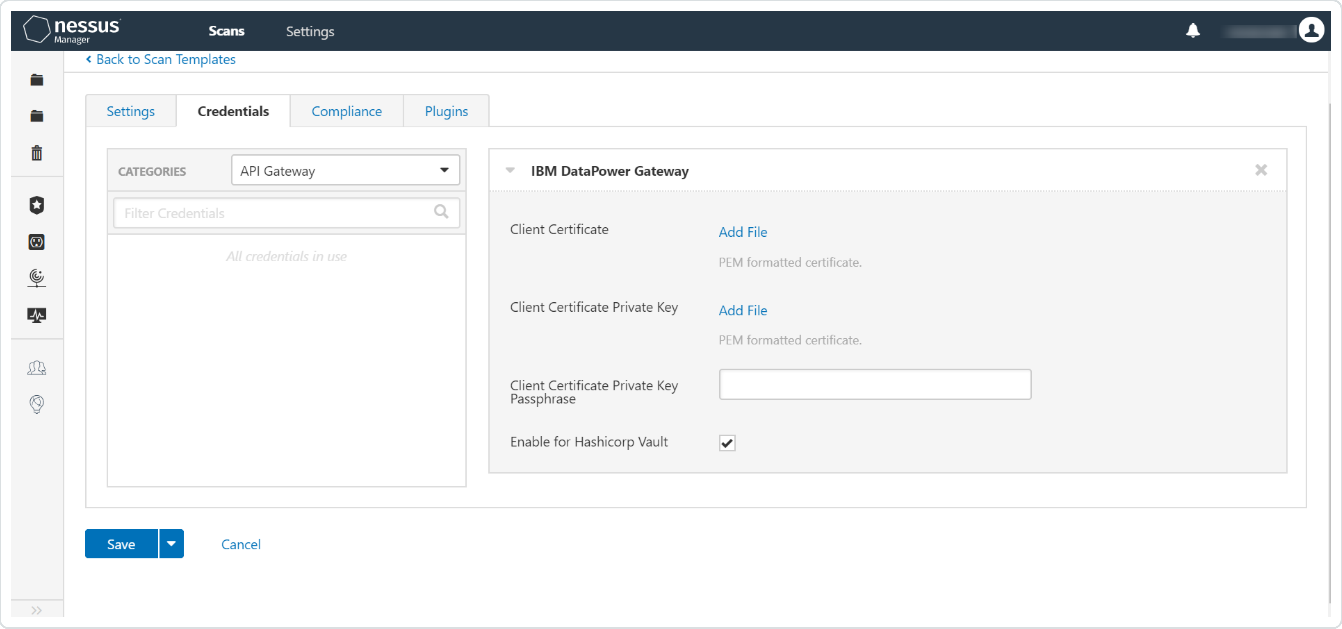
   The selected scan template **Settings** page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a **Description**, **Folder location**, **Scanner location**, and specify **Target groups**.
8. Click the **Credentials** tab.

   The **Credentials** options appear. By default, the **Categories** drop-down box displays **Host**.
9. In the **Categories** drop-down box, select **API Gateway.**

   The **API Gateway** options appear.

10. In the **Categories** list, click **IBM DataPower Gateway**.

    The **IBM DataPower Gateway** options appear.



CATEGORIES: API Gateway

IBM DataPower Gateway

Client Certificate — PEM formatted certificate.

Client Certificate Private Key — PEM formatted certificate.

Client Certificate Private Key Passphrase

Enable for Hashicorp Vault ☑

11. Configure the Credentials.

IBM DataPower Gateway		
Option	Description	Required
Client Certificate	The file that contains the PEM certificate used to communicate with the HashiCorp Vault host.	yes
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes
Client Certificate Private Key Passphrase	The passphrase for the private key.	yes

12. Click **Save**.

    Tenable Vulnerability Management saves the credential.

    The **My Scans** page appears.

Tenable Vulnerability Management for HashiCorp Vault

View the corresponding section to configure your Tenable Nessus application with HashiCorp Vault.

Configure Tenable Vulnerability Management with HashiCorp Vault (Windows and SSH)

Configure Tenable Vulnerability Management with HashiCorp Vault (Database)

Configure Tenable Vulnerability Management with HashiCorp Vault (Windows and SSH)

Required User Role: Standard, Scan Manager, or Administrator

In Tenable Vulnerability Management, you can integrate with HashiCorp Vault using Windows or SSH credentials. Complete the following steps to configure Tenable Vulnerability Management with HashiCorp Vault using these credentials.

Before you begin:

- Ensure you have both a Tenable Vulnerability Management and HashiCorp Vault account.

To integrate Tenable Vulnerability Management with HashiCorp Vault using Windows or SSH credentials:

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 **SSH** or **Windows**.

   The selected credential options appear.
7. In the **Authentication Method** drop-down, select **HashiCorp Vault**.

   The **HashiCorp Vault** options for Windows or SSH appear.

8. (Required) In the **Name** box, type a name for the credential.

9. (Optional) Add a **Description**.

10. Configure the **HashiCorp Vault** credentials.

Windows and SSH Credentials

Option	Description	Required
Hashicorp Vault host	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Hashicorp Vault port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate**(Required) and **Hashicorp Client Certificate Private Key** (Required) appear. Select the appropriate files for the client certificate and private key.	yes
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The path/subdirectory to the authentication endpoint. This is not the full URL. For example: `/v1/auth/approle/login`	yes

Namespace	The name of a specified team in a multi-team environment.	no
Vault Type	The HashiCorp Vault version: KV1, KV2, AD, or LDAP. For additional information about HashiCorp Vault versions, see the [HashiCorp Vault documentation]().	yes
KV1 Engine URL	(KV1) The URL HashiCorp Vault uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL HashiCorp Vault uses to access the KV2 engine. Example: `/v1/kv_mount_name`. No trailing / **Note:** You cannot use the path to the secret for the KV2 Engine URL because an additional string/segment, `data`, gets injected into the read request made to Vault for KV v2 stores. Only enter the name of the KV mount, not the path to the secret, in the **Engine URL** field. **Note:** You do not need to include the `data` segment yourself. If you include it in the secret name/path, the read call to Vault includes `/data/data`, which is invalid.	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL HashiCorp Vault uses to access the Active Directory engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the AD **Vault Type**
LDAP Engine URL	(LDAP) The URL HashiCorp Vault uses to access the LDAP engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the LDAP **Vault**

		Type
Username Source	(KV1 and KV2) A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(KV1 and KV2) The name in Hashicorp Vault that usernames are stored under.	yes
Domain Key	(KV1 and KV2) The name in Hashicorp Vault that domains are stored under.	no
Password Key	(KV1 and KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	(KV1, KV2, and AD) The key secret you want to retrieve values for.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled.) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Domain (Windows)	(Required if Kerberos Target Authentication is enabled.) The domain to which Kerberos Target	yes

	Authentication belongs, if applicable.	
Realm (SSH)	(Required if Kerberos Target Authentication is enabled.) The Realm is the authentication domain, usually noted as the domain name of the target (e.g., example.com).	yes
Use SSL	If enabled, Tenable Vulnerability Management uses SSL for secure communications. Configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, Tenable Vulnerability Management uses SSL for secure communications. Hashicorp Vault must be using SSL to enable this option.	no
Enable for HashiCorp Vault	Enables/disables IBM DataPower Gateway use with HashiCorp Vault.	yes
Escalate Privileges with (SSH)	Use a privilege escalation method such as su or sudo to use extra privileges when scanning. **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 HashiCorp Vault. 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 Vulnerability Management User Guide.	Required if you wish to escalate privileges.

Escalation account credential ID or identifier (SSH)	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

11. Click **Save**.

    Tenable Vulnerability Management saves the credential.

What to do next:

Verify the integration is working.

1. On the **My Scans** page, click the **Launch** button to initiate an on-demand scan.
2. Once the scan completes, click the completed scan.

   The scan details appear.

   Look for a message similar to the following:

   - For Windows: *Microsoft Windows SMB Log In Possible: 10394*. This result validates that authentication was successful.
   - For SSH: *Plugin ID 97993* and the corresponding message - *It was possible to log into the remote host via SSH using 'password' authentication*. This result validates that authentication was successful.

Configure Tenable Vulnerability Management with HashiCorp Vault (Database)

Required User Role: Standard, Scan Manager, or Administrator

In Tenable Vulnerability Management, you can integrate with HashiCorp Vault using Database credentials. Complete the following steps to configure Tenable Vulnerability Management with HashiCorp Vault using SSH.

Enable Database Plugins in the scanner to display them in the output.

Before you begin:

- Ensure you have both a Tenable Vulnerability Management and HashiCorp Vault account.

To integrate Tenable Vulnerability Management with HashiCorp Vault using Database credentials:

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 **Database** section, click **Database**.

   The **Database** options appear.

7. In the **Database Type** drop-down, select your preferred database type: **PostgreSQL**, **DB2**, **MySQL**, **SQL Server**, **Oracle**, or **Sybase ASE**.

8. In the **Auth Type** drop-down, select **HashiCorp Vault**.

   The **HashiCorp Vault** options appear.

9. Configure the **HashiCorp Vault Database** credentials.

Option	Description	Required
Hashicorp Vault host	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Hashicorp Vault port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate** and **Hashicorp Client Certificate Private Key** appear. Select the appropriate files for the client certificate and private key.	yes
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The path/subdirectory to the authentication endpoint. This is not the full URL. For example:	yes

	`/v1/auth/approle/login`	
Namespace	The name of a specified team in a multi-team environment.	no
Vault Type	The HashiCorp Vault version: KV1, KV2, AD or LDAP. For additional information about HashiCorp Vault versions, see the HashiCorp Vault documentation.	yes
KV1 Engine URL	(KV1) The URL HashiCorp Vault uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL HashiCorp Vault uses to access the KV2 engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL HashiCorp Vault uses to access the active directory engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the AD **Vault Type**
LDAP Engine URL	(LDAP) The URL HashiCorp Vault uses to access the LDAP engine. Example: `/v1/path_to_secret`. No trailing /	yes, if you select the LDAP **Vault Type**
Username Source	(KV1 and KV2) A drop-down box to specify whether the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(KV1 and KV2) The name in Hashicorp	yes

	Vault that usernames are stored under.	
Password Key	(KV1 and KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	(KV1, KV2, and AD) The key secret you want to retrieve values for.	yes
Use SSL	If enabled, Tenable Vulnerability Management uses SSL for secure communications. Configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no
Database Port	The port on which Tenable Vulnerability Management communicates with the database.	yes
Auth Type	The authentication method for the database credentials. Oracle values include: • SYSDBA • SYSOPER • NORMAL	yes
Service Type	(Oracle databases only) Valid values include: SID and SERVICE_NAME.	yes
Service	(Oracle database only) A specific field for the configuration for the database.	yes

10. Click **Save**.

Tenable Vulnerability Management saves the credential.

Enable Database Plugins

To enable database plugins:

1. In the scan where you configured the Hashicorp credentials, click the **Plugins** tab.

   The **Plugins** section appears.

2. Click the **Status** button.

3. Click **Save**.

   See the chart for database plugin types and corresponding IDs.

Plugin Type	Plugin ID
MSSQL	91827
Oracle	91825
MySQL	91823
PostgresSQL	91826

Configure Tenable Vulnerability Management with IBM DataPower Gateway

In Tenable Vulnerability Management, you can integrate with HashiCorp Vault using IBM DataPower Gateway credentials. Complete the following steps to configure Tenable Vulnerability Management with HashiCorp Vault using these credentials.

> **Required User Role:** Standard, Scan Manager, or Administrator

Before you begin:

- Ensure you have both a Tenable Vulnerability Management and HashiCorp Vault account.

To integrate Tenable Vulnerability Management with HashiCorp Vault using IBM DataPower Gateway credentials:

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. Under **API Gateway**, click **IBM Datapower Gateway**.

   The **IBM DataPower Gateway** options appear.
7. (Required) In the **Name** box, type a name for the credential.
8. (Optional) Add a **Description**.

9. Configure the credential.

IBM DataPower Gateway		
Option	Description	Required
Client Certificate	The file that contains the PEM certificate used to communicate with the HashiCorp Vault host.	yes
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes
Client Certificate Private Key Passphrase	The passphrase for the private key.	yes

10. Click **Save**.

    Tenable Vulnerability Management saves the credential.

    The **My Scans** page appears.

Tenable Security Center for HashiCorp Vault

View the corresponding section to configure your Tenable Security Center application with Hashicorp Vault.

Configure Tenable Security Center with HashiCorp Vault (Windows)

Configure Tenable Security Center for HashiCorp Vault (SSH)

Configure Tenable Security Center for HashiCorp Vault (Database)

Configure Tenable Security Center with HashiCorp Vault (Windows)

Required User Role: Any

In Tenable Security Center, you can integrate with HashiCorp Vault using Windows credentials. Complete the following steps to configure Tenable Security Center with HashiCorp Vault using Windows.

Before you begin:

- Ensure you have both a Tenable Security Center and HashiCorp Vault account.

To integrate Tenable Security Center with HashiCorp Vault using Windows credentials:

1. Log in to Tenable Security Center.
2. Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.
3. At the top of the page, click **+Add**.

   The **Add Credential** page appears.
4. In the Windows section, click HashiCorp Vault.

   The HashiCorp Vault **Add Credential** page appears.
5. In the **Name** box, type a name for the credential.
6. (Optional) Add a **Description**.
7. (Optional) Add a **Tag** to the credential. For additional information about tags, see the Tags section in the Tenable Security Center documentation.
8. In the **Windows Hashicorp Vault Credential** section, configure the Windows credentials.

Option	Default Value	Required
Hashicorp Host	The Hashicorp Vault IP address or DNS address.	yes

	Note: If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.	
Hashicorp Port	The port on which Hashicorp Vault listens.	yes
Authenticaton Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate** (Required) and **Hashicorp Client Certificate Private Key** (Required) appear. Select the appropriate files for the client certificate and private key.	yes
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The path/subdirectory to the authentication endpoint. This is not the full URL. For example: `/v1/auth/approle/login`	yes
Namespace	The name of a specified team in a multi-team environment.	no
Hashicorp Vault Type	The type of Hashicorp Vault secrets engine: • **KV1** – Key/Value Secrets Engine Version 1 • **KV2** – Key/Value Secrets Engine Version 2 • **AD** – Active Directory	yes
KV1 Engine URL	The URL Tenable Security Center uses to access the Hashicorp Vault secrets engine.	yes

	Example: `/v1/path_to_secret`. No trailing `/`	
Username Source	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) Specifies if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	The key secret you want to retrieve values for.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	(Required if Kerberos Target Authentication is enabled) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes
KDC Transport	(Required if Kerberos Target Authentication is enabled) The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Domain	(Required if Kerberos Target Authentication is enabled) The domain to which Kerberos Target	yes

	Authentication belongs, if applicable.	
Use SSL	When enabled, Tenable Security Center uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no

9. Click **Submit**.

   Tenable Security Center saves the credential.

Configure Tenable Security Center for HashiCorp Vault (SSH)

Required User Role: Any

In Tenable Security Center, you can integrate with HashiCorp Vault using SSH credentials.

Before you begin:

- Ensure you have both a Tenable Security Center and HashiCorp Vault account.

Note: HashiCorp Vault provides options for both KV v1 and v2.

To integrate Tenable Security Center with HashiCorp Vault using SSH credentials:

1. Log in to Tenable Security Center.
2. Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.
3. At the top of the page, click **+Add**.

   The **Add Credential** page appears.
4. Scroll to the **SSH** section.
5. In the Windows section, click HashiCorp Vault.

   The HashiCorp Vault **Add Credential** page appears.
6. In the **Name** box, type a name for the credential.
7. (Optional) Add a **Description**.
8. (Optional) Add a **Tag** to the credential. For additional information about tags, see the Tags section in the Tenable Security Center documentation.
9. In the **SSH Hashicorp Vault Credential** section, configure the SSH credentials.

Option	Default Value	Required
Hashicorp Host	The Hashicorp Vault IP address or DNS address.	yes

	Note: If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *`IP address or hostname/subdirectory path`*.	
Hashicorp Port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate** (Required) and **Hashicorp Client Certificate Private Key** (Required) appear. Select the appropriate files for the client certificate and private key.	yes
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The path/subdirectory to the authentication endpoint. This is not the full URL. For example: `/v1/auth/approle/login`	yes
Namespace	The name of a specified team in a multi-team environment.	no
Hashicorp Vault Type	The type of Hashicorp Vault secrets engine: • **KV1** – Key/Value Secrets Engine Version 1 • **KV2** – Key/Value Secrets Engine Version 2 • **AD** – Active Directory	yes
KV Engine URL	The URL Tenable Security Center uses to access the Hashicorp Vault secrets engine.	yes

	Example: `/v1/path_to_secret`. No trailing /	
Username Source	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) Specifies if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	The key secret you want to retrieve values for.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	(Required if Kerberos Target Authentication is enabled) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes
KDC Transport	(Required if Kerberos Target Authentication is enabled) The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain,	yes

	usually noted as the domain name of the target (for example, example.com). By default, Tenable Security Center uses 443.	
Use SSL	When enabled, Tenable Security Center uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see Privilege Escalation.	no

10. Click **Submit**.

    Tenable Security Center saves the credential.

Configure Tenable Security Center for HashiCorp Vault (Database)

Required User Role: Any

In Tenable Security Center, you can integrate with HashiCorp Vault using database credentials. Complete the following steps to configure Tenable Security Center with HashiCorp Vault using database.

Before you begin:

- Ensure you have both a Tenable Security Center and HashiCorp Vault account.

To integrate Tenable Security Center with HashiCorp Vault using database credentials:

1. Log in to Tenable Security Center.
2. Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.
3. At the top of the page, click **+Add**.

   The **Add Credential** page appears.
4. Go to the **Database** section.
5. Click the database type that you want to use. **(IBM DB2**, **MySQL**, **Oracle Database**, **PostgreSQL**, or **SQL Server**)
6. In the **Name** box, type a name for the credential.
7. (Optional) Add a **Description**.
8. (Optional) Add a **Tag** to the credential. For additional information about tags, see the Tags section in the Tenable Security Center documentation.
9. (For Oracle only) Click the **Source** drop-down to select a source type.
10. In the database credential section, click the **Authentication Method** drop-down.

11. Select **HashiCorp Vault**.

12. In the **Database Credential** section, configure the database credentials.

Option	Credential	Description	Required
Port	Oracle Database IBM DB2 MySQL PostgreSQL SQL Server	The port on which Tenable Security Center communicates with the database.	yes
SID	MySQL	The security identifier used to connect to the database.	yes
Database Name	IBM DB2 PostgreSQL	The name of the database.	no
Instance Name	SQL Server	The SQL server name.	yes
Hashicorp Host	All	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type `IP address or hostname/subdirectory path`.	yes
Hashicorp Port	All	The port on which Hashicorp Vault listens.	yes
Service Type	Oracle	The unique **SID** or **Service**	yes

	Database	**Name** that identifies your database.	
Service	Oracle Database	The **SID** or **Service Name** value for your database instance. **Note:** The **Service** value must match the **Service Type** option parameter selection.	yes
Authentication Type	All	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**.	yes
Client Cert	All	If **Authentication Type** is **Certificates**, the client certificate file you want to use to authenticate the connection.	yes
Private Key	All	If **Authentication Type** is **Certificates**, the private key file associated with the client certificate you want to use to authenticate the connection.	yes
Role ID	All	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	All	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	All	The path/subdirectory to the authentication endpoint. This	yes

		is not the full URL. For example: `/v1/auth/approle/login`	
Namespace	All	The name of a specified team in a multi-team environment.	no
Hashicorp Vault Type	All	The type of Hashicorp Vault secrets engine: • **KV1** – Key/Value Secrets Engine Version 1 • **KV2** – Key/Value Secrets Engine Version 2 • **AD** – Active Directory	yes
KV Engine URL	All	The URL Tenable Security Center uses to access the Hashicorp Vault secrets engine. Example: `/v1/path_to_secret`. No trailing /	yes
Username Source	All	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) Specifies if the username is input manually or pulled from Hashicorp Vault.	yes
Username key	All	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) The name in Hashicorp Vault	no

		that usernames are stored under.	
Username	All	(Only displays if **Username Source** is **Manual Entry**) The name in Hashicorp Vault that usernames are stored under.	yes
Password key	All	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) The key in Hashicorp Vault that passwords are stored under.	no
Secret Name	All	The key secret you want to retrieve values for.	yes
Use SSL	All	When enabled, Tenable Security Center uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	All	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no

13. Click **Submit**.

    Tenable Security Center saves the credential.