Tenable and HashiCorp Vault Integration Guide

Last Revised: June 23, 2021

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.io, Nessus, or Tenable.sc.

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.io, Tenable.sc, or Nessus Manager.

Tenable Role

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

Tenable.io - Standard, Scan Manager, Administrator, or System Administrator

Tenable.sc - Any

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.

Nessus for HashiCorp Vault

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

Configure Nessus Manager with HashiCorp Vault (Windows and SSH)

Configure Nessus Manager with HashiCorp Vault (Database)

Configure Nessus Manager with IBM DataPower Gateway

Configure Nessus Manager with HashiCorp Vault (Windows and SSH)

Required User Role: Standard, Scan Manager, or Administrator

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

Before you begin:

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

To integrate Nessus Managerwith HashiCorp Vault using Windows or SSH credentials:

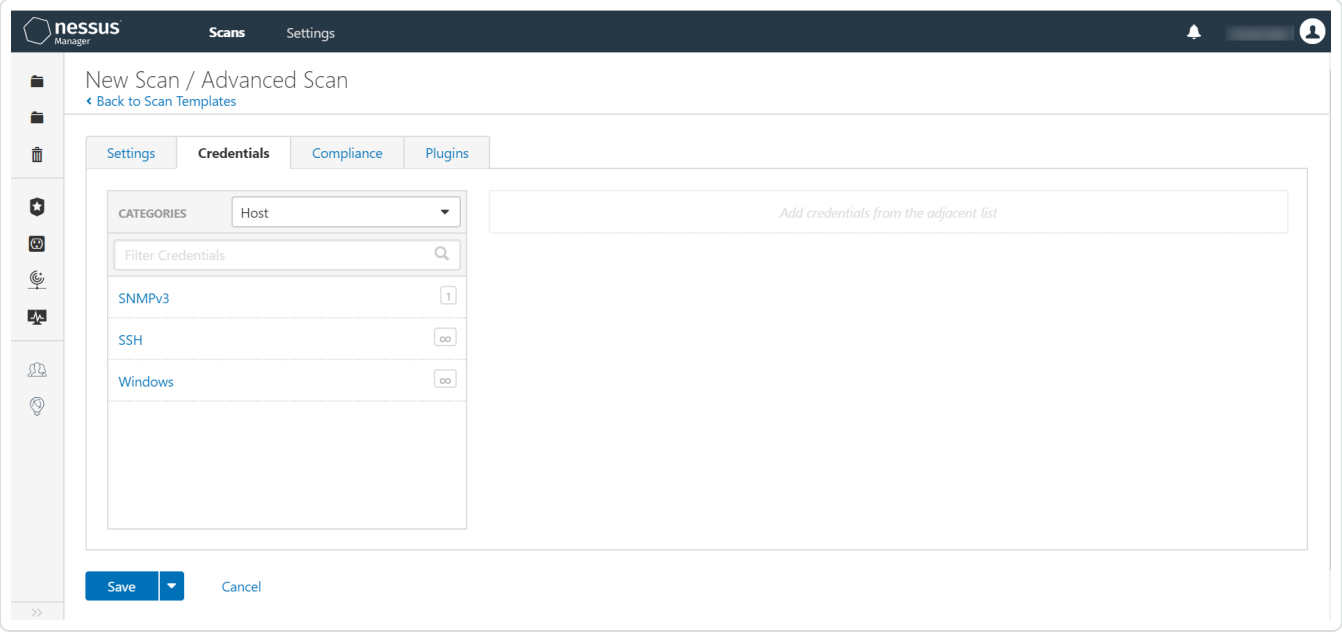
1. Log in to Nessus Manager.
2. Click **Scans**.

   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**.



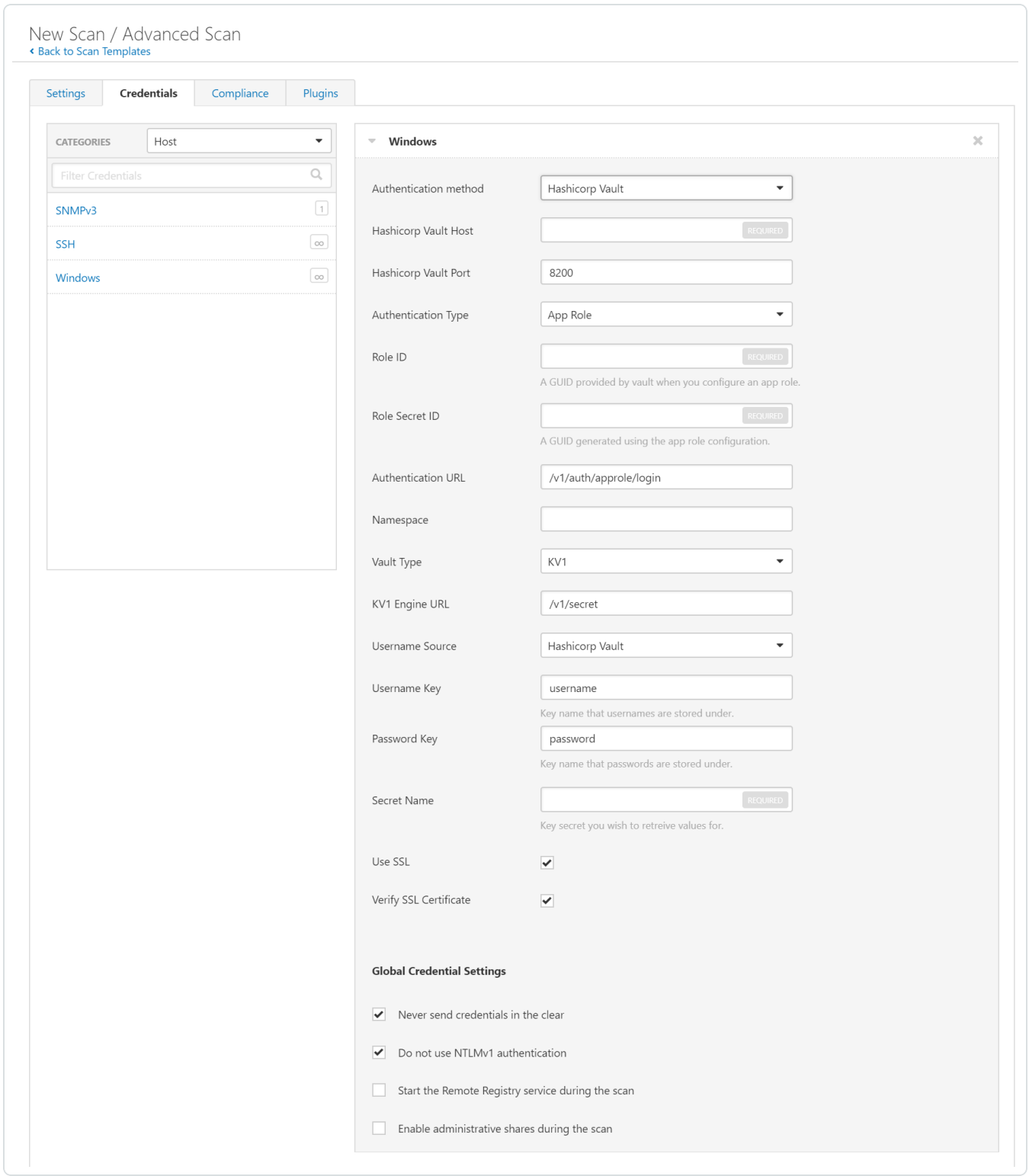
The selected configuration options appear.

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 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 host-name / 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 URL Nessus Manager uses to access Hashicorp Vault.	yes
Namespace	The name of a specified team in a multi-team environment.	no
Vault Type	The HashiCorp Vault version: KV1, KV2, or	yes

	AD. For additional information about HashiCorp Vault versions, see the HashiCorp Vault documentation.	
KV1 Engine URL	(KV1) The URL HashiCorp Vault uses to access the KV1 engine.	yes, if selected for **Vault Type**
KV2 Engine URL	(KV2) The URL HashiCorp Vault uses to access the KV2 engine.	yes, if selected for **Vault Type**
AD Engine URL	(AD) The URL HashiCorp Vault uses to access the active directory engine.	yes, if selected for **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
Secret Name	(KV1, KV2, and AD) The key secret you want to retrieve values for.	yes
Use SSL	If enabled, Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before	no

	enabling this option.	
Enable for HashiCorp Vault	Enables/disables IBM DataPower Gateway use with HashiCorp Vault.	yes

14. Click **Save**.

    Nessus Managersaves 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 Nessus Manager with HashiCorp Vault (Database)

In Nessus Manager, you can integrate with HashiCorp Vault using database credentials. Complete the following steps to configure Nessus Manager with HashiCorp Vault for database credentials.

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

Requirements

Required User Role: Standard, Administrator, or System Administrator

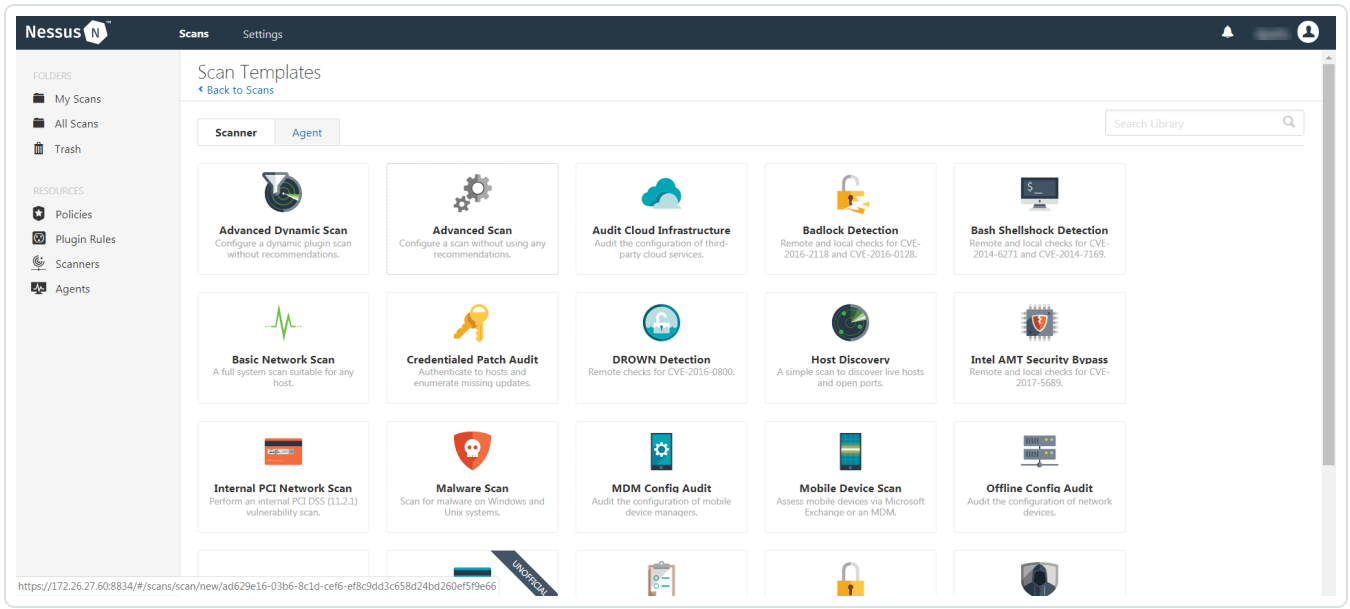
- Nessus Manager account
- HashiCorp Vault account

To integrate Nessus Manager with HashiCorp Vault using database credentials:

1. Log in to 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 **Database**.

   The **Database** options appear below.

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

    The **Database** options appear.

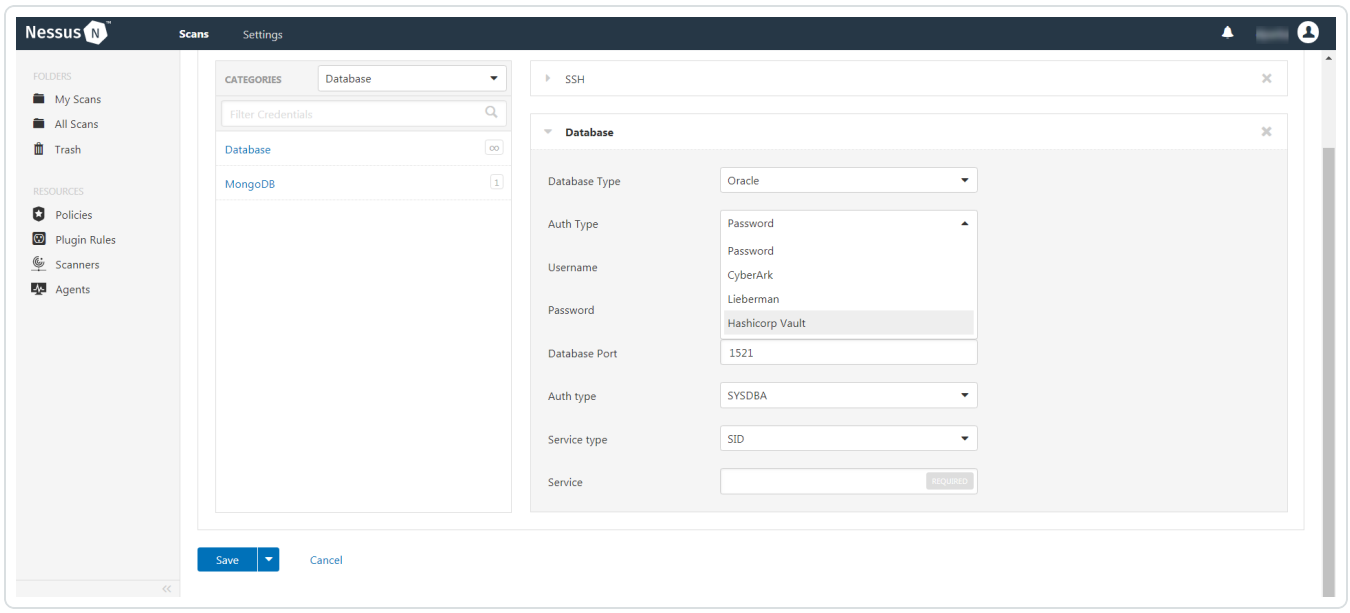
11. In the Database section, click the **Database Type** drop-down box.

    The **Database** options appear.

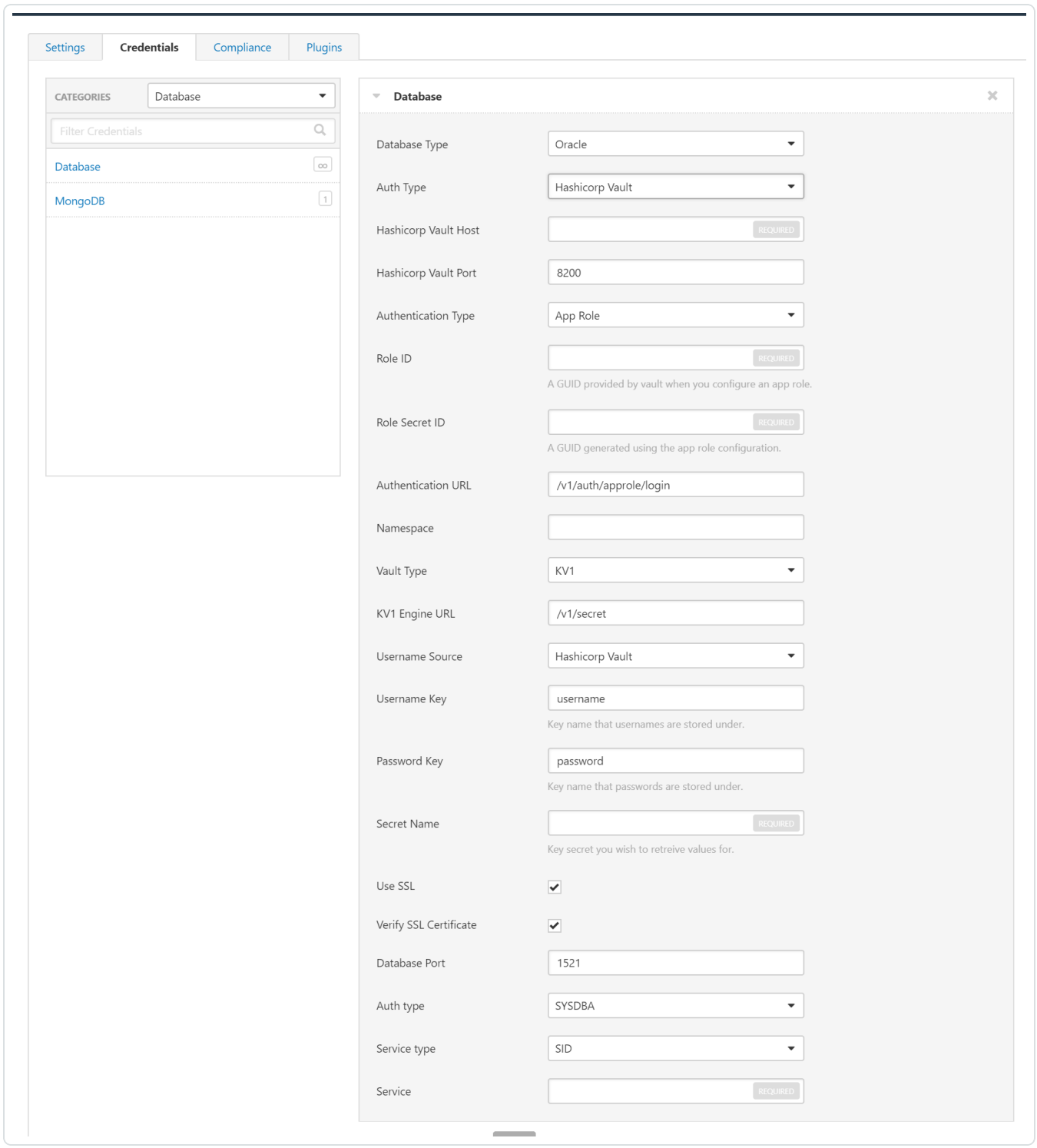
12. In the **Database Type** drop-down box, click your preferred database: **PostgreSQL**, **DB2**, **MySQL**, **SQL Server**, **Oracle**, or **Sybase ASE**.

    The selected **Database** options appear.

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



The HashiCorp Vault options appear.



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 sub-directory 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 URL Nessus Manager uses to access Hashicorp Vault.	yes
Namespace	The name of a specified team in a multi-team environment.	no
Vault Type	The HashiCorp Vault version: KV1, KV2, or AD. 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.	yes, if you select KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL HashiCorp Vault uses to access the KV2 engine.	yes, if you select KV2**Vault Type**
AD Engine URL	(AD) The URL HashiCorp Vault uses to access the active directory engine.	yes, if you select AD **for 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, Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no
Database Port	The port on which 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 Nessus Manager with IBM DataPower Gateway

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

Required User Role: Standard, Scan Manager, or Administrator

Before you begin:

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

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

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

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

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

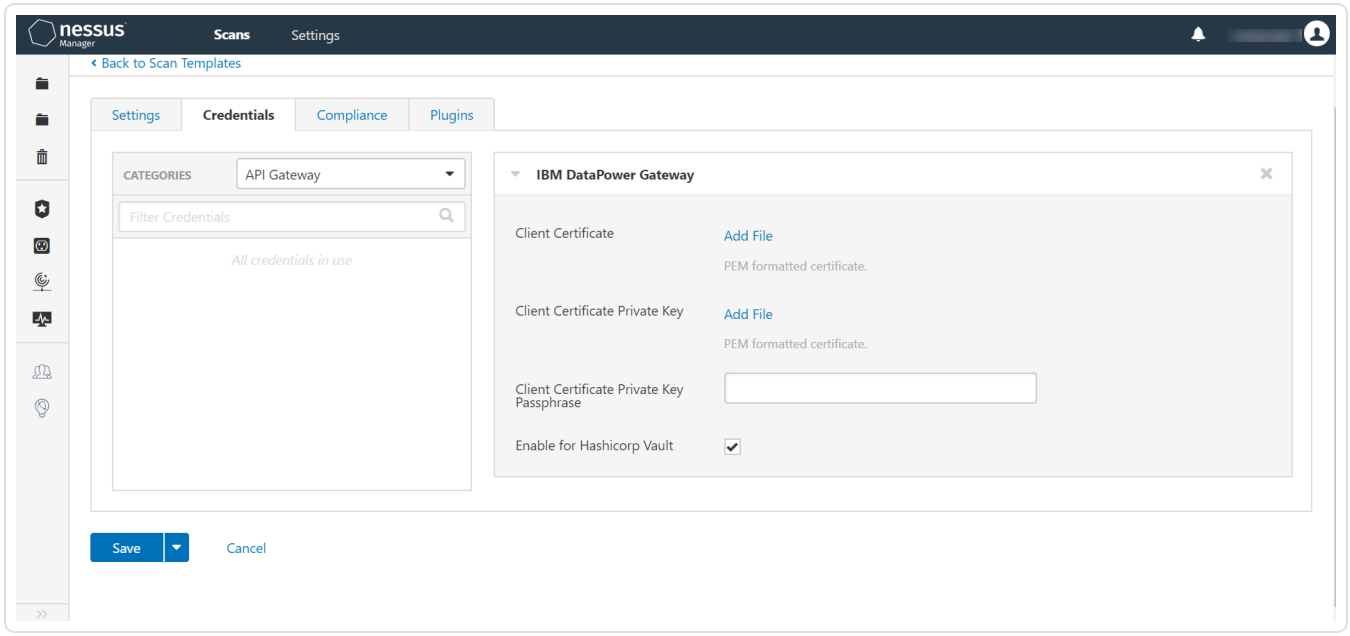
   The selected scan template **Settings** page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a **Description**, **Folder location**, **Scanner location**, and specify **Target groups**.
8.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



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.io saves the credential.

    The **My Scans** page appears.

Tenable.io for HashiCorp Vault

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

Configure Tenable.io with HashiCorp Vault (Windows and SSH)

Configure Tenable.io with HashiCorp Vault (Database)

Configure Tenable.io with HashiCorp Vault (Windows and SSH)

Required User Role: Standard, Scan Manager, or Administrator

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

Before you begin:

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

To integrate Tenable.io with HashiCorp Vault using Windows or SSH credentials:

1. Log in to Tenable.io.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Settings**.

   The **Settings** page appears.
4. Click the **Credentials** widget.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.
5. Click the ⊕ button next to the **Credentials** title.

   The credential form plane appears.
6. In the **Host** section, click **SSH** or **Windows**.

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

   The **HashiCorp Vault** options 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 URL Tenable.io uses to access Hashicorp Vault.	yes
Namespace	The name of a specified team in a multi-team environment.	no

Vault Type	The HashiCorp Vault version: KV1, KV2, or AD. 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.	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL HashiCorp Vault uses to access the KV2 engine.	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL HashiCorp Vault uses to access the active directory engine.	yes, if you select the AD **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
Use SSL	If enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no

Verify SSL Certificate	If enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no
Enable for HashiCorp Vault	Enables/disables IBM DataPower Gateway use with HashiCorp Vault.	yes

11. Click **Save**.

    Tenable.io 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 results 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.io with HashiCorp Vault (Database)

Required User Role: Standard, Scan Manager, or Administrator

In Tenable.io, you can integrate with HashiCorp Vault using Database credentials. Complete the following steps to configure Tenable.io 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.io and HashiCorp Vault account.

To integrate Tenable.io with HashiCorp Vault using Database credentials:

1. Log in to Tenable.io.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Settings**.

   The **Settings** page appears.
4. Click the **Credentials** widget.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.
5. Click the ⊕ button next to the **Credentials** title.

   The credential form plane appears.
6. In the **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 sub-directory 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 URL Tenable.io uses to access Hashicorp Vault.	yes
Namespace	The name of a specified team in a multi-team environment.	no
Vault Type	The HashiCorp Vault version: KV1, KV2, or	yes

	AD. For additional information about HashiCorp Vault versions, see the HashiCorp Vault documentation.	
KV1 Engine URL	(KV1) The URL HashiCorp Vault uses to access the KV1 engine.	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL HashiCorp Vault uses to access the KV2 engine.	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL HashiCorp Vault uses to access the active directory engine.	yes, if you select the AD **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.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this	no

	option.	
Database Port	The port on which Tenable.io 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.io 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.io with IBM DataPower Gateway

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

Required User Role: Standard, Scan Manager, or Administrator

Before you begin:

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

To integrate Tenable.io with HashiCorp Vault using IBM DataPower Gateway credentials:

1. Log in to Tenable.io.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Settings**.

   The **Settings** page appears.
4. Click the **Credentials** widget.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.
5. Click the ⊕ button next to the **Credentials** title.

   The credential form plane appears.
6. 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.io saves the credential.

    The **My Scans** page appears.

Tenable.sc for HashiCorp Vault

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

Configure Tenable.sc with HashiCorp Vault (Windows)

Configure Tenable.sc for HashiCorp Vault (SSH)

Configure Tenable.sc for HashiCorp Vault (Database)

Configure Tenable.sc with HashiCorp Vault (Windows)

Required User Role: Any

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

Before you begin:

- Ensure you have both a Tenable.sc and HashiCorp Vaultaccount.

Note: [[[Undefined variable Integrations.HashiCorp Vault]]] provides options for both KV v1 and v2. However, Tenable.sc only supports integration with KV v1.

To integrate Tenable.sc with HashiCorp Vault using Windows credentials:

1. Log in to Tenable.sc.
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.sc 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. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the sub-directory path. For example, type *IP address or hostname*/*subdirectory path*.	yes
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 URL used to access Hashicorp Vault.	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	yes

	• **AD** – Active Directory	
KV Engine URL	The URL Tenable.sc uses to access the Hashicorp Vault secrets engine.	yes
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
Use SSL	When enabled, Tenable.sc uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no

9. Click **Submit**.

   Tenable.sc saves the credential.

Configure Tenable.sc for HashiCorp Vault (SSH)

Required User Role: Any

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

Before you begin:

- Ensure you have both a Tenable.sc and HashiCorp Vaultaccount.

Note: [[[Undefined variable Integrations.HashiCorp Vault]]] provides options for both KV v1 and v2.

To integrate Tenable.sc with HashiCorp Vault using SSH credentials:

1. Log in to Tenable.sc.
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.sc 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. **Note:** If your Hashicorp Vault installation is in a sub-directory, you must include the subdirectory path. For example, type *IP address or hostname/sub-directory path*.	yes
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 URL used to access Hashicorp Vault.	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.sc uses to access the Hashicorp Vault secrets engine.	yes

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
Use SSL	When enabled, Tenable.sc uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no

10. Click **Submit**.

    Tenable.sc saves the credential.

Configure Tenable.sc for HashiCorp Vault (Database)

Required User Role: Any

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

Before you begin:

- Ensure you have both a Tenable.sc and HashiCorp Vaultaccount.

Note: [[[Undefined variable Integrations.HashiCorp Vault]]] provides options for, both, KV v1 and v2. However, Tenable.sc only supports integration with KV v1.

To integrate Tenable.sc with HashiCorp Vault using database credentials:

1. Log in to Tenable.sc.
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.sc 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	Description	Required
Port (Oracle, IBM, MySQL, PostgreSQL, SQL Server)	The port on which Tenable.sc communicates with the database.	yes
SID (MySQL)	The security identifier used to connect to the database.	yes
Authentication (Oracle, SQL Server)	(Oracle) The role type used for the database authentication. (**Normal, System Operator, Sys- tem Database Administrator**) (SQL Server) The authentication mode the data- base uses. (**SQL** or **Windows**)	yes
Database Name (IBM, PostgreSQL)	The name of the database.	no
Instance Name (SQL Server)	The SQL server name.	yes
Hashicorp Host	(Required) 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 host-name/subdirectory path`*.	yes
Hashicorp Port	(Required) The port on which Hashicorp Vault listens.	yes
Authentication Type (Oracle, SQL Server)	(Oracle) The role type used for the database authentication. (**Normal**, **System Operator**, or **System Database Administrator**)	yes

	(SQL Server) The authentication mode the database uses. (**SQL** or **Windows**)	
Service Type (Oracle)	The unique **SID** or **Service Name** that identifies your database.	yes
Service (Oracle)	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	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 URL Tenable.sc uses to access Hashicorp Vault.	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 Ver-	yes

	sion 1 • **KV2** – Key/Value Secrets Engine Version 2 • **AD** – Active Directory	
KV Engine URL	The URL Tenable.sc uses to access the Hashicorp Vault secrets engine.	yes
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.	no
Username	(Only displays if **Username Source** is **Manual Entry**) 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.	no
Secret Name	The key secret you want to retrieve values for.	yes
Use SSL	When enabled, Tenable.sc uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no

13. Click **Submit**.

    Tenable.sc saves the credential.