How-to Guide: Tenable for Hashicorp Vault

Last Revised: February 21, 2020

Table of Contents

Welcome to Tenable for Hashicorp Vault 3

Requirements 4

Nessus for Hashicorp Vault 5

Configure Nessus with Hashicorp Vault (Windows) 6

Configure Nessus for Hashicorp Vault (SSH) 11

Configure Nessus for Hashicorp Vault (Database) 15

Enable Database Plugins 19

Tenable.io for Hashicorp Vault 20

Configure Tenable.io with Hashicorp Vault (Windows) 21

Configure Tenable.io for Hashicorp Vault (SSH) 25

Configure Tenable.io for Hashicorp Vault (Database) 29

Enable Database Plugins 33

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 or Nessus.

> **Note:** Hashicorp Vault provides options for, both, KV v1 and v2. However, Tenable only supports integration with KV v1.

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 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

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.

> **Note:** Hashicorp Vault provides options for, both, KV v1 and v2. However, Tenable only supports integration with KV v1.

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 with Hashicorp Vault (Windows)

Configure Nessus for Hashicorp Vault (SSH)

Configure Nessus for Hashicorp Vault (Database)

Configure Nessus with Hashicorp Vault (Windows)

In Nessus Manager, you can integrate withHashicorp Vault using Windows credentials. Complete the following steps to configure Nessus with Hashicorp Vault in Windows.

Requirements

- Nessus Manageraccount
- Hashicorp Vault account

Note: Hashicorp Vault provides options for, both, KV v1 and v2. However, Tenable only supports integration with KV v1.

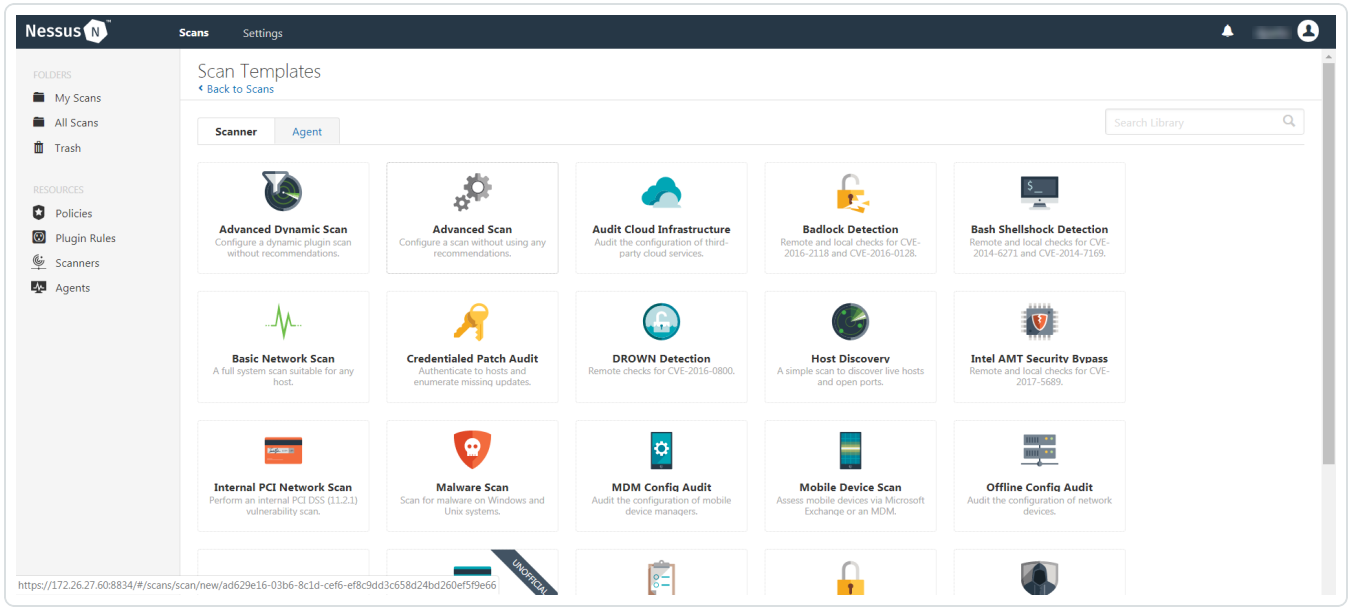
Required User Role: Standard, Administrator, or System Administrator

To integrate Nessus with Hashicorp Vault using Windows 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.

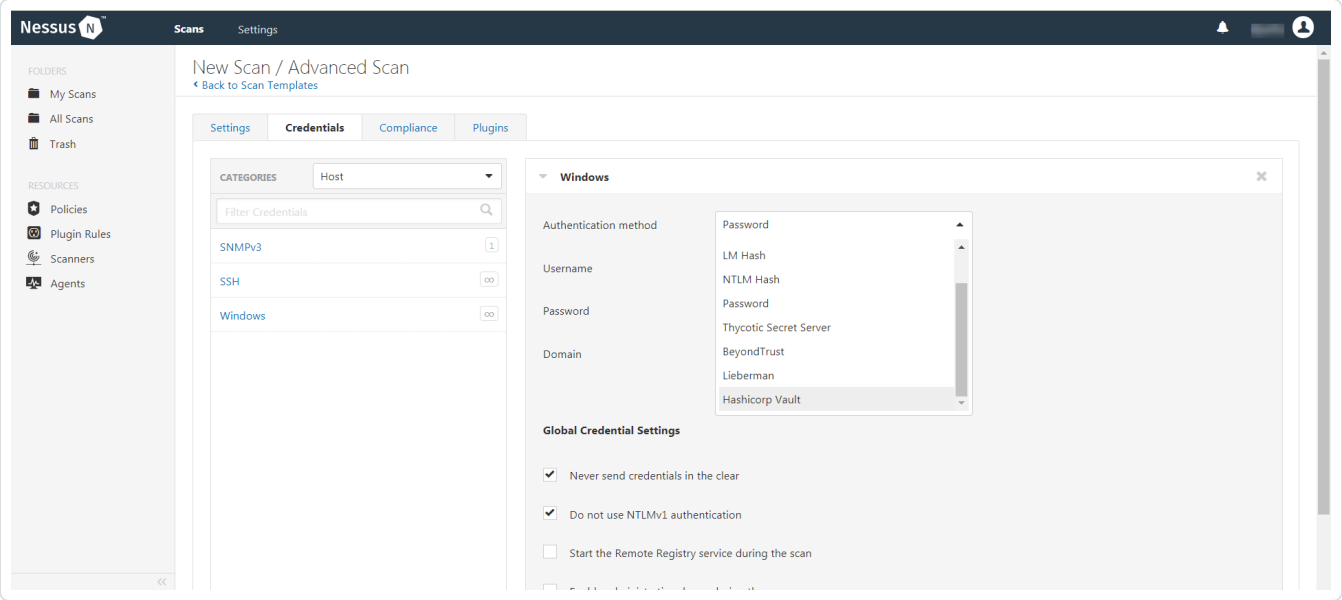
   The **Credentials** options appear. By default, the **Categories** drop-down box displays **Host**.

9. In the left menu, select **Windows**.

   The **Windows** settings appear.

10. In the **Windows** section, click the **Authentication method** drop-down box.

    The **Authentication method** drop-down box options appear.



11. Select **Hashicorp Vault**.

    The **Hashicorp Vault** options appear.

12. Configure the Windows credentials.

Option	Default Value
Hashicorp Vault host	(Required) 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/subdirectory path*.
Hashicorp Vault port	The port on which Hashicorp Vault listens.
Authenticaton Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**
Role ID	(Required) The GUID provided by Hashicorp Vault when you configured your App Role.
Role Secret ID	(Required) The GUID generated by Hashicorp Vault when you configured your App Role.
Authentication URL	The URL Nessus Manager uses to access Hashicorp Vault.
Namespace	The name of a specified team in a multi-team envir-onment.
KV Engine URL	The URL Nessus Manager uses to access the Hashicorp Vault secrets engine.
Username Source	A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.
Username Key	The key name in Hashicorp Vault that usernames are stored under.
Password Key	The key name in Hashicorp Vault that passwords are stored under.
Secret Name	(Required) The key secret you want to retrieve values for.
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.
Verify SSL	If enabled, Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.

13. Click **Save**.

What to do next:

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 - *Microsoft Windows SMB Log In Possible: 10394*. This result validates that authentication was successful.

Configure Nessus for Hashicorp Vault (SSH)

In Nessus Manager, you can integrate with Hashicorp Vault using SSH credentials. Complete the following steps to configure Nessus Manager with Hashicorp Vault using SSH.

Requirements

- Nessus Manager account
- Hashicorp Vault account

Note: Hashicorp Vault provides options for, both, KV v1 and v2. However, Tenable only supports integration with KV v1.

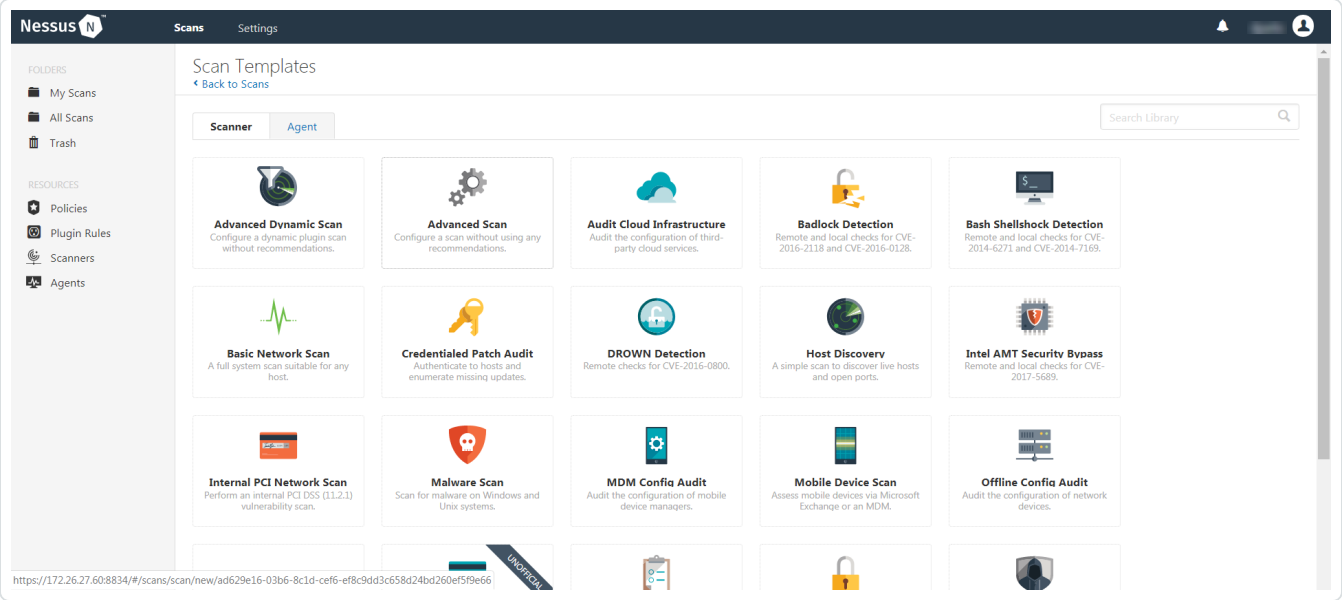
Required User Role: Standard, Administrator, or System administrator

To integrate Nessus Manager with Hashicorp Vault using 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.

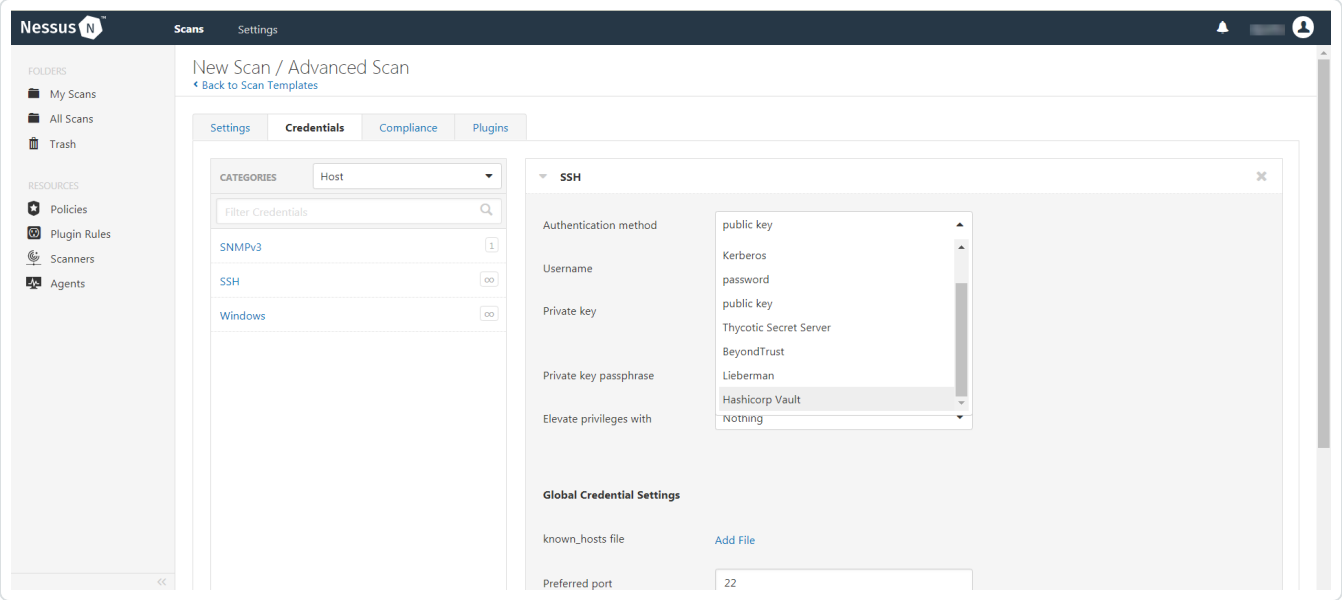
   The **Credentials** options appear. By default, the **Categories** drop-down box displays **Host**

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

   The **SSH** settings appear.

10. In the Windows section, click the **Authentication method** drop-down box.

    The **Authentication method** drop-down box options appear.



11. Select Hashicorp Vault.

    The Hashicorp Vault options appear.

12. Configure each field for SSH authentication.

Option	Default Value
Hashicorp Vault 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*.
Hashicorp Vault port	(Required) The port on which Hashicorp Vault listens.
Hashicorp Vault API URL	The URL Nessus Manager uses to access Hashicorp Vault.
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App

	Role.
Authentication URL	The URL Nessus Manager uses to access Hashicorp Vault.
Namespace	The name of a specified team in a multi-team environment.
KV Engine URL	The URL Nessus Manager uses to access the Hashicorp Vault secrets engine.
Username Source	A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.
Username Key	The key name in Hashicorp Vault that usernames are stored under.
Password Key	The key name in Hashicorp Vault that passwords are stored under.
Secret Name	The key secret you want to retrieve values for.
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.
Verify SSL	If enabled, Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.

13. Click **Save**.

What to do next:

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 **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 Nessus for Hashicorp Vault (Database)

In Nessus Manager, you can integrate with Hashicorp Vault using SSH credentials. Complete the following steps to configure Nessus Manager with Hashicorp Vault using SSH.

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

Requirements

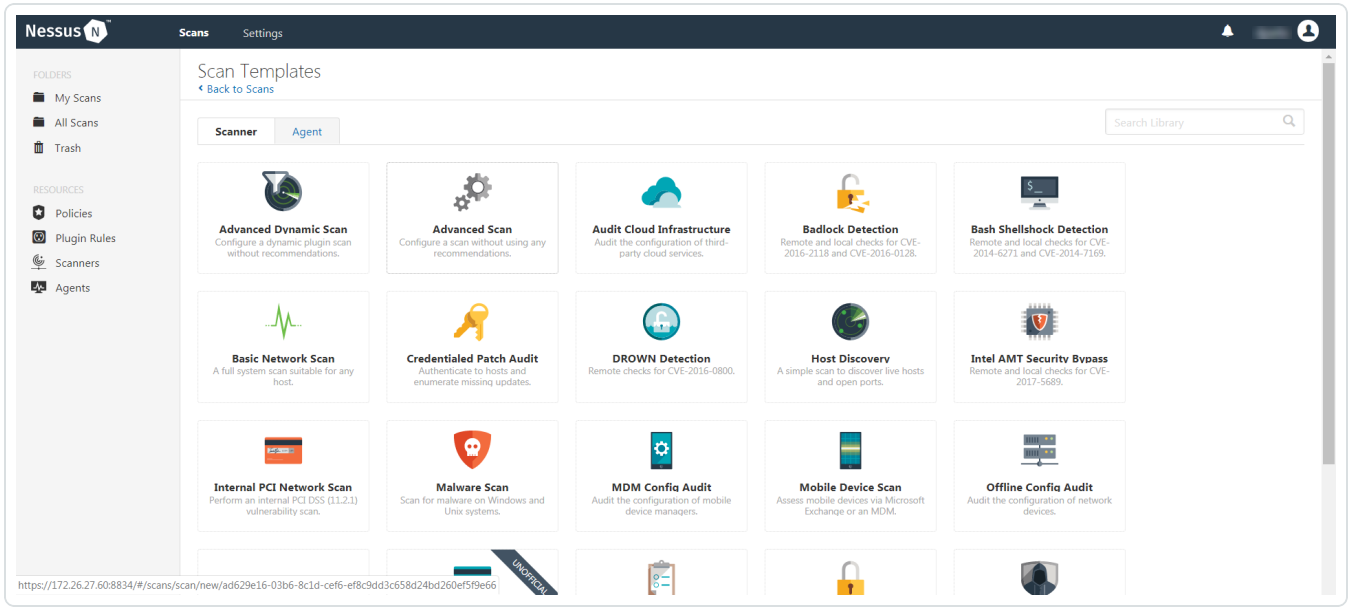
- Nessus Manager account
- Hashicorp Vault account

Note: Hashicorp Vault provides options for, both, KV v1 and v2. However, Tenable only supports integration with KV v1.

Required User Role: Standard, Administrator, or System Administrator

To integrate Nessus Manager with Hashicorp Vault using database credentials:

1. (missing or bad snippet)
2. (missing or bad snippet)
3. (missing or bad snippet)



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. (missing or bad snippet)
9. In the **Categories** drop-down box, select **Database**.

   The **Database** options appear below.

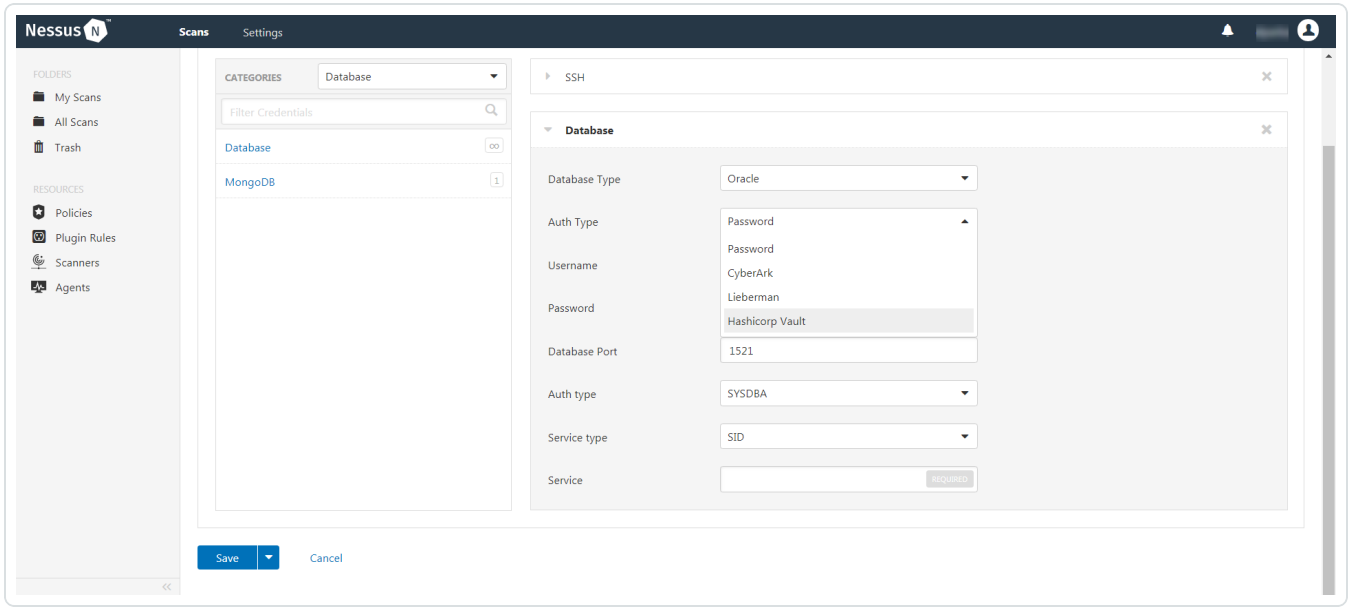
10. In the **Categories** list, click **Database**.

    The **Database** options appear.

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

    The **Database** options appear.

12. In the **Database Type** drop-down box, click **Oracle**.
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 subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Hashicorp Vault port	The port on which Hashicorp Vault listens.	no
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**	no
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.	no
Username Source	A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.	no
Username Key	The key name in Hashicorp Vault that usernames are stored under.	no
Password Key	The key name in Hashicorp Vault that passwords are stored under.	no
Secret Name	The key secret you want to retrieve values for.	no
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 cer-	no

	tificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.	
Database Port	The port on which Nessus Manager communicates with the database.	no
Auth Type	The authentication method for the database credentials. Oracle values include: • SYSDBA • SYSOPER • NORMAL	no
Service Type	(Oracle databases only) Valid values include: SID and SERVICE_NAME.	no
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

Tenable.io for Hashicorp Vault

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

Configure Tenable.io with Hashicorp Vault (Windows)

Configure Tenable.io for Hashicorp Vault (SSH)

Configure Tenable.io for Hashicorp Vault (Database)

Configure Tenable.io with Hashicorp Vault (Windows)

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

Requirements

- Tenable.io account
- Hashicorp Vault account

> **Note:** Hashicorp Vault provides options for, both, KV v1 and v2. However, Tenable only supports integration with KV v1.

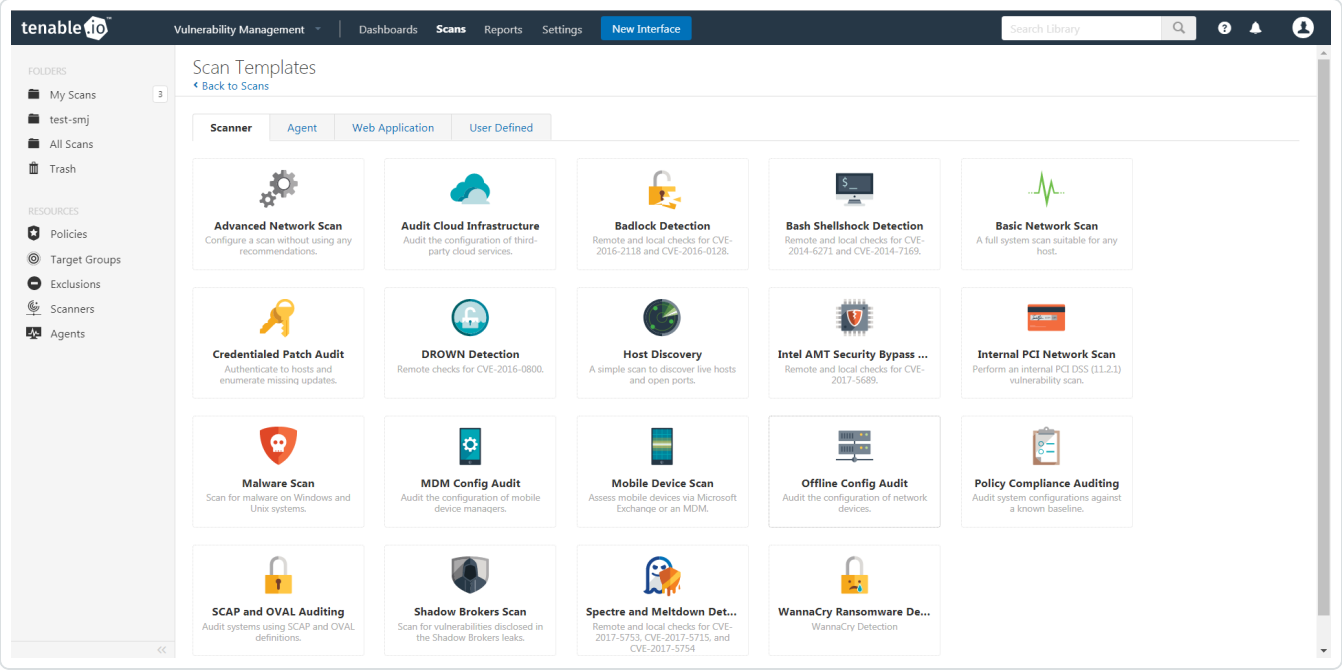
> **Required User Role:** Standard, Scan Manager, or Administrator

To integrate Tenable.io with Hashicorp Vault using Windows credentials:

1. Log in to Tenable.io.
2. In the top navigation bar, 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 left menu, select **Windows**.

   The **Windows** section appears.

10. In the Windows section, click the **Authentication method** drop-down box.

    The **Authentication method** drop-down box options appear.

11. Select Hashicorp Vault.

    The Hashicorp Vault options appear.

12. Configure the Windows credentials.

Option	Default Value
Hashicorp Vault host	(Required) 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/subdirectory path*.
Hashicorp Vault port	The port on which Hashicorp Vault listens.
Authenticaton Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**
Role ID	(Required) The GUID provided by Hashicorp Vault when you configured your App Role.
Role Secret ID	(Required) The GUID generated by Hashicorp Vault when you configured your App Role.
Authentication URL	The URL Tenable.io uses to access Hashicorp Vault.
Namespace	The name of a specified team in a multi-team envir-onment.
KV Engine URL	The URL Tenable.io uses to access the Hashicorp Vault secrets engine.
Username Source	A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.
Username Key	The key name in Hashicorp Vault that usernames are stored under.
Password Key	The key name in Hashicorp Vault that passwords are stored under.
Secret Name	(Required) The key secret you want to retrieve values for.
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.
Verify SSL	If enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.

13. Click **Save**.

    The credential saves.

    The **My Scans** page appears.

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- *Microsoft Windows SMB Log In Possible: 10394*. This results validates that authentication was successful.

Configure Tenable.io for Hashicorp Vault (SSH)

In Tenable.io, you can integrate with Hashicorp Vault using SSH credentials. Complete the following steps to configure Tenable.io with Hashicorp Vault using SSH.

Requirements

- Tenable.io account
- Hashicorp Vault account

Note: Hashicorp Vault provides options for, both, KV v1 and v2. However, Tenable only supports integration with KV v1.

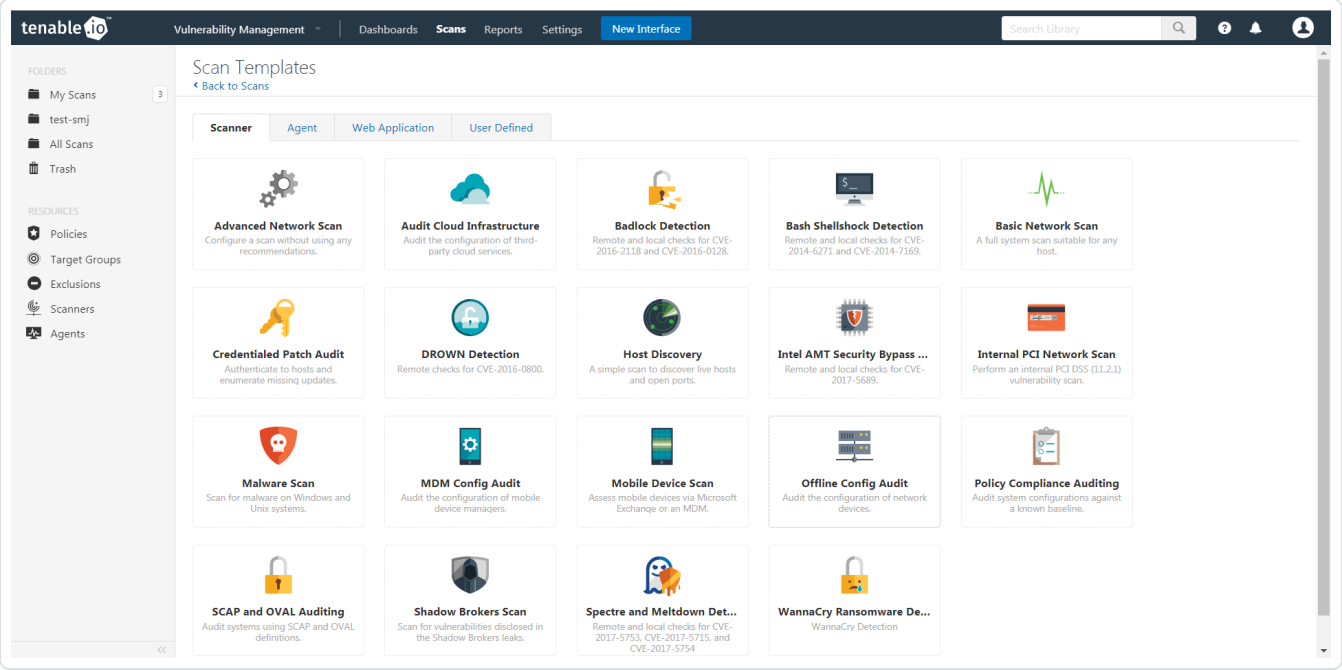
Required User Role: Standard, Scan Manager, or Administrator

To integrate Tenable.io with Hashicorp Vault using SSH credentials:

1. Log in to Tenable.io.
2. In the top navigation bar, 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.

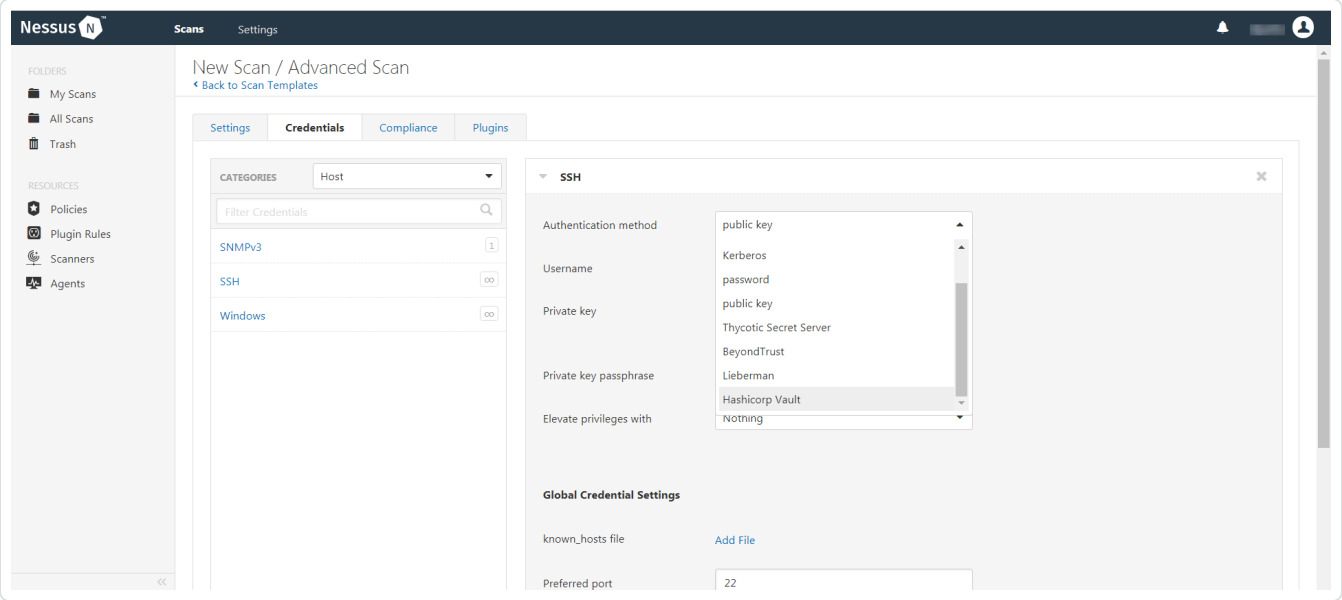
   The **Credentials** options appear. By default, the **Categories** drop-down box displays **Host**.

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

   The **SSH** section appears.

10. In the Windows section, click the **Authentication method** drop-down box.

    The **Authentication method** drop-down box options appear.



11. Select **Hashicorp Vault**.

    The **Hashicorp Vault** options appear.

12. Configure the SSH credentials.

Option	Default Value
Hashicorp Vault 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*.
Hashicorp Vault port	(Required) The port on which Hashicorp Vault listens.
Hashicorp Vault API URL	The URL Tenable.io uses to access Hashicorp Vault.
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.

Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.
Authentication URL	The URL Tenable.io uses to access Hashicorp Vault.
Namespace	The name of a specified team in a multi-team environment.
KV Engine URL	The URL Tenable.io uses to access the Hashicorp Vault secrets engine.
Username Source	A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.
Username Key	The key name in Hashicorp Vault that usernames are stored under.
Password Key	The key name in Hashicorp Vault that passwords are stored under.
Secret Name	The key secret you want to retrieve values for.
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.
Verify SSL	If enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.

13. Click **Save**.

What to do next:

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 has completed, select the completed scan and look for **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 for Hashicorp Vault (Database)

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.

Requirements

- Tenable.io account
- Hashicorp Vault account

Note: Hashicorp Vault provides options for, both, KV v1 and v2. However, Tenable only supports integration with KV v1.

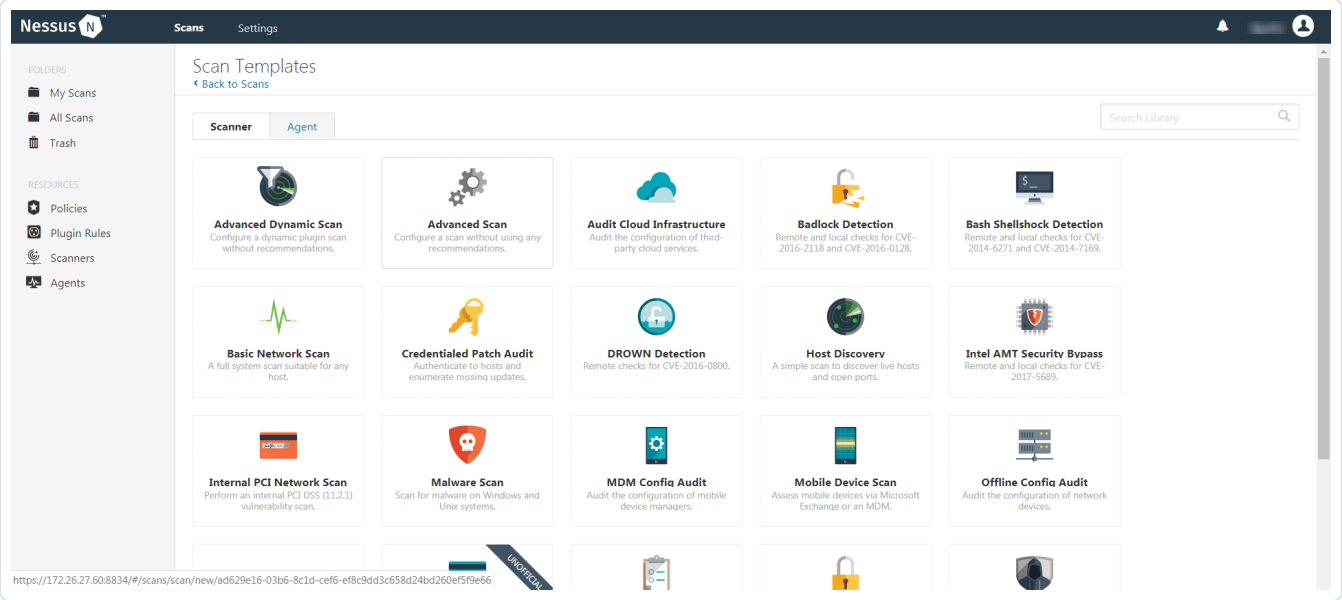
Required User Role: Standard, Scan Manager, or Administrator

To integrate Tenable.io with Hashicorp Vault using database credentials:

1. Log in to Tenable.io.
2. In the top navigation bar, 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. (missing or bad snippet)
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. Click the **Database Type** drop-down box.

    The **Database** options appear.

12. In the **Database Type** drop-down box, click **Oracle**.
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 subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Hashicorp Vault port	The port on which Hashicorp Vault listens.	no
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**	no
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.	no
Username Source	A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.	no
Username Key	The key name in Hashicorp Vault that usernames are stored under.	no
Password Key	The key name in Hashicorp Vault that passwords are stored under.	no
Secret Name	The key secret you want to retrieve values for.	no
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	no

	Vault before enabling this option.	
Database Port	The port on which Tenable.io communicates with the database.	no
Auth Type	The authentication method for the database credentials. Oracle values include: • SYSDBA • SYSOPER • NORMAL	no
Service Type	(Oracle databases only) Valid values include: SID and SERVICE_NAME.	no
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