



Splunk® SOAR (Cloud)

Administer Splunk SOAR (Cloud) current

Manage your organization's credentials with a password vault

Generated: 12/02/2023 12:11 am

Manage your organization's credentials with a password vault

Use credential vaults to centrally manage and monitor credential usage in your organization. Splunk SOAR (Cloud) supports the following password vaults:

- CyberArk Vault Privileged Access Manager
- Hashicorp Vault
- Thycotic Secret Server

As an administrator, you can configure Splunk SOAR (Cloud) to retrieve credentials from these vaults and use them with in assets.

- When used in conjunction with the Splunk SOAR Automation Broker, the Automation Broker will authenticate directly with your supported privileged access manager and retrieve credentials to use with assets.
- If an asset is configured on the Splunk SOAR instance and does not require the Automation Broker, then Splunk SOAR will authenticate with the supported privileged access manager and retrieve credentials to use with assets.

Use CyberArk Vault Privileged Access Manager with Splunk SOAR (Cloud)

Integrate Splunk SOAR (Cloud) with CyberArk's Vault cloud-based Privileged Access Manager feature to retrieve passwords or other fields for assets. This allows you to utilize CyberArk account management features to change passwords on managed products and services without having to manually update Splunk SOAR (Cloud) assets after a password change.

Before you begin, you need to be or be working with your organization's CyberArk administrator. Collect the following items:

- The URL to your organizations CyberArk Vault.
- Your organizations CyberArk Vault username and password.
- The pkcs12 certificate and certificate password for your organizations CyberArk Vault.
 - ◆ This certificate file must be located on the Splunk SOAR (Cloud) file system.

To use CyberArk Vault with Splunk SOAR (Cloud), perform the following steps:

1. From the main menu, select **Administration**.
2. Select **Administration Settings**, then **Password Vault**.
3. In the **Manager** field, select **CyberArk Vault**.
4. Type the entries for the following fields:
 1. URL
 2. Username
 3. Password
 4. Certificate password
5. Upload your certificate file:
 1. Click **Choose File** then select the pkcs12 certificate file from your filesystem.
6. Click **Save Changes**.

Use Hashicorp Vault with Splunk SOAR (Cloud)

Splunk SOAR (Cloud) supports Hashicorp Vault's KV store REST API version 2.

To use Hashicorp Vault with Splunk SOAR (Cloud), perform the following steps:

1. From the main menu, select **Administration**.
2. Select **Administration Settings**, then **Password Vault**.
3. In the **Manager** field, select **Hashicorp Vault**.
4. Get the URL and Token from your Hashicorp administrator.
5. Select the **Verify server certificate** check box to verify that the HTTPS certificate is trusted.
6. Click **Save Changes**.

Once you have Hashicorp access configured, you need to know the paths and names of the secrets you want to use from the Hashicorp Vault.

Use Hashicorp Vault to provide credentials with assets

You can use Hashicorp to automatically supply credentials when working with assets.

1. From the main menu, select **Apps**.
2. In the list of apps, find one to configure such as the Palo Alto Networks Firewall and click **Configure New Asset**.
3. Open the **Asset Settings** tab for that asset.
4. Click **Advanced** to expand the advanced configuration section.
5. In the Credential Management section, select the fields you want to get from Hashicorp Vault, and the path and key to use. For example, you can specify **/secret/autofocus** in the Path field and **apikey** in the Key field to retrieve an API key used to authenticate to the AutoFocus service.
6. Click **Save**.

Use Thycotic Secret Server with Splunk SOAR (Cloud)

Splunk SOAR (Cloud) can use Thycotic's API to access secrets managed by Secret Server. Usernames and passwords can be stored in Thycotic Secret Server for both users and assets which require a login to use.

Splunk SOAR (Cloud) does not support Delinea Secret Server, a product which replaces Thycotic Secret Server.

In order for Splunk SOAR (Cloud) to use secrets managed by Thycotic Secret Server you must provide:

- The URL to your organization's Thycotic Secret Server. You only need to include a port number in the URL if the Thycotic Secret Server is unreachable without a port number. Certain network and server configurations might require you to include port numbers in the URL. `https://<your.organization's.secret.server>:<port number>`
- The username and password of the account which will retrieve secrets using the API.
- Optional: The Organization ID set in Secret Server for use in the Thycotic Secret Server API.

These values are used to make an oauth2 token for Thycotic Secret Server. Once authenticated, Splunk SOAR (Cloud) uses the `SearchSecretsByFolder` API to access the managed secrets.

Set the login secret in Thycotic Secret Server

You must set up the login information in Secret Server before you can use it to access Splunk SOAR (Cloud). For more information on Thycotic Secret Server, see the documentation on the Thycotic website.

1. Create the required folders.
2. Use the **Create Secret** widget, selecting the template as **Password**.
3. Enter the required items in the mandatory fields of **secret** and **Password**.

Set the Thycotic Secret Server settings in Splunk SOAR (Cloud)

Add the required information to create the oauth2 token for Thycotic Secret Server in Splunk SOAR (Cloud)'s administration settings. This token is for connecting to Thycotic Secret Server.

1. From the Main Menu, select **Administration**.
2. Select **Administration Settings > Password Vault**.
3. Select **Thycotic Secret Server** from the drop-down list in the **Manager** field.
4. Set the URL for your Thycotic Secret Server instance.
5. Specify the username and password Splunk SOAR (Cloud) will use to access secrets.
6. Optional: Set the organization id.
7. Click **Save Changes**.

If you have assets that require logins, and those logins are managed by Thycotic Secret Server, then you must set credential management in the asset's configuration, in **Apps > <Asset Name> > Asset Settings > Advanced**.