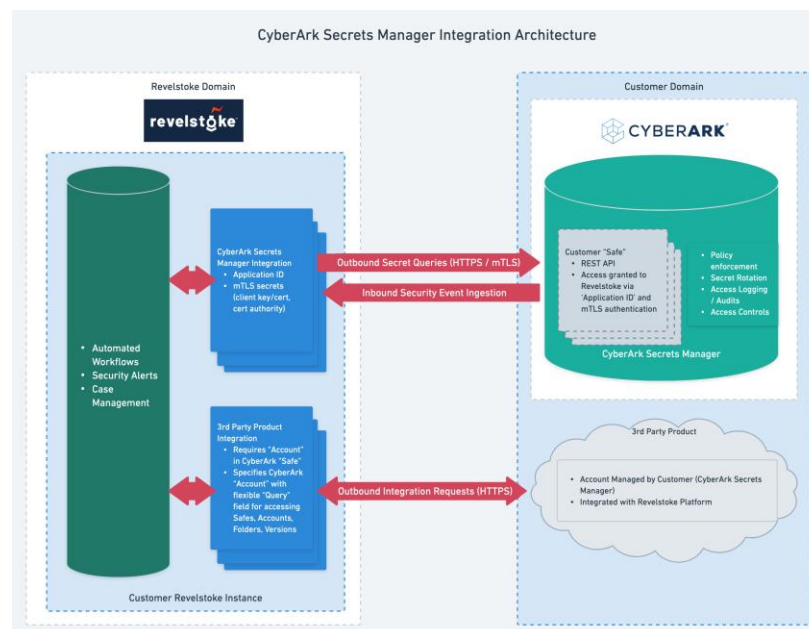


Revelstoke + CyberArk CCP Integration Guide

CyberArk Secrets Manager & CCP can automate privileged access management, provide contextual information from the CyberArk Vault, and improve incident response for analysts and SOC teams.

How It Works

Revelstoke's seamless, secure access to account secrets in CyberArk A reduces time integrating security products with Revelstoke and increases security hygiene by allowing users to manage their secrets in a single centralized, access-controlled environment.



The customer's CyberArk Secrets Manager, AAM, and CPP installation and the Revelstoke Platform instance coexist in parallel. The Revelstoke Platform can have one or more integration instances, each of which acts as a distinct CyberArk AAM client. These integration instances can be configured with their own unique security settings, such as application ID and client certificate credentials, allowing for independent access to specific safes, accounts, and folders for different teams and organizations. The configured CyberArk instances act as gateways for configuring third-party integrations on the Revelstoke Platform, which require secret account material from CyberArk AAM to access during security orchestration, automation, and response tasks.

Requirements

The Central Credential Provider (CCP) is the agentless method used to integrate with CyberArk allowing UiPath to securely retrieve credentials from a vault without deploying an agent on the server. A client certificate is necessary to ensure secure retrieval of the credential.

- A network that allows for interconnectivity between the Orchestrator machines and the CyberArk server.
- CyberArk® Central Credential Provider must be installed on a machine that allows HTTPS connections.
- CyberArk® Enterprise Password Vault
- A client certificate is necessary to ensure secure retrieval of the credential.

For more information about installing and configuring CyberArk® applications, please visit their [official page](#).

Support

If you need any help getting the CyberArk Secrets Manager up and running, please do not hesitate to reach out to us via email at info@revelstoke.io

Integration Walkthrough

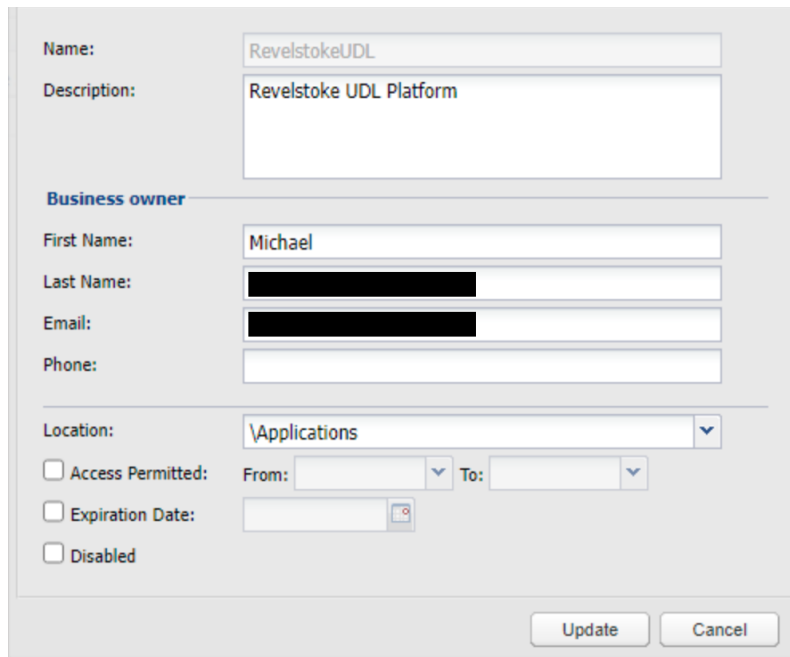
From the CyberArk® PVWA, you must perform the following steps:

- Create an application for your Revelstoke instance and add client certificates.
- Create a Safe and add members to it to ensure proper permissions.

In CyberArk

Creating a Revelstoke Application

1. In CyberArk's PVWA, log in with a user that has permissions to manage applications (it requires Manage Users authorization).
2. In the **Applications** tab, click **Add Application**. The **Add Application** window is displayed.



Name: RevelstokeUDL

Description: Revelstoke UDL Platform

Business owner

First Name: Michael

Last Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Location: \Applications

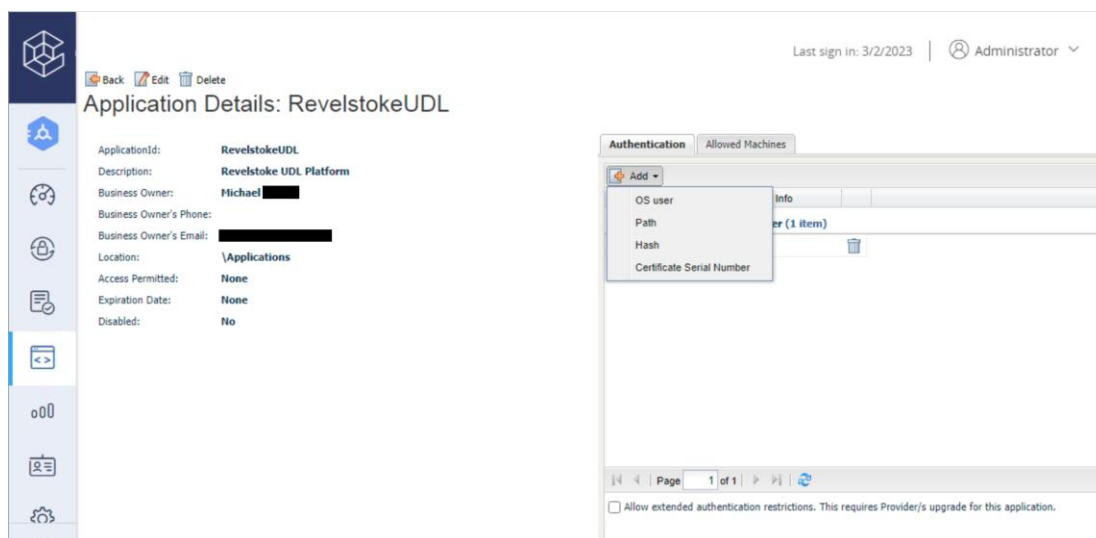
☐ Access Permitted: From: [REDACTED] To: [REDACTED]

☐ Expiration Date: [REDACTED]

☐ Disabled

Update Cancel

3. On the **Add Application** window, specify the following information:
 - a. **Name** field - a custom name for the application, such as RevelstokeUDL.
 - b. **Description** - a short description to help you specify the purpose of the new application.
 - c. In the **Business owner** section, specify contact information about the application's business owner.
 - d. **Location** - the path of the application within the Vault hierarchy. If a location is not specified, the application is added in the same location as the user who is creating this application.
4. Click **Add**. The application is added, and its details are displayed on the **Application Details** page.



Back Edit Delete

Last sign in: 3/2/2023 | Administrator

Application Details: RevelstokeUDL

Application ID: RevelstokeUDL

Description: Revelstoke UDL Platform

Business Owner: Michael [REDACTED]

Business Owner's Phone: [REDACTED]

Business Owner's Email: [REDACTED]

Location: \Applications

Access Permitted: None

Expiration Date: None

Disabled: No

Authentication Allowed Machines

Add

- OS user
- Path
- Hash
- Certificate Serial Number

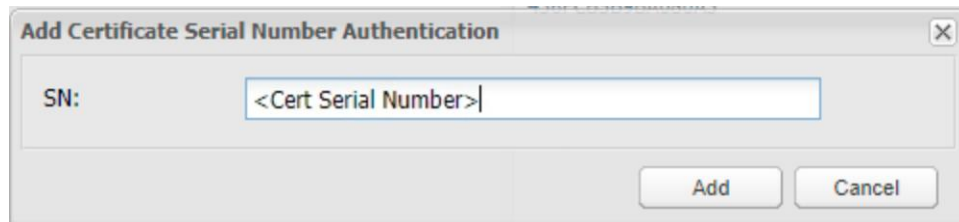
Info

1 Item

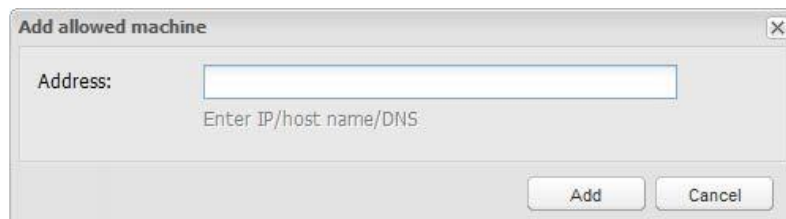
Page 1 of 1

☐ Allow extended authentication restrictions. This requires Provider/s upgrade for this application.

5. Select the **Allow extended authentication restrictions** checkbox. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
 - a. **Supported authentication methods:**
 - i. Allowed Machines
 - ii. OS User
 - iii. Client Certificates
6. Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. The Revelstoke Platform will access CyberArk AAM using the Central Credential Provider REST API with a provisioned client certificate and key.
7. In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
8. Select the authentication characteristic to specify.
9. Select **Certificate Serial Number**. The following window appears.



10. Specify the Certificate Serial Number.
11. Specify the application's Allowed Machines. This information enables AAM to make sure that only applications that run from specified machines can access their passwords.
 - a. In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.



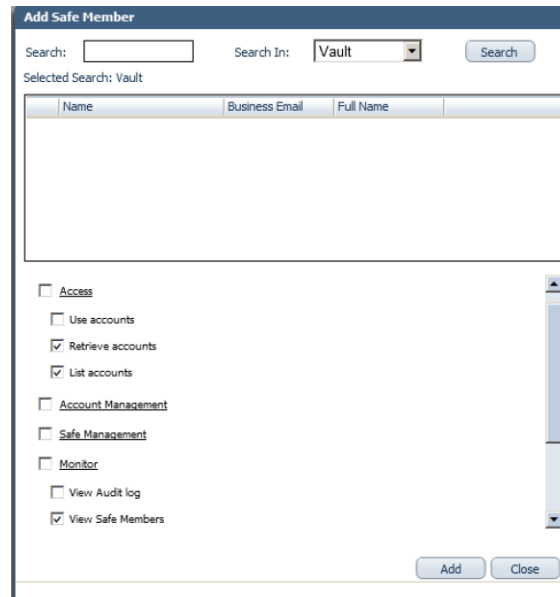
- b. In the **Address** box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab. Confirm with your Revelstoke contact on the appropriate machine info to supply here.

Creating a Revelstoke Safe

Safes are required to help you better manage your accounts. Also, you can add safe members to ensure proper authorization. CyberArk® recommends adding a **credential provider** (a user with full rights over the credentials can add and manage them) and the previously created application as safe members. The latter enables Revelstoke to find and retrieve the passwords stored in the safe.

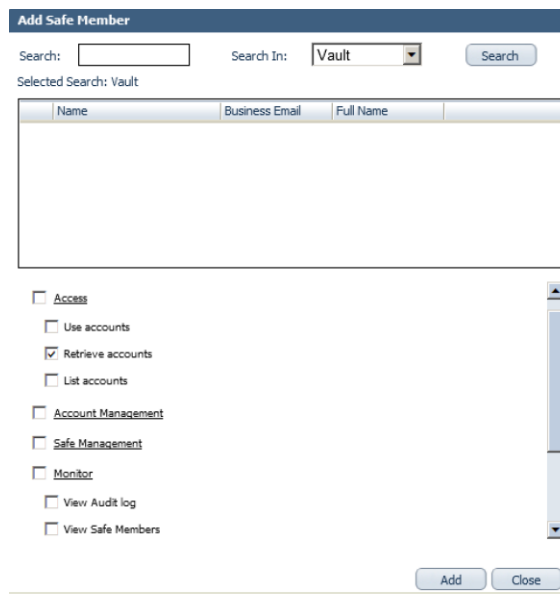
For the application to perform its functionality or tasks, the application must have access to existing accounts, or new accounts to be provisioned in CyberArk Vault.

1. In the **Policies** tab, under the **Access Control (Safes)** section, click **Add Safe**. The **Add Safe** page is displayed.
2. Fill in the **Safe Name** field and **Description** fields.
3. Click **Save**. The **Safe Details** window is displayed.
4. NOTE: In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:
 - **Manually** – Add accounts manually one at a time, and specify all the account details.
 - **Automatically** – Add multiple accounts automatically using the Password Upload feature.
5. For this step, you require the **Add accounts** authorization in the Password Safe. For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide**.
6. Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.
7. Add the provider user (where the Central Credential Provider is installed) and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.
8. Add the Provider user as a Safe Member with the following authorizations:
 - List accounts
 - Retrieve accounts.
 - View Safe Members
 - **Note:** When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.



9. Add the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve accounts.

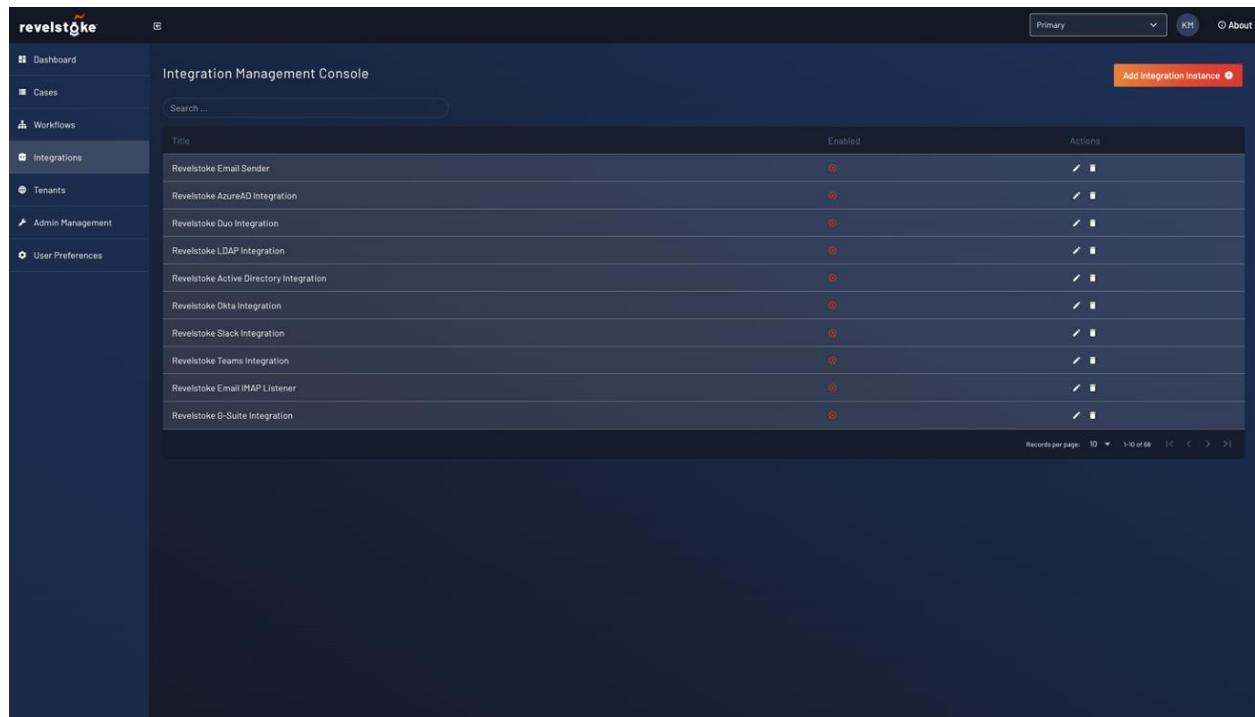


10. If the Safe is configured for object level access, make sure that both the provider user and the application have access to the password(s) to retrieve.

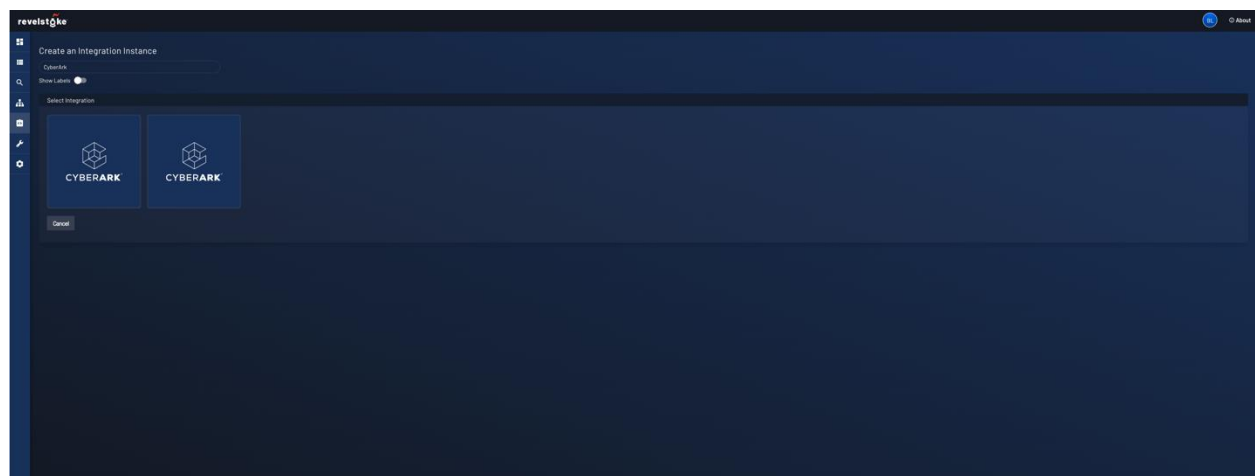
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

In Revelstoke

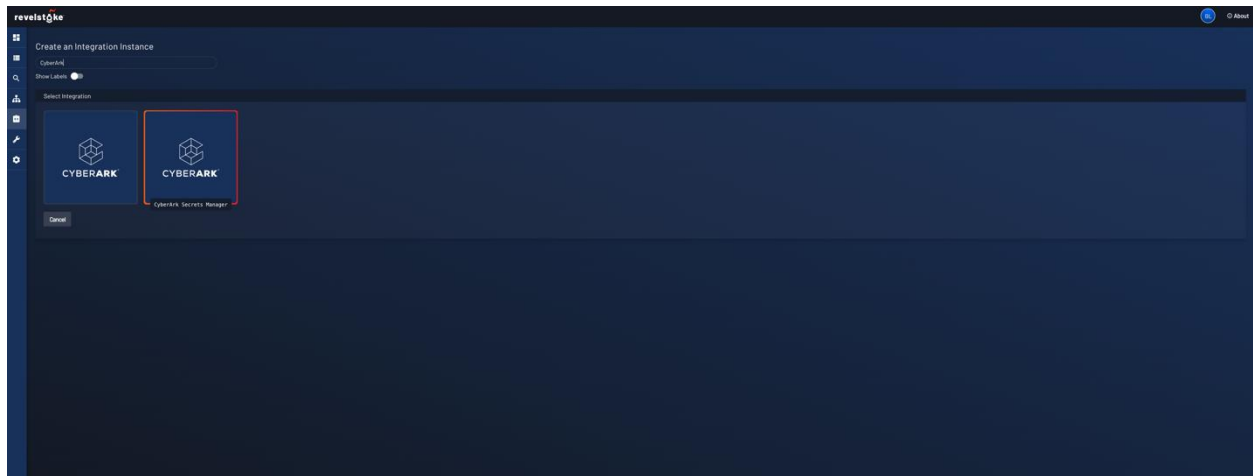
1. In your Revelstoke account, navigate to the integrations page



2. Select **Add Integration Instance**
3. Type in the Search bar CyberArk



4. Hover over the returned search results and CyberArk Secrets Manager will display



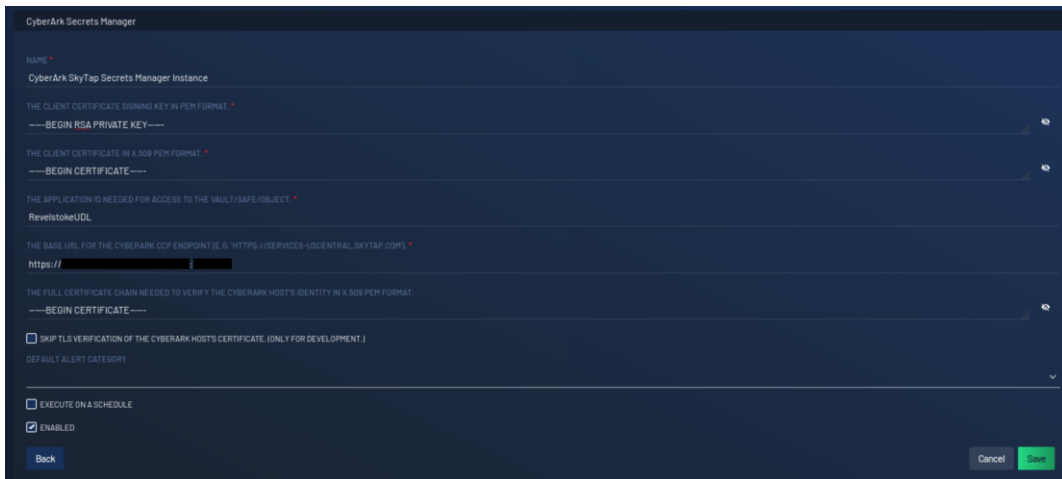
5. Select the **CyberArk** Secrets Manager Integration.
6. Using the new 'Application' setup in the previous steps.

- **Required Fields:**

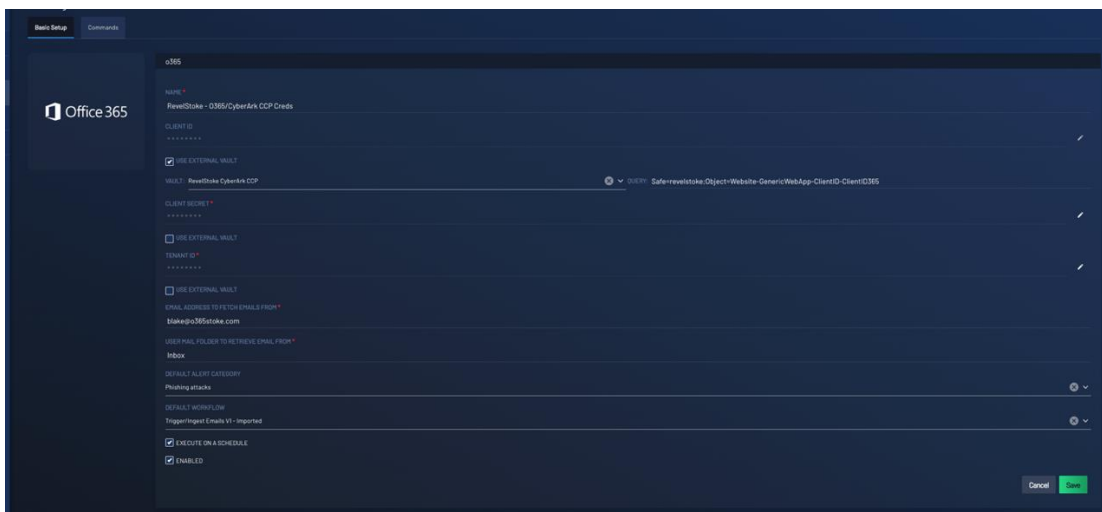
1. Client Certificate Signing Key (X.509 PEM format) – This should be the private key associated with the client certificate provisioned and configured for the CyberArk 'Application.'
2. Client Certificate (X.509 PEM format) – This certificate should have the serial number configured to match the CyberArk 'Application' setup in previous steps.
3. Application ID – The application ID configured in CyberArk (typically: "RevelstokeUDL")
4. CyberArk CCP Endpoint (Base URL) – This is the base URL needed to access the Central Credential Provider endpoint.
5. Full Certificate Chain For Server Verification (X.509 PEM format) – A collection of all certificates needed to verify the server's (CyberArk CCP endpoint) certificate. This should include the entire chain (intermediates) excluding the root certificate authority.
6. Enabled – Set to true to enable the integration instance.

- Note: Once the secret credential fields are saved (certs, key) into the secure repository they will no longer be visible and you must replace them entirely to modify later, if necessary.
- This configuration will be "shared" by any other 3rd party integration instances that need to access account secrets using the configured CyberArk Secrets Manager Application.

Additional “Instances” may be configured as separate ‘Applications’ (with unique ‘Application ID’, client cert/key) if necessary for different teams, organizations, access privilege levels (e.g. for more granular auditing in the CyberArk platform.)



8. Click **Save**.
9. Next, add or edit the integration instance for the 3rd party product that requires an account secret from CyberArk Secrets Manager configured above.
 - a. Locate a 3rd party product configuration property (e.g. Password) that should be replaced with a secret from the CyberArk Secrets Manager
 - b. Select “Use External Vault”
 - c. Choose the “Vault” to match the ‘name’ of the CyberArk Secrets Manager Instance configured in the previous steps.
 - d. Set the “Query” field for the desired secret using the flexible query format (non-regex) specified for the CCP REST API. A simple example is “Safe=<safe>;Object=<account id>”



10. Once configured, the Revelstoke Platform will query the <secret> data for the given query result and use it for the specified configuration item when accessing the 3rd party security product.

How to Disable

To stop the Revelstoke project from creating triggers in CyberArk, you will need to disable the CyberArk integration in Revelstoke.

1. Select the Revelstoke project that is configured to trigger CyberArk incidents.
2. Navigate to the **Integrations** page.
3. Under the **CyberArk** section click the **Pencil** icon.
4. Uncheck Enabled and then select **Save** to stop creating triggers.

How to Remove

1. In your Revelstoke account, navigate to the **Integrations** page.
2. Select the **Trash** icon.

Select **Yes, delete** to remove CyberArk instance from Revelstoke.

