Using CyberArk with Maverics Identity Orchestration

Break up with your outdated IDP, keep the complex access policies you love, and replace it with modern authentication and passwordless protection from CyberArk Workforce — all without rewriting your apps.

- Give every app the full protection of CyberArk — even legacy ones that don't 'speak' modern identity protocols or are located on-prem
- Keep your existing access policies and take a low-risk, phased coexistence approach to migration off your existing IDP
- Fully retire your legacy identity license and support costs, and easily adopt the latest CyberArk security services such as passkeys without disrupting users

Learn how you can use Maverics to extend CyberArk as an IDP to a legacy, non-standard app. The following is a sample configuration and is subject to change. For the latest steps, please refer to the Maverics Identity Orchestration Platform Documentation.

Prerequisites

Sign up for a Maverics account and complete the **Getting Started: Evaluation Environment** tutorial in the Learning Center. This tutorial will help you configure an environment.

You will need to have access to CyberArk Workforce Identity. If you don't have access, sign up for a CyberArk Workforce Identity or B2B free trial.

Start setting up CyberArk in Maverics

After completing the Getting Started: Evaluation Environment tutorial, proceed to the Learning Center tutorial, **Extend CyberArk to a Legacy, Non-Standard App**.

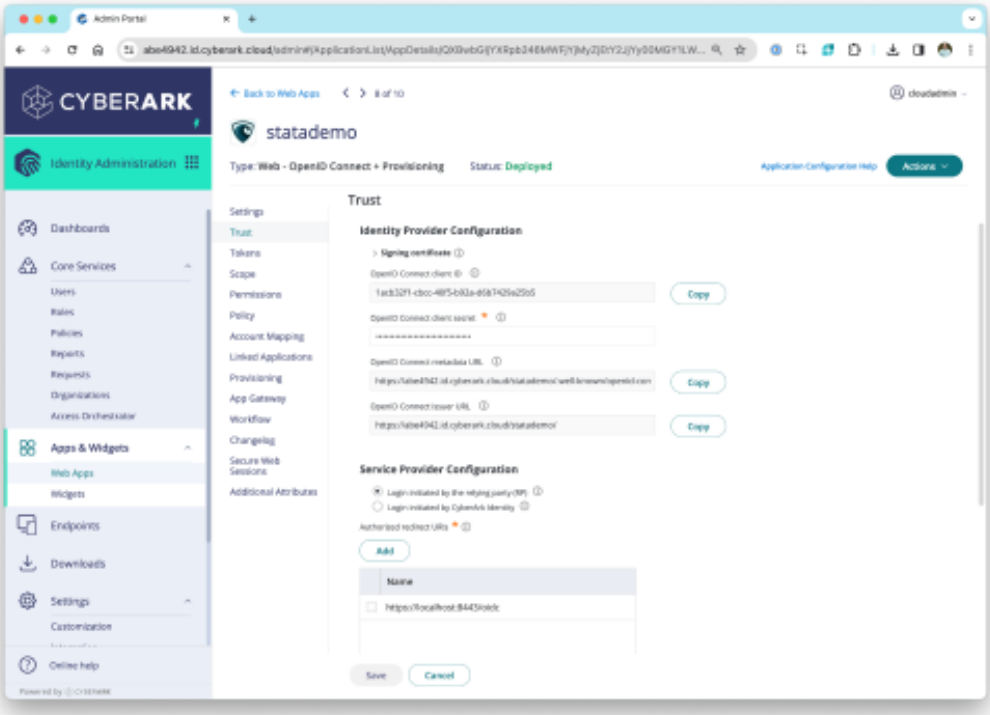
1. Load the recipe in Maverics. The recipe includes the demo configuration for an identity fabric, a proxy application app type, and a user flow. Click the link in the Learning Center to the CyberArk recipe, then click **Create.**

2. Create an evaluation environment. In the dropdown for Type choose **Evaluation**. Enter **Evaluation** as the name, then click **Save import**. If you already have an Evaluation environment select **None**.
3. The user flow loaded by the recipe defines the experience users will have when they go to access it. Navigate to the user flows list and click **Extend CyberArk to a Legacy, Non-Standard App**.
4. From the top of the page, click the **Deploy...** button to select a revision and environment.
5. Select a revision to deploy. Select the **Evaluation** environment. Click the **Preview** button to navigate to the deployment preview page.
6. You can now compare your revision to previous deployments. To deploy the configuration to your Evaluation environment, click the **Deploy** button at the top of the page.
7. Go to: https://localhost:8443 and skip past any browser security warnings to view the initial state of the legacy app. Canary Bank is currently using a legacy web access management system.
   If you don't see the app, be sure you have completed Getting Started: Evaluation Environment and have an orchestrator connected to your Evaluation environment.

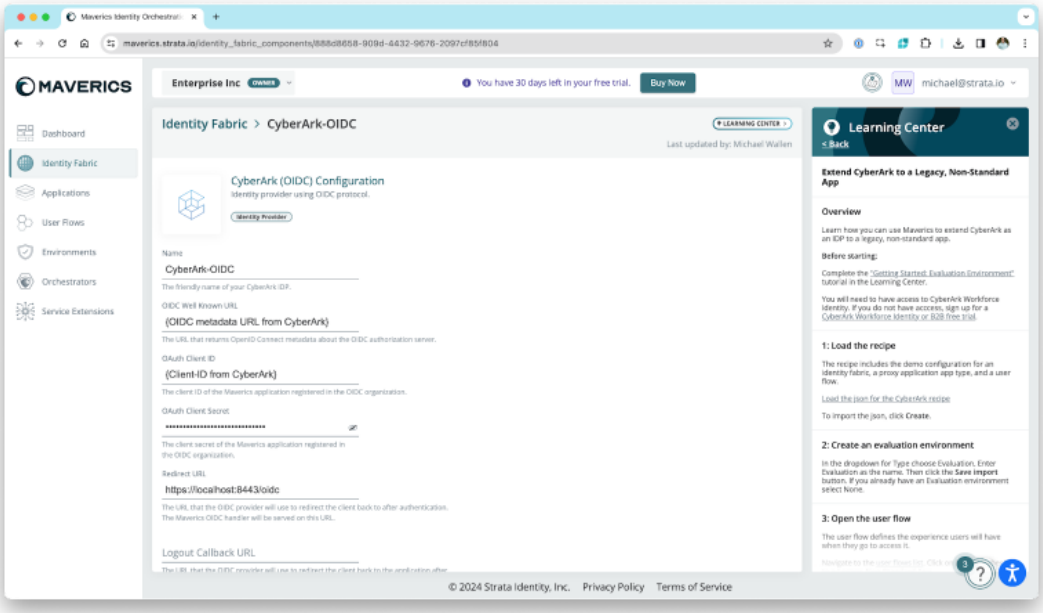
Set up Maverics in CyberArk

The next step is to create an OIDC app in CyberArk and configure CyberArk (OIDC) as part of your identity fabric in Maverics.

1. Follow the CyberArk docs to add and configure the custom OpenID Connect application.
2. In app's **Trust settings** tab, in the Service Provider configuration check **Login initiated by the relying party (RP)** and add `https://localhost:8443/oidc` as an authorized redirect URI.



3. Configure CyberArk (OIDC) in Maverics. Go to Identity Fabric and click **CyberArk-OIDC** from the list.



4. From the CyberArk app settings copy the OpenID Connect metadata URL and paste it into the **OIDC Well Known URL field** in Maverics.
5. From the app settings in CyberArk,, copy the **OpenID Connect client ID and secret**. Go back to Maverics and paste them into the corresponding fields. Click **Update**.

Finish setting up CyberArk in Maverics

The final step is to complete the CyberArk setup in Maverics.

1. Open the user flow. The user flow defines the experience users will have when they go to access it. Navigate to the user flows list. Click **Extend CyberArk to a Legacy, Non-Standard App**.
2. Open the "/" policy. Under Access Control Policies and click **Resource location: /**.
3. Edit the "/" access control policy. Within the Authentication section, select **CyberArk-OIDC**.
4. Scroll down to Headers section and add the following headers:

   SM_USER, CyberArk-OIDC, email
   firstname, CyberArk-OIDC, given_name
   lastname, CyberArk-OIDC, family_name

5. Click the **Commit** button, followed by **Ok**. Then click the **Deploy...** button to navigate to the Choose revision and environment modal.
6. Select a revision to deploy. Select the **Evaluation** environment. Click the **Preview** button to navigate to the deployment preview page.
7. In the deployment preview screen you can compare current revision with previous deployments. From the top of the page, click the **Deploy** button.
8. Try the new user login flow. Open a private browser and navigate to https://localhost:8443.
   You will be redirected to CyberArk to log in. Sign in with your CyberArk credentials. Upon success you will see the Canary Bank dashboard with the user info in the profile area.