

INTEGRATION GUIDE FOR CYBERARK PAM

BEYOND
IDENTITY

INTRODUCTION

This guide provides information on how to:

- Set up Beyond Identity as a passwordless authentication solution for your CyberArk PAM self-hosted environment.

PREREQUISITES

Ensure that you have the following:

1. A CyberArk PAM self-hosted environment with system admin privileges.

Section 1: Beyond Identity Configuration

1. Login to Beyond Identity Admin Console
2. Go to Integrations > OIDC > Add OIDC Client
3. Enter the following values:
Name: CyberArk OIDC
Redirect URIs:
<https://components.cyberark.local/PasswordVault/api/Auth/OIDC/beyondidentity/Token>
Token Signing Algorithm: RS256
Auth Method: client secret post



The screenshot shows a web form titled "Add OIDC Client". It has five main input sections: "Name" with the value "CyberArk OIDC", "Redirect URIs" with the value "al/PasswordVault/api/Auth/OIDC/beyondidentity/Token", "Token Signing Algorithm" with a dropdown menu showing "RS256", "Auth Method" with a dropdown menu showing "client secret post", and "Login Hint Validation Config" with a toggle switch labeled "DISABLED". At the bottom right of the form are two buttons: "Cancel" and "Save Changes".

4. Click **Save Changes**
5. Copy the Client ID and Client Secret

Section 2: CyberArk Configuration

PVWA Settings

1. Login to CyberArk PVWA as an Administrator
2. Go to **Administration > OIDC Authentication**
3. Complete the OIDC configuration as follows:

Display name (optional): Beyond Identity

Provider ID: BeyondIdentity

Discovery URL: <https://admin.byndid.com/v2/.well-known/openid-configuration>

Client ID: Obtained from Beyond Identity Step 5 above.

Client Authentication method: Click on **Basic**

Application Secret: Obtained from Beyond Identity Step 5 above.

User name claim (optional): sub

Select **Enable OpenID Provider**

Click **Save**

4. Go to **Administration > Configuration options**, and then Click **Options**

Go to **Access Restriction** and right click to select **Add AllowedReferrer**

Edit Properties

BaseUrl: <https://auth.byndid.com>

Click **Apply** and then Click **OK**

Go to **Authentication Methods** and select the value of the Provider ID as entered in step 3 above, and update the properties as shown below:

DisplayName: Beyond Identity

Enabled: Yes

Click **Apply** and then Click **OK**

Optional Configuration

CyberArk PAM allows users to login in either with their username and password or an alternate login option. Follow the steps below to enforce Beyond Identity passwordless authentication:

1. Login to CyberArk PVWA as an Administrator
2. Go to **Administration > Configuration Options**, and then click **Options**
3. Go to **Authentication Methods** and select an authentication method that is not OIDC. For example: windows

4. Set the value of **Properties** as below:
 - a. **Enabled:** No
5. Repeat steps 3 and 4 to disable other authentication options.

Setting up test users

User Enrollment

1. To enroll a user in the Beyond Identity experience, login to the Beyond Identity Admin Console and add users.
2. Enrolled user will receive an email from Beyond Identity welcoming them to the new Identity Provider.
 - a. See image below for reference:



Your organization is using Beyond Identity, a new sign-in experience for you to securely sign into your corporate applications without passwords. Follow the steps below to get started.

Step 1: Get Authenticator

Download and install the Beyond Identity Authenticator for your device. Go to Step 2 if this device already has the Authenticator installed.

[View Download Options](#)

Step 2: Register credential

Use the link below to register your new credential to this device. Don't wait long - **this link expires in 7 days.**

[Register New Credential](#)

Once registered, your credential can be set up on other devices with the Authenticator installed.

3. Each enrolled user will be asked to follow the two steps below:
 - a. Step 1: Download the Beyond Identity Authenticator to their device.
 - i. When the user clicks “View Download Options”, the Beyond Identity Authenticator downloads page will open in a browser with all supported platforms displayed. The user should download and install the Beyond Identity Authenticator on their device if they have not already.

- ii. Now that the user has the Authenticator installed on their device, they should proceed to Step 2 as there is not yet a user credential associated with the Authenticator on that device.
- b. Step 2: Register their Credential in the Beyond Identity IdP.
 - i. By clicking on Step 2 “**Register New Credential**”, the user’s credential will get enrolled in the Beyond Identity service on the back end. On the front end, users who click Step 2 will be taken to the Beyond Identity Authenticator where they will see the progress of their credential registration. Once completed, the user will see a credentials in the Authenticator.
 - ii. See example image below:

