



Badge Setup Guide:

CyberArk Identity Integration via OIDC

Confidential Information of Badge Inc.

Table of Contents

Getting Started and Prerequisites.....	3
Prerequisites	3
Step 1: Configuring Badge.....	3
Client Name.....	4
Client Secret	4
Logo URI.....	4
Redirect URI	5
Grant Types	5
OIDC Response Types	5
OAuth Scopes	5
Client Authentication Method	5
Completing Badge's OIDC Setup – OIDC Client ID.....	5
Step 2: Configuring CyberArk Identity.....	6
External Identity Provider – Settings.....	6
External Identity Provider – Group Mappings.....	7
External Identity Provider – Inbound Metadata	7
External Identity Provider – Outbound Metadata	7
External Identity Provider – Authentication	8
External Identity Provider – Routing Rules	8
Step 3: Testing and Rollout.....	9
Initial Testing.....	9
Wider Rollout	9
FAQ's and Troubleshooting.....	10

Getting Started and Prerequisites

This setup guide walks a Badge administrator through integrating Badge with their CyberArk Identity deployment. In this architecture, Badge may perform some or all authentication of users to CyberArk Identity.

Badge will be configured as an external identity provider (IdP) as defined by CyberArk Identity. This is sometimes referred to as Inbound Federation to CyberArk Identity. A CyberArk Identity rule will be configured so that all users of specified domains accessing CyberArk Identity will use Badge for authentication. CyberArk Identity will behave like an Identity broker for authentication, allowing these users to authenticate through Badge to access any apps or services connected to CyberArk Identity.

Completing this integration involves setting up OIDC configuration parameters in your Badge deployment as well as OIDC parameters in your CyberArk Identity deployment. This guide begins with the Badge configuration and then covers the steps required in CyberArk Identity. User synchronization via SCIM is covered in a different setup guide.

Prerequisites

You will need:

- CyberArk Workforce Identity
- Badge SaaS or Badge on-prem

Before starting the below steps, it may be helpful to review this process from the CyberArk Identity perspective which is described as adding an external identity provider via OIDC. See the CyberArk Identity [Federate with an external IdP using OIDC instructions](#) on this process.

Step 1: Configuring Badge

Navigate to your Badge admin web console and login. If you are using Badge SaaS, navigate to <https://bageinc.com/ui/admin>. If you are using Badge on-prem, navigate to the domain or IP address of the server hosting Badge with the same path. For example, “<https://127.0.0.1/ui/admin>”.

Navigate to Applications->OIDC Clients. Click “New Client” to create a new OIDC connection.



Create Client

Client Name *

This name will be displayed to users when they log in to the client application with badge.

Client Secret *

Secret used to authenticate this client with Badge if "Client Secret" is selected for "Client Authentication Method". This value is not stored in plaintext by Badge, and it **cannot be recovered** if lost. You must store it securely yourself.

Logo URI

URI for a logo image to display during login.

Redirect URI *

URI to redirect to upon OAuth completion.

Advanced Options

Grant Types *

Authorization Code Refresh Token

OAuth grant types that can be requested by this client.
For more info, see [OAuth2 Grant Types](#).

OIDC Response Types *

code id_token token none code token code id_token
id_token token code id_token token

Response types that can be requested by this client.
For more info, see [OAuth Response Types](#) and [OIDC Response Types](#).

OAuth Scopes *

openid email profile

OAuth scopes that can be requested by this client.

Client Authentication Method *

Client Secret (POST Body)

Method that the client will use to authenticate with Badge. Set this to **Client Secret (Basic Auth)** or **Client Secret (POST Body)** for web applications with a backend server that will authenticate by passing the secret back to Badge. Set this to **Private Key JWT** for web applications with a backend server that will authenticate by passing a **JSON Web Token** signed by JWKS. Clients using this auth method must register a **JSON Web Key Set** by providing either a JWKS URI or JSON Web Key Set. Set this to **None** for mobile apps or client-only web apps. For more information on client authentication methods, see [OpenID Connect - Client Authentication](#).

CANCEL CREATE

Badge presents several fields to be defined to complete the setup. The following explains each field, whether it is optional or required, and what to place in it.

Client Name

Client name is required. This is the name that is presented to users when they log in to this OIDC client. In this case, **CyberArk Identity** would be a commonly used Client Name. You may choose a name that you prefer.

Client Secret

This field is required. This value is not stored in plaintext by Badge, and it **cannot be recovered** if lost. You must store it securely and have it ready for use in the next section. It is recommended to use a long and complex value. If this value is lost and needed again, you will have to start over by setting a new value here, and then setting that new value in CyberArk Identity as well.

Logo URI

This field is optional. This can be the path to a logo image that can be displayed to users during their login experience.

Redirect URI

Redirect URI is required. Enter any valid URL as a placeholder for now. You will return to this section and edit in the correct value once it is created in CyberArk Identity in the following section.

Grant Types

The two default values of `Authorization Code` and `Refresh Token` are required as minimums. Additional grant types are optional and not typically needed.

OIDC Response Types

The default values populated here upon creation are required. That includes `code`, `id_token`, `token`, `none`, `code token`, `code id_token`, `id_token token`, and `code id_token token`.

OAuth Scopes

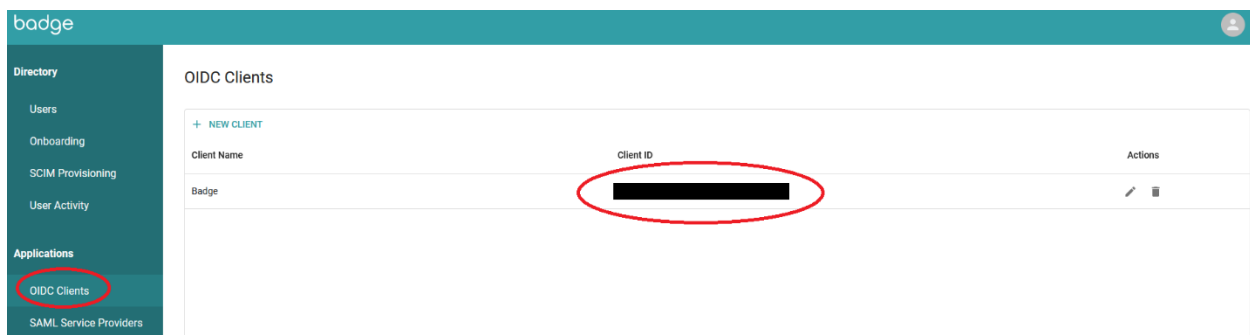
OAuth Scopes are required. At a minimum `openid`, `email`, and `profile` are required.

Client Authentication Method

Client Authentication Method is required. Set this to `Client Secret (POST Body)`.

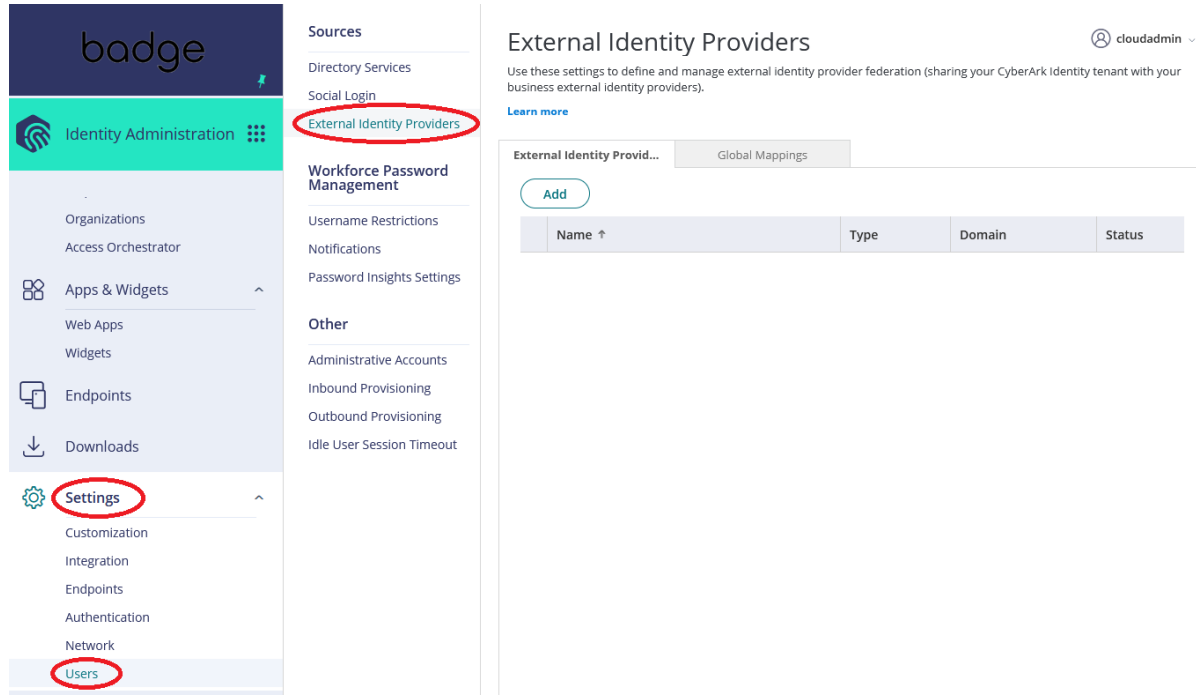
Completing Badge's OIDC Setup – OIDC Client ID

Go back to the Clients screen and you will see your newly created OIDC client listed as shown in the below screenshot. Note the client ID listed next to the name of your client, and have it on hand for use in the next section.



Step 2: Configuring CyberArk Identity

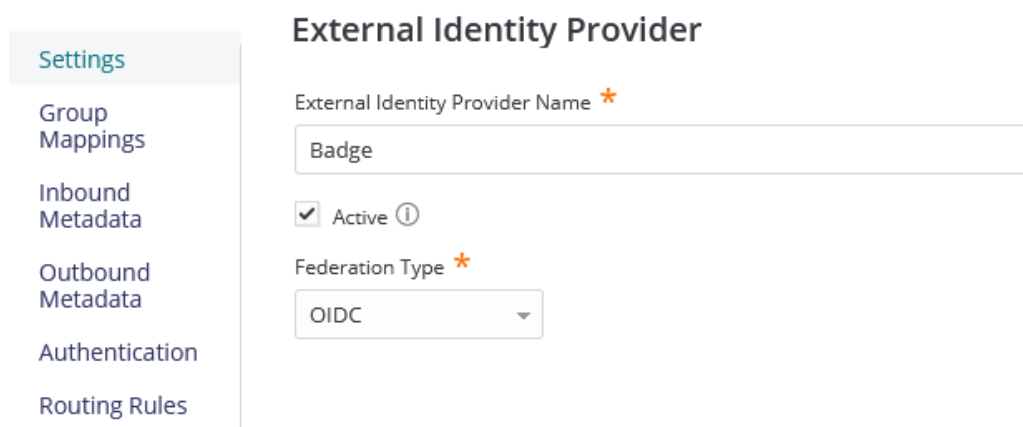
Login to your CyberArk Identity admin console and navigate to **Settings -> Users -> External Identity Providers** as shown in the below screenshot.



Select the **Add** button to continue. The following fields on each page will need to be filled in as part of that process.

External Identity Provider – Settings

Enter **Badge** as the External Identity Provider Name, select **OIDC** as the Federation type, and tick the box to set this Active. Your page should look like the following screenshot.



Select **Group Mappings** to proceed.

External Identity Provider – Group Mappings

Leave this page blank. No group mappings are needed. Select **Inbound Metadata** to proceed.

External Identity Provider – Inbound Metadata

Select **Authorization Code** as the grant type and disable PKCE. Enter the Client ID and Client Secret that you retrieved and defined in the previous Badge configuration section above. For Metadata URL, enter <https://login.badgeinc.com/.well-known/openid-configuration> as shown in the following screenshot.

The screenshot shows the 'External Identity Provider' configuration page. On the left is a sidebar with navigation links: Settings, Group Mappings, Inbound Metadata (highlighted), Outbound Metadata, Authentication, and Routing Rules. The main content area is titled 'External Identity Provider' and contains the following fields:

- Configure the Open ID provider settings for this external identity provider.**
- Select the grant type ***: A dropdown menu with 'Authorization Code' selected.
- Enable PKCE**: An unchecked checkbox.
- Client ID ***: A text input field containing a redacted value, with a 'Copy' button to its right.
- Client Secret ***: A text input field containing a redacted value, with a 'Copy' button to its right.
- Metadata URL ***: A text input field containing 'dgeinc.com/.well-known/openid-configuration', with a 'Copy' button to its right.

Select **Outbound Metadata** to proceed.

External Identity Provider – Outbound Metadata

Edit Scopes to include **openid**, **profile**, and **email**. Your page should look similar to the following screenshot.

The screenshot shows the 'External Identity Provider' configuration page. On the left is a sidebar with navigation links: Settings, Group Mappings, Inbound Metadata, Outbound Metadata (highlighted), Authentication, and Routing Rules. The main content area is titled 'External Identity Provider' and contains the following fields:

- Setup the RP settings and provide to external identity providers with whom you will federate.**
- Redirect URL ***: A text input field containing a redacted value, with a 'Copy' button to its right.
- Initiate login URL ***: A text input field containing a redacted value, with a 'Copy' button to its right.
- Post logout redirect URI ***: A text input field containing a redacted value, with a 'Copy' button to its right.
- Scopes ⓘ**: A dropdown menu with 'openid', 'profile', and 'email' selected.

Badge Proprietary and Confidential. Do not distribute.

Copy the Redirect URL shown. In another window, navigate back to the Badge web admin page -> OIDC Clients. Edit the OIDC client you created in Step 1 above. Replace the placeholder URL used for Redirect URI with the Redirect URL from CyberArk Identity. Re-enter the same Client Secret from Step 1 above. Select Update to save and finish.

Back in CyberArk Identity, select **Authentication** to proceed.

External Identity Provider – Authentication

Select **Required** for “Map federated user to existing directory user.” Enter **email** for “Federated user attribute to be mapped.” Select **CyberArk Cloud Directory** for “Mapped Directory service.” Select **Name** for “Directory user attribute to be mapped.” Ensure no checkboxes are selected. Your page should look like the following screenshot.

The screenshot shows the 'External Identity Provider' configuration page. On the left is a sidebar with navigation links: Settings, Group Mappings, Inbound Metadata, Outbound Metadata, Authentication (highlighted), and Routing Rules. The main content area is titled 'External Identity Provider' and contains the following settings:

- 'Map federated user to existing directory user' is set to 'Required' via a dropdown menu.
- 'Federated user attribute to be mapped' is set to 'email' in a text input field.
- 'Mapped Directory service' is set to 'CyberArk Cloud Directory' via a dropdown menu.
- 'Directory user attribute to be mapped' is set to 'Name' in a dropdown menu.
- Four checkboxes are present at the bottom, all of which are unchecked:
 - Update cloud users with federated user attributes
 - Add mapped users to federated groups
 - Allow mapping to users in other federations
 - Create cloud user if unable to map

Select **Routing Rules** to proceed.

External Identity Provider – Routing Rules

Select **Add** and enter the domain(s) of the users that will use Badge to authenticate into CyberArk Identity. Any user whose username ends in a domain defined here will be routed to authenticate with Badge during the CyberArk Identity login process.

It is recommended to also create a CyberArk Identity role named **Badge Users** or similar. This will allow you to control testing and rollout in the next section. Only users that are both in the defined domains *and* in the role will be routed to use Badge as an authenticator.

Your page should look similar to the following screenshot.

Settings

Group Mappings

Inbound Metadata

Outbound Metadata

Authentication

Routing Rules

External Identity Provider

Configure the routing rules to route the user to the external identity provider for authentication. At least one condition must be provided. If more than one condition is added, then all the conditions must be satisfied.

Federated Domains ⓘ

Add

Name	
your-domain-here.com	

User Agent ⓘ

Any

Roles ⓘ

Badge Users

Save

Cancel

Select **Save** at the bottom of the page to finish. Congratulations, you have completed the setup and configuration of Badge and CyberArk Identity!

Step 3: Testing and Rollout

Initial Testing

In CyberArk Identity, choose or create a new user for the purposes of testing. Ensure that the test user exists in one of the federated domains and is assigned into the defined role. Navigate to your Badge web admin page and create the user in the Users page.

In a new browser or incognito window, navigate to your CyberArk Identity tenant login page. Attempt to log in as the test user. You will be redirected to Badge to complete the one-time factor enrollment, then complete the login process.

Wider Rollout

At this point, you have proven the functionality of the Badge and CyberArk OIDC integration. Next, it is recommended to set up a SCIM connection between Badge and CyberArk Identity so that users are automatically synchronized from CyberArk Identity into Badge, eliminating the need to manually create users in the Badge admin web page.

To continue your rollout, add users or groups to the assigned role as you see fit and ensure that all appropriate domains are defined in the routing rules page of the External Identity Provider settings.

Badge Proprietary and Confidential. Do not distribute.

FAQ's and Troubleshooting

The following are some common questions or points to be aware of during setup, testing, and troubleshooting. If your questions are not answered by the below points, reach out to info@badgeinc.com for further assistance .

When entering the OIDC parameters in CyberArk Identity, ensure that values are entered precisely. For example, it is common to accidentally introduce a trailing space or miss a trailing / which will result in errors.