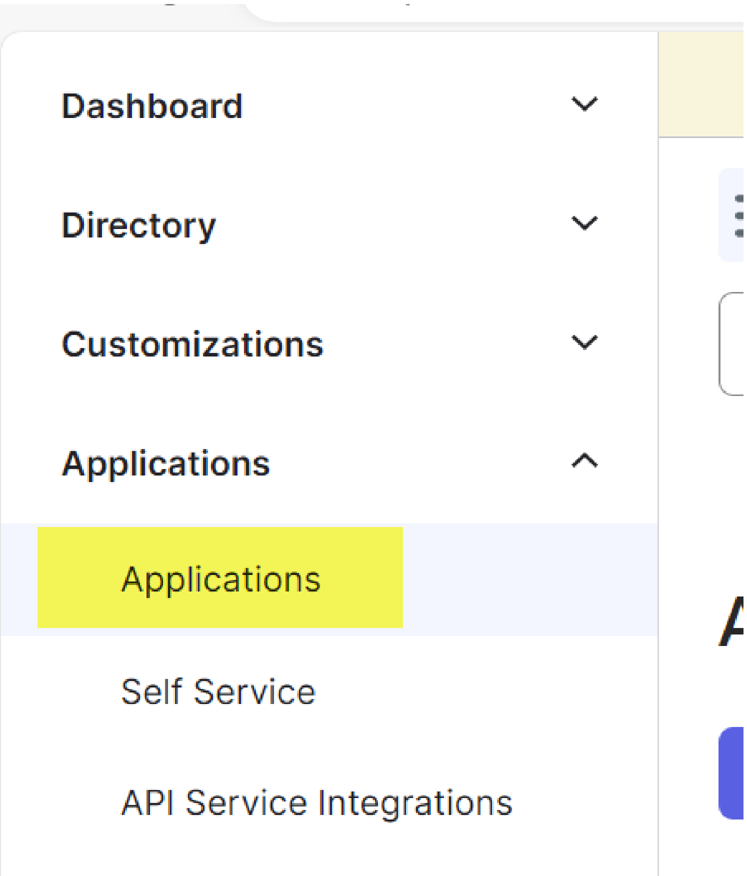
Introduction

This document provides an example of how to configure Okta as the Identity Provider supporting Single Sign-on into the RadiantOne Control Panel. This configuration has been validated for RadiantOne v8.

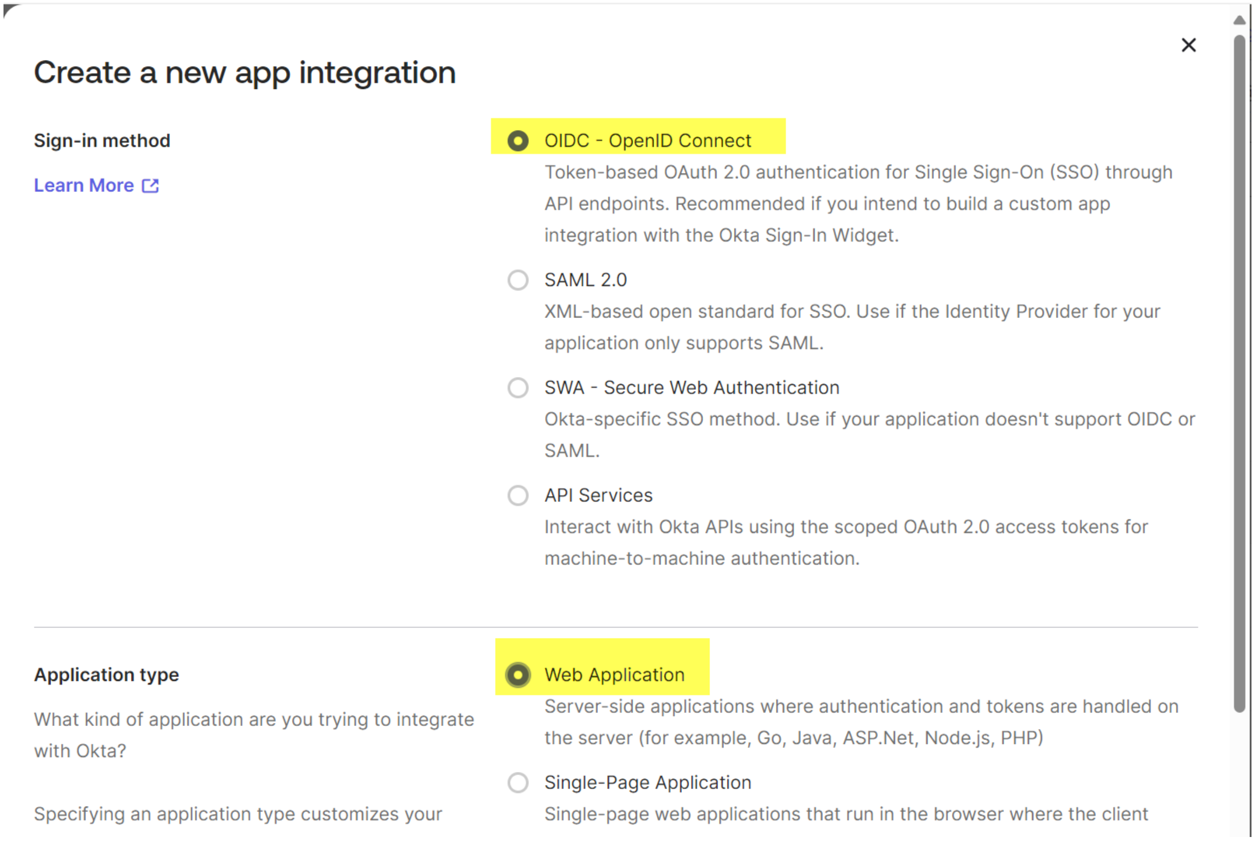
Okta Configuration

Perform the following steps in your Okta tenant.

1. Login with an administrator account and go to Administration > Applications > Applications.



2. Click CREATE APP INTEGRATION.
3. Select OIDC for the sign-in method and Web Application for the type.



Create a new app integration

Sign-in method

Learn More

● OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

○ SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

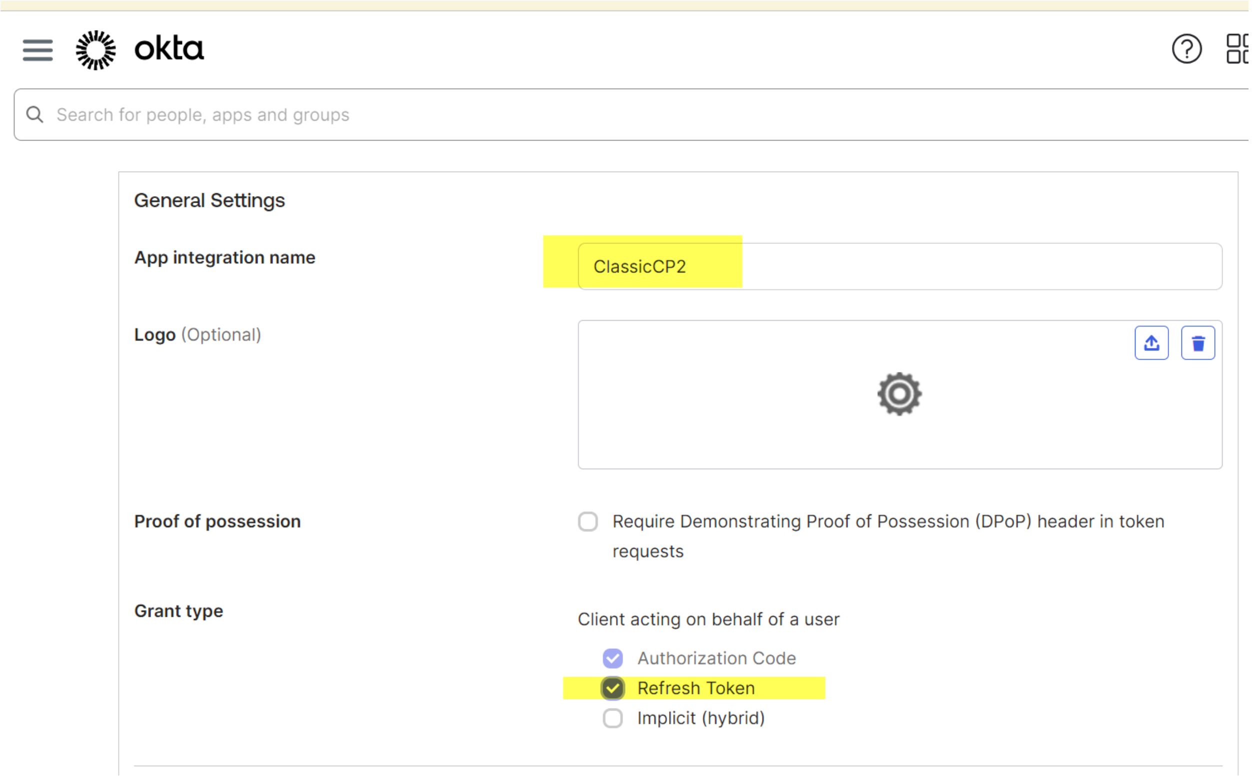
What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your

● Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

○ Single-Page Application
Single-page web applications that run in the browser where the client

4. Click NEXT.
5. Enter App Integration Name and choose "Refresh Token" for grant type.



General Settings

App integration name: ClassicCP2

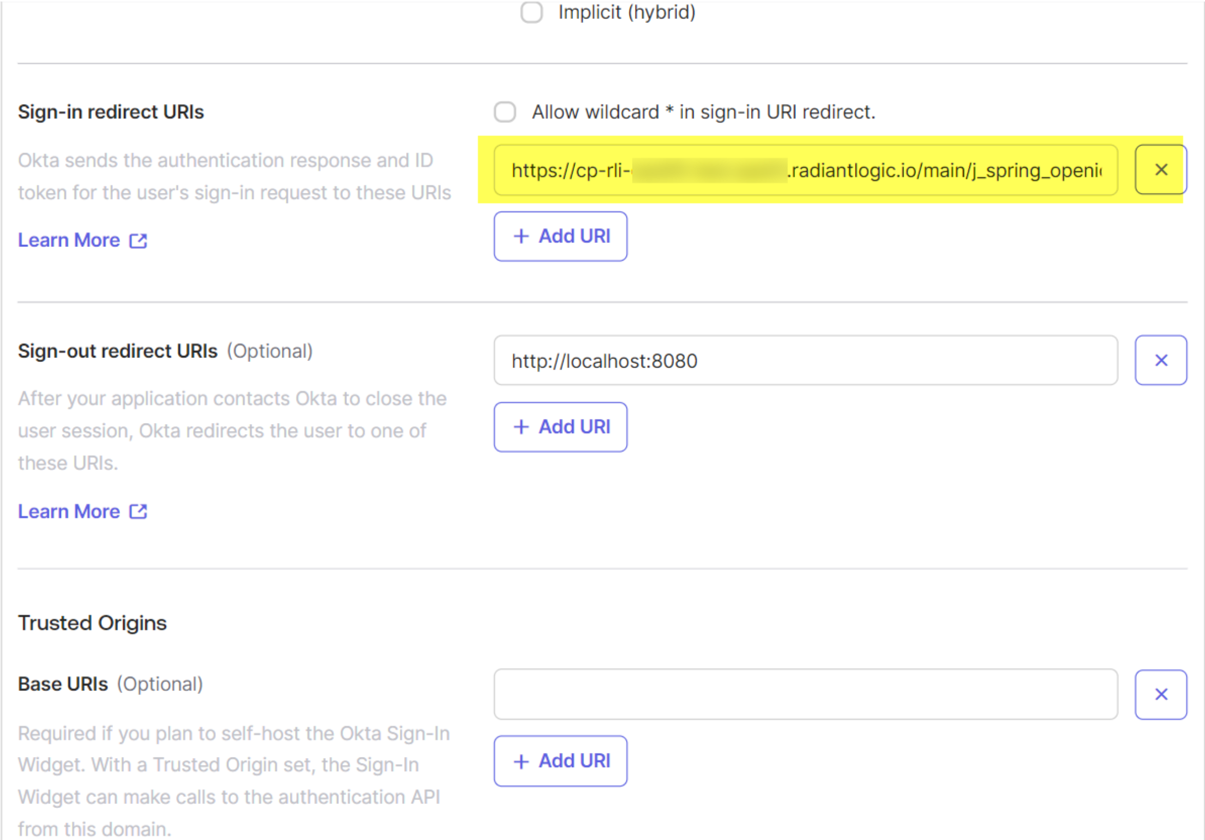
Logo (Optional)

Proof of possession: □ Require Demonstrating Proof of Possession (DPoP) header in token requests

Grant type: Client acting on behalf of a user

☑ Authorization Code
☑ Refresh Token
□ Implicit (hybrid)

6. Enter the URL for the Control Panel in the Sign In Redirect URI. An example is shown below. *https://cp-rli-naregion.radiantlogic.io/main/j_spring_openid_security_check*



□ Implicit (hybrid)

Sign-in redirect URIs

□ Allow wildcard * in sign-in URI redirect.

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

Learn More

https://cp-rli-[redacted].radiantlogic.io/main/j_spring_openi

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

Learn More

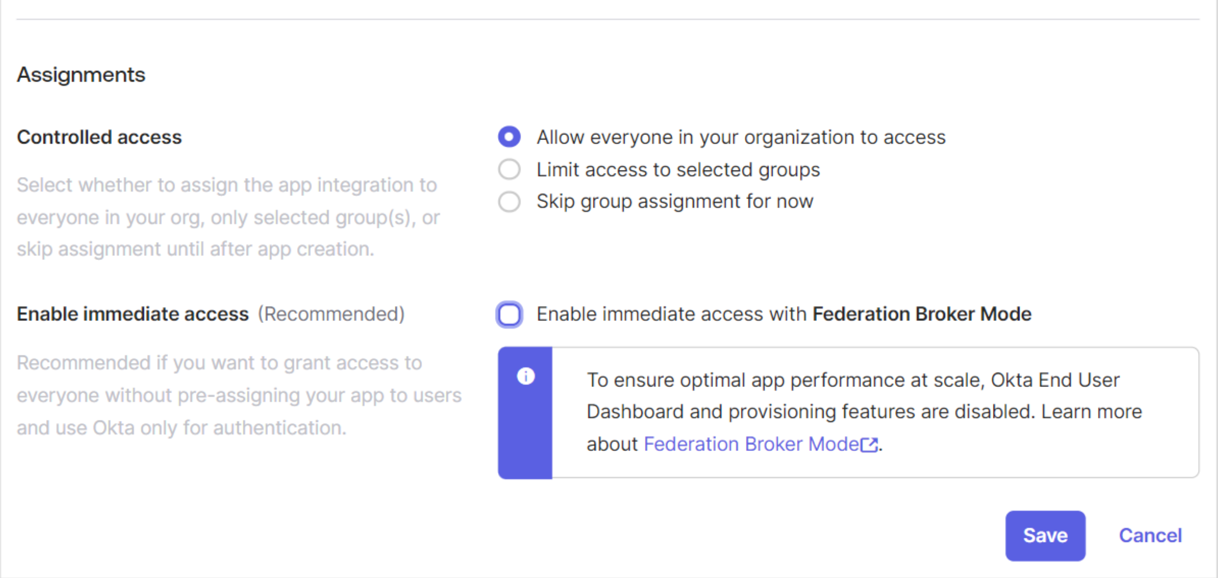
http://localhost:8080

Trusted Origins

Base URIs (Optional)

Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.

7. Select the applicable authorization and click SAVE.



Assignments

Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

● Allow everyone in your organization to access
○ Limit access to selected groups
○ Skip group assignment for now

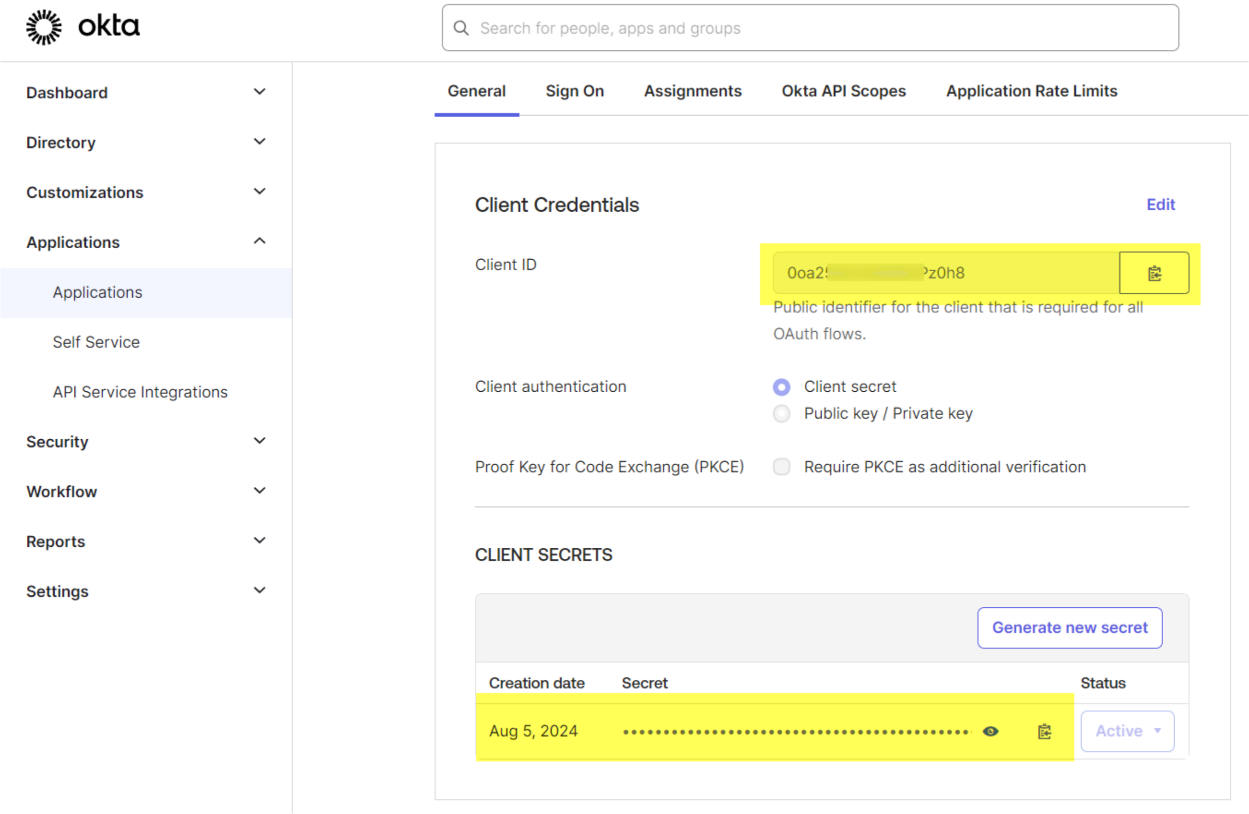
Enable immediate access (Recommended)

Recommended if you want to grant access to everyone without pre-assigning your app to users and use Okta only for authentication.

□ Enable immediate access with **Federation Broker Mode**

To ensure optimal app performance at scale, Okta End User Dashboard and provisioning features are disabled. Learn more about Federation Broker Mode.

8. On the GENERAL tab, copy the client ID and secret. These are required for the RadiantOne configuration.



Client Credentials

Client ID: 0oa2[redacted]z0h8

Public identifier for the client that is required for all OAuth flows.

Client authentication: ● Client secret ○ Public key / Private key

Proof Key for Code Exchange (PKCE): □ Require PKCE as additional verification

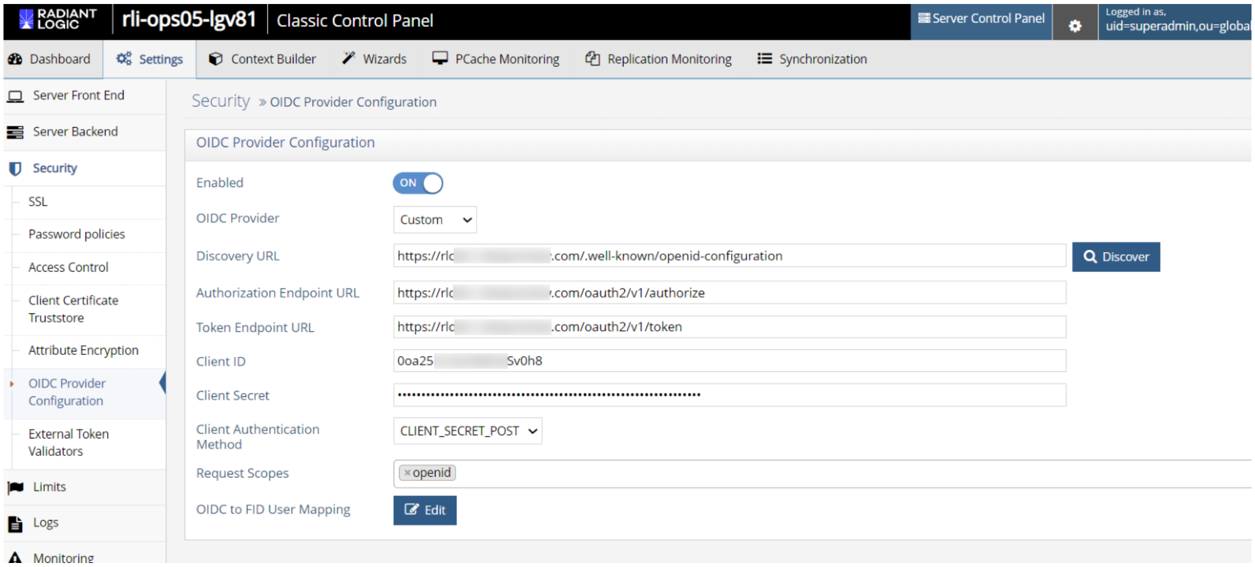
CLIENT SECRETS

Creation date	Secret	Status
Aug 5, 2024	••	Active

Control Panel Configuration

1. Log into the RadiantOne Control Panel as an administrator allowed to edit security settings.
2. Navigate to Settings > Security > OIDC Provider Configuration.
3. Enable the OIDC Configuration with the toggle.
4. Select CUSTOM from the OIDC Provider drop-down list.
5. Enter the OIDC discovery URL for the OKTA tenant and click Discover. This auto-populates the Authorization Endpoint URL and the Token Endpoint URL (you can manually enter these if needed).
6. Enter the Client ID and Client Secret you saved from the Okta setup into their respective properties.

7. This configuration uses the CLIENT_SECRET_POST authentication method and openid as the scope.



Enabled: ON

OIDC Provider: Custom

Discovery URL: https://rlc[redacted].com/.well-known/openid-configuration

Authorization Endpoint URL: https://rlc[redacted].com/oauth2/v1/authorize

Token Endpoint URL: https://rlc[redacted].com/oauth2/v1/token

Client ID: 0oa25[redacted]Sv0h8

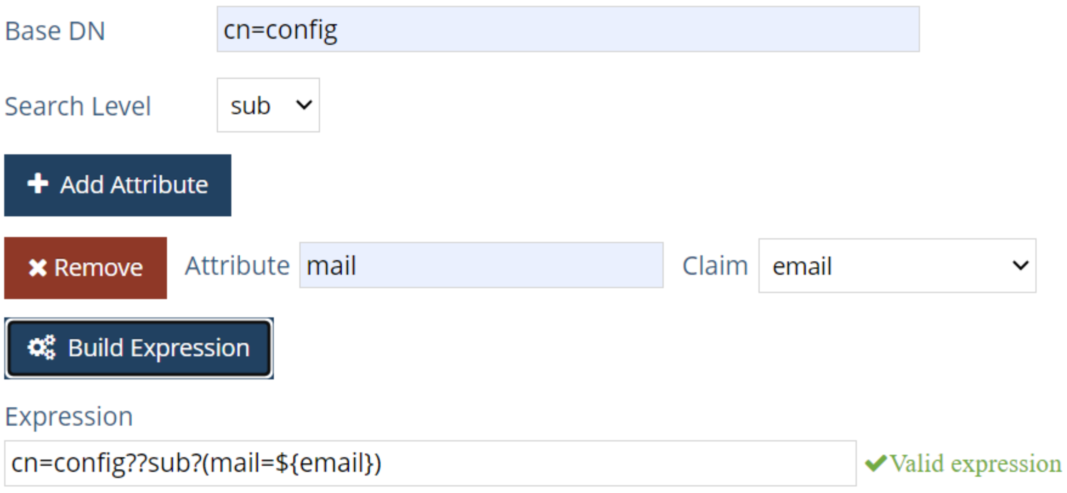
Client Secret: ••

Client Authentication Method: CLIENT_SECRET_POST

Request Scopes: ×openid

OIDC to FID User Mapping: Edit

8. Click EDIT next to OIDC to FID User Mapping. This setting is used to translate the account that authenticates with Okta to a delegated admin user in RadiantOne. This can be a simple mapping (DN substitution using claim values if needed) or a complex mapping with lookups in the RadiantOne namespace to match claim values to profile attributes. In the following example, the email claim received from the Okta authentication is used to lookup the identity in the RadiantOne namespace to locate the admin account below the cn=config naming context that has this value for the mail attribute.



Base DN: cn=config

Search Level: sub

Attribute: mail

Claim: email

Expression

```
cn=config??sub?(mail=${email})
```

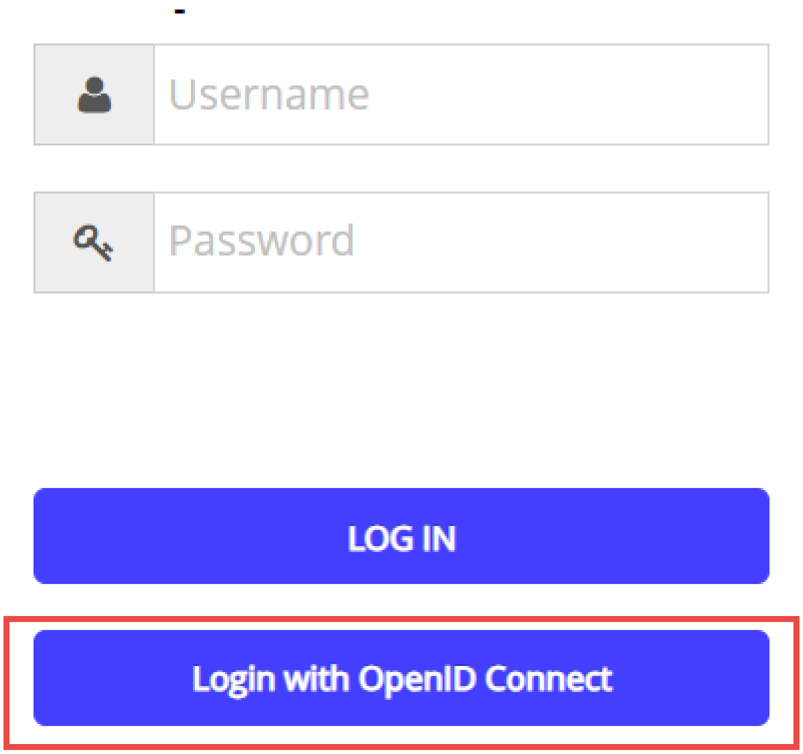
✓ Valid expression

9. Click Save.

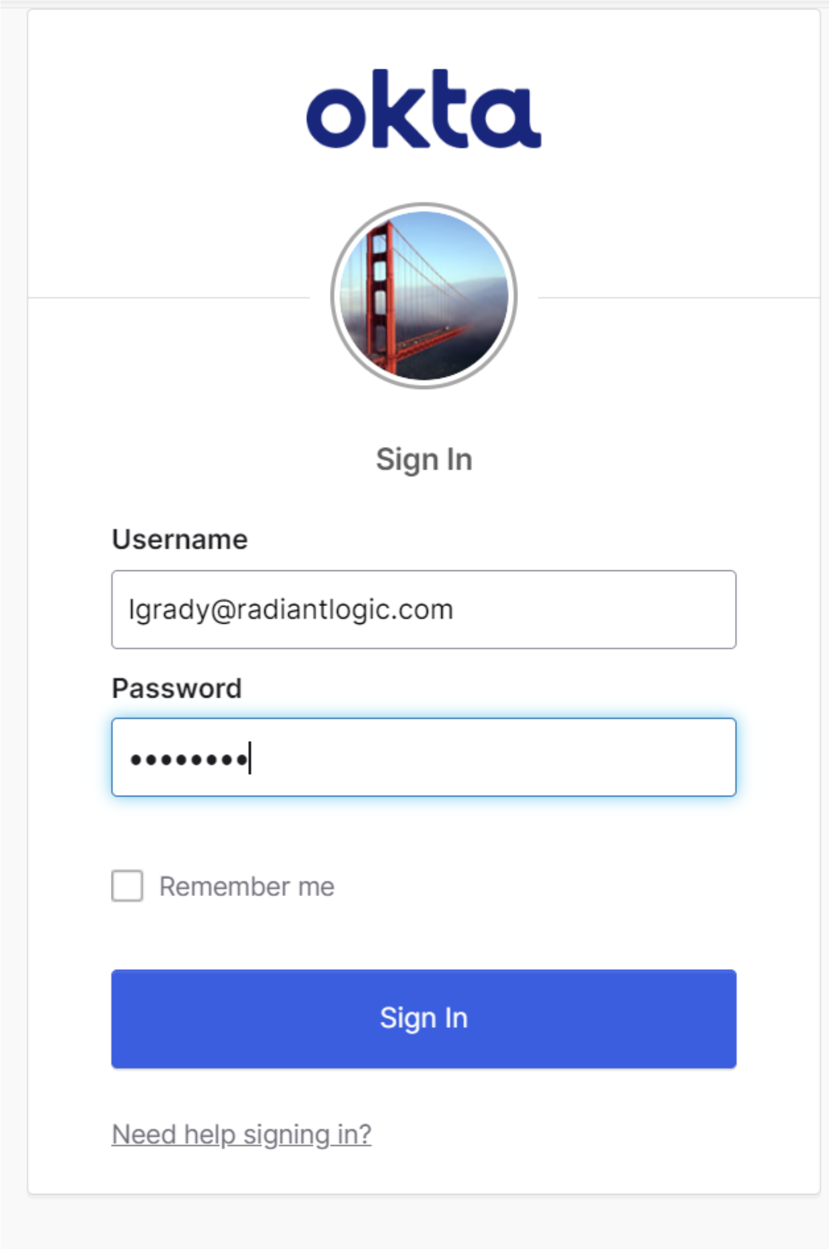
Testing SSO

To test SSO:

1. Log out of the RadiantOne Control Panel.
2. Click the **Login with Open ID Connect** option on the RadiantOne Control Panel.



This redirects to OKTA where the user (not already logged into OKTA) is prompted to login:



Sign In

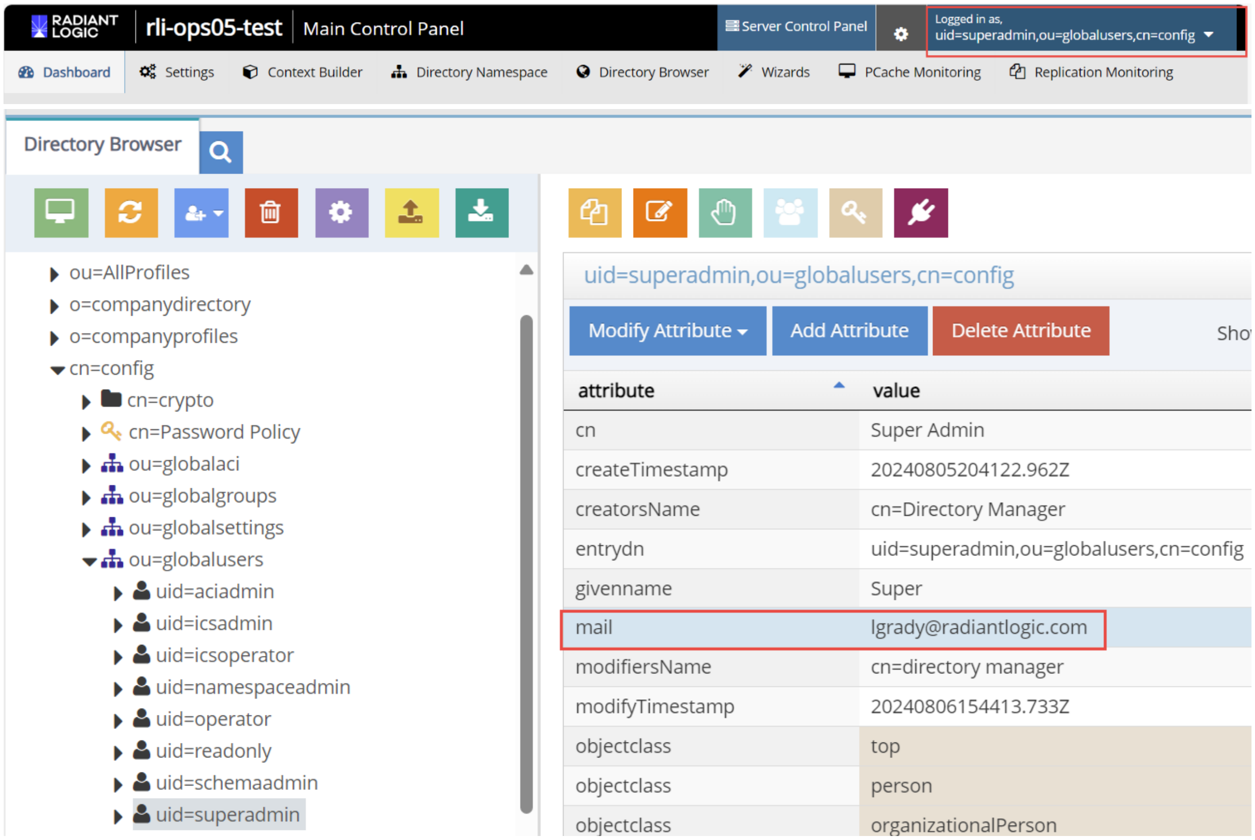
Username

lgrady@radiantlogic.com

Password

••••••••

3. After clicking "Sign In" the user should be automatically logged into the RadiantOne Control Panel as the admin account matching the OIDC to FID User Mapping.



uid=superadmin,ou=globalusers,cn=config

attribute	value
cn	Super Admin
createTimestamp	20240805204122.962Z
creatorsName	cn=Directory Manager
entrydn	uid=superadmin,ou=globalusers,cn=config
givenname	Super
mail	lgrady@radiantlogic.com
modifiersName	cn=directory manager
modifyTimestamp	20240806154413.733Z
objectclass	top
objectclass	person
objectclass	organizationalPerson