

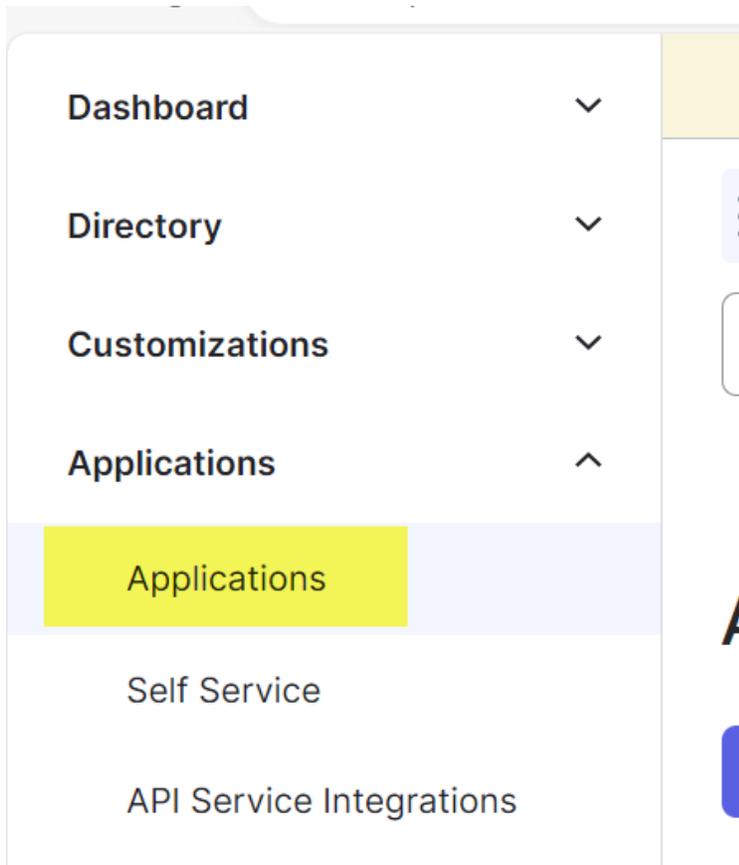
Introduction

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

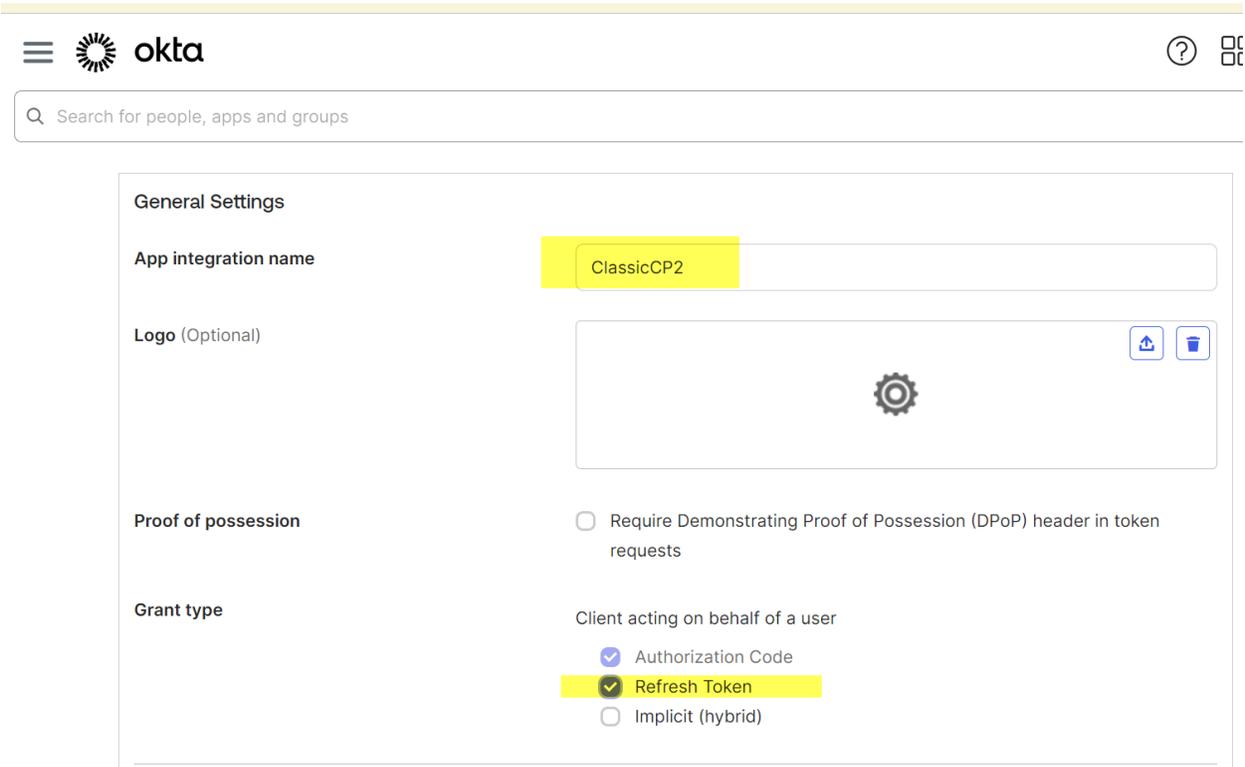
What kind of application are you trying to integrate with Okta?

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.



The screenshot shows the Okta SSO Control Panel configuration page. At the top left is the Okta logo and a search bar. The main content area is titled "General Settings" and contains the following fields:

- App integration name:** A text input field containing "ClassicCP2".
- Logo (Optional):** A large empty box with a gear icon in the center and upload/delete icons in the top right corner.
- Proof of possession:** A checkbox labeled "Require Demonstrating Proof of Possession (DPoP) header in token requests", which is currently unchecked.
- Grant type:** A section titled "Client acting on behalf of a user" with three radio button options:
 - Authorization Code (checked)
 - Refresh Token (highlighted in yellow)
 - Implicit (hybrid) (unchecked)

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

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

Allow wildcard * in sign-in URI redirect.

[Learn More](#) 

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](#) 

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

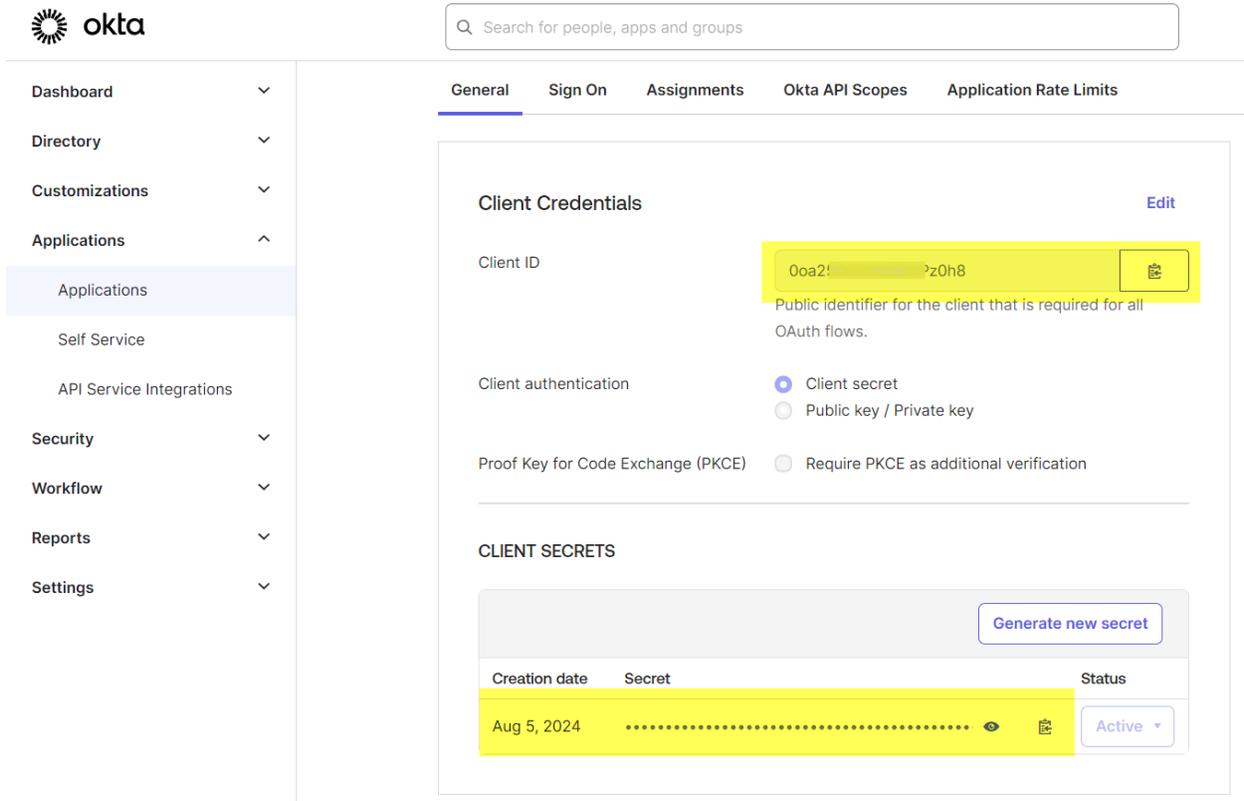
Enable immediate access (Recommended)

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**

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

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

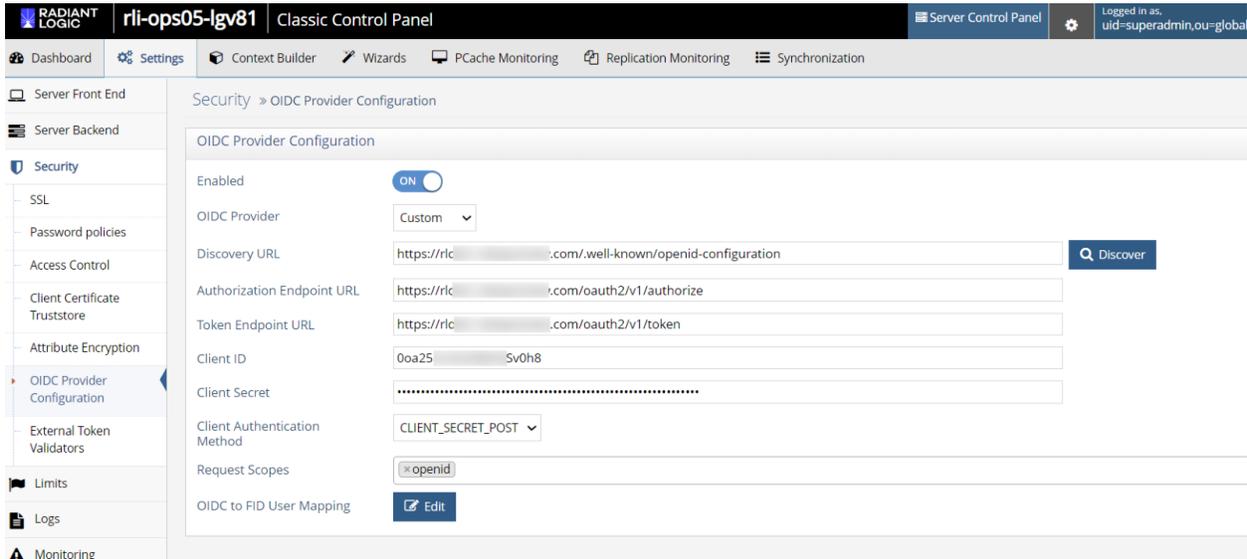


The screenshot shows the Okta SSO Control Panel interface. On the left is a navigation menu with options like Dashboard, Directory, Customizations, Applications, Self Service, API Service Integrations, Security, Workflow, Reports, and Settings. The main content area is titled 'Client Credentials' and has tabs for General, Sign On, Assignments, Okta API Scopes, and Application Rate Limits. The 'General' tab is active. Under 'Client Credentials', there is a 'Client ID' field containing '00a2!...' and 'z0h8'. Below it is a 'Client authentication' section with radio buttons for 'Client secret' (selected) and 'Public key / Private key'. There is also a 'Proof Key for Code Exchange (PKCE)' section with a radio button for 'Require PKCE as additional verification'. At the bottom, there is a 'CLIENT SECRETS' table with columns for 'Creation date', 'Secret', and 'Status'. A 'Generate new secret' button is located above the table. The table contains one entry with a creation date of 'Aug 5, 2024', a masked secret, and a status of 'Active'.

Control Panel Configuration

- Log into the RadiantOne Control Panel as an administrator allowed to edit security settings.
- Navigate to Settings > Security > OIDC Provider Configuration.
- Enable the OIDC Configuration with the toggle.
- Select CUSTOM from the OIDC Provider drop-down list.
- 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).
- Enter the Client ID and Client Secret you saved from the Okta setup into their respective properties.

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



The screenshot shows the 'OIDC Provider Configuration' page in the Okta SSO Control Panel. The page is titled 'Security > OIDC Provider Configuration'. The configuration is enabled. The OIDC Provider is set to 'Custom'. The Discovery URL is 'https://rlc...com/.well-known/openid-configuration'. The Authorization Endpoint URL is 'https://rlc...com/oauth2/v1/authorize'. The Token Endpoint URL is 'https://rlc...com/oauth2/v1/token'. The Client ID is '0oa25' and the Client Secret is 'Sv0h8'. The Client Authentication Method is 'CLIENT_SECRET_POST'. The Request Scopes are 'openid'. There is an 'Edit' button next to the 'OIDC to FID User Mapping' field.

- 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

Search Level ▼

+ Add Attribute

✕ Remove Attribute Claim ▼

⚙ Build Expression

Expression ✔ Valid expression

9. Click Save.

Testing SSO

To test SSO:

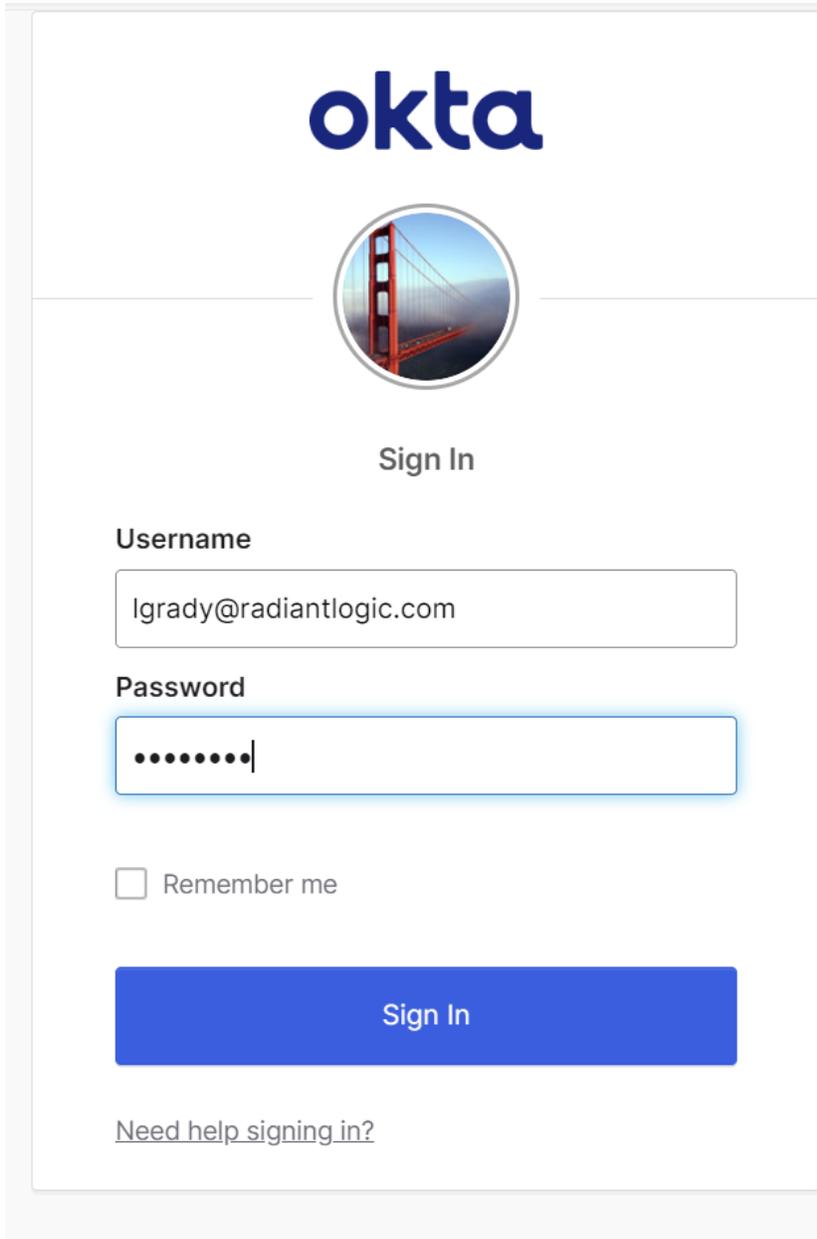
1. Log out of the RadiantOne Control Panel.
2. Click the **Login with Open ID Connect** option on the RadiantOne Control Panel.

-

LOG IN

Login with OpenID Connect

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



The image shows a screenshot of the Okta Sign In page. At the top center is the Okta logo. Below it is a circular profile picture placeholder containing an image of the Golden Gate Bridge. Underneath the profile picture is the text "Sign In". The form contains two input fields: "Username" with the value "lgrady@radiantlogic.com" and "Password" with masked characters "••••••••". Below the password field is a checkbox labeled "Remember me" which is unchecked. At the bottom of the form is a large blue button labeled "Sign In". Below the button is a link that says "Need help signing in?".

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.

RADIANT LOGIC rli-ops05-test Main Control Panel
Server Control Panel
Logged in as, uid=superadmin,ou=globalusers,cn=config

Dashboard Settings Context Builder Directory Namespace Directory Browser Wizards PCache Monitoring Replication Monitoring

Directory Browser

- ▶ ou=AllProfiles
- ▶ o=companydirectory
- ▶ o=companyprofiles
- ▼ cn=config
 - ▶ cn=crypto
 - ▶ cn>Password Policy
 - ▶ ou=globalaci
 - ▶ ou=globalgroups
 - ▶ ou=globalsettings
 - ▼ ou=globalusers
 - ▶ uid=aciadmin
 - ▶ uid=icsadmin
 - ▶ uid=icsoperator
 - ▶ uid=namespaceadmin
 - ▶ uid=operator
 - ▶ uid=readonly
 - ▶ uid=schemaadmin
 - ▶ uid=superadmin

uid=superadmin,ou=globalusers,cn=config

Modify Attribute
Add Attribute
Delete Attribute
Show

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