ORACLE

OpenID Connect Single Sign-On for Oracle CPQ with Oracle Identity Cloud Service Integration Guide

Oracle CPQ Updates 23B and Later

March 2023

TABLE OF CONTENTS

REVISION HISTORY

DATE	WHAT'S CHANGED	NOTES
31 MAR 2023		Initial document creation for Oracle CPQ 23B.

INTRODUCTION

Oracle CPQ 23B adds support for OpenID Connect (OIDC) as a Single Sign-On (SSO) option. OIDC is an extension of the existing OAuth Provider configuration available for use with Oracle Identity and Access Management (IAM)'s Identity Domains and Oracle Identity Cloud Services (IDCS). OIDC adds an identity layer to OAuth 2.0 that enables a federated SSO solution between Oracle and Custom Applications configured in IDCS.

OpenID Connect is based on RESTful web services using JSON schema that include an ID token for sharing user information, such as the type of credential used for authentication, when a user is authenticated, and user properties (e.g., first name, last name, email id).

> **Note:** This document references IDCS to refer to Oracle Identity and Access Management (IAM)'s Identity Domains and Identity Cloud Services (IDCS).

Purpose

This guide describes the steps to setup OpenID Connect SSO between Oracle CPQ Cloud & Oracle Identity Cloud Service (IDCS). This guide is intended for administrators responsible for integrations with OpenID Connect for Single Sign-On between Oracle CPQ and Oracle Identity Cloud. This guide assumes administrators have prior Oracle CPQ and IDCS experience.

Prerequisites

The following prerequisites are required:

- Oracle Identity Cloud instance
- Oracle CPQ site with Update 23B or later

Optionally, after OpenID Connect is setup between Oracle CPQ and Oracle Identity Cloud, administrators can integrate with Oracle CX Sales. Refer to the Integrating CX Sales with Oracle CPQ document in the Oracle Help Center.

INTEGRATION

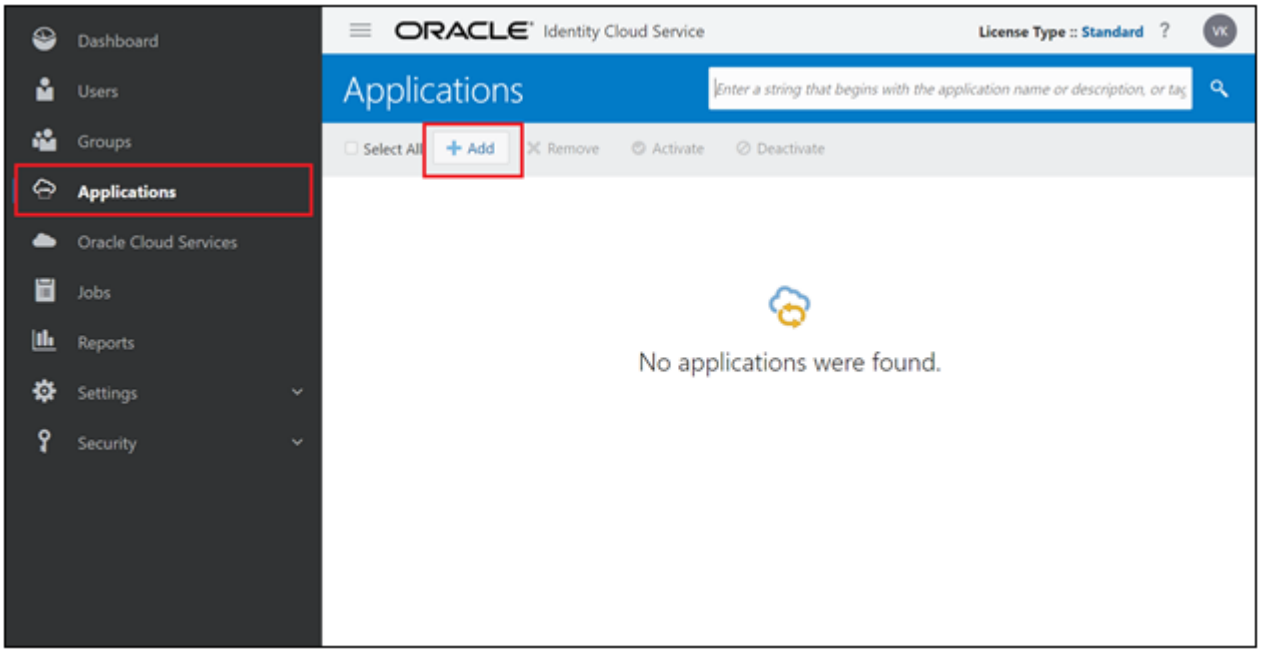
OpenID Connect integration between IDCS and Oracle CPQ requires the following high-level steps:

1. Register an OpenID Connect Client in IDCS
2. Create an OAuth Provider Integration in Oracle CPQ
3. Enable OpenID Connect for Single Sign-On
4. Set up Users

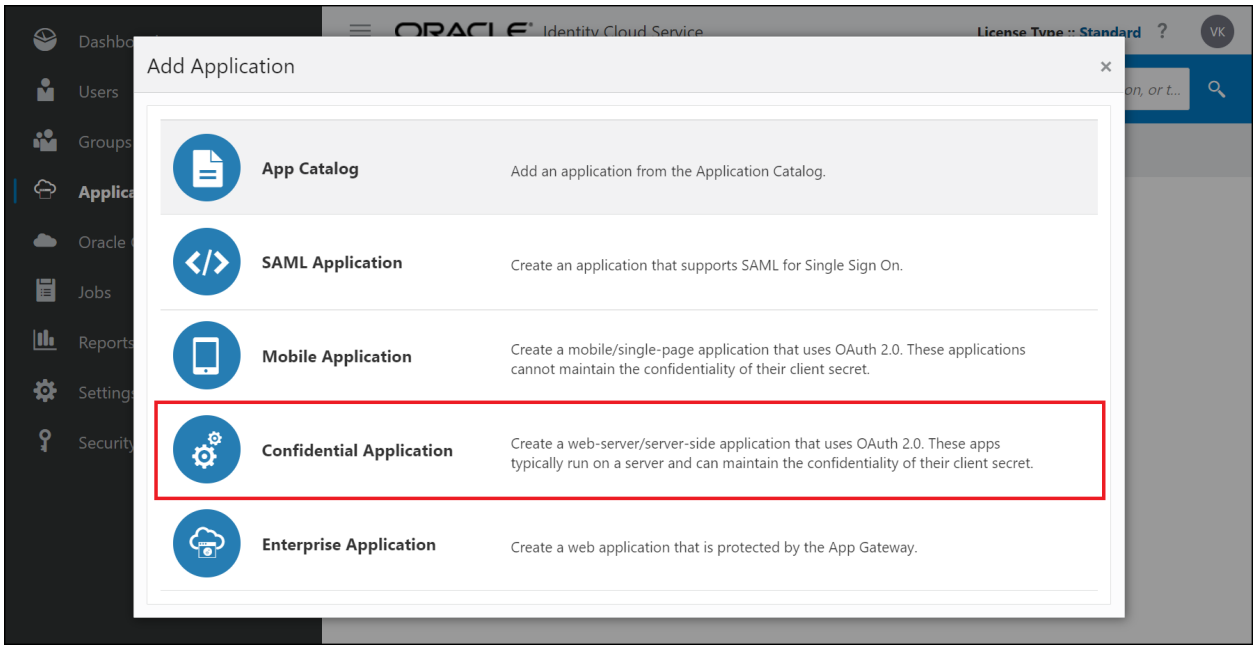
Register an OpenID Connect Client in IDCS

To register an OpenID Connect client in IDCS, perform the following steps:

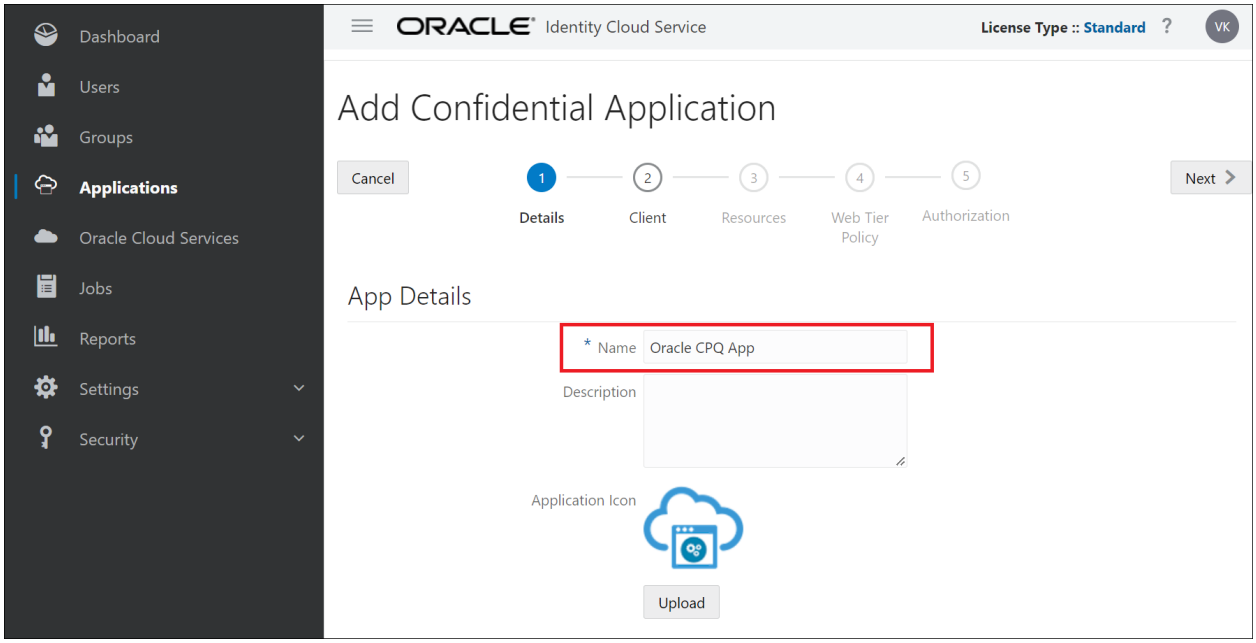
1. Login to IDCS.
2. Click on the **Navigation Drawer** to open the navigation menu.
3. Select **Applications**.
4. Click the **Add** button. The Add Application dialog box displays.



5. Click **Confidential Application**. The Add Confidential Application wizard displays.

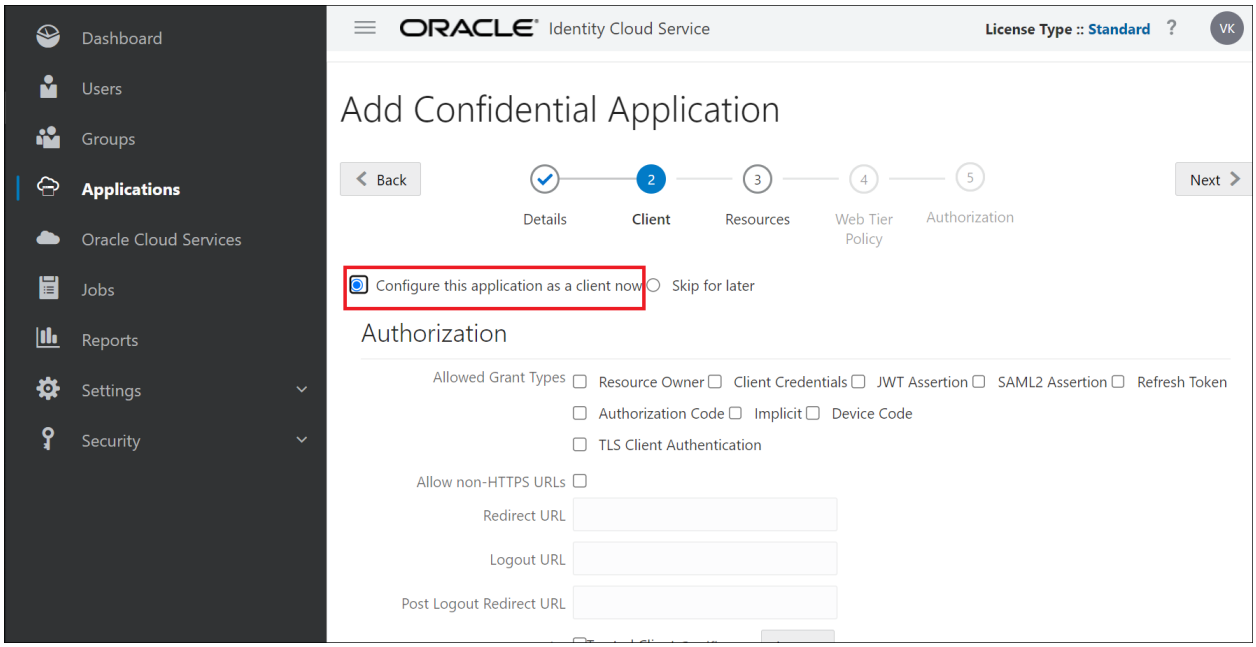


6. Enter the **Name** in the App Details section.
7. (Optional) Enter a **Description** for the application.

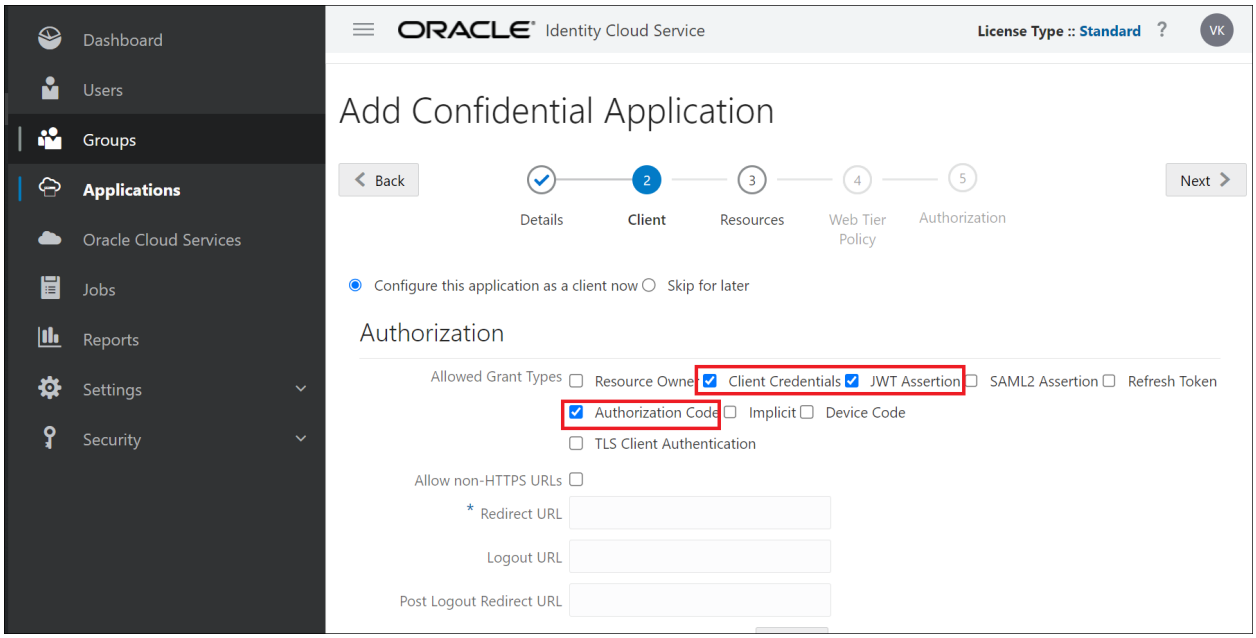


8. Click **Next**. The wizard moves to the Client details.

9. Select the **Configure this application as a client now** button.

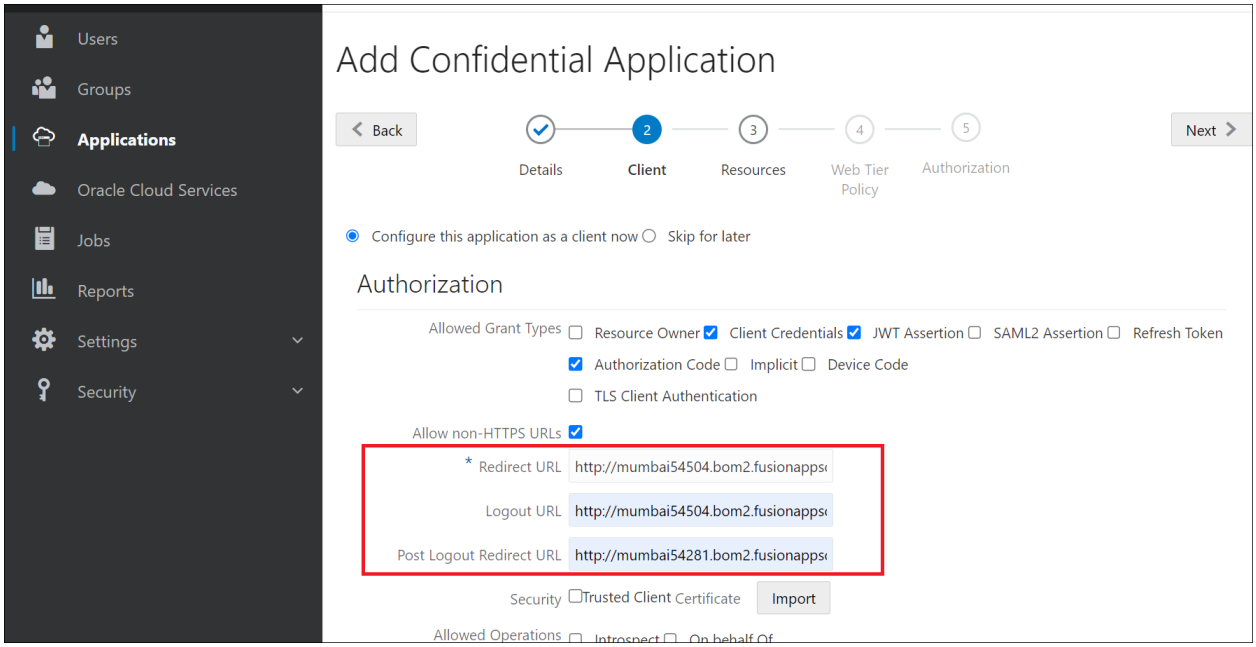


10. Select **Client Credentials** checkbox for Allowed Grant Types.
11. Select the **JWT Assertion** checkbox for Allowed Grant Types.
12. Select the **Authorization Code** checkbox for Allowed Grant Types.



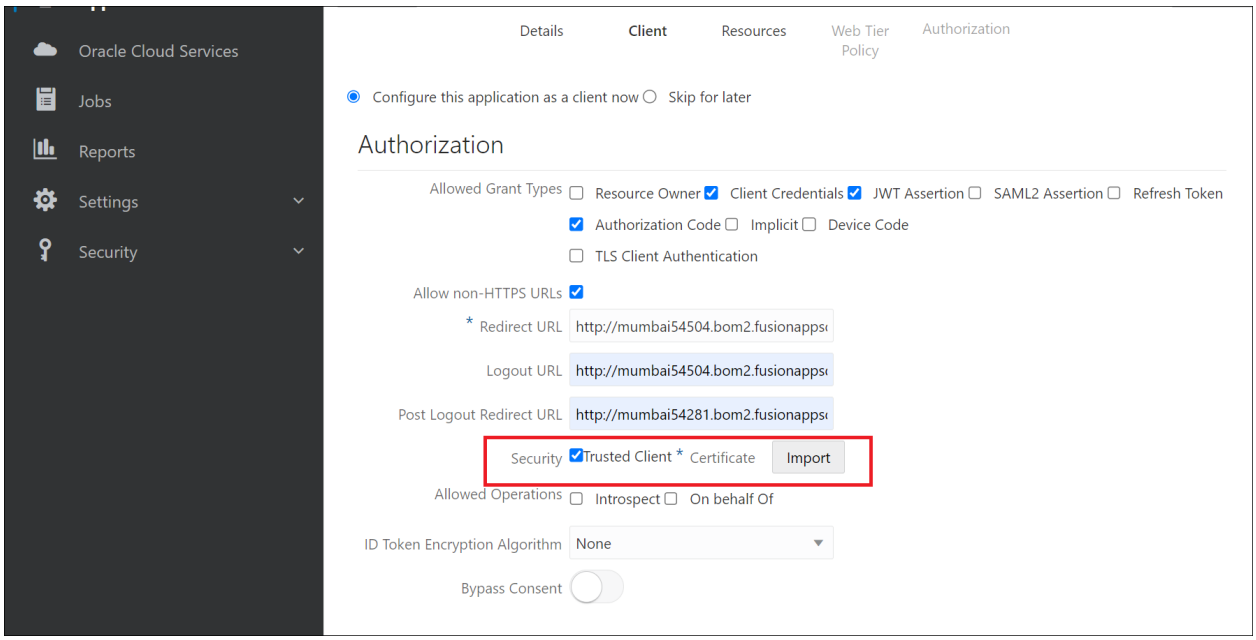
13. Enter valid value in **Redirect URL** field. For example:
`http://<cpqHostName>/sso/openid_connect_redirect.jsp`
14. Enter a valid value in the **Logout URL** field. For example: `http://<cpqHostName>/logout.jsp`

15. Enter a valid value in the **Post Logout Redirect URL** field. For example:
`http://<cpqHostName>/sso/openid_connect_request.jsp`



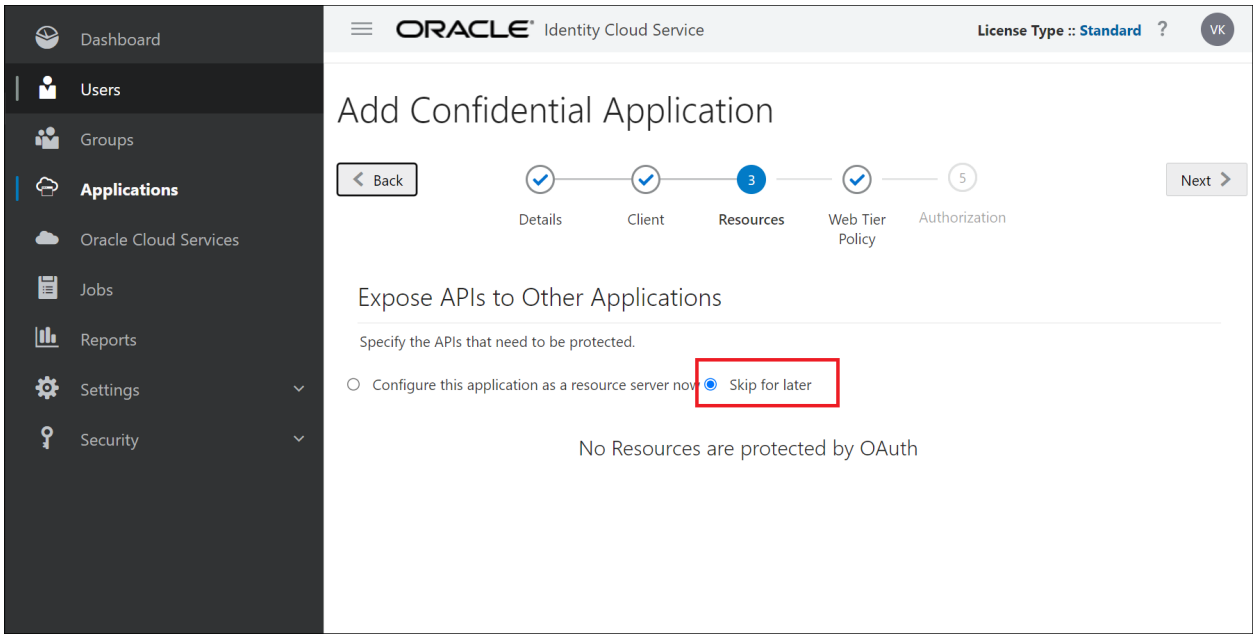
16. Select the **Trusted Client** checkbox for Security to make the Certificate option mandatory.

17. Click on the **Import** button to import the Oracle CPQ certificate. The certificate can be downloaded from the OAuth Provider page in the Oracle CPQ Integration Center.

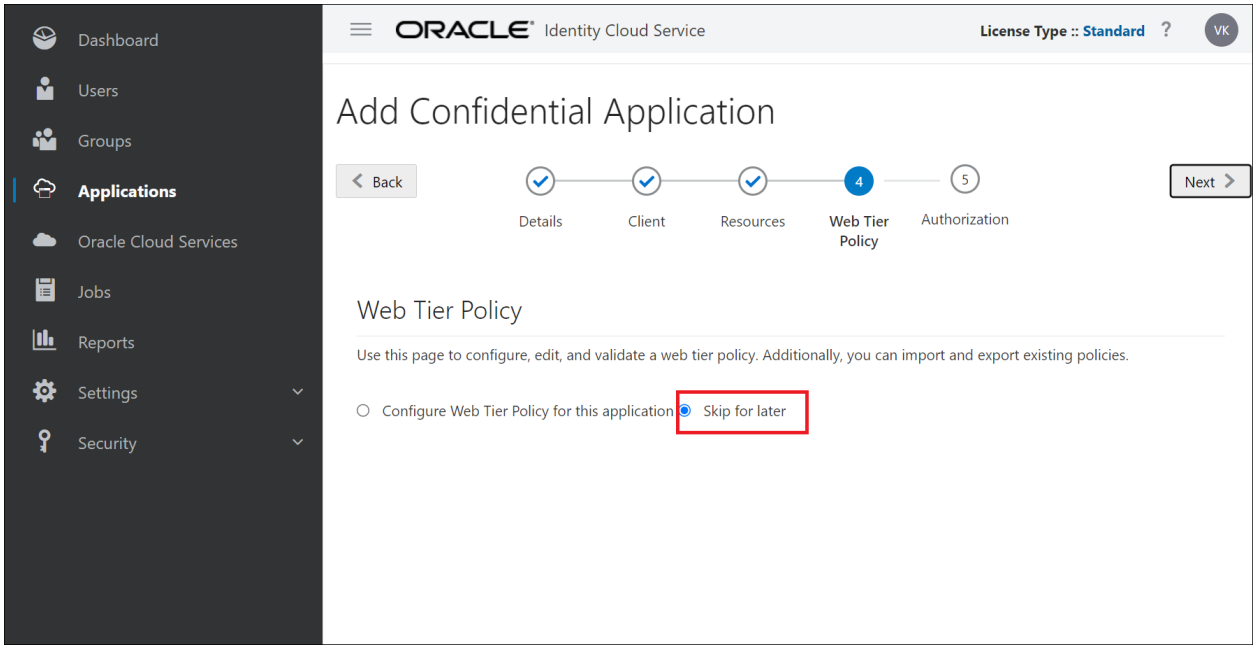


18. Click **Next** to configure Resources for the confidential application.

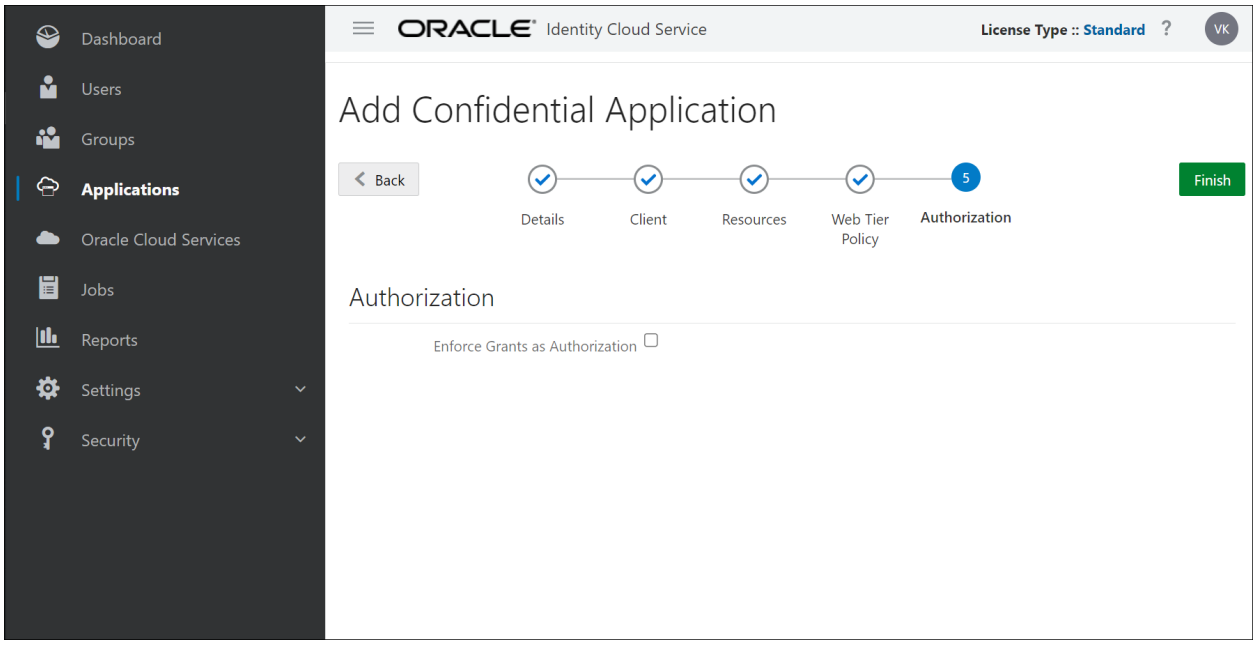
19. Select **Skip for later** for Expose APIs to Other Applications.



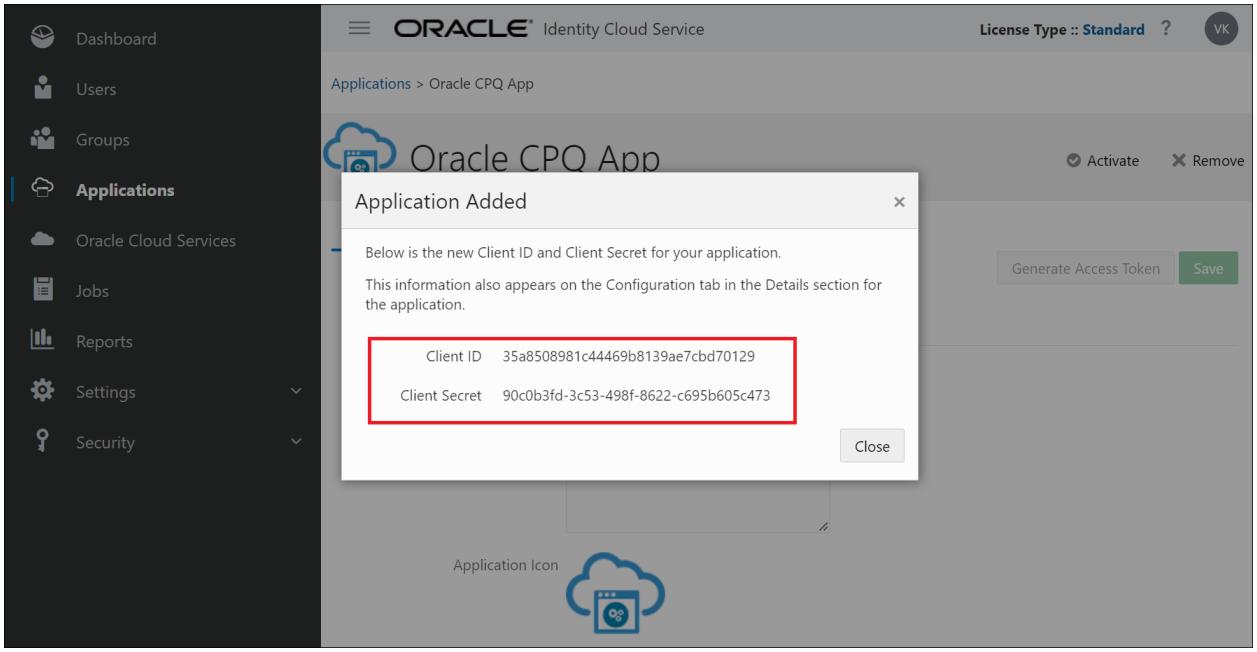
20. Select **Skip for later** for Web Tier Policy.



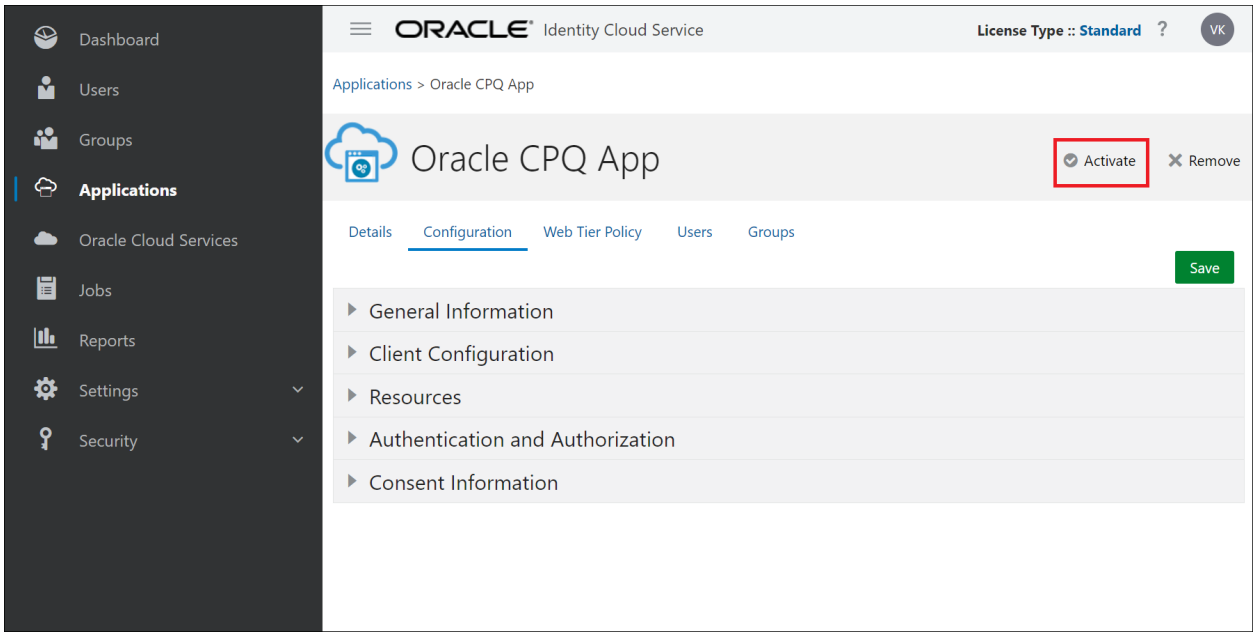
21. Click **Finish** for Authorization. The confidential application is created.



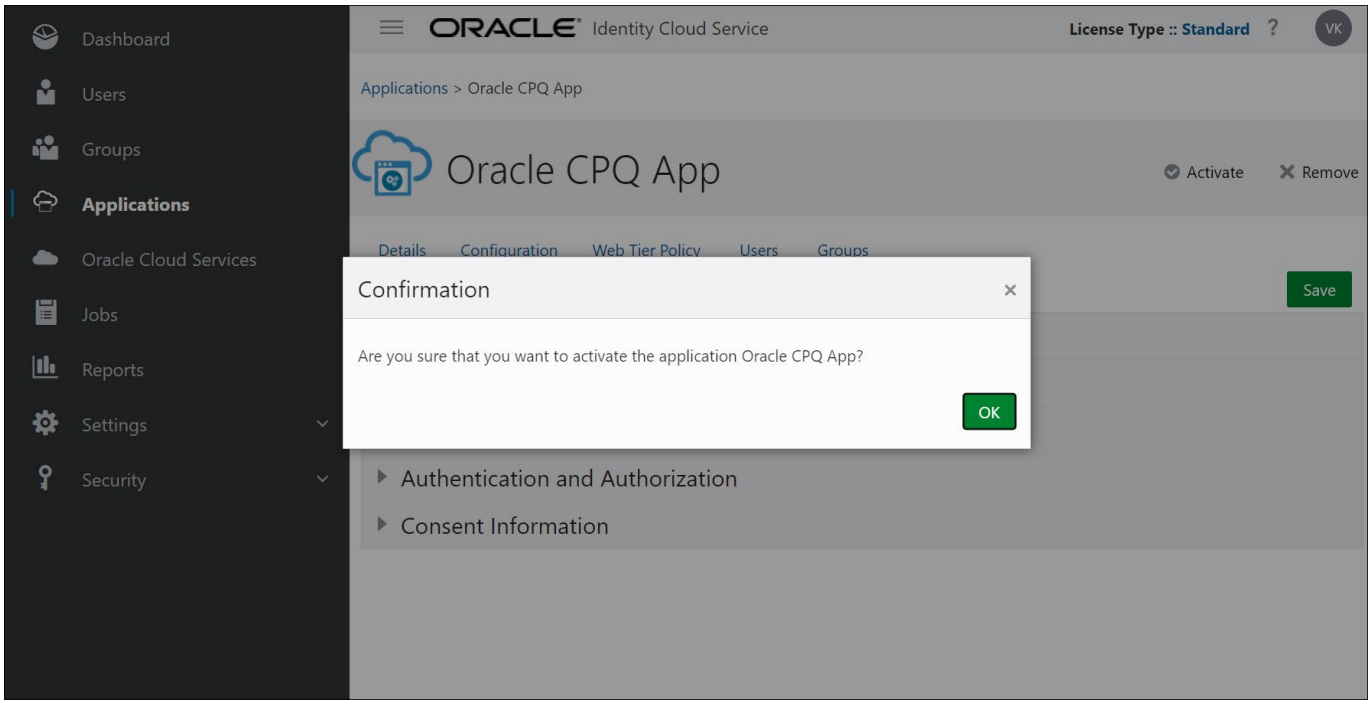
22. The Application Added dialog displays with the Client ID and Client Secret details. Note the **Client ID** & **Client Secret** as these are required to setup OAuth Provider in Oracle CPQ. Click **Close**.



23. Click **Activate** to activate the confidential application.



24. A confirmation dialog box displays, click **Ok**.



Create an OAuth Provider Integration in Oracle CPQ

Customers must open a Service Request (SR) on My Oracle Support to enable the OAuth Provider integration type in the Oracle CPQ Integration Center. When the integration type is enabled, administrators can use the Integration Center to create an OAuth Provider integration for CPQ. The OAuth Provider integration authenticates inbound and outbound REST communications with CPQ. Oracle CPQ customers should only enable this integration type when they want another OAuth provider, such as Oracle IDCS, to authenticate REST API calls with Oracle CPQ.

To set up Oracle IDCS as an OAuth Provider, perform the following steps:

1. Navigate to the Admin Home page.
2. Click **Integration Center** in the Integration Platform section. The Integration Center opens.
3. Click **Create Integration**.
4. Select **OAuth Provider** from the Type drop-down. The Vendor field defaults to the name of the OAuth Provider. This is a read-only field.
5. Enter the valid OAuth issuer name in the **Issuer** field. This field validates the access token obtained is issued by the correct provider.

   The OAuth Issuer for Oracle IDCS is: `https://identity.oraclecloud.com/`
6. Enter the base URL of the OAuth Provider in the **Tenant URL** field.
7. Enter the token endpoint used for obtaining the OAuth token in the **Token Endpoint** field.

   The Token Endpoint for Oracle IDCS is: `/oauth2/v1/token`
8. Enter the scope used for accessing the public key of the OAuth Provider in the **Scope** field.

   The OAuth Provider Scope for Oracle IDCS is: `urn:opc:idm:__myscopes__`

TENANT SIGNING CERTIFICATE SETUP

The public certificate validates the access token during inbound REST API calls. The public certificate is obtained from the OAuth server using OAuth client credentials.

9. Choose one of the following methods to set up the certificate:
   - Click **Choose File** next to Upload Certificate to browse to the certificate file then click Save to save the file.
   - Click the **Retrieve Certificate** checkbox to retrieve the certificate details. The following fields are required by the system to retrieve the certificate, enter the following:
     - **JWKS Endpoint** – the endpoint of the OAuth server to which the client connects to obtain the public key. The JWKS endpoint for Oracle IDCS is: `/admin/v1/SigningCert/jwk`
     - **JWKS Authorized Client ID** – the client ID of any trusted client registered with the OAuth Provider
     - **JWKS Authorized Client Secret** – the client secret of any trusted client registered with the OAuth Provider

CLIENT APP CONFIGURATION

Use this section to configure Oracle CPQ outbound REST API calls.

10. Enter the Client Id of the Oracle CPQ application registered with IDCS in the **Client Id** field. Refer to the Client ID provided in Step 22 in the Register an OpenID Connect Client instructions.

OPENID CONNECT

Use this section to configure OpenID Connect SSO solution between Oracle and custom applications configured in IDCS.

11. Enter the valid IDCS authorization endpoint in the Authorization Endpoint field. Oracle CPQ uses this endpoint to get the authorization grant from IDCS.

    The authorization endpoint for Oracle IDCS is `/oauth2/v1/authorize`

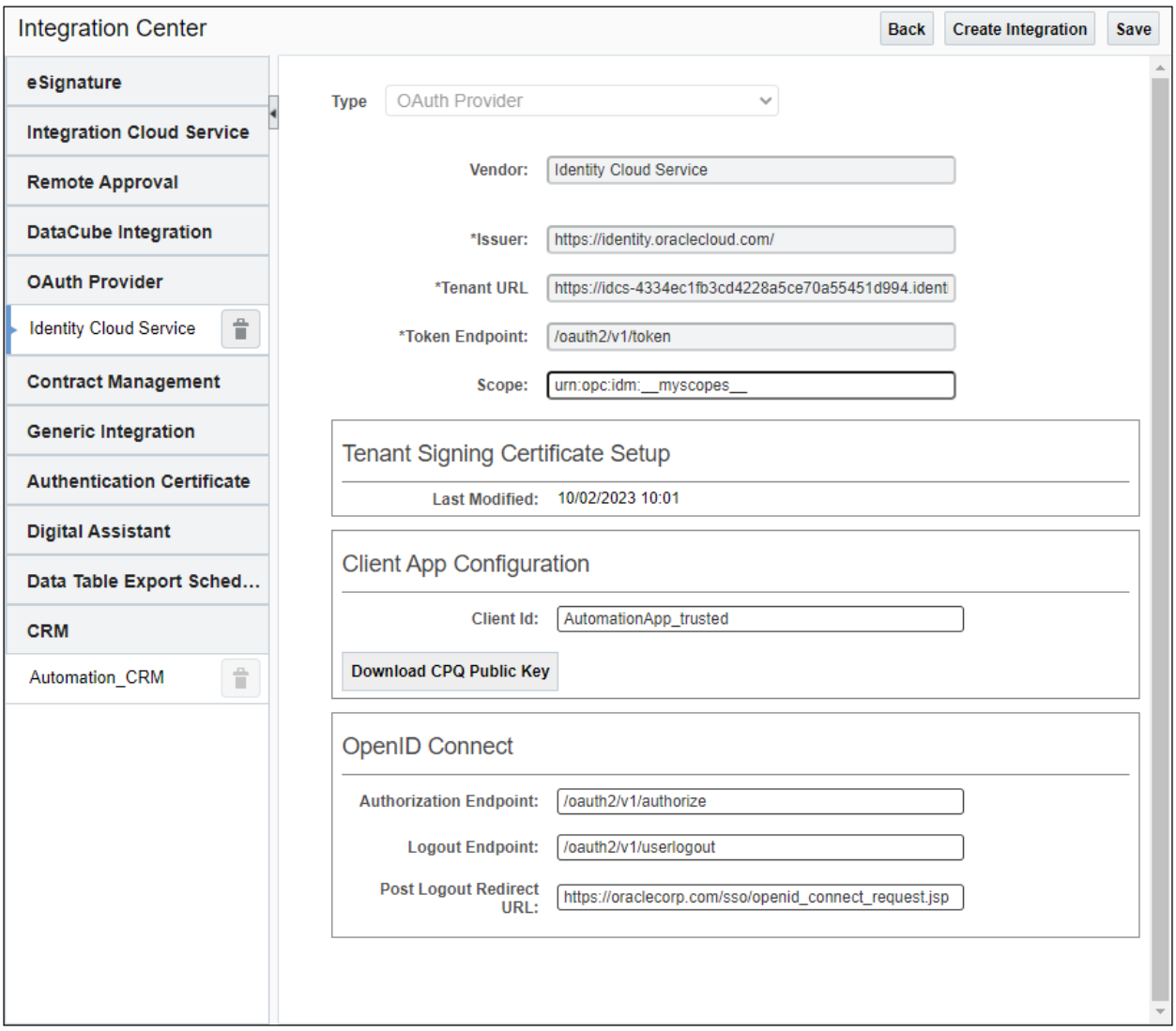
12. Enter the valid URL called by Oracle CPQ during the logout process to terminate the user session in IDCS in the Logout Endpoint field.

    The logout endpoint value is:`/oauth2/v1/userlogout`

13. Enter the URL for the user to be redirected to after logging out of Oracle CPQ in the Post Logout Redirect URL field. Refer to the Step 15 in the Register an OpenID Connect Client in IDCS instructions.

    The post logout redirect URL is: `http://<yourcpqSiteUrl>/sso/openid_connect_request.jsp`

14. Click **Save**.



Enable OpenID Connect for Single Sign-On

Once the OAuth Provider with OpenID Connect Integration is setup, complete the following steps to enable OpenID Connect for Single Sign-On.

1. Click **Single Sign-On** in the Integration Platform section of the Oracle CPQ Home page. The Single Sign-On Settings page displays.
2. Select **OpenID Connect** from the Single Sign-On Method drop-down.

3. Click **Apply**. The OAuth Provider with OpenID Connect Integration is connected with the Single Sign-On settings.
4. (Optional) Log a Service Request (SR) with My Oracle Support to include the site domains in the iframe domain allowlist. This step is only required if you are embedding Oracle CPQ in another application that is not already registered in the allowlist.

Notes:

- If enabling Single Sign-On using OpenID Connect between Oracle CX Sales and Oracle CPQ, refer to Integrating CX Sales with Oracle CPQ for steps to setup the Action URLs for a process.
- After moving a site from SAML to OpenID Connect, all SSO logged in users should close all of their browsers and re-login.

Setup Users

User accounts must be created in both IDCS and Oracle CPQ and then linked between the two applications. This document provides the steps for manually setting up users.

> **Note:**
>
> Manually setting up users is one method of creating and syncing user information between IDCS and Oracle CPQ. Alternatively, you may choose a different method as follows:
>
> - Create an application using the CPQ App Template in IDCS to sync user information IDCS to CPQ. Users are created one by one in IDCS and they are synced to CPQ automatically. You will need to modify the general CPQ App Template to set up OpenID Connect using this method.
> - Perform Bulk Import of users and user groups from CSV files to IDCS.
>
> Refer to User Administration Overview in the Oracle CPQ Administrative Online Help and/or Administering Oracle Identity Cloud Service in the Oracle Help Center.

1. To create a user account in IDCS, refer to Create User Accounts in the Administering Oracle Identity Cloud Service Help Center document.
2. To create a user account in Oracle CPQ, refer to *Creating a User* in the Setting Up Users article of Oracle CPQ Administrative Online Help.
3. To link a user between the two applications, refer to *Register a User Login for External OAuth* in the User Integration Page of Oracle CPQ Administrative Online Help.

> **Notes:**
>
> - If enabling Single Sign-On using OpenID Connect between Oracle CX Sales and Oracle CPQ, refer to the Integrating CX Sales with Oracle CPQ > Configuring the Integration URLs for steps to setup the Action URLs for a process.
> - After moving a site from SAML to OpenID Connect, all SSO logged in users should close all of their browsers and re-login.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com  facebook.com/oracle  twitter.com/oracle