



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



Oracle CPQ Updates 23B and Later

March 2023

Copyright © 2023, Oracle and/or its affiliates

TABLE OF CONTENTS

Revision History.....	2
Introduction.....	2
Purpose.....	2
Prerequisites.....	2
Integration.....	3
Register an OpenID Connect Client in IDCS.....	3
Create an OAuth Provider Integration in Oracle CPQ.....	10
Tenant Signing Certificate Setup.....	10
Client App Configuration.....	10
OpenID Connect.....	11
Enable OpenID Connect for Single Sign-On.....	12
Setup Users.....	13

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

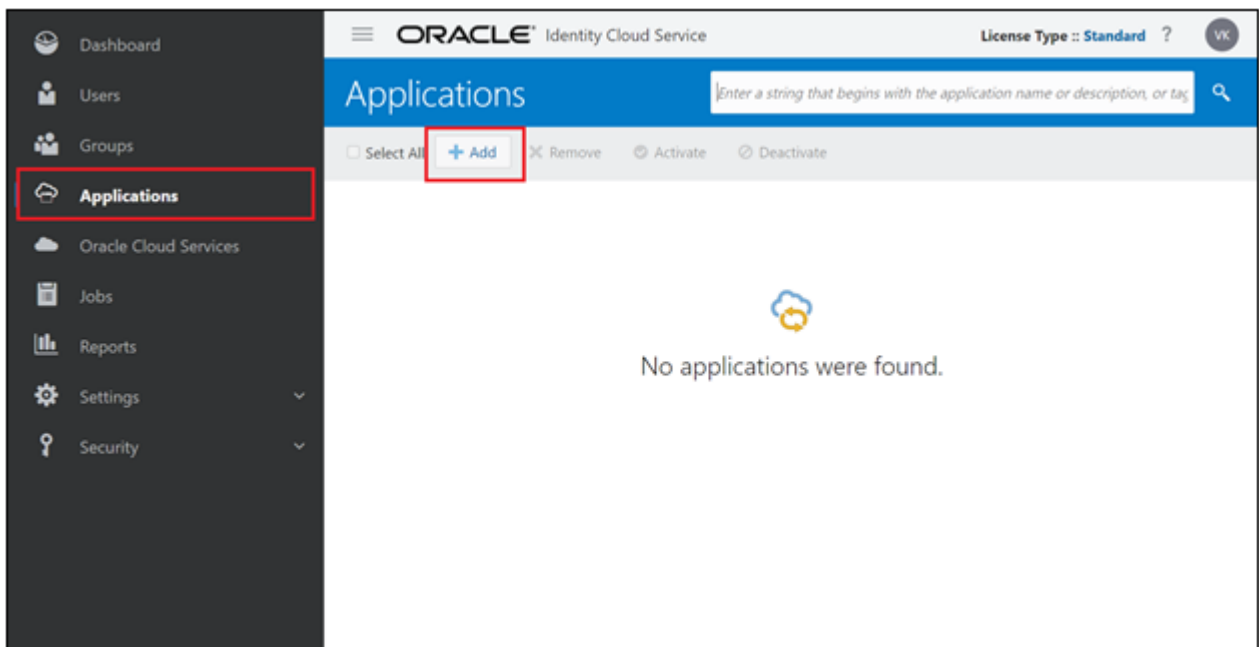
OpenID Connect integration between IDCS and Oracle CPQ requires the following high-level steps:

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](#)

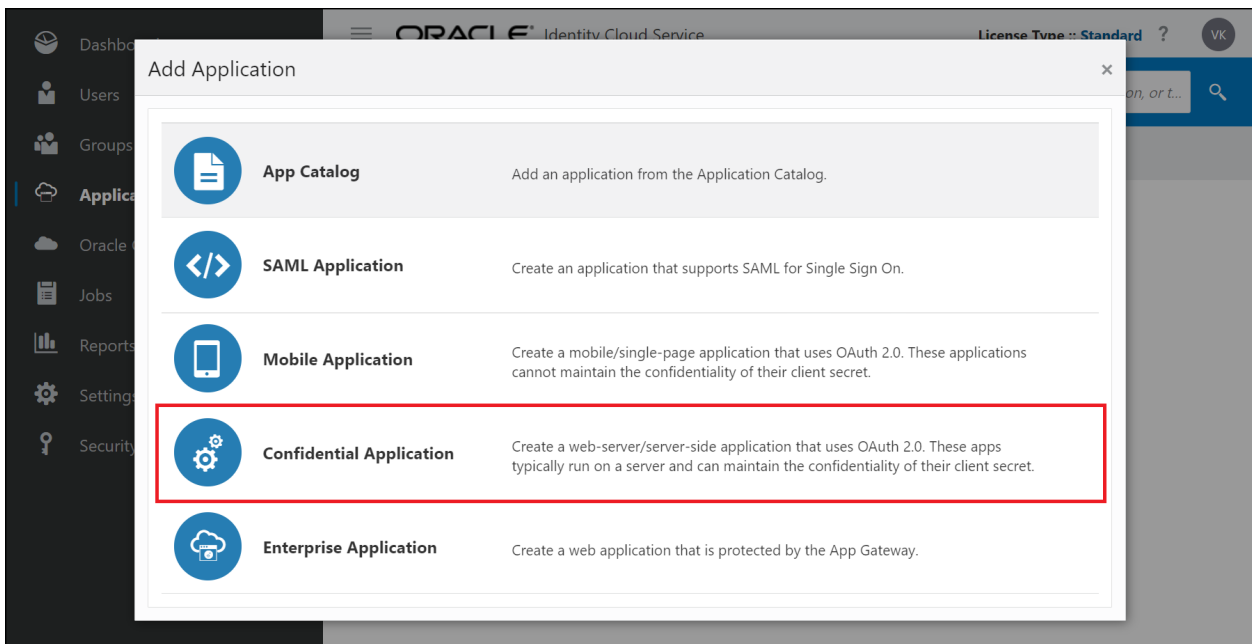
Register an OpenID Connect Client in IDCS

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

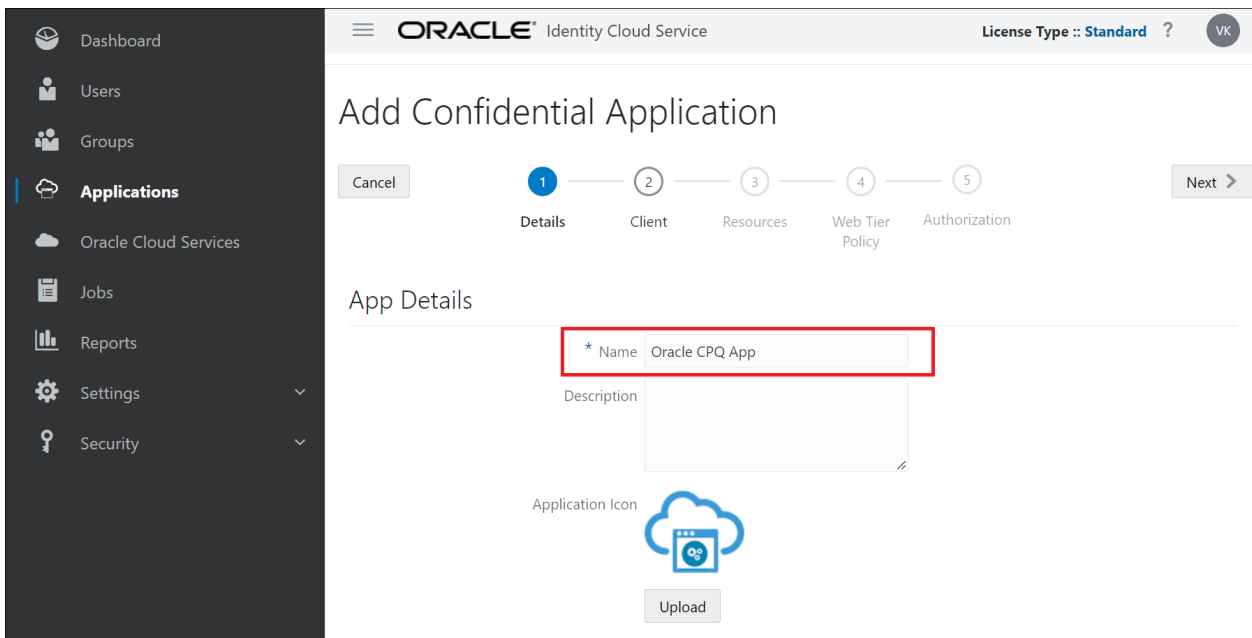
1. Login to IDCS.
2. Click on the **Navigation Drawer** to open the navigation menu.
3. Select **Applications**.
4. Click the **Add** button. The Add Application dialog box displays.



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.

Dashboard
Users
Groups
Applications
Oracle Cloud Services
Jobs
Reports
Settings
Security

ORACLE Identity Cloud Service License Type :: Standard ? VK

Add Confidential Application

< Back Details Client Resources Web Tier Policy Authorization Next >

Configure this application as a client now Skip for later

Authorization

Allowed Grant Types Resource Owner Client Credentials JWT Assertion SAML2 Assertion Refresh Token
 Authorization Code Implicit Device Code
 TLS Client Authentication

Allow non-HTTPS URLs

Redirect URL

Logout URL

Post Logout Redirect URL

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.

Dashboard
Users
Groups
Applications
Oracle Cloud Services
Jobs
Reports
Settings
Security

ORACLE Identity Cloud Service License Type :: Standard ? VK

Add Confidential Application

< Back Details Client Resources Web Tier Policy Authorization Next >

Configure this application as a client now Skip for later

Authorization

Allowed Grant Types Resource Owner Client Credentials JWT Assertion SAML2 Assertion Refresh Token
 Authorization Code Implicit Device Code
 TLS Client Authentication

Allow non-HTTPS URLs

* Redirect URL

Logout URL

Post Logout Redirect URL

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`

Add Confidential Application

← Back Details **Client** Resources Web Tier Policy Authorization Next >

Configure this application as a client now Skip for later

Authorization

Allowed Grant Types Resource Owner Client Credentials JWT Assertion SAML2 Assertion Refresh Token

Authorization Code Implicit Device Code

TLS Client Authentication

Allow non-HTTPS URLs

* Redirect URL

Logout URL

Post Logout Redirect URL

Security Trusted Client Certificate

Allowed Operations Introspect On behalf Of

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.

Add Confidential Application

Details **Client** Resources Web Tier Policy Authorization

Configure this application as a client now Skip for later

Authorization

Allowed Grant Types Resource Owner Client Credentials JWT Assertion SAML2 Assertion Refresh Token

Authorization Code Implicit Device Code

TLS Client Authentication

Allow non-HTTPS URLs

* Redirect URL

Logout URL

Post Logout Redirect URL

Security Trusted Client * Certificate

Allowed Operations Introspect On behalf Of

ID Token Encryption Algorithm

Bypass Consent

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

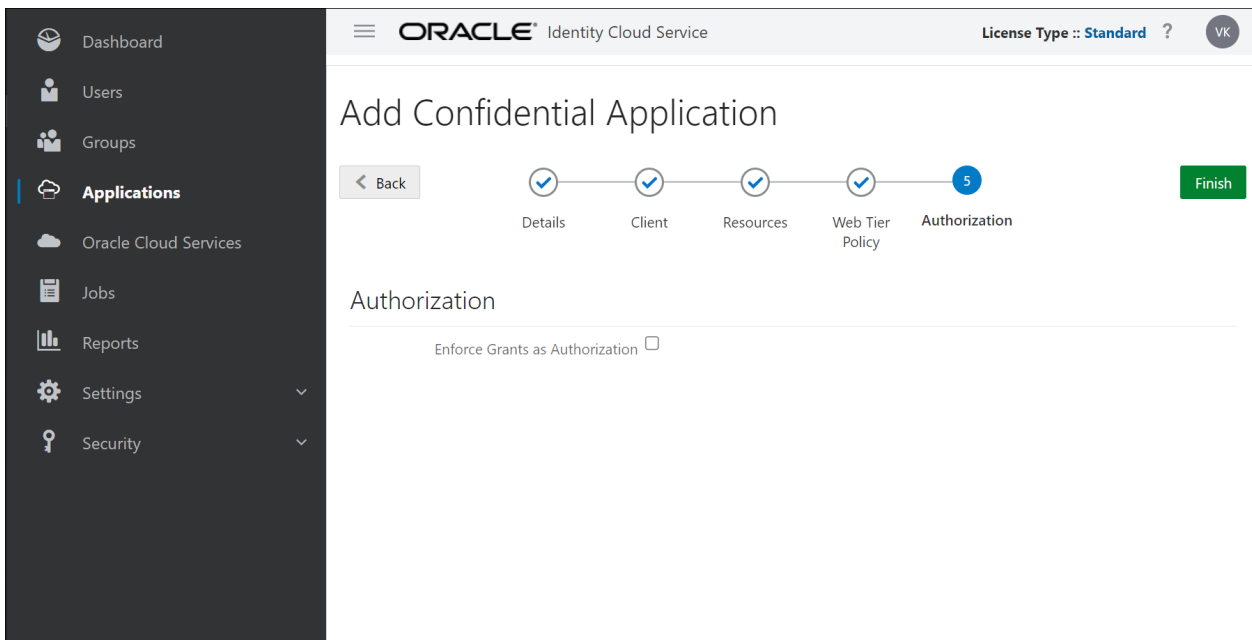
19. Select **Skip for later** for Expose APIs to Other Applications.

The screenshot shows the Oracle Identity Cloud Service interface. The left sidebar contains navigation options: Dashboard, Users, Groups, Applications (highlighted), Oracle Cloud Services, Jobs, Reports, Settings, and Security. The main content area is titled 'Add Confidential Application' and shows a progress bar with five steps: Details, Client, Resources (current step, highlighted with a blue circle and the number 3), Web Tier Policy, and Authorization. Below the progress bar, the section is titled 'Expose APIs to Other Applications' with the instruction 'Specify the APIs that need to be protected.' There are two radio button options: 'Configure this application as a resource server now' and 'Skip for later' (which is selected and highlighted with a red box). Below the options, it states 'No Resources are protected by OAuth'. A 'Back' button is on the left and a 'Next' button is on the right.

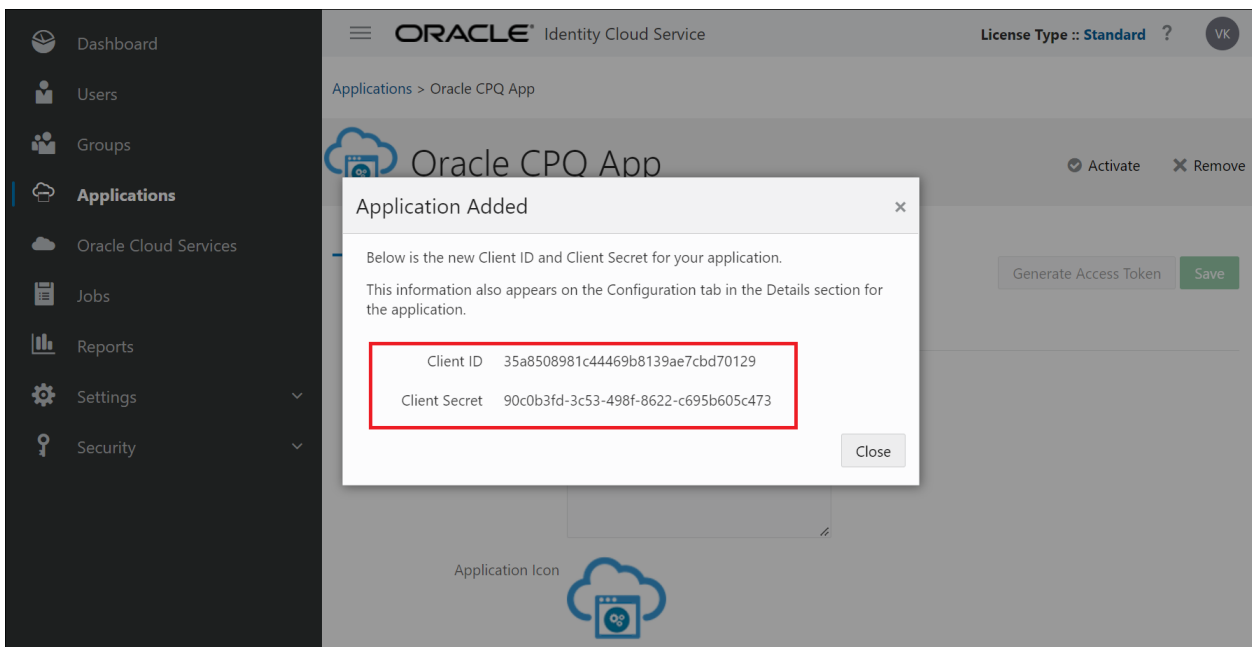
20. Select **Skip for later** for Web Tier Policy.

The screenshot shows the Oracle Identity Cloud Service interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Add Confidential Application' and shows a progress bar with five steps: Details, Client, Resources, Web Tier Policy (current step, highlighted with a blue circle and the number 4), and Authorization. Below the progress bar, the section is titled 'Web Tier Policy' with the instruction 'Use this page to configure, edit, and validate a web tier policy. Additionally, you can import and export existing policies.' There are two radio button options: 'Configure Web Tier Policy for this application' and 'Skip for later' (which is selected and highlighted with a red box). A 'Back' button is on the left and a 'Next' button is on the right.

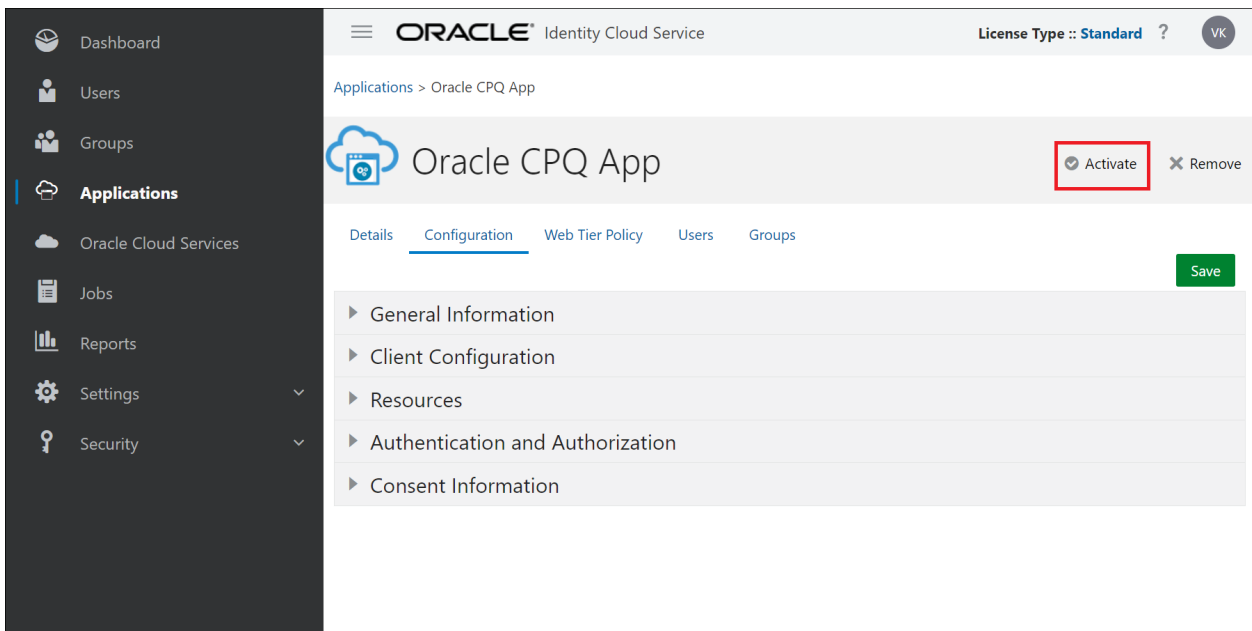
21. Click **Finish** for Authorization. The confidential application is created.



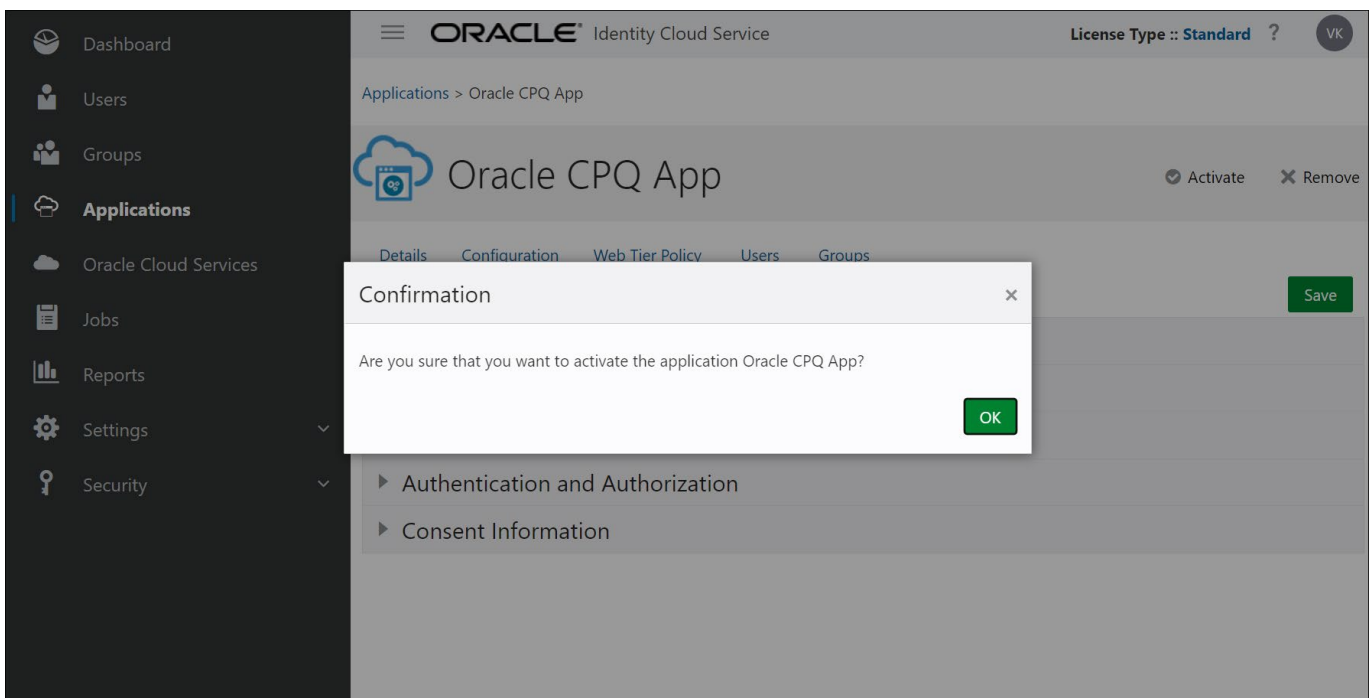
22. The Application Added dialog displays with the Client ID and Client Secret details. Note the **Client ID & Client Secret** as these are required to setup OAuth Provider in Oracle CPQ. Click **Close**.



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**.

The screenshot shows the 'Integration Center' interface. On the left is a navigation pane with categories like eSignature, Integration Cloud Service, Remote Approval, DataCube Integration, OAuth Provider, Identity Cloud Service, Contract Management, Generic Integration, Authentication Certificate, Digital Assistant, Data Table Export Sched..., CRM, and Automation_CRM. The main area is titled 'Type: OAuth Provider' and contains several configuration sections:

- Vendor:** Identity Cloud Service
- *Issuer:** https://identity.oraclecloud.com/
- *Tenant URL:** https://idcs-4334ec1fb3cd4228a5ce70a55451d994.ident
- *Token Endpoint:** /oauth2/v1/token
- Scope:** urn:opc.idm:__myscopes__

Below these fields are three sections:

- Tenant Signing Certificate Setup:** Last Modified: 10/02/2023 10:01
- Client App Configuration:** Client Id: AutomationApp_trusted. A button labeled 'Download CPQ Public Key' is present.
- OpenID Connect:** Authorization Endpoint: /oauth2/v1/authorize; Logout Endpoint: /oauth2/v1/userlogout; Post Logout Redirect URL: https://oraclecorp.com/sso/openid_connect_request.jsp

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.

Single Sign-On Settings

Single Sign-On Method: OpenID Connect ▼

OpenID Connect

Please ensure OAuth Provider is setup correctly in the [Integration Center](#).

[Back to Top](#)

Apply **Update** **Back**

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 CPO > 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

Copyright © 2023, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

