

Oracle® Cloud

Using the Oracle CPQ Adapter with Oracle Integration 3



F45574-11
December 2025



Oracle Cloud Using the Oracle CPQ Adapter with Oracle Integration 3,

F45574-11

Copyright © 2022, 2025, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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.

Contents

About This Content

1 Understand the Oracle CPQ Adapter

Oracle CPQ Adapter Capabilities	1
What Application Version Is Supported?	2
About Oracle CPQ Adapter Use Cases	2
Workflow to Create and Add an Oracle CPQ Adapter Connection to an Integration	2

2 Create an Oracle CPQ Adapter Connection

Prerequisites for Creating a Connection	1
Create a Connection	8
Configure Connection Properties	9
Configure Connection Security	10
Configure the Endpoint Access Type	12
Test the Connection	12
Upload a Certificate to Connect with External Services	13

3 Add the Oracle CPQ Adapter Connection to an Integration

Basic Info Page	1
Trigger Request Page	1
Trigger Response Page	2
Invoke Operation Page	2
Summary Page	4

4 Troubleshoot the Oracle CPQ Adapter

Configuration Error When Using the Oracle CPQ Adapter as a Trigger Connection with a REST Catalog URL	1
Updating the WSDL Definitions of Data Tables	1

About This Content

This guide describes how to configure this adapter as a connection in an integration in Oracle Integration.

Audience

This guide is intended for developers who want to use this adapter in integrations in Oracle Integration.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Resources

See these Oracle resources:

- Oracle Cloud at <http://cloud.oracle.com>
- *Using Integrations in Oracle Integration 3*
- *Using the Oracle Mapper with Oracle Integration 3*
- Oracle Integration documentation on the Oracle Help Center.

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Understand the Oracle CPQ Adapter

Review the following conceptual topics to learn about the Oracle CPQ Adapter and how to use it as a connection in integrations in Oracle Integration. A typical workflow of adapter and integration tasks is also provided.

Topics:

- [Oracle CPQ Adapter Capabilities](#)
- [What Application Version Is Supported?](#)
- [About Oracle CPQ Adapter Use Cases](#)
- [Workflow to Create and Add an Oracle CPQ Adapter Connection to an Integration](#)

Note

There are overall service limits for Oracle Integration. A service limit is the quota or allowance set on a resource. See [Service Limits](#).

Oracle CPQ Adapter Capabilities

The Oracle Configure, Price, and Quote (CPQ) Cloud Adapter enables you to create an integration with an Oracle CPQ application.

The Oracle CPQ Adapter enables you to convert sales opportunities into revenue by automating the quoting and sales order process with guided selling, dynamic pricing, and a workflow approval process.

Oracle CPQ extends sales automation to include the creation of an optimal quote, which enables sales personnel to configure and price complex products; select the best options, promotions, and deal terms; and include upsell and renewals, all using automated workflows.

The main use case for Oracle CPQ is as the trigger (source) in an integration in which Oracle CX Sales and B2B Service (formerly Oracle Engagement Cloud) is the invoke (target). This adapter replicates the point-to-point integration that exists today between Oracle CPQ and Oracle CX Sales and B2B Service. Oracle CPQ is the trigger (source) of the record application. A synchronize process is triggered as you update and save data in Oracle CPQ, but it can also be configured by the administrator of the application. The Oracle CPQ Adapter can also be configured as the invoke (target) in an integration.

The Integration Store provides prebuilt integration flows with Oracle CPQ and Oracle CX Sales and B2B Service for quote creation, opportunity import, and quote update.

The Oracle CPQ Adapter supports connecting to private resources that are in your virtual cloud network (VCN) with a private endpoint. This support is for REST-based APIs only. See [Connect to Private Resources in Provisioning and Administering Oracle Integration 3](#) and [Configure the Endpoint Access Type](#). This type of connection does not use the connectivity agent.

The Oracle CPQ Adapter is one of many predefined adapters included with Oracle Integration. See the [Adapters](#) page in the Oracle Help Center.

What Application Version Is Supported?

For information about which application version is supported by this adapter, see the [Connectivity Certification Matrix](#).

About Oracle CPQ Adapter Use Cases

The Oracle CPQ Adapter can be used as the invocation trigger (source) for quotes and the Oracle SOAP APIs can be used as the invoke (target). Another use case is an Oracle CX Sales and B2B Service (formerly Oracle Engagement Cloud) integration that uses quote data to interact with an opportunity business object and its revenue items.

Workflow to Create and Add an Oracle CPQ Adapter Connection to an Integration

You follow a very simple workflow to create a connection with an adapter and include the connection in an integration in Oracle Integration.

Step	Description	More Information
1	Decide where to work	<ul style="list-style-type: none"> Work in a project (see why working with projects is preferred in <i>Using Integrations in Oracle Integration 3</i>). Work outside a project.
2	Create the adapter connections for the applications you want to integrate. The connections can be reused in multiple integrations and are typically created by the administrator.	Create an Oracle CPQ Adapter Connection
3	Create the integration. When you do this, you add trigger and invoke connections to the integration.	Create Integrations and Add the Oracle CPQ Adapter Connection to an Integration
4	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in <i>Using Integrations in Oracle Integration 3</i>
5	(Optional) Create lookups that map the different values used by those applications to identify the same type of object (such as gender codes or country codes).	Manage Lookups in <i>Using Integrations in Oracle Integration 3</i>
6	Activate the integration.	Manage Integrations in <i>Using Integrations in Oracle Integration 3</i>
7	Monitor the integration on the dashboard.	Monitor Integrations During Runtime in <i>Using Integrations in Oracle Integration 3</i>
8	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Track Integration Instances in <i>Using Integrations in Oracle Integration 3</i>
9	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in <i>Using Integrations in Oracle Integration 3</i>

2

Create an Oracle CPQ Adapter Connection

A connection is based on an adapter. You define connections to the specific cloud applications that you want to integrate.

Topics:

- [Prerequisites for Creating a Connection](#)
- [Create a Connection](#)
- [Upload a Certificate to Connect with External Services](#)

Prerequisites for Creating a Connection

You must satisfy the following prerequisites to create a connection with the Oracle CPQ Adapter.

- [Register with the Oracle CPQ Site](#)
- [Obtain the SOAP WSDL from the Oracle CPQ Site](#)
- [Obtain the REST Catalog URL](#)
- [OAuth using JWT User Assertion Security Policy Prerequisites](#)

Register with the Oracle CPQ Site

After registration, you then receive an email with information that you use to create a connection on the Connections page. See [Configure Connection Properties](#) and [Configure Connection Security](#).

Obtain the SOAP WSDL from the Oracle CPQ Site

- Note the following details:
 - The WSDL must be generated by the Oracle CPQ site to integrate with Oracle Integration.
 - Web Services 2.0 must be used to generate the URL needed to generate the WSDL.
 - The Commerce SOAP server URL endpoint must be used to generate the URL needed to generate the WSDL.
 - The commerce process to integrate with Oracle Integration must be used to generate the URL needed to generate the WSDL.

Oracle Integration uses the Oracle CPQ transaction WSDL to understand the valid data and operations provided by Oracle CPQ.

To access the Oracle CPQ transaction WSDL:

1. Log in to the Oracle CPQ site that you want integrate with Oracle Integration.
2. To open the Admin home page, click **Admin**.
The Admin home page appears.
3. Under **Integration Platform**, click **Web Services**.

4. For the **Web Service Version**, select **2.0**.
5. Ensure that the **Commerce** tab is the current tab.
6. From the **Process Name** list, select the name of the commerce process to integrate with Oracle Integration.
7. In the **SOAP Server URL** field, append `?WSDL` to the end of the value.

For example: `https://site_URL/v2_0/receiver/commerce/processVarName?WSDL`.

where:

- `site_URL` is the base URL of the Oracle CPQ site.
- `processVarName` is the variable name of the selected commerce process.
- Optional: To confirm that the URL is correct, open it in a web browser. A page of WSDL should appear.

Use the URL you created as needed in Oracle Integration to reference the Oracle CPQ transaction WSDL.

Obtain the REST Catalog URL

You specify a REST catalog URL to access an Oracle CPQ application's business resources for outbound connections. The REST catalog URL is formatted as follows:

```
http(s)://site_URL/rest/v3/metadata-catalog
```

where `site_URL` is the base URL of the Oracle CPQ site.

Note that:

- Use the latest REST catalog version available at your Oracle CPQ site for the invoke connection.
- You must be on Oracle CPQ release 2016R2 or above to use the REST catalog in the Oracle CPQ Adapter.

OAuth using JWT User Assertion Security Policy Prerequisites

This section describes the steps to make inbound REST API calls to Oracle CPQ with Oracle Cloud Infrastructure Identity and Access Management-provided OAuth tokens.

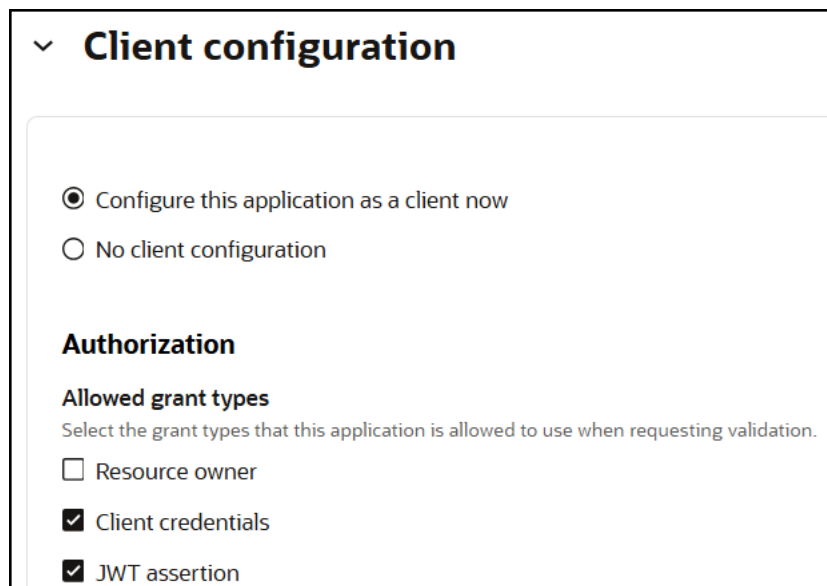
- [Register Oracle CPQ as a Resource in Oracle Cloud Infrastructure Identity and Access Management](#)
- [Register External Application Client in Oracle Cloud Infrastructure Identity and Access Management](#)
- [Set Up the User In Oracle Cloud Infrastructure Identity and Access Management](#)
- [Create an OAuth Provider Integration In Oracle CPQ](#)
- [Link Oracle CPQ and the Oracle Cloud Infrastructure Identity and Access Management User](#)
- [Prepare User and Client Assertions](#)
- [Obtain the OAuth Token From Oracle Cloud Infrastructure Identity and Access Management](#)

Register Oracle CPQ as a Resource in Oracle Cloud Infrastructure Identity and Access Management

1. In the navigation pane, click **Identity & Security**.
2. Click **Domains**.
3. Select your compartment.
4. Select the identity domain.
5. In the menu bar, click **Integrated applications**.
This is the location at which you create the client application for your grant type.



6. Click **Add application**.
7. Select **Confidential Application**, then click **Launch workflow**.
8. Enter a name.
9. Click **Submit**.
10. Click the **OAuth configuration** tab, then the **Edit OAuth configuration** subtab.
11. In the **Resource server configuration** panel, select **Configure this application as a resource server now**.
12. In the **Primary audience** field, enter the Oracle CPQ site URL.
13. Click the **Add scopes** toggle, then click **Add**.
14. In the **Scope** field, enter `/api`.
15. Optionally enter a display name and description, then click **Add**.
16. In the **Client configuration** section, select **Configure this application as a client now**.
17. In the **Authorization** section, select **Client credentials** and **JWT assertion** for the **Allowed grant types**.



18. In the **Client type** section, select **Trusted**.

19. In the **Certificate** section, click **Import certificate** to import the CPQ client certificate. This certificate can be downloaded from the **OAuth Provider** integration in the **Integration Center**.
20. In the **Alias** field, enter a meaningful name.
21. Drag and drop the certificate file or select to browse for it by clicking in the field. This is the file downloaded in Step [19](#).
22. Click **Import**.
23. At the bottom of the wizard, click **Submit**. The details page for the client application is displayed.
24. Click **Activate**, and then **Activate application** to activate the client application for use. The application is now active.
25. In the menu bar, click the **OAuth configuration** tab.
26. In the **General Information** section, note the client ID and client secret values. These values are required when creating the OAuth Provider integration CPQ in the **JWKS Authorized Client ID** and **JWKS Authorized Client Secret** fields, respectively.

General Information

Client ID bba

Client secret

Show secret ⋮

Register External Application Client in Oracle Cloud Infrastructure Identity and Access Management

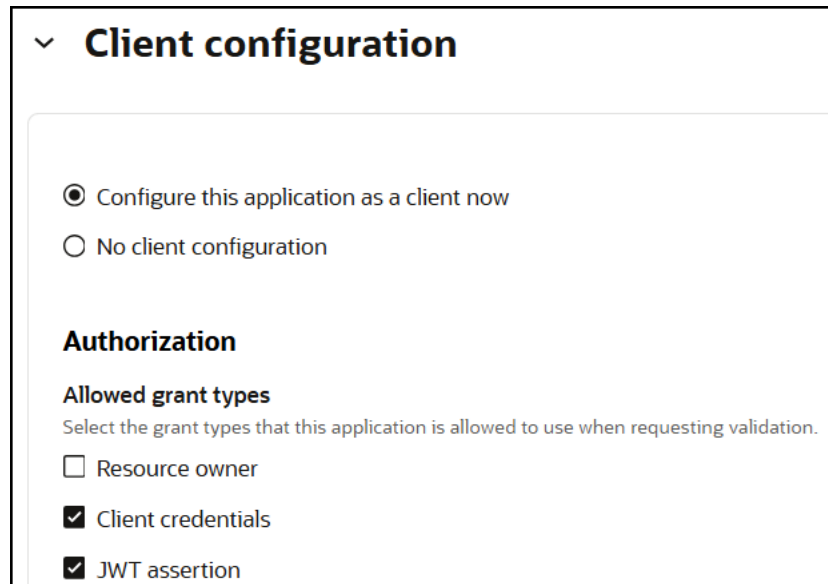
1. In the navigation pane, click **Identity & Security**.
2. Click **Domains**.
3. Select your compartment.
4. Select the identity domain.
5. In the menu bar, click **Integrated applications**. This is the location at which you create the client application for your grant type.

Details User management Administrators Dynamic groups Directory integrations **Integrated applications** Oracle cloud services Federation Domain policies

Integrated applications

6. Click **Add application**.
7. Select **Confidential Application**, then click **Launch workflow**.
8. Enter a name.
9. Click **Submit**.

10. Click the **OAuth configuration** tab, then the **Edit OAuth configuration** subtab.
11. In the **Client configuration** panel, select **Configure this application as a client now**.
12. In the **Authorization** section, select **Client credentials** and **JWT assertions** in the **Allowed grant types** section.



Client configuration

Configure this application as a client now

No client configuration

Authorization

Allowed grant types

Select the grant types that this application is allowed to use when requesting validation.

Resource owner

Client credentials

JWT assertion

13. For **Client type**, ensure that **Trusted** is selected.
14. In the **Certificate** section, click **Import Certificate**. This certificate is *not* available in Oracle CPQ. The external entity that wants to call the Oracle CPQ REST API must provide this certificate.

Note

The private key corresponding to the client certificate is used to obtain the token from Oracle Cloud Infrastructure Identity and Access Management. Keep it ready for use.

15. In the **Alias** field, enter a meaningful name. This name is used later to prepare the assertions.
16. Drag and drop the certificate file or select to browse for it by clicking in the field.
17. Click **Import**.
18. Click the **Add Resources** toggle.
19. Click **Add scope**.
20. Search for and expand the Oracle CPQ resource application that you created in Step 8.
21. Select the scopes, then click **Add**.
22. At the bottom of the wizard, click **Submit**. The details page for the client application is displayed.
23. Click **Activate**, and then **Activate application** to activate the client application for use. The application is now active.
24. In the menu bar, click the **OAuth configuration** tab.

25. In the **General Information** section, note the client ID value.

Set Up the User In Oracle Cloud Infrastructure Identity and Access Management

1. Create users in Oracle Cloud Infrastructure Identity and Access Management. See [Managing Users](#).

Create an OAuth Provider Integration In Oracle CPQ

1. Set up the integration between Oracle Cloud Infrastructure Identity and Access Management and Oracle CPQ. See [OAuth Provider Integration](#).

Link Oracle CPQ and the Oracle Cloud Infrastructure Identity and Access Management User

1. Link Oracle CPQ and the Oracle Cloud Infrastructure Identity and Access Management user. See [Register a User Login for External OAuth](#) in the Administration section.

Prepare User and Client Assertions

1. Prepare user and client assertions to get the token from Oracle Cloud Infrastructure Identity and Access Management. User and client assertions are JWT assertions that contains header and claims. See [Client/User JWT Assertion](#). To learn more about JWT, see [Introduction to JSON Web Tokens](#).

Some of the claims and their corresponding values are listed below. See the above documentation for details about claims not provided here.

Table 2-1 Client/User Assertion Headers

Claim	Value
kid	Alias value obtained from Step 15

Table 2-2 Client Assertion Body/Claims

Claim	Value
sub	Client ID obtained in Step 25
iss	Client ID obtained in Step 25
aud	https://identity.oraclecloud.com/

Table 2-3 User Assertion Body/Claims

Claim	Value
sub	Oracle Cloud Infrastructure Identity and Access Management user name
iss	Client ID obtained in Step 25
aud	https://identity.oraclecloud.com/

Sample User Assertion

```
eyJ4NXQjUzI1NiI6Imh6TWlyWkhEWXBQdFFGTelqLXdiUjBvWlVLQ0l0cjIza0g3VWNKQVpiaZAiLCJ4
NXQiOiJnanI2TnhuV2RST1ZyN0o5MXdDUVZEeXk2Sk0iLCJraWQiOiJrZXk0b2F1dGgiLCJhbGc
iOiJSUzI1NiJ9.
eyJzdWIiOiJqb2huLmRvZUBleGFtcGxlLmNvbSIsImF1ZCI6Imh0dHBzOlwvXC9pZGVudG10eS5
vcmFjbGVjbG91ZC5
```



Create a Connection

Before you can build an integration, you must create the connections to the applications with which you want to share data.

Note

You can also create a connection in the integration canvas. See Define Inbound Triggers, Outbound Invokes, and Actions.

To create a connection in Oracle Integration:

1. Decide where to start:
 - Work in a project (see why working with projects is preferred).
 - a. In the navigation pane, click **Projects**.
 - b. Select the project name.
 - c. Click **Integrations** .
 - d. In the **Connections** section, click **Add** if no connections currently exist or **+** if connections already exist. The Create connection panel opens.
 - Work outside a project.
 - a. In the navigation pane, click **Design**, then **Connections**.
 - b. Click **Create**. The Create connection panel opens.
2. Select the adapter to use for this connection. To find the adapter, scroll through the list, or enter a partial or full name in the **Search** field.
3. Enter the information that describes this connection.

Element	Description
Name	Enter a meaningful name to help others find your connection when they begin to create their own integrations.
Identifier	Automatically displays the name in capital letters that you entered in the Name field. If you modify the identifier name, don't include blank spaces (for example, SALES OPPORTUNITY).

Element	Description
Role	<p>Select the role (direction) in which to use this connection.</p> <p>Note: <i>Only</i> the roles supported by the adapter you selected are displayed for selection. Some adapters support all role combinations (trigger, invoke, or trigger and invoke). Other adapters support fewer role combinations.</p> <p>When you select a role, only the connection properties and security policies appropriate to that role are displayed on the Connections page. If you select an adapter that supports both invoke and trigger, but select only one of those roles, you'll get an error when you try to drag the adapter into the section you didn't select.</p> <p>For example, assume you configure a connection for the Oracle Service Cloud (RightNow) Adapter as only an invoke. Dragging the adapter to a trigger section in the integration produces an error.</p>
Keywords	Enter optional keywords (tags). You can search on the connection keywords on the Connections page.
Description	Enter an optional description of the connection.
Share with other projects	<p>Note: This field only appears if you are creating a connection in a project.</p> <p>Select to make this connection publicly available in other projects. Connection sharing eliminates the need to create and maintain separate connections in different projects.</p> <p>When you configure an adapter connection in a different project, the Use a shared connection field is displayed at the top of the Connections page. If the connection you are configuring matches the same type and role as the publicly available connection, you can select that connection to reference (inherit) its resources.</p> <p>See Add and Share a Connection Across a Project.</p>

4. Click **Create**.

Your connection is created. You're now ready to configure the connection properties, security policies, and (for some connections) access type.

5. Follow the steps to configure a connection.

The connection property and connection security values are specific to each adapter. Your connection may also require configuration with an access type such as a private endpoint or an agent group.

6. Test the connection.

Configure Connection Properties

Enter connection information so your application can process requests.

1. Go to the **Properties** section.

- In the **Connection Type** field, select the URL type to use in this integration. This field is available for connections with the invoke role or trigger and invoke role.

Note

If you want to use the Oracle CPQ Adapter as a trigger connection in an integration, you must specify a SOAP WSDL URL. If you specify a REST catalog URL, you receive an error when adding the connection as a trigger in an integration.

- SOAP WSDL URL**
 - REST Catalog URL**
- In the **Connection URL** field, specify the URL to use in this integration. To obtain the URL, see [Prerequisites for Creating a Connection](#).

Configure Connection Security

Configure security for your Oracle CPQ Adapter connection by selecting the security policy and login credentials.

If you are using Oracle Fusion Applications CPQ, you can only connect with the OAuth using JWT User Assertion security policy. If you are using Big Machines (BM) CPQ, you can connect with either the Username Password Token or OAuth using JWT User Assertion security policy.

- Go to the **Security** section.
- Select the security policy to use from the **Security policy** list:
 - Username Password Token**
 - OAuth using JWT User Assertion**
- If you select **Username Password Token**:
 - Enter your login credentials. The only requirement is that you must have API access in Oracle CPQ. Beyond that it does not matter which user is configured. To obtain the login credentials, see [Prerequisites for Creating a Connection](#).
- If you select **OAuth using JWT User Assertion**:
 - Enter the following details.

Element	Description
Access token URI	Enter the URL to which to send a request to obtain the access token. For example: <code>https://accounts.google.com/o/oauth2/token</code>

Element	Description
JWT headers in JSON format	<p>Upload the JWT header . json file. For example:</p> <pre>{ "kid": "externalClientAppVivek1", "typ": "JWT", "alg": "RS256" }</pre> <p>Where:</p> <ul style="list-style-type: none"> • kid: The alias name of the public certificate you upload when creating the client application in Oracle Cloud Infrastructure Identity and Access Management. • typ: The type of the JWT. • alg: The algorithm to use. <p>See OAuth using JWT User Assertion Security Policy Prerequisites.</p>
JWT payload in JSON format	<p>Upload the JWT payload . json file. For example:</p> <pre>{ "sub": "joe.smith@mycompany.com", "aud": "https://identity.oraclecloud.com/", "iss": "1234adafghvdscscsdf", "exp": 1740475177, "iat": 1739870304 }</pre> <p>Where:</p> <ul style="list-style-type: none"> • sub: The user name with access to the Oracle CPQ API. • aud: The identity domain audience <code>https://identity.oracle.com/</code>. The signing algorithm must be RS256. • iss : The client ID of the client application created in Oracle Cloud Infrastructure Identity and Access Management. • exp: The expiry time. • iat: The issue time of the token. <p>See OAuth using JWT User Assertion Security Policy Prerequisites.</p>
JWT private key alias	<p>Enter the JWT private key alias. This is the same alias you specified when uploading the signing key certificate on the Certificates page. See Upload a Certificate to Connect with External Services.</p>
Scope	<p>(Optional) Enter the scope:</p> <p><i>Oracle_CPQ_site_URL/api</i></p>
Access token request	<p>(Optional) Enter the request to obtain the access token. The format you specify can vary by service provider.</p>

Configure the Endpoint Access Type

Configure access to your endpoint. Depending on the capabilities of the adapter you are configuring, options may appear to configure access to the public internet, to a private endpoint, or to an on-premises service hosted behind a fire wall.

- [Select the Endpoint Access Type](#)
- [Ensure Private Endpoint Configuration is Successful](#)

Select the Endpoint Access Type

1. Go to the **Access type** section.
2. Select the option for accessing your endpoint.

Option	This Option Appears If Your Adapter Supports ...
Public gateway	Connections to endpoints using the public internet.
Private endpoint	Connections to endpoints using a private virtual cloud network (VCN). Note: To connect to private endpoints, you must complete prerequisite tasks in the Oracle Cloud Console. Failure to do so results in errors when testing the connection. See <i>Connect to Private Resources in Provisioning and Administering Oracle Integration 3</i> and <i>Troubleshoot Private Endpoints in Using Integrations in Oracle Integration 3</i> . Note: The Oracle CPQ Adapter only supports REST-based connections with private endpoints.

Ensure Private Endpoint Configuration is Successful

- To connect to private endpoints, you must complete prerequisite tasks in the Oracle Cloud Console. Failure to do so results in errors when testing the connection. See *Connect to Private Resources in Provisioning and Administering Oracle Integration 3*.
- When configuring an adapter on the Connections page to connect to endpoints using a private network, specify the fully-qualified domain name (FQDN) and *not* the IP address. If you enter an IP address, validation fails when you click **Test**.

Test the Connection

Test your connection to ensure that it's configured successfully.

1. In the page title bar, click **Test**. What happens next depends on whether your adapter connection uses a Web Services Description Language (WSDL) file. Only some adapter connections use WSDLs.

If Your Connection...	Then...
Doesn't use a WSDL	The test starts automatically and validates the inputs you provided for the connection.


If Your Connection...	Then...
Uses a WSDL	<p>A dialog prompts you to select the type of connection testing to perform:</p> <ul style="list-style-type: none"> • Validate and Test: Performs a full validation of the WSDL, including processing of the imported schemas and WSDLs. Complete validation can take several minutes depending on the number of imported schemas and WSDLs. No requests are sent to the operations exposed in the WSDL. • Test: Connects to the WSDL URL and performs a syntax check on the WSDL. No requests are sent to the operations exposed in the WSDL.

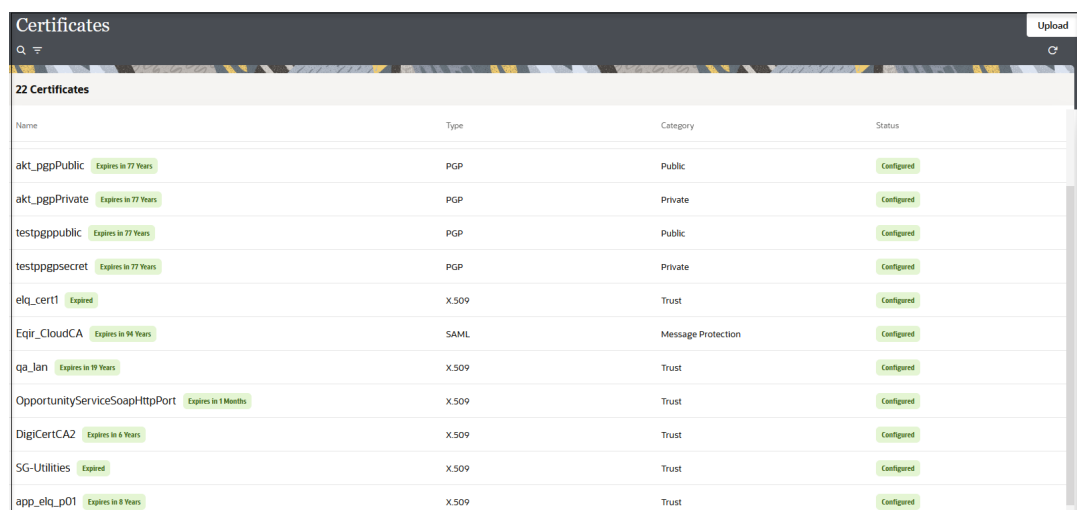
2. Wait for a message about the results of the connection test.
 - If the test was successful, then the connection is configured properly.
 - If the test failed, then edit the configuration details you entered. Check for typos and verify URLs and credentials. Continue to test until the connection is successful.
3. When complete, click **Save**.

Upload a Certificate to Connect with External Services

Certificates allow Oracle Integration to connect with external services. If the external service/endpoint needs a specific certificate, request the certificate and then import it into Oracle Integration.

If you make an SSL connection in which the root certificate does not exist in Oracle Integration, an exception error is thrown. In that case, you must upload the appropriate certificate. A certificate enables Oracle Integration to connect with external services. If the external endpoint requires a specific certificate, request the certificate and then upload it into Oracle Integration.

1. Sign in to Oracle Integration.
2. In the navigation pane, click **Settings**, then **Certificates**.
All certificates currently uploaded to the trust store are displayed on the Certificates page.
3. Click **Filter**  to filter by certificate expiration date, status, and type. Certificates installed by the system cannot be deleted.



Name	Type	Category	Status
akt_pgpPublic <small>Expires in 77 Years</small>	PGP	Public	Configured
akt_pgpPrivate <small>Expires in 77 Years</small>	PGP	Private	Configured
testpgppublic <small>Expires in 77 Years</small>	PGP	Public	Configured
testpgppsecret <small>Expires in 77 Years</small>	PGP	Private	Configured
elq_cert1 <small>Expired</small>	X.509	Trust	Configured
Eqir_CloudCA <small>Expires in 94 Years</small>	SAML	Message Protection	Configured
qa_jan <small>Expires in 19 Years</small>	X.509	Trust	Configured
OpportunityServiceSoapHttpPort <small>Expires in 1 Month</small>	X.509	Trust	Configured
DigiCertCA2 <small>Expires in 6 Years</small>	X.509	Trust	Configured
SG-Utilities <small>Expired</small>	X.509	Trust	Configured
app_elq_p01 <small>Expires in 8 Years</small>	X.509	Trust	Configured

4. Click **Upload** at the top of the page.
The Upload certificate panel is displayed.

5. Enter an alias name and optional description.
6. In the **Type** field, select the certificate type. Each certificate type enables Oracle Integration to connect with external services.
 - [Digital Signature](#)
 - [X.509 \(SSL transport\)](#)
 - [SAML \(Authentication & Authorization\)](#)
 - [PGP \(Encryption & Decryption\)](#)
 - [Signing key](#)

Digital Signature

The digital signature security type is typically used with adapters created with the Rapid Adapter Builder. See Learn About the Rapid Adapter Builder in Oracle Integration in *Using the Rapid Adapter Builder with Oracle Integration 3*.

1. Click **Browse** to select the digital certificate. The certificate must be an X509Certificate. This certificate provides inbound RSA signature validation. See RSA Signature Validation in *Using the Rapid Adapter Builder with Oracle Integration 3*.
2. Click **Upload**.

X.509 (SSL transport)

1. Select a certificate category.
 - a. **Trust**: Use this option to upload a trust certificate.
 - i. Click **Browse**, then select the trust file (for example, .cer or .crt) to upload.
 - b. **Identity**: Use this option to upload a certificate for two-way SSL communication.
 - i. Click **Browse**, then select the keystore file (.jks) to upload.
 - ii. Enter the comma-separated list of passwords corresponding to key aliases.

Note

When an identity certificate file (.jks) contains more than one private key, all the private keys must have the same password. If the private keys are protected with different passwords, the private keys cannot be extracted from the keystore.

- iii. Enter the password of the keystore being imported.
 - c. Click **Upload**.

SAML (Authentication & Authorization)

1. Note that **Message Protection** is automatically selected as the only available certificate category and cannot be deselected. Use this option to upload a keystore certificate with SAML token support. Create, read, update, and delete (CRUD) operations are supported with this type of certificate.
2. Click **Browse**, then select the certificate file (.cer or .crt) to upload.
3. Click **Upload**.

PGP (Encryption & Decryption)

1. Select a certificate category. Pretty Good Privacy (PGP) provides cryptographic privacy and authentication for communication. PGP is used for signing, encrypting, and decrypting files. You can select the private key to use for encryption or decryption when configuring the stage file action.
 - a. **Private:** Uses a private key of the target location to decrypt the file.
 - i. Click **Browse**, then select the PGP file to upload.
 - ii. Enter the PGP private key password.
 - b. **Public:** Uses a public key of the target location to encrypt the file.
 - i. Click **Browse**, then select the PGP file to upload.
 - ii. In the **ASCII-Armor Encryption Format** field, select **Yes** or **No**.
 - **Yes** shows the format of the encrypted message in ASCII armor. ASCII armor is a binary-to-textual encoding converter. ASCII armor formats encrypted messaging in ASCII. This enables messages to be sent in a standard messaging format. This selection impacts the visibility of message content.
 - **No** causes the message to be sent in binary format.
 - iii. From the **Cipher Algorithm** list, select the algorithm to use. Symmetric-key algorithms for cryptography use the same cryptographic keys for both encryption of plain text and decryption of cipher text. The following supported cipher algorithms are FIPS-compliant:
 - AES128
 - AES192
 - AES256
 - TDES
 - c. Click **Upload**.

Signing key

A signing key is a secret key used to establish trust between applications. Signing keys are used to sign ID tokens, access tokens, SAML assertions, and more. Using a private signing key, the token is digitally signed and the server verifies the authenticity of the token by using a public signing key. You must upload a signing key to use the OAuth Client Credentials using JWT Client Assertion and OAuth using JWT User Assertion security policies in REST Adapter invoke connections. Only PKCS1- and PKCS8-formatted files are supported.

1. Select **Public** or **Private**.
2. Click **Browse** to upload a key file.

If you selected **Private**, and the private key is encrypted, a field for entering the private signing key password is displayed after key upload is complete.
3. Enter the private signing key password. If the private signing key is not encrypted, you are not required to enter a password.
4. Click **Upload**.

3

Add the Oracle CPQ Adapter Connection to an Integration

When you drag the Oracle CPQ Adapter into the trigger or invoke area of an integration, the Adapter Endpoint Configuration Wizard appears. This wizard guides you through the configuration of the Oracle CPQ Adapter endpoint properties.

These topics describe the wizard pages that guide you through configuration of the Oracle CPQ Adapter as a trigger or invoke in an integration.

Topics:

- [Basic Info Page](#)
- [Trigger Request Page](#)
- [Trigger Response Page](#)
- [Invoke Operation Page](#)
- [Summary Page](#)

Basic Info Page

You can enter a name and description on the Basic Info page of each adapter in your integration.

Element	Description
What do you want to call your endpoint?	Provide a meaningful name so that others can understand the responsibilities of this connection. You can include English alphabetic characters, numbers, underscores, and hyphens in the name. You can't include the following characters: <ul style="list-style-type: none">• No blank spaces (for example, My Inbound Connection)• No special characters (for example, #;83& or righ(t)now4) except underscores and hyphens• No multibyte characters
What does this endpoint do?	Enter an optional description of the connection's responsibilities. For example: This connection receives an inbound request to synchronize account information with the cloud application.

Trigger Request Page

View the Oracle CPQ trigger request values for your integration.

You can view the Transaction business object to receive from the Oracle CPQ application as a request document to start the integration flow.

Element	Description
Business Object	View the Transaction business object. This object is from a CPQ Commerce process. This is the business object that you receive from the Oracle CPQ application as a request document to start this integration flow. This business object is automatically selected based on the content of the WSDL file you specified when creating the Oracle CPQ connection.

Trigger Response Page

View the Oracle CPQ trigger response values for your integration.

Element	Description
Send a Response	Indicates that a response business object is sent from the integration flow to the Oracle CPQ application. This option is automatically configured and cannot be changed.
Response Type	Indicates that the business object is sent back synchronously to the source application. This option is automatically configured and cannot be changed.
Business Object	Displays the Transaction business object. This object is from a CPQ Commerce process. This business object is automatically selected based on the content of the WSDL file you specified when creating the Oracle CPQ connection.

Invoke Operation Page

View and configure the Oracle CPQ invoke operation values for your integration.

Element	Description
CPQ API Version 2	Displays Commerce.

Element	Description
Select an Operation	<p>Select an operation. These operations come from the WSDL you specified when creating the connection.</p> <ul style="list-style-type: none"> • Add a Transaction: Adds a new item to an existing transaction performing the Add from Catalog action. The input parameters include the process, the document, the action on the document, and the items to be added. • Create Transaction: Supports the creation of a commerce Transaction without line items and transactions with nonconfigurable line items from a specified process. For all transactions required to be created with configurable line items, the Configuration SOAP API must be invoked. This action returns the transaction ID. • Export File Attachments: Exports a file attachment using one of two methods to stream the data through SOAP: <ul style="list-style-type: none"> – Inline base64 content in a SOAP message – Binary stream with MIME containers through an MTOM transmission These methods read and write multiple attributes at once per transaction. This API can only be used by full-access users with the Modify Users permission. There are two modes available for use: <ul style="list-style-type: none"> – Content: Retrieves the content of the attached fields. – Metadata: Retrieves the file information or metadata for the referenced fields. • Get Transaction: Returns the complete Transaction XML content for the given Transaction ID. • Import File Attachments: Imports a file attachment using one of two methods to stream the data through SOAP: <ul style="list-style-type: none"> – Inline base64 content in a SOAP message – Binary stream with MIME containers through an MTOM transmission These methods read and write multiple attributes at once per transaction. This API can only be used by full-access users with the Modify Users permission. There are two modes available for use: <ul style="list-style-type: none"> – Update: Attaches a file or set of files to the transaction – Delete: Removes a file from the file attachment attribute • Remove from Transaction: Removes an item from an existing transaction by performing the Remove Line Items action. The input parameters include the document ID, document number, process name, and document name. • Update Transaction: Updates an existing transaction by performing the Modify and Auto-fill actions. The Create Document action is not supported.
Business Objects	Displays the Transaction business object.

Summary Page

You can review the specified adapter configuration values on the Summary page.

Element	Description
Summary	<p>Displays a summary of the configuration values you defined on previous pages of the wizard.</p> <p>The information that is displayed can vary by adapter. For some adapters, the selected business objects and operation name are displayed. For adapters for which a generated XSD file is provided, click the XSD link to view a read-only version of the file.</p> <p>To return to a previous page to update any values, click the appropriate tab in the left panel or click Go back.</p> <p>To cancel your configuration details, click Cancel.</p>

4

Troubleshoot the Oracle CPQ Adapter

The following topic can help you troubleshoot problems you may encounter with the Oracle CPQ Adapter.

Topics:

- [Configuration Error When Using the Oracle CPQ Adapter as a Trigger Connection with a REST Catalog URL](#)
- [Updating the WSDL Definitions of Data Tables](#)

Configuration Error When Using the Oracle CPQ Adapter as a Trigger Connection with a REST Catalog URL

If you create and successfully test an Oracle CPQ Adapter connection, but receive the following error when adding the connection as a trigger in the integration canvas, ensure that you specified a SOAP WSDL URL on the Connections page. When used as a trigger connection, the Oracle CPQ Adapter requires the use of a SOAP WSDL URL and does not work with a REST catalog URL.

Root cause of the Exception : Inbound is not supported

Updating the WSDL Definitions of Data Tables

When Oracle Integration calls Oracle CPQ with the Oracle CPQ Adapter, you can receive the following error:

```
Fault Code : nsl:FailedAuthentication\nFault String :  
The security token could not be authenticated or authorized
```

If you receive this error, update the WSDL definitions of the data tables (for example, after a site refresh).

1. From the Administration Platform page of the Oracle CPQ application, go to the Web Services (Test) page.
2. Click **Generate Schema and WSDL**.
3. Read the line **Data Tables: Generated when table definition is updated**.
4. Open the Oracle CPQ > Data Tables page.
5. Locate the data table in the navigation pane (filter for the data table, if necessary).
6. Right-click the data table.
7. Select **Deploy**.
8. Check the WSDL again.

Additional integration troubleshooting information is provided. See Troubleshoot Oracle Integration in *Using Integrations in Oracle Integration 3*.