

Oracle® Cloud

Using the Oracle HCM Cloud Adapter with Oracle Integration Generation 2



E85426-45
October 2024



Oracle Cloud Using the Oracle HCM Cloud Adapter with Oracle Integration Generation 2,

E85426-45

Copyright © 2017, 2024, 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

Preface

Audience	v
Documentation Accessibility	v
Diversity and Inclusion	v
Related Resources	vi
Conventions	vi

1 Understand the Oracle HCM Cloud Adapter

Oracle HCM Cloud Adapter Capabilities	1-1
Oracle HCM Cloud Adapter Restrictions	1-3
What Application Version Is Supported?	1-4
Oracle HCM Cloud Adapter Use Cases	1-4
Workflow to Create and Add an Oracle HCM Cloud Adapter Connection to an Integration	1-4

2 Create an Oracle HCM Cloud Adapter Connection

Prerequisites for Creating a Connection	2-1
Subscribe to Oracle HCM Cloud	2-1
Assign Required Roles to an Integration User	2-2
Request Access to Atom Feeds and REST APIs Capabilities on Your Oracle HCM Cloud Instances	2-3
Create an HCM-compliant .dat File to Use the HCM Data Loader	2-3
Upload Files to Oracle WebCenter Content	2-3
Perform Prerequisites to Set Up the OAuth Authorization Code Credentials Security Policy	2-3
Set Up the OAuth Authorization Code Credentials Security Policy with the Oracle Fusion Applications Identity Domain	2-4
Set Up the OAuth Authorization Code Credentials Security Policy with a Non-Oracle Fusion Applications Identity Domain	2-7
Set Up the OAuth Authorization Code Credentials Security Policy with Oracle Identity Cloud Service	2-11
Verify the Status of Location-Based Access Control (LBAC)	2-16
Specify the Oracle HCM Cloud Service Catalog Service WSDL or Service Interface URL (For Connections Created Prior to 2/18/20)	2-16

For Fusion Applications Releases 10 Through 12	2-16
For Fusion Applications Releases 13 and Later	2-20
Create a Connection	2-20
Configure Connection Properties	2-21
Configure Connection Security	2-22
Test the Connection	2-24
Upload an SSL Certificate	2-25
Refresh Integration Metadata	2-26

3 Add the Oracle HCM Cloud Adapter Connection to an Integration

Basic Info Page	3-1
Trigger Request Page	3-2
Trigger Response Page	3-2
Invoke Action Page	3-4
Invoke Operation Page	3-5
Invoke Child Resources Page	3-9
Invoke Descriptive and Extensible Page	3-9
Summary Page	3-10

4 Implement Common Patterns Using the Oracle HCM Cloud Adapter

Upload a File to Oracle WebCenter Content	4-1
Subscribe to Atom Feeds in a Scheduled Integration	4-4
Process Future Dated Entries on Their Effective Dates	4-5
Process Future Dated Entries Immediately	4-8
Configure the Extract Bulk Data Option in an Integration	4-9
Invoke an Endpoint Dynamically	4-10
Import Business Objects with the HCM Data Loader (HDL)	4-15
Select Extensible and Descriptive Flexfields in an Integration	4-20

5 Troubleshoot the Oracle HCM Cloud Adapter

Avoid Missing Atom Entries When Processing Them Page-Wise	5-1
Unsupported SOAP APIs Available for Selection	5-1
ATOM Feeds Option Not Appearing for Selection in the Operations Page	5-2
Manual Metadata Refresh is Required if Updating the Connection to Use the Interface Catalog URL	5-2

Preface

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

Note:

The use of this adapter may differ depending on the features you have, or whether your instance was provisioned using Standard or Enterprise edition. These differences are noted throughout this guide.

Topics:

- [Audience](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Related Resources](#)
- [Conventions](#)

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also

mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

See these Oracle resources:

- Oracle Cloud
<http://cloud.oracle.com>
- *Using Integrations in Oracle Integration Generation 2*
- *Using the Oracle Mapper with Oracle Integration Generation 2*

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.

Understand the Oracle HCM Cloud Adapter

Review the following conceptual topics to learn about the Oracle HCM Cloud 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 HCM Cloud Adapter Capabilities](#)
- [Oracle HCM Cloud Adapter Restrictions](#)
- [What Application Version Is Supported?](#)
- [Oracle HCM Cloud Adapter Use Cases](#)
- [Workflow to Create and Add an Oracle HCM Cloud Adapter Connection to an Integration](#)

Oracle HCM Cloud Adapter Capabilities

The Oracle HCM Cloud Adapter enables you to create an integration with Oracle Human Capital Management (HCM) Cloud applications. You select business objects that an integration receives from Oracle HCM Cloud as a request and as a response.

The Oracle HCM Cloud Adapter enables customers to easily integrate their on-premises or SaaS applications with Oracle HCM Cloud without having to know about the specific details involved in the integration.

The Oracle HCM Cloud Adapter provides the following benefits:

- Integrates easily with the Oracle HCM Cloud application's WSDL file to produce a simplified, integration-centric WSDL.
- Generates automatic mapping to the exposed business object that you select during adapter configuration as a trigger connection. A business object represents a self-contained business document that can be acted upon by the integration. An integration can send requests to create a new record for that business object. They can send a request either to update or delete an existing record for a business object. Integrations can also send requests to retrieve information about one or more records representing that business object.
- Supports invoking of business objects using the HCM Data Loader, regardless of how they were created. The HCM Data Loader is a tool for bulk-loading and maintaining data. The data can be from any source. You use the HCM Data Loader for data migration, ongoing maintenance of Oracle HCM Cloud data, and coexistence scenarios where core HR data is uploaded regularly.
See [Introduction to HCM Data Loader](#) and [Overview of Automating Data Loading of HCM Data Loader](#).
- Exposes the Business Resource (REST) API, which represents an Oracle Fusion Applications REST API resource.

You can select parent business resources and their corresponding child business resources on the Operations page in the Adapter Endpoint Configuration Wizard. Support is provided in the invoke (outbound) direction. If you select a top-level resource on the

Operations page, you can also select sub-resources on the Sub-Resources page. See [Invoke Child Resources Page](#)

- Simplified connection creation: Automatically identifies the required service catalog service WSDL and optional interface catalog URL to use based on the Oracle HCM Cloud host name you specify when creating a new connection on the Connections page.
- Supports consuming extensible flexfields (EFFs) and descriptive flexfields (DFFs) for REST resources. You can select specific EFFs and DFFs in the Adapter Endpoint Configuration Wizard of an Oracle HCM Cloud Adapter invoke connection. You can then map the EFFs and DFFs in the mapper. See [Select Extensible and Descriptive Flexfields in an Integration](#).
- Supports consumption of the Oracle HCM Cloud REST API. This enables the Oracle HCM Cloud Adapter to consume REST services under Oracle HCM Cloud when configured as an invoke connection. See [All REST Endpoints of REST API for Oracle HCM Cloud](#) for details about supported REST resources.
- Automatically handles security policy details required to connect to the Oracle HCM Cloud application.
- Supports the following security policies for selection during Oracle HCM Cloud Adapter connection configuration:
 - Username Password Token With PGP Key Support
 - Username Password Token
 - OAuth Authorization Code Credentials
- Provides standard error handling capabilities.
- Enables you to map business objects that have polymorphic data structures.
- Dynamically invokes a REST endpoint/URL at runtime without requiring you to configure any extra invoke connection or REST outbound details. See [Invoke an Endpoint Dynamically](#).
- Supports subscribing to the HCM Atom feed. Atom feeds enable you to track changes made to feed-enabled resources in Oracle Global Human Resources Cloud. For any updates of interest to downstream applications such as new hires, terminations, employee transfers, and promotions, Oracle Global Human Resources Cloud publishes Atom feeds. The Oracle HCM Cloud Adapter's Atom feed subscription feature enables you to select a feed of interest. This feature must be used in a scheduled manner because there is a need to poll for updates at regular intervals. This is done by selecting a scheduled orchestration template when creating the integration.

This feature is supported when using the Oracle HCM Cloud Adapter as an invoke connection in an integration.

Prior to HCM release 18c, future-dated Atom entries appeared in their respective Atom feed immediately once the future-dated action was taken.

Starting with HCM release 18c, there is a change in the way future-dated updates are returned by the HCM service. Atom feed entries appear by default once the future-dated actions become effective. You can select to process these future-dated Atom entries immediately on the Operations page of the Adapter Endpoint Configuration Wizard. The default behavior is to process future-dated Atom updates in the future.

See [Poll of REST API for Oracle HCM Cloud](#).

See [Atom Feeds of REST API for Oracle HCM Cloud](#).

- Enables you to upload files to Oracle WebCenter Content (Universal Content Manager) in encrypted or unencrypted format. Oracle WebCenter Content provides a unified repository

to store unstructured content, enabling organizations to deliver the content to business users in the proper format. See [Upload a File to Oracle WebCenter Content](#).

 **Note:**

Downloading files from Oracle WebCenter Content is not supported.

- Supports HCM data extracts, a flexible tool for generating data files and reports. The Oracle HCM Cloud Adapter works as an extract discovering tool under Oracle HCM Cloud. The data extract process is automated as per the following steps:
 - Invoking the given HCM data extract by the client outside the Oracle HCM Cloud Adapter.
 - Discovering the extract as delivered in Oracle WebCenter Content.
 - Fetching the extract output in its format as it is delivered to Oracle WebCenter Content and persisting the extract to Oracle Integration staging.
 - Defining the XML schema by the user for the extract output for transformation using a stage file action that is available in an orchestrated integration.

 **Note:**

The user must understand how to download the schema and how to schedule and run HCM extracts from the Oracle HCM Cloud user interface. See [Define Extracts of HCM Extracts](#).

This feature is supported when using the Oracle HCM Cloud Adapter as an invoke connection in an integration.

- Supports a set of SOAP services. For the supported list, see [Business Object Services of SOAP Web Services for HCM](#). The following integration behavior occurs:
 - For new integrations, only the supported SOAP services are displayed for selection when configuring the Oracle HCM Cloud Adapter in the Adapter Endpoint Configuration Wizard. Unsupported SOAP services are not displayed.
 - For existing integrations, you can edit, view, and activate old integration as before. If you add a new adapter endpoint to an existing integration, only supported SOAP services are available for selection in the Adapter Endpoint Configuration Wizard.

Oracle HCM Cloud Adapter Restrictions

Note the following Oracle HCM Cloud Adapter restrictions.

- The System for Cross-Domain Identity Management (SCIM) REST API under Oracle HCM Cloud is not discoverable through the Oracle Application Development Framework. Therefore, the Oracle HCM Cloud Adapter is unable to list those resources during design time. As an alternative, use the REST Adapter with the SCIM REST API under Oracle HCM Cloud.
- Downloading files from Oracle WebCenter Content is not supported.
- Oracle Applications Cloud REST API framework versions 6 and above are not supported. Using these versions results in a runtime error. See [Set the REST Framework Version in REST API for Oracle Fusion Cloud HCM](#).

 **Note:**

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

What Application Version Is Supported?

For information about which application version is supported by this adapter, see the Connectivity Certification Matrix.

See [Connectivity Certification Matrix](#).

Oracle HCM Cloud Adapter Use Cases

Common use cases for the Oracle HCM Cloud Adapter are as follows:

- New employee onboarding
- Integrate with third-party benefits providers such as health insurance providers
- Extract employee data monthly from Oracle HCM Cloud for payroll

Workflow to Create and Add an Oracle HCM Cloud 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	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 HCM Cloud Adapter Connection
2	Create the integration. When you do this, you add trigger and invoke connections to the integration.	Create Integrations and Add the Oracle HCM Cloud Adapter Connection to an Integration
3	Map data between the trigger connection data structure and the invoke connection data structure.	Map Data in <i>Using Integrations in Oracle Integration Generation 2</i>
4	(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 Generation 2</i>
5	Activate the integration.	Manage Integrations in <i>Using Integrations in Oracle Integration Generation 2</i>
6	Monitor the integration on the dashboard.	Monitor Integrations in <i>Using Integrations in Oracle Integration Generation 2</i>

Step	Description	More Information
7	Track payload fields in messages during runtime.	Assign Business Identifiers for Tracking Fields in Messages and Manage Business Identifiers for Tracking Fields in Messages in <i>Using Integrations in Oracle Integration Generation 2</i>
8	Manage errors at the integration level, connection level, or specific integration instance level.	Manage Errors in <i>Using Integrations in Oracle Integration Generation 2</i>

Create an Oracle HCM Cloud 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 an SSL Certificate](#)
- [Refresh Integration Metadata](#)

Prerequisites for Creating a Connection

Satisfy the following prerequisites specific to your environment to create a connection with the Oracle HCM Cloud Adapter.

- [Subscribe to Oracle HCM Cloud](#)
- [Assign Required Roles to an Integration User](#)
- [Request Access to Atom Feeds and REST APIs Capabilities on Your Oracle HCM Cloud Instances](#)
- [Create an HCM-compliant .dat File to Use the HCM Data Loader](#)
- [Upload Files to Oracle WebCenter Content](#)
- [Perform Prerequisites to Set Up the OAuth Authorization Code Credentials Security Policy](#)
- [Verify the Status of Location-Based Access Control \(LBAC\)](#)
- [Specify the Oracle HCM Cloud Service Catalog Service WSDL or Service Interface URL \(For Connections Created Prior to 2/18/20\)](#)

Subscribe to Oracle HCM Cloud

Subscribe to Oracle HCM Cloud. This action enables you to create an Oracle HCM Cloud user account with the correct privileges. You specify this user account when creating an Oracle HCM Cloud Adapter connection on the Connections page.

For information about specifying these credentials on the Connections page, see [Configure Connection Security](#). For information about subscribing, see [Oracle HCM Cloud](#).

Assign Required Roles to an Integration User

To use the Oracle HCM Cloud Adapter in an integration, you must assign specific roles to an integration user.

Associating the Integration User with the Following Roles and Privileges

You associate the user with the following roles and privileges.

Role	Description
ALL_INTEGRATION_POINTS_ALL_DATA	Starting with release 12, this role is no longer supported. When existing customers upgrade to release 12, users with this role continue using it, although it is hidden from the Security Console. If you create a new integration user in release 12 or later, you cannot assign this role.
ORA_HRC_HUMAN_CAPITAL_MANAGEMENT_INTEGRATION_SPECIALIST_JOB	Human Capital Management Integration Specialist. The role applies to Releases 12 and 13.
AttachmentsUser	Provides access to the Attachments security group to download the log file or the output file with the HCM Integration Service. Starting with Release 12, this role is automatically shipped. You must verify that this role is automatically assigned to the user.
SOAOperator	The SOA Operator role.
FND_MANAGE_CATALOG_SERVICE_PRIV	Role for managing the web services catalog.
For Oracle CRM Cloud implementations, you can also assign the Customer Relationship Management Application Administrator role.	See Customer Relationship Management Application Administrator (Job Role) of Security Reference for CX Sales and B2B Service .

Additional roles may be required as per each interface requirements.

Using the Security Console

Use the Security Console to manage application security such as roles, users, certificates, and administration tasks. Access to the Security Console is provided by the predefined **Security Manager** role. Access the Security Console in the following ways:

- Use the Manage Job Roles or Manage Duties tasks in the Setup and Maintenance work area.
- Select **Navigator > Tools > Security Console**.



Request Access to Atom Feeds and REST APIs Capabilities on Your Oracle HCM Cloud Instances

Oracle HCM Cloud Atom feeds and Oracle HCM Cloud REST APIs support is available by default in the Oracle HCM Cloud Adapter in Oracle Integration. However, for the Oracle HCM Cloud application, you must first request access to Atom feeds and REST APIs capabilities on your Oracle HCM Cloud instance(s).

See the steps described in My Oracle Support Note [2060899.1](#). Once these are enabled in your Oracle HCM Cloud application, Atom feeds and REST APIs appear in the Oracle HCM Cloud Adapter in Oracle Integration.

Create an HCM-compliant .dat File to Use the HCM Data Loader

If you want to use the HCM Data Loader for bulk-loading and maintaining data, you must create a .dat file that is HCM-compliant. See your Oracle HCM Cloud documentation for instructions.

Upload Files to Oracle WebCenter Content

You must satisfy the following prerequisites if you want to upload a file to Oracle WebCenter Content (Universal Content Manager) with the Oracle HCM Cloud Adapter.

- Create a PGP Public Key for Encrypted File Upload:

To upload encrypted files, a PGP public key is required. You must generate the PGP public key and save it for upload. The supported algorithm for the public key is RSA for encryption and the key size must be 1024 bits in length.

The process for uploading files into Oracle HCM Cloud is:

- You encrypt files using the Oracle HCM Cloud public key.
- The data-loading process decrypts files using the Oracle HCM Cloud private key.

See [Set up Encryption for File Transfer](#) in *HCM Data Loader*.

- Configure Security and User Access

Once you have configured security groups and doc accounts for the file to upload, you can configure the Oracle HCM Cloud Adapter to upload the file to Oracle WebCenter Content.

Perform Prerequisites to Set Up the OAuth Authorization Code Credentials Security Policy

Perform the following prerequisites to set up the OAuth Authorization Code Credentials security policy with an Oracle Fusion Applications identity domain, a non-Oracle Fusion Applications identity domain (for example, the Oracle Integration identity domain), or Oracle Identity Cloud Service.

Topics:

- [Set Up the OAuth Authorization Code Credentials Security Policy with the Oracle Fusion Applications Identity Domain](#)

- Set Up the OAuth Authorization Code Credentials Security Policy with a Non-Oracle Fusion Applications Identity Domain
- Set Up the OAuth Authorization Code Credentials Security Policy with Oracle Identity Cloud Service

Set Up the OAuth Authorization Code Credentials Security Policy with the Oracle Fusion Applications Identity Domain

You must create a resource application to represent the Oracle Fusion Applications resource and a client application for Oracle Integration to use the OAuth Authorization Code Credentials security policy. Once these tasks are completed, you can successfully configure a connection on the Connections page. You do not need to create any JWT signing certificates for upload into Oracle Fusion Applications.

- Create an Identity Domain Resource Application to Represent the Oracle Fusion Applications Resource
- Create the Confidential Client Application for Oracle Integration
- Resolve Errors That Occur When Clicking Provide Consent

Create an Identity Domain Resource Application to Represent the Oracle Fusion Applications Resource

1. Create an identity domain resource application to represent the Oracle Fusion Applications resource.
 - a. Log in to the identity domain as the domain administrator.
 - b. In the navigation pane, click **Identity & Security**.
 - c. Click **Domains**.
 - d. Select your compartment.
 - e. Click the identity domain.
 - f. In the navigation pane, click **Integrated applications**.
 - g. Click **Add application**.
 - h. Select **Confidential Application**, then click **Launch workflow**.
2. a. On the Details page, provide a name (for example, FA Resource), and click **Next**.
 - b. On the Client page, click **Next** without making changes.
 - c. On the Resources page, click **Configure this application as a resource server now**.
 - d. Optionally update the value in the **Access Token Expiration** field.
 - e. Select **Is Refresh Token Allowed**.
 - f. In the **Primary Audience** field, add the Oracle Fusion Applications URL and port. This is the primary recipient where the token is processed.

`https://FA_URL:443`

- g. In the **Scopes** section, click **Add**.
- h. In the **Scope** field, enter `/`.
- i. In the **Description** field, enter `All`.
- j. Select **Requires Consent**.

- k. Click **Add**, then click **Next**.
- l. On the Web Tier Policy and Authorization pages, click **Next** without making any changes.
- m. Click **Finish** to complete resource application creation.
- n. Click **Activate** to activate your client application. The resource server representing the resource is now active.

Create the Confidential Client Application for Oracle Integration

1. Sign in as the identity domain administrator to the Oracle Cloud Infrastructure Console.
2. In the navigation pane, click **Identity & Security**.
3. Click **Domains**.
4. Select your compartment.
5. Click the identity domain.
6. In the navigation pane, click **Integrated applications**.
7. Click **Add application**.
8. Select **Confidential Application**, then click **Launch workflow**.
9. Enter a name. The remaining fields on this page are optional and can be ignored.
10. Click **Next**.
11. In the **Client configuration** box, select **Configure this application as a client now**.
12. For authorization code, select **Refresh token** and **Authorization code** in the **Allowed grant types** section.
13. In the **Redirect URL** field, enter the redirect URL of the client application. After user login, this URL is redirected to with the authorization code. You can specify multiple redirect URLs. This is useful for development environments in which you have multiple instances, but only one client application due to licensing issues. For example:

 **Note:**

If you don't know the following information, check with your administrator:

- If your instance is new or upgraded from Oracle Integration Generation 2 Generation 2 to Oracle Integration Generation 2.
- The complete instance URL with the region included (required for new instances).

For Connections...	Include the Region as Part of the Redirect URL?	Example of Redirect URL to Specify...
--------------------	---	---------------------------------------

Created on new Oracle Integration Generation 2 instances	Yes.	<code>https:// OIC_instance_URL.region.ocp.oraclecloud. com/icsapis/agent/oauth/callback</code>
--	------	---

For Connections...	Include the Region as Part of the Redirect URL?	Example of Redirect URL to Specify...
Created on instances upgraded from Oracle Integration Generation 2 Generation 2 to Oracle Integration Generation 2	No. This applies to both: <ul style="list-style-type: none"> • New connections created after the upgrade • Existing connections that were part of the upgrade 	<code>https:// OIC_instance_URL.ocp.oraclecloud.com/ icsapis/agent/oauth/callback</code>

For the OAuth authorization code to work, the redirect URI must be set properly.

- Under **Resources**, click **Add Scope** to add appropriate scopes. If the Oracle Fusion Applications instance is federated with the identity domain, the Oracle Integration cloud service application is listed among the resources for selection. This enables the client application to access Oracle Integration.
- Search for the Oracle Fusion Applications resource application created in [Create an Identity Domain Resource Application to Represent the Oracle Fusion Applications Resource](#).
- Select the resource and click **>**.
- Select the scope, then click **Add**.
- Click **Next** without making changes on the Resource and Web Tier Policy pages.
- On the Authorization page, click **Finish**.
The Application Added dialog shows the client ID and client secret values.
- Copy and save these values. You need this information when creating a connection for the OAuth Authorization Code Credentials security policy on the Connections page.
Note the following details for successfully authenticating your account on the Connections page.

If The...	Then...
Identity domain safeguarding Oracle Integration and the Oracle Fusion Applications resource application are the same.	Log in to Oracle Integration using the local Oracle Fusion Applications user created earlier. You must create a connection and click Provide Consent on the Connections page for authentication to succeed.
Identity domain safeguarding Oracle Integration and the Oracle Fusion Applications resource application are different.	Log in to Oracle Integration using a general Oracle Integration developer account, create a connection, and click Provide Consent on the Connections page. You need to log in to the Oracle Fusion Applications resource identity domain application using the local Oracle Fusion Applications user account created earlier.

- Activate the application.

Resolve Errors That Occur When Clicking Provide Consent

After you configure the OAuth Authorization Code Credentials security policy on the Connections page, you must test your connection.

If you are logged in to Oracle Integration with an Oracle Integration user account and click **Provide Consent** to test the OAuth flow, consent is successful. However, when you test the connection, it fails with an **Unauthorized 401** error.

This error occurs because the Oracle Integration user account with which you logged in is not part of Oracle Fusion Applications.

1. Log out of Oracle Integration and log back in with a user account that exists in Oracle Fusion Applications.
2. Return to the Connections page and retest the connection.
The connection is successful this time.

Set Up the OAuth Authorization Code Credentials Security Policy with a Non-Oracle Fusion Applications Identity Domain

You must set up trust between Oracle Fusion Applications and an identity domain and create a client application for Oracle Integration to use the OAuth Authorization Code Credentials security policy. Once these tasks are completed, you can successfully configure a connection on the Connections page. Use this option when you are integrating with a non-Oracle Fusion Applications identity domain, such as the Oracle Integration identity domain.

- [Set Up Trust Between Oracle Fusion Applications and an Identity Domain](#)
- [\(Optional\) Create a Local User](#)
- [Create the Confidential Client Application for Oracle Integration](#)
- [Avoid Potential Errors When Testing Your Connection with a Nonfederated User Account](#)

Set Up Trust Between Oracle Fusion Applications and an Identity Domain

1. Get the JWK signing certificates from the identity domain of Oracle Integration.
 - a. Get the REST API of the identity domain endpoint that gives you the signing certificate endpoint. For example:

`/admin/v1/SigningCert/jwk`

See [All REST Endpoints](#) in *REST API for Oracle Identity Cloud Service*.

- b. Copy the endpoint.
 - c. Get the identity domain URL from the Oracle Cloud Infrastructure Console or from the Oracle Integration **About** menu.
 - d. Add that URL to the front of the signing certificate and use a tool (for example, `postman`) to invoke the REST APIs. For example:

`https://identity_domain_URL.identity.oraclecloud.com/admin/v1/`
`SigningCert/jwk`

- e. Perform a GET call to retrieve the payloads of the certificates. There are two sections in the payload:
 - Identity domain certificate
 - Certificate authority (CA) certificate

Examples of the type of response you receive are provided. See [Retrieve the Tenant's Signing Certificate in JWK Format](#).

- f. Copy both certificate sections into separate files. Note that the headers and footers in the files must be in the following exact format to be successfully uploaded to Oracle Fusion Applications:

-----BEGIN CERTIFICATE-----
content_of_certificate
...
...
-----END CERTIFICATE-----

You can validate the certificate. For example:

```
openssl x509 -in IDCS.cert -noout -text
```

2. File a service request (SR) with Oracle Fusion Applications and attach your certificates for upload. You cannot upload the certifications yourself.
3. Create a resource application in an Oracle Integration identity domain to represent the Oracle Fusion Applications resource.
 - a. Log in to the identity domain as the domain administrator.
 - b. In the navigation pane, click **Identity & Security**.
 - c. Click **Domains**.
 - d. Select your compartment.
 - e. Click the identity domain.
 - f. In the navigation pane, click **Integrated applications**.
 - g. Click **Add application**.
 - h. Select **Confidential Application**, then click **Launch workflow**.
 - i. On the Details page, provide a name (for example, FA Resource), and click **Next**.
 - j. On the Client page, click **Next** without making changes.
 - k. On the Resources page, click **Configure this application as a resource server now**.
 - l. Optionally update the value in the **Access Token Expiration** field.
 - m. Select **Is Refresh Token Allowed**.
 - n. In the **Primary Audience** field, add the Oracle Fusion Applications URL and port. This is the primary recipient where the token is processed.

`https://FA_URL:443`

- o. In the **Scopes** section, click **Add**.
p. In the **Scope** field, enter `/`.
q. In the **Description** field, enter `All`.
r. Select **Requires Consent**.
s. Click **Add**, then click **Next**.
t. On the Web Tier Policy and Authorization pages, click **Next** without making any changes.
u. Click **Finish** to complete resource application creation.

- v. Click **Activate** to activate your client application. The resource server representing the resource is now active.

(Optional) Create a Local User

 **Note:**

The following step is required if the Oracle Fusion Applications user is *not* federated with an identity domain or whichever identity provider you are using.

1. Create an identity domain local user. *Carefully* review the following table to see if you already have a local user.

Scenario	Do I Need to Create a Local User?
You have an Oracle Fusion Applications user federated with the identity domain that is protecting Oracle Integration.	No. You do not need to create the local identity domain Oracle Fusion Applications user. This is because identity domain already has Oracle Fusion Applications users in its repository.
You do <i>not</i> have federation between Oracle Fusion Applications and the identity domain that is protecting Oracle Integration.	Yes. You must create the local identity domain Oracle Fusion Applications user that you plan to use with the OAuth setup in Oracle Integration.

The identity domain administrator must create a nonfederated local username in the identity domain that matches the user in Oracle Fusion Applications. If you have already used and invoked Oracle Fusion Applications REST endpoints, you likely already created a user with the necessary roles and accesses to invoke the REST endpoints of Oracle Fusion Applications. This user must be created in the identity domain and have a local user password.

Create the Confidential Client Application for Oracle Integration

1. Sign in as the identity domain administrator to the Oracle Cloud Infrastructure Console.
2. In the navigation pane, click **Identity & Security**.
3. Click **Domains**.
4. Select your compartment.
5. Click the identity domain.
6. In the navigation pane, click **Integrated applications**.
7. Click **Add application**.
8. Select **Confidential Application**, then click **Launch workflow**.
9. Enter a name. The remaining fields on this page are optional and can be ignored.
10. Click **Next**.
11. In the **Client configuration** box, select **Configure this application as a client now**.
12. For authorization code, select **Refresh token** and **Authorization code** in the **Allowed grant types** section.
13. In the **Redirect URL** field, enter the redirect URL of the client application. After user login, this URL is redirected to with the authorization code. You can specify multiple redirect

URLs. This is useful for development environments in which you have multiple instances, but only one client application due to licensing issues. For example:

 **Note:**

If you don't know the following information, check with your administrator:

- If your instance is new or upgraded from Oracle Integration Generation 2 Generation 2 to Oracle Integration Generation 2.
- The complete instance URL with the region included (required for new instances).

For Connections...	Include the Region as Part of the Redirect URL?	Example of Redirect URL to Specify...
Created on new Oracle Integration Generation 2 instances	Yes.	<code>https:// OIC_instance_URL.region.ocp.oraclecloud. com/icsapis/agent/oauth/callback</code>
Created on instances upgraded from Oracle Integration Generation 2 to Oracle Integration Generation 2	No. This applies to both: <ul style="list-style-type: none"> • New connections created after the upgrade • Existing connections that were part of the upgrade 	<code>https:// OIC_instance_URL.ocp.oraclecloud.com/ icsapis/agent/oauth/callback</code>

For the OAuth authorization code to work, the redirect URI must be set properly.

14. Under **Resources**, click **Add Scope** to add appropriate scopes. If the Oracle Fusion Applications instance is federated with the identity domain, the Oracle Integration cloud service application is listed among the resources for selection. This enables the client application to access Oracle Integration.
15. Search for the Oracle Fusion Applications resource application created in [Set Up Trust Between Oracle Fusion Applications and an Identity Domain](#).
16. Select the resource and click **>**.
17. Select the scope, then click **Add**.
18. Click **Next** without making changes on the Resource and Web Tier Policy pages.
19. On the Authorization page, click **Finish**.
The Application Added dialog shows the client ID and client secret values.
20. Copy and save these values. You need this information when creating a connection for the OAuth Authorization Code Credentials security policy on the Connections page.
Note the following details for successfully authenticating your account on the Connections page.

If The...	Then...
Identity domain safeguarding Oracle Integration and the Oracle Fusion Applications resource application are the same.	Log in to Oracle Integration using the local Oracle Fusion Applications user created earlier. You must create a connection and click Provide Consent on the Connections page for authentication to succeed.
Identity domain safeguarding Oracle Integration and the Oracle Fusion Applications resource application are different.	Log in to Oracle Integration using a general Oracle Integration developer account, create a connection, and click Provide Consent on the Connections page. You need to log in to the Oracle Fusion Applications resource identity domain application using the local Oracle Fusion Applications user account created earlier.

21. Activate the application.

Avoid Potential Errors When Testing Your Connection with a Nonfederated User Account

After you configure the OAuth Authorization Code Credentials security policy on the Connections page, you must test your connection.

If you are logged in to Oracle Integration with an Oracle Integration user account and click **Provide Consent** to test the OAuth flow, consent is successful. However, when you test the connection, it fails with an `Unauthorized 401` error.

This error occurs because the Oracle Integration user account with which you logged in is not part of Oracle Fusion Applications.

1. Log out of Oracle Integration and log back in with a user account that exists in Oracle Fusion Applications.
2. Return to the Connections page and retest the connection.
The connection is successful this time.

Set Up the OAuth Authorization Code Credentials Security Policy with Oracle Identity Cloud Service

You must set up trust between Oracle Fusion Applications and Oracle Identity Cloud Service and create a client application for Oracle Integration if you want to use the OAuth Authorization Code Credentials security policy. Once these tasks are completed, you can successfully configure a connection on the Connections page.

 **Note:**

The following instructions apply *only* to cloud tenancies that still use Oracle Identity Cloud Service. Most cloud tenancies have been migrated to identity domains, which require different configuration instructions. See [Set Up the OAuth Authorization Code Credentials Security Policy with the Oracle Fusion Applications Identity Domain](#) or [Set Up the OAuth Authorization Code Credentials Security Policy with a Non-Oracle Fusion Applications Identity Domain](#). If you are unsure of your environment, check with your administrator.

- [Set Up Trust Between Oracle Fusion Applications and Oracle Identity Cloud Service](#)
- [Create the Confidential Client Application for Oracle Integration](#)

- [\(Optional\) Create a Local User](#)
- [Avoid Potential Errors When Testing Your Connection with a Nonfederated User Account](#)

Set Up Trust Between Oracle Fusion Applications and Oracle Identity Cloud Service

1. Get the JWK signing certificates from the Oracle Identity Cloud Service of Oracle Integration.
 - a. Get the REST API of the Oracle Identity Cloud Service endpoint that gives you the signing certificate endpoint. For example:

```
/admin/v1/SigningCert/jwk
```

See [All REST Endpoints](#) in *REST API for Oracle Identity Cloud Service*.

- b. Copy the endpoint.
- c. Get the Oracle Identity Cloud Service URL from the Oracle Cloud Infrastructure Console or from the Oracle Integration **About** menu.
- d. Add that URL to the front of the signing certificate and use a tool (for example, `postman`) to invoke the REST APIs. For example:

```
https://IDCS_URL.identity.oraclecloud.com/admin/v1/SigningCert/jwk
```

- e. Perform a GET call to retrieve the payloads of the certificates. There are two sections in the payload:
 - Oracle Identity Cloud Service certificate
 - Certificate authority (CA) certificate

Examples of the type of response you receive are provided. See [Retrieve the Tenant's Signing Certificate in JWK Format](#).

- f. Copy both certificate sections into separate files. Note that the headers and footers in the files must be in the following exact format to be successfully uploaded to Oracle Fusion Applications:

```
-----BEGIN CERTIFICATE-----  
content_of_certificate  
.  
.  
-----END CERTIFICATE-----
```

You can validate the certificate. For example:

```
openssl x509 -in IDCS.cert -noout -text
```

2. Upload the certificates to the Oracle Fusion Applications Security Console.
 - a. Log in to Oracle Fusion Applications as a user with the IT Security Manager role.
 - b. In the navigation pane, select **Tools**, then **Security Console**.
 - c. Select **API authentication** in the left navigation pane.
 - d. Click **Create Oracle API Authentication Provider**, then click **Edit** in the upper right.

- e. In the **Trusted Issuer** field, enter:

`https://identity.oraclecloud.com`

- f. In the **Token Types** section, select **JWT**.
- g. Click **Save and Close**.
- h. Click **Inbound API Authentication Public Certificates**, then click **Add New Certificate**.
- i. Enter a name in the **Certificate Alias** field (for example, `MY_IDCS_CERT`).
- j. In the **Import Public Certificate** field, click **Choose File** to upload the first certificate file, then click **Save**.
- k. Repeat these steps to upload the second certificate file.

3. Create an Oracle Identity Cloud Service resource application to represent the Oracle Fusion Applications resource.
 - a. Log in to Oracle Identity Cloud Service as the Oracle Identity Cloud Service administrator.
 - b. In the left navigation pane, click **Applications**, then click **Add**.
 - c. Click **Confidential Application**.
 - d. On the Details page, provide a name (for example, `FA Resource`), and click **Next**.
 - e. On the Client page, click **Next** without making changes.
 - f. On the Resources page, click **Configure this application as a resource server now**.
 - g. Optionally update the value in the **Access Token Expiration** field.
 - h. Select **Is Refresh Token Allowed**.
 - i. In the **Primary Audience** field, add the Oracle Fusion Applications URL and port. This is the primary recipient where the token is processed.

`https://FA_URL:443`

- j. In the **Scopes** section, click **Add**.
The Add Scope dialog appears.
- k. In the **Scope** field, enter `/`.
- l. In the **Display Name** field, enter a display name.
- m. In the **Description** field, enter `All`.
- n. Select **Requires Consent**.
- o. Click **Add**.
- p. Click **Next** to move to the next page in the wizard.
- q. On the Web Tier Policy page, click **Next** without making any changes.
- r. On the Authorization page, click **Next** without making any changes.
- s. Click **Finish** to complete resource application creation.
- t. Click **Activate** to activate your client application. The resource server representing the resource is now active.

(Optional) Create a Local User **Note:**

The following step is only required if the Oracle Fusion Applications user is *not* federated with Oracle Identity Cloud Service or whichever identity provider you are using.

1. Create an Oracle Identity Cloud Service local user. Carefully review the following table to see if you already have a local user.

Scenario	Do I Need to Create a Local User?
You have an Oracle Fusion Applications user federated with the Oracle Identity Cloud Service that is protecting Oracle Integration.	No. You do not need to create the local Oracle Identity Cloud Service Oracle Fusion Applications user. This is because Oracle Identity Cloud Service already has Oracle Fusion Applications users in its repository.
You do <i>not</i> have federation between Oracle Fusion Applications and the Oracle Identity Cloud Service that is protecting Oracle Integration.	Yes. You must create the local Oracle Identity Cloud Service Oracle Fusion Applications user that you plan to use with the OAuth setup in Oracle Integration.

The Oracle Identity Cloud Service administrator must create a nonfederated local username in Oracle Identity Cloud Service that matches the user in Oracle Fusion Applications. If you have already used and invoked Oracle Fusion Applications REST endpoints, you likely already created a user with the necessary roles and accesses to invoke the REST endpoints of Oracle Fusion Applications. This user must be created in Oracle Identity Cloud Service and have a local user password.

Create the Confidential Client Application for Oracle Integration

1. Sign in as the Oracle Identity Cloud Service administrator to the Oracle Cloud Infrastructure Console. This administrator must have Oracle Identity Cloud Service instance access.
2. In the left navigation pane, select **Applications**, then click **Add** to add a client application.
3. Select **Confidential Application**.
The Add Confidential Application wizard is displayed.
4. On the Details page, enter an application name, and click **Next**.
5. On the Client page, click **Configure this application as a client now**.
6. In the **Authorization** section, select **Refresh Token** and **Authorization Code**.
7. In the **Redirect URL** field, enter your Oracle Integration instance URL and port. For example:

`https://OIC_URL:443/icsapis/agent/oauth/callback`

For the OAuth authorization code to work, the redirect URI must be set properly.

8. Under **Resources**, click **Add Scope** to add appropriate scopes.

If the Oracle Fusion Applications instance is federated with the Oracle Identity Cloud Service instance, the Oracle Integration cloud service application is listed among the resources for selection. This enables the client application to access Oracle Integration.

9. Search for the Oracle Fusion Applications resource application created in [Set Up Trust Between Oracle Fusion Applications and Oracle Identity Cloud Service](#).
10. Select the resource and click **>**.
11. Select the scope, then click **Add**.
12. Click **Next** without making changes on the Resource and Web Tier Policy pages.
13. On the Authorization page, click **Finish**.
The Application Added dialog shows the client ID and client secret values.
14. Copy and save these values. You need this information when creating a connection for the OAuth Authorization Code Credentials security policy on the Connections page.
Note the following details for successfully authenticating your account on the Connections page.

If The...	Then...
Oracle Identity Cloud Service safeguarding Oracle Integration and the Oracle Fusion Applications resource application are the same.	Log in to Oracle Integration using the local Oracle Fusion Applications user created earlier. You must create a connection and click Provide Consent on the Connections page for authentication to succeed.
Oracle Identity Cloud Services safeguarding Oracle Integration and the Oracle Fusion Applications resource application are different.	Log in to Oracle Integration using a general Oracle Integration developer account, create a connection, and click Provide Consent on the Connections page. You need to log in to the Oracle Fusion Applications resource Oracle Identity Cloud Service application using the local Oracle Fusion Applications user account created earlier.

15. Activate the application.

Avoid Potential Errors When Testing Your Connection with a Nonfederated User Account

After you configure the OAuth Authorization Code Credentials security policy on the Connections page, you must test your connection.

If you are logged in to Oracle Integration with an Oracle Integration user account and click **Provide Consent** to test the OAuth flow, consent is successful. However, when you test the connection, it fails with an `Unauthorized 401` error.

This error occurs because the Oracle Integration user account with which you logged in is not part of Oracle Fusion Applications.

1. Log out of Oracle Integration and log back in with a user account that exists in Oracle Fusion Applications.
2. Return to the Connections page and retest the connection.
The connection is successful this time.

Verify the Status of Location-Based Access Control (LBAC)

Check if you have enabled Location-Based Access Control (LBAC) for Fusion Applications (for Oracle HCM Cloud).

If LBAC is enabled, you must allowlist (explicitly allow identified entities access) the Oracle Integration NAT Gateway IP address in your LBAC. If you do not perform this task, you can receive a `401 Access Denied` error or `403 Forbidden` error from Oracle Fusion Applications.

See [How Location-Based Access Works](#) in *Securing SCM* and Doc ID 2615294.1 at [Oracle Support Services](#).

Specify the Oracle HCM Cloud Service Catalog Service WSDL or Service Interface URL (For Connections Created Prior to 2/18/20)

The steps in this section are only required for existing connections created prior to the initial release of the simplified connections page on 2/18/20. For existing connections, you are prompted to specify a mandatory Oracle HCM Cloud service catalog service WSDL (for accessing business objects) in the **HCM Services Catalog WSDL URL** field and optional interface catalog URL (for accessing the outbound endpoint using REST resources) in the **Interface Catalog URL** field.

 **Note:**

For new connections created with the initial release of the simplified connections page on 2/18/20, the preconfiguration details described in this section are not required. All WSDLs and URLs are automatically identified for you based on the Oracle HCM Cloud host name that you specify in the **HCM Cloud Host** field on the Connections page.

The following sections describe how to obtain the service catalog service WSDL and interface catalog URL:

- [For Fusion Applications Releases 10 Through 12](#)
- [For Fusion Applications Releases 13 and Later](#)

For Fusion Applications Releases 10 Through 12

Obtain the Oracle Fusion Applications Releases 10 through 12 service catalog service WSDLs and interface catalog URLs through the following methods.

- [Obtain the Service Catalog Service WSDL for Releases 10 Through 11](#)
- [Obtain the Service Catalog Service WSDL for Release 12](#)
- [Obtain the Interface Catalog URL](#)

Obtain the Service Catalog Service WSDL for Releases 10 Through 11

WSDL Requirements	Where Do You Get the WSDL?
<p>The URL must be that of a service catalog service WSDL. The service catalog service is a Fusion Application service that returns a list of external services available for integration. It allows clients to retrieve information about all public Fusion Application service endpoints available for that instance.</p> <p>The service catalog service enables clients to retrieve information about all public Oracle Fusion Application service endpoints available for that instance. The information it returns is specific to the particular cloud instance and also reflects the new services that may have been introduced in patches applied to the instance. This service is used to programmatically discover the SOAP services available on the cloud instance and retrieve the necessary metadata to invoke the SOAP services to manage business objects.</p>	<p>The developer creating an Oracle HCM Cloud connection must work with the Oracle HCM Cloud service administrator to get the concrete WSDL URL for the service catalog service provisioned for the specific SaaS application.</p>

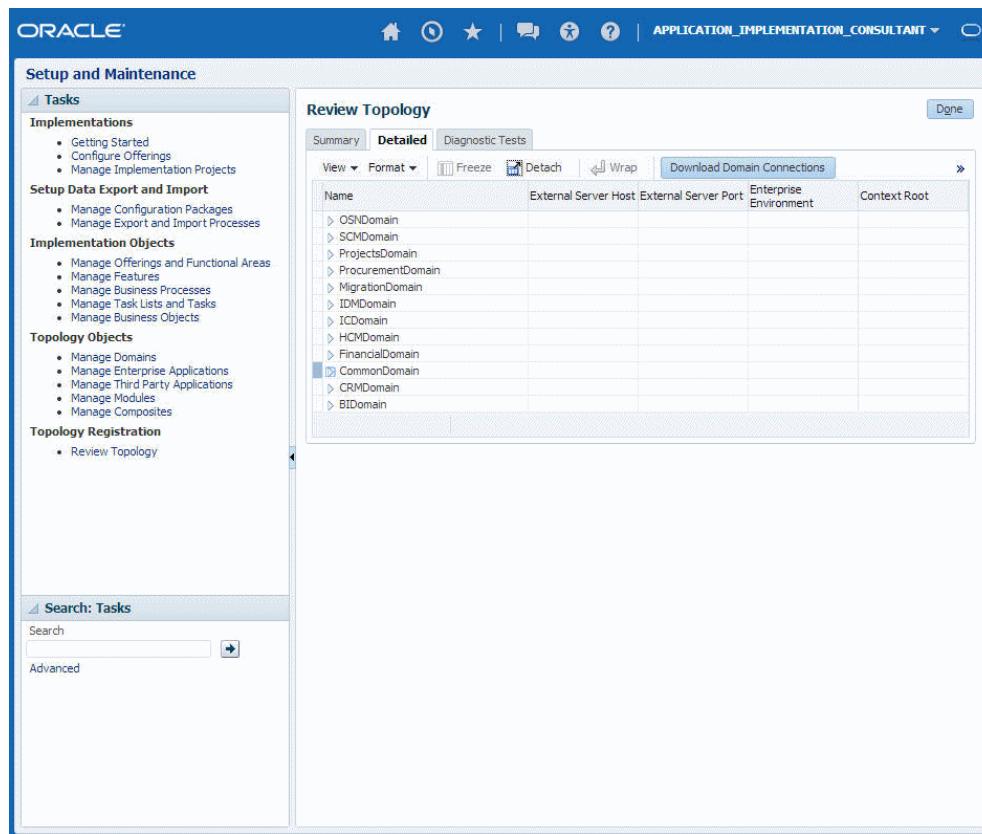
This section describes how to derive the external virtual host and port for a tokenized service catalog service WSDL. The topology information in the Topology Registration setup task contains the external virtual host and port for the domains and applications. The following instructions describe the steps for deriving the values using the service catalog service WSDL URL as an example: https://atf_server:port/fndAppCoreServices/ServiceCatalogService.

To access the Review Topology page, the ASM_REVIEW_TOPOLOGY_HIERARCHY_PRIV entitlement must be granted to the user's job role. The entitlement is granted to the ASM_APPLICATION_DEPLOYER_DUTY duty role, which is inherited by the duty roles ASM_APPLICATION_DEVELOPER_DUTY and ASM_APPLICATION_ADMIN_DUTY.

If the menu items and tasks described in the following procedure are not available in your cloud instance, your user account is missing the required role. Contact your cloud instance security administrator for assistance.

1. Log in to the cloud instance.
2. Click the **Navigator** icon in the global area in the top part of the window, then chose **Setup and Maintenance** under the **Tools** heading.
3. Select **Review Topology** under the **Topology Registration** section in the **Tasks** regional area on the left side of the window.
4. Click the **Detailed** tab in the middle of the window.

The tab shows the list of domains configured in the cloud instance.



5. Map the token name for the service path value to the domain name in the Topology Manager:

Token Name in Service Path	Domain Name
atf_server	CommonDomain
crm_server	CRMDomain
fin_server	FinancialDomain
hcm_server	HCMDomain
ic_server	ICDomain
prc_server	ProcurementDomain
prj_server	ProjectsDomain
scm_server	SCMDomain

6. Expand the domain name and select any external virtual host and port for the J2EE applications that are deployed on the domain. In the sample window, the values for this particular instance are **fs-your-cloud-hostname** and **443**, respectively.

Name	External Server Host	External Server Port	Context Root
Image Process Management	fs-your-cloud-hostname	443	or...
Inbound Refinery	fs-your-cloud-hostname	443	or...
Zms Stock Quote			or...
Zms Rss Feed			or...
WLM			or...
TopologyManagerService	fs-your-cloud-hostname	443	or...
Setup Web Services Policy Mgr	fs-your-cloud-hostname	443	or...
Setup-SOA	fs-your-cloud-hostname	443	or...
Setup-ESS	fs-your-cloud-hostname	443	or...
Setup Diagnostic Dashboard	fs-your-cloud-hostname	443	or...
Setup	fs-your-cloud-hostname	443	or...
Security Token Service	fs-your-cloud-hostname	443	or...
Search ESS	fs-your-cloud-hostname	443	or...
ST Conference			or...
PJPG6 Primavera Application	fs-your-cloud-hostname	6030	or...
Oracle University			or...
Oracle Portal Home			or...
Oracle Fusion Applications Tec			or...
Applications Core Setup	fs-your-cloud-hostname	443	or...
fndWebServices			fndWebServices
fndSetup			fndSetup
fndAppCoreServices			fndAppCoreServices
Oracle Fusion Applications For			or...
Oracle Documentation Portal			or...
My Oracle Support Community			or...

7. Replace the `domainName_server:PortNumber` with the external virtual host and port identified in the previous step. For example:

`https://fs-your-cloud-hostname:port/fndAppCoreServices/ServiceCatalogService?wsdl`

Obtain the Service Catalog Service WSDL For Release 12

To obtain the physical endpoint of your instance, perform the following steps:

1. Log in to the Fusion Applications home page. For example:

`https://acme.fs.us2.oraclecloud.com/homePage/faces/FuseWelcome`

Where `acme` is the system name and `fs` is a Fusion Applications domain.

2. Copy `https://acme.fs.us2.oraclecloud.com/` and append `fndAppCoreServices/ServiceCatalogService?WSDL`. For example:

`https://acme.fs.us2.oraclecloud.com/fndAppCoreServices/ServiceCatalogService?WSDL`

Obtain the Interface Catalog URL

The interface catalog URL takes the following format:

`https://fusxxxx-fs-ext.us.oracle.com/helpPortalApi/otherResources/latest/interfaceCatalogs`

For Fusion Applications Releases 13 and Later

Obtain the Oracle Fusion Applications Release 13 and later service catalog service WSDLs and interface catalog URLs through the following methods.

- [Obtain the Service Catalog Service WSDL](#)
- [Obtain the Interface Catalog URL](#)

Obtain the Service Catalog Service WSDL

To obtain the physical endpoint of your instance, perform the following steps:

1. Log in to the Fusion Applications home page. For example:

`https://acme.fa.us6.oraclecloud.com/fscmUI/faces/FuseWelcome`

Where `acme` is the system name and `us6` is the data center.

2. Copy `https://acme.fa.us6.oraclecloud.com/` and append it with `fscmService/ServiceCatalogService?WSDL`. For example:

`https://acme.fs.us2.oraclecloud.com/fscmService/ServiceCatalogService?WSDL`

Obtain the Interface Catalog URL

The interface catalog URL takes the following format:

`https://fusxxxx-fa-ext.us.oracle.com/fscmRestApi/otherResources/latest/interfaceCatalogs`

Create a Connection

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

To create a connection in Oracle Integration:

1. In the left navigation pane, click **Home > Integrations > Connections**.
2. Click **Create**.

Note:

You can also create a connection in the integration canvas of:

- An orchestrated integration (See Define Inbound Triggers and Outbound Invokes.)
- A basic routing integration (See Add a Trigger (Source) Connection.)

3. In the Create Connection — Select Adapter dialog, 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 and click



Search.

4. In the Create Connection dialog, enter the information that describes this connection.
 - a. Enter a meaningful name to help others find your connection when they begin to create their own integrations. The name you enter is automatically added in capital letters to the **Identifier** field. If you modify the identifier name, don't include blank spaces (for example, SALES OPPORTUNITY).
 - b. Enter optional keywords (tags). You can search on the connection keywords on the Connections page.
 - c. Select the role (direction) in which to use this connection (trigger, invoke, or both). Only the roles supported by the adapter are displayed for selection. 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. For example, let's say 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.
 - d. Enter an optional description of the connection.
5. Click **Create**.

Your connection is created. You're now ready to configure the connection details, such as connection properties, security policies, connection login credentials, and (for certain connections) agent group.

Configure Connection Properties

Enter connection information so your application can process requests.

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

The fields that are displayed are based on your version of Oracle Integration.

2. For new connections created with the initial release of the simplified connections page on 2/18/20, the **HCM Cloud Host** field is displayed. Enter the Oracle HCM Cloud host name. For example:

`https://customer_chosen_domain_name.fa.DC.oraclecloud.com`

Note:

The Oracle HCM Cloud host name can easily be derived from the Oracle HCM Cloud login URL. For example: `https://customer_chosen_domain_name.fa.DC.oraclecloud.com/fscmUI/faces/FuseWelcome`

3. For existing connections created prior to the initial release of the simplified connections page on 2/18/20, the **HCM Services Catalog WSDL URL** and **Interface Catalog URL** fields are displayed. Specify the URLs to use in this integration.
 - a. In the **HCM Services Catalog WSDL URL** field, specify the URL to use in this integration.

b. In the **Interface Catalog URL** field, optionally specify the URL to consume Oracle HCM Cloud REST API business resources.

If the interface catalog URL is not specified, the **Subscribe to Updates (via ATOM Feed)** option does not appear for selection on the Actions page of the Adapter Endpoint Configuration Wizard.

Configure Connection Security

Configure security for your Oracle HCM Cloud Adapter connection by selecting the security policy and security token.

1. Go to the **Security** section.
2. Select the security policy to use. Based on your selection, the page is refreshed to display various login credential fields.

Element	Description
Username Password Token With PGP Key Support	<p>Specify the following details to upload an encrypted file to Oracle WebCenter Content (Universal Content Management (UCM)). The supported algorithm for the public key is RSA for encryption and key size should be 1024 bits long.</p> <ul style="list-style-type: none">• Username: Enter the username.• Password: Enter the password.• Client PGP Private Key: Click  , then browse for and upload the private key to decipher encrypted content. The supported algorithm for the private key is RSA for decryption and the key size must be 1024 bits in size.• Client PGP Passphrase: Enter the passphrase registered with the PGP private key.• PGP Public Key for UCM Upload: Click  , then browse for and upload the public key to encrypt the file. The PGP public key must already be created. See Upload Files to Oracle WebCenter Content.
Username Password Token	<p>You receive the username and password to enter when subscribing to Oracle HCM Cloud.</p> <ul style="list-style-type: none">• Username: Enter the username.• Password: Enter the password.

Element	Description
OAuth Authorization Code Credentials	<ul style="list-style-type: none"> Client ID: Enter the client identifier (ID) issued during OAuth client application creation. The client ID identifies the client (the software requesting an access token) making the request. See Set Up the OAuth Authorization Code Credentials Security Policy with Oracle Identity Cloud Service. Client Secret: Enter the client secret issued during OAuth client application creation. See Set Up the OAuth Authorization Code Credentials Security Policy with Oracle Identity Cloud Service. Authorization Code URI: Enter the URI from which to request the authorization code. This endpoint is used to initiate the OAuth authentication and authorization process during which a user is directed to the OAuth server to provide credentials, to review granted permissions, and to provide consent. <p><code>https://IDCS_URL/oauth2/v1/authorize</code></p> <ul style="list-style-type: none"> Access Token URI: Enter the URI to use for the access token. A request must be sent to this URI to obtain an access token. <p><code>https://IDCS_URL/oauth2/v1/token</code></p> <ul style="list-style-type: none"> Scope: Enter the scopes specified during OAuth client application creation: <ul style="list-style-type: none"> The URL that corresponds to the federated Oracle Fusion Application instance. <code>offline_access</code> <p><code>https://FA_URL:443/offline_access</code></p> <p>Scopes enable you to specify the type of access you need. Scopes limit access for the OAuth token. They do not grant any additional permission beyond that which the user already possesses. See Set Up the OAuth Authorization Code Credentials Security Policy with Oracle Identity Cloud Service.</p> <ul style="list-style-type: none"> Client Authentication: You can optionally configure OAuth flows with client authentication. This is similar to the Postman user interface feature for configuring client authentication. <ul style="list-style-type: none"> Send client credentials as basic auth header: Pass the client ID and client secret in the header as basic authentication.

Element	Description
	<ul style="list-style-type: none"> Send client credentials in body: Pass the client ID and client secret in the body as form fields. <p>When configuration is complete, perform the following steps:</p> <ol style="list-style-type: none"> Click Provide Consent to test the OAuth flow. If the Oracle Identity Cloud Service Oracle Integration and Oracle Fusion Applications users are different, log in to the respective instance when prompted. Note: You are not prompted to log in if these users are the same. Return to the Connections page and click Test. <p>Note: If you receive an Unauthorized 401 error when testing your connection with a nonfederated user account, you may be logged in with the wrong user account. See Avoid Potential Errors When Testing Your Connection with a Nonfederated User Account.</p>

Test the Connection

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

- In the page title bar, click **Test**. What happens next depends on whether your connection uses a Web Services Description Language (WSDL) file.

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

- 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, verify URLs and credentials, and download the diagnostic logs for additional details. Continue to test until the connection is successful.
- When complete, click **Save**.

Upload an SSL Certificate

Certificates are used to validate outbound SSL connections. If you make an SSL connection in which the root certificate does not exist in Oracle Integration, an exception 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.

To upload an SSL certificate:

1. In the left navigation pane, click **Home > Settings > Certificates**.

All certificates currently uploaded to the trust store are displayed in the Certificates dialog. The



link enables you to filter by name, certificate expiration date, status, type, category, and installation method (user-installed or system-installed). Certificates installed by the system cannot be deleted.

Name	Type	Category	Status
mykey3 EXPIRES IN 1 MONTHS	X.509	Identity	Configured
mykey2 EXPIRED	X.509	Identity	Configured
recert1586867745048 EXPIRES IN 4 YEARS	X.509	Trust	Configured
recert1586863610817 EXPIRES IN 4 YEARS	X.509	Trust	Configured
recert1586857607511 EXPIRES IN 4 YEARS	X.509	Trust	Configured
recert1586857416600 EXPIRES IN 4 YEARS	X.509	Trust	Configured

2. Click **Upload** at the top of the page.
The Upload Certificate dialog box is displayed.
3. Enter an alias name and optional description.
4. In the **Type** field, select the certificate type. Each certificate type enables Oracle Integration to connect with external services.
 - **X.509 (SSL transport)**
 - **SAML (Authentication & Authorization)**
 - **PGP (Encryption & Decryption)**

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.
- c. Click **Upload**.

Refresh Integration Metadata

You can manually refresh the currently-cached metadata available to adapters that have implemented metadata caching. Metadata changes typically relate to customizations of integrations, such as adding custom objects and attributes to integrations. There may also be cases in which integrations have been patched, which results in additional custom objects and attributes being added. This option is similar to clearing the cache in your browser. Without a manual refresh, a staleness check is only performed when you drag a connection into an

integration. This is typically sufficient, but in some cases you may know that a refresh is required. For these cases, the **Refresh Metadata** menu option is provided.

To refresh integration metadata:

 **Note:**

The **Refresh Metadata** menu option is only available with adapters that have implemented metadata caching.

1. In the left navigation pane, click **Home > Integrations > Connections**.
2. Go to the row of the connection to refresh.
3. Select **Refresh Metadata** from the  menu.

A message is displayed indicating that the refresh was successful.

Metadata refresh for connection "connection_type" has been initiated successfully.

Add the Oracle HCM Cloud Adapter Connection to an Integration

When you drag the Oracle HCM Cloud 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 HCM Cloud Adapter endpoint properties.

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

Topics:

- [Basic Info Page](#)
- [Trigger Request Page](#)
- [Trigger Response Page](#)
- [Invoke Action Page](#)
- [Invoke Operation Page](#)
- [Invoke Child Resources Page](#)
- [Invoke Descriptive and Extensible 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

Enter the Oracle HCM Cloud trigger request values for your integration. The values you specify start the integration.

Element	Description
Select a Business Object	Select the business object from the Oracle HCM Cloud application to receive as a request that starts the integration.
Filter by object name	Type the initial letters of the name to filter the display of business objects.

Trigger Response Page

Enter the Oracle HCM Cloud trigger response values for your integration.

- Immediate (synchronous) response: A response business object is immediately returned as output. You select **Immediate** as the response type on the Response page and select the business object as part of the response to the client.
- Delayed (asynchronous) response: A callback service to which to route the callback is exposed. You select **Delayed** as the response type on the Response page and select the operation and business object that comprise a successful callback response, a failed callback response, or both.
- No response is required: You select **None** on the Response page because a response is not required.

The Response page looks as follows:

The screenshot shows the Oracle HCM Cloud Response page. The sidebar on the left has tabs for 'Basic Info', 'Request', and 'Response', with 'Response' being the active tab. The main content area has a 'Response Type' section with three radio buttons: 'Immediate' (selected), 'Delayed', and 'None'. Below this is a 'Select a Business Object' section. It includes a 'Filter by object name' input field and a dropdown menu showing a list of objects. The 'Account' object is currently selected in the dropdown.

The following table describes the fields available if an immediate (synchronous) response is required.

Table 3-1 Response Type — Immediate (Synchronous) Response is Required

Element	Description
Response Type	Select Immediate for the Oracle HCM Cloud application to wait until a response is received from the integration. This is also known as the request and response message exchange pattern. This is the default selection.
Filter by object name	Type the initial letters to filter the display of business objects.
Select a Business Object	Select the business object to receive from the Oracle HCM Cloud application as a response. A description of the selected business object is displayed below this list.
Name	Displays the name of the selected business object.
Description	Displays the description of the selected business object.

The following table describes the fields available if a delayed (asynchronous) callback response is required. You can configure a successful callback response, a failed callback response, or both.

Table 3-2 Response Type — Delayed (Asynchronous) Response is Required

Element	Description
Response Type	Select Delayed to configure a successful callback response, a failed callback response, or both. This enables you to configure the operation and business objects that you want the Oracle HCM Cloud application to process as part of a successful callback response, failed callback response, or both.
Successful Response/Failed Response	Select the type of callback to configure. After configuring one type of callback (for example, successful), you can configure the other type (for example, failed). <ul style="list-style-type: none"> Successful Response: Select to configure the operation and business objects that you want the Oracle HCM Cloud application to process as part of a successful callback response sent by the integration. Failed Response: Select to configure the operation and business objects that you want the Oracle HCM Cloud application to process as part of a failed callback response sent by the integration.
Select the operation to perform on the business object	Select the operation to perform on the business object.
Life Cycle	Displays the current state of the selected business document. Active indicates the business document is available for use. Deprecated indicates the business document is nearing the end of use and must be used with caution.

Table 3-2 (Cont.) Response Type — Delayed (Asynchronous) Response is Required

Element	Description
Name	Displays the name of the selected business object.
Description	Displays the description of the selected business object.

The following table describes the fields available if no response is required.

Table 3-3 None — No Response is Required

Element	Description
Response Type	Select None .
Select a Business Object	If you select None , this section is hidden.

Invoke Action Page

Select the Oracle HCM Cloud invoke action for your integration.

Element	Description
What Would You Like to do with Oracle HCM Cloud Adapter	<ul style="list-style-type: none"> Query, Create, Update, or Delete Information: Select to query business objects such as employee records or perform operations for employee onboarding, data synchronization, and so on. Subscribe to Updates (via Atom Feed): Select to receive the latest Atom feed updates since a specific date for new hires, new jobs, and so on. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Note:</p> <p>The Subscribe to Updates (via Atom Feed) option is currently supported for Releases 11 and higher of Oracle HCM Cloud.</p> <ul style="list-style-type: none"> Extract Bulk Data using HCM Extracts: Select to receive several records as a data file on payroll records, time sheets, and others. Send Files to HCM Cloud: Select to upload files to Oracle WebCenter Content (Universal Content Manager) in encrypted or unencrypted format. Import Bulk Data using HCM Data Loader (HDL): Select to import bulk data using the HCM Data Loader. </div>

Invoke Operation Page

Enter the Oracle HCM Cloud invoke operation values for your integration.

See the appropriate section based on your selection on the Actions page:

- [Business Objects, Services, and Business \(REST\) Resources](#)
- [Atom Feeds](#)
- [Data Extracts](#)
- [File Upload to WebCenter \(UCM\)](#)
- [HCM Data Loader](#)

Business Objects, Services, and Business (REST) Resources

If you select **Query, Create, Update, or Delete Information** on the Actions page, the following fields are displayed.

Element	Description
Browse by	Select to browse by business object or service. There is a one-to-one correspondence between the business object and service. The service acts on the business document. <ul style="list-style-type: none">• Business Objects: Select to browse a list of available business objects.• Services: Select to browse a list of available services.• Business (REST) Resources: Select to browse a list of available business (REST) resources exposed by the interface catalog URL. Select the business object or service.
Select a Business Object (displayed if Business Objects is selected)	Select the business object to use.
Select a Service (displayed if Services is selected)	Select the service to use.
Select a Service Application (displayed if Business (REST) Resources is selected)	Select the business (REST) resource to use. You can then click Browse and configure a child response to select the corresponding child business resources of that parent to use. Note: Existing integrations created prior to the introduction of this feature can be edited to select parent business resources and their corresponding child business resources. See About the REST APIs in <i>REST API for Oracle Fusion Cloud HCM</i> for details about supported REST resources.

Element	Description
Browse and configure a child response	<p>Click to access a page to select the following:</p> <ul style="list-style-type: none"> • The child and subchild business resources of the selected parent business resource • The operation to perform on the child and subchild business resources <p>After you click Ok, the link name changes to View and edit the configuration of a child resource. Both the parent and child business resources are displayed on the Summary page.</p> <p>To reset to your original selections, click this link, then click Reset.</p>
Filter by type	<p>Type the initial letters to filter the display of business objects, services, or business (REST) resources.</p>
Select the Operation to Perform on the Business Object/Resource or Service	<p>Select the operation to perform on the selected business object, business (REST) resource, or service.</p> <p>Note: If you select get, only the following query parameters are supported:</p> <ul style="list-style-type: none"> • expand • fields • onlyData
Life Cycle	<p>Displays the state of the selected business object or service. Deprecated indicates the business document is nearing the end of use and must be used with caution.</p>
Name	<p>Displays the name of the selected business object or service.</p>
Description	<p>Displays the description of the selected business object or service.</p>

Atom Feeds

If you selected the **Subscribe to Updates (via ATOM Feed)** option on the Actions page, the following fields are displayed.

 **Note:**

Any new Atom feed endpoint that uses Employee-related feeds (for example, new hire, assignment, termination, and updates) with a business object now uses the Workers resource in both design time and runtime. The Workers resource is visible in the mapper.

Any existing Atom feed endpoint continues to use the Emps resource for employee-related feeds with a business object for backward compatibility and to avoid the need for remapping.

Element	Description
Select an Atom Feed	<p>Select the feed of interest to the downstream application.</p>

Element	Description
Learn more about HCM Cloud ATOM feeds	Click to access a page that describes how Atom feed subscriptions work.
Max entries to process	Select the number of feeds to process.
Process Future Dated Entries Immediately	<p>Select to process future-dated feeds immediately. If not selected, future-dated feeds are processed when the effective date is reached. The integration is responsible for handling not-yet-effective, future-dated entries.</p> <p>The elements that appear in the mapper are different based on your selection. If Process Future Dated Updates Immediately is not selected, the request mapper shows the updated-min element under ApplicationPullParameter. If Process Future Dated Updates Immediately is selected, the request mapper shows the published-min element under ApplicationPullParameter. This makes future-dated Atom entries appear in their respective Atom feed immediately once the future-dated action is taken.</p>
Include Business Object in ATOM Feeds	<p>Select this checkbox to send an HTTP request for each entry in the feed to the ATOM server to fetch the business object snapshot.</p> <ul style="list-style-type: none"> • If not selected, changed and context attributes are used during design time and runtime, the operation name in the mapper does not have the suffix WithBO, and the business object is not shown under the operation name element. • If selected, context attributes, changed attributes, and business object snapshots are used. <p>The maximum number of entries to process is set to 1000 entries and cannot be changed. This sets the value of the query parameter page-size that is sent as part of the request to the Atom server to get the feed. ATOM server returns a maximum of 1000 entries as part of the feed.</p>

Data Extracts

If you selected the **Extract Bulk Data using HCM Extracts** option on the Actions page, the following questions are displayed to complete the configuration.

Element	Description
What is the Integration Name for HCM Extracts	Specify the name. The HCM extract with a matching integration name is downloaded to Oracle Integration.
Specify release date-time of extract	Specify the time of the extract. The extracts released after the specified date-time are eligible for download. A sample specified date-time value is 6/22/17 5:04 AM.

Element	Description
Select actions that need to perform on extract in following list	<p>Select the actions to perform on the extract:</p> <ul style="list-style-type: none"> • Decrypt the extract: Extract is decrypted if it is in encrypted form and PGP information is present in the connection configuration. • Unzip the extract: Extract is unzipped if it is in a zipped format. <p>The selected actions are performed on the extract after download to Oracle Integration.</p>

File Upload to WebCenter (UCM)

If you selected **Send Files to HCM Cloud** on the Actions page, select the security group and doc account required for uploading the file.

Element	Description
Security Group	Select the security group in which to upload the file. A security group is a set of files grouped under a unique name. Every file in the content server repository belongs to a security group. Access to security groups is controlled by permissions assigned to roles on the content server. Roles are assigned to users where they are maintained in Oracle Fusion Applications. The default security group in Fusion Applications is FAFusionImportExport.
Doc Account	Select the doc account to assign to the file. In Fusion Applications, every content item has an account assigned to it. You must have the appropriate permission to the account such as read and/or write. The access to the document is the intersection between account permissions and security group permissions. There are several Fusion Applications accounts.
Encrypt the File	<p>Select this checkbox to encrypt the file before upload to UCM. To select this checkbox, you must have selected to encrypt the file when configuring the Oracle HCM Cloud Adapter connection on the Connections page. See Configure Connection Security.</p> <p>Note: The Oracle HCM Cloud Adapter does not support file encryption during an HDL import operation. The HCM Data Loader (HDL) File Encryption option only denotes whether or not the file being uploaded through the HDL operation is PGP-encrypted. If there is a requirement to upload an encrypted file, the encryption must be done using the stage file action Encrypt file operation before the HCM HDL endpoint is called. See Configure a Stage File Action in Using Integrations in Oracle Integration Generation 2.</p>

HCM Data Loader

If you selected **Import Bulk Data using HCM Data Loader (HDL)** on the Actions page, select the operation to perform against the target HCM Data Loader application.

Element	Description
Submit an HCM Data Loader Job	<p>Select to trigger the upload of the data (.dat) file from Oracle Integration into Oracle WebCenter Content. The Oracle HCM Cloud Adapter uploads the ZIP file containing the .dat file to Oracle WebCenter Content and invokes the HCM Data Loader importAndLoad operation, which returns an HCM Data Loader process ID. The .dat file must be HDL-compliant.</p> <p>If you select this operation, the page refreshes to display the following fields:</p> <ul style="list-style-type: none"> • Security Group: Select the security group. • Doc Account: Select the documentation account. • HCM Data Loader (HDL) File Encryption: Select None or PGP Unsigned, which provides Pretty Good Privacy (PGP) unsigned encryption of the .dat file.
Query the Status of an HCM Data Loader Job	Select to retrieve the status of an HCM Data Loader job submitted by this integration. The Oracle HCM Cloud Adapter invokes the HCM Data Loader getDataSetStatus operation to get the status of the HCM Data Loader process.

A use case that describes importing bulk data using the HCM Data Loader (HDL) is provided. See [Import Business Objects with the HCM Data Loader \(HDL\)](#).

Invoke Child Resources Page

Select the child resources to include with the parent resource selected on the Operations page. This helps to minimize the size of the integration WSDL file. If you do not select any child resources, all child resources (including custom resources) associated with the parent resource are included by default in the integration WSDL file. This increases the size of the WSDL file and can cause memory issues in Oracle Integration. This page is only displayed if you select a top-level parent resource on the Operations page.

Select a maximum of ten child resources to include in either the request payload sent to the external API or the response message received from the external API. Do not select child resources that are not required for use by this integration.

Element	Description
Select Child Resources	Select the child resources to use. Only the child resources associated with the parent resource you selected on the Operations page are displayed for selection.
Your Selected Child Resources	Displays the selected child resources.

Invoke Descriptive and Extensible Page

Select the descriptive flexfield (DFF) or extensible flexfield (EFF) and associated contexts. A flexfield is a flexible data field that your organization can customize to meet your business needs without programming. It provides a set of placeholder fields (segments) associated with a business object.

Two types of flexfields are supported for selection:

- Descriptive flexfield: A field you customize to enter additional information for which your Oracle Fusion Applications product has not already provided a field.
- Extensible flexfield: Similar to a descriptive flexfield in that it provides a customizable expansion space that implementers (such as Oracle Fusion Applications users) can use to configure additional attributes (segments) without additional programming.

Element	Description
Select Flexfields(s)	Select a flexfield to see the configured contexts.
Select Context(s)	Select a maximum of 20 contexts to include in either the request payload sent to the external API or the response message received from the external API.
Number of Contexts Selected	Displays the number of selected contexts.

Summary Page

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

Element	Description
Summary	Displays a summary of the configuration values you defined on previous pages of the wizard. 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. To return to a previous page to update any values, click the appropriate tab in the left panel or click Back . To cancel your configuration details, click Cancel .

Implement Common Patterns Using the Oracle HCM Cloud Adapter

You can use the Oracle HCM Cloud Adapter to implement the following common patterns.

Topics:

- [Upload a File to Oracle WebCenter Content](#)
- [Subscribe to Atom Feeds in a Scheduled Integration](#)
- [Configure the Extract Bulk Data Option in an Integration](#)
- [Invoke an Endpoint Dynamically](#)
- [Import Business Objects with the HCM Data Loader \(HDL\)](#)
- [Select Extensible and Descriptive Flexfields in an Integration](#)

 **Note:**

Oracle Integration offers a number of prebuilt integrations, known as *recipes*, that provide you with a head start in building your integrations. You can start with a recipe, and then customize it to fit your needs and requirements. Depending upon the solution provided, a variety of adapters are configured in the prebuilt integrations. See the Recipes and Accelerators page on the Oracle Help Center.

Upload a File to Oracle WebCenter Content

You can upload a file to Oracle WebCenter Content (Universal Content Manager) with the Oracle HCM Cloud Adapter. The file to upload can be either encrypted or unencrypted. This section provides a high-level overview for performing this scenario.

To upload a file to Oracle WebCenter Content:

1. Create an Oracle HCM Cloud Adapter connection with the **Invoke** role. During connection configuration, you can select to optionally encrypt the file to upload by selecting the **PGP Public Key for UCM Upload** checkbox.

Credentials

You can configure the Security Policy for this connection. Please select the Security Policy.

Security Policy

Your application/endpoint requires that users and services provide security credentials for access. Specify the login credentials below.

Property Name	Upload File	Property Value
* User name		jsmith
* Password		*****
* Confirm Password		*****
Client PGP Private Key	<input type="checkbox"/>	Private Key required to decipher encrypted content
Client PGP Passphrase		Passphrase registered with PGP Private Key
Confirm Client PGP Passphrase		Passphrase registered with PGP Private Key
PGP Public Key for UCM Upload	<input checked="" type="checkbox"/>	<input type="button" value="Upload"/> Public Key required for UCM Upload to encrypt file

2. Create an orchestrated integration.
3. Drag the Oracle HCM Cloud Adapter to the invoke part of the integration canvas. This invokes the Adapter Endpoint Configuration Wizard.
4. On the Actions page, select **File Upload to WebCenter (UCM)**.

What would you like to do with HCM Cloud?

Query, Create, Update or Delete Information
Query business objects such as employee records etc or perform operations for employee onboarding, data sync etc.

Extract Bulk Data using HCM Extracts
Receive several records as data file on payroll records, timesheet etc

Subscribe to Updates (via ATOM Feed)
Receive latest updates since a specific date on new hires, jobs etc.

File Upload to WebCenter (UCM)
The service is a controlled check-in to Content Server.

5. On the Operations page, select the following mandatory values:
 - **Security Group:** Select the security group to which the file to upload belongs. A security group is a set of files grouped under a unique name. Every file in the UCM server repository belongs to a security group. Access to security groups is controlled by permissions assigned to roles on the content server. Roles are assigned to users where they are maintained on Oracle Fusion Applications. The default security group in Fusion Applications **FAFusionImportExport**.

- **Doc Account:** Select the doc account for the file to upload. In Fusion Applications, every content item has an account assigned to it. You must have the appropriate permission to the account such as read and/or write. Access to the document is the intersection between account permissions and security group permissions.

This service retrieves a copy of a content item without performing a check out.

File Upload to WebCenter (UCM)

File Upload Parameters

* Security Group

FAFusionImportExport
IPMSYS_APP_1
IPMSYS_APP_2
PersonalSpaces
Public

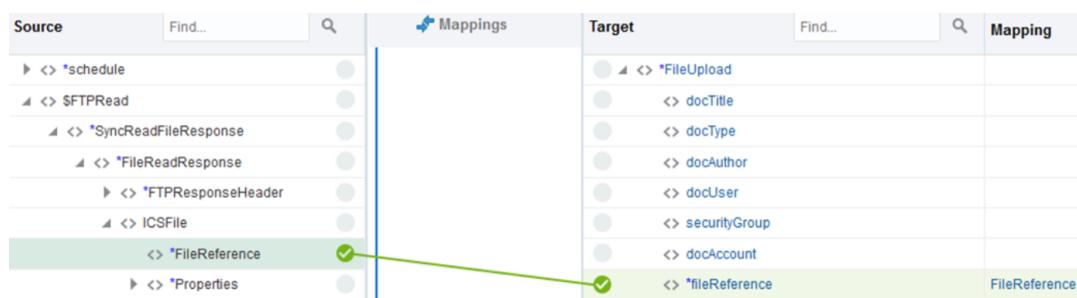
* Doc Account

#none
AUTHEN
PEWebCenter/PU
PUBLIC
UCM_Spaces/PU

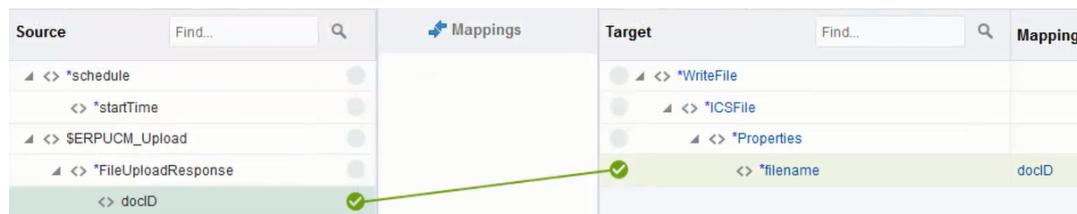
File Options

Encrypt the File

6. If you selected to encrypt the file to upload on the Connections page in Step 1, select **Encrypt the File**.
7. Once the UCM file upload endpoint is saved, provide the reference to the file to upload to UCM.



You can also override the security group and doc account that you previously set by hard coding new values in the mapper that receive reference during runtime.



If file upload is successful, a document ID is returned. Use the document ID for downstream processing.

8. Complete design of the integration.

Subscribe to Atom Feeds in a Scheduled Integration

This use case provides an overview of creating a scheduled orchestrated integration using the Oracle HCM Cloud Adapter to subscribe to Atom feeds. Atom feeds enable you to track changes made to feed-enabled resources in Oracle Global Human Resources Cloud. For any updates of interest to downstream applications such as new hires, terminations, employee transfers, and promotions, Oracle Global Human Resources Cloud publishes Atom feeds.

For this use case, the Oracle HCM Cloud Adapter is configured with the Atom feed **Employee Update**. This feed consists of three updates (**PrimaryPhoneNumber**, **CitizenshipStatus**, and **CitizenshipId**). An FTP Adapter is also configured to write any feed updates to an FTP server.

There are two types of entries published by Oracle Global Human Resources Cloud in any feed:

- Entries that are already effective.
- Entries that are effective in the future (known as future dated entries).

Design the integration based on these requirements. If the integration must process future dated entries, there are the following options:

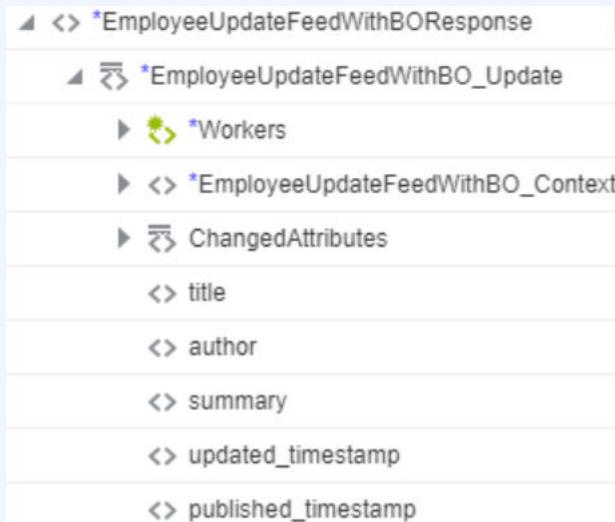
- Future dated entries are processed on their effective dates.
- Future dated entries are processed immediately.

Note:

Any new Atom feed endpoint that uses Employee-related feeds (for example, new hire, assignment, termination, and updates) with a business object now uses the Workers resource in both design time and runtime. The Workers resource is visible in the mapper.

Any existing Atom feed endpoint continues to use the Emps resource for employee-related feeds when it is already deployed with a business object for backward compatibility and to avoid the need for remapping. All new deployments with the Atom feed must use the Workers business object.

The following example shows the Employee update feed with a business object in the mapper:



Process Future Dated Entries on Their Effective Dates

Oracle Global Human Resources Cloud processes future dated entries on their effective dates. This use case provides an overview of how to design this type of integration.

1. On the Connections page, create and configure an Oracle HCM Cloud Adapter with the following details:
 - a. Specify a name.
 - b. In the Configure Connectivity dialog, specify *both* a service catalog WSDL URL and an interface catalog URL. If the interface catalog URL is not specified, the **Subscribe to Updates (via Atom Feed)** option is not displayed on the Actions page of the Adapter Endpoint Configuration Wizard.
 - c. In the Credentials dialog, select the **Username Password Token** security policy and specify the login credentials.
2. On the Integrations page, create a scheduled orchestrated integration.
3. Drag the Oracle HCM Cloud Adapter into the integration canvas as an invoke connection and configure the Adapter Endpoint Configuration Wizard with the following details:
 - a. On the Basic Info page, specify a name (for this example, `getData`).

- b. On the Actions page, select **Subscribe to Updates (via Atom Feed)**.
- c. On the Operations page, select the following:
 - From the **Atom feed** list, select **Employee Update**.
 - Select the **Include Business Object in Atom Feeds** checkbox to send an HTTP request for each entry in the feed to the Atom server to fetch the latest snapshot of the business resource. The checkbox behavior is as follows:
 - Not selected: Context and changed attributes are used during design time and runtime. The operation name in the mapper does not have the suffix **WithBO** and the business object is not shown under the operation name element.
 - Selected: Both context attributes and business object attributes are used during design time and runtime. The operation name in the mapper has the suffix **WithBO**.
 - Select the maximum number of entries to process from the **Max entries to process** list.
This sets the value of the **page-size** query parameter that is sent as part of the request to the Atom server to get the feed. The Atom feed size is limited by this number. The recommendation is to use a small number for this option and have the integration execute more frequently.

4. Double-click the schedule icon, and select **Edit** to create a schedule parameter (for this example, named **ts**). The initial value must be a timestamp to which to start. Entries are received during runtime from this timestamp onwards. The timestamp must be of following format:

YYYY-MM-DDTHH:MM:SS:sssZ e.g. 2018-06-03T02:34:06.000Z

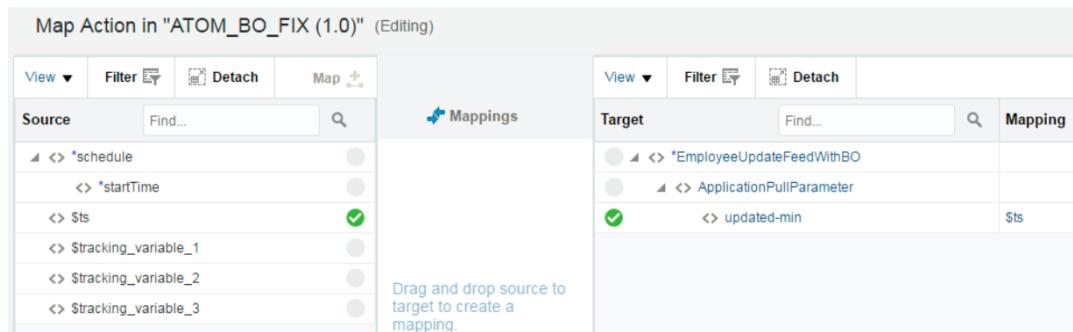
where:

- **YYYY:** Four-digit year
- **MM:** Two-digit month (01=January, and so on)
- **DD:** Two-digit day of the month (01 through 31)
- **hh:** Two digits of the hour (00 through 23) (am/pm NOT allowed)
- **mm:** Two digits of the minute (00 through 59)
- **ss:** Two digits of the second (00 through 59)
- **s:** Three digits representing a decimal fraction of a second (that is, milliseconds)

This parameter ensures that new entries are processed every time the integration is invoked. The timestamp of the last processed entry must be stored in this parameter. This value is available across invocations of the integration. For the first request, the **updated-min** query parameter value is blank, which returns the latest *n* number of entries in the feed, where *n* is the value selected for the **Max entries to process** option on the Operations page.

Parameter Name	Description	Value
ts	Type a description	2018-06-03T02:34:06.000Z

- In the request mapper between the schedule and the Oracle HCM Cloud Adapter, map **\$ts** (timestamp value) to **updated-min**. The Oracle HCM Cloud Adapter sends the **updated-min** query parameter to the Atom server when requesting a feed. The Atom server returns a feed with updated entries occurring after newer updates to the timestamp value. This enables new updates to be processed every time and prevents the same update from being processed multiple times.



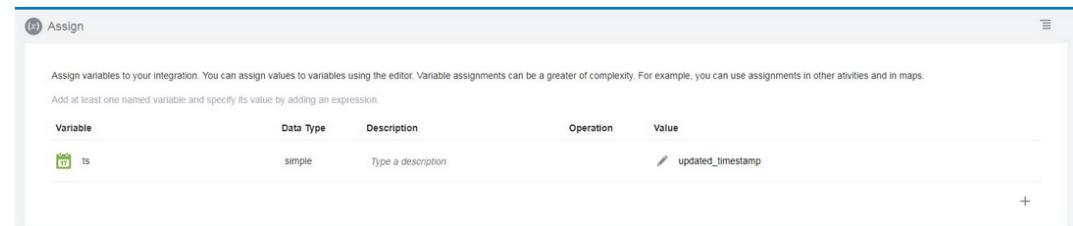
- Add and configure a **For Each** action below the Oracle HCM Cloud Adapter in the integration canvas.

Because the **Include Business Object in Atom Feeds** option was selected on the Operations Page, the mapper shows the business object (**Workers**), the context (**EmployeeUpdateFeedWithBO_Context**), the changed attributes (**ChangedAttributes**), and the timestamp. The timestamp is the updated element from the feed's entry. This is used to track processed entries. This is done with the help of the schedule parameter. The first **For Each** action iterates through the entries.

- Add and configure a second **For Each** action inside the first **For Each** action to iterate through the changed attributes.
- Add and configure an FTP Adapter inside the second **For Each** action in the integration.

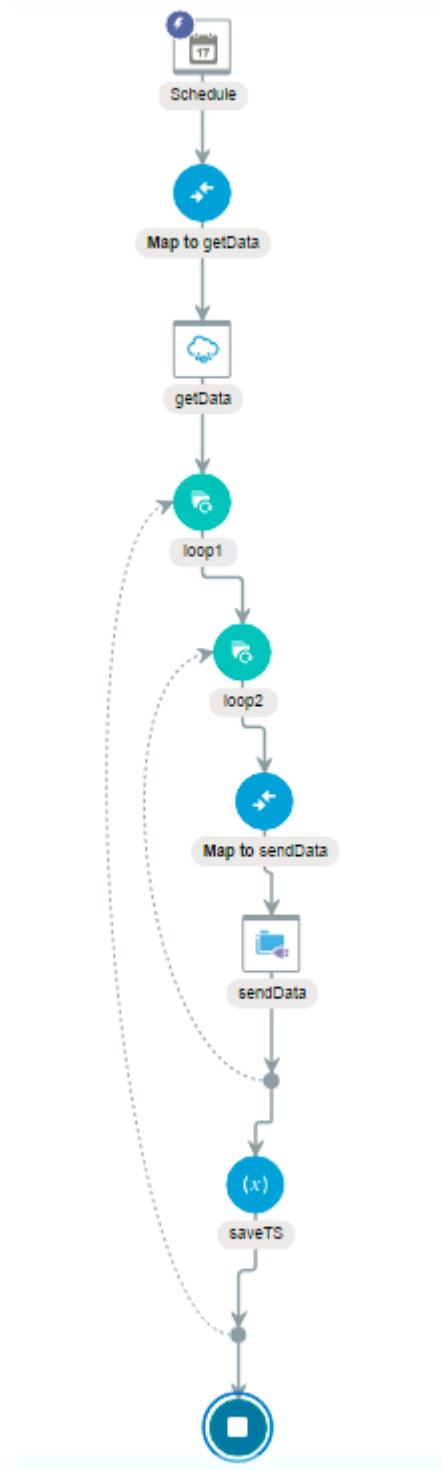
For each changed attribute, a file is written to the FTP server. You can also use a REST Adapter connection to send multiple patch requests to an endpoint with these changes. At the end of the first loop (for this example, named **loop1**), the **ts** schedule parameter is updated with the timestamp of the entry. This is stored in the database and available for subsequent invokes. This value is persisted across subsequent integration runs and also across deactivations and activations. This is how the processed entries are tracked. Because the **ts** schedule parameter is used in the request mapping, in subsequent invokes it uses its value from the database. Therefore, only new entries are processed.

- Add an **Assign** action at the bottom of the first **For Each** action (**loop1**). The assign activity is placed at the end of **loop1** for fault tolerance. If a fault occurs when writing to the FTP location, the updated timestamp of the last processed entry is used for the next invoke.



The **updated_timestamp** element is selected from the update element (entry in the feed) as the value for schedule parameter **ts** as follows.

When the integration is invoked by the schedule, a file is created in the FTP directory for each of the changed attributes. The complete design of the integration is as follows:

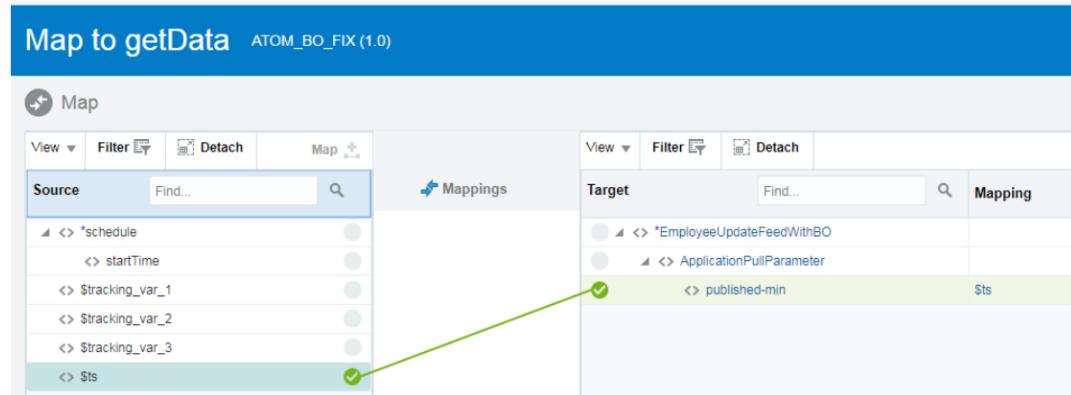


Process Future Dated Entries Immediately

Oracle Global Human Resources Cloud processes future dated entries immediately, as soon as they are published. This use case provides an overview of the differences between

designing an integration to process future dated entries on their effective dates and designing an integration to process future dated entries immediately.

- On the Operations page, select **Process Future Dated Entries Immediately**. Enabling this checkbox changes the request map to have a different query parameter, **published-min**.
- In the request mapper between the schedule and the Oracle HCM Cloud Adapter, map **\$ts** (timestamp value) to **published-min**.



- To make future dated entries available immediately in the feed, you must send **published_timestamp** as **published-min** in the request. **published_timestamp** must also be persisted in the **ts** scheduled parameter to process new entries in subsequent invokes of the flow. **ts** must store the **published_timestamp**.

Summary

In summary, the following changes are required in the integration for handling future dated entries.

Future Dated Entries Options	Request Parameters	Timestamp Stored in Schedule Parameter
Processed immediately	published-min	published_timestamp
Processed on their effective dates	updated-min	updated_timestamp

Configure the Extract Bulk Data Option in an Integration

You can use the extract bulk data option in an orchestrated integration. This section provides a high-level design of an integration using this feature.

Note:

You must schedule and create the HCM data extract in Oracle HCM Cloud. It must be configured with a delivery option of type **WebCenter Content**. When configuring this delivery option, the **Integration Name** field must be populated with a unique value that is later specified in the **What is the Integration Name for HCM Extracts** field of the Operations page when configuring the Oracle HCM Cloud Adapter.

To configure an extract bulk data integration:

1. Create a scheduled, orchestrated integration pattern.
2. Add a schedule parameter to store the processed Document ID and initialize it with a value of 0. An HCM extract is associated with a Document ID. Once the extract is processed by the integration, the ID is stored in the schedule parameter. This value is required as input by the data extract operation in the Oracle HCM Cloud Adapter.
3. Drag the Oracle HCM Cloud Adapter to the invoke section of the integration canvas and configure the extract bulk data operation.
4. Configure the mapper for the data extract operation and map the **schedule** parameter with the **lastProcessedDocumentID** field.
5. Drag a **Stage File** action to the integration canvas. This invokes the Configure Stage File Action wizard.
 - a. On the Configure Operation page, select the **Read File in Segments** operation.
 - b. Map the **filename** and **directory** from the data extract response payload in the Expression Builder:
 - XPath to **filename**: \$getFile/nsmpr2:GetFileResponse/nsmpr2:HcmDataExtractResponse/nsmpr2:ICSFile/nsmpr1:Properties/nsmpr1:filename
 - XPath to **directory**: \$getFile/nsmpr2:GetFileResponse/nsmpr2:HcmDataExtractResponse/nsmpr2:ICSFile/nsmpr1:Properties/nsmpr1:directory
 - c. On the Schema Options page, select an existing schema from the file system.
 - i. On the Format Definition page, upload the extract schema. This schema should belong to the HCM extract and must be exported from Oracle HCM Cloud.
 - ii. For the **Select Repeating Batch Element** field, click the **Expression Builder** icon. The extract schema is shown in the **Source** tree.
 - iii. Identify and select the repeating element from the schema.
 - d. In the **Stage File** scope, use any appropriate adapter to process the extract.
6. Immediately after the **Stage File** scope, assign the processed Document ID in the schedule parameter. This enables you to use this value the next time the Oracle HCM Cloud Adapter is invoked.

Invoke an Endpoint Dynamically

You can dynamically invoke a REST endpoint/URL at runtime without configuring additional invoke connection or REST outbound details. As long as the Oracle HCM Cloud REST APIs return a response with HATEOS links, you can use this feature by mapping the HATEOS link to the invoke connection. This feature is useful in situations that require invoking a REST endpoint dynamically or when the endpoint is not known at design time. This feature is also useful in situations that require invoking multiple REST services, all of which accept the same input payload and return the same response payload as configured for the outbound endpoint.

For these cases, this feature eliminates the need to create multiple connections to invoke each REST endpoint.

 **Note:**

Note the following restrictions.

- The request and response schema must be the same as provided during endpoint configuration.
- Template parameters are not supported while mapping these properties.
- The HTTP verb cannot be changed for the endpoint URL. For example, if the endpoint is configured to use POST, the outgoing request uses POST even if the endpoint URI changes at runtime.
- Because the endpoint URL is determined at runtime, there is no facility to test whether the security credentials provided during connection configuration also work with the new endpoint URL. If you think the endpoint URL determined at runtime requires a different authorization header than the original URL, you may need to provide a mapping for the authorization standard header.

This use case provides a high level overview of one way to design an integration that uses dynamic endpoints. You retrieve child objects using the REST API (for example, Primary Address is a child object of the Account parent object). The integration is designed as follows.

- An initial invoke is configured to get the Account object by using the REST API. The response of this REST API does not provide the child objects. Instead, there are HATEOS links to the child objects (that is, the Primary Address object).
- A second invoke uses the HATEOS links from the earlier response to make another invoke connection to the REST endpoint to fetch the child Primary Address object using dynamic REST endpoint support.

To change the endpoint configuration at runtime, you map one or more of the various properties under the **ConnectivityProperties** target element.

1. Create an orchestrated integration.
2. Drag an adapter into the integration canvas as an trigger connection (it can be any adapter).
3. Configure the adapter in the Adapter Endpoint Configuration Wizard.
4. Drag an initial Oracle HCM Cloud Adapter into the integration canvas as an invoke connection.
5. Configure it to use the **hcmRESTApp** service application, the **Account** object (business resource), and the **get** operation.

The response of the first invoke connection contains a collection of HATEOS links, each pointing to a child object such as **Primary Address**.

6. In the mapper between the trigger adapter connection and the Oracle HCM Cloud Adapter invoke connection, map source elements to target elements. For this example, a **PartyNumber** source element is passed to an **id** target element.

Source	Mappings	Target	Mapping
↳ *process			
↳ Account			
↳ PartyId			
↳ PartyNumber	✓		
		↳ *get	
		↳ *TemplateParameters	
		✓ <> *id	PartyNumber
		↳ *QueryParameters	

7. Add a for-each action to iterate between the HATEOS links. The value in the **Repeating Element** field is from the response object.

For Each

For Each action enables iterating over a repeating element and executing one or more activities within its contained scope. Specify the repeating element by selecting from the source tree on the left and provide a name for the current element. The current element can be used for activities within the For Each scope.

Name: linkforloop
Description: Enter a brief description...
Repeating Element: \$getacc/nssrcmpr:getResponse/nssrcmpr:Accounts/nsmpr9:links
Current Element Name: linkobj

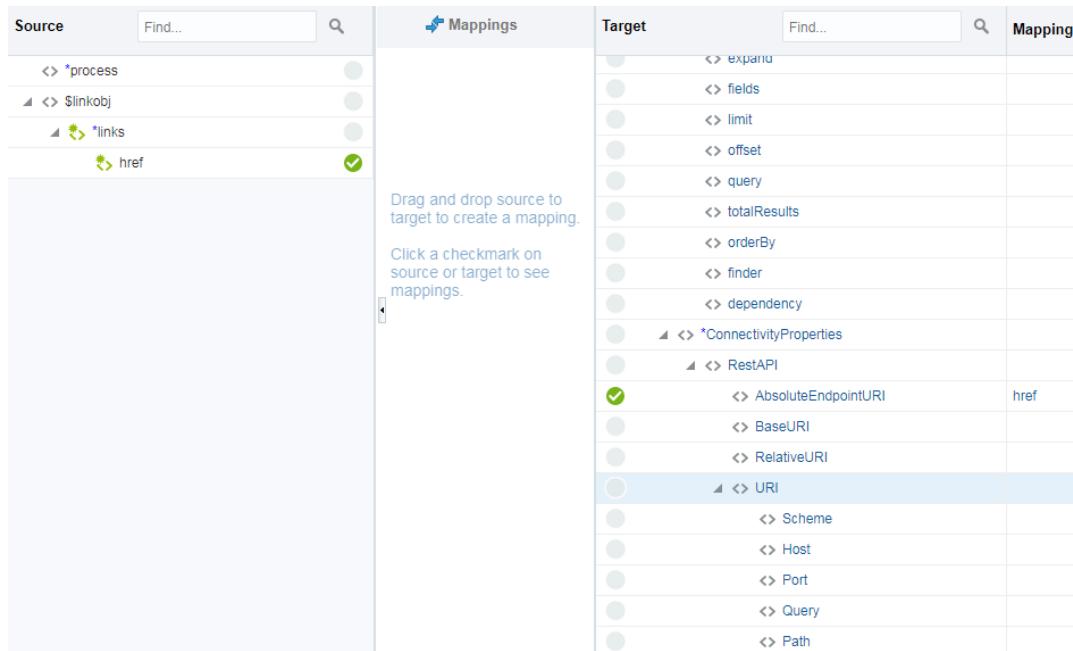
8. Add a switch action to get the HATEOS link corresponding to the **Primary Address** object.

Inputs

Expression Name
Provide a name or short description for the expression.

name = "PrimaryAddress"

9. Drag the Oracle HCM Cloud Adapter into the switch action as the second invoke connection.
10. Configure it to use the **hcmRESTApp** service application, the **Primary Address** object (business resource), and the **getAll** operation. This object uses dynamic REST endpoint support. The **Primary Address** is a collection of links. The **getAll** operation is selected for getting all the HATEOS links.
11. In the mapper immediately before the second Oracle HCM Cloud Adapter invoke connection, expand **RestApi** under **ConnectivityProperties** in the target section.
12. From the source section, map **href** to **AbsoluteEndpointURI** under **ConnectivityProperties**. The **ConnectivityProperties** schema element supports dynamic REST endpoints. The **href** element points to the **Primary Address** object link. The **href** element is invoked by the Oracle HCM Cloud Adapter.



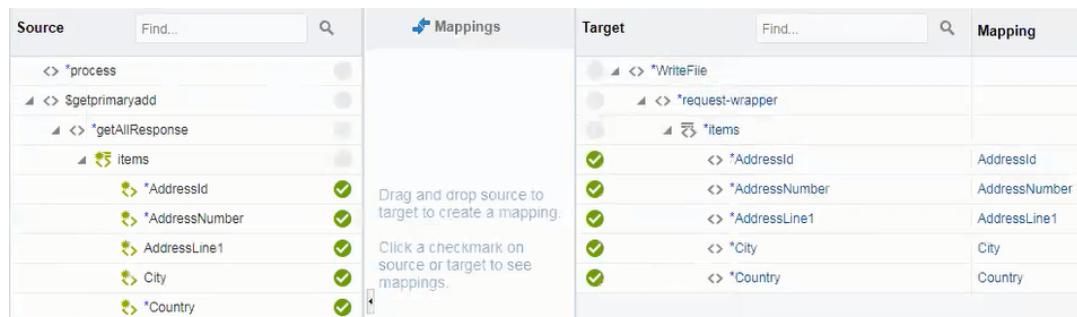
13. If necessary, map other nodes under **ConnectivityProperties**. The runtime values provided by these mappings dynamically configure the request.

You can also hover the cursor over these properties for brief descriptions.

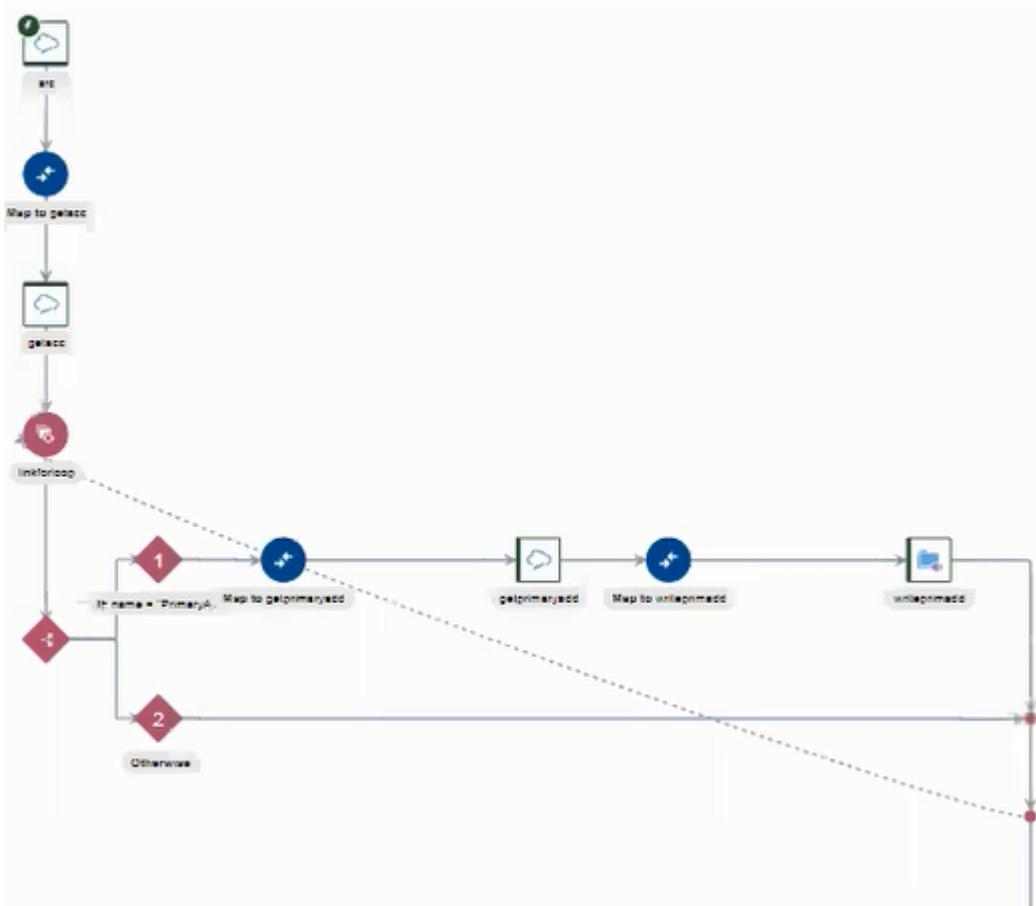
Element	Description
AbsoluteEndpointURI	Represents the absolute endpoint URL that the REST Adapter invokes. Empty values are ignored. To route the request to an endpoint URL determined at runtime, provide a mapping for this element. AbsoluteEndpointURI takes first precedence among other URL-related properties under ConnectivityProperties .
BaseUri	The equivalent of the base URL provided during connection configuration. To substitute only the base URI and retain the rest of the URL, provide a mapping for this element. The mapping is ignored if AbsoluteEndpointURI has a nonempty runtime value.
RelativeUri	Forms the part of the endpoint URI between BaseUri and ?. The mapping has no effect if BaseUri has an empty runtime value or AbsoluteEndpointURI has a nonempty runtime value. The runtime value must start with a /.
Uri	Use the various elements under this node to substitute runtime values for the specific parts of an endpoint URL.
Scheme	Provide a mapping to change only the scheme of the endpoint URL. Supported values are HTTP and HTTPS .
Host	Provide a mapping to change only the Host portion of the endpoint URL

Element	Description
Port	Provide a mapping to change only the port of the endpoint URL.
Query	Provide a mapping to change only the query portion of the endpoint URL. A query portion follows the ?.
Path	Provide a mapping to change only the path portion of the endpoint URL. A Path is the part of a URI between the hostname and ?.
Plugin	The various properties under this node impact the way the REST Adapter invokes the endpoint URL.
PostQueryString	When the runtime value is true and the HTTP verb is POST, the query string parameters are sent using POST as form parameters. The default is false .
UseFormUrlEncoding	When the runtime value is false , the REST Adapter uses RFC 3986-compliant encoding to encode the query parameters. The default is true . This is the equivalent of setting the custom header x-ics-use-x-www-form-urlencoded to false . See section “RFC 3986 Support for Encoding Query Parameters” for more information on x-ics-use-x-www-form-urlencoded . x-ics-use-x-www-form-urlencoded takes precedence when both are set.

14. Drag an FTP Adapter to the switch action for writing the **Primary Address** object response to a file on an FTP server.
15. In the mapper between the Oracle HCM Cloud Adapter and the FTP Adapter, map the **Primary Address** object details.



16. When complete, integration design looks as follows:

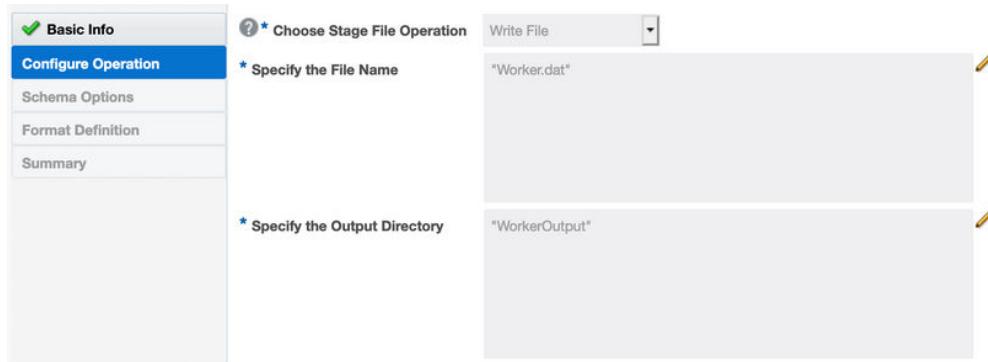


17. Activate and invoke the integration. The Oracle HCM Cloud Adapter invokes the endpoint URI determined at runtime.

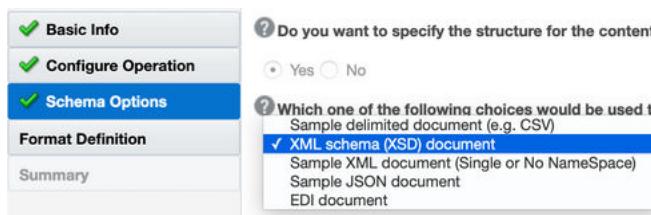
Import Business Objects with the HCM Data Loader (HDL)

You can design an integration that imports business objects using the HCM Data Loader. This use case provides a high-level overview.

1. Create an orchestrated integration to read source files staged on an FTP server that have Oracle HCM Cloud information. As an example, the source file information can consist of new hires information in a CSV file from Oracle Taleo Enterprise Edition.
2. Add a stage file action to the integration to generate the worker-delimited data file using a business object template file you obtained from Oracle HCM Cloud.
 - a. On the Configure Operation page, select the **Write File** operation, specify the file name as **Worker.dat**, and specify the output directory as **WorkerOutput**.

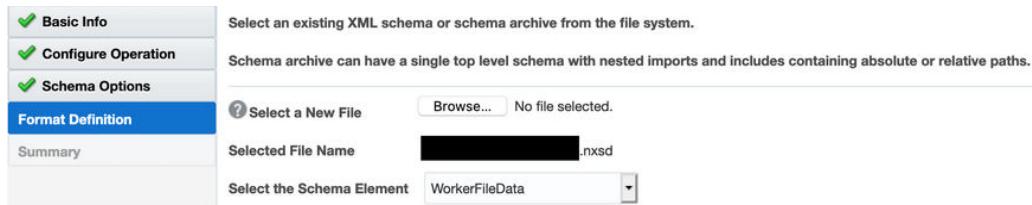


b. On the Schema Options page, select **XML schema (XSD) document**. You provide the business object template file in the next step.



c. Click **Browse** and upload the business object template file you obtain from Oracle HCM Cloud.

d. On the Format Definition page, select the **WorkerFileData** schema element. This is the main element for the delimited data file.



e. On the Summary page, click **Done** to save the stage file action.

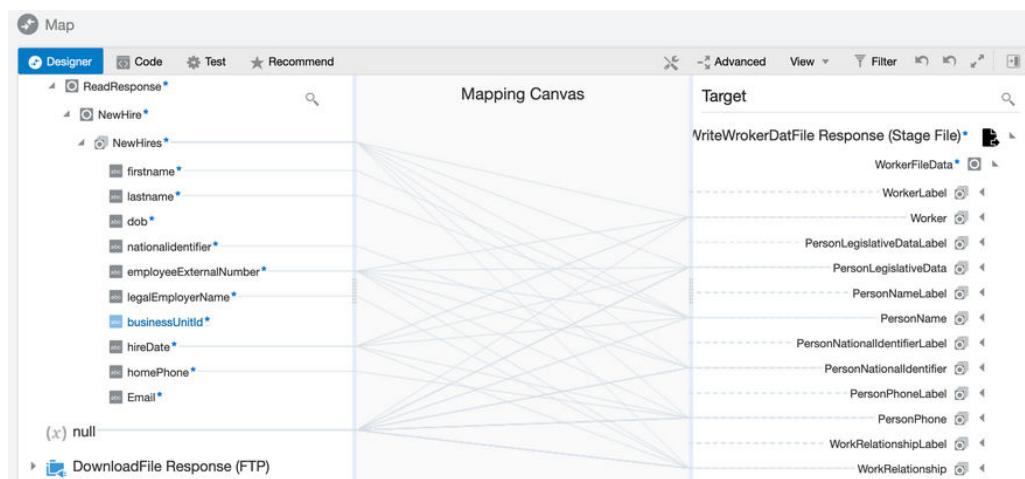
3. Map the elements from the source CSV file to the business object template file. Use the mapper to map the source file elements with the target elements depicted in the schema.

The **Sources** tree shows all available values and fields to use in this mapping. The **Target** tree shows the Write hierarchy. This is a representation of the basic structure for a `Worker.dat` file.

a. For the field labels in the **Target** tree, enter the corresponding header title. For example, under the **WorkerLabel** parent, the **EffectiveStartDateLabel** has the value of **EffectiveStartDate**. These values correspond to the header column within the final DAT file generated.

b. For the data sections of the **Target** tree, map the values from the **Sources** tree or enter default values.

c. Map the repeating element **recordName** value to the repeating element of the parent-specific section values. In this example, **NewHires** requires mapping with parent data sections such as **Worker**, **PersonLegislativeData**, **PersonName**, and so on.



4. Create a second stage file action using the **ZIP File** operation to generate the ZIP file to send to the **Submit HDL Job** operation.
5. Configure the Oracle HCM Cloud Adapter in the Adapter Endpoint Configuration Wizard to use the **Submit an HCM Data Loader job** operation.
 - a. Select the **Import Bulk Data using HCM Data Loader (HDL)** action.

- Basic Info
- Actions
- Operations
- Summary

What would you like to do with Oracle HCM Cloud Adapter?

Query, Create, Update or Delete Information
Query business objects such as employee records etc or perform operations for employee onboarding, data sync etc.

Subscribe to Updates (via ATOM Feed)
Subscribe to changes made to feed-enabled resources in Oracle HCM Cloud.

Import Bulk Data using HCM Data Loader (HDL)
Import and Load data files into HCM Cloud using HDL.

Receive Files from HCM Cloud
Download HCM bulk data files from Universal Content Management (UCM)

Send Files to HCM Cloud
Upload files to the Universal Content Management (UCM) in HCM Cloud. Please note this will only upload the files and not perform any additional operation on the file like Import Bulk Data using HDL option..

- b. Select the **Submit an HCM Data Loader job** operation.

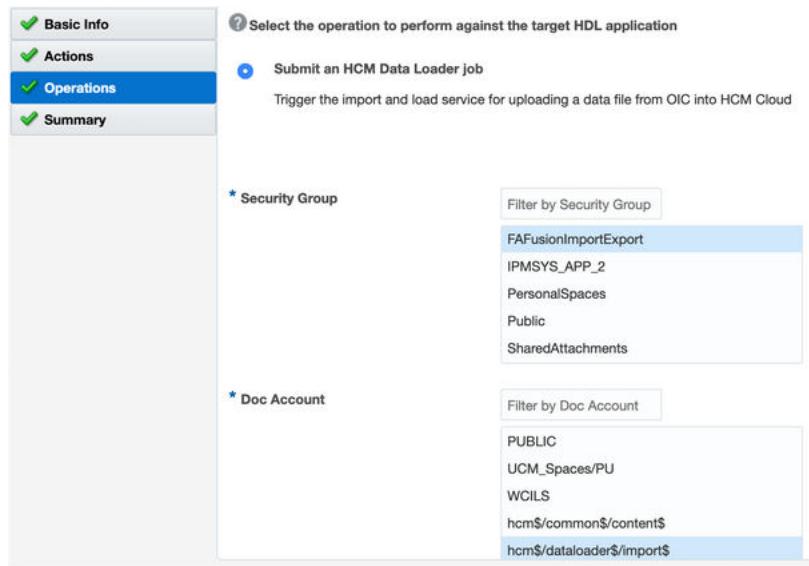
- Basic Info
- Actions
- Operations
- Summary

Select the operation to perform against the target HDL application

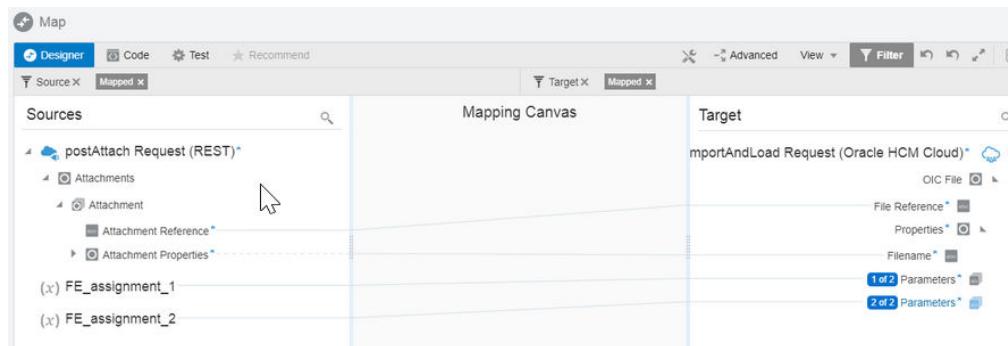
Submit an HCM Data Loader job
Trigger the import and load service for uploading a data file from OIC into HCM Cloud

Query the status of an HCM Data Loader job
Retrieve the status of an HCM Data Loader job submitted by this flow.

- c. Select the security group and doc account configuration parameters for submitting the Oracle HDL job.

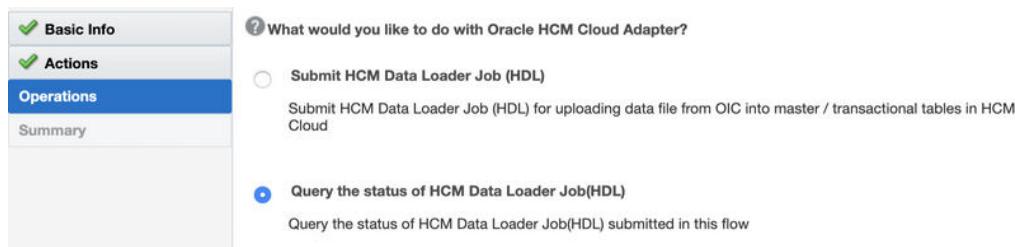


d. Map the file reference. If you want to send additional parameters to the **importAndLoad** operation, use the **Parameters** element.

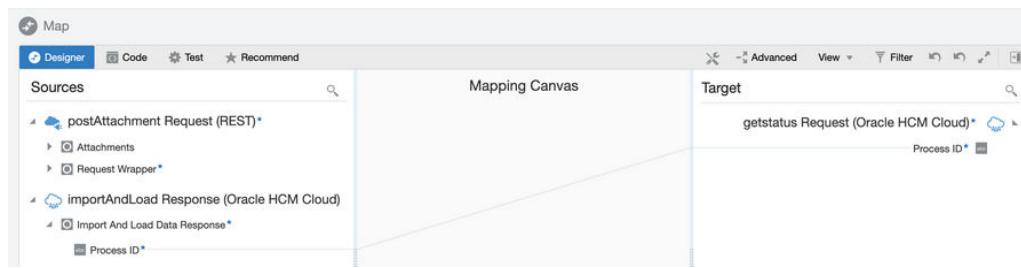


6. Configure a second Oracle HCM Cloud Adapter in the Adapter Endpoint Configuration Wizard to use the **Query the status of HCM Data Loader Job (HDL)** operation. This action can run inside a loop until the HDL job status is identified as started or any other status that you want.

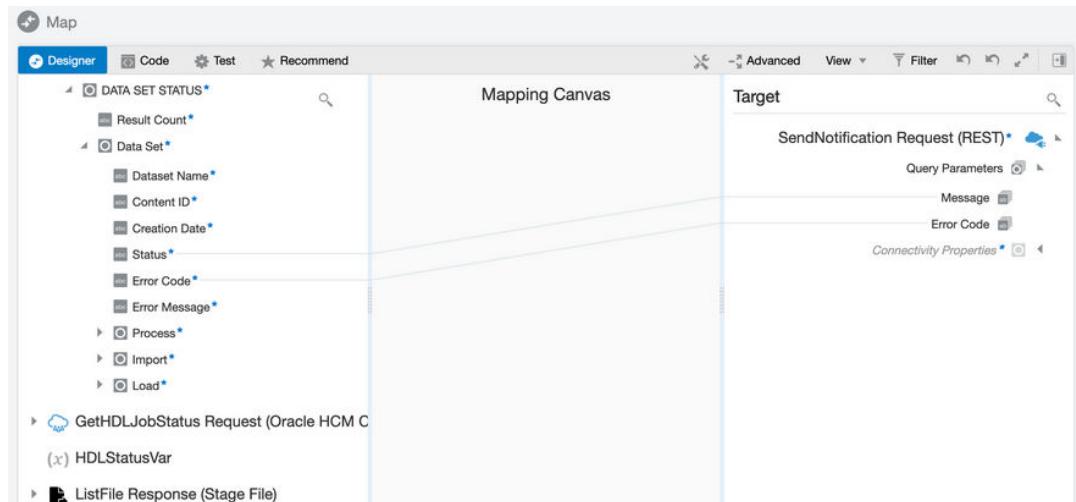
a. Select **Query the status of HCM Data Loader Job (HDL)**.



b. Map the **Process ID** to **getStatus Request (Oracle HCM Cloud) > Process ID**.



7. Map the response from the **Query the status of HCM Data Loader job (HDL)** operation.



Oracle Integration provides extensive visibility into the job status by including status information at various states (for example, job, load, and import states). Compare the status of the job as per your business requirement. The overall status can be one of the following values:

Status	Meaning	Comments
NOT STARTED	The process has not yet started. It is waiting or ready.	If this value is returned, poll again after waiting for some time.
DATA_SET_UNPROCESSED	The process is running, but the data set has not yet been processed.	If this value is returned, poll again after waiting for some time.
IN_PROGRESS	The process is running.	If this value is returned, poll again after waiting for some time.
COMPLETED	The data set completed successfully.	Job is completed, you can fetch the output.
CANCELLED	Either the data set load or data set import was canceled.	Job is canceled.

Select Extensible and Descriptive Flexfields in an Integration

You can select specific extensible flexfields (EFFs) and descriptive flexfields (DFFs) in the Adapter Endpoint Configuration Wizard of an Oracle HCM Cloud Adapter invoke connection. You can then map the EFFs and DFFs in the mapper.

The following use case provides an overview of how to design this type of integration.

1. Create an orchestrated integration.
2. Add a REST Adapter as a trigger connection.
3. Enter the following details:
 - a. On the Basic Info page, enter a name.
 - b. On the Resource Configuration page, select the **POST** action and **Configure a request payload for this endpoint** and **Configure this endpoint to receive the response**.
 - c. On the Request page, select the following:
 - i. Select **JSON sample** as the request payload and enter the JSON sample.
 - ii. From the **Element** list, select **request-wrapper**.
 - iii. For the media type of the request body, select **JSON**.
 - d. On the Response page, select the following:
 - i. Select **JSON sample** as the response payload and enter the JSON sample.
 - ii. From the **Element** list, select **response-wrapper**.
 - iii. For the media type of the response body, select **JSON**.
4. Add an Oracle HCM Cloud Adapter as an invoke connection.
5. Enter the following details.
 - a. On the Basic Info page, enter a name.
 - b. On the Actions page, select **Query, Create, Update, or Delete Information**.
 - c. On the Operations page, select **Business (REST) Resources** from the **Browse by** list.
 - d. Select an appropriate business resource and operation to perform on the resource.
 - e. On the Child Resources page, select child resources with extensible or descriptive flexfields.
 - f. On the Descriptive and Extensible page, select a specific flexfield and associated contexts.
6. In the request mapper between the two adapters, map appropriate source and target flexfields. For example:
7. In the response mapper after the Oracle HCM Cloud Adapter, map appropriate source and target flexfields. For example:
8. Save the integration.



9. Create business identifiers for tracking the integration during runtime.
10. Activate the integration.

Troubleshoot the Oracle HCM Cloud Adapter

Review the following topics to learn about troubleshooting issues with Oracle HCM Cloud Adapter.

Topics:

- [Avoid Missing Atom Entries When Processing Them Page-Wise](#)
- [Unsupported SOAP APIs Available for Selection](#)
- [ATOM Feeds Option Not Appearing for Selection in the Operations Page](#)
- [Manual Metadata Refresh is Required if Updating the Connection to Use the Interface Catalog URL](#)

Additional integration troubleshooting information is provided. See [Troubleshoot Oracle Integration](#) in *Using Integrations in Oracle Integration Generation 2* and the [Oracle Integration Troubleshooting page](#) on the Oracle Help Center.

Avoid Missing Atom Entries When Processing Them Page-Wise

The Oracle HCM Cloud Adapter fetches fewer entries from the Atom server as compared to Postman or `curl` in a single invoke. The Oracle HCM Cloud Adapter provides a solution to avoid missing these entries when processing them page-wise.

Assume you fetch a single page of entries when polling an Atom feed with Postman. If the last entry in the response/page has an identical updated timestamp as the next few entries on the consecutive invoke's response/page, these further entries (with the same updated timestamp) are never included in the subsequent response because the `updated-min` parameter is not inclusive. Similarly, in case future dated updates need to be fetched immediately and the published timestamp needs to be used, if the last entry in the response/page has an identical published timestamp as the next few entries on the consecutive invoke's response/page, these further entries (with the same published timestamp) are never included in the subsequent response because the `published-min` parameter is not inclusive.

To fix this issue, the Oracle HCM Cloud Adapter processes $N-$ entries (the number of entries with the same updated timestamp/published timestamp towards the end of the page). Here, N is the total number of entries on the page. The remaining entries are included in the next invocation. This ensures that no entries are skipped.

Unsupported SOAP APIs Available for Selection

When browsing for services on the Operations page of the Adapter Endpoint Configuration Wizard, unsupported services may appear for selection. If you select an unsupported service (for example, the CreateWorker service), a null pointer exception is displayed.

See Chapter [Business Object Services](#) in *SOAP Web Services for HCM* for the only supported SOAP APIs.

ATOM Feeds Option Not Appearing for Selection in the Operations Page

If the **Subscribe to Updates (via ATOM Feed)** option does not appear for selection on the Actions page in the Adapter Endpoint Configuration Wizard, note the following potential causes:

- The interface catalog URL has not been specified on the Connections page.
- The Atom feed feature may not be enabled for your Oracle Integration instance. Contact Oracle Support Services.

See [Configure Connection Properties](#).

Manual Metadata Refresh is Required if Updating the Connection to Use the Interface Catalog URL

If an existing Oracle HCM Cloud Adapter connection is updated to add the interface catalog URL, you must manually refresh the metadata. Go to the Connections page and find the Oracle HCM Cloud Adapter to refresh.

See [Refresh Integration Metadata](#).