Oracle Oracle® BI Cloud Connector Console

Creating a Business Intelligence Cloud Extract
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preface</strong></td>
<td>i</td>
</tr>
<tr>
<td>1 Overview to Extracting Data from FA Cloud Sources</td>
<td>1</td>
</tr>
<tr>
<td>Overview to Extracting Fusion Applications Cloud Data</td>
<td>1</td>
</tr>
<tr>
<td>Extracting Data from a Fusion Applications Cloud Data Source</td>
<td>1</td>
</tr>
<tr>
<td>2 Dialog Reference</td>
<td>5</td>
</tr>
<tr>
<td>Provisioning a User for BI Cloud Connector Console Access</td>
<td>5</td>
</tr>
<tr>
<td>Provisioning a User to Access BI Cloud Connector Content in Universal Content Management</td>
<td>5</td>
</tr>
<tr>
<td>BI Cloud Connector Enabled Data Stores Page</td>
<td>6</td>
</tr>
<tr>
<td>Specify Which Offerings to Extract</td>
<td>7</td>
</tr>
<tr>
<td>Perform Advanced Extract Configuration</td>
<td>9</td>
</tr>
<tr>
<td>Create and Manage an Offering</td>
<td>9</td>
</tr>
<tr>
<td>Add a Datastore for an Offering</td>
<td>10</td>
</tr>
<tr>
<td>Reset Last Extract Date For All Enabled Data Stores</td>
<td>11</td>
</tr>
<tr>
<td>Configure Flexfield Label Languages</td>
<td>11</td>
</tr>
<tr>
<td>Configure Extract Preferences</td>
<td>11</td>
</tr>
<tr>
<td>Configure Where to Load Data</td>
<td>12</td>
</tr>
<tr>
<td>Preview a Data Store</td>
<td>13</td>
</tr>
<tr>
<td>Specify When to Extract Data</td>
<td>14</td>
</tr>
<tr>
<td>Create a New or Edit an Existing Data Extract Schedule</td>
<td>14</td>
</tr>
<tr>
<td>View Last Run Status for a Data Extract</td>
<td>16</td>
</tr>
<tr>
<td>View Last Run Status for a Deleted Record Extract</td>
<td>17</td>
</tr>
<tr>
<td>Manage Files in External Storage for Custom Warehouse Integration</td>
<td>17</td>
</tr>
<tr>
<td>BI Cloud Connector Preferences</td>
<td>19</td>
</tr>
<tr>
<td>3 Encrypting and Decrypting Extracts</td>
<td>21</td>
</tr>
<tr>
<td>Encrypting Extracts</td>
<td>21</td>
</tr>
<tr>
<td>Decrypting Extracts</td>
<td>21</td>
</tr>
</tbody>
</table>
Preface

This preface introduces information sources that can help you use the application.

Using Oracle Applications

Using Applications Help

Use help icons

?  

to access help in the application. If you don’t see any help icons on your page, click your user image or name in the global header and select Show Help Icons. Not all pages have help icons. You can also access Oracle Applications Help.

Watch: This video tutorial shows you how to find help and use help features.

You can also read Using Applications Help.

Additional Resources

- Community: Use Oracle Cloud Customer Connect to get information from experts at Oracle, the partner community, and other users.
- Guides and Videos: Go to the Oracle Help Center to find guides and videos.
- Training: Take courses on Oracle Cloud from Oracle University.

Conventions

The following table explains the text conventions used in this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>boldface</td>
<td>Boldface type indicates user interface elements, navigation paths, or values you enter or select.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates file, folder, and directory names, code examples, commands, and URLs.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Greater than symbol separates elements in a navigation path.</td>
</tr>
</tbody>
</table>
Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website. Videos included in this guide are provided as a media alternative for text-based help topics also available in this guide.

Contacting Oracle

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit My Oracle Support or visit Accessible Oracle Support if you are hearing impaired.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: oracle_fusion_applications_help_ww_grp@oracle.com.
1 Overview to Extracting Data from FA Cloud Sources

Overview to Extracting Fusion Applications Cloud Data

Introduction to extracting data from Oracle Fusion Applications Cloud data sources.

Topics

• Extracting Data from a Fusion Applications Cloud Data Source

Extracting Data from a Fusion Applications Cloud Data Source

To extract data from a Fusion Applications Cloud data source, you use the BI Cloud Connector to schedule a once-only or regular data load, known as a Cloud Extract. For example, you might extract data from Oracle Fusion HCM Cloud. You can load the extracted data into an Oracle Cloud Storage Service area or into an Oracle Universal Content Management (UCM) server.
Starting BI Cloud Connector
To extract Fusion Applications Cloud data, you use BI Cloud Connector, which is deployed on your Fusion Applications pod.

You start BI Cloud Connector using a HTTP URL based on the following format: http://FA OHS Host:FA OHS Port/biacm. You can also start BI Cloud Connector using the Web link and login details supplied to you by Oracle Cloud Support.

Loading Data into a Cloud Storage Service Area
To perform a Cloud Extract into an Oracle Cloud Storage Service area, you select the Cloud Storage Service storage type in BI Cloud Connector.
Loading Data into a UCM Storage Area
To perform a Cloud Extract into a UCM storage area, you select the UCM storage type in BI Cloud Connector.

Scheduling a Cloud Extract
To keep your data up-to-date, you use the Manage Extract Schedules option in BI Cloud Connector to create a regular Cloud Extract. For example, you might schedule a Cloud Extract to execute at 2.00 AM each day.

Monitoring a Cloud Extract
To monitor the last extract run, you use the Manage Extract Schedules page in BI Cloud Connector.
2 Dialog Reference

Provisioning a User for BI Cloud Connector Console Access

To provision access to the BI Cloud Connector for a user, use the Security Console to create an administrative role that inherits BICC privileges from existing roles and assign the user to that role.

To provision a user:

1. In Fusion, navigate to the Security Console in the Navigator.
2. In the Security Console, create a BIACM_ADMIN role.
   a. Click Create Role.
   b. In the Basic Information page, enter the following values and click Next.

<table>
<thead>
<tr>
<th>Role Name</th>
<th>BIACM_ADMIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Code</td>
<td>BIACM_ADMIN</td>
</tr>
<tr>
<td>Role Category</td>
<td>BI - Abstract Roles</td>
</tr>
</tbody>
</table>

   c. Click the Add icon in the Role Hierarchy list
   d. In the Add Role Membership dialog box, search for ESS.
   e. In the search results, confirm that the ESS Administrator role appears, then click Add Role Membership.
   f. Search for ORA_ASM_APPLICATION_IMPLEMENTATION_ADMIN_ABSTRACT and click Add Role Membership.
   g. Close the Add Role Membership dialog box.
   h. Click Next.
   i. In the Users page, click Add User.
   j. In the Add User dialog box, search for the name of the user you want to assign access to, then click Add User to Role.
   k. Close the Add User dialog box.
   l. Click Next.
   m. Click Save and Close.

Provisioning a User to Access BI Cloud Connector Content in Universal Content Management

To provision access to the BI Cloud Connector content in Universal Content Management (UCM), use the Security Console to create an administrative role and assign a user to that role.

To provision an administrator:

1. In Fusion, navigate to the Security Console in the Navigator.
2. In the Security Console, create a BICC_UCM_CONTENT_ADMIN role.
   a. Click Create Role.
   b. In the Basic Information page, enter the following values and click Next.

<table>
<thead>
<tr>
<th>Role Name</th>
<th>BICC_UCM_CONTENT_ADMIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Code</td>
<td>BICC_UCM_CONTENT_ADMIN</td>
</tr>
<tr>
<td>Role Category</td>
<td>BI - Abstract Roles</td>
</tr>
</tbody>
</table>

   c. In the Add Role Membership dialog box, search for OBIA_EXTRACTTRANSFORMLOAD_RWD and click Add Role Membership.
   d. Close the Add Role Membership dialog box.
   e. In the Users page, click Add User.
   f. In the Add User dialog box, search for the name of the user you want to assign access to, then click Add User to Role.
   g. Close the Add User dialog box.
   h. Click Next.
   i. Click Save and Close.

**BI Cloud Connector Enabled Data Stores Page**

Use BI Cloud Connector to extract Business Intelligence data from a Fusion Applications Cloud data source into an Oracle Storage Service or UCM server. For instructions on loading data, refer to the Business Intelligence documentation for your product. If you’re using BI Cloud Connector with Oracle BI Applications, before you start, refer to the Fusion Applications compatibility matrix for BI Cloud Connector to ensure that your product version is supported.

**How to Use the Cloud Extract Configuration and Execution Tool**

When you log in, use the Enabled Data Stores dialog to search the View Objects (VOs) by Offering that are enabled for extract. To view a list of enabled Data Stores for an Offering, click the Manage Offerings and Data Stores button in the panel tab and select the Manage Offerings and Data Stores link, select an Offering, and use the Data Store for Offering list to view the Data Stores and their last extract date and other properties.

To extract Business Intelligence data from a Fusion Applications Cloud data source, perform the following tasks in the order they appear in the panel tab:

- Click the Configure External Storage button and select the Configure External Storage link to specify the storage area into which you want to load the data.
- Click the Manage Extract Schedules button and select the Manage Extract Schedules button to create a schedule for one-time or recurring data extraction and to monitor the last scheduled run and verify completion.

**How to Review View Object to Database Lineage Mappings**

To review the mappings between BI VOs and database tables and columns, review the following documents and spreadsheets on Oracle Cloud Customer Connect.

- R13.x HCM BI Cloud Adapter BI View Object to Database Lineage Mapping Spreadsheet
- R13.x FSCM BI Cloud Adapter BI View Object to Database Lineage Mapping Spreadsheet
Specify Which Offerings to Extract

Click the **Configure Cloud Extract** button in the panel tab and select the **Configure Cloud Extract** link to open the Offerings dialog, where you can select offerings that you want to extract, specify VOs from which to extract data, and set up once-only or regular data extracts.

**Offering**

<table>
<thead>
<tr>
<th>Field Name or Option</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offerings list</td>
<td>View the offerings that are available for extraction. Click an offering to view and configure its data stores.</td>
</tr>
<tr>
<td>Search</td>
<td>Enter an offering name and click Search to locate it in the list.</td>
</tr>
<tr>
<td>Actions &gt; Create Offering</td>
<td>Create a new offering and specify its VOs.</td>
</tr>
<tr>
<td>Actions &gt; Reset Last Extract Date</td>
<td>Specify the last extract date from which extraction should begin for incremental loads.</td>
</tr>
<tr>
<td>Actions &gt; Configure Flex Label Languages</td>
<td>Specify a language for flexfield labels.</td>
</tr>
<tr>
<td>Actions &gt; Extract Administration</td>
<td>Specify extract parameters, including: job timeout; CSV file size to split files by; retry parameters in case of intermittent BI Server connection or query failures; and extract schedule email notification frequency and recipients.</td>
</tr>
<tr>
<td>List View</td>
<td>View the Offerings list as a list with Actions icon for each offering.</td>
</tr>
<tr>
<td>Grid View</td>
<td>View the Offerings list as a grid with Actions icon for each offering.</td>
</tr>
<tr>
<td>Offering Action &gt; Delete</td>
<td>Delete the currently selected offering and its corresponding VO association. Available only for user-defined offerings.</td>
</tr>
<tr>
<td>Offering Action &gt; Edit</td>
<td>Change the Offering Name and VO association of the currently selected offering.</td>
</tr>
<tr>
<td>Offering Action &gt; Reset to Shipped Content</td>
<td>Reset the offering to shipped content, removing any changes made.</td>
</tr>
<tr>
<td>Offering Action &gt; Reset to Full Extract</td>
<td>Reset the last extract date so that a full data load is performed for the offering, instead of an incremental load. You typically use this option if your business requirements have changed or when fact data has been corrupted.</td>
</tr>
<tr>
<td>Actions &gt; Export Customization</td>
<td>Collect modification information from source environment and export as compressed CSV files.</td>
</tr>
<tr>
<td>Actions &gt; Import Customization</td>
<td>Apply modifications to the destination environment from exported compressed CSV files.</td>
</tr>
</tbody>
</table>

Click the **Configure Cloud Extract** button in the panel tab and select the **Export Customization** link to collect modification information from the source environment and export it as compressed CSV files. Select the **Import Customization** link to modifications to the destination environment from exported compressed CSV files. In the Import Customization dialog box, click Browse and specify exported customization files, then click **Import**.
Data Store for Offering: Offering name

Click an offering in the Offerings list open the Data Store for Offering: Offering Name page, where you can specify View Objects VOIs from which to extract data.

<table>
<thead>
<tr>
<th>Field Name or Option</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Stores list</td>
<td>View the data areas that are available for extraction for the offering you clicked.</td>
</tr>
<tr>
<td>Actions &gt; Advanced Extract</td>
<td>Specify initial extract date and chunking for creation date and primary key for full loads.</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>View &gt; Columns</td>
<td>Select columns to be displayed in the Offerings list.</td>
</tr>
<tr>
<td>View &gt; Detach</td>
<td>Pop out the section of the dialog box so you can see more data.</td>
</tr>
<tr>
<td>View &gt; Reorder Columns</td>
<td>Change the display order of the columns in the Data Stores list.</td>
</tr>
<tr>
<td>View &gt; Query By Example</td>
<td>Filter the displayed results by entering the first few letters of a name.</td>
</tr>
<tr>
<td>Add</td>
<td>Specify a new Data Store for an offering. For example, you might want to add a view object (VO) for extraction. To add a VO, in the wizard’s Datastore details page, provide the VO name, then specify whether you want to disable effective data filter, which allows for extraction of all historical records, if required. Enter any required query filter, using column references following the format <strong>DATASTORE</strong>.&lt;BI VO Column Name&gt;. In the wizard’s Select Columns page, select the column types for the select query from the Column Filter drop-down list, then uncheck the columns you don’t want included in the SELECT list. If the VO is defined as Effective Date Disabled, you can select the Natural Key option for a Primary Key Column to define a natural key.</td>
</tr>
<tr>
<td>Remove</td>
<td>Delete the currently selected Data Store.</td>
</tr>
<tr>
<td>Query by Example</td>
<td>Filter the displayed results by entering the first few letters of a name.</td>
</tr>
<tr>
<td>Detach</td>
<td>Pop out the section of the dialog box so you can see more data.</td>
</tr>
<tr>
<td>Actions &gt; Reset to Full Extract</td>
<td>Reset the last extract date so that a full data load is performed at the next load for the data store/VO, instead of an incremental load. You typically use this option if your business requirements have changed or if fact data has been corrupted.</td>
</tr>
<tr>
<td>Actions &gt; Reset to Shipped Content</td>
<td>Reset the VO to shipped content, removing any changes made.</td>
</tr>
<tr>
<td>Actions &gt; Export Metadata Definition</td>
<td>Export metadata definition for the VO.</td>
</tr>
<tr>
<td>Actions &gt; Export UI Label</td>
<td>Export user interface labels for the VO. A zip file is generated with files for each configured language.</td>
</tr>
<tr>
<td>Actions &gt; Test Data Store</td>
<td>Test extract from the selected Data Store.</td>
</tr>
<tr>
<td>Actions &gt; Advanced Extract</td>
<td>Specify initial extract date and chunking for creation date and primary key for full loads.</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Last Extract Date</td>
<td>View the date and time when the Data Store was last extracted.</td>
</tr>
<tr>
<td>Preview</td>
<td>View the VO definition and column list.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the Data Store list.</td>
</tr>
<tr>
<td>Export Columns</td>
<td>Export metadata definition or user interface labels for a selected VO. Select whether you want to export Metadata Definition or UI Labels. For UI Labels, a zip file is generated with files for each configured language.</td>
</tr>
<tr>
<td>Last Extract Date</td>
<td>View the date and time when the Data Store was last extracted.</td>
</tr>
</tbody>
</table>

Click the Configure Cloud Extract button in the panel tab and select the Review Cloud Extract Configuration link to return to the Enabled Data Stores dialog box.
Perform Advanced Extract Configuration

Select Actions > Advanced Extract Configuration in the Data Store for Offering page of the Offering dialog to open the Advanced Extract Configuration For: Data store name dialog, where you can set advanced extract configuration for a selected data store. For full extracts, you can enable chunking by creation date or by primary key.

Filter and/or Chunk By Creation Date Columns

<table>
<thead>
<tr>
<th>Field Name or Option</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column list</td>
<td>View the columns that are available for designation as creation date. Select the Is Creation Date option for the appropriate column.</td>
</tr>
<tr>
<td>Initial Extract Date</td>
<td>Optionally, specify the initial date from which the full extract should be performed. This option requires selection of the Is Creation Date option for a column or columns in the column list which represent the Creation Date.</td>
</tr>
<tr>
<td>Support chunking</td>
<td>Optionally, select By Creation Date to chunk by to specify a number of days by which to extract date range batches or chunks of data. This option requires selection of the Is Creation Date option for a column or columns in the column list which represent the Creation Date.</td>
</tr>
<tr>
<td>Number of Days</td>
<td>If you have selected to support chunking by creation date, specify the number of days, for example 365, by which to chunk extracts.</td>
</tr>
</tbody>
</table>

Chunk By Primary Key Column

<table>
<thead>
<tr>
<th>Field Name or Option</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support chunking</td>
<td>Support chunking by numeric primary key. This option requires a single numeric primary key column for the data store.</td>
</tr>
<tr>
<td>Number of Rows</td>
<td>Specify a number of rows to chunk extracts by.</td>
</tr>
</tbody>
</table>

Create and Manage an Offering

Click Actions > Create Offering in the Offerings dialog to open the Manage Offering dialog, where you can specify a new offering and associate a data store.

Manage Offering

<table>
<thead>
<tr>
<th>Field Name</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offering Code</td>
<td>Enter a code for the offering.</td>
</tr>
<tr>
<td>Offering Name</td>
<td>Enter a name for the offering. This is the name that will appear in the list of Business Intelligence Applications Offerings in the Configure Cloud Extract dialog.</td>
</tr>
</tbody>
</table>
Associate Data Store

In the Associate Data Store section of the dialog, filter for the data store, then select and click the **Move selected items to other list** button to add the VO, then click **Save**.

Add a Datastore for an Offering

Click the **Add** button in the Data Store for Offering dialog to open the Define Datastore dialog box, where you can specify a new data store for the selected offering.

Datstore Details Page

1. Enter the following information and click **Next**.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Store Key</td>
<td>Enter the VO name for datastore.</td>
</tr>
<tr>
<td>Disable Effective date filter</td>
<td>Enable this option if there is a requirement to extract all historical records. Note that the VO not validated as being effective dated in nature, so set this option only after confirming the nature of the data.</td>
</tr>
<tr>
<td>Extract Data Store Metadata</td>
<td>Enable this option to generate an mdcsv file with the data extract.</td>
</tr>
<tr>
<td>Query Filter</td>
<td>Enter the Query Filter in the Oracle BI Enterprise Edition select_physical supported format. All column references should follow the format underscore ( _ ) underscore ( _ ) DATASTORE underscore ( _ ) underscore ( _ )dot(.)&gt;BI VO Column Name&gt;, for example <strong>DATASTORE</strong>.ViewApplicationId=0 where ViewApplicationId is the column name in the BI VO and of data type number.</td>
</tr>
</tbody>
</table>

2. In the Associate Offerings section of the page, select the names of the offerings you want to associate with the datastore and click the **Move selected items to other list** button to add them, then click **Save**.

3. Click **Next** to navigate to the Select Columns page. The column definitions are fetched from the BI repository. By default, the table shows the date type columns so the user can select which of these columns should be included in the incremental filter query.

Select Columns Page

By default, the Column Name table shows the Date Type column so you can select which of these columns is included in the incremental filter query. Click the Column Filter drop-down list to switch from the default filter to Primary Key Columns or All Columns.

By default, all of the columns are selected for query. In the columns list, deselect the Used in Select list option for any columns you don’t want included.

If the VO is defined as Effective Date Disabled, you can view the Primary Key Columns and select the Natural Key option for a column to define a natural key.
For custom VOs, primary keys are retrieved from the repository (RPD). You can override these and set your own by selecting the Primary Key option for a column. To reset primary keys to those defined in the repository, click the Retrieve PK button.

### Reset Last Extract Date For All Enabled Data Stores

Click Actions > Reset Last Extract Date in the Offerings dialog to open the Reset Last Extract Date For All Enabled Data Stores dialog.

Specify the last extract date from which extraction should begin for incremental loads for the selected Offering. You typically use this option if your business requirements have changed or when fact data has been corrupted. Click OK to reset.

### Configure Flexfield Label Languages

Click Actions > Configure Flex Label Languages in the Offerings dialog to open the Configure Flex Label Languages dialog, in which you can specify a language for flex labels.

In the Flex Label Languages list, scroll to select the language you want, then click the Move selected items to other list button to add it to the selected list, then click Save and Close. To suspend extraction of flexfield labels during extraction, select the Suppress Flex Label Extract option.

### Configure Extract Preferences

Click Actions > Extract Preferences to open the Extract Preferences dialog, where you can specify preferences for extracts.

#### Language

In the Preferred Extract Language field, select language you would prefer extracts be made in.

#### Job Settings

In the Timeout in Hours field, enter the number of hours before a job times out. The default is 1. By default, the job fails on timeout. Deselect Timeout Force Fail if you prefer that timed out jobs not be failed.

#### File Parameters

In the Compression type field, select the type of compression you’d like to use. In the Split file size (GB) field, specify the file size by which extracted CSV files are divided for a single VO. The default is 1 GB. You can set the file size from one to five GB.

In the Uploaded file expiry (Days) field, enter the number of days you’d like the extract files to persist.

File Parameters settings can be overridden at the schedule level when creating schedules and assigning external storages to them.
Extract Mode
Select the **Bypass OTBI Metadata for all data stores** option to bypass OTBI metadata.

External Storage
Select the **Upload to Multiple External Storage** option to increase the number of external storages that can be selected in the External Storage list when creating or editing schedules. The default is one storage, and the maximum is two.

Retry Parameters
During extraction, connections to the BI Server or queries may fail, causing retries. In the Analytic server connection retry limit field, specify the number of connection attempts made to complete the extraction. In the Analytic server query retry limit field, specify the number of times a query is resubmitted.

The Analytic server connection retry limit setting can be overridden at the schedule level when creating schedules and assigning external storages to them.

Global Extract Schedule Notification
To send notifications when scheduled extract events occur, select the notifications you want upon extract start, success, or failure. In the Mail To Addresses, enter email addresses, separated by commas, to which you want notifications sent.

Global Extract Schedule Notification settings can be overridden at the schedule level when creating schedules and assigning external storages to them.

Configure Where to Load Data
Click the **Configure External Storage** button in the panel tab and select the **Configure External Storage** link to open the Configure External Storage dialog box, where you can specify storage areas into which Cloud data is loaded. For example, to load into one or more Oracle Cloud Storage Service instances, select the Storage Service Connection Configuration tab. Select the UCM Connection Configuration tab to configure Universal Content Management Server connections.

Storage Type — Cloud Storage Service
Specify the connection details for one or more Oracle Storage Service instances by clicking the name of a provisioned connection or clicking Add to create a new connection. Click Delete to delete an existing connection.

Storage areas are associated with extract schedules. You can have as many Cloud Storage Service containers as are required by your Cloud application integrations, but each should be used for its own requirements, so that there's no overlap between them. Runtime metadata, including the last extract date, is managed across all storage locations, so configuring the same data store in multiple schedules with different external storage configurations results in loss of incremental data.

Use the following fields in the Storage Service Connection Configuration page to specify the connection details:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name for the connection.</td>
</tr>
<tr>
<td>OAC External Storage</td>
<td>Select this option if the connection is to an Oracle Analytics Cloud (OAC) storage service. You can specify only one OAC storage service connection. Note that encryption is disabled for OAC storage.</td>
</tr>
</tbody>
</table>
### Field Name | How to Use
---|---
Protocol | Specify http for non-SSL, or https for SSL connection.
Host | Specify the Host name for the Oracle Storage Service. For example, mystorage.storage.oraclecloud.com.
Port | Specify the port number (optional).
User Name | Specify the user that is provisioned to load data. The user should have privileges to upload files in the container specified. User credentials will be stored in the Weblogic credential store under oracle.apps.security/FUSION_APPS_OBIA_STORAGESERV_USER-KEY.
Password | Specify the password for the user specified in the User Name field.
Service Name | Specify the service name of the Oracle Cloud Storage Service. For example, gse-otbie1.
Container | Specify the name of the container that is allocated to upload extracted files.
Data Encryption — Support Encryption | If you want to encrypt communication, select this option and use the Import Certificate option below to specify the encryption keys.
Import Certificate | Click Browse and navigate to and select the location of the key file, or type the literal path location and file name.
Download Folder | Shows the directory in the domain server where the Batch Extract file is downloaded to reset extract dates before the extraction process.
Upload Folder | Shows the directory in the domain server where files are temporarily extracted by the cloud extractor before uploading to the storage service.

### Storage Type — UCM
Specify the connection details for a Universal Content Management (UCM) on-premises data source using the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Specify http for non-SSL, or https for SSL. If you select https here, you must also enable HTTPS on the UCM server, using the UCM Server Console.</td>
</tr>
<tr>
<td>Host</td>
<td>Specify the host name for the UCM Server. For example, myserver.company.com</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port number of the UCM Server (optional). For example, 7012.</td>
</tr>
<tr>
<td>Download Folder</td>
<td>Shows the directory in the domain server where the Batch Extract file is downloaded to reset extract dates before the extraction process.</td>
</tr>
<tr>
<td>Upload Folder</td>
<td>Shows the directory in the domain server where files are temporarily extracted by the cloud extractor before uploading to UCM.</td>
</tr>
</tbody>
</table>

### Preview a Data Store
Click a data store link in the Data Store for Offering dialog to open the Data Store Preview dialog, where you can preview a selected data store’s columns and enable and disable the data store and its effective date filter.
Specify When to Extract Data

Click the Manage Extract Schedules button in the panel tab and select the Manage Extract Schedules link to open the Manage Extract Schedules dialog, where you can set up a once-only or regular data extract of Business Intelligence data from an Oracle Applications Cloud data source. For example, you might want to extract data from your Cloud data source once per day at midnight. You can also monitor an extract here.

Monitor a Cloud Extract

In the Schedules dialog, click Actions and select the option for the last run corresponding to the job type, Cloud Data Extract or Deleted Record Extract. Each job type displays in its own dialog, which lists the last cloud extract or deleted record extract status of each VO with status of SUCCESS or FAILURE for each data store and error messages in the case of failures. The ESS Request Id column displays the job for which the VO extraction last ran.

Scheduled jobs also write logs that can be used to review issues causing errors or shared with Oracle Support to resolve a service request. To download logs, click Help and select Download Logs.

Create a New or Edit an Existing Data Extract Schedule

In the Manage Extract Schedules dialog, click Add or Edit to create a new Cloud data extract or edit an existing one. For example, you might want to extract data from your Cloud data source once per day at midnight. For a once-only data extract,
use the Simple option in the Recurrence drop down list. You can only create a schedule if there is not an active schedule for the selected job type (for example, Cloud Data Extract, Deleted Record Extract, or Data and Delete Record Extract). Click Next to specify the data stores for extract for an offering in the Data Store List page.

Schedule Details

<table>
<thead>
<tr>
<th>Field Name or Option</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job Type</strong></td>
<td>To extract data, select Application Data Extract. To sync the Cloud system to your source data, select Active Primary Key Extract, which extracts primary key values to identify deleted records. To combine both Cloud Data Extract and Delete Record Extract into one job, select Application Data and Active Primary Key Extract. To purge expired files from Universal Content Management (UCM), select Delete Expired UCM Files. When a file is extracted and uploaded to UCM, it has a default expiration of 90 days. Expired files are soft deleted from UCM and may eventually require purging to preserve space. The job deletes only expired files from the OBIAImport security group. To delete all of the files uploaded to one or more selected external storages, select Delete Files in Storage. For a storage service, this job deletes all files from the container associated with the external storage. For UCM, it deletes all file uploaded to the OBIAImport security group.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Specify a short name to identify the schedule in the Schedules list.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Specify a brief description to identify the schedule, which is only displayed on the Edit Schedule dialog.</td>
</tr>
<tr>
<td><strong>Global Data Store List</strong></td>
<td>Accept the default of No to select data stores for extraction. Select Yes to use the Global Data Store.</td>
</tr>
<tr>
<td><strong>Recurrence</strong></td>
<td>Specify how often you want the extract to be performed. To create a once-only data extract, select Simple.</td>
</tr>
<tr>
<td><strong>Hourly Interval</strong></td>
<td>Specify the number of hours to perform hourly interval extracts by (if you select Hourly in the Recurrence list).</td>
</tr>
<tr>
<td><strong>Date and Time</strong></td>
<td>Specify the date and time to perform a once-only extract (if you select Simple in the Recurrence list).</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>Specify the time to start an extract, in the format HH:MM:SS AM/PM. For example, 3:00:00 AM.</td>
</tr>
<tr>
<td><strong>Day</strong></td>
<td>For weekly schedules, select the check box next to each day on which you want to extract data. For Monthly or Yearly extracts, select the day of the month on which you want to extract data.</td>
</tr>
<tr>
<td><strong>Month</strong></td>
<td>For Yearly (annual) schedules, select the month in which you want to extract data.</td>
</tr>
</tbody>
</table>

Data Store List

<table>
<thead>
<tr>
<th>Field Name or Option</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Offering</strong></td>
<td>Select an offering to extract.</td>
</tr>
<tr>
<td><strong>Data Store List</strong></td>
<td>Lists the data stores for a selected offering.</td>
</tr>
<tr>
<td><strong>Enabled for Extract</strong></td>
<td>Select to enable a data store for extract.</td>
</tr>
<tr>
<td><strong>Query By Example</strong></td>
<td>Filter the displayed results by entering the first few letters of a name.</td>
</tr>
<tr>
<td><strong>Detach</strong></td>
<td>Pop out the section of the dialog box so you can see more data.</td>
</tr>
</tbody>
</table>
External Storage
For seamless integration, you can configure a schedule to use application-specific storage service containers, allowing you to schedule extracts for multiple integrations.

**Note:** To optimize the extraction flow and force reuse of the extracted data files across integrations, it’s preferable that separate storage containers be used when there is no overlap on the data stores required for each integration. Runtime metadata, including the last extract date, is managed across all storage locations, so configuring the same data store in multiple schedules with different external storage configurations results in loss of incremental data. If an overlap on the data stores is required, you can enable advanced extract options for extract jobs to upload the same data files to two separate external storage locations. To do this, select the Upload to Multiple External Storage option in the Extract Preferences dialog box.

<table>
<thead>
<tr>
<th>Field Name or Option</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Storage</td>
<td>For extracts, select a data store to upload the extract to. By default, you can select one. If the Upload to Multiple External Storage option is selected in your extract preferences, you can select two data stores if an overlap of the data stores is required. If you’re deleting expired UCM files, the UCM external storage is selected. If you’re deleting files in storage, select one or more from the list of external storages to delete.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notification</th>
<th>Select one of the following options: Use Global Extract Notification to use the global settings defined in the Extract Preferences dialog box; Define Notification to set notifications for the schedule and override the global settings; or None, the notifications you want upon extract start, success, or failure. In the Mail To Addresses, enter email addresses, separated by commas, to which you want notifications sent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify On</td>
<td>If you have selected Define Notification for the schedule, select the notifications you want upon extract start, success, or failure.</td>
</tr>
<tr>
<td>Mail to Addresses</td>
<td>Enter email addresses, separated by commas, to which you want notifications sent.</td>
</tr>
<tr>
<td>Use Global File Parameters</td>
<td>Select Yes to use the global file parameter settings defined in the Extract Preferences dialog box. Select No to set parameters for the schedule and override the global settings.</td>
</tr>
<tr>
<td>Compression Type</td>
<td>Select the type of compression you’d like to use for the schedule.</td>
</tr>
<tr>
<td>Split file size (GB)</td>
<td>Specify the file size by which extracted CSV files are divided for a single VO for the schedule. The default is 1 GB. You can set the file size from one to five GB.</td>
</tr>
<tr>
<td>Uploaded file expiry (Days)</td>
<td>Enter the number of days you’d like the extract files to persist for the scheduled extract.</td>
</tr>
</tbody>
</table>

View Last Run Status for a Data Extract

In the Manage Extract Schedules dialog, click **Actions** and select a a last run status for a run type to view logging and status for each VO for the last extraction job for each, indicated by the ESS Request Id. Click **Detach** to expand the dialog to full size.
Statues
The status for each data store is displayed in the Status column. In the event of an error, the error message is displayed in the Message column. Status includes:

- **ERROR**: Extract failed with the error message displayed in the Message column.
- **EXTRACT_SUCCESS**: Extract ran successfully.
- **UPLOAD_SUCCESS**: Upload to external storage ran successfully.

View Last Run Status for a Deleted Record Extract
In the Manage Extract Schedules dialog, click **Actions** and select **Last Run Status for Active Primary Key Extract** to open the Last Run Status for Active Primary Key Extract dialog, which provides logging and status for each VO for the last extraction job for each, indicated by the ESS Request Id. Click **Detach** to expand the dialog to full size.

Statues
The status for each data store is displayed in the Status column. In the event of an error, the error message is displayed in the Message column. Status includes:

- **ERROR**: Extract failed with the error message displayed in the Message column.
- **EXTRACT_SUCCESS**: Extract ran successfully.
- **UPLOAD_SUCCESS**: Upload to external storage ran successfully.

Manage Files in External Storage for Custom Warehouse Integration
During extract, view object (VO) data in compressed files is uploaded to external storage with a manifest file that lists the files from the current batch. Use the information in the manifest file to process data. For a custom warehouse implementation, you must manage the manifest file and its content.

Data Uploaded to External Storage
The following files are uploaded as compressed files with .zip extensions with the file name format of `file_[VONAME]-batch[number]-[TIMESTAMP]`:

- Comma-separated value (.csv) files: VO data and are uploaded as compressed files.
- Metadata comma-separated value (.mdcsv) files: metadata files with details about columns and data type definitions for Data Stores (BIVOs).
- Primary Key comma-separated value (.pecsv) files: data files with primary key column values used to identify deleted records in the warehouse.
The uploaded files are detailed in a manifest file, whose name format depends on the configured storage area. Universal Content Manager (UCM) manifest files are named `MANIFEST.MF`. Cloud Storage Service manifest files have a file name format of `MANIFEST-[TIMESTAMP].MF`.

**Note:** To support parsing of the comma-separated value files, column values are wrapped in double quotes. The double quote value in the column is escaped using two consecutive double quote values. Because of this, a custom delimiter isn’t required.

### Manifest File Formats and Content

The first line of a manifest file describes the source version. In UCM `MANIFEST.MF` files, the body of the file contains information about each of the uploaded files in the format `vo_name;ucm_document_id;md5_check_sum_value`. For example, in the below sample line from a UCM manifest file, 9526 is the UCM document ID of the uploaded file, `;b2af2bf486366e2c2cb7598849f0df2e` is the check sum value.

```
crmanalyticsam_partiesanalyticsam_customer;9526;b2af2bf486366e2c2cb7598849f0df2e
```

In Cloud Storage Service `MANIFEST-[TIMESTAMP].MF` files, the body of the file contains information about each of the uploaded files in the format `extract_uploaded_filename;md5_check_sum_value`. For example, in the below sample line from a Storage Service manifest file, `file_fscmtopmodelam_analyticsserviceam_currenciestlpvo-batch1209716923-20150615_105514.zip` is the uploaded file name, and `;fa981be0caf70a9a52df3aceb9998cc9` is the check sum value.

```
file_fscmtopmodelam_analyticsserviceam_currenciestlpvo-
batch1209716923-20150615_105514.zip;fa981be0caf70a9a52df3aceb9998cc9
```

### Downloading and Processing Content from UCM

To download extracted content from UCM, search for `DOCTITLE` `MANIFEST.MF` and sort by `DOCDATE` in DESC order. This provides all of the manifest UCM files in order by docid. Download each `MANIFEST` file using docid. Parse the lines in the manifest file to download data files using their respective `ucm_document_ids`. You can use the `md5_check_sum_value` to verify downloaded file content. After downloading the files, unzip them and process them based on their file extension, for example by `.csv`, `.mdcsv`, or `.pecsv`.

Once the data files are processed, rename the corresponding `MANIFEST.MF` file in UCM by adding a timestamp prefix in the format `[TIMESTAMP]_MANIFEST.MF` so that it’s not reused in the next download from UCM. Expire the manifest file and all the processed files after 30 days so that UCM storage doesn’t run out of space.

### Downloading and Processing Content from Cloud Storage Service

To download extracted content from Cloud Storage Service, search for `MANIFEST-` and sort by filename. This provides all of the manifest files in order by date. Download each manifest file and parse the lines in the manifest file to download data files using their respective file names. You can use the `md5_check_sum_value` to verify downloaded file content. After downloading the files, unzip them and process them based on their file extension, for example by `.csv`, `.mdcsv`, or `.pecsv`.

Once the data files are processed, rename the corresponding manifest file in Storage Service by adding a timestamp prefix in the format `[TIMESTAMP]_MANIFEST` so that it’s not reused in the next download. Expire the manifest file and all the processed files after 30 days so that storage doesn’t run out of space.
BI Cloud Connector Preferences

Set preferences for the BI Cloud Connector, including regional settings, display language, and accessibility options.

<table>
<thead>
<tr>
<th>Preference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regional</td>
<td>Select the regional options, which include indicating the country, date format, time format, number format, currency, and time zone.</td>
</tr>
<tr>
<td>Language</td>
<td>Select the display language for the BI Cloud Connector Console.</td>
</tr>
<tr>
<td>Accessibility</td>
<td>Select accessibility options, such as use of a screen reader, high color contrast, and font size.</td>
</tr>
</tbody>
</table>

To set Regional and Language preferences, click the Preferences button in the panel tab and select the Regional link or Language link. To save your changes, click Save. To set Accessibility preferences, click the Accessibility button, make changes to your settings, and click Apply.
3 Encrypting and Decrypting Extracts

Encrypting Extracts

BI Cloud Connector supports signed and unsigned encryption using Pretty Good Privacy (PGP) for files uploaded to Universal Content Management (UCM). Optionally, you can enable signed extract files and download a generated signing key.

Before setting up encryption, generate a key pair using PGP and export the public key from the key pair to a location from which it can be imported. Encryption is performed using an imported public key. You use the private key from the key pair to decrypt your extracts.

To set up encryption for a data store:

1. Click the Configure External Storage button in the panel tab and select the Configure External Storage link to open the Configure External Storage dialog box.
2. Select the UCM Connection Configuration tab.
3. In the Data Encryption section, select Data Encryption.
4. Click Browse to import the public key from the key pair you generated. In the File Upload dialog box, navigate to your key file, select it, and click Open. Click Update... to update a key. Imported keys are stored in the GnuPG keyring on the server host.
5. Optionally, select Sign Extract File to generate a signing key for your extracts.
6. If you choose to sign the extract files, click the Download BICCC Public Key button to save the signing key.
   a. In the Opening biccc.gpg dialog box, select Save File and click Browse to select a location to save the signing key.
   b. Click Save.
7. In the Key list, select the Key Id, then click Actions > Set as default to set a default key.
8. To delete a key, select Actions > Delete.

Encrypted extracts uploaded to UCM are stored with a suffix of .gpg.

Decrypting Extracts

BI Cloud Connector encrypts files before upload to Universal Content Management using the imported public key you provide. Use your private key to decrypt uploaded files.

To decrypt and verify signed files, download the signing key and verify that the keys are imported into the keystore and appear in the Key list in the Configure External Storage dialog box. Use the following command to decrypt both signed and unsigned .gpg files:

```
gpg --decrypt <inbound_file_name> --output <output_file_name>
```