Oracle® FCCM Investigation Hub Cloud Service

Using Investigation Hub Administration Tools

ORACLE®

Oracle FCCM Investigation Hub Cloud Service Using Investigation Hub Administration Tools, Release 25.11.01

G27608-05

Contents

1 Introduction

2 Getting Started

3 Case Priority

4 Configure Case System Parameters

5 Audit History

6 Queue Management

7   Case Assignment Rules

8   Exporting and Importing Objects

Preface

Using Investigation Hub Administration help you to configure Case Parameters and workflows, leveraging Case Designer and Workflow Designer.

Audience

This document is intended for users who are responsible for provisioning and activating Oracle FCCM Cloud Service or for adding other users who would manage the services, or for users who want to develop Oracle Cloud applications.

Help

Use Help Icon 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 the https://docs.oracle.com/en/ to find guides and videos.

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

For more information, see these Oracle resources:

- Oracle Public Cloud: http://cloud.oracle.com

- Community: Use https://community.oracle.com/customerconnect/ to get information from experts at Oracle, the partner community, and other users.

- Training: Take courses on Oracle Cloud from https://education.oracle.com/oracle-cloud-learning-subscriptions.

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which user supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that user enter.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: https://support.oracle.com/portal/.

1

Introduction

About Investigation Hub Administration

Investigation Hub Administration Tools help you to configure Case Parameters and workflows, leveraging Case Designer and Workflow Designer.

For most case types, Workflow Designer allows users to define new statuses, actions, action reasons, and workflow steps directly within the UI. These workflows can also be mapped to a case type(s).

Additionally, users can use jurisdiction to further refine correlation rules, which are used to define the conditions upon which a case would be generated. Leveraging the case designer, these correlation rules can be mapped to case types, and new case types can be defined.

For Transaction Filtering case types, the PMF Orchestration Guide facilitates built-in tools for orchestration of human and automatic workflow interfaces. This enables the Administrator to create process-based Case Investigation. It also enables the Administrator to model business processes and workflow.

> ⓘ **Note**
>
> From 24.08.01 release ensure that you use the iHub's **Workflow Designer** instead of AAI PMF Designer.

Investigation workflow can vary based on the type of case being investigated. The case investigation and resolution are supported by various actions, which can be specific to the case type. Access to types of cases and actions are controlled based on the user role and access privileges. Administrators design the workflow using the PMF Orchestration Guide.

During case investigation, Case Analysts and Case Supervisors search, investigate, and resolve cases. After a case is created and appears in the application, user actions towards investigation and resolution change the status of a case from new (New) to closure (Closed as True Positive or Closed as False Positive).

This section contains the following topics:

- Getting Started includes instructions on how to login to the application.

- PMF Orchestration Guide is a design and execution framework that enables Process Pipeline developers to implement various Pipelines modeled by business analysts. Process Pipeline developers use the framework to orchestrate the Business Pipelines within services, and also to design the artifacts that participate in the Pipelines, in order to complete their implementation.

- Case Priority explains how to add and edit the Case Priority.

- Configure Case System Parameters explains how to edit the Case System Parameters.

- Audit History explains how to track the record changes made in system configuration.

- Exporting and Importing Objects explains how to migrate the objects.

2

Getting Started

This section provides step-by-step instructions to access the Investigation Hub Administration.

Accessing Investigation Hub Administration

To access the Investigation Hub Administration, follow these steps:

1. Enter the URL in the web browser.

2. The **Oracle Cloud** login page is displayed.

3. Enter your **User ID** and **Password**.

4. Click **Sign In**. The **Applications** landing page is displayed.

5. Click **Application Navigation** ≡ icon at the top left corner and the **Navigation List** displays the **Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service** module.

6. Click **Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service**. The menu options are displayed.

7. Click **Application Administration** and then click **Investigation Hub Administration**

8. Click the required option such as Process Modeling Framework, Case Priority, Case System Parameters, or Audit History.

3
Case Priority

Correctly prioritizing cases allows investigators to understand which cases should be worked on first.

You can configure Investigation Hub to prioritize cases according to your requirements, based on case type, jurisdiction, and business domain. Investigators can later choose to change the case priority for individual cases manually, if needed.

To access the Case Priority List page, follow these steps:

1. Navigate to the landing page.
2. Click the **Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service** to access the Navigation List. The Navigation List displays the list of modules.
3. Click **Application Administration** and then click **Investigation Hub Administration**
4. Select **Case Priority**. The Case Priority List page opens and displays the case priority list.
5. Click ❮ to view the current settings for each priority level in this list.

3.1 Add Case Priority

To configure case priority, follow these steps:

1. Navigate to the Case Priority page by selecting **Case Type Priority** from the Navigation List. The **Case Priority List** page is displayed.
2. Click **Add** ⊞ . The **Add Case Priority Type** window is displayed.
3. Enter the details as mentioned in the following table.

Table 3-1   Add Case Priority Type - Field Description

Field	Description
Jurisdiction	Select one or more jurisdictions or select All.
Business Domain	Select one or more business domains or select All.
High	Define the case score range at which a case is considered High priority. You must set both a High limit and a Low limit for the range, for example, 67 to 100. Ranges cannot overlap.
Low	Define the case score range at which a case is considered Low priority. You must set both a High limit and a Low limit for the range, for example, 0 to 33. Ranges cannot overlap.
Medium	Define the case score range at which a case is considered Medium priority. You must set both a High limit and a Low limit for the range, for example, 34 to 66. Ranges cannot overlap.

> **ⓘ Note**
>
> The fields which are marked with asterisk * are mandatory.

3.2 Edit Case Priority

To edit a previously configured case priority, follow these steps:

1. Navigate to the **Case Priority** page. The **Case Priority List** page is displayed.

2. Select the **Case Priority** and click **Edit** ✏️ . The **Edit Case Priority** window is displayed.

3. Modify the priority ranges as required.

> **ⓘ Note**
>
> The **Jurisdiction**, **Case Type**, and **Business Domain** cannot be edited.

4. Click **Save**. A confirmation message is displayed: *Saved Successfully*. The Case Priority is updated in the Case Priority list.

3.3 Delete Case Priority

To delete a previously configured case priority, follow these steps:

1. Navigate to the **Case Priority** page. The **Case Priority List** page is displayed.

2. Select one or more **Case Priority** and click **Delete** 🗑️ . A confirmation message is displayed: *Are you sure you want to delete the record(s)?*

3. Click **OK**. The Case Priority list is updated.

4

Configure Case System Parameters

Case System Parameters are used to set default format definitions, which will be used throughout the application.

For example, if you have defined the default Date Format as dd/MM/yyyy, then dates will appear in this format everywhere in the application. The following table details the Case System Parameters which are pre-configured with the application.

Table 4-1   Seeded System Parameters

Parameter ID	Parameter Name	Parameter Description	Parameter Value
1	Date Format	This parameter specifies the date format to be used across Investigation Hub application. Supported formats are MM/dd/yyyy and dd/MM/yyyy. **Note**: If you modify the default Date Format, it will not be reflected in the **Investigation Hub** application.	Default value is dd/MM/yyyy
2	Date with Time Format	This parameter specifies the date with time format to be used across Investigation Hub application. Supported formats are MM/dd/yyyy HH24:MI:SS , MM/dd/yyyy HH:MI:SS AM, dd/MM/yyyy HH24:MI:SS and dd/MM/yyyy HH:MI:SS AM. Please make sure date format is matching with date format provided in the Date Format parameter. **Note**: If you modify the default Date with Time Format, it will not be reflected in the **Investigation Hub** application.	Default value is DD/MM/YYYY HH24:MI:SS
3	Base Currency	This parameter specifies the base currency code for the installation. This currency code will be prefixed with a space to the amount values across the application except for the transaction amount. For Transactions, it will display the currency in which the transaction is done.	USD
4	Valid Formats for Documents	This parameter specifies the supported type of documents for evidence upload.	PDF, JS, TXT, XLS, JPG, PPT, DOC, ZIP, HTML, PNG
5	Days for Setting Case Due Date	This attribute defines the number of days to be added to calculate the default due date for a case when the case is created. Case due date will be case creation date plus the days entered for setting case due date.	30
6	Transaction History Period	Number of days for the transaction history. This parameter will determine how many days of transaction history the system will display to the investigator.	120
8	Amount Display Format	This parameter specifies the format in which the amount fields should be displayed across the application.	99,999,999,999,999,999.99

Table 4-1   (Cont.) Seeded System Parameters

Parameter ID	Parameter Name	Parameter Description	Parameter Value
9	Number of days for calculating Nearing Due Date cases	This parameter specifies the number of days to be considered for identifying the nearing due date cases.	10
10	Minutes after which locked case should be force unlocked	This parameter specifies the number of minutes to be considered to wait for before force unlocking a locked case. For optimal system behavior, it is recommended to set the value above 15 minutes.	30
11	Case Result Export Limit	This parameter specifies the maximum number of cases which can be exported from the Search Results list.	10000
12	Append User ID with Username	This parameter specifies whether the User ID displays next to the user name in the Investigation Hub UI. Valid values are Y or N. This helps differentiate users with similar names.	N
13	CMCS Manual Quantifind Service	This V_PARAMeter specifies the V_ATTRibutes for the ECM Quantifind batch service. The value of this V_PARAMeter should be set to Y.	Y
14	CMCS Batch Quantifind Service	This V_PARAMeter specifies the V_ATTRibutes for the ECM Quantifind batch service. The value of this V_PARAMeter should be set to Y.	N
15	Kyc Network Graph Node Limit	Number of nodes in Network Diagram. This parameter will determine how many Nodes will be displayed in the Network diagram for KYC Batch Case.	1000

Editing Case System Variables

To edit the default value of a case system parameter, follow these steps:

1. Navigate to the **Case System Parameter List** page.

2. Select a parameter and click **Edit** . The **Edit Case System Parameter** pane is displayed.

3. Edit the system parameter value as required.

> ⓘ **Note**
>
> You can edit only the **Parameter Value**.

4. Click **Save**. A confirmation message is displayed: *Saved Successfully*.

5

Audit History

The Audit History provides to track the record changes made in system configuration.

You can track what field changed, what it changed from and to, who did it, and when. Audit History mainly serves the following purposes:

- Capture a full audit trail of configuration changes to meet legal requirements.
- Assist with system troubleshooting when needed.

You can track changes made to the following Admin screens:
- **Jurisdiction**
- **Security Mappings**
- **Business Domains**
- **Case Priority**
- **Case System Parameters**

Searching Audit History Records

You can search for specific records from the Audit History. You can search by action taken, by time frame (from-to), and by the user who took action.

To search for records, follow these steps:

1. Click **Application Navigation** ☰ icon at the top left corner and the **Navigation List** displays the **Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service** module.

2. Click **Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service**. The menu options are displayed.

3. Click **Application Administration**.

4. Click **Investigation Hub Administration**, and then select **Audit History**. The **Audit History** page is displayed.

5. Select the following details:

    - **Action Taken**: Select one or multiple action types.

    - **Who**: Select a user.

    - **Date From**: This filters the list with the records whose creation date is greater than or equal to the date entered.

    - **Date To**: This filters the list with the records whose creation date is less than or equal to the date entered.

6. Click **Apply**. The Audit History page displays information about the records that match the values you have selected.

7. Click **Reset** to discards the data entered by you and resets the contents to their original state. Saved changes cannot be reset using this option. This is applicable only when you are editing and want to reset the data.

6

Queue Management

As an Admin user, you can view the Case Assignment-related Queues currently available in the System in a tabular format.

When you go to the Queue Management screen, you can view the Queue Name, Mapped User Groups, Queue Created Date, and Queue Created By.

A queue can be viewed as a container that holds cases meeting pre-defined criteria. You must define queues before they can be used. Queues will then need to be mapped to user groups so the filters can be applied. This is a separate activity from defining security mapping. The assigned cases appear in your queue. You can create a new queue and also add from existing queues.

You can look up records using the Queue Name. You can look for queue names in the **Search by Queue Name** search bar. In the **Search Field** text box you can look for user groups. The list can also be sorted by columns.

6.1 Viewing the Queue Management Page

This section describes how to navigate to the Queue Management page.
To view the Queue Management page, follow these steps:

1. Navigate to the **Applications** landing page.

2. Click the Navigation Menu to access the Navigation List. The Navigation List displays the list of modules.

3. Click **Application Administration** and then click **Investigation Hub Administration**.

4. Select **Queue Management**. The Queue Management page opens.

Table 6-1   Queue Management Table Columns and their Description

Columns	Descriptions
Queue Name	Name of Queue. For example: • TM Cases (Filter - Case Type=TM) or • FR_TM_Loan_L1 (Filter - Case Type=TM, Jurisdiction=FR, Business Domain=Loan, Account=1)
Mapped User Groups	Name of mapped User Groups. For example, IHUB Admin User Group or UK_KYC_Manager.
Create Date	Queue create date.
Create By	User who created the Queue.
Actions	Actions you can take on Queues: • Create New Queue • Create Queue Existing

6.2 Creating Queue

You can create a new queue for your cases.
To create a new queue, follow these steps:

1. Navigate to the **Applications** landing page.

2. Click the Navigation Menu to access the Navigation List. The Navigation List displays the list of modules.

3. Click **Application Administration** and then click **Investigation Hub Administration**.

4. Select **Queue Management**. The Queue Management page opens.

5. Click the plus icon to create a queue. The **Create Queue** pop-up appears.

6. Enter the following details:

Table 6-2   Create New Queue Table Fields and their Description

Column	Description
Queue Name	Enter a name for the Queue. It must be a unique name which is not used before.
Select Attributes	Select one or multiple options from the available attributes. For each attribute, you can combine with appropriate operators to create filters as indicated below: • Due In: >, >=, =, <, <= • Scenarios: multi-select list • Primary Entity type: >, >=, =, <, <= • Number of Prior SARs on Primary Entity: >, >=, =, <, <= • Number of events in case: >, >=, =, <, <= • Number of external entity in case: >, >=, =, <, <= • Number of accounts in case: >, >=, =, <, <= • Transaction Amount for TF: <, >, =, >=, <= • Transaction Currency for TF: in, not in • Number of Matches for TF: <, >, =, >=, <=

7. Click **Save**. The Queue is created and displayed in the Queue List.

6.3 Editing an Existing Queue

You can edit an existing queue by changing the Queue Name and its attribute, and save.
To edit an existing queue, follow these steps:

1. Navigate to the Applications landing page.

2. Click the Navigation Menu to access the Navigation List. The Navigation List displays the list of modules.

3. Click **Application Administration** and then click **Investigation Hub Administration**.

4. Select **Queue Management**. The **Queue Management** page opens.

5. Under the Actions column, against an existing queue, click the **Edit** icon. The **Edit Existing Queue** pop-up appears.

6. Make the required changes and click **Save**. The queue is updated and displayed in the Queue List.

> ⓘ **Note**
>
> Any queue edited or deleted shall be impacted on the Queue Management screen.

6.4 Deleting a Queue

You can delete queues when they are no longer required.
To delete a queue, follow these steps:

1. Navigate to the Applications landing page.

2. Click the Navigation Menu to access the Navigation List. The Navigation List displays the list of modules.

3. Click **Application Administration** and then click **Investigation Hub Administration**.

4. Select **Queue Management**. The Queue Management page opens.

5. Under the Actions column, against an existing queue, click the **Delete** icon. The Delete Queue pop-up appears with a confirmation.

6. Click **Delete**. The queue is deleted and removed from the Queue List. The queue also disappears from any existing User Group Queue mappings.

> ⓘ **Note**
>
> Any queue edited or deleted shall be impacted on the Queue Management screen.

6.5 Assigning User Groups to Queues

You can assign user groups to queues as an Admin user so that users in the selected user groups can see those cases in their case list. You can map one or multiple user groups to the selected queue.
After mapping queues to user group, the user in the user group can view the cases in the mapped queues in their case list.

To assign a user group to a queue, follow these steps:

1. Navigate to the Applications landing page.

2. Click the Navigation Menu to access the Navigation List. The Navigation List displays the list of modules.

3. Click **Application Administration** and then click **Investigation Hub Administration**.

4. Select **Queue Management**. The Queue Management page opens.

5. Under the Actions column, against an existing queue, click the Assign to User Group icon. The Assign to User Group popup appears.

6. From the **Select User Group** drop-down, select one or multiple user groups. In the **Search** Field text box you can look for user groups.

7. Click **Save**. The queue is mapped with the selected user groups and displayed in the Queue List.

7

Case Assignment Rules

Case Assignment rules can be configured so that cases are automatically assigned to pre-defined queues.

A queue can be viewed as a container that holds cases meeting pre-defined criteria. You must define queues before they can be used. Queues will then need to be mapped to user groups so the filters can be applied. This is a separate activity from defining security mapping. The assigned cases appear in your queue. You can create a new queue and also add from existing queues.

The UserGroup-Security Mappings are displayed in a tabular format so that you can view the mapping between Casetype-Jurisdiction-BusinessDomain to Usergroup. You can search records by user groups and sort the list by columns. On the Case Assignment Rules page you can search for rules using the Search by User Group filter.

7.1 Viewing the Case Assignment Rules Page

This section describes how to navigate to the Case Assignment Rules page.
To view the Case Assignment Rules page, follow these steps:

1. Navigate to the Applications landing page.

2. Click the Navigation Menu to access the Navigation List. The Navigation List displays the list of modules.

3. Click **Application Administration** and then click **Investigation Hub Administration**.

4. Select **Case Assignment Rules**. The **Case Assignment Rules** page opens.

Table 7-1   Case Assignment Rules Table Columns and their Description

Columns	Description
User Group	Name of User Group. For example, IHUB Admin User Group or UK_KYC_Manager.
Case Type	The case type for cases which can trigger AML_CA case creation. For example, AML_SURV.
Jurisdiction	The jurisdiction, such as geographic locations and legal boundaries, to which the case belongs. For example, AMEA or FR.
Business Domain	Name of Business Domain. For example: Mortgage.

Table 7-1   (Cont.) Case Assignment Rules Table Columns and their Description

Columns	Description
Mapped Queues	List of Mapped Queues. For example: • TM Cases (Filter - Case Type=TM) or • FR_TM_Loan_L1 (Filter - Case Type=TM, Jurisdiction=FR, Business Domain=Loan, Account=1)
Actions	Actions you can take on queues: • Add New Queue • Add From Existing Queues

7.2 Adding a New Queue

You can add a new queue for your cases.
To add a new queue, follow these steps:

1. Navigate to the **Applications** landing page.

2. Click the **Navigation Menu** to access the Navigation List. The Navigation List displays the list of modules.

3. Click **Application Administration** and then click **Investigation Hub Administration**.

4. Select **Case Assignment Rules**. The Case Assignment Rules page opens.

5. Under the **Actions** column, click the three dots and then select **Add New Queue**. The **Add New Queue** page appears.

6. Enter the following details:

Table 7-2   Create New Queue Table Fields and their Description

Column	Description
Queue Name	Enter a name for the Queue. It must be a unique name which is not used before.
Select Attributes	Select one or multiple options from the available attributes. For each attribute, you can combine with appropriate operators to create filters as indicated below: • Due In: >, >=, =, <, <= • Scenarios: multi-select list • Primary Entity type: >, >=, =, <, <= • Number of Prior SARs on Primary Entity: >, >=, =, <, <= • Number of events in case: >, >=, =, <, <= • Number of external entity in case: >, >=, =, <, <= • Number of accounts in case: >, >=, =, <, <=

7. Click **Save**. The Queue is created and displayed in the Case Assignment Rules List.

7.3 Adding from an Existing Queue

You can add a queue to your user group from existing queues.
To add a queue to your user group from existing queues, follow these steps:

1. Navigate to the Applications landing page.

2. Click the Navigation Menu to access the Navigation List. The Navigation List displays the list of modules.

3. Click **Application Administration** and then click **Investigation Hub Administration**.

4. Select **Case Assignment Rules**. The Case Assignment Rules page opens.

5. Under the **Actions** column, click the three dots and then select **Add From Existing Queues**. The Add From Existing Queues appears.

6. From the **Select Queue Name** drop-down, select one or multiple queues.

7. Click **Save**. The queue is mapped with the selected user groups and displayed in the Case Assignment Rules List.

7.4 Editing an Existing Queue

You can edit an existing queue by changing the Queue Name and its attribute, and save.
To edit an existing queue, follow these steps:

1. Navigate to the Applications landing page.

2. Click the Navigation Menu to access the Navigation List. The Navigation List displays the list of modules.

3. Click **Application Administration** and then click **Investigation Hub Administration**.

4. Select **Case Assignment Rules**. The Case Assignment Rules page opens.

5. Select one of records from the Primary Rules list. The record details is displayed in the bottom drawer.

6. Under the Actions column, click the Edit icon. The Edit Existing Queue pop-up appears.

7. Make the required changes and click **Save**. The queue is updated and displayed in the Case Assignment Rules List.

> ⓘ **Note**
>
> Any queue edited or deleted shall be impacted on the Case Assignment Rules screen.

7.5 Deleting Queue Mapping

You can delete queue mapping when they are no longer required.
To delete a queue mapping, follow these steps:

1. Navigate to the Applications landing page.

2. Click the Navigation Menu to access the Navigation List. The Navigation List displays the list of modules.

3. Click **Application Administration** and then click **Investigation Hub Administration**.

4. Select **Case Assignment Rules**. The **Case Assignment Rules** page opens.

5. Select one of records from the Primary Rules list. The User Details page pops up in the bottom drawer.

6. Under the Actions column, click the Delete icon. A confirmation message appears.

7. Click Delete. The mapping between user group and queue is deleted and removed from the Queue List. The queue also disappears from any existing User Group Queue mappings.

> ⓘ **Note**
>
> Any queue edited or deleted shall be impacted on the Case Assignment Rules screen.

8

Exporting and Importing Objects

Object Migration is the process of migrating or moving System Settings and Parameters between environments.

You may want to migrate objects for reasons such as managing global deployments on multiple environments or creating multiple environments so that you can separate the development, testing, and production processes.

You can replicate the System Settings and Parameters from one environment to another without manually re-setting everything to save manual effort and prevent human error.

Prerequisites

- The IHUB Administrator must have access to the Object Migration Admin (OBJMIGADMIN) Group Role before using the Admin Configuration Migration functionality.

- When migrating CM_ADMIN related Objects, if the PMF_PROCESS workflow and User Groups are unavailable in the target environment, you must first migrate the associated PMF_PROCESS workflow and User Groups.

- When migrating IHUB_ADMIN related Objects, if the User Groups are unavailable in the target environment, you must first migrate the associated User Groups.

> ⓘ **Note**
>
> - If User Groups are not available in the target environment, User Groups migration is required for Security Mapping and Case Actions/Statuses.
>
> - Report Types must be migrated from Reference Data upload (applicable for Security Mapping).
>
> **Migrating CM_ADMIN Related Objects**
>
> - The PMF_PROCESS workflow migration is required for Case Actions, Case Statuses, Case Types, Case Priority, and Case Rules and is not required for Business Domain, Case System Parameters, and Jurisdictions.

About Exporting and Importing Objects

You can migrate (import/export) the following Object Types using the Admin Configuration Migration functionality:

- **Schedule**: Schedule provides instructions to schedule the execution of defined processes. When a schedule is migrated, the associated batch is also migrated.

- **Batch**: A batch is a collection of jobs that are planned to run automatically at predetermined intervals without any user input. When a batch is migrated, the batch and the associated pipeline information are migrated.

- **Batch_Group**: A set of individual batches are consolidated to form a single Batch_Group. When migrating a Batch_Group, all the associated batches, tasks, and pipeline information is also migrated.

- **Pipeline**: A pipeline is an embedded data processing engine that runs inside the application to filter, transform, and migrate data on-the-fly. Pipelines are a set of data processing elements called widgets connected in series, where the output of one widget is the input to the next element.

- **Job**: Jobs provide a set of instructions to execute workflow pipelines based on the set threshold values.

- **PMF_Process**: PMF_Processes are defined to sequence the workflow Pipelines of the applications, and to design the artifacts that participate in the Pipelines, to implement the Pipelines. Export of the PMF process will take care of dependent metadata, such as data fields, and transition rules associated with the PMF process, that are defined in PMF.

- **Role**: Roles are used to mapping functions to a defined set of groups to ensure user access system security.

- **Groups**: Groups are used to map Roles. Specific User Groups can perform only a set of functions associated with that group.

- **CM_ADMIN** : The CM_ADMIN object type refers to all the case management-related admin screens in the FCCM Cloud application. Under this object type, you can export case management related admin metadata and settings for Business Domain, Case Actions/ Statuses, Case Priority, Case Rules, Case System Parameters, Case Types, Jurisdictions and Security Mapping.

- **IHUB_ADMIN**: The IHUB_ADMIN object type refers to all the investigation hub-related admin screens in the Investigation Hub application. Under this object type, you can export Investigation Hub related admin metadata and settings for KYC Match Quality Configuration, Default Graph UI Settings, Manage Case Template, Configure Match Quality of Events, Workflow Manager, Case Designer, Security Mapping and Request For Information Management (RFI).

> ⓘ **Note**
>
> If the total file size of the IHUB_ADMIN object type exceeds 500KB, it is advised to export the object categories (code) individually.

8.1 Exporting Objects

To export the objects, follow these steps:

1. Enter the application URL in the browser's URL field. The **Oracle Cloud Account Sign In** window appears.

2. Provide your **User Name** and **Password**.

3. Click **Sign In**. The **Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service** home page appears.

4. Click **Application Navigation** ☰ icon to hide the Application Navigation List.

5. Click **Business Processes** and then click **Admin Configuration Migration**.

6. Select **Export**. The **Object Export Summary** page appears.

   For more information on how to export objects, see Object Export Definitions.

8.2 Importing Objects

To import the objects, follow these steps:

1. Enter the application URL in the browser's URL field. The **Oracle Cloud Account Sign In** window appears.

2. Provide your **User Name** and **Password**.

3. Click **Sign In**. The **Financial Services Analytical Applications** home page appears.

4. Click **Application Navigation** ☰ icon to hide the Application Navigation List.

5. Click **Business Processes** and then click **Admin Configuration Migration**.

6. Select **Import**. The **Object Import Summary** page appears.

   For more information on how to import objects, see Object Import Definitions.