Oracle® Financial Crime and Compliance Management Investigation Hub Cloud Service

Using Investigation Hub Administration Tools

Release 24.2.1
F93447-02
February 2024

Oracle Financial Crime and Compliance Management Investigation Hub Cloud Service Using Investigation Hub Administration Tools, Release 24.2.1

F93447-02

Copyright © 2024, Oracle and/or its affiliates.

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.

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`.

Contents

Preface

Using Investigation Hub Administration describes how to configure the case status, actions, and types used in Process Modeling Framework (PMF) to define the case investigation workflow.

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 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.

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

This section includes the following topics:

- Getting Started includes instructions on how to login to the application.
- Case Statuses explains how to add and edit case statuses.
- Case Actions explains how to add and edit actions.
- Mapping Case Actions explains how to map Non-Status Changing Case Actions to statuses and user roles.
- Configure Case System Parameters explains how to edit the case system parameters.
- Case Priority explains how to add and edit Case Priority.
- Admin Audit History explains how to track the record changes made in system configuration.
- Exporting and Importing Objects explains how to migrate the objects.

About Investigation Hub Administration

Investigation Hub Administration Tools help you to configure the case status, actions, and types used in Process Modeling Framework (PMF) to define the case investigation workflow. To define a case workflow, you must complete the following tasks:

- Define Case Statuses that represent steps in the workflow.
- Define Case Actions to be used in the workflow.

Investigation workflows 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 workflows using the Processing Modelling Framework.

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).

Administration and Configuration Activities

The Administration and Configuration Activities of the Investigation Hub application include:

- Case Actions settings to add new case statuses, configure case action data, and configure standard comment data. The Administrator can configure whether or not the case actions require a comment, a reassignment, or a due-date.
- Processing Modelling Framework 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 workflows.

2
Getting Started

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

Accessing Investigation Hub Administration

To access the application, 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 **Investigation Hub Administration**.

3
Case Statuses

Case statuses help users navigate cases as they progress through the workflow towards investigation and resolution.

A case status is associated to a workflow action; when an action is executed, the status of a case changes. For example, when an Analyst recommends a case for closure to the Supervisor, the case status changes from **Investigation** to **Recommend for Closure**.

Administrators can add a new case status code based on the following pre-existing case status types:

- **New**: Cases not assigned to any user yet.
- **Assigned**: Cases assigned to users but not under investigation.
- **Investigation**: Cases assigned to users and are under investigation.
- **Under Review**: Cases for which recommendations are made, but not yet approved by the Case Supervisor.
- **Closed**: Cases closed without requiring any further action, or with recommendation for further action to be taken, or, after generating a Compliance Regulatory Reporting (CRR) report.

All Case workflows must contain the following statuses; New, Assigned and Investigation. This can be copied from the Out Of Box Workflow.

The newly added case status can be used in PMF to enhance your workflow. For more information, see Process Modeling Framework.

3.1 Add a New Case Status

To add a new Case Status, follow these steps:

1. Navigate to the **Applications** landing page.
2. Click the **Application Navigation** ≡ icon to access the **Navigation List**. The Navigation List displays the list of modules.
3. Select **Investigation Hub Administration**, and then select **Case Actions/Statuses**. The Case Action/Statuses page is displayed.
4. Select the **Case Statuses** tab.
5. Click **Add** +. The **Add New Status** window displays.
6. Enter the parameters as described in the following table.

Table 3-1 Add New Status - Field Description

Field	Description
Status Code	Enter the status code of case. These Status Codes are used as stages in the PMF workflow, moving the case through the workflow. This field accepts only alphanumeric and hyphen values. Other special characters are not allowed. This code cannot be edited after the case status has been added.
Status Name	Enter the new status name.
Status Type	Select the appropriate status type for the status code from the drop-down list. Status Types are used to group multiple similar statuses. You must have at least one code in the PMF workflow as the Starting status type. You can have multiple status codes for Close status types.

7. Click **Save**. A confirmation message is displayed: *Added Successfully*.

3.2 Edit Case Status

To edit a user-defined Case Status, follow these steps:

1. Navigate to the **Case Actions/Statuses** page.
2. Select the **Case Statuses** tab. Select the **Status Code** and click **Edit** ✎. The Edit Status window is displayed.
3. Edit the **Status Type** and **Status Name** as required.

> **Note:**
>
> You cannot edit the **Status Code**.

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

> **Note:**
>
> If you have configured the out-of-the-box case status ‘Pending Review’ (PNDR) in the Case Workflow, the ‘Review in Progress’ (RNPR) case status must be the next connected status. Cases are completely disabled in PNDR status and become enabled only when the Reviewer opens the case to trigger the update in the Case Workflow from PNDR status to RNPR status.

4
Case Actions

Case Actions allow users to move cases through the workflow, including analysis, providing evidence, and making recommendations.

Administrators create and define case actions, map the action to statuses and then create the workflow using PMF.

During action definition, Administrators make decisions like whether the case action requires a comment, a reassignment, or a due date. You can allow multiple actions to be taken simultaneously by setting the Action Order, dictate whether the action will update the case status, and so on. After defining the actions, you must map them to a status, case type, and user role. For more information, see Mapping Case Actions.

You can create and define actions in the following categories:

- Email
- Evidence
- Assign
- Escalate
- Resolution
- Research & Review
- Monitor
- Export
- Print
- Reopen
- Due Date

4.1 Add a New Case Action

> **Note:**
>
> Adding new case action is not supported in this release.

To add a new Case Action, follow these steps:

1. Navigate to the **Case Actions/Statuses** page.
2. Select the **Case Actions** tab.
3. Click **Add** ＋. The **Add New Action** window is displayed.
4. Enter one or multiple parameters as described in the following table.

Table 4-1 Add New Action - Field Description

Field	Description
Action Category	Select the Category within which this action is displayed on the Take Action window. This cannot be edited after the action has been added. For example, the **Send Email** action is in the **Email** category. Action categories allow you to segment actions into logical groups for easy reading on the UI. This does not affect the action in any way.
Action Code	Enter a new action code. This is the unique code of the action that identifies the action. For example, CA123. This code is not displayed on the UI. This cannot be edited after the action has been added.
Action Name	Action name that is displayed on the UI, except for the **Audit History** window.
Action Name on Audit History	Action name that is displayed on the **Audit History** window.
Action Order	The order used to display status and non-status changing actions on the **Take Action** window of Case Investigation when multiple actions are taken together. A lower number indicates higher precedence on the **Take Action** window. This ordering can also include the Action Category. For example, if the **Resolution** action category has three different actions, then the action with the lowest order number is displayed first on the **Take Action** window. This allows multiple actions with different resulting statuses to be taken at the same time and enforces that the action with the highest action order will be the one to affect the resulting status. For example, an action with resulting status Print has action order 10. It is taken at the same time as an action with resulting status Closed that has action order 20. Both actions will be applied and visible in the Audit. The resulting status will be Closed. NOTE: The action order of client-created actions should be lower than the action order of system-initiated actions for Reassignment (CA202A) and Ownership Change (CA103S).
Default Due Date	Enter the number of days after this action is taken that the case will become due. The due date will be assigned to the case as the System Date + Number of days defined here.
Status Changing Action	Select whether this action should change the case status. This is mandatory for Investigation Hub processing. It is recommended that the resulting status defined here is the same that is defined in PMF.
Action Description	Enter comments when adding this action. This must be provided for auditing purposes.

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

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

4.2 Edit Case Action

To edit an existing Case Action, follow these steps:

1. Navigate to the **Case Actions/Statuses** page.
2. Select the **Case Actions** tab.
3. Select the Action Code and click **Edit** ✎. The **Edit Action** window is displayed.
4. Edit the Case Action details as required.

> **Note:**
>
> - You cannot edit the **Action Code** and **Action Category** fields.
> - The fields which are marked with asterisk * are mandatory.

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

5

Mapping Case Actions

This topic provides information about mapping case actions to user roles and case statuses.

Administrators use the **Actions Mapping** tab to map Non-Status Changing Case Actions to user roles, and case statuses. Mapping actions in this way allows you to restrict which actions are available for users to move cases through the workflow.

5.1 Mapping Actions to Statuses

When you map Case Statuses to an Action, then that action is only available when a case is in the mapped statuses.
To map the Action to a Status, follow these steps:

1. Navigate to the **Case Actions/Statuses** page.
2. Select the **Actions Mapping** tab.
3. Select the Action from the **Select Non-Status Changing Case Action** drop-down list. The Selected Statuses list is updated with all the available statuses.
4. Select the Status from the **Available Statuses** list and move to the **Selected Statuses** list. You can move multiple statuses at once by using either the Ctrl or Shift button and selecting multiple (or all) statuses from the **Available Statuses** list and clicking **Select** › . You can move all statuses by clicking **Select All** » .
5. Click **Save**. A confirmation message is displayed: *Saved Successfully*.
6. 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.

5.2 Mapping Actions to User Roles

When a User Role, such as Supervisor or Analyst, is mapped to an Action, then that particular User Role is allowed to perform the mapped action. Each Action can be mapped to multiple User Roles. User Roles must also be mapped to an appropriate User Group. For more information, see Identity Management.

To map the Action to a User Role, follow these steps:

1. Navigate to the **Case Actions/Statuses** page.
2. Select the **Action Mapping** tab.
3. Select the Action from the Select Non-Status Changing Case Action drop-down list. The **Selected User Role** list is updated with all the available User Role.
4. Select the User Role from the **Available User Role** list and move it to the **Selected User Role** list. You can move multiple User Roles at once by using either the Ctrl or Shift

button and selecting multiple (or all) user roles from the **Available User Roles** list and clicking **Select** ›. You can move all statuses by clicking **Select All** »

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

6. 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

Mapping Action Reasons

The Action Reason Mapping feature allows the Administrators to map reasons to status changing actions related to case type. Action reasons are shown under the Reason drop-down in the Take Action pop-up window whenever the status changing action is selected. Administrators can also designate whether or not report generation is required for the particular action reason and configure the necessary report type.

> **Note:**
>
> When migrating Action Reason Mapping, you must first migrate the associated PMF_PROCESS workflow.

6.1 Adding Action Reasons

To add an action reason, follow these steps:

1. Navigate to the **Case Actions/Statuses** page.
2. Select the **Action Reason Mapping** tab.
3. Select the Case Type from the **Select Case Type** drop-down list. The **Action List** is displayed.
4. Under **Action List**, click **Expand** ‹. The Action is expanded.
5. Click **Add** +. The **Add Reason** window opens.
6. Enter the fields as described in the following table.

Table 6-1 Add Reason - Field Description

Field	Description
Reason Name	Enter a name for the reason.
Reason Description	Enter a description for the reason.
Report Generation Required	Select this check box, if you want to generate a report. When you select the check box, the **Report Type** drop-down appears. From the **Report Type** drop-down, select an option.

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

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

6.2 Editing Action Reasons

To edit an action reason, follow these steps:

1. Navigate to the **Case Actions/Statuses** page.
2. Select the **Action Reason Mapping** tab.
3. Select the Case Type from the **Select Case Type** drop-down list. The **Action List** is displayed.
4. Under **Action List**, click **Expand** < . The Action is expanded.
5. Click **Edit** ✎. The **Edit Reason** window opens.
6. Edit the Action Reason details as required.

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

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

6.3 Deleting Action Reasons

To delete an action reason, follow these steps:

1. Navigate to the **Case Actions/Statuses** page.
2. Select the **Action Reason Mapping** tab.
3. Select the Case Type from the **Select Case Type** drop-down list. The **Action List** is displayed.
4. Under **Action List**, click **Expand** < . The Action is expanded.
5. Click **Delete** 🗑. A confirmation message appears.
6. Click **OK** to delete the action reason. A confirmation message is displayed: *Deleted Successfully*.

7 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 7-1 Seeded System Parameters

Parameter ID	Parameter Name	Purpose	Default Values
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.	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.	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
7	Amount Display Format	This parameter specifies the format in which the amount fields should be displayed across the application.	99,999,999,999,999,999,999.99
8	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

Table 7-1 (Cont.) Seeded System Parameters

Parameter ID	Parameter Name	Purpose	Default Values
9	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
10	Case Result Export Limit	This parameter specifies the maximum number of cases which can be exported from the Search Results list.	10000
11	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
12	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 System Parameter** window is displayed.
3. Edit the System Parameter Value as required. You can edit only the Parameter Value.
4. Click **Save**. A confirmation message is displayed: *Saved Successfully*.

8 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 **Applications** landing page.
2. Click the **Application Navigation** ☰ icon to access the Navigation List. The Navigation List displays the list of modules.
3. Select **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.

8.1 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 8-1 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.

8.2 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.

8.3 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.

9

Admin Audit History

The Admin Audit History records change made in system configuration.

You can track what field changed, what it changed from and to, who did it, and when. Admin 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 Statuses**
- **Case Actions (Action Tab, Action Mapping Tab, and Action Reason Mapping Tab)**
- **Case Priority**
- **Case System Parameters**

Searching Admin Audit History Records

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

To search for records, follow these steps:

1. Navigate to the **Applications** landing page.
2. Click the **Application Navigation** ≡ icon to access the Navigation List. The **Navigation List** displays the list of modules.
3. Select **Investigation Hub Administration**, and then select **Audit History**. The **Audit History** page opens.
4. Select and enter 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.
5. Click **Apply**. The Audit History page displays information about the records that match the values you have entered/selected.

6. 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.

10

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 and IHUB_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.

> **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.
>
> **Migrating IHUB _ADMIN Related Objects**
>
> - The PMF_PROCESS workflow migration is required for the Manage Case Template and not required for Default Graph UI Settings and Configure Match Quality of Events.

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 Default Graph UI Settings, Manage Case Template and Configure Match Quality of Events.

10.1 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 **Financial Services Analytical Applications** home page appears.
4. Click **Application Navigation** ≡ icon to hide the Application Navigation List.
5. Click **Admin Configuration Migration** and then select **Export**. The **Object Export Summary** page appears.

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

10.2 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 **Admin Configuration Migration** and then select **Import**. The **Object Import Summary** page appears.

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