Oracle® FCCM Investigation Hub Cloud Service

User Roles and Privileges

Release 26.08.01
G29434-13
August 2026

Oracle FCCM Investigation Hub Cloud Service User Roles and Privileges, Release 26.08.01

G29434-13

Contents

Preface

User Roles and Privileges provides information about mapping users, groups, roles, and functions to access the application.

Audience

This document is intended for users who are responsible for provisioning and activating Oracle FCCM Investigation Hub 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

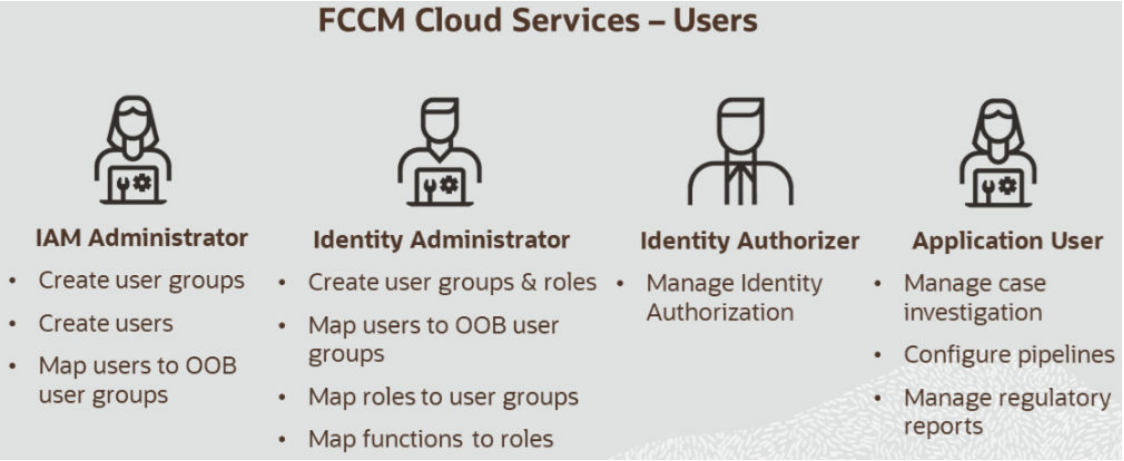
User Roles and Privileges

This topic provides information about mapping users, groups, roles, and functions to access the application.

In Oracle Financial Crime and Compliance Management Cloud Service, users have roles through which they gain access to functions and data.

Users can have any number of roles. The following figure shows the User Persona Details.

Figure 1-1 FCCM Cloud Services Users



> **Note**
>
> User-Group mapping changes from Identity Access Management will take time to sync with application. If these changes are made during an active user session then it will be reflected on next login.

About User Access Mapping

In order to allow users to access functions in the application, Administrators must classify users and the functions they are permitted to access.

The Functions imply controlling various actionable units in the application via functional access. For example, create a case, add a customer, add an account, and so on. Users are mapped to groups, which must be mapped to specific security attributes, such as Business Domain and Jurisdiction. Groups are mapped to Roles, and Roles are mapped to Functions. Users can perform activities associated with their user group throughout the functional areas of the application. Before mapping security attributes, you must complete the following:

1. Create users

2. Map users to user groups
3. Create business domain
4. Create jurisdictions
5. Map user groups to security attributes

Security within the Application

Security layers control how you interact with the application. Users may only access cases that are mapped to their user group. For more information about mapping users to user groups, see Provision Users.

Table 1-1 Security Details within the Application

Security Layer Type	Controls	Description
Roles	Access to Features and Functions	User roles identify which features and functions the user can access within the application. For example, Case Analysts can access and take action on cases.
Business Domains	Access to Case and Business Information	You can restrict access along operational business lines and practices, such as Retail Banking. Users can only see cases that are assigned to at least one of the business domains their user group is mapped to.
Jurisdictions	Access to Case Information	You can restrict access using geographic locations and legal boundaries. Users can only see cases that belong to the jurisdiction their user group is mapped to.

Role-Based Access Control

Role-based security in Oracle Financial Services Crime and Compliance Management Cloud Service controls who can do what on which data.

Role-based access allows you to configure the following:

- **Who**: The role assigned to a user.
- **What**:The functions that users with the role can perform.
- **Which Data**: The set of data that users with the role can access when performing the function.

2

User Group and Roles Mapping

This topic provides the User Group, User Role mapping, and activities for Oracle FCCM Investigation Hub Cloud Service.

User Group and Roles Mapping in Oracle FCCM Cloud Service

This table shows the User Groups and Roles required for activation of Oracle FCCM Cloud Service.

Table 2-1 User Group and Roles Mapping in Oracle FCCM Cloud Service

Group	User Role	Functions
Identity Administrator	Identity Administrator	• View the reports • View the object storage • View the OAUTH credentials • Perform the Identity and access management operations
Identity Authorizer	Identity Authorizer	Authorize the Identity and access management operations
IAM Administrator	IAM Administrator	• Create users • Map users to IDNTY_ADMIN group • Map users to IDNTY_AUTH group

> **Note**
>
> The new user should have the following roles to access Home page of the Cloud application.
>
> - Function read role
> - Group read role
> - User read role
> - Role read role

User Group and Roles Mapping in Investigation Hub Cloud Service

This table shows User Groups and Roles required for accessing the Investigation Hub Cloud Service.

Table 2-2 User Group and Roles Mapping in Investigation Hub Cloud Service

Group	User Role	Functionality
IHUB Administrator Group	IHUB Administrator	• Configure case statuses • Configure case actions • Add New Case Type • Add correlation rules • Set priority level for Currency Transaction Reporting (CTR) reports • Configure Event Decisions • Configure Default Graph UI Settings • Configure Match Quality for Customer Screening Events and KYC events • Manage Case Template • Manage Questionnaires • Set Transaction Filtering Case Closure Configuration • Configure Workflow Designer
IHUB Analyst Group	IHUB Analyst	• Search for cases • Investigate cases • Generate Dossier • Recommend case closure • Request for Information (RFI)
IHUB Supervisor Group	IHUB Supervisor	• Overwrite updates made by Analyst • Search for cases • Investigate cases • Generate Dossier • Approve or reject recommendations to close cases • Close cases • Request for Information (RFI)
IHRTANALYSTGRP	IHRTCSANALYST	Users have access for screening entities or individuals and creating cases.
IHTFANALYSTGRP	IHTFANALYST	User added to this group has to mandatory review all the events before closing a case, and can escalate, recommend block and recommend release of cases.
IHTFSUPERVISORGRP	IHTFSUPERVISOR	User added to this group has to mandatory review all the events before closing a case, and can release, reject and block a case.
IHUSCTRMENUGRP	IHUSCTRMENU	Users added to this group get the ihub Currency Transaction Reporting menu.
NA	IHRTCSSCREEN	Users with this role can screen entities or individuals in Real-Time Customer Screening.

Table 2-2 (Cont.) User Group and Roles Mapping in Investigation Hub Cloud Service

Group	User Role	Functionality
NA	IHRTCSCREATE	Users with this role can access only screening history and create cases from screened records in Real-Time Customer Screening. **Note** If admin has disabled the Enable Screening History Access toggle button from the Customer Screening Configurations page, the screening history page in Real-Time Customer Screening is not available.
Custom Group	Custom Role	Create custom group and custom role and provide the following roles and functions for users to view iHUB cases. For example, create a custom user group (IHUBVIEWGRP) with the following roles: • FUNC_READ • GRP_READ • USR_READ • ROLE_READ • IHUBVIEWROLE And, create a custom role (IHUBVIEWROLE) with the following functions: • IHCASELIST • IHCASEINV • OFS_AMLCS

Table 2-2 (Cont.) User Group and Roles Mapping in Investigation Hub Cloud Service

Group	User Role	Functionality
IHRTANALYSTGRP	IHRTCSSCREENINGHISTORY	This role is required to access the Screening History UI in the IHUBRT application. By default the IHRTCSSCREENINGHISTORY role is mapped to the IHRTANALYSTGRP group, so existing RTCS analyst users will have access to the **Screening History** tab by default.

Table 2-3 User Privileges in Investigation Hub

Privileges	Case Supervisor	Case Analyst
Access Cases	x	x
Search for Cases	x	x
View Case List	x	x
View Case Summary	x	x
View Event Details	x	x
Set Event Decision	x	x
Generate Dossier	x	x
View/Expand Graph	x	x
View Graph History	x	x
Edit Graph Settings	x	x
View Alerted transactions	x	x
Add/View Accounts	x	x
Add/View Customers	x	x
Add/View Transactions	x	x
Add/View External Entities	x	x
View Related Case	x	x
View Related Events	x	x
Set Case Assignee	x	x
Recommend Close without Regulatory Report		x
Recommend Close with Regulatory Report		x
Reject Recommendation	x	
Close a Case as False Positive	x	
Close a Case as True Positive	x	
View Evidence (Attachment and Comment list)	x	x
Add Document	x	x
View Attachments	x	x
Add/Edit Narrative	x	x
View Narrative	x	x
Add Investigation Comments	x	x
Generate CRR Reports	x	
Save Search Criteria of Case List	x	x
Export Case List in Excel	x	x

Table 2-3 (Cont.) User Privileges in Investigation Hub

Privileges	Case Supervisor	Case Analyst
Export Transactions in Excel	x	x
Cancel Filing	x	x
Request for Approval		x
Approve	x	
Real-Time Customer Screening		x

Table 2-4 User Privileges in Investigation Hub Administrator

Privileges	Case Administrator
Add Case Status	x
Edit/Delete Case Status	x
Add Case Action	x
Edit/Delete Case Action	x
Add Case Action Reason	x
Edit/Delete Case Action Reason	x
Mapping Case Type to Workflow	x
Add New Configuration to Workflow	x
Edit/Delete Workflow Configuration	x
Configuring Case System Parameters	x
Add Business Domains	x
Edit Business Domains	x
Add Jurisdictions	x
Edit Jurisdictions	x
Configuring Security Mappings	x
Manage Case Template	x
Create Case Template	x
Edit/Delete Case Template	x
Configure Default Graph UI Settings	x
Configure Match Quality of Events	x
Add Case Type	x
Edit Case Type	x
Add Correlation Rule	x
Edit Correlation Rule	x

User Group and Roles Mapping for Transaction Monitoring Cloud Service

This table shows the User Groups and Roles required for Transaction Monitoring Cloud Service.

Table 2-5 User Group and Roles Mapping for Transaction Monitoring Cloud Service

Group	User Role	Functionality
Pipeline Administrator Group	Pipeline Administrator	• Configure pipelines • Configure threshold sets

Table 2-5 (Cont.) User Group and Roles Mapping for Transaction Monitoring Cloud Service

Group	User Role	Functionality
Threshold Administrator Groups	CS Administrator	Load watch list data

User Group and Roles Mapping for Scheduler Service

This table shows the User Groups and Roles required for Scheduler Service in Investigation Hub.

Table 2-6 User Group and Roles Mapping for Scheduler Service

Group	User Role	Functionality
Job Administrator Group	Job Administrator	Manage jobs
Scheduler Administrator Group	Scheduler Administrator	Manage batches

User Group and Roles Mapping for Process Modelling Framework (PMF)

This table shows the User Groups and Roles required for Process Modelling Framework (PMF) in Investigation Hub.

Table 2-7 User Group and Roles Mapping for Process Modelling Framework (PMF)

Group	User Role	Functionality
IHUB Administrator Group	Manage Workflow Monitor	Access the Manage Workflow Monitor window. **Note:** The mapping of this role does not allow view, edit, and add actions.
IHUB Administrator Group	Workflow Access	Access the Process Modeller menu from the Navigation Tree. **Note:** The mapping of this role does not allow view, edit, and add actions.
IHUB Administrator Group	Workflow Monitor Access	Access the Process Monitor window. **Note:** The mapping of this role does not allow view, edit, and add actions.
IHUB Administrator Group	Workflow Read	View the PMF workflow
IHUB Administrator Group	Workflow Write	Perform view, edit, and add actions in PMF

> **Note**
>
> Administrators must be mapped to all the roles described in the preceding table to allow them to perform these operations in PMF.

3

Using Investigation Hub Documentation

Oracle FCCM Investigation Hub Cloud Service documentation helps you activate and use your subscription.

Table 3-1 Investigation Hub Workflow

Sequence	Action	Functions
1	Subscription	Activating Subscription
2	User Authentication	• Create users • User group and role mapping
3	Data Loading	Upload required data files to Object Store
4	Application Security Mapping	• Business Domains • Jurisdiction • Mapping of Security Attributes
5	Configure Transaction Monitoring Administration	• Copy Scoring Pipeline • Add threshold for the new jurisdiction • Create a job for this new threshold • Add this job to the applicable batch • Update Scoring Pipeline with new threshold • Execute the batch
6	Configure Investigation Hub Administration	• Configure Case Priority • Configure Case System Parameters • Audit History • Queue Management • Case Assignment • Export Objects • Import Objects
7	Accessing Investigation Hub Administration	• Configure Workflow Designer • Configure Case Designer • Set CTR priority • Currency Transaction Reporting Administration • Customer Screening Configurations • Default Graph UI Settings • KYC Match Quality Configuration • Manage Case Templates • Manage RFI and Notification Configurations • Transaction Filtering Configuration • Configure PMF • Implement PMF using Case Types UI

Table 3-1 (Cont.) Investigation Hub Workflow

Sequence	Action	Functions
8	Batch Processing	• Data Preparation • Data Uploading • Data Processing • Execute Batches
9	Investigating Cases	• Analyzing the case • Create Dossier • Override KYC Risk Score • View watchlist details • Upload evidence • Updating case status • Assigning the case • Updating narrative • Updating case priority • Adding transactions for CS cases • Request for Information • Link or merge or close duplicate cases • Close the case
10	Generating CTR Reports	Generating the report

Investigation Hub for Real-Time Screening Workflow

Table 3-2 Real-Time Screening Workflow

Sequence	Action	Functions
1	Subscription	Activating Subscription
2	User Authentication	• Create users • User group and role mapping
3	Add Watchlist Management	• Manage Private Watch List • Manage Synonym Words
4	Performing Real-Time Screening	• Screening Individual/Entity records • Create Real-Time screening cases