# Oracle® FCCM Investigation Hub Cloud Service

## User Roles and Privileges

Release 24.02.01
F93451-03
February 2024

Oracle FCCM Investigation Hub Cloud Service User Roles and Privileges, Release 24.02.01

F93451-03

# 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 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

# Overview of Securing Oracle FCCM Cloud Service

Oracle Financial Services Crime and Compliance Management Cloud Service is secure as delivered. This guide explains how to enable user access to Oracle Financial Services Crime and Compliance Management Cloud Service functions and data. You perform some of the tasks in this guide either only or mainly during implementation. Most, however, can also be performed later and as requirements emerge. This topic summarizes the scope of this guide and identifies the contents of each chapter.

The Oracle Financial Services Crime and Compliance Management Cloud Service is a platform for hosting software as a service (SaaS) applications and this platform provides a secure consistent environment for the deployment and operation of SaaS applications. It also provides unified security features to all services deployed on the platform in the areas of user identity management and the management of access entitlements provisioned to users.

# 2 Application User Setup

### Overview of Application Users

During implementation, you prepare your Oracle Applications Cloud service for application users. Decisions made during this phase determine how you manage users by default. Most of these decisions can be overridden. However, for efficient user management, you're recommended to configure your environment to both reflect enterprise policy and support most or all users.

For more information, see the User Summary Page and User Roles and Privileges.

### Creating Users

During implementation, you can use the Create User task to create test application users. By default, this task creates a minimal person record and a user account. After implementation, you should use the Hire an Employee task to create application users. The Create User task isn't recommended after implementation is complete. This topic describes how to create a test user using the Create User task.

For more information, see the Creating the Application Users.

# 3

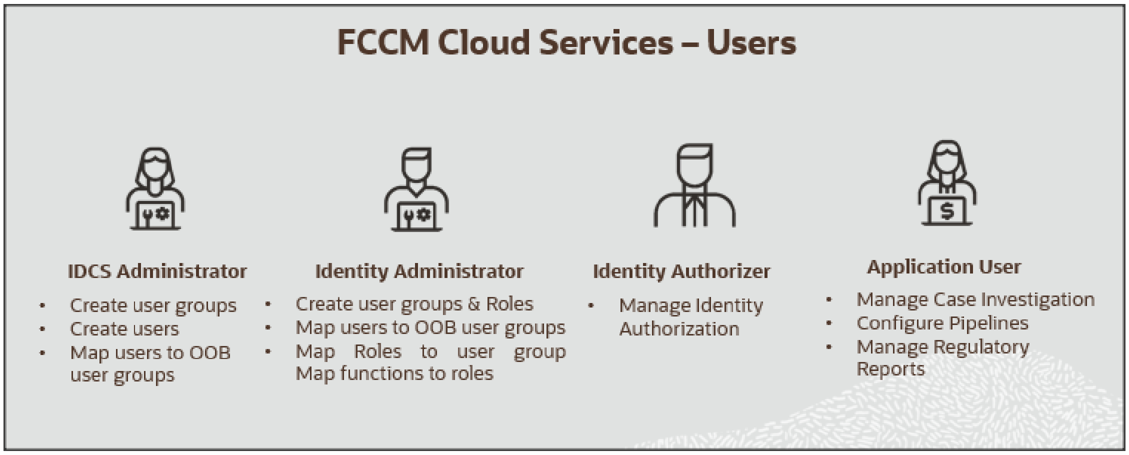
# User Roles and Privileges

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 3-1    User Persona Details**



FCCM Cloud Services – Users

IDCS Administrator

- Create user groups
- Create users
- Map users to OOB user groups

Identity Administrator

- Create user groups & Roles
- Map users to OOB user groups
- Map Roles to user group Map functions to roles

Identity Authorizer

- Manage Identity Authorization

Application User

- Manage Case Investigation
- Configure Pipelines
- Manage Regulatory Reports

**Note:**

User-Group mapping changes from IDCS will take 5 minutes to sync with application. If these changes are made during active user session then it will be reflected on next login.

### 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.

**Table 3-1    Role-based Access Control**

| Component | Description |
|---|---|
| Who | Is a role assigned to a user? |
| What | Is a function that users with the role can perform? |
| Which Data | Is the set of data that users with the role can access when performing the function? |

**Table 3-2 Examples of Role-based Access Control**

| Who | What | Which Data |
|---|---|---|
| Data Administrator | Can perform Data Preparation and ingestion | Business Data |
| Case Analyst | Can view cases and update cases | Business and Operational Data |

> **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

### 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, etc.

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 users interact with the application.

**Table 3-3 Security Layer**

| 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.<br>For example, Case Analysts can access and take action on cases. |

**Table 3-3 (Cont.) Security Layer**

| Security Layer Type | Controls | Description |
|---|---|---|
| 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. |

### User Group and Roles Mapping in Oracle FCCM Cloud Service

The following table provides the User Group, User Role mapping, and activities.

**Table 3-4 User Group and Roles Mapping for Investigation Hub**

| Group | User Role | Functionality |
|---|---|---|
| Identity Administrator | Identity Administrator | • View the reports<br>• View the object storage<br>• View the OAUTH credentials<br>• Perform the Identity and access management operations |
| Identity Authorizer | Identity Authorizer | Authorize the Identity and access management operations |
| IDCS Administrator | IDCS Administrator | • Create users<br>• Map users to **IDNTY_ADMIN** group<br>• Map users to **IDNTY_AUTH** group |
| IHUB Administrator Group | IHUB Administrator | • Configure jurisdictions and business domains<br>• Configure case statuses<br>• Configure case actions<br>• Configure case system parameters<br>• Configure Default Graph UI Settings<br>• Manage Case Template |
| IHUB Analyst Group | IHUB Analyst | • Search for cases<br>• Investigate cases<br>• Generate Dossier<br>• Recommend case closure |
| IHUB Supervisor Group | IHUB Supervisor | • Overwrite updates made by Analyst<br>• Search for cases<br>• Investigate cases<br>• Generate Dossier<br>• Approve or reject recommendations to close cases<br>• Close cases |

### Table 3-5 Transaction Monitoring User Groups (TM Group - OFS_TM)

| Group | User Role | Functionality |
|---|---|---|
| Pipeline Administrator Group | Pipeline Administrator | • Configure pipelines<br>• Configure threshold sets |
| Threshold Administrator Groups | CS Administrator | Load watch list data |

### Table 3-6 Scheduler Service User Groups

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

### Table 3-7 Process Modelling Framework (PMF) User Groups

| Group | User Role | Functionality |
|---|---|---|
| IHUB Administrator Group | Manage Workflow Monitor | Access the Manage Workflow Monitor window.<br>**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.<br>**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.<br>**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.

## User Roles in Investigation Hub

### Table 3-8 User Roles for Case Analyst and Supervisor

| Privileges | Case Supervisor | Case Analyst |
|---|---|---|
| Access Cases | x | x |
| Search for Cases | x | x |
| View Case List | x | x |
| View Case Summary | x | x |

**Table 3-8 (Cont.) User Roles for Case Analyst and Supervisor**

| Privileges | Case Supervisor | Case Analyst |
|---|---|---|
| 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 |
| Export Transactions in Excel | x | x |

## User Roles in Investigation Hub Administrator

**Table 3-9 User Roles in Investigation Hub Administrator**

| Privileges | Case Admin |
|---|---|
| Add Case Status | x |
| Edit Case Status | x |
| Add Case Action | x |
| Edit Case Action | x |
| Mapping the Action to Status | x |
| Mapping the Action to User Role | x |
| Configuring Case System Parameters | x |
| Add Business Domains | x |

**Table 3-9 (Cont.) User Roles in Investigation Hub Administrator**

| Privileges | Case Admin |
|---|---|
| Edit Business Domains | x |
| Add Jurisdictions | x |
| Edit Jurisdictions | x |
| Configuring Security Mappings | x |
| Manage Case Template | x |
| Create Case Template | x |
| Update Case Template | x |
| Delete Case Template | x |
| Configure Default Graph UI Settings | x |

4

# Using Investigation Hub Documentation

This topic describes workflow for the Investigation Hub.

**Table 4-1 Workflow for Investigation Hub**

| Workflow Process | Functionality |
|---|---|
| Subscription | Activating Subscription |
| User Authentication | • Create users<br>• User group and role mapping |
| Data Loading | Upload required data files to Object Store |
| Application Security Mapping | • Business Domains<br>• Jurisdiction<br>• Mapping of Security Attributes |
| Configure Transaction Monitoring Administration | • Copy Scoring Pipeline<br>• Add threshold for the new jurisdiction<br>• Create a job for this new threshold<br>• Add this job to the applicable batch<br>• Update Scoring Pipeline with new threshold<br>• Execute the batch |
| Configure Investigation Hub Administration | • Configure Status and Actions<br>• Map of Case Action to Status, Case Type, user role<br>• Configure PMF<br>• Implement PMF using Case Types UI |
| Batch Processing | • Data Preparation<br>• Data Uploading<br>• Data Processing<br>• Execute Batches |
| Investigating Cases | • Analyzing the case<br>• Create Dossier<br>• Close the case |
| Generating CRR Reports | Generating the report |