Oracle® FCCM Transaction Monitoring Cloud Service

User Roles and Privileges

Release 24.02.01
G10716-01
February 2024

Oracle FCCM Transaction Monitoring Cloud Service User Roles and Privileges, Release 24.02.01

G10716-01

Primary Authors: (primary author), (primary author)

Contributing Authors: (contributing author), (contributing author)

Contributors: (contributor), (contributor)

Contents

Preface

Getting Started with Transaction Monitoring describes how to access the Oracle FCCM Transaction Monitoring Cloud Service.

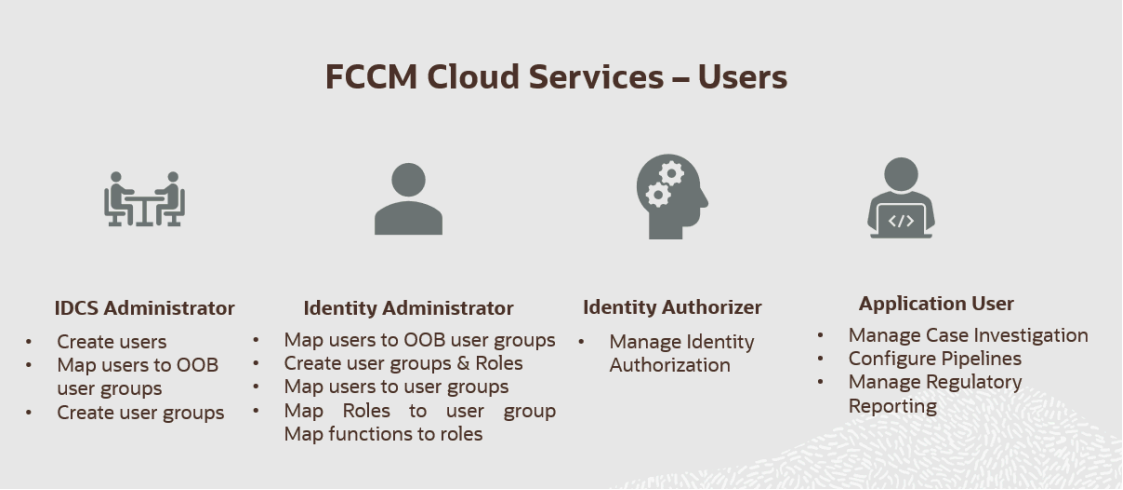
1

User Roles and Privileges

In Oracle Financial Services 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 Service Users



> **Note:**
>
> User-Group mapping changes from IDCS will take 5 minutes 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 domains,
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	This security layer identifies 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. For more information about Business Domains, see Create business domains.
Jurisdictions	Access to Case Information	You can restrict access using geographic locations or legal boundaries. Users can only see cases that belong to the jurisdiction their user group is mapped to. For more information about Jurisdictions, see Configuring Jurisdictions.

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.
- Data Administrators can perform Data Preparation and Ingestion using Business data
- Case Analysts can view cases using Business and Operational data

2

User Group and Roles Mapping

This section provides the User Group, User Role mapping, and activities for Oracle FCCM Transaction Monitoring 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 reports • View the object storage • View the OAUTH credentials • Perform Identity and Access Management operations
Identity Authorizer	Identity Authorizer	Authorize the Identity and access management operations
IDCS Administrator	IDCS Administrator	• Create users • Map users to IDNTY_ADMIN group • Map users to IDNTY_AUTH group

User Group and Roles Mapping in Transaction Monitoring Cloud Service

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

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

Group	User Role	Functions
Pipeline Administrator Group	Pipeline Administrator	• Configure pipelines • Configure threshold sets View reports
Threshold Administrator Groups	CS Administrator	Load watch list data

User Group and Roles Mapping for Case Management

This table shows the User Groups and Roles required for Case Management.

Table 2-3 User Group and Roles Mapping in Case Management

Group	User Role	Functions
CM Administrator Group	CM Administrator	• Configure jurisdictions and business domains • Configure case statuses • Configure case actions • Configure case types • Configure case system parameters
CM Analyst Group	CM Analyst	• Search for cases • Investigate cases • Set a case due date • Recommend case closure
CM Supervisor Group	CM Supervisor	• Map jurisdictions to pipelines • Perform real-time screening • Overwrite updates made by Analyst • Promote to case • Search for cases • Investigate cases • Set a case due date • Approve or reject recommendations to close cases • Close cases

Table 2-4 User Roles in Case Investigation

Privileges	Case Supervisor	Case Analyst
Access Cases	X	X
Search for Cases	X	X
View Case List	X	X
View Dashboard	X	X

Table 2-4 (Cont.) User Roles in Case Investigation

Privileges	Case Supervisor	Case Analyst
Edit Case Context	X	X
View Event Details	X	X
Set Event Decision	X	
Add/ Delete/ View Accounts	X	X
Add/ Delete/ View Customers	X	X

Table 2-4 (Cont.) User Roles in Case Investigation

Privileges	Case Supervisor	Case Analyst
Add/ Delete/ View Transactions	X	X
Add/ Delete/ View External Entities	X	X
View Related Case	X	X
View Related Events	X	X
Clear Due Date	X	X
Set Due Date	X	X

Table 2-4 (Cont.) User Roles in Case Investigation

Privileges	Case Supervisor	Case Analyst
Set Case Owner	X	X
Set Case Assignee	X	X
Recommend Close without Regulatory Report		X
Recommend Close with Regulatory Report		X

Table 2-4 (Cont.) User Roles in Case Investigation

Privileges	Case Supervisor	Case Analyst
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

Table 2-4 (Cont.) User Roles in Case Investigation

Privileges	Case Supervisor	Case Analyst
Add Document	X	X
Remove Document	X	X
View Attachments	X	X
Remove Attachments	X	X
Add Narrative	X	X
View Narrative	X	X
View Audit History	X	X

Table 2-4 (Cont.) User Roles in Case Investigation

Privileges	Case Supervisor	Case Analyst
Add Investigation Comments	X	X
Own a Case	X	X
Generate CRR Reports	X	
Viewing Case Reports	X	X
Save Case Search Criteria of Report	X	X

Table 2-4 (Cont.) User Roles in Case Investigation

Privileges	Case Supervisor	Case Analyst
Update Case Search Criteria of Report	X	X
Delete Case Search Criteria of Report	X	X
Export the Report in Excel	X	X

Table 2-5 User Roles in Case Management Administrator

Privileges	Case Admin
Access Cases	X
Add Case Status	X

Table 2-5 (Cont.) User Roles in Case Management Administrator

Privileges	Case Admin
Edit Case Status	X
Add Case Action	X
Edit Case Action	X
Mapping the Action to Status	X
Mapping the Action to Case Type	X
Mapping the Action to User Role	X
Configuring Case System Parameters	X
Add Business Domains	X
Edit Business Domains	X
Add Jurisdictions	X
Edit Jurisdictions	X
Add Case Types	X
Edit Case Types	X

Table 2-5 (Cont.) User Roles in Case Management Administrator

Privileges	Case Admin
Configuring Security Mappings	X

User Group and Roles Mapping for Scheduler Service

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

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

Group	User Role	Functions
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 Transaction Monitoring.

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

Group	User Role	Functions
CM 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
CM Administrator Group	Workflow Access	Access the Process Modeler menu from the Navigation Tree **Note:** The mapping of this role does not allow view, edit, and add actions

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

Group	User Role	Functions
CM Administrator Group	Workflow Monitor Access	Access the Process Monitor window **Note:** The mapping of this role does not allow view, edit, and add actions
CM Administrator Group	Workflow Read	View the PMF workflow
CM 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 Transaction Monitoring Documentation

Oracle FCCM Transaction Monitoring Cloud Service documentation helps you activate and use your subscription.

Table 3-1 Transaction Monitoring Cloud Services Workflow

Sequence	Action	Functions
1	Subscription	Activating Subscription
2	User Authentication	• Create users • User group and role mapping
3	Load Customer Specific Data	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 thresholds for the new jurisdictions • Create jobs for new thresholds • Add this job to the applicable batch • Update Scoring Pipeline with new threshold • Execute the batch
6	Configure Case Management Administration	• Configure Status and Actions • Configure Case Type • Map Case Actions to Status, Case Type, user roles • Configure PMF • Implement PMF using Case Types UI
7	Batch Processing	• Data Preparation • Data Uploading • Data Processing • Execute Batches
8	Investigating Cases	• Analyzing the case • Close the case • Report the case
9	Generating CRR Reports	Generating the report