

Oracle® FCCM Transaction Monitoring Cloud Service

User Roles and Privileges



Release 24.11.01
G18717-01
November 2024

ORACLE®

Oracle FCCM Transaction Monitoring Cloud Service User Roles and Privileges, Release 24.11.01

G18717-01

Copyright © 2024, Oracle and/or its affiliates.

Contents

Preface

1 User Roles and Privileges

About User Access Mapping	1-1
Role-Based Access Control	1-2

2 User Group and Roles Mapping

3 Using Transaction Monitoring Documentation

Preface

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

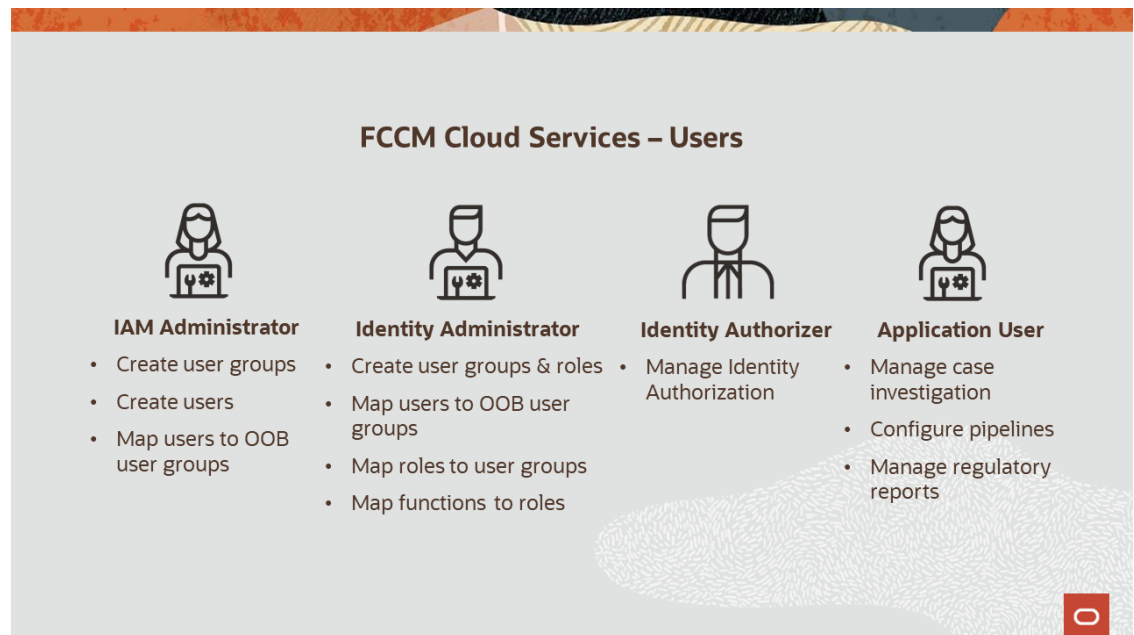
1

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 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 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 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 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
IAM Administrator	IAM Administrator	- Create users - Map users to IDNTY_ADMIN group - Map users to IDNTY_AUTH group
DPADMN	Data Platform Administrator	View the Data Platform Menu and to configure the data platform UI for EDD, Connector and PMF

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	- All Pipelines access: Note: This function provides access to the pipeline user interface and functionalities, but not the pipelines themselves. - Configure pipelines - Configure threshold sets - View reports
Threshold Admin Group	Common Pipelines access	- Data API Pipeline Access - Data Loading Pipeline Access - Data Pipeline Pipeline Access

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

Group	User Role	Functions
Threshold Admin Group	Threshold Editor Admin Role	• AML access code • FCC Common Function • PIPELINE Common Function • Threshold Editor/ Simulator Access Load watchlist data
Threshold Admin Group	SCORING pipelines access role	Scoring Pipeline Access
Threshold Admin Group	SCENARIO pipelines access role	Scenario Pipeline Access
Threshold Admin Group	• Function Read Role • Group Read Role • Role Read Role • User Read Role	• Function Summary • Function View • Group Summary • Group View • Role Summary • Role View • User Summary • User View

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 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 2-3 (Cont.) User Group and Roles Mapping in Case Management

Group	User Role	Functions
CM Admin User Group	CM Admin Role	• Action Mapping Save Button • Action Reason Mapping Add Button • Action Reason Mapping Edit Button • Action Reason Mapping Remove Button • Action Status Mapping • Admin Audit access • AML access code • Application Security Mapping • Business Domain • Business Domain Add Button • Business Domain Edit Button • Case Actions Add Button • Case Actions Edit Button • Case Priority Add Button • Case Priority Edit Button • Case Priority Remove Button • Case Rule Add Button • Case Rule Edit Button • Case Rule Remove Button • Case Rules • Case Status Add Button • Case Status Edit Button • Case System Parameter Edit Button • Case Type • Case Type Add Button • Case Type Edit Button • Cm access role • CM Admin Access • CM Admin Config Migration • CM Admin Export Config Migration • CM Admin Import Config Migration • FCC Common Function • Group Summary • Jurisdiction • Jurisdiction Add Button • Jurisdiction Edit Button • Security Mapping Save Button • System Parameters • Workflow CRUD API Access • Workflow Execute API Access • Workflow Read API Access

Table 2-3 (Cont.) User Group and Roles Mapping in Case Management

Group	User Role	Functions
CM Admin User Group	SCORING pipelines access role	Scoring Pipeline Access
CM Admin User Group	Data pipelines access role	Data Pipeline Pipeline Access
CM Admin User Group	Canned Report Access	Enable Canned Report
CM Admin User Group	- Workflow Access - Workflow Monitor Access - Workflow Read - Workflow Write	- Link Access to Workflow and Process Definitions - Summary Access to Workflow and Process Definitions - View Workflow and Process Monitor - Service Summary - Summary Access to Workflow and Process Definitions - View Workflow and Process Definitions - Workspace Summary - Add Workflow and Process Definitions - Delete Workflow and Process Definitions - Edit Workflow and Process Definitions - Service Summary - Workspace Summary
CM Admin User Group	Tag Features	- Function Summary - Tag - Tag Advance
CM Admin User Group	- Document Admin UI - Document Archival Role - Document Summary View	- Enable Doc Service Admin UI - Enable Doc Archival - Enable Doc Service Common UI
CM Admin User Group	- Function Read Role - Group Read Role - Role Read Role - User Read Role	- Function Summary - Function View - Group Summary - Group View - Role Summary - Role View - User Summary - User View

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
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
Set Case Owner	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
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
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
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
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
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

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

Group	User Role	Functions
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
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	Subscribe	Activating Subscription
2	Provision Users	• 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