

# Oracle® FCCM Transaction Monitoring Cloud Service

## User Roles and Privileges



Release 24.2.1  
F95099-01  
February 2024

ORACLE®

Oracle FCCM Transaction Monitoring Cloud Service User Roles and Privileges, Release 24.2.1

F95099-01

Copyright © 2024, Oracle and/or its affiliates.

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

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

Contributors: (contributor), (contributor)

# 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

---

---

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.

This documentation is in preproduction status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

---

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

# Preface

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

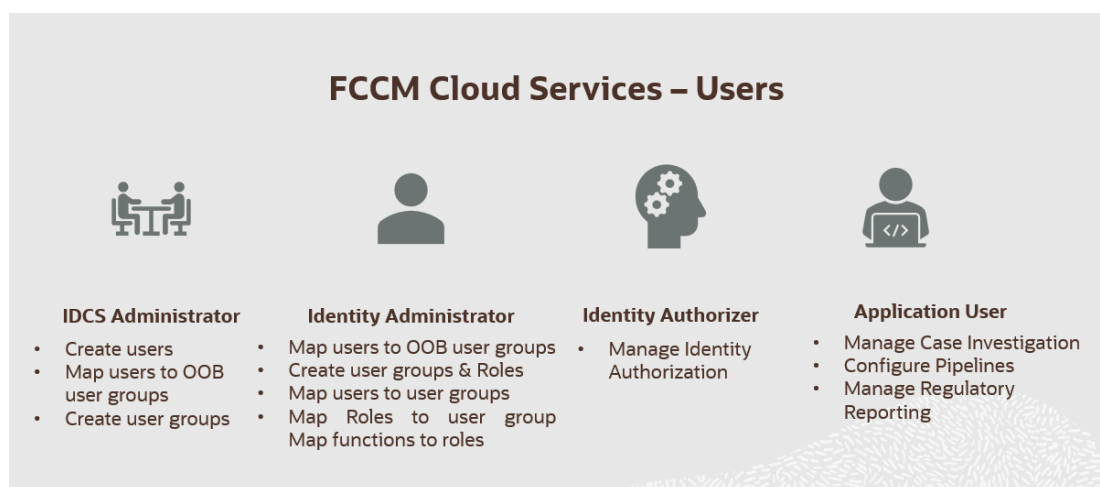
# 1

## 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 <a href="#">Business Domains</a> .
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 <a href="#">Jurisdictions</a> .

## 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	<ul style="list-style-type: none"><li>• View reports</li><li>• View the object storage</li><li>• View the OAUTH credentials</li><li>• Perform Identity and Access Management operations</li></ul>
Identity Authorizer	Identity Authorizer	Authorize the Identity and access management operations
IDCS Administrator	IDCS Administrator	<ul style="list-style-type: none"><li>• Create users</li><li>• Map users to IDNTY_ADMIN group</li><li>• Map users to IDNTY_AUTH group</li></ul>

### 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	<ul style="list-style-type: none"><li>• Configure pipelines</li><li>• Configure threshold sets View reports</li></ul>
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	<ul style="list-style-type: none"> <li>• Configure jurisdictions and business domains</li> <li>• Configure case statuses</li> <li>• Configure case actions</li> <li>• Configure case types</li> <li>• Configure case system parameters</li> </ul>
CM Analyst Group	CM Analyst	<ul style="list-style-type: none"> <li>• Search for cases</li> <li>• Investigate cases</li> <li>• Set a case due date</li> <li>• Recommend case closure</li> </ul>
CM Supervisor Group	CM Supervisor	<ul style="list-style-type: none"> <li>• Map jurisdictions to pipelines</li> <li>• Perform real-time screening</li> <li>• Overwrite updates made by Analyst</li> <li>• Promote to case</li> <li>• Search for cases</li> <li>• Investigate cases</li> <li>• Set a case due date</li> <li>• Approve or reject recommendations to close cases</li> <li>• Close cases</li> </ul>

**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

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

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

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

Pr ivi le ge s	Case Supervisor	Case Analyst
Ad d/ De let e / Vi ew Cu sto m er s	X	X
Ad d/ De let e / Vi ew Tr an sa cti on s	X	X
Ad d/ De let e / Vi ew Ex ter nal En titi es	X	X
Vi ew Re lat ed Ca se	X	X

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

Privileges	Case Supervisor	Case Analyst
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

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

Pr ivi le ge s	Case Supervisor	Case Analyst
Re co m m en d C l o s e w i t h o u t R e g u l a t o r y R e p o r t		X
Re co m m en d C l o s e w i t h R e g u l a t o r y R e p o r t		X
Re j e c t R e c o m m e n d a t i o n	X	

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

Pr ivi le ge s	Case Supervisor	Case Analyst
Cl os e a Ca se as Fal se Po siti ve	X	
Cl os e a Ca se as Tr ue Po siti ve	X	
Vi ew Ev ide nc e (At tac h m en t an d Co m m en t list )	X	X

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

Pr ivi le ge s	Case Supervisor	Case Analyst
Ad d Do cu m en t	X	X
Re m ov e Do cu m en t	X	X
Vi ew Att ac h m en ts	X	X
Re m ov e Att ac h m en ts	X	X
Ad d Na rra tiv e	X	X
Vi ew Na rra tiv e	X	X

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

Pr ivi le ge s	Case Supervisor	Case Analyst
Vi ew Au dit Hi sto ry	X	X
Ad d Inv est iga tio n Co m m en ts	X	X
O wn a Ca se	X	X
Ge ne rat e C R R Re po rts	X	
Vi ew ing Ca se Re po rts	X	X

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

Pr ivi le ge s	Case Supervisor	Case Analyst
Sa ve Ca se Se ar ch Cri ter ia of Re po rt	X	X
Up da te Ca se Se ar ch Cri ter ia of Re po rt	X	X
De let e Ca se Se ar ch Cri ter ia of Re po rt	X	X

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

<b>Privileges</b>	<b>Case Supervisor</b>	<b>Case Analyst</b>
Export the Report in Excel	X	X

**Table 2-5 User Roles in Case Management Administrator**

<b>Privileges</b>	<b>Case Admin</b>
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

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

Privileges	Case Admin
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   <b>Note:</b> 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   <b>Note:</b> The mapping of this role does not allow view, edit, and add actions
CM Administrator Group	Workflow Monitor Access	Access the Process Monitor window   <b>Note:</b> 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	<a href="#">Subscription</a>	Activating Subscription
2	<a href="#">User Authentication</a>	<ul style="list-style-type: none"> <li>• Create users</li> <li>• User group and role mapping</li> </ul>
3	<a href="#">Data Loading</a>	Upload required data files to Object Store
4	<a href="#">Application Security Mapping</a>	<ul style="list-style-type: none"> <li>• Business Domains</li> <li>• Jurisdiction</li> <li>• Mapping of Security Attributes</li> </ul>
5	<a href="#">Configure Transaction Monitoring Administration</a>	<ul style="list-style-type: none"> <li>• Copy Scoring Pipeline</li> <li>• Add thresholds for the new jurisdictions</li> <li>• Create jobs for new thresholds</li> <li>• Add this job to the applicable batch</li> <li>• Update Scoring Pipeline with new threshold</li> <li>• Execute the batch</li> </ul>
6	<a href="#">Configure Case Management Administration</a>	<ul style="list-style-type: none"> <li>• Configure Status and Actions</li> <li>• Configure Case Type</li> <li>• Map Case Actions to Status, Case Type, user roles</li> <li>• Configure PMF</li> <li>• Implement PMF using Case Types UI</li> </ul>
7	<a href="#">Batch Processing</a>	<ul style="list-style-type: none"> <li>• Data Preparation</li> <li>• Data Uploading</li> <li>• Data Processing</li> <li>• Execute Batches</li> </ul>
8	<a href="#">Investigating Cases</a>	<ul style="list-style-type: none"> <li>• Analyzing the case</li> <li>• Close the case</li> <li>• Report the case</li> </ul>
9	<a href="#">Generating CRR Reports</a>	Generating the report