Oracle® FCCM Know Your Customer Cloud Service

User Roles and Privileges

Release 26.08.01
G59607-01
August 2026

ORACLE

Oracle FCCM Know Your Customer Cloud Service User Roles and Privileges, Release 26.08.01

G59607-01

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 Know Your Customer 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

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 Financial Services Crime and Compliance Management Oracle Financial Services Crime and Compliance Management Cloud Service is a platform for hosting software as a service (SaaS) applications from Oracle's Financial Services Global Business Unit (FSGBU). 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 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 Creating the Application Users.

3

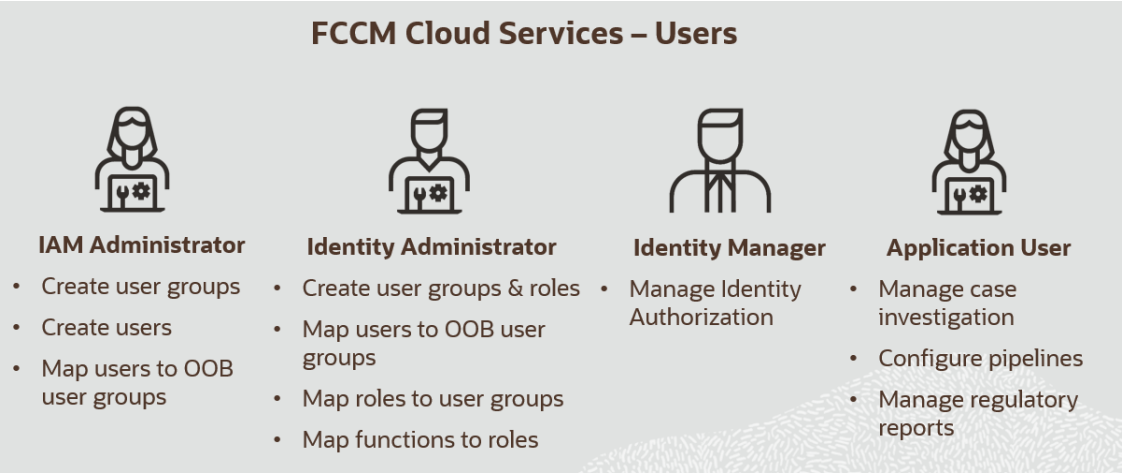
User Roles and Privileges

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



> **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.

Role-Based Access Control

Role-based security in Oracle Financial Services Crime and Compliance Management Know Your Customer 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, analyze, and act on cases	Business and Operational Data

User Group and Roles Mapping in Oracle FCCM Cloud Service

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

Table 3-3 User Group and Roles Mapping for KYC

Group	User Role	Function
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.
DPADMIN	FRC Data Platform Administrator	View the Data Platform Menu and to configure the data platform UI for EDD, Connector and PMF.
DPADMIN	FRC Data Platform Administrator	Add these roles to the DPADMIN user group to enable export and import of EDD and Connectors through Object Migration: • CATLGCREXP • CATLGCRIMP • DIOBJEXP • DIOBJIMP • FILE_ADV • OM_ADM • OMEXADVND • OMIMADVND
Data Maintenance Admin (DMIADMIN)	Canned Report Access (ENBCANNED)	View and access Reports for Download from the Admin Console.
	Data Maintenance Interface	View Available Data Maintenance (DMI) forms Download from the Admin Console.
KYCPADMINGRP	Data Maintenance Interface	View, edit, and delete Data Maintenance Interface forms.
Pipeline Administrator Group	KYC Administrator	• Configure pipelines • Configure threshold sets

Table 3-3 (Cont.) User Group and Roles Mapping for KYC

Group	User Role	Function
KYC Admin Group	KYC Admin Role	• FCC Common Function • KYC Age of Incorporation Configuration • KYC Behavioral Risk Indicator • KYC Case Creation Reason • KYC CIP Verified Status Configuration • KYC Custom Risk Indicator • KYC Jurisdiction Pipeline Mapping • KYC Length of Relationship Configuration • KYC Periodic Review Assessment Config • KYC Risk Category Configuration • KYC Risk Dimension • KYC Risk Element Configuration • KYC System Parameters • Relationship Type Assessment Mapping
KYC Admin Group	Pipeline Jurisdiction Mapping Maintainer Role	Pipeline Jurisdiction Access
KYC Admin Group	Common Pipelines access	• Data API Pipeline Access • Data Loading Pipeline Access • Data Pipeline Access
KYC Admin Group	KYC pipelines access role	KYC Pipeline Access
KYC Admin Group	SCORING pipelines access role	Scoring Pipeline Access
KYC Admin Group	WATCHLIST pipelines access role	Watchlist Pipeline Access
KYC 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
KYC Admin Group	Canned Report Access	Enable Canned Report
Job Administrator Group	KYC Administrator	Manage jobs
Scheduler Administrator Group	KYC Administrator	Manage batches
Master Data Administrator Group	KYC Administrator	Configure master data
Watchlist Administrator Group	KYC Administrator	• Manage private watch lists • Manage synonyms • Manage stop keywords

Table 3-3 (Cont.) User Group and Roles Mapping for KYC

Group	User Role	Function
KYC Analyst Group	KYC Analyst	• Search for cases • Investigate cases • Set a case due date • Recommend case closure • Perform risk assessments • Promote to case
KYC Group	KYC Analyst	• Search for cases • Investigate cases • Set a case due date • Recommend case closure • Perform risk assessments • Promote to case
KYC Group	KYC Supervisor	• Search for cases • Investigate cases • Set a case due date • Approve or reject recommendations to close cases • Close cases • Perform risk assessments • Overwrite updates made by Analyst • Promote to case
KYC Supervisor Group	KYC Supervisor	• Search for cases • Investigate cases • Set a case due date • Approve or reject recommendations to close cases • Close cases • Perform risk assessments • Overwrite updates made by Analyst • Promote to case

User Roles and Activities in KYC

Table 3-4 User Roles for KYC Analyst and Supervisor

Privileges	KYC Supervisor	KYC Analyst
Search for Cases	x	x
Investigate Cases	x	x
Set a case due date	x	x
Recommend case closure		x
Perform risk assessments	x	x
Promote to case	x	x
Perform risk assessments	x	x
Approve or reject recommendations to close cases	x	
Close cases	x	

User Roles in KYC Administrator

Table 3-5 User Roles in KYC Administrator

Privileges	KYC Administrator
Load watch list data	x
Configure pipelines	x
Configure threshold sets	x
Configure dimension data	x
Map jurisdictions to pipelines	x
Manage jobs	x
Configure master data	x

4

Using KYC Documentation

This topic describes workflow for KYC.

Table 4-1 Workflow for KYC

Workflow Process	Functionality
Subscription	Activating Subscription
User Authentication	• Create users • User group and role mapping
Configure Master Data	Configure master data through the data load service. This data is also used in the onboarding JSON.
Dimension Data	Configuring KYC specific dimension data
Mapping Jurisdiction to Pipeline	Map Jurisdiction and Entity Type to Pipeline
Application Security Mapping	• Map Business Domains • Map Jurisdiction
Configure Pipeline	• Import Pipelines • Create KYC Pipelines • Configure Widgets • Map Pipeline to Job • Map Job to Jurisdiction
Watch List Management	• Manage Private Watch List • Manage Synonym Words • Load Watchlist Data
Risk Assessment	Assess the risk that a customer poses to a bank or Financial Institutions.
Investgating Cases	• Analyzing the case • Close the case