Oracle® FCCM Know Your Customer Cloud Service

User Roles and Privileges

Release 24.05.01
F98092-02
May 2024

ORACLE

Oracle FCCM Know Your Customer Cloud Service User Roles and Privileges, Release 24.05.01

F98092-02

Copyright © 2024, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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.

Contents

Preface

Audience iv
Help iv
Documentation Accessibility iv
Diversity and Inclusion iv
Related Resources iv
Conventions v
Comments and Suggestions v

1 Overview of Securing Oracle FCCM Cloud Service

2 Application User Setup

3 User Roles and Privileges

4 Using KYC Documentation

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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

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 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.

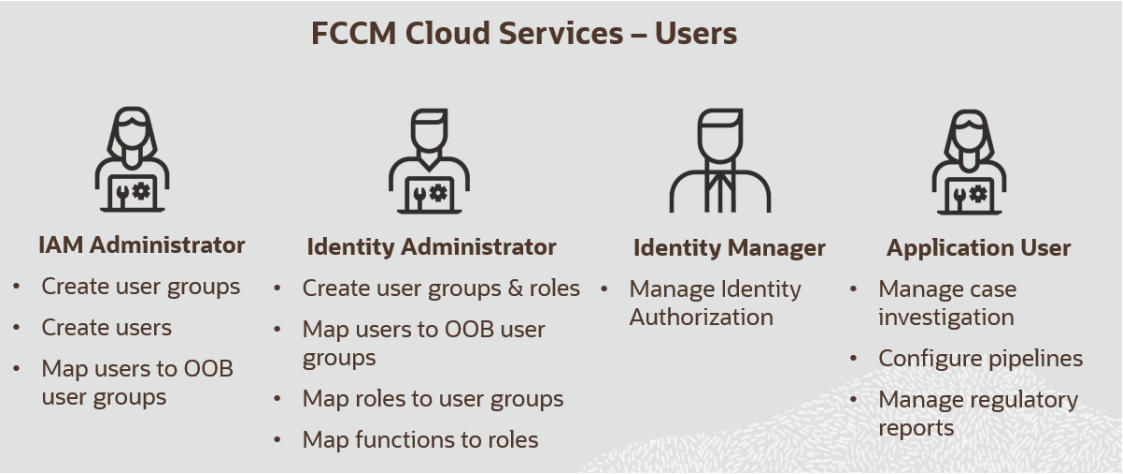
3
User Roles and Privileges

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?

Table 3-1 (Cont.) Role-based Access Control

Component	Description
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	Functionality
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
IAM Administrator	IAM Administrator	• Create users • Map users to **IDNTY_ADMIN** group • Map users to **IDNTY_AUTH** group
Pipeline Administrator Group	KYC Administrator	• Configure pipelines • Configure threshold sets
KYC Administrator Group	KYC Administrator	• Configure dimension data • Map jurisdictions to pipelines • Load watch list data
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
KYC Analyst Group	KYC Analyst	• Search for cases • Investigate cases • Set a case due date • Recommend case closure • Perform risk assessments • Promote to case

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

Group	User Role	Functionality
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