Oracle FCCM Cloud Service Customer Screening

User Roles and Privileges

Release 24.2.1
F90805-01
February 2024

Oracle FCCM Cloud Service Customer Screening User Roles and Privileges, Release 24.2.1

F90805-01

Contents

Preface

User Roles and Privileges explains how to enable user access to Oracle Financial Services Crime and Compliance Management Customer Screening Cloud Service functions and data.

Audience

This document is intended for users who are responsible for provisioning and activating Oracle Customer Screening Cloud services 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.

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.

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.

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.

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 Oracle Financial Services Crime and Compliance Management Cloud Service is a platform for hosting software as a service (SaaS) applications and 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

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 the User Summary Page and User Roles and Privileges.

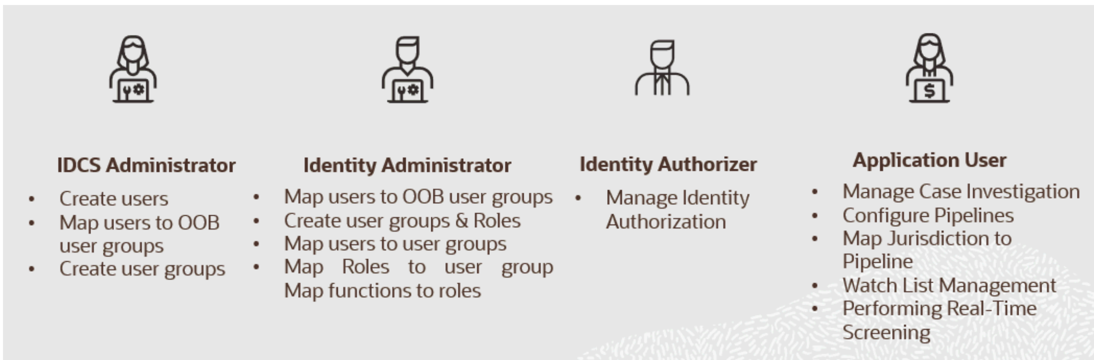
During implementation, you can use the Create User task to create test application users. By default, this task creates a minimal person record and a user account. After implementation, you should use the Hire an Employee task to create application users. The Create User task isn't recommended after implementation is complete. This topic describes how to create a test user using the Create User task. For more information, see the Creating the Application Users.

3
User Roles and Privileges

In Oracle Financial Services Crime and Compliance Management Customer Screening 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 IDCS will take five minutes to sync with the application. If these changes are made during the active user session then it will be reflected on the next login.
- You can create and manage Application users as per your requirements. For example, you can map Pipeline Admin group and CM Admin group to one user.

3.1 Role-Based Access Control

Role-based security in Oracle FCCM Customer Screening Cloud Service controls who can do what on which data.

The following table summarizes role-based access.

Table 3-1 Role-based Access

Component	Description
Who	The role assigned to a user.

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

Component	Description
What	The functions which users with the role can perform.
Which Data	The set of data which users with the role can access when performing the function.

The following table provides examples of role-based access.

Table 3-2 Examples of role-based access.

Who	What	Which Data
Data Administrators	Prepare and ingest data	Business data
Case Analysts	View, analyze, and act on cases	Business data and Operational data

Note:

The new user should have the following roles to access Home page of the Cloud application.

- Function read role
- Group read role
- User read role
- Role read role

3.2 User Group and User Role Mapping

Provides the User Group and User Role mapping.

Table 3-3 User Group and User Role Mapping

User Groups	User Roles	Activities
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

Table 3-3 (Cont.) User Group and User Role Mapping

User Groups	User Roles	Activities
IDCS Administrator	IDCS Administrator	• Create users • Map users to **IDNTY_ADMIN** group • Map users to **IDNTY_AUTH** group
Pipeline Administrator Group	Pipeline Administrator	• Configure pipelines • Configure threshold sets
CS Administrator Group	CS Administrator	Map jurisdictions to pipelines
Job Administrator Group	Job Administrator	Manage jobs
Scheduler Administrator Group	Scheduler Administrator	Manage batches
Watchlist Administrator Group	Watchlist Administrator	• Manage private watch lists • Manage synonyms & stop words • Manage Index Management
CS Analyst Group	CS Analyst	Perform real-time screening
CM Analyst Group	CM Analyst	• Search for cases • Investigate cases • Set a case due date • Close Cases • Recommend case closure
CM Supervisor Group	CM Supervisor	• Search for cases • Investigate cases • Set a case due date • Approve or reject recommendations to close cases • Close cases
CM Administrator Group	CM Administrator	• Configure Jurisdictions and business domains • Configure case statuses • Configure case actions • Configure case types • Configure case priority • Configure security mapping • Configure case system parameters • Configure and monitor PMF Workflows
MasterData Admin Group	MasterData Admin Role	Configure master data fields

3.3 User Roles and Activities in Customer Screening

Information about privileges in customer screening.

Table 3-4 User Roles and Activities

Privileges	CS Analyst	Watchlist Administrator	CS Administrator	CM Analyst	CM Supervisor	CM Administrator
Manage private watchlists		X				
Manage synonyms & stop words		X				
Manage Index Management UI		X				
Map jurisdictions to pipelines			X			
Search for cases				X	X	
Investigate cases				X	X	
Set a case due date				X	X	
Recommend case closure				X		
Perform real-time screening						
Approve or reject recommendations to close cases					X	
Close cases				X	X	
Configure jurisdictions and business domains						X
Configure case statuses, actions, types, and priority						X
Configure security mappings						X
Configure case system parameters						X
Configure & monitor PMF workflows						X

4

Using Customer Screening Documentation

Provides insight into the workflow of CS and related documents.

Table 4-1 Workflow for CS

Sequence	Document Reference	Description
1	Subscription	Activate Subscription
2	User Authentication	• Create users • User group and role mapping
3	Configure Master Data	Configure master data through the data load service, and they are used in the onboarding JSON
4	Data Loading	Upload required data files to Object Store
5	Mapping Jurisdiction to Pipeline	Map Jurisdiction and Entity Type to Pipeline
6	Configure Pipeline	• Import the ready-to-use pipelines • Create a copy of the imported pipelines • Create new pipelines and configure • Execute the batch
7	Application Security Mapping	• Create security attributes • Map Security Attributes to users
8	Watch List Management	• Manage Private Watch List • Manage Synonym Words
9	Configure Case Management	• Configure Status and Actions • Configure Case Types • Map of Case Action to Status, Case Type, user role • Configure PMF • Implement PMF using Case Types UI
10	Batch Processing	• Define a Batch • Define a Task • Schedule a Batch • Execute a Batch • Monitor a Batch
11	Investigating Cases	• Search Case • Analyze the case • Perform Real-Time Screening • Close the case