Oracle FCCM Cloud Service Transaction Filtering

User Roles and Privileges

Release 26.05.01
G55850-01
May 2026

Oracle FCCM Cloud Service Transaction Filtering User Roles and Privileges, Release 26.05.01

G55850-01

Copyright © 2024, 2025, 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

Copyright © 2024, 2025, Oracle and/or its affiliates.

Preface

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

Audience

This document is intended for users who are responsible for provisioning and activating Oracle Transaction Filtering 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.

Copyright © 2024, 2025, Oracle and/or its affiliates.

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 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/.

Copyright © 2024, 2025, Oracle and/or its affiliates.

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.

Copyright © 2024, 2025, Oracle and/or its affiliates.

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.

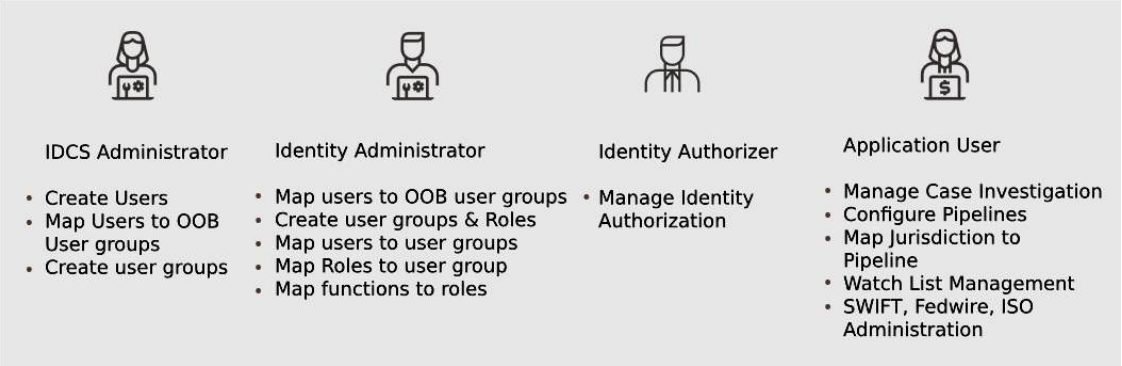
Copyright © 2024, 2025, Oracle and/or its affiliates.

3
User Roles and Privileges

Oracle Financial Services Crime and Compliance Management Transaction Filtering 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 Roles and Privileges



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 Transaction Filtering 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.
What	The functions which users with the role can perform.

Copyright © 2024, 2025, Oracle and/or its affiliates.

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

Component	Description
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

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

Table 3-3 User Group and User Role Mapping

User Groups	User Roles	Activities
TF Admin User Group	Common Pipelines access	• Data API Pipeline Access • Data Loading Pipeline Access • Data Pipeline Pipeline Access
TF Admin User Group	Pipeline Admin Role	• AML access code • FCC Common Function • Pipeline Access • PIPELINE Common Function
TF Admin User Group	TF pipelines access role	TF Pipeline Access
TF Admin User Group	WATCHLIST pipelines access role	Watchlist Pipeline Access

Copyright © 2024, 2025, Oracle and/or its affiliates.

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

User Groups	User Roles	Activities
TF Admin User Group	TF Admin	• TF Application Level Parameter Access • TF FEDWIRE CONFIGURATION ACCESS • TF ISO Configuration Access • TF Pipeline Jurisdiction and Business Mapping • TF SWIFT Configuration Access
TF Admin User Group	Threshold Editor Admin Role	• AML access code • FCC Common Function • PIPELINE Common Function • Threshold Editor/ Simulator Access
TF Admin User Group	Watchlist Admin Role	• OFS_CSCS • Watchlist Admin Access
TF Admin User Group	• Workflow Access • Workflow Monitor Access	• Link Access to Workflow and Process Definitions • Summary Access to Workflow and Process Definitions • View Workflow and Process Monitor
TF Admin User Group	Batch Advance Role	• Batch Add Function • Batch Copy Function • Batch Delete Function • Batch Execute Function • Batch Modify Function • Batch Purge Function • Batch Schedule Function • Batch Summary Function • Batch View Function • Function Summary
TF Admin User Group	Batch Authorization Role	• Batch Authorize Function • Batch Summary Function • Batch View Function • Function Summary
TF Admin User Group	Batch Maintenance Role	• Batch Modify Function • Batch Summary Function • Batch View Function • Function Summary
TF Admin User Group	• Batch Notification Role • Batch Read Role • Batch Write Role	• Batch Notification Function • Batch Summary Function • Batch View Function • Function Summary • Batch Add Function • Batch Copy Function • Batch Modify Function
TF Admin User Group	Canned Report Access	Enable Canned Report

Copyright © 2024, 2025, Oracle and/or its affiliates.

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

User Groups	User Roles	Activities
CM Analyst Group	CM Analyst	Map users to CM Analyst Group
CM Supervisor Group	CM Supervisor	Map users to CM Supervisor Group
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

3.3 User Roles and Activities in Transaction Filtering

The following table details the privileges in Transaction Filtering.

Table 3-4 User Roles and Activities

Privileges	TF Administrator	IHub TF Analyst	IHub TF Supervisor
Manage private watch lists	Yes	No	No
Manage synonyms & stop words	Yes	No	No
Manage Index Management UI	Yes	No	No
Map jurisdictions to pipelines	Yes	No	No
Search for cases	No	Yes	Yes
Investigate cases	No	Yes	Yes
Set a case due date	No	Yes	Yes
Recommend case closure	No	Yes	No
Approve or reject recommendations to close cases	No	No	Yes
Close cases	No	Yes	Yes
Configure jurisdictions and business domains	Yes	No	No
Configure case statuses, actions, types, and priority	Yes	No	No
Configure security mappings	Yes	No	No
Configure case system parameters	Yes	No	No
Configure & monitor PMF workflows	Yes	No	No

Copyright © 2024, 2025, Oracle and/or its affiliates.

4

Using Transaction Filtering Documentation

Workflow of TF and related documents.

The following table provide insight into workflow of TF and related documents.

Table 4-1 Workflow for TF

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 Group Execution	• 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

Copyright © 2024, 2025, Oracle and/or its affiliates.