

Oracle® FCCM Monitor Cloud Service

User Privileges



Release 24.11.01
G18871-01
November 2024

ORACLE®

Copyright © 2020, 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

1	Preface	
1.1	Audience	1-1
1.2	Help	1-1
1.3	Related Resources	1-1
1.4	Comments and Suggestions	1-1
2	User Roles and Privileges	
3	Using FCCM Monitor Documentation	

1

Preface

This preface introduces information sources that can help you use the Oracle Financial Services Crime and Compliance Management Monitor application.

1.1 Audience

This document is intended for users who are responsible for provisioning and activating Oracle FCCM Cloud Service or for adding other users who would manage the services, or for users who want to develop Oracle Cloud applications.

1.2 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.

1.3 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>.

1.4 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/>.

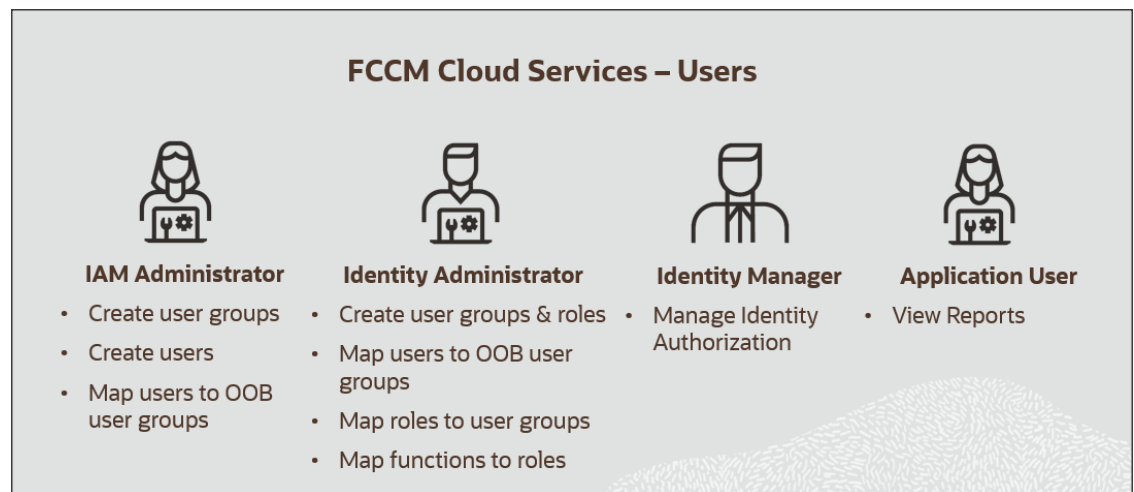
2

User Roles and Privileges

In Oracle Financial Services Monitor 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 2-1 User Roles and Privileges



Note:

- User-Group mapping changes from IAM will take five minutes to sync with application. If these changes are made during active user session then it will be reflected on next login.

Role-Based Access Control

Role-based security in Oracle Financial Services Compliance Monitor Cloud Service controls who can do what on which data.

Table 2-1 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?

This table provides some examples of role-based access

Table 2-2 role-based access

Who	What	Which Data
Data Administrator	Can perform Data Preparation and ingestion	Business Data
Case Analyst	Can view cases and update cases	Business and Operational Data

User Group, Role, and Activities

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

Table 2-3 User Group, Role, and Activities

User Groups	User Role	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
IAM Administrator	IAM Administrator	- Create users - Map users to IDNTY_ADMIN group - Map users to IDNTY_AUTH group
MNTRCCOGRP	MonitorCS CCO Group	CCO dashboard
MNTRDEPUTYCCOGRP	MonitorCS Deputy CCO Group	CCO dashboard
MNTRCMSUPGRP	MonitorCS CM Supervisor Group	Case Management dashboard
		TM Dashboard
MNTRRRSUPGRP	MonitorCS RR Supervisor Group	Regulatory Report dashboard
MNTRKYCSUPGRP	MonitorCS KYC Supervisor Group	KYC dashboard
MNTRCMANALYSTGRP	MonitorCS CM Analyst Group	Case Management dashboard but only those cases owned by them
MNTRCSSUPGRP	MonitorCS CS Supervisor Group	CS dashboard
MNTRTFSUPGRP	MonitorCS TF Supervisor Group	TF dashboard

Table 2-3 (Cont.) User Group, Role, and Activities

User Groups	User Role	Activities
MNTRADMNGRP	MonitorCS Analytics Admin Group	Create Custom Reports.
 Note: User can save Custom Reports in / Shared Folders/ MONITORCS Ad-hoc Analysis folder		
MNTRSRVCADMNGRP	MonitorCS Service Admin Group	Admin Activities -Configure Security Mapper and Trigger Batch

3

Using FCCM Monitor Documentation

This section facilitate you perform the following tasks in using FCCM Monitor Documentation.

FCCM Monitor Workflow

Table 3-1 FCCM Monitor Workflow

Workflow	Cloud Service	Activities
1	Subscription	Activating Subscription
2	User Authentication	• Create users • Add User to Group
3	Application Security	Application Security Administration helps Administrators classify users and the data that they are permitted to access.
4	Loading Data	Data that is present in the application layer is processed and loaded into the reporting layer.
5	Replication Utility	Replication Utility - a tool to ensure data consistency across multiple databases enabling efficient data replication and synchronization.
6	Getting Started	Explains the steps to log in to the FCCM Monitor cloud service and provides a brief overview of the users and their roles
7	Case Management Reports	To view Case Management reports.
8	Productivity Reports	To view Productivity Reports
9	SAR Reports	To view SAR Reports
10	KYC Reports	To view KYC Reports