

Oracle® FCCM Monitor Cloud Service

Administration Guide



Release 25.05.01

G35573-03

May 2025

ORACLE®

Copyright © 2000, 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

1	Preface	
	Audience	1-1
	Help	1-1
	Related Resources	1-1
	Comments and Suggestions	1-1
2	Identity Management	
3	Application Security Mapping	
4	Loading Data	
	Monitor Cloud Service Batch Tasks	4-1
5	Loading Custom Data - Placeholder Tables	
6	Replication Utility	

1

Preface

FCCM Monitor Administration Guide guides you step-by-steps instruction to use Oracle Financial Crime and Compliance Management Monitor cloud service.

Audience

This document is intended for users who are responsible for provisioning and activating Oracle FCCM 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>.

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

Identity Management

Using Identity Management, administrators can manage fine grained and coarse-grained entitlements. Coarse-grained entitlements consist of fewer functions than fine-grained entitlements. Authorizers can authorize the entitlement mappings.

For more information on mapping user group and roles, see [User Roles and Privileges](#).

For more information, see [Identity Management](#).

3

Application Security Mapping

Application Security Administration helps Administrators classify users and the data that they are permitted to access. Users are mapped to user groups, which must be mapped to specific security attributes, such as Business Domain, Jurisdiction, and Case Type. Users can then perform activities associated with their user group throughout the functional areas in the application.

For more information, see [Application Security Mapping](#).

4

Loading Data

Data that is present in the application layer is processed and loaded into the reporting layer. The Scheduler Service allows you to process data from the application to reporting tables by scheduling and running batches.

For more information, see [Load Data](#).

The following tasks are performed in the Scheduler Service to process data:

1. Process data once, daily (once in a day), weekly, or on a customized schedule.
2. Schedule a date and time for each batch to run.
3. To process data from application layer into the reporting tables, you must run the batch using the Schedule Batch feature in the Scheduler Services. For more information, see [Scheduler Services](#).



Note:

In the Scheduler Batch, you must select the ready-to-use batch name (**MonitorCSbatch**) to run the batch.

Monitor Cloud Service Batch Tasks

Ensure that only tasks relevant to SKUs included in provisioning are monitored. Any tasks linked to SKUs outside the provisioning scope must be excluded from the monitorCS batch by selecting the **Exclude Jobs** option in the **Schedule Batch** screen.

For example, if KYC is not included in the provisioning, then all KYC-related tasks listed below—from SI. No. 13 to 18—should be excluded from the `monitorCS` batch using the **Exclude Jobs** option in the **Schedule Batch** screen.

Table 4-1 Monitor CS batch tasks

SI.No.	TaskName	RelatedSKU
1	StartBatchADW	Common
2	FCCRSourceLoad	Transaction Monitoring
3	FCCRTMReplication	Transaction Monitoring
4	FCCRReplication	Transaction Monitoring
5	FCCRDeltaLoad	Transaction Monitoring
6	FCCRCMSourceLoad	CaseManagement
7	FCCRCMReplication	CaseManagement
8	FCCRCMDeltaLoad	CaseManagement
9	FCCRCMAccountRisk	CaseManagement
10	FCCRCMCustomerRisk	CaseManagement
11	FCCRCCasePrimaryEntity	CaseManagement

Table 4-1 (Cont.) Monitor CS batch tasks

Sl.No.	TaskName	RelatedSKU
12	FCCRCMDDataLoad	CaseManagement
13	FCCRKYCSourceLoad	KYC
14	FCCRKYCReplication	KYC
15	FCCRKYCDeltaLoad	KYC
16	FCCRKYCOBRequest	KYC
17	FCCRKYCProspect	KYC
18	FCCRKYCDataLoad	KYC
19	FCCRRRSourceLoad	CRR
20	FCCRRRReplication	CRR
21	FCCRRRDeltaLoad	CRR
22	FCCRRRRegReport	CRR
23	FCCRRRDataLoad	CRR
24	FCCRCSSourceLoad	Customer Screening
25	FCCRCSDDataLoad	Customer Screening
26	FCCRTFSourceLoad	Transaction Filtering
27	FCCRTFDataLoad	Transaction Filtering
28	FCCRSecurityMapper	Common
29	FCCRDeltaPurge	Common
30	EndBatchADW	Common

**Note:**

Common tasks must never be excluded from batch.

5

Loading Custom Data - Placeholder Tables

We can load the custom data related to Case status.

You can use the following CSV files to insert the custom data. And these CSV files have to be uploaded to the Object Store. Then execute the Batch **MonitorCSPlaceholderLoad** to load the data to the tables.

The following are CSV files to be uploaded to the Object Store:

- YYYYMMDD_PLACEHOLDER1.csv
- YYYYMMDD_PLACEHOLDER1_MAP.csv

Sample files of the above CSV files are available at [Financial Crime and Compliance Management Monitor Cloud Service Reference Documents](#).

The CSV file formats are as follows:

File Name: YYYYMMDD_PLACEHOLDER1.csv

Table 5-1 Sample Data

PLACEHOLDER1_ID	PLACEHOLDER1_CODE	PLACEHOLDER1_CODE_DESC	PLACEHOLDER1_CODETYPE
1	L1	Status of Level 1 Employee	Status
2	L2	Status of Level 2 Employee	Status
3	L4	Status of Level 4 Employee	Status

File Format:

File Name: YYYYMMDD_PLACEHOLDER1_MAP.csv

Table 5-2 Sample Data

PLACEHOLDER1_ID	PLACEHOLDER1_CODEVAL	PLACEHOLDER1_CODETYPE
1	INV	Case Status
1	NW	Case Status
2	INV	Case Status
2	CLS	Case Status
3	NW	Case Status

Note:

The sample text file name YYYYMMDD_FILEWATCHER.txt (empty file) must be pushed along with the above mentioned CSV files.

6

Replication Utility

Replication Utility is a valuable tool for organizations that need to ensure data consistency and availability across multiple databases or systems, enabling efficient data replication and synchronization.



Note:

- To perform the Replication process, the Base table and Target table structure must be in sync, if not, you can not perform this activity.

A Replication Utility is a tool or software that is used to replicate or copy data from one source to one or more target destinations. It is commonly used in database management systems to ensure data consistency and availability across multiple locations or servers.

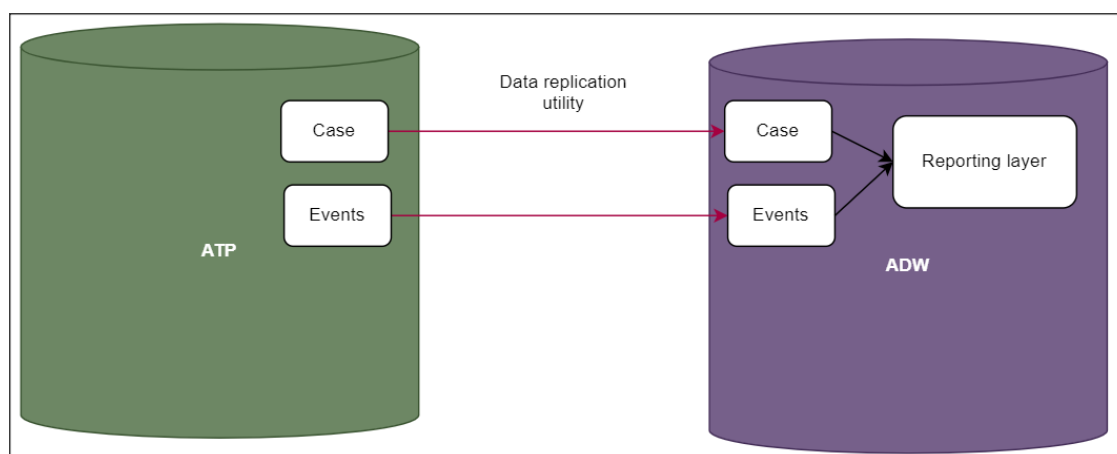
The Replication Utility typically works by capturing changes made to the source data and then applying those changes to the target destinations. This allows for real-time or near-real-time synchronization of data between different databases or systems.

Key features of Replication Utility may include:

- **Data synchronization:** It ensures that data changes made in the source database are replicated to the target databases, keeping them up to date.
- **Replication modes:** It supports different replication modes such as one-way replication (from source to target), two-way replication (bidirectional), or multi-master replication.
- **Conflict resolution:** In case of conflicting changes made to the same data in different locations, the Replication Utility may provide mechanisms to resolve conflicts and maintain data integrity.
- **Performance optimization:** It may include features to optimize replication performance, such as compression, filtering, or batching of data changes.
- **Monitoring and management:** Replication Utility often provides monitoring and management tools to track the replication process, view replication status, and troubleshoot any issues that may arise.

Using Replication Utility

The replication utility is a tool that is used to copy data from a source schema to a target schema. It is designed to identify any changes in the source data and update the target schema accordingly. In the context of the Oracle FCCM cloud reporting solution, this utility is specifically used to update the ADW reporting schema from the ATP application schema. The replication utility is primarily developed using PL/SQL, a procedural language used for Oracle database programming.



A database link is established in ADW (Autonomous Data Warehouse) to retrieve data from ATP (Autonomous Transaction Processing). This is achieved through a job in ADW, which utilizes the system global area (SGA), program global area (PGA), and other database resources of ADW. The purpose of this setup is to minimize the processing dependency on ATP.

There are several dependencies associated with using the database link:

- **ADW Wallet:** The ADW instance requires a wallet that contains the necessary credentials and certificates to establish a secure connection with ATP.
- **ADW Access to Object Store:** ADW needs access to an object store, which is a designated location for storing files and data. This access is necessary for retrieving any required files or data during the replication process.
- **Timely Refresh of Named Credentials:** The named credentials used for authentication with ATP need to be refreshed periodically to ensure the security of the connection. This involves updating the fingerprint associated with the credentials.

Table 6-1 fcc_replication_batch_run

N_RUN_SKEY	D_MIS_DATE	N_RUN_STATUS	V_BATCH_RUN_I D	N_RUN_DATE
1	28-06-2022	1	ADW_1656420618 626_20220628_1	28-06-2022

Table 6-2 fcc_replication_audit

SOURCE_T ABLE	TARGET_TA BLE	RUN_SKEY	RECORD_IN SERIED	RECORD_U PDATED	RECORD_D ELETE	RUN_DATE
fcc_cust_dim	fccr_cust_dim	1	CUST038388 3	CUST838382	CUST327722	
fcc_cust_dim	fccr_cust_dim	1	CUST978788 8	CUST876127	CUST176512	30-may-2023

- The replication audit table is designed to store the actual internal ID or sequence of the changed record, along with the new run ID. This information is crucial for updating dependent tables in the replication process.

- To optimize performance, the audit table is partitioned based on the target table name. This allows for efficient retrieval and management of the replicated data. Additionally, the audit table is further sub-partitioned based on either the run_key or run_date, depending on the specific requirements of the replication process.
- As for the maintenance of the audit table, whether to truncate or purge the table is left to the discretion of the customer. This decision can be based on factors such as data retention policies, storage limitations, and performance considerations.

Table 6-3 fcc_replication_run_book

SOURCE_TABLE	TARGET_TABLE	JOS_STATUS	RUN_KEY	RUN DATE
fcc_cust_dim	fccr_cust_dim	Finished	1	30-may-2023