Oracle® FCCM Monitor Cloud Service

Administration Guide

Release 26.02.01
G52146-01
February 2026

Oracle FCCM Monitor Cloud Service Administration Guide, Release 26.02.01

G52146-01

Contents

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 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.

> **Note**
>
> Ensure to map the security attributes to at least one MonitorCS User Group and save your changes before running the Monitor CS batch.

> **Note**
>
> - To create a new custom user group from the Admin Console, navigate to the **Identity Management** tab and click the "+" icon on the **User Group** tile. In the group definition screen, ensure the **Group ID** starts with the "MNTR" prefix (for example, MNTRRRSUPGRP).
> - To create a new custom user group from the IDCS console, use "MNTR" as the prefix for the **Group Name**.

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.

> **Note**
>
> Ensure that security attributes are mapped to Monitor CS User Group before batch execution.

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 Sl. No. 10 to 13—should be excluded from the `monitorCS` batch using the **Exclude Jobs** option in the **Schedule Batch** screen.

Table 4-1 Monitor CS batch tasks

Sl.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

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

Sl.No.	TaskName	RelatedSKU
7	FCCRCMReplication	CaseManagement
8	FCCRCMDeltaLoad	CaseManagement
9	FCCRCMDataLoad	CaseManagement
10	FCCRKYCSourceLoad	KYC
11	FCCRKYCReplication	KYC
12	FCCRKYCDeltaLoad	KYC
13	FCCRKYCDataLoad	KYC
14	FCCRRRSourceLoad	CRR
15	FCCRRRReplication	CRR
16	FCCRRRDeltaLoad	CRR
17	FCCRRRDataLoad	CRR
18	FCCRCSSourceLoad	Customer Screening
19	FCCRCSDataLoad	Customer Screening
20	FCCRTFSourceLoad	Transaction Filtering
21	FCCRTFDataLoad	Transaction Filtering
22	FCCRSecurityMapper	Common
23	FCCRDeltaPurge	Common
24	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.

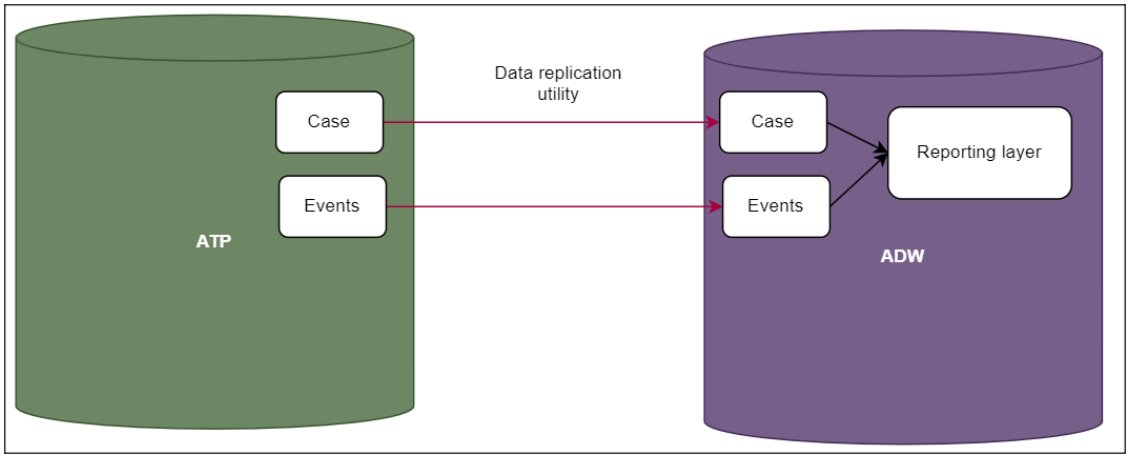
The Replication Utility typically works by capturing changes made to the source data and then applying those changes to the target destinations. This allows for real-time or near-real-time synchronization of data between different databases or systems.

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_ID	N_RUN_DATE
1	28-06-2022	1	ADW_1656420618626_20220628_1	28-06-2022

Table 6-2 fcc_replication_audit

SOURCE_TABLE	TARGET_TABLE	RUN_SKEY	RECORD_INSERTED	RECORD_UPDATED	RECORD_DELETE	RUN_DATE
fcc_cust_dim	fccr_cust_dim	1	CUST0383883	CUST838382	CUST327722	
fcc_cust_dim	fccr_cust_dim	1	CUST9787888	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_skey 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_SKEY	RUN DAE
fcc_cust_dim	fccr_cust_dim	Finished	1	30-may-2023