# Oracle Financial Services Compliance Regulatory Reporting

## US SAR Administration Guide

**Release 8.1.2.5.0**

**June 2023**

**F26032-01**

ORACLE
Financial Services

ORACLE

OFS CRR US SAR Administration Guide

Copyright © 2024 Oracle and/or its affiliates. All rights reserved.

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.

For information on third party licenses, click here.

# Document Control

**Table 1: Document Control**

| Revision Number | Revision Date | Change Log |
|---|---|---|
| 2.0 | September 2024 | • Added a note for FOI and Tin type in the Table 5.<br>• Added a note for removed USSAR role users in the Table 5. |
| 1.9 | July 2024 | • Added `DIM_CRR_REF_DETAIL.xlsx` row in the Table 5.<br>• Added 6.13 Configuring CAR section. |
| 1.8 | May 2024 | Added a section - Populating Phone Number Through Posting. |
| 1.7 | January 2024 | • A note is added to in the DIM_EXTRNL_USERS_LIST`.xlsx` in Table 5.<br>• Added Populating Identification Type Through Posting section. |
| 1.6 | November 2023 | Updated Configuring CAR section. |
| 1.5 | September 2023 | • Added `DIM_EXTRNL_USERS_LIST.xlsx` row in the Table 5.<br>• Added Configuring Set Due Date Button section.<br>• A note is added under *Configuring Automatic E-File Submission* sub section in Configuring Secure Direct Transfer Mode (SDTM) section. |
| 1.4 | June 2023 | No content updates for this release. |
| 1.3 | May 2023 | • Added Configuring Unknown Branch Indicator.<br>• Updated language pack related tables in Table 5 in the Loading the Client-Specific Data section. |
| 1.2 | March 2023 | • Updated parameter in the Configuring Default Domain 1 section.<br>• Removed Configuring Filing Institution Information section as it is no more required<br>• Added Configuring CAR section. |
| 1.1 | December 2022 | • Updated Configuring Activity Information section<br>• Added Configuring Default Domain 1 section<br>• Added Configuring Multiple Reports in the Single Instance section<br>• Added Configuring Multiple Currencies sections<br>• Added Configuring Purge section<br>• Added Configuring Due Date sections<br>• Added Managing Purge Batch Tasks section |

**Table 1: Document Control**

| Revision Number | Revision Date | Change Log |
|---|---|---|
| 1.0 | June 2022 | • Updated the Configuring Secure Direct Transfer Mode (SDTM) section in the Configuring Parameters chapter.<br>• Added Configuring XSD Parameters and Configuring Lookback Period in the Days section in Configuring Parameters chapter.<br>• Added the Configuring Security Attributes for Users section. |

# Contents


**1 About This Guide ... 3**

1.1 Who Should Use This Guide ... 3

1.2 How This Guide is Organized ... 3

1.3 Where to Find More Information ... 3

1.4 Conventions ... 4

**2 Administration Workflow ... 1**

**3 Setting Users and Configuring Security Attributes ... 2**

3.1 Creating Users ... 2

3.2 Mapping Users To User Groups ... 2

3.3 Configuring Security Attributes for Users ... 3

*3.3.1 Configuring Security Attributes for Users without JIT ... 3*

*3.3.2 Configuring Security Attributes for Users with JIT ... 3*

3.4 Logging in and Resetting Password ... 5

**4 Loading Data into the OFSCRR Application ... 6**

4.1 Loading the Client-Specific Data ... 6

*4.1.1 Uploading Excel ... 8*

4.2 Loading Product Supplied Metadata ... 9

**5 Integrating with the ECM Application ... 10**

5.1 Configuring Webservice in OFSCRR ... 10

5.2 Configuring CRR Service URL in Atomic Schema ... 10

5.3 Configuring Webservice in OFSECM ... 11

*5.3.1 Updating OFSCRR Webservice password in OFSECM ... 11*

5.4 Configuring Processing Modeling Framework (PMF) ... 12

5.5 Populating Identification Type Through Posting ... 12

5.6 Populating Phone Number Through Posting ... 12

**6 Configuring Parameters ... 13**

6.1 Configuring Report Lock Period ... 13

6.2 Configuring Activity Information ... 13

6.3 Configuring Default Domain 1 ... 14

6.4 Transferring Primary CUST ACCT Only ..... 14
6.5 Configuring Multiple Instances ..... 14
*6.5.1 Configuring Multiple Instance Attribute Flag ..... 14*
*6.5.2 Configuring PMF ..... 15*
*6.5.3 Configuring Report URLs ..... 15*
*6.5.4 Configuring Case Jurisdiction and Report Type Mapping ..... 15*
6.6 Configuring Secure Direct Transfer Mode (SDTM) ..... 16
*6.6.1 Configuring Multiple Reports in the Single Instance ..... 21*
6.7 Configuring XSD Parameters ..... 22
6.8 Configuring Multiple Currencies ..... 22
6.9 Configuring Unknown Branch Indicator ..... 23
6.10 Configuring Lookback Period in the Days ..... 23
6.11 Configuring Purge ..... 24
6.12 Configuring Due Date ..... 24
*6.12.1 Configuring Set Due Date Button ..... 24*
6.13 Configuring CAR ..... 25
*6.13.1 Configuring Document Type ..... 25*
**7 Managing Batches ..... 27**
7.1 Prerequisites for SDTM Batches ..... 27
7.2 Creating SDTM Batches ..... 27
7.3 Managing Purge Batch Tasks ..... 29
7.4 Executing Batches ..... 29
7.5 Updating Batches ..... 30
**8 OFSAA Support Contact Details ..... 32**
**9 Send Us Your Comments ..... 33**

# 1 About This Guide

This guide provides instructions to configure the Oracle Financial Services Compliance Regulatory Reporting Report (OFSCRR) application.

**Topics**:

- Who Should Use This Guide
- How This Guide is Organized
- Where to Find More Information
- Conventions

## 1.1 Who Should Use This Guide

The *OFSCRR Administration Guide* is designed for Oracle Financial Services Administration Users and Super Users. The list of responsibilities is as follows:

- Configure, maintain, and adjust the system
- Maintain user accounts and roles, archive data, and load data feeds

## 1.2 How This Guide is Organized

This guide includes the following chapters:

- Chapter 2, Administration Workflow, explains the administration workflow in the OFSCRR application.
- Chapter 3, Setting Users and Configuring Security Attributes, details the steps involved in creating users.
- Chapter 4, Loading Data into the OFSCRR Application, details the steps for loading client-specific data and product supplied metadata.
- Chapter 5, Integrating with the ECM Application, details the steps involved in integrating the OFSCRR application with OFSECM.
- Chapter 6, Configuring Parameters, explains the steps to configure the report lock period, activity information, default domain, SDTM, and transferring primary customer account.
- Chapter 7, Managing Batches, describes steps to create, execute and manage batches.

## 1.3 Where to Find More Information

For more information on the OFSCRR application, refer to the following documents in OHC:

- Oracle Financial Services Compliance Regulatory Reporting Installation Guide
- Oracle Financial Services Compliance Regulatory Reporting Data Model Reference Guide
- Oracle Financial Services Compliance Regulatory Reporting Release Notes/ReadMe
- Oracle Financial Services Compliance Regulatory Reporting User Guide
- Oracle Financial Services Compliance Regulatory Reporting Web Services Guide

To find additional information about how Oracle Financial Services solves real business problems, see our website at www.oracle.com/financialservices.

## 1.4 Conventions

Table 1 lists the conventions used in this guide.

**Table 1: Conventions Used in this Guide**

| Conventions | Descriptions |
|---|---|
| Italics | • Names of books, chapters, and sections as references<br>• Emphasis |
| Bold | • An Object of an action (menu names, field names, options, button names) in a step-by-step procedure<br>• Commands typed at a prompt<br>• User input |
| `Monospace` | • Directories and subdirectories<br>• File names and extensions<br>• Process names<br>• Code sample, including keywords and variables within a text and as separate paragraphs, and user-defined program elements within a text |
| Asterisk | Mandatory fields in the User Interface |
| <Variable> | Substitute input value |

# 2 Administration Workflow

This chapter describes the Administrator workflow in the OFSCRR application.

**Figure 1: Administrator workflow**

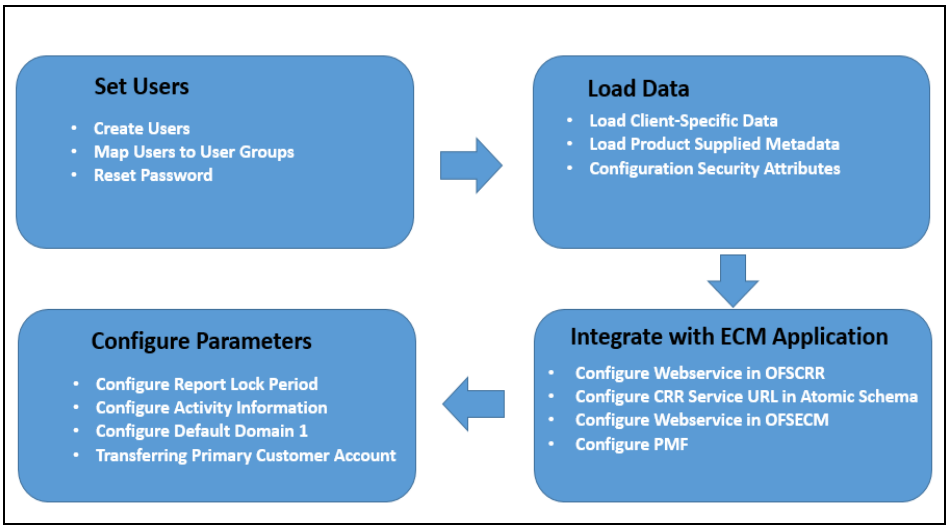



Table 2 lists the administration workflow in tabular format.

**Table 2: Administrator workflow**

| Workflow | Description |
|---|---|
| Setting Users and Configuring Security Attributes | Provide access to users in the OFSCRR application through the user groups. |
| Loading Data into the OFSCRR Application | Load-client specific data and product supplied metadata in the OFSCRR application. |
| Integrating with the ECM Application | Integrate the OFSECM application with the OFSCRR application to post cases to generate reports with the Webservice calls. |
| Configuring Parameters | Configure the report lock period, activity information, default domain, Secure Direct Transfer Mode (SDTM), and transferring primary customer account. |

# 3 Setting Users and Configuring Security Attributes

This chapter describes how to provide access to users in the OFSCRR application through the user groups.

**Topics**:


- Creating Users
- Mapping Users To User Groups
- Configuring Security Attributes for Users
- Logging in and Resetting Password


## 3.1 Creating Users

To create users, follow these steps:

1. To create the users, log in as SYSADMIN. For more information, see the *Object Administration* section in the Oracle Financial Services Analytical Applications Infrastructure User Guide.

   **NOTE** If you are integrating the OFSCRR application with the OFSECM application, it is optional to create the OFSCRR Administrator user. The user mapped to the role of OFSECM Administrator can be mapped to the role of OFSCRR Administrator.

2. Map the users to the pre-defined user groups, which in turn map to the user role. For more information, see the *Object Administration* section in the Oracle Financial Services Analytical Applications Infrastructure User Guide.

   Table 3 provides information about the predefined user groups that are mapped to the created users.

   **Table 3: Users and Groups**

| Group Code | Group Name | Group Description |
|---|---|---|
| RRUSANALYST | RR US Analyst | RR US Analyst User Group |
| RRUSAUDITOR | RR US Auditor | RR US Auditor User Group |
| RRUSSUPER | RR US Super User | RR US Super User Group |
| RRUSSUPERVISOR | RR US Supervisor | RR US Supervisor Group |
| RRADMINISTRATOR | RR US Administrator | RR Administrator Group |

## 3.2 Mapping Users To User Groups

Use Table 4 to map the users to pre-defined user groups.

**Table 4: Mapping Users to User Groups**

| Users | Group Description | Group Name |
|---|---|---|
| Analyst | RR US Analyst | RRUSANALYST |
| Supervisor | RR US Supervisor | RRUSSUPER |
| Super User | RR US Super User | RRUSSUPERVISOR |
| Auditor | RR US Auditor | RRUSAUDITOR |
| Admin User | RR Administrator Group | RRADMINISTRATOR |

## 3.3 Configuring Security Attributes for Users

Security Attributes help an organization classify users based on their geography, jurisdiction, and business domain to restrict access to the data they can view. You need to map the roles with access privileges. As these roles are associated with user groups, the users associated with the user groups can perform activities throughout various functional areas in the CRR application.

Types of user creations - With JIT (Just in Time) and without JIT.

**Topics**:

- Configuring Security Attributes for Users without JIT
- Configuring Security Attributes for Users with JIT

### 3.3.1 Configuring Security Attributes for Users without JIT

To configure security attributes for users through OFSAA (without JIT), follow these steps:

1. Log in as the Administrator user.
2. Click **User Administratio**n. Select Regulatory Report User's Attribute Administration. The User Attribute page is displayed.
3. Select the a user from the User Name drop-down list.
4. Assign attributes to each user from the drop-down list.
5. Click Save. The confirmation message is displayed.

### 3.3.2 Configuring Security Attributes for Users with JIT

To configure security attributes for users with JIT, follow these steps:

1. Post-installation steps, login as SYSADMN and update the following in the System Configuration Details.
   a. Select Authentication Type as **LDAP Authentication** and **SMS Authorization.**
   b. Click **Add** and provide your LDAP Server Details and click **Save**.
   c. Enable JIT provisioning option.

2. Execute the following statement to enable JIT sync.

```
UPDATE CONFIGURATION set paramvalue = 'Y' where paramname='JIT_IS_SYN-
C_GRP_ENABLED'; COMMIT;
```

> **NOTE** If a new user is added to a group or an existing user is removed from the group, in the next login, remapping the security attributes is done only if `JIT_IS_SYNC_GRP_ENABLED` is set to 'Y'.

3. Create Application User Groups and Users mappings in the LDAP Server.

   In the Atomic Schema, a new table `FCC_GROUP_SEC_ATTR_MAP` is introduced to configure the Security attributes mapping to the Application User Groups.

4. To configure security attributes to the User groups, login to the Atomic Schema in the `FCC_GROUP_SEC_ATTR_MAP` table and populate the following columns with the mentioned values.
   - Valid values for V_GROUP_CD column are the User groups mapped to the User.
   - Valid values for V_SEC_ATTR_CD column are DOMAIN1, DOMAIN2, DOMANI3, DOMAIN4, and DOMAIN5.
   - Valid values for V_SEC_ATTR_VAL column are the values that are available in DIM_DOMAIN1, DIM_DOMAIN2, DIM_DOMANI3, DIM_DOMAIN4, and DIM_DOMAIN5 table, respectively.

5. Log in with the New User in the Application and verify whether the Security attributes mapping is successful.

6. Update `tnsnames.ora` file with CRR atomic schema as follows.

```
<atomic_schema_name>=
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = <hostname>)(PORT = <port_number>))
(CONNECT_DATA =
  (SERVER = DEDICATED)
  (SERVICE_NAME = <service_name>)
 )
)
```

> **NOTE** If the atomic schema name created has underscore(_), then remove the underscore and update. For example, CRR_atomic must be updated as `CRR-atomic`.

7. If there are no changes to User group mapping and only changes to Security attribute mapping, then follow these steps to create and execute the respective batches which will populate the required tables with the updated security attributes:
   a. Log in as an Admin user.
   b. Navigate to Run Rule Framework and create a Batch for CRR.
   c. Add CRR task `FN_FCC_CRR_JIT_SYNCH` to the batch.
   d. Navigate to the **Common Tasks** menu, select **Operations** and click **Batch Execution** to execute the batch.

For more information batches, see Run Rule Framework Chapter in the Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide.

## 3.4 Logging in and Resetting Password

To log in and reset password, follow these steps:

1. Log in with each created user in the OFSCRR application. The Password Reset page is displayed.

   **NOTE** This page is displayed when a user logs in for the first time immediately after that user has been created, or every time the SYSADMN user resets the password. For example, when the user forgets the password or when the password is locked.

2. Reset the password. The OFSCRR application login page is displayed.

   **NOTE** You must log in to the application using the new password.

3. The OFSCRR application landing page is displayed. Click **Compliance Regulatory Reporting**.
4. Hover over **US-SAR** and select Search and List page, Create New Report, or File Regulatory Reports to open the OFSCRR application.

   **NOTE** Follow these steps whenever a new user is added or modified (for User Details, User Group mapping, Security Attribute mapping, and Password Change).

# 4 Loading Data into the OFSCRR Application

This chapter explains how to load data into the OFSCRR application.

**Topics**:

- Loading the Client-Specific Data
- Loading Product Supplied Metadata

## 4.1 Loading the Client-Specific Data

A client-specific data is data such as jurisdictions, filing institution information, business domains, transmitter Information, and so on. This section explains the steps to load the client specific data into the OFSCRR application.

To load the client-specific data, follow these steps:

1. Navigate to `<ftpshare path>/STAGE/Excelupload/Templates`.
2. The `<ftpshare path>` is the same path given in the variable `OFSAAI FTP` in `OFSAAI_InstallConfig.xml` while installing OFSAAI. For more information, see *Configuring OFSAAI_InstallConfig.xml File* section in the Oracle Financial Services Compliance Regulatory Reporting Installation Guide.
3. Download the following Excel sheets in the Template folder to the Windows machine from the path given in step 1.

   Table 5 describes the table name and reference to the data model.

**Table 5: Excel Sheets**

| Group Code | Group Name | Group Description |
|---|---|---|
| DIM_DOMAIN1.xlsx | Provide the list of all jurisdictions that are available in OFSECM. | Security Attribute1 Static Information section. |
| DIM_DOMAIN2.xlsx | Provide the list of all business domains which are available in OFSECM. | Security Attribute2 Static Information section. |
| DIM_DOMAIN3.xlsx | Provide the list of all case types and case sub types which are available in OFSECM. | Security Attribute3 Static Information section. |
| DIM_DOMAIN4.xlsx | Provide the list of all organizations that are available in OFSECM. | Security Attribute4 Static Information section. |
| DIM_DOMAIN5.xlsx | Provide the list of all scenario classes which are available in OFSECM. | Security Attribute5 Static Information section. |
| DIM_COUNTRY.xlsx | Provide the list of all countries that need to be made available to the application | Country Information section |
| DIM_STATES.xlsx | Provide the list of all states for the countries that need to be made available to the application. | State Information section |
| FCT_TRANSMITTER_INFO.xlsx | Provide the list of all transmitter Information. | Transmitter Information section |
| DIM_FILING_INST.xlsx | Provide the list of all filing institution information. | Filing Institution Information section |
| FCT_BRANCH_INFO.xlsx | Provide the list of all branch information. | Branch Information section |
| FCT_FININST_INFO.xlsx | Provide the list of all financial institutions. | Financial Institution section |
| DIM_DOMAIN1_TL.xlsx | Provide the list of all jurisdictions that are available in OFSECM for language pack. | Security Attribute1 Static Information section. |
| DIM_DOMAIN2_TL.xlsx | Provide the list of all business domains which are available in OFSECM for language pack. | Security Attribute2 Static Information section. |
| DIM_DOMAIN3_TL.xlsx | Provide the list of all case types and case sub types which are available in OFSECM for language pack. | Security Attribute3 Static Information section. |

| Group Code | Group Name | Group Description |
|---|---|---|
| DIM_DOMAIN4_TL.xlsx | Provide the list of all organizations that are available in OFSECM for language pack. | Security Attribute4 Static Information section. |
| DIM_DOMAIN5_TL.xlsx | Provide the list of all scenario classes which are available in OFSECM for language pack. | Security Attribute5 Static Information section. |
| FCT_BRANCH_INFO_TL.xlsx | Provide the list of all branch information for language pack. | Branch Information section |
| DIM_FILING_INST_TL.xlsx | Provide the list of all filing institution information for language pack. | Filing Institution Information section |
| FCT_TRANSMITTER_INFO_TL.xlsx | Provide the list of all transmitter Information for language pack. | Transmitter Information section |
| FCT_FININST_INFO_TL.xlsx | Provide the list of all financial institutions for language pack. | Financial Institution section |
| DIM_EXTRNL_USERS_LIST.xlsx | Provide the list of all the external users | External User section<br>**NOTE**:<br>• SYSTEM User must be created with the User ID as **1**.<br>• To populate the removed USSAR role users in the Search filters, Template Type( N_REPTYPE_SKEY) must be mapped to **1**. |
| DIM_CRR_REF_DETAIL.xlsx | Provide the list of all the Source code to CRR reference details. | Source Code to CRR Reference Details.<br>**NOTE**:<br>• For Form of Identification (FOI), the CODE_SET_ID must be ***DocType***<br>• For Tin Type, the CODE_SET_ID must be ***TinType***.. |

4. Add data to each Excel sheet as per your report requirement. For more information, see the Oracle Financial Services Data Model Reference Guide.

### 4.1.1 Uploading Excel

This option helps you to populate excel sheet data into the table.

To upload the Excel sheet, follow these steps:

1. Log in to the OFSCRR application as the Administrator user.

2. Navigate to Compliance Regulatory Reporting. Click **Excel Upload (Atomic)**.
3. Select the **Excel Upload**. The Excel Upload page is displayed.

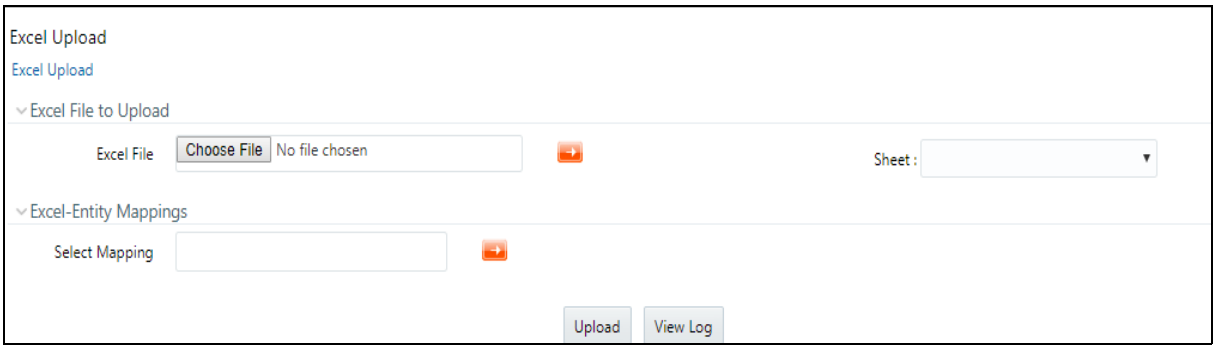



**Figure 2: Excel Upload**

4. Click **Choose File from** Excel File to Upload. Select the sheet from the drop-down list.
5. In the Excel - Entity Mappings section, click the **Select the Mapping** arrow. Select the table name with the same name as the Excel sheet.
6. Click **Upload**. The confirmation message is displayed.

## 4.2 Loading Product Supplied Metadata

This section explains how to load the pre-packaged data of the OFS CRR application, such as the ISO code of the country, template (US SAR) specific codes, and so on.

To load the product supplied metadata, follow these steps:

1. Execute the SQL `AtomicUSSAR.sql` in the CRR Atomic schema.

   This file is packaged in the CRR installer kit under the path OFS_CRR_PACK/OFS_CRR/ProductSuppliedMetadata/USSAR.

# 5 Integrating with the ECM Application

The OFSECM application is integrated with the OFSCRR application to post cases to generate reports with Webservice calls. For more information about Webservice calls, see the Oracle Financial Services Webservices Guide.

Both the OFSECM application and the OFSCRR applications must be configured to use Webservice.

> **NOTE** This is an optional configuration and is required only when you want to integrate the OFSCRR application with the OFSECM application.

**Topics**:

- Configuring Webservice in OFSCRR
- Configuring CRR Service URL in Atomic Schema
- Configuring Webservice in OFSECM
- Configuring Processing Modeling Framework (PMF)
- Populating Identification Type Through Posting
- Populating Phone Number Through Posting

## 5.1 Configuring Webservice in OFSCRR

The OFSCRR application's webservice is already configured with a default username and password. This default password must be reset before the OFSCRR application and the OFSECM application integration. This step is mandatory for security reasons.

To update the password, follow these steps:

1. Log in as the Administrator.
2. Navigate to the Compliance Regulatory Reporting application and select the **Administration** option.
3. Select **Webservice Configuration**. The Configuring Web service User ID and Password page is displayed.
4. Enter the User ID as rruser.

   > **NOTE** Do not add any other user name.

5. Enter the desired password.
6. Click **Save**. A confirmation message is displayed.

## 5.2 Configuring CRR Service URL in Atomic Schema

To configure the CRR service URL in the Atomic Schema, execute the following SQL command:

```
UPDATE CRR_CONFIGURATION SET V_PARAM_VALUE= '<URL>'
WHERE V_PARAM_NAME= 'CRR_SERVICE_URL';
```

```
commit;
```

> **NOTE** <URL> must be in the following format:
> http://<Web application server name>:<port>/<context>

## 5.3 Configuring Webservice in OFSECM

To configure Webservice in the OFSECM application, follow these steps:

1. Login to the OFSECM application as Administrator.
2. Navigate to Financial Services Case Management.
3. Select **Case Management Configuration** and click **Manage Common Parameters**. The Manage Common Parameter page is displayed.
4. Select **Deployment Based** from the Parameter Category drop-down list.
5. Select **Regulatory Report Solution Web Service** from the Parameter Name drop-down list.
6. Set Parameter Value text box = Y.
7. Update the OFSCRR web service URL by setting the following attribute values:
   - Attribute1 value = rruser,
   - Attribute 3 Value = `<URL>/RRSService/InitiateRequest`
   - Attribute 4 Value = `<URL>/CRRframeworkDataingestion`

> **NOTE** <URL> must be in the following format:
> http://<Web application server name>:<port>/<context>

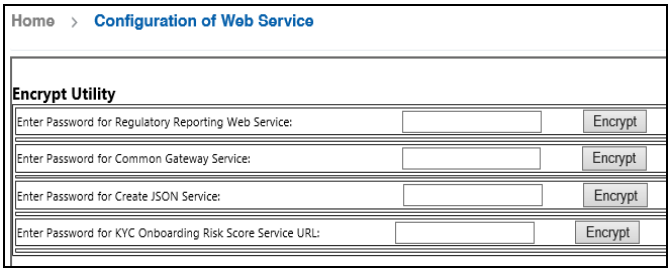
8. Click **Save**. A confirmation message is displayed.

### 5.3.1 Updating OFSCRR Webservice password in OFSECM

To update the OFSCRR Webservice password in OFSECM, follow these steps:

1. Login to the OFSECM application as the Administrator.
2. Navigate to Financial Services Case Management. Select *Case Management Configuration*.
3. Click **Configuration of Web Service**. The Configuration of the Web Service page is displayed.

**Figure 3: Configuration of Web Service**



4. Enter the password for *Regulatory Reporting Web Service* and click **Encrypt**.

> **NOTE** Enter the same password as set in OFSCRR.

5. Logout from the application.

## 5.4 Configuring Processing Modeling Framework (PMF)

The Enterprise Case Management Processing Modeling Framework (PMF) facilitates built-in tooling for the orchestration of human and automatic workflow interfaces. This enables the Administrator to create process-based ECM. It also enables the Administrator to model business processes and workflow.

To perform the PMF configuration, see the Configuring PMF chapter in ECM Administration Guide.

## 5.5 Populating Identification Type Through Posting

To populate data in the Identification Type drop-down list in the Form of Identification in the Subject Information tab, *kdd_case_cust_id_doc.doc_type_cd* table must contain Mantas code.

The mapping between Mantas and CRR code is as follows:

Use Table 6 to map Mantas and CRR codes.

**Table 6: Mapping Mantas and CRR codes**

| Mantas | CRR |
|---|---|
| kdd_case_cust_id_doc.doc_type_cd (table) | FCT_IDENTIFICATION.N_IDTYPE_SKEY (table) |
| Non-Resident Alien Identifier (NR) | Alien registration (1001) |
| Alien Registration Number (AR) | Alien registration (1001) |
| Passport Identifier (PP) | Passport (1002) |
| Any other Mantas code | Other (1000) |

## 5.6 Populating Phone Number Through Posting

If the customer is the suspect in the case and the customer contains phone numbers in the kdd_case_cust_phons table then the CRR application will pick the customer's phone numbers from the above table. If a customer does not have phone numbers in the kdd_case_cust_phons table then the CRR application will pick phone numbers from the kdd_case_involved_party_detail table.

# 6 Configuring Parameters

This chapter explains various configurations performed in the CRR Application.

**Topics**:


- Configuring Report Lock Period
- Configuring Activity Information
- Configuring Default Domain 1
- Transferring Primary CUST ACCT Only
- Configuring Multiple Instances
- Configuring Secure Direct Transfer Mode (SDTM)
- Configuring XSD Parameters
- Configuring Multiple Currencies
- Configuring Unknown Branch Indicator
- Configuring Lookback Period in the Days
- Configuring Purge
- Configuring Due Date
- Configuring CAR


## 6.1 Configuring Report Lock Period

If a user forgets to log off from the OFS CRR application or if the OFS CRR screen is closed while accessing a report, the report gets locked for a pre-configured duration. By default, the duration is 60 minutes. This duration can be altered as per your requirement by changing `<DURATION IN MINUTES>`. It may be more than 60 minutes or less than 60 minutes.

To alter the duration, execute the following SQL using OFS CRR atomic schema user:

```
UPDATE APPLN_PARAMETERS SET V_ATTRIBUTE_VALUE1= '<DURATION IN MINUTES>'

WHERE V_ATTRIBUTE_NAME1= 'LOCK PERIOD IN MINUTES';

COMMIT;
```

## 6.2 Configuring Activity Information

This attribute specifies if the information of activity dates and amount from ECM has to be captured in CRR or not. The field accepts only a Y or N value. Y indicates enabling capturing activity info, and N indicates disabling the same.

This parameter is set to `Y` if activity dates/amount has to be imported from ECM. If not, the parameter is set to `N`.

To configure activity information in the application parameter, follow these steps:

Log into the Atomic schema and execute the following query:

```
UPDATE APPLN_PARAMETERS SET V_ATTRIBUTE_VALUE1 = '<Y or N>' where
n_param_identifier=16;

COMMIT;
```

## 6.3 Configuring Default Domain 1

This parameter identifies the default jurisdiction (domain 1) assignment while creating a report manually in OFSCRR.

Execute the following query in OFSCRR atomic schema as required

```
UPDATE APPLN_PARAMETERS SET V_ATTRIBUTE_VALUE2 = '<VALUE OF DEFAULT DOMAIN 1>' WHERE
V_ATTRIBUTE_NAME1 = 'ENABLE DEFAULT DOMAIN1';COMMIT;
```

By default, the flag to enable default domain 1 in the UI is set to `Y`. OFS CRR can be configured not to display any default value for domain 1 in the UI while creating a new report by setting the flag to `N`.

Execute the following query in OFS CRR atomic schema as required.

```
UPDATE APPLN_PARAMETERS SET V_ATTRIBUTE_VALUE1 = '<Y or N>' WHERE V_ATTRIBUTE_NAME1 =
'ENABLE DEFAULT DOMAIN1';COMMIT;
```

## 6.4 Transferring Primary CUST ACCT Only

This parameter defines the accounts that are transferred from the cases to the CRR Application.

By default, the flag is set to `Y`, which means that only those accounts which are involved in an activity (case) and for which the subject is a primary customer are transferred to the CRR Application.

If you want to bring all the accounts of the subjects involved in an activity (that is, they are part of the case) then set the flag to `N` by executing the below query in the atomic schema.

```
UPDATE APPLN_PARAMETERS SET V_ATTRIBUTE_VALUE1 = 'N' WHERE N_PARAM_IDENTIFIER = 50;
COMMIT;
```

## 6.5 Configuring Multiple Instances

This configuration enables multiple instances (STRs) of the OFS CRR application from the single OFS ECM instance. You can use a single OFS ECM application instance to generate multiple report types.

This section covers the following topics:

- Configuring Multiple Instance Attribute Flag
- Configuring PMF
- Configuring Report URLs
- Configuring Case Jurisdiction and Report Type Mapping
- Configuring Secure Direct Transfer Mode (SDTM)
- Configuring Multiple Reports in the Single Instance

### 6.5.1 Configuring Multiple Instance Attribute Flag

To configure multi instances of the OFS CRR application, follow these steps:

1. Login to the OFSECM application as an Administrator.
2. Navigate to Financial Services Case Management.
3. Select **Case Management Configuration** and click **Manage Common Parameters**. The Manage Common Parameter page is displayed.

4. Select **Deployment Based** on the **Parameter Category** drop-down list.
5. Select **Regulatory Report Solution Web Service** from the Parameter Name drop-down list.
6. Set Parameter Value text box = **Y**.
7. Update the multiple instance attribute flag by setting, **Attribute 6 value = Y**.
8. Click **Save**. A confirmation message is displayed.

### 6.5.2 Configuring PMF

To enable two or more **Generate SAR** actions in the OFS ECM application for each SAR type, you must configure a process modeling framework. For more information, see the *Configuring Processing Modeling Framework* chapter in the Administration and Configuration Guide.

### 6.5.3 Configuring Report URLs

Login into the ECM Atomic Schema and execute the following SQL statement by replacing the placeholder:

```
update KDD_REG_REPORT_TYPE t set t.REPORT_URL = '<URL for SAR>/services/
InitiateRequest' where t.REG_TYPE_CD = 'USSAR';
```

For example, update `KDD_REG_REPORT_TYPE t set t.REPORT_URL = 'http://whf00abc:1200/CRR808/services/InitiateRequest' where t.REG_TYPE_CD = 'USSAR';`

### 6.5.4 Configuring Case Jurisdiction and Report Type Mapping

> **NOTE** One or more jurisdictions can be mapped to only one Regulatory Report Type if the **MultiInstance** option is enabled.
>
> For example, if AMEA and APAC are mapped to US SAR, then they cannot be mapped to any other STRs.

In the Enterprise Case Management (ECM) application, case jurisdiction must be mapped to the report type to generate a report in the OFS CRR US SAR application.

To perform this activity, follow these steps:

1. Login into the ECM Atomic Schema and execute the following SQL statement by replacing the following placeholders
   - **##Jurisdiction Code##** : The values for `KDD_JRSDCN_REPORT_TYPE_MAP.JRSDCN_CD` must come from the table `KDD_JRSDCN.JRSDCN_CD`.
   - **##Regulatory Report Type Code##**: The values for `KDD_JRSDCN_REPORT_TYPE_-MAP.REG_TYPE_CD` must come from the table `KDD_REG_REPORT_TYPE.REG_TYPE_CD`.
2. Insert into `KDD_JRSDCN_REPORT_TYPE_MAP values ('##Jurisdiction Code##', '##Regulatory Report Type Code##');`

   For example, insert into `KDD_JRSDCN_REPORT_TYPE_MAP values ('JRSD1' , 'RTYP1');`

## 6.6 Configuring Secure Direct Transfer Mode (SDTM)

FinCEN's Secure Direct Transfer Mode (SDTM) is a mechanism to transfer E-Files automatically to FinCEN's E-Filing system after an E-File is generated in the OFS CRR US SAR application UI.

This feature allows you to select if you would like to continue with manually submitting files to FinCEN or configure the CRR application to automatically submit them via the SDTM application.

**Configuring Automatic E-File Submission**

If you select to enable SDTM and have an automated submission, then E-Files are transferred automatically to the designated SDTM client directory upon creation. The SDTM client then retrieves these transferred E-Files from the designated directory and uploads them to FinCEN's system.

> **NOTE** If any attachments are included in the report, in that case, E-Files will not be transferred as .xml to the designated directory. It will transfer a zip file containing xml and attachments.

When Message batch is executed, it picks up all the message xmls from the configured folder to be uploaded against respective E-Files in the application.

During this message xml upload process, the Tracking ID is updated (as the BSA ID info is not present in the message xml) in case there is an error, the contents of the message xml is displayed in the Acknowledgement tab.

For more information, see Managing Batches. If the batch is successful, the message XMLs are transferred to the Archive directory.

The SDTM application also retrieves acknowledgements and places them in the designated Acknowledgment directory. An Acknowledgement batch must be executed to parse the received files. Once the batch is successful, all the acknowledgements are parsed against the respective E-Files and then transferred to the Archive directory. These acknowledgements are populated in the Acknowledgment tab of OFS CRR US SAR application UI.

If you select submission mode as automatic and do not enable SDTM, you have to run the E-File batch to transfer E-Files to the designated directory.

> **NOTE** Only system generated E-Files are considered via E-File batch.

**Configuring Manual E-File Submission**

If you select the submission mode to be manual, you have to manually submit the E-Files in FinCEN's E- Filing system, and you have to download the confirmation message XMLs from the same system.

Once the FinCEN's E-Filing system confirms the request, then you can download the Acknowledgement and upload it against the E-File from the E-Filed Status tab in the OFS CRR US SAR application.

Using the SDTM feature, you can also perform the following configurations.

> **NOTE** These configurations are applicable only for Automatic submission if you select submission mode as S.

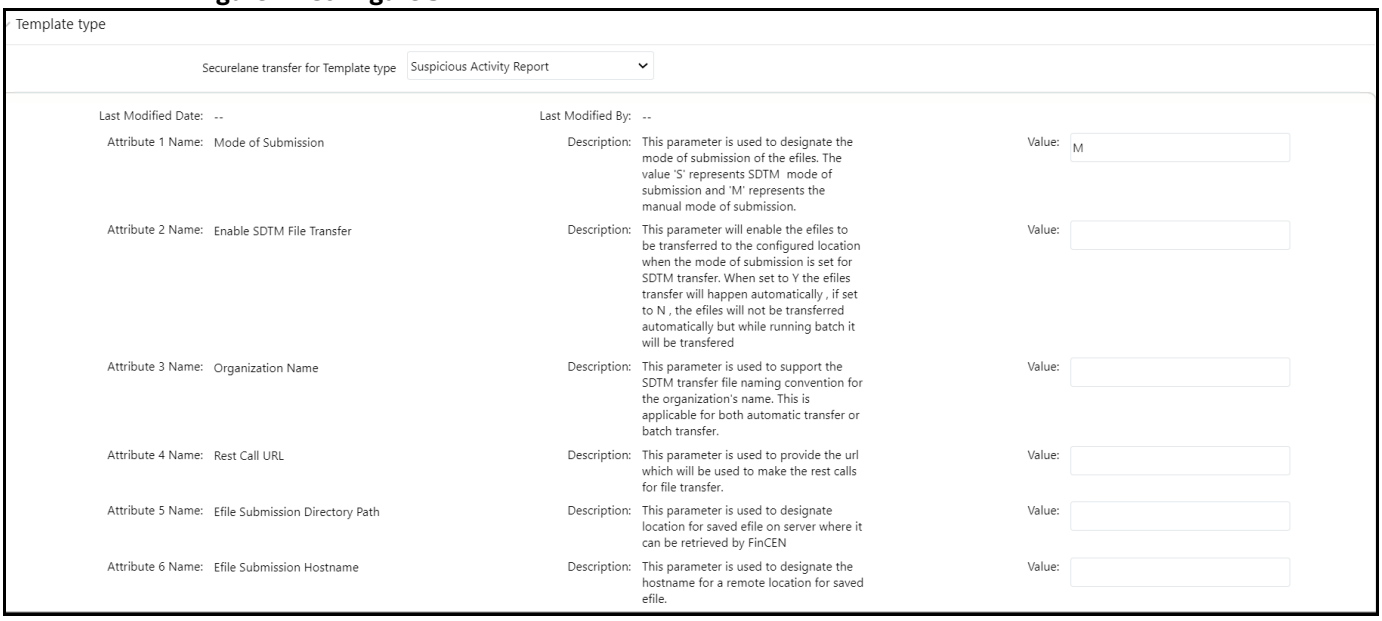
- Configure the E-File submission path, hostname, username, and password for the directory
- Configure Message Directory submission path, hostname, username, and password for the directory

- Configure Acknowledgement Directory submission path, hostname, username, and password for the directory
- Configure the Archive Directory submission path, hostname, username, and password for the directory

To configure SDTM, follow these steps:

1. Log in to the OFS CRR application as an Administrator.
2. Select Compliance Regulatory Reporting.
3. Click **Administration** and select **User Administration**. Click **Configure SDTM Parameters**. The Template Type page is displayed.
4. Select **Suspicious Activity Report** from the SDTM transfer for Template type drop-down. The configuration details are displayed.

**Figure 4: Configure SDTM**




5. Enter the information in the **Value** fields.

   Table 7 provides SDTM configuration parameters.

**Table 7: SDTM Configuration Parameters**

| Fields | Description |
|---|---|
| Attribute 1 Name:<br>Mode of Submission | Enter the mode of submission as S or M in the Value field.<br>This parameter is used to designate the mode of submission of the E-Files. The value 'S' represents the SDTM submission and 'M' represents the manual mode of submission.<br>**NOTE**: If you select M as your mode of submission, then no need to update other fields on the page. M is the default value. |

**Table 7: SDTM Configuration Parameters**

| Fields | Description |
|---|---|
| Attribute 2 Name:<br>Enable SDTM File Transfer | Enter the mode of submission as Y or N in the Value field.<br>If you set it to Y, the E-Files transfer automatically. If you set it to N, the E-Files do not transfer automatically, but if you run the E-File batch, they will be transferred.<br>This parameter enables the E-Files to be transferred to the configured outbound location when the mode of submission is set for SDTM transfer. |
| Attribute 3 Name:<br>Organization Name | Enter the organization name in the Value field.<br>This parameter is used to support the SDTM E-File naming convention for the organization's name. This is applicable for both automatic transfer and E-File batch transfer.<br>SDTM E-File naming convention is as per the FinCEN guidelines - `SARXST.<unique_value>.<SDTM_UID>.xml.`<br>SDTM UID is the organization’s name, and this is the value expected in attribute value -3)<br>For example, `SARXST.20221117153559.sdtmabcbank.xml.` |
| Attribute 4 Name:<br>Rest Call URL | Enter the rest call URL in the Value field.<br>This parameter is used to provide the URL which is used to make the rest calls for E-File transfer from UI.<br>This REST call URL invokes an API that transfers E-Files from application doc storage to an outbound folder.<br>**Note**: This REST call URL is applicable when the Mode of Submission value is set to S and Enable SDTM File Transfer (Attribute 2 Name) value is set to Y.<br>For example, http://<hostname>:<port>/<context> |
| Attribute 5 Name:<br>E-File Submission Directory Path | Enter the full name of the outbound E-File submission directory path in the Value field.<br>This parameter is used to provide the location of the outbound folder which holds the E-Files to be sent to FinCEN via SDTM.<br>For example, directory path -< /scratch/devuser/SDTMFiles/Efiles><br>**Note**: If this directory path is available in the remote server, then you need to provide the Hostname (Attribute 6), Username (Attribute 7), and Password (Attribute 8). |
| Attribute 6 Name:<br>E-File Submission Hostname | Enter the E-File submission hostname in the Value field.<br>This parameter is used to provide the hostname of the outbound location for the E-Files on the server, where it can be sent to FinCEN via the SDTM application.<br>For example, 10.172.10.11<br>**Note**: This field is applicable if the E-File Submission Directory Path is configured on a remote server different from the CRR application server. |

**Table 7: SDTM Configuration Parameters**

| Fields | Description |
|---|---|
| Attribute 7 Name:<br>E-File Submission Username | Enter the E-File submission username in the Value field.<br>This parameter is used to identify the username required to log in to the remote server, which has an outbound directory configured as defined in Attribute 6.<br>**Note**: This field is applicable if the E-File Submission Directory Path is configured on a remote server different from the CRR application server. |
| Attribute 8 Name:<br>E-File Submission Password | Enter the E-File submission password in the Value field.<br>This parameter is used to log in to access the remote outbound directory for E-File submission.<br>**Note**: This field is applicable if the E-File Submission Directory Path is configured on a remote server different from the CRR application server. |
| Attribute 9 Name:<br>Message Directory Path | Enter the message directory path in the Value field.<br>This parameter is used to provide the location of the inbound folder, which holds the messages XML files received from FinCEN via SDTM.<br>For example, the Message Directory path –<br>< /scratch/devuser/SDTMFiles/ Messages><br>**Note**: If this directory path is available in the remote server, then you need to provide the Hostname (Attribute 10), Username (Attribute 11), and Password (Attribute 12). |
| Attribute 10 Name:<br>Message Directory Hostname | Enter the message directory hostname in the Value field.<br>This parameter is used to provide the hostname of the inbound location for the message XML files received from FinCEN via the SDTM application.<br>For example, 10.172.10.11<br>**Note**: This field is applicable if the Message Directory Path is configured on a remote server different from the CRR application server. |
| Attribute 11 Name:<br>Message Directory Username | Enter the message directory username in the Value field.<br>This parameter is used to identify the username required to log in to the remote server which has an inbound directory configured as defined in Attribute 10.<br>**Note**: This field is applicable if the Message Directory Path is configured on a remote server different from the CRR application server. |
| Attribute 12 Name:<br>Message Directory Password | Enter the message directory password in the Value field.<br>This parameter is used for logging in to access the remote an inbound directory for message XML files.<br>**Note**: This field is applicable if the Message Directory Path is configured on a remote server different from the CRR application server. |

**Table 7: SDTM Configuration Parameters**

| Fields | Description |
|---|---|
| Attribute 13 Name:<br>Acknowledgement Directory Path | Enter the acknowledgement directory path in the Value field.<br>This parameter is used to provide the location of the inbound folder which holds the Acknowledgement XML files received from FinCEN via SDTM.<br>For example,<br>Acknowledgement Directory path -< /scratch/devuser/SDTMFiles/ Acknowledgement ><br>**Note**: If this directory path is available in the remote server, then you need to provide the Hostname (Attribute 14), Username (Attribute 15), and Password (Attribute 16). |
| Attribute 14 Name:<br>Acknowledgement Directory Hostname | Enter the acknowledgement directory hostname in the Value field.<br>This parameter is used to provide the hostname of the inbound location for the Acknowledgement XML files received from FinCEN via the SDTM application.<br>For example, 10.172.10.11<br>**Note**: This field is applicable if the Acknowledgement Directory Path is configured on a remote server different from the CRR application server. |
| Attribute 15 Name:<br>Acknowledgement Directory Username | Enter the acknowledgement directory username in the Value field.<br>This parameter is used to identify the username required to log in to the remote server which has an inbound directory configured as defined in Attribute 14.<br>**Note**: This field is applicable if the Acknowledgement Directory Path is configured on a remote server different from the CRR application server. |
| Attribute 16 Name:<br>Acknowledgement Directory Password | Enter the acknowledgement directory password in the Value field.<br>This parameter is used for logging in to access the remote inbound directory for Acknowledgement XML files.<br>**Note**: This field is applicable if the Acknowledgement Directory Path is configured on a remote server different from the CRR application server. |
| Attribute 17 Name:<br>Archive Directory Path | Enter the archive directory path in the Value field.<br>This parameter is used to provide the location of the folder which holds the Archived E-Files, Message XMLs, and Acknowledgement files once the Acknowledgement batch is executed successfully.<br>For example,<br>Archive Directory path -< /scratch/devuser/SDTMFiles/ Archive ><br>**Note**: If this directory path is available in the remote server, then you need to provide the Hostname (Attribute 18), Username (Attribute 19), and Password (Attribute 20). |
| Attribute 18 Name:<br>Archive Directory Hostname | Enter the archive directory hostname in the Value field.<br>This parameter is used to provide the hostname of the Archive directory location.<br>For example, 10.172.10.11<br>**Note**: This field is applicable if the Archive Directory Path is configured on a remote server different from the CRR application server. |

**Table 7: SDTM Configuration Parameters**

| Fields | Description |
|---|---|
| Attribute 19 Name:<br>Archive Directory Username | Enter the archive directory username in the Value field.<br>This parameter is used to identify the username required to log in to the remote server which has the Archive directory location configured as defined in Attribute 18.<br>**Note**: This field is applicable if the Archive Directory Path is configured on a remote server different from the CRR application server. |
| Attribute 20 Name:<br>Archive Directory Password | Enter the archive directory password in the Value field.<br>This parameter is used for logging in to access the remote Archive directory location.<br>**Note**: This field is applicable if the Archive Directory Path is configured on a remote server different from the CRR application server. |

6. Click **Save**. A confirmation message is displayed.

**NOTE** These configurations are applicable only for Automatic submission if you select submission mode as S.

## 6.6.1 Configuring Multiple Reports in the Single Instance

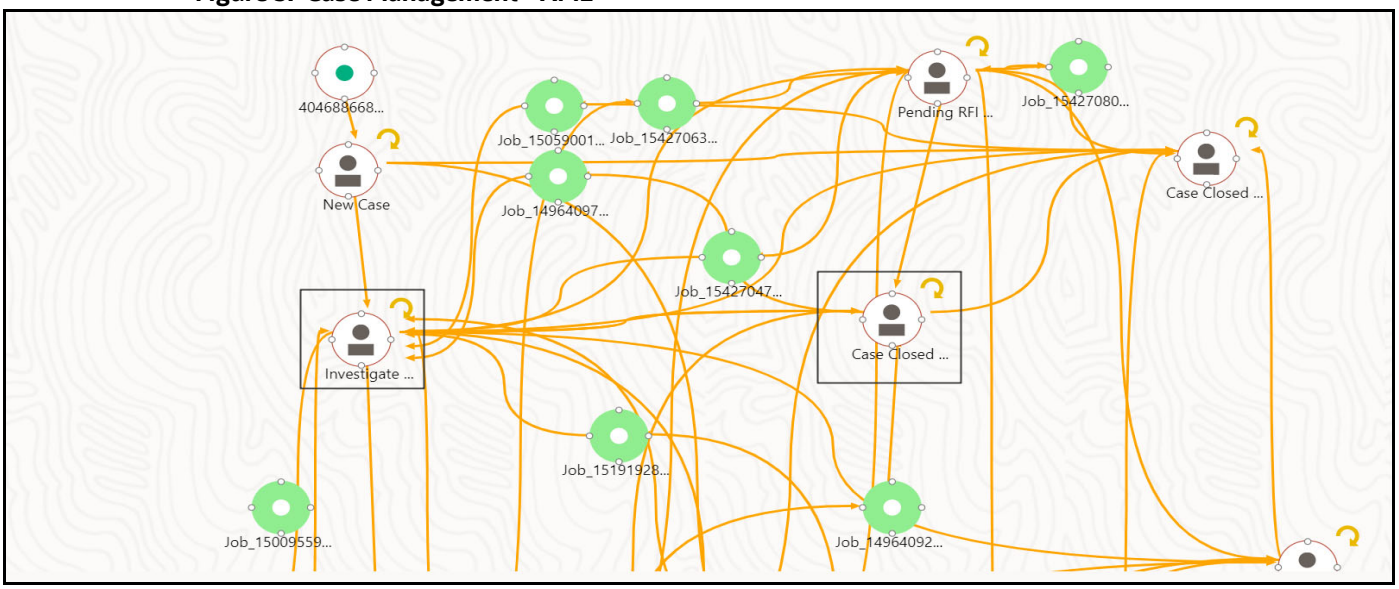
This option allows you to configure multiple report types on a single instance of ECM. For example, you can configure CA STR and US SAR together in one instance of ECM.

This configuration allows you to select one or more report types (SAR or STR) to provide a resolution to the selected case. For example, in the ECM application, you can select US SAR or CA STR to provide a resolution to a selected case.

To configure multiple report types in a single instance, follow these steps:

1. Login to the OFSECM application as an Administrator.
2. Navigate to Financial Services Case Management.
3. Select **Common Tasks** . Click **Process Modelling Framework**. Select **Process Modeller**. The Process Modeller page is displayed.
4. Select **Case Management - AML**. The Case Management - AML page is displayed.

**Figure 5: Case Management - AML**




5. To add another Report (template - US SAR or CS STR), double-click on **Investigate**, an Investigate Case window is displayed.

6. Click **Transition**. The existing jobs are displayed. You can select one of them or add a new transition.

7. To add a new transition, click **Add** icon. The Add New Transition Node Job window is displayed (provides the job number from which you are adding the transition).

8. Click **Connect To**. Select **Case Closed SAR Filed** job from the drop-down list and Transition List - Job_1495627329012_Job_1495627329012.

9. Click **Save**. A confirmation message is displayed.

   The newly added Report type (SAR or STR) is displayed in the OFS ECM Application Take Action window to take action on the selected case for resolution.

## 6.7 Configuring XSD Parameters

This section provides the correct path for MiscellaneousCRR folder for XSD to work.

To configure XSD parameters, follow these steps:

1. Login into Config schema and update the following paramvalue in the query:

   ```
   select * from configuration where paramname ='V_ABS_CONTEXT_PATH';
   ```

2. To get this parmavalue, go to `Deployedpath/<contextname.ear>/<contextname.war>`

> **NOTE** Under this section (Deployedpath/<contextname.ear>/<contextname.war>), you will get MiscellaneousCRR and grant 777 * permission to this folder.

## 6.8 Configuring Multiple Currencies

This feature enables you to decide on what currency column from ECM to be made default currency for a specific report type. For example, US SAR uses the Base currency, whereas CA-STR uses Activity

currency. This parameter is configurable in the application parameter. While fetching data from ECM, the CRR application checks this parameter to determine the default currency for the CRR report type.

To configure multiple currencies in the application parameters, follow these steps:

1. Log into the Atomic schema and execute the following query.

   ```
   update APPLN_PARAMETERS set V_ATTRIBUTE_VALUE2 = 'A' where N_PARAM_IDENTIFIER =
   59;
   ```

   "B" for Base currency type, "A" for Activity currency type and "F" for functional currency type.

## 6.9 Configuring Unknown Branch Indicator

If you want unknown branch indicator must be checked by default, then you must configure it in the Appln_Parameters table.

- If you want unknown branch indicator to be checked by default, then set value as Y.
- If you want unknown branch indicator to be unchecked by default, set value as N or NULL.

To configure unknown branch Indicator in the application parameters, follow these steps:

1. Log into the Atomic schema and execute the following query.

   ```
   update APPLN_PARAMETERS set V_ATTRIBUTE_VALUE1 = 'Y' where N_PARAM_IDENTIFIER =
   58;
   ```

## 6.10 Configuring Lookback Period in the Days

This configuration allows you to customize the Created Date From in the Report Search and List, Approved Tab Search, E-File Tab Search, and Acknowldgment Tab Search.

- Attribute value for Report Search and List - 1
- Attribute value for E-File tab Search and List - 2
- Attribute value for Acknowldgment tab Search and List - 3
- Attribute value for Approved Tab Search and List - 4

To configure the lookback period in days, follow these steps:

1. Login into Atomicschema and update the following paramvalue in the query:

   ```
   update appln_parameters t set t.v_attribute_value1 = <no of days> where
   t.n_param_identifier=57;
   ```

   ```
   E-File Tab
   ```

   ```
   update appln_parameters t set t.v_attribute_value2 = <no of days> where
   t.n_param_identifier=57;
   ```

   ```
   Ack Tab
   ```

   ```
   update appln_parameters t set t.v_attribute_value3 = <no of days> where
   t.n_param_identifier=57;
   ```

   ```
   Approve Tab
   ```

   ```
   update appln_parameters t set t.v_attribute_value4 = <no of days> where
   t.n_param_identifier=57;
   ```

## 6.11 Configuring Purge

This feature allows you to purge reports based on a Purge Look Back Period parameter configuration where anything older that number of months entered into this value is deleted. To execute the purge, you must run the Purge batch job. For more information on Running the batch, see. Managing Purge Batch Tasks.

To configure CRR purge in the application parameter, follow these steps:

1. Log into the Atomic schema and execute the following query.

   ```
   update appln_parameters set V_ATTRIBUTE_VALUE1 =<month> where appln_parame-
   ters.N_PARAM_IDENTIFIER = 60;
   ```

2. Set the number of months your organization requires for report archival.

   **NOTE** Reports which are older than this value are automatically purged.

For example, if regulations require reports to be maintained for six years, you can set the Purge Look Back Period parameter to 72 months. If your organization chooses to maintain these reports for a longer period, set the parameter to meet your business needs.

## 6.12 Configuring Due Date

The Due Date action allows you to set a due date or modify an existing due date of a SAR.

The due date is set based on the date the SAR creation request is sent from the OFS ECM to OFS CRR. This is the period during which the SAR must be filed with FinCEN. The Due date is configurable, and by default, it is set to 30 days from the date of SAR creation as per FinCEN guidelines.

To modify the due date parameter, follow these steps:

1. Log into the Atomic schema and execute the following query.

   ```
   update appln_parameters set V_ATTRIBUTE_VALUE1 = <No of days> where
   t.n_param_identifier=24;
   ```

   Due date= report created date + number of days from the above query.

### 6.12.1 Configuring Set Due Date Button

Use this section to configure the Set Due Date button on the CRR UI.

To configure set due date button, follow these steps:

1. Log in as a *sysadmin* user and select Identity Management.
2. On the Security Management menu, select User Administration, click the **User Group Role Map**.
3. Search for the corresponding group role in the User Group ID (for example, USSUPER, USSUPERVISOR, and so on) . The respective User group roles are displayed.
4. Select the required User Group ID by selecting the checkbox. Mapped roles associated with the selected group role are displayed.
5. Click the **Map** button.

6. Now select or de-select the 'RR Due Date with Edit' for the corresponding group role and click **OK**.

> **NOTE** Selecting 'RR Due Date with Edit' to the group role will display the Set Due Date action button on the Search and List page and Report Details page for the user mapped with the corresponding group role. Deselect 'RR Due Date with Edit' to the group role will remove the Set Due Date action button for the user mapped with the corresponding group role.

7. To authorize the user, log in as *sysauth* and select Identity Management
8. On the Security Management menu, select User Administration, click the **User Group Authorization**.
9. Select the required Group Name and go to Mapped or Unmapped roles section.
10. Select the required role and click **Authorize**.

## 6.13 Configuring CAR

A Continuing Activity Report (CAR) is filed on suspicious activity that continues after an initial SAR is filed with FinCEN.

In the ECM system, when you close and file a SAR on an AML case, a new Continuing Activity (AML_CA) case is created, and an Initial Report is created in the CRR system.

When SAR is uploaded in FinCEN system, the FinCEN revert with Message XML. This Message XML must be uploaded in CRR application via Batch. This where CAR API updates the case due date.

In the CRR system, when an initial SAR is filed with FinCEN, you will receive an Acknowledgment generated by the FinCEN E-File System. The acknowledgment file contains a BSA Identifier.

The SAR filed details are passed to the ECM system. An API URL is invoked to send this information from CRR to ECM.

> **NOTE** This is applicable only for SDTM enabled configuration.

To configure the API URL, follow these steps:

1. Log into the Atomic schema and execute the following query.

   ```
   update appln_parameters set V_ATTRIBUTE_VALUE4 = <http://<hostname>:<port>/
   <context>/ecmcrr-rest-api> where t.n_param_identifier=2;
   ```

   For example, http://<hostname>:<port>/<context>/`ecmcrr-rest-api`

   This API URL update is required to send the Basic Details (Previous Case, Total Suspicious Amount, Date Range of Suspicious Activity, Prior BSA Identification Number, Cumulative Violation Amount, SAR Filed Date), Subject of Previous SAR (Customer, External Entity, and Account), Typologies from the SAR (Cyber Events, Fraud Type, Gaming Activities, etc.), Narrative of the filed SAR, and CAR due date from CRR to ECM.

# 7 Managing Batches

This chapter explains you how to create and execute a new batch. And also guides you how to update, monitor, schedule, and execute the existing batches.

**Topics**:

- Prerequisites for SDTM Batches
- Creating SDTM Batches
- Managing Purge Batch Tasks
- Executing Batches
- Updating Batches

## 7.1 Prerequisites for SDTM Batches

To create and execute the SDTM batches, follow these steps.

1. Navigate the `$FIC_HOME/ficdb/conf` and update the file `CRRRestCALL.properties` with the rest call URL

   For example, `RESTCALL_URL=http://whf00xxx.in.oracle.com:8139/contextname`
2. Navigate to `ficdb/bin` and set the permission for the following sh files to 775.
   - TransferEfileToSecurelane.sh
   - TransferMSGToSecurelane.sh
   - TransferAckToSecurelane.sh

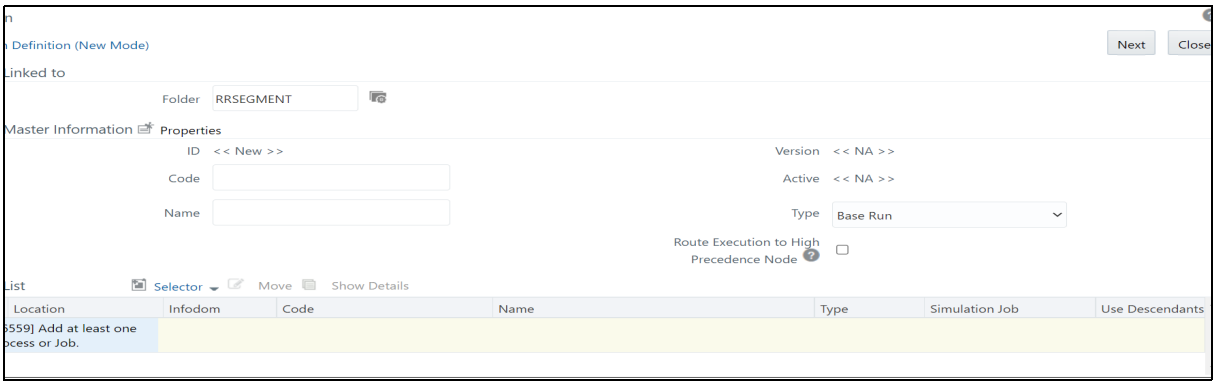
## 7.2 Creating SDTM Batches

Use this section to set new parameters to create SDTM batches.

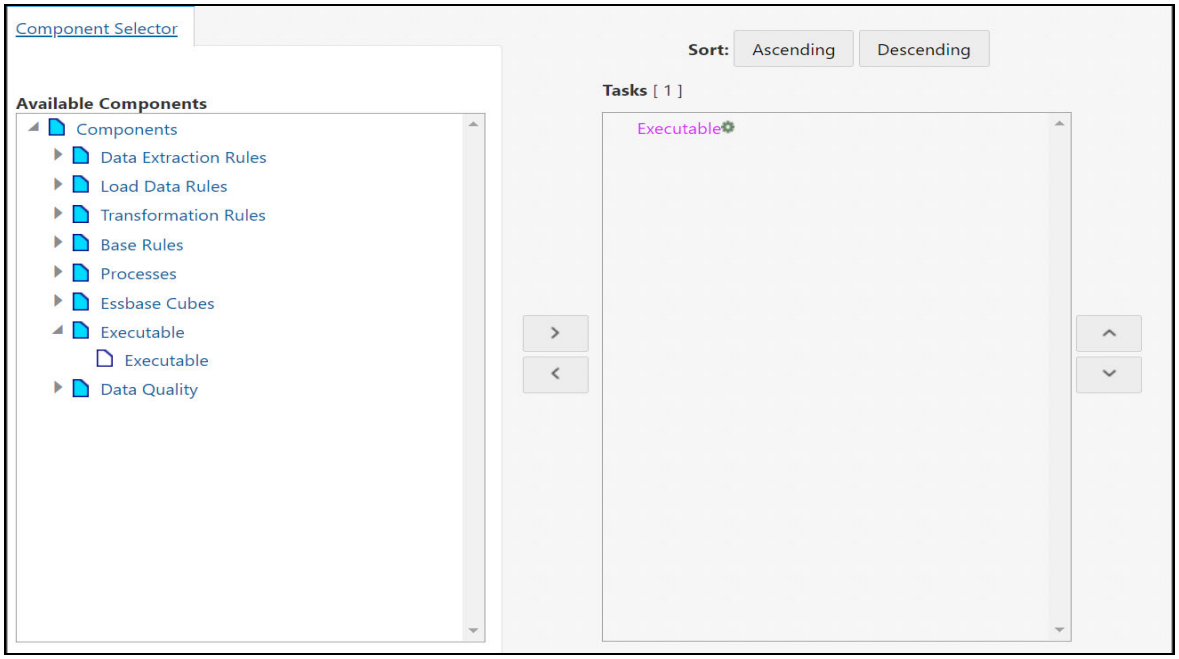
For more information, see Run Rule Framework Chapter in the Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide.

To create the batches, follow these steps:

1. Log in as CRR Administrator user.
2. Click Financial Services Regulatory Reporting. A Navigation List LHS is displayed.
3. Click **Compliance Regulatory Reporting**. Select **Common Tasks**. A common Tasks menu is displayed.
4. Click the **Run** sub-menu in Rule Run Framework. A Run page is displayed.
5. Click the **New** button. A Run Definition page is displayed.
6. Click **Folder** Icon . The Folder Selector window is displayed.
7. Select **RRSEGMENT** folder from the list and click **OK**. The Run page is displayed.




8. Enter a unique code and name in respective fields.
9. Select **Job** from the **Selector** drop-down list. A Selector Component window is displayed.
10. Under the **Available Component** list, expand **Executable** and select **Executable** component and click Right arrow. The selected component is displayed in the Task list.




11. In the Task list, right click on the **Executable** to add parameters.
12. Click on **Add Parameters**. The Parameters dialog is displayed.

> **NOTE** Add values in double quotes. For example, “TransferEfileToSecure-lane.sh”

- parameter 1 - sh file name to be invoked through batch.

  Sh file names for all the batches are as follows:

  - Efile transfer - TransferEfileToSecurelane.sh
  - Acknowledgement Batch - TransferAckToSecurelane.sh

- Message Batch - TransferMSGToSecurelane.sh

- parameter 2 - Batch Id - Any unique number

  For example: "TransferAckToSecurelane.sh","4444"

13. Click OK to add the parameter and click OK again to close the window. The Run Definition page is displayed.
14. Click on the **Next** button on the right top of the page. Click **Save** to complete the batch creation process. A confirmation message is displayed, and click **OK**.

    On successful creation, you are navigated to the Run page and the newly created batch is displayed in the list.

## 7.3 Managing Purge Batch Tasks

CRR Purge is used by financial institutions to purge SAR and exemptions after a configurable period, based on regulatory and business requirements. In order to use the CRR Purge feature, you must run the CRR_Purge batch task.

This task does not display by default. In order to display this task, you must execute a Fire Run.

To create a batch, follow these steps:

1. Log into US SAR application with Admin user.
2. Select **Common Task**. Click **Operation** and then **Batch Maintenance**. The Batch Maintenance page is displayed.
3. For CRR purge, add the task as FN_CRR_PURGE.

For more information on how to create and execute Fire Runs, see Operation section in OFS AAI User Guide.

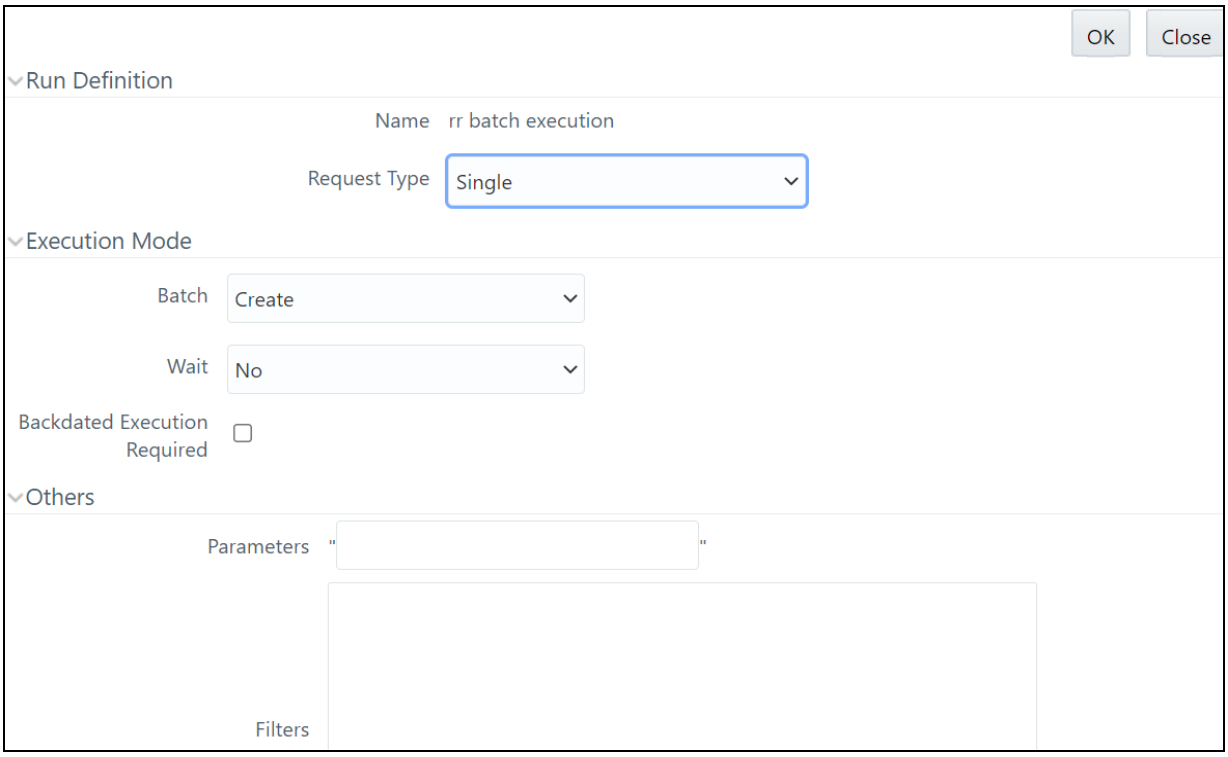
## 7.4 Executing Batches

Use this section to execute newly created batches for the first time.

To execute the batches, follow these steps:

1. Log into US SAR application as Admin user.
2. Select Common Task. Click Operation and then Batch Execution. The Batch Execution page is displayed.
3. For the first time, select Batch Mode as Run. Select required Batch Number
4. Click Execute Batch.

For more information on how to create and execute batches, see Operation section in OFS AAI User Guide.




5. Select **Create and Execute** from the Batch drop-down.
6. Set the MIS date and click **OK**. A confirmation message is displayed. A batch is created and executed for the first time.

## 7.5 Updating Batches

Use this section to update the existing batches that you have created using Run Rule Framework.

For subsequent times, the user can go to the Batch Execution submenu under the Operations.

To update the existing batches, follow these steps:

1. On the **Common Tasks** menu, select **Operations**.

   Using operations, you can perform the following actions. The list of the following operation tasks are displayed. For more information, see Operations Chapter in the Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide.

   - Batch Maintenance
   - Batch Execution
   - Batch Scheduler
   - Batch Monitor
   - Processing Report
   - Batch Cancellation
   - View Log
2. Click **Batch Monitor**. The Batch Monitor page is displayed.

3. Select the required batch, select the Information Date date, Batch Run ID, and click Start Monitoring. The Batch Status, Tasks Details, and Event Logs details are displayed. Based on the details, you can take appropriate action.

**NOTE** Make sure the below servers are up and running before executing the batch apart from App and Web server:

-ICCServer

-MessageServer

-Router

-AMServer

# OFSAA Support Contact Details

Raise a Service Request (SR) in My Oracle Support (MOS) for queries related to OFSAA applications.

# Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.

ORACLE