Oracle Financial Services Compliance Regulatory Reporting

US SAR Administration Guide

Release 8.1.2.2.0

September 2022

F26032-01

ORACLE
Financial Services

ORACLE

OFS CRR US SAR Administration Guide

Document Control

Table 1: Document Control

Version Number	Revision Date	Change Log
1.0	September 2022	No content update

Contents

1 About This Guide

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

Topics:

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 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 • Emphasis
Bold	• An Object of an action (menu names, field names, options, button names) in a step-by-step procedure • Commands typed at a prompt • User input
`Monospace`	• Directories and subdirectories • File names and extensions • Process names • 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

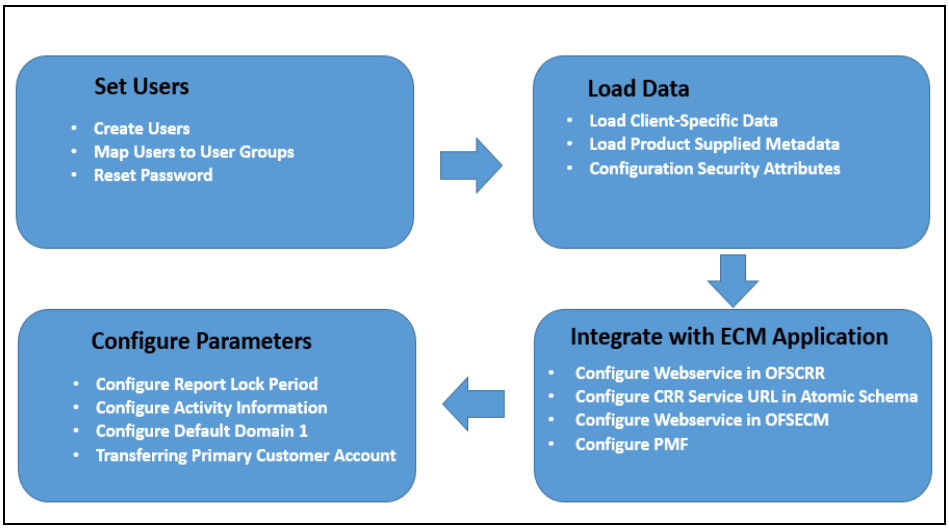


Table 2 lists the administration workflow in tabular format.

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:

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:

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 steps to load the client specific data in to 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 type 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

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.

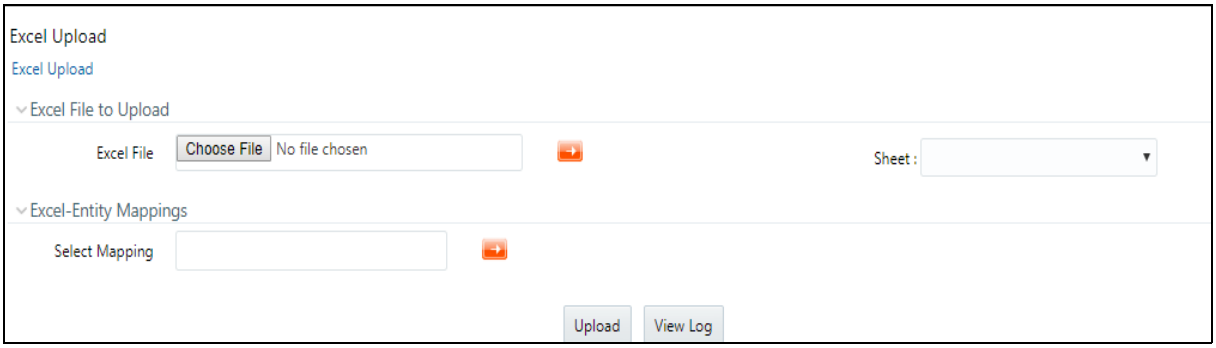


Figure 2: Excel Upload

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:

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 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:

5.1 Configuring Webservice in OFSCRR

The OFSCRR application's webservice is already configured with a default user name 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`

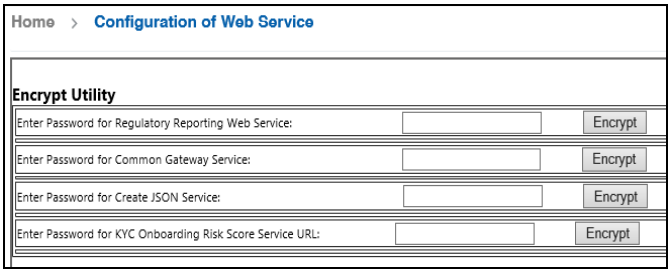
   NOTE <URL> must be in the following format:
   http://<Web application server name>:<port>/<context>
8. Click **Save**. A confirmation message is displayed.

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.

6 Configuring Parameters

This chapter explains various configurations performed in the CRR Application.

Topics:

6.1 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 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 Activity Information

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

```
UPDATE APPLN_PARAMETERS SET V_ATTRIBUTE_VALUE1 = '<Y or N>' WHERE V_ATTRIBUTE_NAME1 =
'ACTIVITY AMOUNT AND DATES FLAG'COMMIT;
```

6.3 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 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

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 STR** actions in the OFS ECM application for each STR 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 **isMultiInstance** 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)

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

This option allows you to select a submission mode as Automatic (select parameter as S) or Manual (select parameter as M) to transfer an E-File to a designated directory.

Configuring Automatic E-File Submission

If you select submission mode as S and enable SDTM as Y then E-Files are transferred automatically to the designated directory. The FinCEN's E-Filing system retrieves these transferred E-Files from the designated directory and uploads them to its system.

The FinCEN E-File system transfers the confirmation message for the submitted E-Files in the designated directory. The message XMLs are parsed against the respective E-Files when the Message batch is executed. For more information, see Managing Batches. If the batch is successful, the message XMLs are transferred to the Archive directory.

An Acknowledgement batch must be executed to parse an acknowledgement received from the FinCEN E-Filing system upon submitting an E-File. The FinCEN's E-Filing system transfers

acknowledgements to the configured Acknowledgment directory. Once the batch is successful, all the acknowledgements are parsed against the respective E-Files and acknowledgement XMLs are 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 S and enable SDTM as N then you have to run the E-File batch to transfer E-Files to the designated directory.

Configuring Manual E-File Submission

If you select submission mode as M then you have to manually submit the E-Files in the FinCEN's E-Filing system and you have to download a 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 option, you can also perform the following configurations.

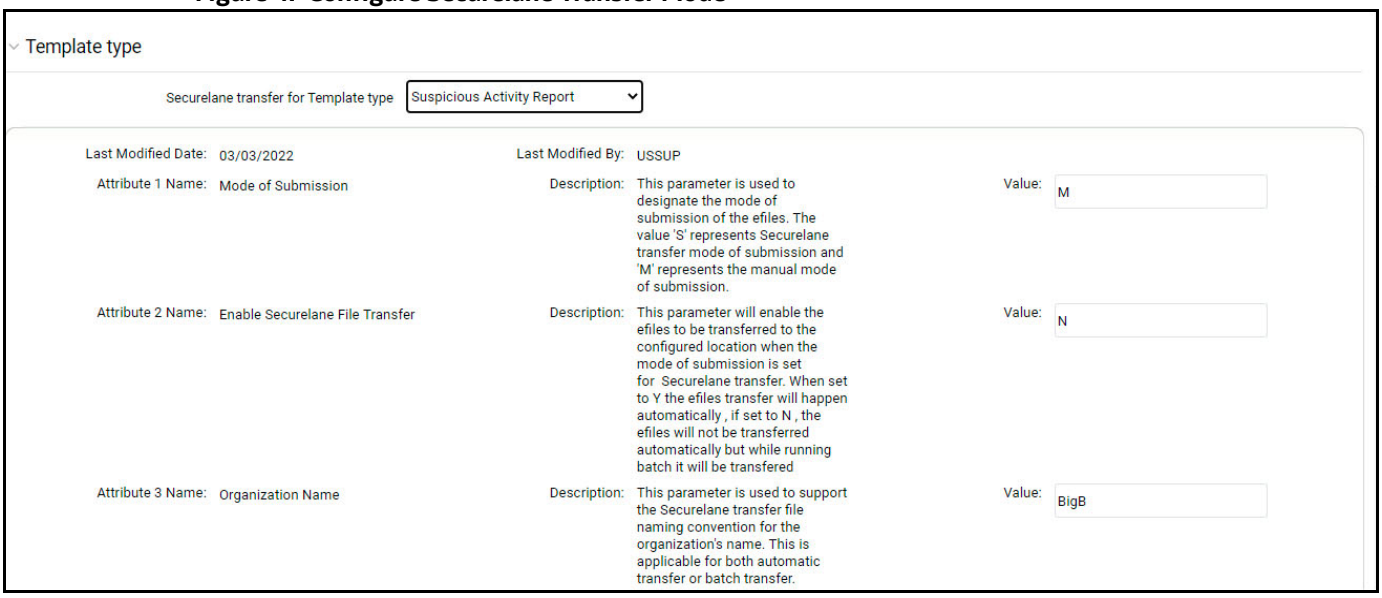
> **NOTE** These configurations are applicable only for Automatic submission. If you select submission mode as S.

- Configure 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 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 Securelane Parameters**. The Template Type page is displayed.
4. Select **Suspicious Activity Report** from the Securelane transfer for Template type drop-down. The configuration details are displayed.

Figure 4: Configure Securelane Transfer Mode



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

   Table 6 provides Securelane Transfer Mode configuration parameters.

Table 6: SDTM Configuration Parameters

Fields	Description
Attribute 1 Name: Mode of Submission	Enter the mode of submission as S or M in the Value field. This parameter is used to designate the mode of submission of the E-Files. The value 'S' represents Securelane transfer mode of submission and 'M' represents the manual mode of submission. **NOTE**: If you select M as your mode of submission, then no need to update other fields on the page.
Attribute 2 Name: Enable Securelane File Transfer	Enter the mode of submission as Y or N in the Value field. If you set to Y, the E-Files transfer automatically. If you set to N, the E-Files do not transfer automatically but if you run the batch they will be transferred. This parameter enables the E-Files to be transferred to the configured location when the mode of submission is set for Securelane transfer.
Attribute 3 Name: Organization Name	Enter the organization name in the Value field. This parameter is used to support the Securelane transfer file naming convention for the organization's name. This is applicable for both automatic transfer and batch transfer.
Attribute 4 Name: Rest Call URL	Enter the name of the rest call URL in the Value field. This parameter is used to provide the URL which is used to make the rest calls for file transfer.
Attribute 5 Name: E-File Submission Directory Path	Enter the name of the E-File submission directory path in the Value field. This parameter is used to designate a location for saved E-File on the server where it can be retrieved by FinCEN.

Table 6: SDTM Configuration Parameters

Fields	Description
Attribute 6 Name: E-File Submission Hostname	Enter the E-File submission hostname in the Value field. This parameter is used to designate the hostname for a remote location for saved E-File.
Attribute 7 Name: E-File Submission Username	Enter the E-File submission user name in the Value field. This parameter is used to identify the user name for the remote directory login for E-File.
Attribute 8 Name: E-File Submission Password	Enter the E-File submission password in the Value field. This parameter is used to identify the encrypted password for the remote directory login for E-File.
Attribute 9 Name: Message Directory Path	Enter the message directory path in the Value field. This parameter is used to designate a location for returned message file on the server where it can be retrieved by FinCEN.
Attribute 10 Name: Message Directory Hostname	Enter the message directory hostname in the Value field. This parameter is used to designate the hostname for a remote location of the response directory.
Attribute 11 Name: Message Directory Username	Enter the message directory username in the Value field. This parameter is used to identify the username for the remote directory login for the response directory.
Attribute 12 Name: Message Directory Password	Enter the message directory password in the Value field. This parameter is used to identify the encrypted password for the remote directory login for the response directory.
Attribute 13 Name: Acknowledgement Directory Path	Enter the acknowledgement directory path in the Value field. This parameter is used to designate a location for returned Acknowledgement file on the server where it can be retrieved by FinCEN.
Attribute 14 Name: Acknowledgement Directory Hostname	Enter the acknowledgement directory hostname in the Value field. This parameter is used to designate the hostname for a remote location of the response directory.
Attribute 15 Name: Acknowledgement Directory Username	Enter the acknowledgement directory username in the Value field. This parameter is used to identify the username for the remote directory login for the response directory.
Attribute 16 Name: Acknowledgement Directory Password	Enter the acknowledgement directory password in the Value field. This parameter is used to identify the encrypted password for the remote directory login for the response directory.
Attribute 17 Name: Archive Directory Path	Enter the archive directory path in the Value field. This parameter is used to designate the location for archiving the E-Files, messages, and acknowledgements after the processing is completed.

Table 6: SDTM Configuration Parameters

Fields	Description
Attribute 18 Name: Archive Directory Hostname	Enter the archive directory hostname in the Value field. This parameter is used to designate the hostname for a remote location for the archive directory.
Attribute 19 Name: Archive Directory Username	Enter the archive directory username in the Value field. This parameter is used to identify the username for the remote archive directory login.
Attribute 20 Name: Archive Directory Password	Enter the archive directory password in the Value field. This parameter is used to identify the encrypted password for the remote archive directory login.

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

6.7 Configuring XSD Parameters

This section provides 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 Lookback Period in Days

This configuration allows you 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 lookback period in days, follow these steps:

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

   ```
   select * from appln_parameters where n_param_identifier='57';
   ```

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:

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

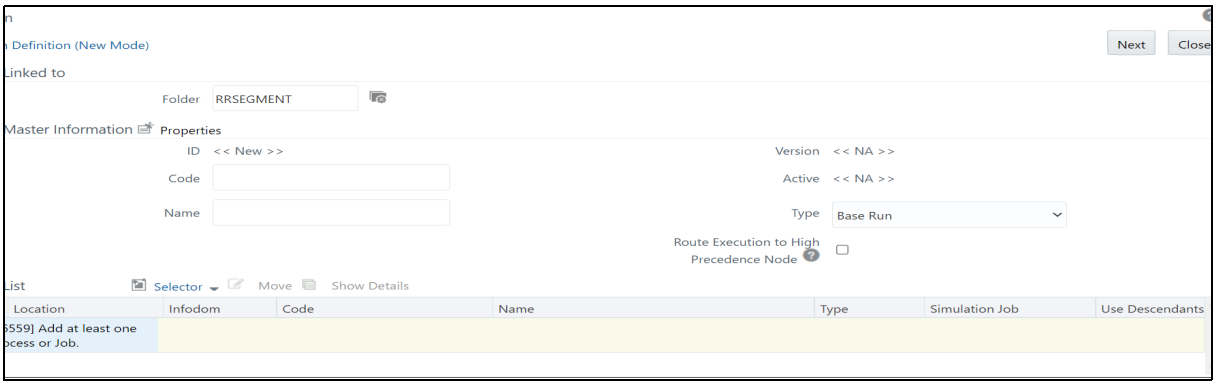
7.2 Creating SDTM Batches

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

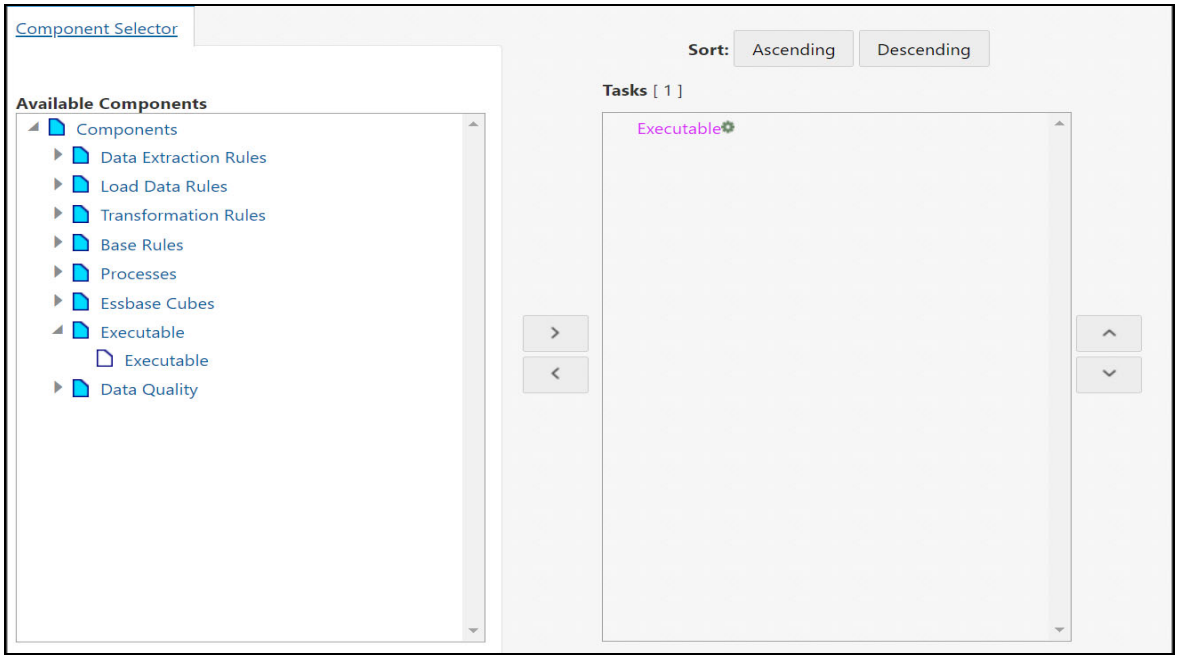
For more information, see Run Rule Framework Chapter in the Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide.

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.

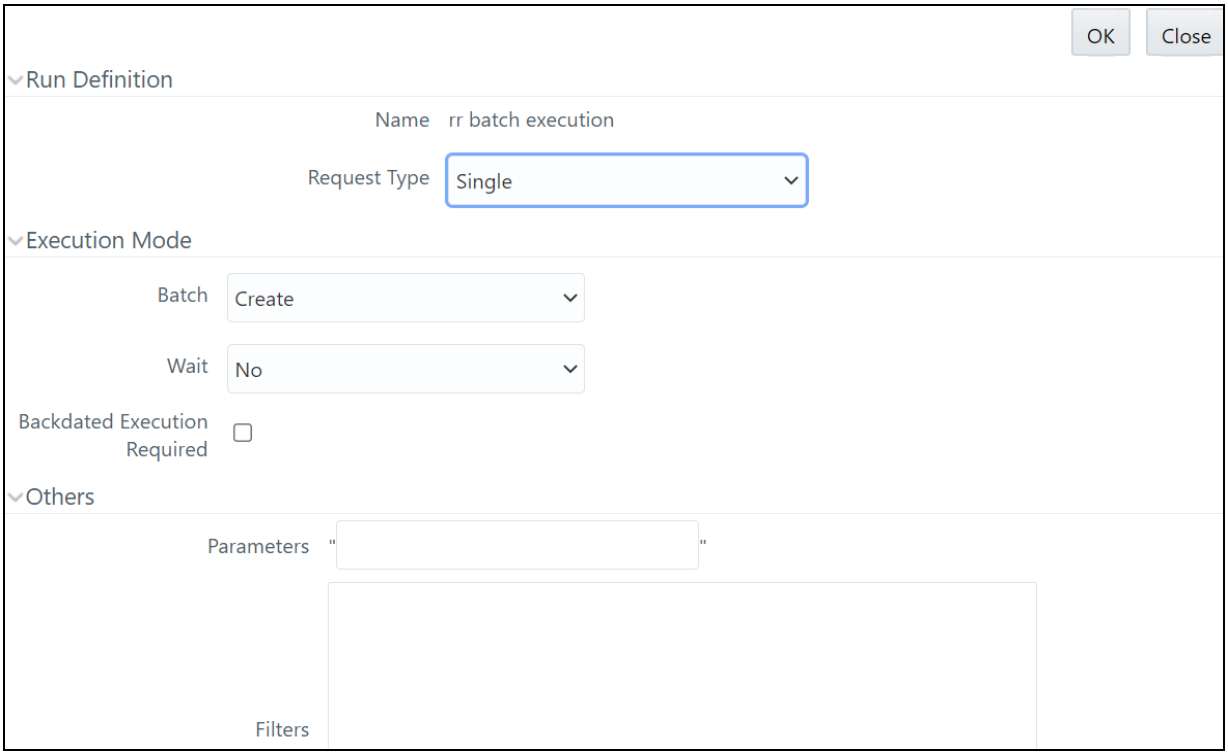
    On successful creation, you are navigated to the Run page and the newly created batch is displayed in the list.

7.3 Executing Batches

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

To execute the batches, follow these steps:

1. On the **Run** page, select the batch from the list or filter batches using search criteria such as Code, Name, Folder, and so on.
2. Click **Fire Run**. The Fire Run window is displayed.



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

7.4 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.