Oracle® Financial Services Customer Screening

Administration Guide

Release 8.1.2.09.0
G31367-07
April 2025

Oracle Financial Services Customer Screening Administration Guide, Release 8.1.2.09.0

G31367-07

Contents

Index

Document Control

Table Revision History

Version Number	Revision Date	Change Log
8.1.2.9.0	January 2026	• Updated Create Database Schema for the new workspace section. • Added Preparing the Dow Jones Watchlist section.
8.1.2.8.0	February 2025	Updated Workspace Creation Post-Configuration section.
8.1.2.8.0	January 2025	Updated Generate User Password and Generate Token sections.
8.1.2.8.0	December 2024	Added Appendix T: CS Matching Batch Issue with EDQ Execution section.
8.1.2.8.0	October 2024	• Added Merging the Events based on the Watchlist ID for CS Alerts section. • Added Appendix S: API to Check the Status of EDQ Job section
8.1.2.8.0	August 2024	• Automatic refresh of DJW Sanction List Reference. • Added content and screens for the section: Registering the OFSAA Environment Details.
8.1.2.7.0	July 2024	• Added point 6 and 7 to the section: Configuring Additional Columns on the Alert List page. • Added section 7.11: Configuring Additional Columns on the Related Alerts page.
8.1.2.7.0	February	• Added Configuring Bulk Action on the Events section. • Added Splitting the Alerts Based on the Event Type Configuration section. • Added Customer Screening Staged Data Simulation Pipeline information in Pipeline section.
8.1.2.6.0	October 2023	Added the following Chapter: • Simulation • Appendix R: Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMITin Python Interpreter • Mandatory Configuration for imported EDQ project

Table (Cont.) Revision History

Version Number	Revision Date	Change Log
8.1.2.5.1	August 2023	• Added CSALRTSTS function code in the Function Codes for User Groups table . • Added Configuring the Customer ID parameter for getting real time alerts in getAlertListForCustIdZipperCS API section.
8.1.2.5.0	June 2023	• Added Reviewer user role information. • Updated Application Level Configuration section with information on Bulk Action. • Added Configuring Bulk Action Feature for the Alert List section. • Added Appendix Q: Function Codes for User Groups section.
8.1.2.4.1	April 2023	• Added Appendix P: Configurations Required to Open ECM Case or CSAM Alert from RT Screening if RT Screening and ECM/ CSAM are in Different Servers section. • Added Appendix O: CS and ECM Table Mapping for Alert Status Customization section. • Added Appendix N: Adding New Alert Level Action and Standard Comments section. • Added Populating Country Code section. • Added Addition of Extra Fields in Customer Details section .
8.1.2.4.0	March 2023	• Added File Upload section. • Added OWS Migration section. • Added Application Level Configuration section. • Added Fix for Primary Key Constraints section.

Table (Cont.) Revision History

Version Number	Revision Date	Change Log
8.1.2.3.0	December 2022	• Added Appendix N: Adding New Alert Level Action and Standard Comments section. • Added Configuring the New Priority section. • Added information about enhanced UI experience in the Queue,Alert List, and Alert Details which support more than the high, medium, and low classifications per queue in Grid View section.
8.1.2.2	October 2022	• Added Merging Case Types section. • Added Screening Watch List Records in Real-Time section with information about source request ID. • Updated Screening Watch List Records in Real-Time with information about merging case types and events. • Added Suppression of Alerts section.
8.1.2.0	July 2022	• Added Enabling L2 Investigation and OAS for Customer Screening. • Added Configuring Additional Columns on the Alert List page.

1

About This Guide

This guide explains the concepts of Oracle Financial Services Customer Screening (OFS CS) and provides step-by-step instructions to navigate to the Customer Screening web pages, analyzing, acting on, and researching the business information.

1.1 Intended Audience

The instructions in this guide are written with the assumption that the user has a good understanding of Enterprise Case Management (ECM), Financial Crime Data Model (FCDM), Oracle Enterprise Data Quality (OEDQ) and has knowledge of Sanctions (SAN), Politically Exposed Persons (PEP), Enhanced Due Diligence (EDD), and Country Prohibition Screening (PRB).

The Customer Screening User Guide is designed for the following users:

- **Analyst:** This user works on the alerts within the application frequently. This user's specific role determines what they can view and perform within the application.
- **Supervisor:** This user works on the alerts within the application daily and is typically a higher- level Analyst or Compliance Officer.

1.2 Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support (MOS).

For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info

OR visit:

http:// www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing-impaired.

1.3 How this Guide is Organized

The Customer Screening User Guide includes the following chapters:

- Introduction provides an overview of Customer Screening and the architecture used.
- Getting Started explains common elements of the interface and how to configure the Financial Services Analytical Applications Customer Screening home page.
- General Configurations provides information on how to prepare watch list data, configure the different property files in Customer Screening, how to download the full and delta watch lists, how to filter watch list data, and how to configure General Data Protection Regulations (GDPR) for users.
- Integrations with Enterprise Case Management provides information on the different cases classes used for Customer Screening in Enterprise Case Management, view the correlation rules, what cases are linked to the case being investigated, and the workflows used for the different case types.
- Real-Time Screening shows the real-time user interface used for Customer Screening and how to run the real-time screening job using the Financial Data Crime Model (FCDM).

- Batch Screening provides information on how to prepare and analyze data and how to run the batch screening job using the Financial Data Crime Model (FCDM).
- OWS Migration provides information about migrating the existing Oracle Watchlist Screening (OWS) customer data to Oracle Financial Services Customer Screening (OFS CS).
- Simulation provides information about the user to test new configurations in a sandbox environment and compare the results with the existing set-up by integrating with the OFS Compliance Studio Application.
- ML Integration with Customer Screening provides information about the step-by-step instructions to integrate ML with customer screening.
- Appendix A: Screening Non-Latin Character Sets provides information on how to perform matching for non-Latin data.
- Appendix B: Risk Scoring Reference Data shows the different reference data tables used to calcu- late risk scores in Customer Screening.
- Appendix C: Preconfigured Watch List Information provides information on the different watch lists used in Customer Screening.
- Appendix D: Splitting Jobs Using Multiple EDQ Servers provides information on splitting jobs across multiple severs.
- Appendix E: Viewing Snapshots of Tables in EDQ provides information on the EDQ table UI.
- Appendix F: Configurations for the Bearer Token provides information on the Bearer Token con- figuration.
- Appendix G: Error Logs provides information on the types of failure encounters.
- Appendix H: Out Of Box process to move Alerts from CS_ALERTS of one DB instance to FCC_ZCS_ALERTS of another DB instance.
- Appendix I: API to create the Alerts in the Zipper Alerts table (FCC_ZCS_ALERTS) provides information on steps to configure system to create Zipper Alerts.
- Appendix J: PMF Configurations for Pool of Analyst provides information on PMF configuration.
- Appendix K: Invoking the PMF Workflow from backend provides information on invoking the PMF Workfkow from backend for the Alert.
- Appendix L: Mapping the PMF Workflow for Different Jurisdiction and domain provides information on the `AAI_WF_APP_DEFINITION_MAP` table in Config Schema stores the mapping of object type data to the Process Modeller Framework (PMF) workflow.
- Appendix M: User Group Customization provides information on User Group Customization.
- Appendix N: Adding New Alert Level Action and Standard Comments
- Appendix O: CS and ECM Table Mapping for Alert Status Customization
- Appendix P: Configurations Required to Open ECM Case or CSAM Alert from RT Screening if RT Screening and ECM/CSAM are in Different Servers
- Appendix Q: Function Codes for User Groups
- Appendix R: Setting the ZEPPELIN_INTERPETER_OUTPUT_ LIMIT in Python Interpreter
- Appendix S: API to Check the Status of EDQ Job
- Appendix T: CS Matching Batch Issue with EDQ Execution

Related Topics

- #unique_45/unique_45_Connect_42_GUID-E1E2C87F-6929-46E1-B262-197A7B596A56

1.4 Where to Find More Information

For more information about Oracle Financial Services Customer Screening, see the following Customer Screening application documents, which can be found on the Oracle Help Center page:

- Oracle Financial Services Customer Screening Matching Guide
- Oracle Financial Services Customer Screening Data Interfaces Guide

To find additional information about how Oracle Financial Services solves real business problems, see our website at Oracle for Financial Services Home page.

1.5 Conventions Used in This Guide

The following table mentions the conventions used in this guide.

Table 1-1 Conventions Used

Conventions	Meaning
Italics	Namesof books as references Emphasis Substituteinput values
Bold	Menunames, field names, options, button names Commands typed at a prompt Userinput
Monospace	Directoriesand subdirectories File names and extensions Codesample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text
Hyperlink	Hyperlinktype indicates the links to external websites, internal document links to sections.
Asterisk (*)	Mandatory fields in User Interface.
<Variable>	Substitute input value.

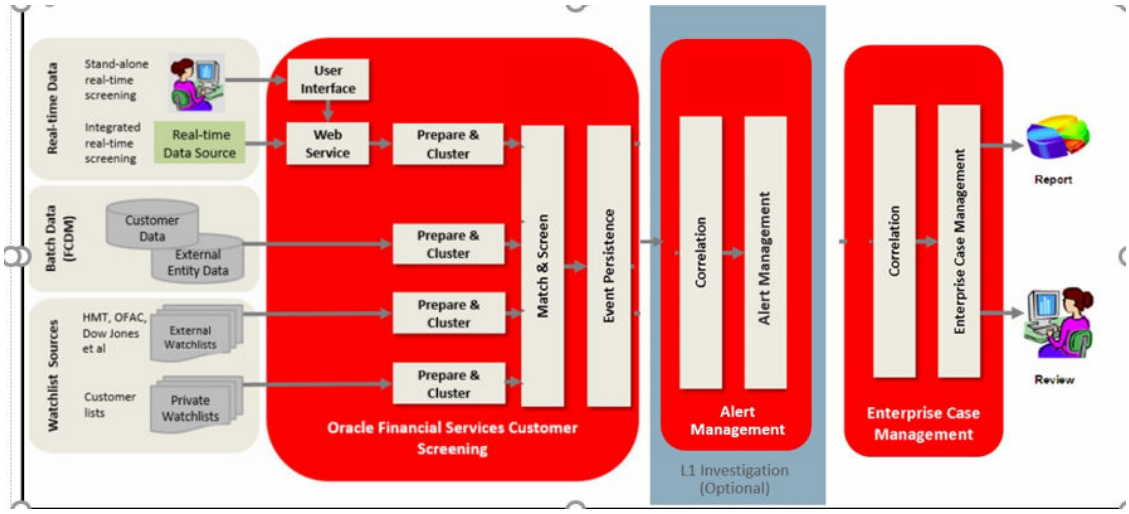
2 Introduction

Oracle Financial Services Customer Screening (OFS CS) enables organizations to effectively and efficiently screen their customers so that they can successfully meet anti-bribery, anti-corruption, export control, and other legal regulations as well as to meet anti-money laundering and counter- terrorist financing legislations. Screening customers enables organizations to keep track of and avoid the risk of being exposed to suspicious or sanctioned individuals and organizations. Customer Screening uses the Oracle Enterprise Data Quality (OEDQ) platform to manage watch list data and apply match rules, Process Modelling Framework (PMF) to generate alerts, and Enterprise Case Management (ECM) to investigate cases generated from the alerts based on the match rules.

2.1 Architecture Overview

This image shows the movement of data from a real-time data source, data from watch list sources such as OFAC, HM Treasury, and Dow Jones. This data then moves to the Customer Screening user interface where it is prepared and screened. Finally, cases are generated based on the matches in Enterprise Case Management (ECM). We have also introduced Alert Management for L1 investigation for rapid dis-positioning of Alerts (optional).

Figure 2-1 Customer Screening Architecture



3
Getting Started

This chapter provides step-by-step instructions to login to the Oracle Financial Services Customer Screening (OFS CS) application and the different features of the application.

3.1 Accessing the Financial Services Analytical Applications Customer Screening Home Page

Access to the Customer Screening application depends on the Internet or Intranet environment. The system administrator provides the intranet address uniform resource locator (URL), User ID, and Password.

> **Note**
>
> The first time you log in, you will be prompted to change your password.

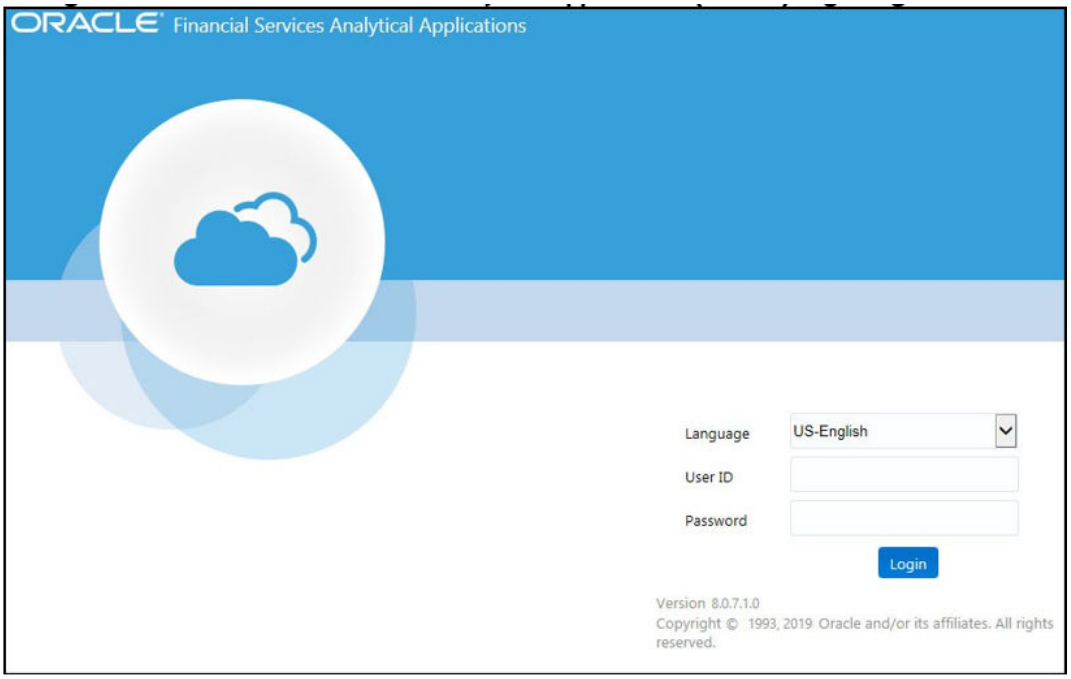
To access the **Oracle Financial Services Analytical Applications Customer Screening Home page**, follow these steps:

1. Enter the URL into your browser using the following format:
   `<scheme/ protocol>://<ip address/ hostname>:<port>/<context-name>/ login.jsp`

   For example: `https://myserver:9080/ofsaaapp/login.jsp`

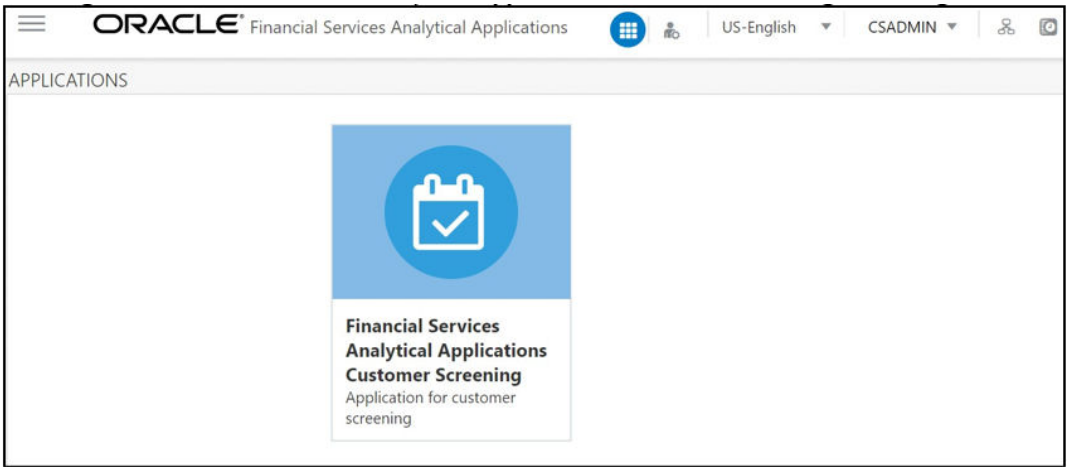
   The Oracle Financial Services Analytical Applications (OFSAA) login page is displayed.

Figure 3-1 OFSAA login page



2. Select the language from the **Language** drop-down list. This allows you to use the application in the language of your selection.
3. Enter your User ID and Password in the respective fields.
4. Click **Login**. The **Financial Services Analytical Applications Customer Screening** Home page is displayed.

Figure 3-2 Financial Services Analytical Applications Customer Screening tile



Click the **Financial Services Analytical Applications Customer Screening** tile to open the OFS CS Home page.

3.2 Managing the Oracle Financial Services Analytical Applications (OFSAA) Page

From the OFSAA Application page, you can access the menus for the different message configurations. For information on the different menus, see Oracle Financial Services Analytical Applications Infrastructure Administration and Configuration Guide.

> **Note**
>
> To create, edit user definitions, view, manage, modify, and delete user information, see the User Maintenance section in the Oracle Financial Services Advanced Analytical Applications Infrastructure User Guide 8.1.1.0.0.

3.3 Queue Management

Queue Management is a common dashboard where the following users can see queues related to CS and TF that are created by the Queue Administrator and the System (Out Of Box):

- Reviewer
- Analyst
- Supervisor
- Senior Supervisor
- Queue Administrator

You can view the Queue details in the following formats:

- List View
- Grid View

By default, queue details are displayed in the List View. Only queue admin can assign the user groups for the queues in the Grid View.

For more information on Queue Administrator, see the **OFS Sanctions Queue Management User Guide**.

3.3.1 List View

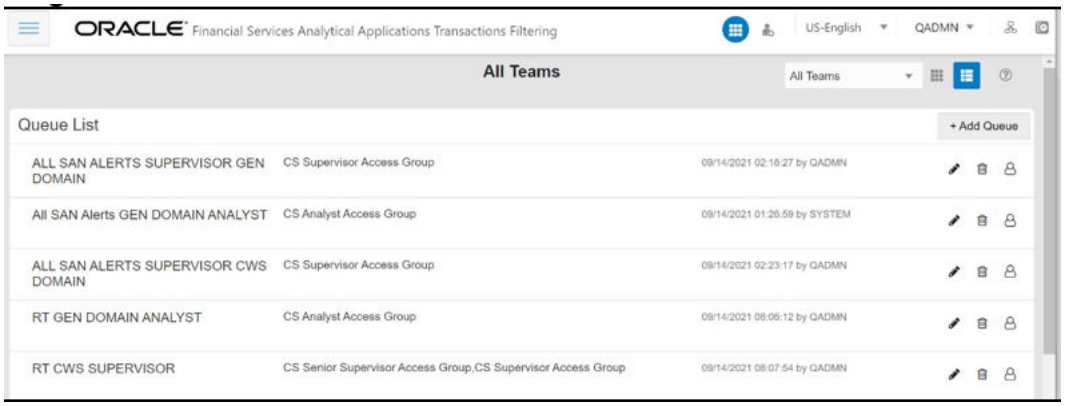
1. Log in to the application as Reviewer, Analyst, Supervisor, or Senior Supervisor.
2. Select the Financial Services Analytical Applications Customer Screening.
3. From the Application Navigation List, select Queue Management.

You can select the **hamburger** icon to view the Queue List for **All Teams** in List View.

By default, queue details are displayed in the List View.

Queue List displays the queues assigned to all user groups and the value. **All Team** is selected in the drop-down list and is disabled. It is displayed as the title for Queue List.

Figure 3-3 Queue List in List View



The following details are displayed in the List View for **All Team**:

- Queue Name
- User Group names (that are assigned by the Queue Administrator)
- Date Time Created By (For example, 09/09/2021 14:06:39 by QADMIN/SYSTEM)
- Queue Action

You can view ten queues in Queue List and use the navigation to view the next set of queues.

You can perform the following actions on each queue:

- **+Add Queue:** Click button top-right in the Queue List to add a new queue (only for Queue Admin).
- **Delete:** Click the Ellipsis menu and then select Delete and click **Yes** to delete the queue.
- **Edit:** Click the Ellipsis menu and then select Edit to edit the queue details and click **Finish**.
- **Open:** Click the Ellipsis menu and then select Open to open the queue to see its details.
- **Assign:** Click the Ellipsis menu and then select Assign to assign the queue to Groups (only for Queue Admin).
  - Select the Groups to assign the queue.
  - Click Assign.

You can change the order of queues are as follows:

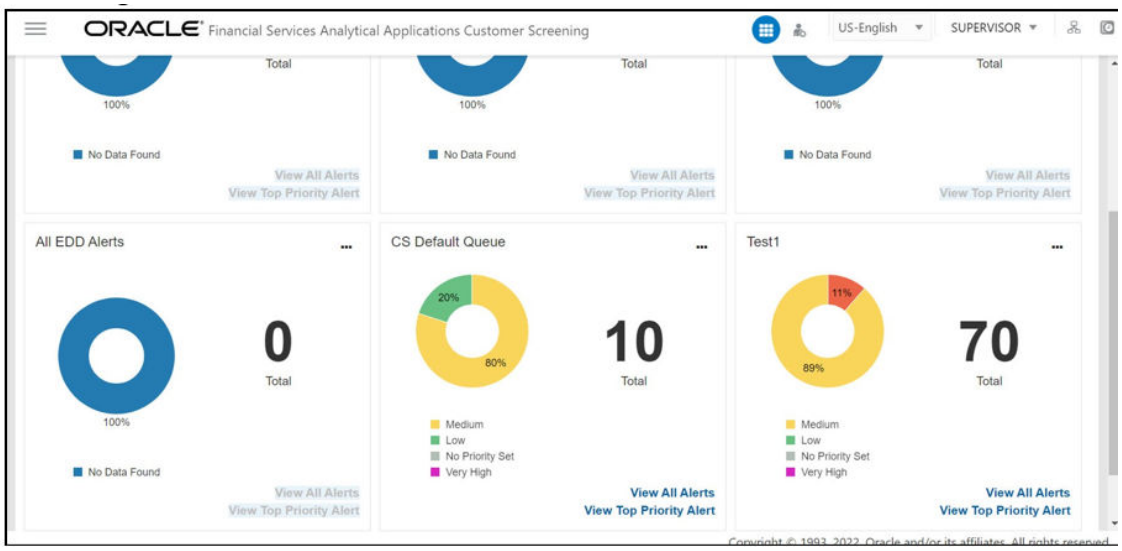
- According to your requirement, you can select the Queue to change the order, drag and drop in the list.
- Perform the following steps:
  1. Select the Queue and right-click. The menu options are displayed as **Cut**, **Paste Before**, and **Paste After**. The only Cut is enabled.
  2. Select **Cut**.
  3. Locate the cursor wherever it needs to be added and right-click. The menu options are **Cut**, **Paste Before**, and **Paste After**. Only **Paste Before** and **Paste After** are enabled.
  4. Select the **Paste Before** or **Paste After** to place the Queue.

3.3.2 Grid View

You can select the thumb view icon to view the **Queue List** for **All Teams** in Grid View.

Queue List displays the queues assigned to all user groups and the value. **All Team** is selected in the drop-down list and is disabled. It is displayed as the title for Queue List.

Figure 3-4 Queue List in Grid View



> **Note**
>
> Only Reviewer/Analyst/Supervisor/Senior Supervisor can view the number of alerts details in each Queue.

The Queue List appears in doughnut charts displays each cell's data as a slice of a doughnut. A pie chart data visualization uses a single circle divided into "slices," each slice representing a numerical proportion of the whole circle's value. Hover over the slices to see the details of the **Series** and the **Value** of the queue.

By default, the color-coding displayed for three priorities of the alerts and the **Total** numeric value indicates the number of alerts in that Queue.

The following are the default priorities in the application:

- High
- Medium
- Low

An Admin can configure any number of priorities and color code that needs to be displayed on the Queue Management Dashboard against each of the priority based on their requirement in the backend based on the match score, screening type, event type, jurisdiction and business domain.

The Queue Management dashboard displays all the priorities defined by the admin and the number of alerts meeting the priority condition. If there are alerts which does not fall under any priority criteria are displayed as **No Priority Set**.

To configure the priorities and color code see Configuring the New Priority section.

Priority configuration for all the alerts to be defined before Customer Screening.

You can view six queues in Queue List and use the navigation to view the next set of queues. You can perform the following actions on each queue:

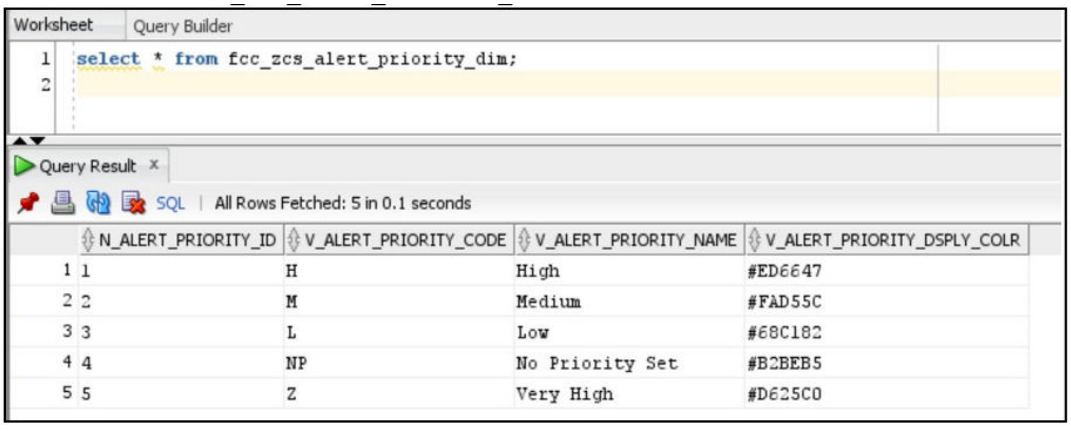
- **+Add Queue:** Click button top-right in the Queue List to add a new queue (only for Queue Admin).
- **Delete:** Click the Ellipsis menu and then select Delete and click **Yes** to delete the queue.
- **Edit:** Click the Ellipsis menu and then select Edit to edit the queue details and click **Finish**.
- **Open:** Click the Ellipsis menu and then select Open to open the queue to see its details.
- **Assign:** Click the Ellipsis menu and then select Assign to assign the queue to Groups (only for Queue Admin).
  - Select the **Groups** to assign the queue.
  - Click **Assign**.

3.3.3 Configuring the New Priority

To configure the priority and color code for the alerts, follow the below steps:

1. Access the Atomic Schema and access the FCC_ZCS_ALERT_PRIORITY_DIM table.
2. Change the following parameter value:
   - N_ALERT_PRIORITY_ID
   - V_ALERT_PRIORITY_CODE
   - V_ALERT_PRIORITY_NAME
   - V_ALERT_PRIORITY_DSPLY_COLR

Figure 3-5 FCC_ZCS_Alert Priority_DIM_table



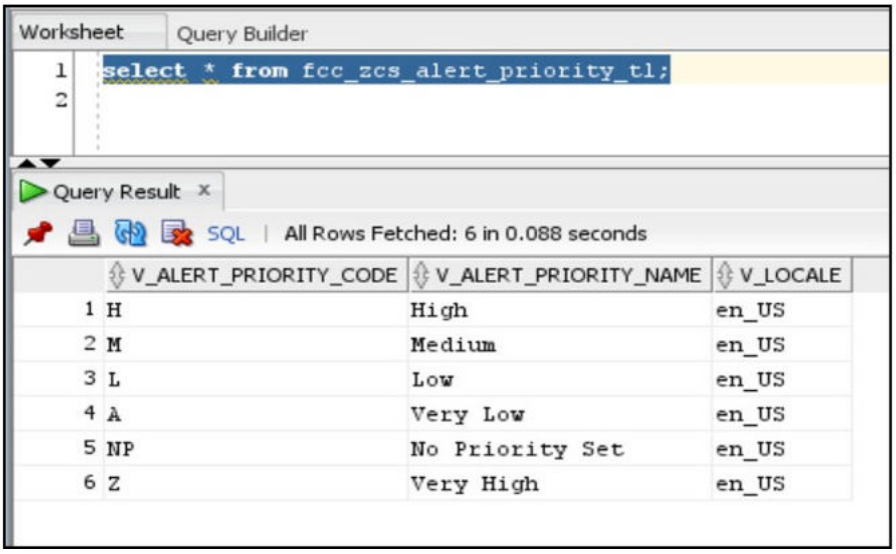

```
MERGE INTO FCC_ZCS_ALERT_PRIORITY_DIM T USING (
SELECT '4' N_ALERT_PRIORITY_ID, 'B' V_ALERT_PRIORITY_CODE, 'Lower
```

```
Medium' V_ALERT_PRIORITY_NAME, '#25C0D6' V_ALERT_PRIORITY_DSPLY_COLR
FROM DUAL) S
ON ( T.N_ALERT_PRIORITY_ID = S.N_ALERT_PRIORITY_ID )
WHEN MATCHED THEN UPDATE SET T.V_ALERT_PRIORITY_CODE =
S.V_ALERT_PRIORITY_CODE, T.V_ALERT_PRIORITY_NAME =
S.V_ALERT_PRIORITY_NAME, T.V_ALERT_PRIORITY_DSPLY_COLR =
S.V_ALERT_PRIORITY_DSPLY_COLR
WHEN NOT MATCHED THEN INSERT
(N_ALERT_PRIORITY_ID,V_ALERT_PRIORITY_CODE,V_ALERT_PRIORITY_NAME,V_ALERT
_PRIORITY_DSPLY_COLR)
VALUES
(S.N_ALERT_PRIORITY_ID,S.V_ALERT_PRIORITY_CODE,S.V_ALERT_PRIORITY_NAME,S
.V_ALERT_PRIORITY_DSPLY_COLR)
/
```

3. **Access** the FCC_ZCS_ALERT_PRIORITY_TL **table**.
4. Change the following parameter value:
   - V_ALERT_PRIORITY_CODE
   - V_ALERT_PRIORITY_NAME
   - V_LOCALE

> **Note**
>
> The FCC_ZCS_ALERT_PRIORITY_DIM table and FCC_ZCS_ALERT_PRIORITY_TL table must have the same parameter value entry.

Figure 3-6 FCC_ZCS_Alert_Priority_TL




```
MERGE INTO FCC_ZCS_ALERT_PRIORITY_TL T USING (
SELECT 'B' V_ALERT_PRIORITY_CODE, 'Lower Medium' V_ALERT_PRIORITY_NAME,
'en_US' V_LOCALE FROM DUAL) S
ON ( )
```

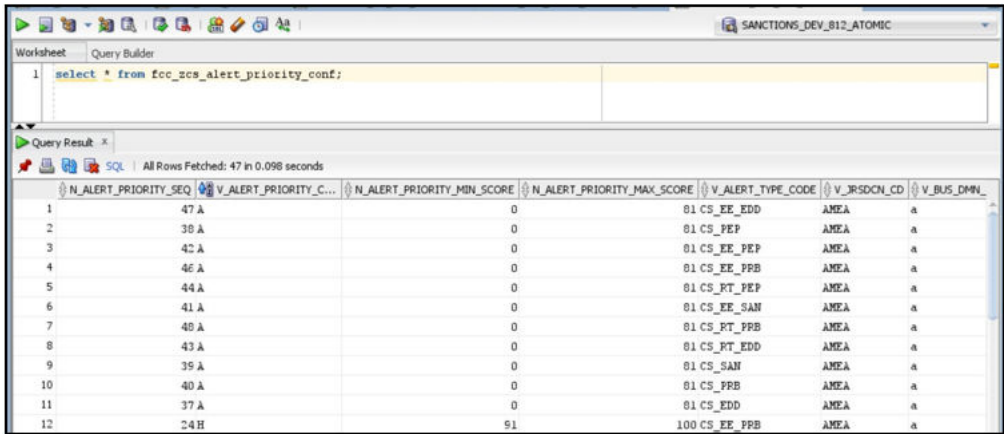
```
WHEN MATCHED THEN UPDATE SET T.V_ALERT_PRIORITY_CODE =
S.V_ALERT_PRIORITY_CODE, T.V_ALERT_PRIORITY_NAME =
S.V_ALERT_PRIORITY_NAME, T.V_LOCALE = S.V_LOCALE
WHEN NOT MATCHED THEN INSERT
(V_ALERT_PRIORITY_CODE,V_ALERT_PRIORITY_NAME,V_LOCALE)
VALUES
(S.V_ALERT_PRIORITY_CODE,S.V_ALERT_PRIORITY_NAME,S.V_LOCALE)
/
```

The priority for the new alerts are decided based on the score configured for the priority.

To define the priority and color code for the new alerts created based on the score, follow the below steps:

1. Access the Atomic Schema and access the FCC_ZCS_ALERT_PRIORITY_CONF table.
2. Change the following parameter value:
   - N_ALERT_PRIORITY_SEQ
   - V_ALERT_PRIORITY_CODE
   - N_ALERT_PRIORITY_MIN_SCORE
   - N_ALERT_PRIORITY_MAX_SCORE
   - V_ALERT_TYPE_CODE

Figure 3-7 FCC_ZCS_Alert_Priority_Conf_table




```
MERGE INTO FCC_ZCS_ALERT_PRIORITY_CONF T USING (
SELECT '37' N_ALERT_PRIORITY_SEQ, 'B' V_ALERT_PRIORITY_CODE, '81'
N_ALERT_PRIORITY_MIN_SCORE, '85' N_ALERT_PRIORITY_MAX_SCORE, 'CS_RT_SAN'
V_ALERT_TYPE_CODE, 'AMEA' V_JRSDCN_CD, 'a' V_BUS_DMN_LIST_TX FROM DUAL)
S
ON ( T.N_ALERT_PRIORITY_SEQ = S.N_ALERT_PRIORITY_SEQ )
WHEN MATCHED THEN UPDATE SET T.V_ALERT_PRIORITY_CODE =
S.V_ALERT_PRIORITY_CODE, T.N_ALERT_PRIORITY_MIN_SCORE =
S.N_ALERT_PRIORITY_MIN_SCORE, T.N_ALERT_PRIORITY_MAX_SCORE =
S.N_ALERT_PRIORITY_MAX_SCORE, T.V_ALERT_TYPE_CODE = S.V_ALERT_TYPE_CODE,
T.V_JRSDCN_CD = S.V_JRSDCN_CD, T.V_BUS_DMN_LIST_TX = S.V_BUS_DMN_LIST_TX
WHEN NOT MATCHED THEN INSERT
(N_ALERT_PRIORITY_SEQ,V_ALERT_PRIORITY_CODE,N_ALERT_PRIORITY_MIN_SCORE,N
```

```
_ALERT_PRIORITY_MAX_SCORE,V_ALERT_TYPE_CODE,V_JRSDCN_CD,V_BUS_DMN_LIST_T
X)
VALUES
(S.N_ALERT_PRIORITY_SEQ,S.V_ALERT_PRIORITY_CODE,S.N_ALERT_PRIORITY_MIN_S
CORE,S.N_ALERT_PRIORITY_MAX_SCORE,S.V_ALERT_TYPE_CODE,S.V_JRSDCN_CD,S.V_
BUS_DMN_LIST_TX)
/
```

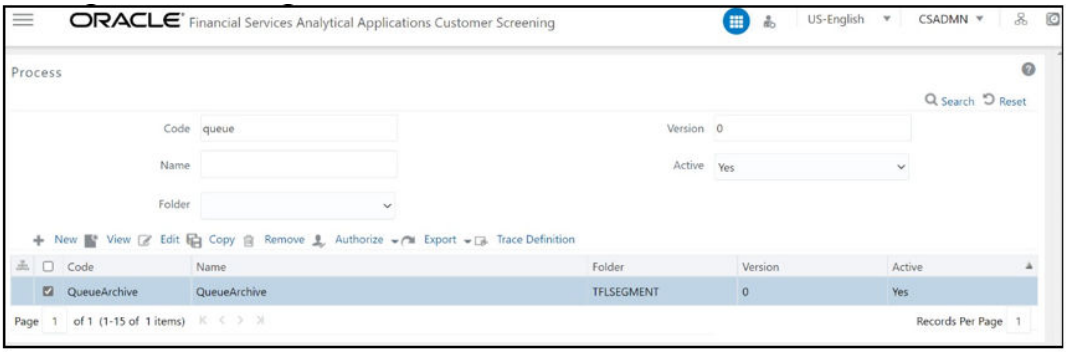
3.3.4 Archiving a Queue

To archive inactive queues, follow these steps:

1. Log on to the Customer Screening application.
2. Click **Common Tasks**, then click **Rule Run Framework**, and then click **Process**.

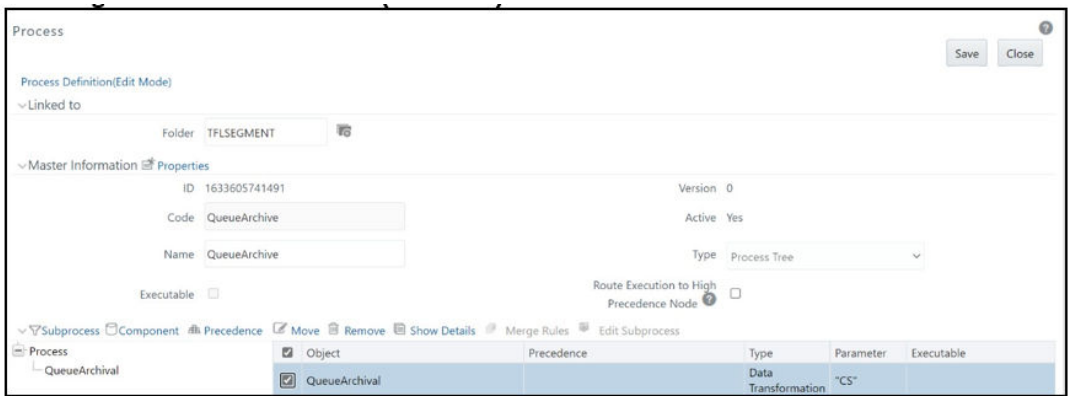
   The Process page is displayed.
3. Search for **Queue** in the **Code** field and select `Queue Archive`.

Figure 3-8 Process Page



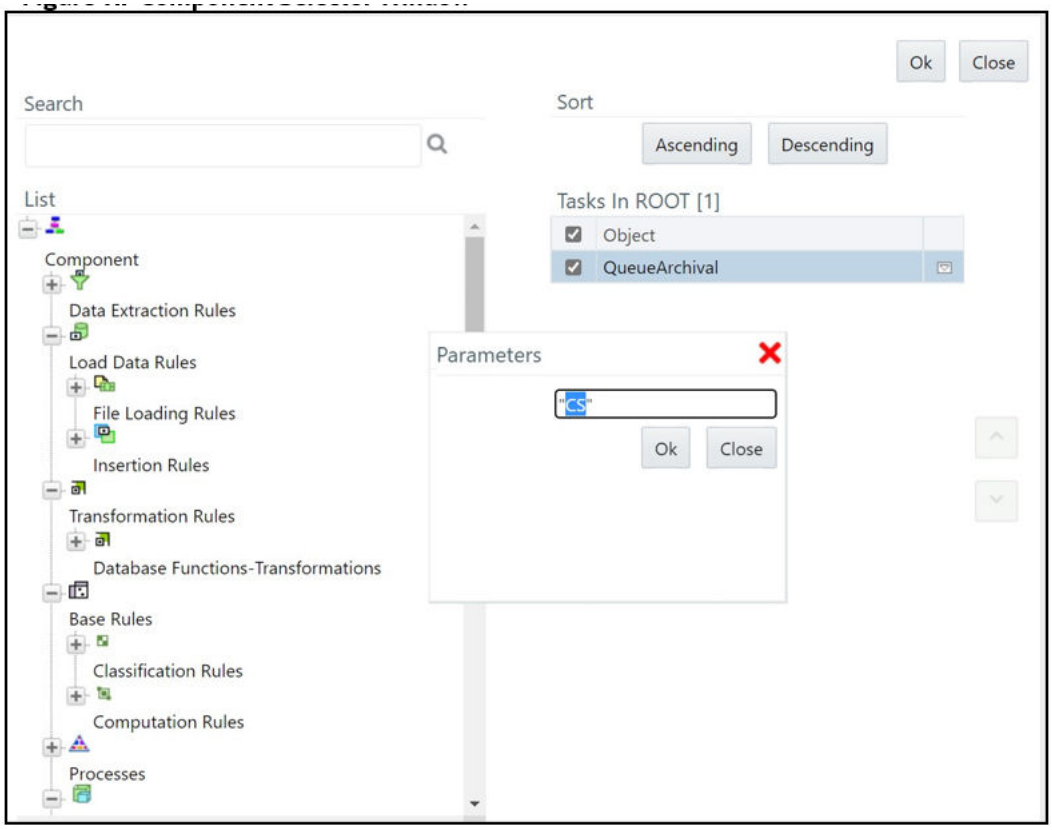
4. 4. Click **Edit**. The **Process** page opens in **Edit** mode.

Figure 3-9 Process Definition (Edit Mode)



5. Select the `QueueArchival` object and then select **Component**.
6. In the **Parameters** window, select the `QueueArchival` task and then click **drop-down list**. By default the parameter value will be selected as "`TF`". Change the parameter to "`CS`".

Figure 3-10 Component Selector window



7. Click **OK** to close the **Parameters** window.
8. Click **OK**.
9. Click **Save**.

   A confirmation message appears, click **Yes** to save the definition as a new version. A successful message appears, click **Close**.

3.4 Troubleshooting Your Display

If you experience problems logging into Oracle Financial Services Customer Screening or with your display, the browser settings may be incompatible with running OFSAA Applications. The following sections provide instructions to set your Web display options for OFSAA Applications.

3.4.1 Enabling JavaScript

This section describes how to enable JavaScript using the **Scripting** setting. To do this, follow these steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**.

   The **Internet Options** dialog box is displayed.
3. Click the **Security** tab and then click **Local Intranet**.
4. Click **Custom Level**.

   The **Security Settings** dialog box is displayed.

5. In the **Settings** list and under the **Scripting** setting, enable all options.
6. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

3.4.2 Enabling Cookies

Cookies must be enabled. If you have problems troubleshooting your display, contact your System Administrator.

3.4.3 Enabling Temporary Internet Files

Temporary Internet files are pages that you view on the Internet and store in a folder for quick viewing later. You must adjust this setting to always check for new versions of a stored page.

To enable Temporary Internet Files, follow these steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**.

   The **Internet Options** dialog box is displayed.
3. In the **General** tab, click **Settings**.

   The **Settings** dialog box is displayed.
4. Select **Every visit to the page**. Selecting this option ensures that the temporary files are cleared every time.
5. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

3.4.4 Enabling File Downloads

This section describes how to enable file downloads with the following steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**.

   The **Internet Options** dialog box is displayed.
3. Click the **Security** tab and then click **Local Intranet**.
4. Click **Custom Level**.

   The **Security Settings** dialog box is displayed.
5. In the **Downloads** section, ensure that the **Enable** check box is selected for all options.
6. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

3.4.5 Setting Printing Options

This section explains how to enable printing background colors and images with the following steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**.

   The **Internet Options** dialog box is displayed.
3. In **Settings**, click the **Advanced** tab.
4. In the **Printing** tab, click **Print background colors and images**.

5. Click **OK** to exit the **Internet Options** dialog box.

> **Note**
>
> For best display results, use the default font settings in your browser.

3.4.6 Enabling the Pop-Up Blocker

You may have trouble running the Customer Screening Application when the IE Pop-up Blocker is enabled. It is recommended to add the URL of the application to the list of allowed sites in the Pop-up Blocker Settings in the IE Internet Options.

To enable the Pop-up Blocker, follow these steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**.

   The **Internet Options** dialog box is displayed.
3. Click the **Privacy** tab.

   In the **Pop-up Blocker** setting, select **Turn on Pop-up Blocker**.
4. Click **Settings** to open the **Pop-up Blocker Settings** dialog box.
5. In the **Pop-up Blocker Settings** dialog box, enter the URL of the application in the text area.
6. Click **Add**. The URL appears in the **Allowed Sites** list.
7. Click **Close**, then click **Apply** to save the settings.
8. Click **OK** to exit the **Internet Options** dialog box.

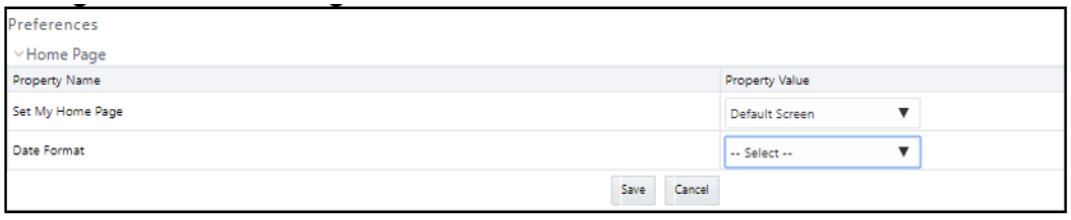
3.4.7 Setting Preferences

Use the **Preferences** section to set the **Financial Services Analytical Applications Customer Screening** Home page.

To access this section, follow these steps:

1. In the **Financial Services Analytical Applications Customer Screening** Home page, select **Preferences** from the user name drop-down list to open the **Preferences** page.

Figure 3-11 Preferences page



2. In the **Set My Home page** drop-down list, select the window that you want to view when you log in.

   When a new application is installed, the related window for that application is found in the drop- down list.

3. In the **Date Format** drop-down list, select the date format that you want to see. The options available are `dd/mm/yyyy` or `mm/dd/yyyy`.
4. Click **Save** to save your preferences.

4

General Configurations

Some configurations must be done before screening customer or external entity data, such as configuring run profiles to control elements of the watch lists and how screening is performed, preparing private watch lists using the Private List Interface (PLI) and use them for screening, analyzing watch list data, configuring match rules and clusters, configuring real-time and batch screening, configuring risk scores in watch lists and scheduling the Customer Screening run job. You can also configure the delta watch lists for the Dow Jones watch list, enable the General Data Protection Regulation (GDPR), and enable or disable the Data Quality (DQ) check.

The Watch List Management, Customer Screening, External Entity, and Real-time screening property files can be configured using run profiles in the `FICDB/conf` directory. You can use run profiles to specify the configuration settings that will override the default settings. The following run profiles are available in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory when you log in to the WinSCP server:

- `watch list-management.properties`
- `customer-screening.properties`
- `external-entity-screening.properties`
- `customer-screening-real-time.properties`

The watch `list-management.properties` run profile controls the following attributes:

- Which watch lists are downloaded
- How filtering is applied to the watch lists
- How to apply the Data Quality check to the watch lists

The `customer-screening.properties` and `external-entity-screening.properties` run profiles control the screening of customers and external entities respectively in batches.

The `customer-screening-real-time.properties` run profile controls the screening of customers in real-time.

4.1 Due Date and Time Configuration

Users with the Customer Screening Administrator role can use the Due Date and Time Configuration section to set the alerts' due date and time. The alerts will be prioritized based on these configuration values.

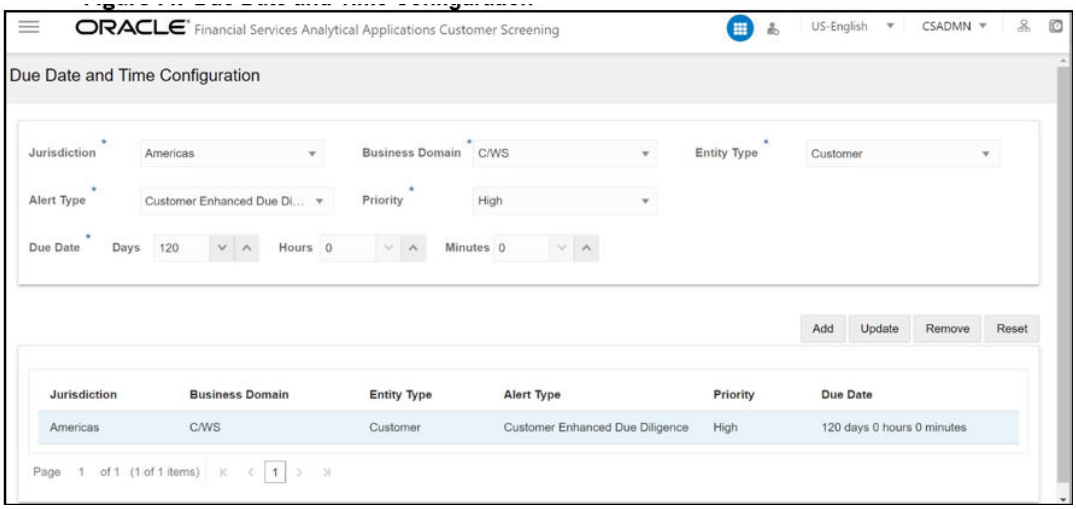
> **Note**
>
> The Due Date and Time Configuration is applicable only for Alert Management in the L1 investigation.

To access **Due Date and Time Configuration** section, follow these steps:

1. Click the **hamburger** icon to view the Application Navigation List.

2. From the **Application Navigation List**, select **Due Date and Time Configuration**. The **Due Date and Time Configuration** page appears.

Figure 4-1 Due Date and Time Configuration



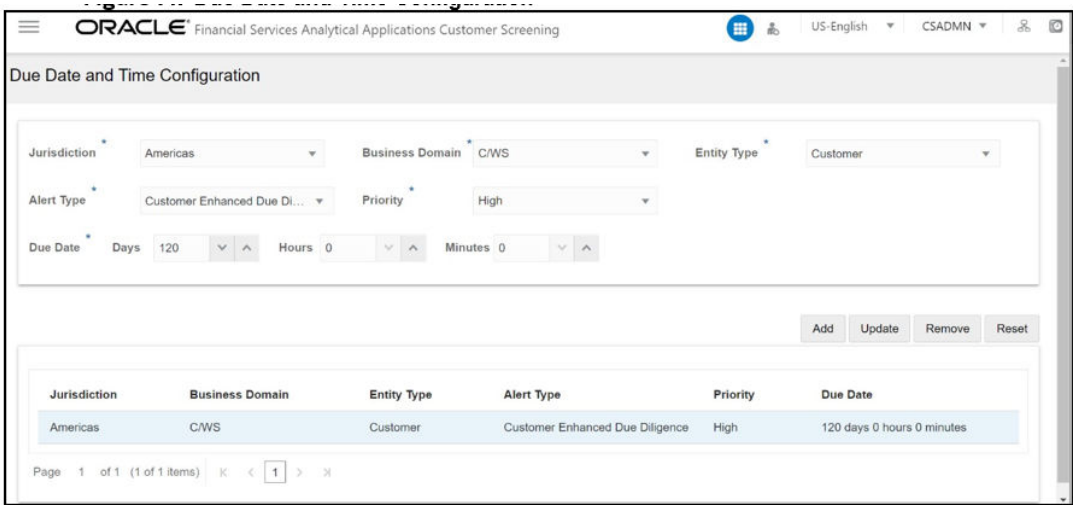
3. Provide details in the following mandatory fields in the following table:

Table 4-1 Conventions Used

Fields	Description
Jurisdiction	Select the jurisdiction value from the drop-down list.
Business Domain	Select the business domain to which the individual or entity belongs to.
Entity Type	Select the Entity Type as Customer, External Entity or Real-Time from the drop- down list.
Alert Type	Select the Alert Type value from the drop-down list. The values appear based on the selected entity type.
Priority	Select the alert priority value from the drop-down list.
Due Date	Select the due date values for the alert.

4. Click **Add**. The Due Date Configuration is added to the list.
   - Click **Reset** if you want to clear all the fields and enter new values.

Figure 4-2 Due Date and Time Configuration

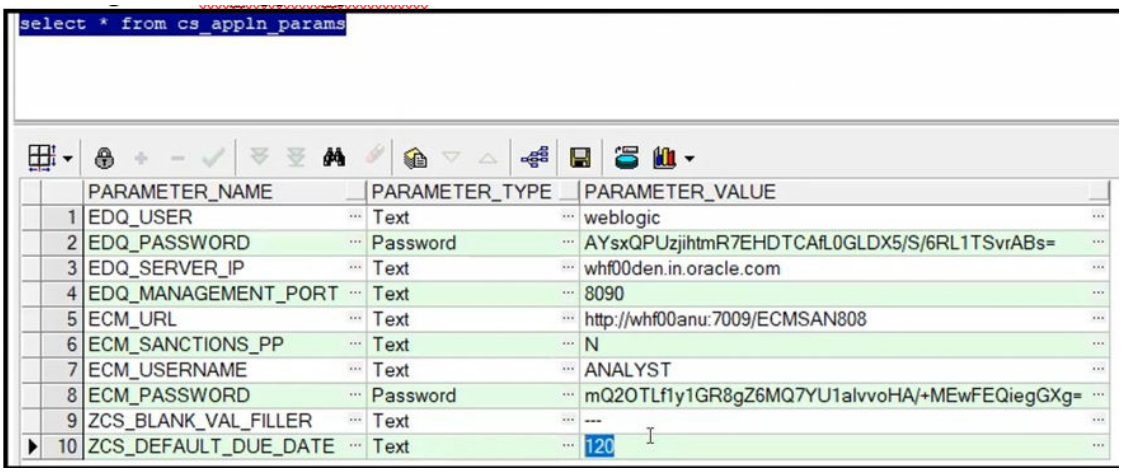


5. You can perform the following actions on the existing configurations:
   - **Update:** Select the configuration from the list, change any field values, and then click **Update**.
   - **Remove:** Select the configuration from the list and then click **Remove**.
   - **Reset:** Select the configuration from the list and then click **Reset** to reset the given field values.

> **Note**
>
> If the Due Date is not configured, the alerts will be prioritized based on the default configuration with Due Date as 120 days. You can reset the default Due Date with the `CS_appln_params` table.

6. To change the Default Due Date configuration, you have to access the Atomic Schema and access the `CS_appln_params` table and change the `ZCS_DEFUALT_DUE_DATE` parameter value.

Figure 4-3 CS_appln_params table



4.2 Setting the Priority

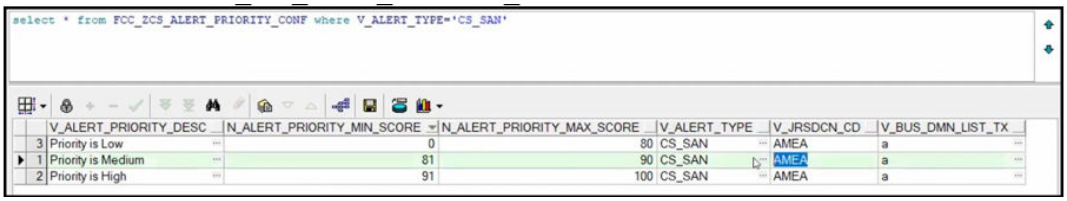
The Setting the Priority section describes how to set the alert priority as per your requirement. To set the priority of the alert, follow these steps:

1. Access the Atomic Schema and access the FCC_ZCS_ALERT_PRIORITY_CONF table.
2. Change the following parameter values:

> **Note**
>
> Setting the Priority is applicable only for Alert Management in the L1 investigation.

- n_alert_priority_min_score
- n_alert_priority_max_score
- v_jrsdcn_cd
- v_bus_dmn_list_tx

Figure 4-4 FCC_ZCS_ALERT_PRIORITY_CONF table



4.3 Security Mapping

The Security Mapping section describes how to change the security mapping. To change the security mapping, follow these steps.

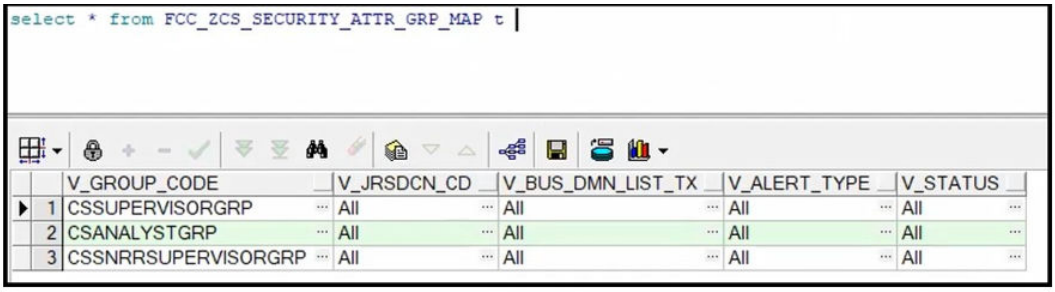
1. Access the Atomic Schema and access the `FCC_ZCS_SECURITY_ATTR_GRP_MAP` table.
2. Provide the values for the following columns:

> **Note**
>
> The Security Mapping is applicable only in the L1 Investigation for Alert Management.

- `V_GROUP_CODE`
- `V_JRSDCN_CD`
- `V_BUS_DMN_LIST_TX`
- `V_ALERT_TYPE`
- `V_STATUS`

The sample data is provided in the installer.

Figure 4-5 FCC_ZCS_SECURITY_ATTR_GRP_MAP table



	V_GROUP_CODE	V_JRSDCN_CD	V_BUS_DMN_LIST_TX	V_ALERT_TYPE	V_STATUS
1	CSSUPERVISORGRP	All	All	All	All
2	CSANALYSTGRP	All	All	All	All
3	CSSNRRSUPERVISORGRP	All	All	All	All

4.4 Preparing Watch List Data

Customer Screening is preconfigured to handle reference data from the following sources:

- HM Treasury
- OFAC
- EU Consolidated List
- UN Consolidated List
- World-Check
- Dow Jones Watch List
- Dow Jones Anti-Corruption List
- Accuity

You can also use your private watch list using the **Private List Interface (PLI)**. For more information, see The Private List Interface (PLI) chapter in the Oracle Financial Services Data Interfaces Guide.

Note

1. Watch lists can be downloaded automatically by setting the appropriate values in the run profile, or by downloading the watch list from the watch list provider's website. For information on downloading the watch lists, see Appendix C: Preconfigured Watch List Information.
2. The first time a watch list is downloaded, the staging value must be set to **Y**. This ensures that data in the staging tables is refreshed every time the watch list is downloaded.
3. The Accuity, Dow Jones, Dow Jones Anti-Corruption, and World-Check watch lists are provided as paid services. To use a watch list, you must register for an account on the watch list provider's website.

4.4.1 Preparing the Dow Jones Watchlist

This section explains how to configure Dow Jones watchlist and Dow Jones List Reference Mapper Feed to ingest Dow Jones watchlist data.

4.4.1.1 Dow Jones List Reference Mapper Feed Configuration

Use this section to configure Dow Jones List Reference Mapper Feed.

The Dow Jones List Reference Mapper Feed streamlines the integration of external watchlist data into Dow Jones' screening systems. It allows for flexible field mapping, ensuring accurate data translation from various sources. This feature automates the ingestion and updating of watchlists, supporting compliance with regulatory requirements.

To enable this feature, you must complete the following one-time setup procedure by applying patch 36921923.

4.4.1.2 Dow Jones List Watchlist Management Configuration

Use this section to configure Dow Jones List Watchlist Management.

You must configure both Dow Jones watchlist and Dow Jones List Reference Mapper Feed to ingest Dow Jones watchlist data.

The following Dow jones feeds are supported by product:

- Dow jones Trifecta feed- Sample URL : https://djrcfeed.dowjones.com/WL-SOC-AME/XML
- Dow jones Standard feed- Sample URL : https://djrcfeed.dowjones.com/XML/dailyfullfeed
- Dow Jones List Reference Mapper Feed Configuration:https://djrcfeed.dowjones.com/list-reference-mapper

4.4.1.3 Configuring Dow Jones Watchlist in EDQ

This example describes how to edit the watch list-management.properties run profile to allow you to download and configure the DJW list.

To automatically download the DJW list, set the following values in the watch list-management.properties run profile:

- phase.DJW\ -\ Download.enabled = Y (for downloading full list)
- phase.DJW\ -\ Download\ Delta.enabled = Y (for downloading delta list)
- phase.DJW\ -\ Stage\ reference\ lists.enabled = Y
- phase.DJW\ -\ Sanction_List_Reference.enabled = Y
- phase.DJW\ -\ Keywords_Preparation.enabled = Y

To manually download the DJW watch list using the Oracle Enterprise Data Quality (OEDQ) server,

1. Set `phase.DJW\ -\ Download.enabled = Y (for downloading full list) and phase.DJW\ -\ Download\ Delta.enabled = Y` (for downloading delta list).
2. Enter your user name and password in file `download-djw.sh/download-djw.bat` present in the location `{}/oedq.local.home/commandarea.`

   If the OEDQ server is connected to the internet through a proxy server, you must provide values for the following attributes in the proxy server:

   - proxy_host. For example, proxy.example.microsoft.com.
   - proxy_port. For example, 80.
   - proxy_username. For example, username.

- proxy_password. For example, password.

4.4.1.4 Filtering

Use this section for Filtering.

To prepare the DJW list without filtering, set the following value in the `watch list-management.properties` run profile:

phase.DJW\ -\ Prepare\ without\ filtering.enabled = Y

To prepare the DJW list with filtering, set the following values in the watch list-management.properties run profile:

phase.DJW\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = Y

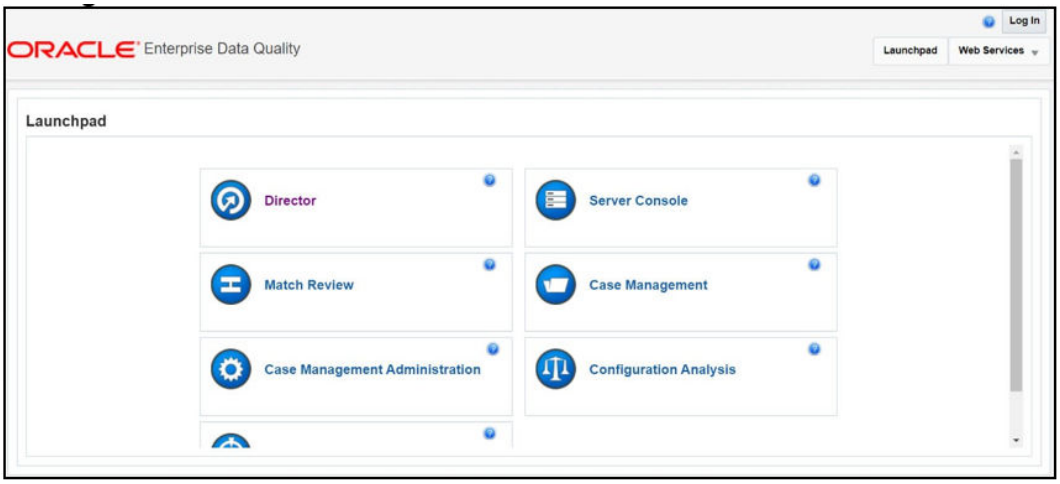
phase.DJW\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = Y

4.4.2 Preparing the Accuity Watchlist

The following steps explain how to edit the risk element scores for the Accuity watch list:

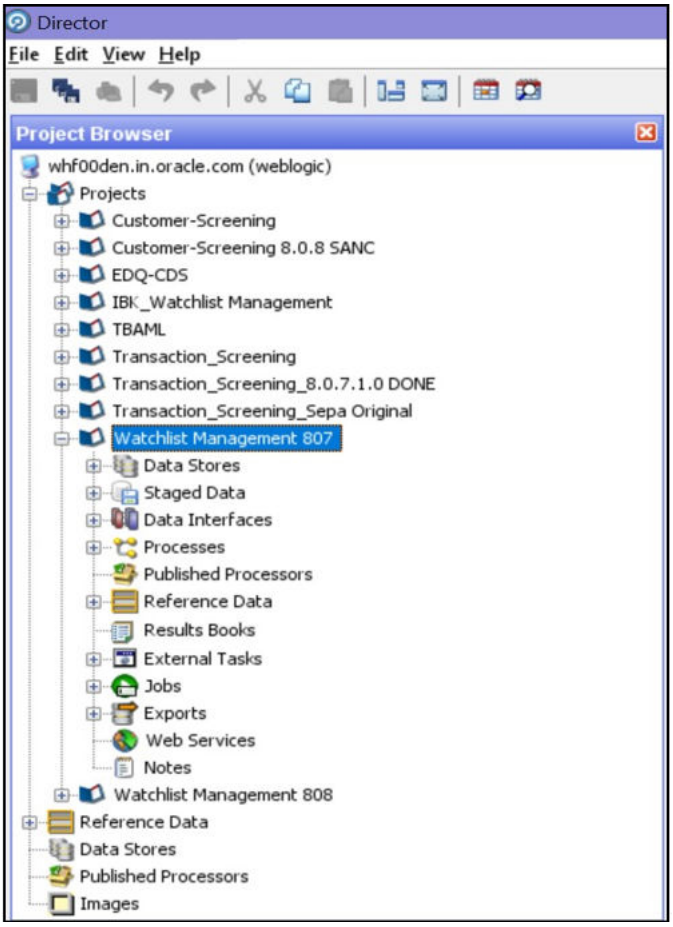
1. Go to the EDQ URL and open the **Director** menu. The **Director** Landing page is displayed.

Figure 4-6 Director Menu in EDQ

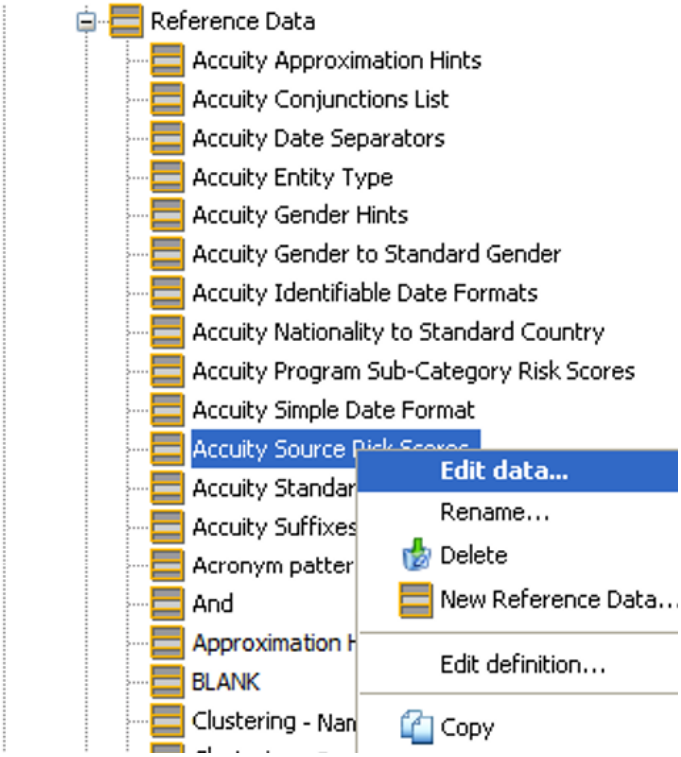


2. In the **Director** Landing page, expand the **Watch list Management** project in the **Project Browser** pane.

Figure 4-7 Project Browser pane

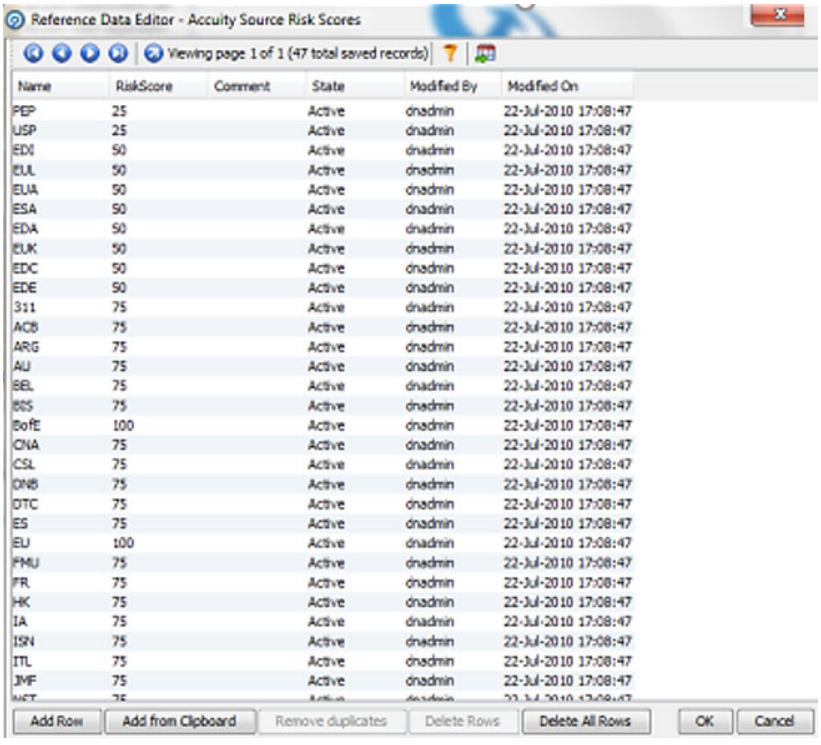


3. Expand the **Reference Data** node.
4. Right-click **Accuity Source Risk Scores** and select **Edit** data.



5. In the **Reference Data Editor – Accuity Source Risk Scores** window, the risk score appears in editable mode.

Figure 4-8 Reference Data Filters for Accuity



> **Note**
>
> If you edit the risk scores, you must rerun the `Download, Prepare, Filter and Export All Lists` jobs in the `Watch list Management` project and the `MAIN` job in the `Customer- Screening` project in EDQ. Until this is done, the generated matches will not show the new risk scores. For more information on how to view the jobs, see Analyzing the Data Quality of Customer Data and External Entity.

4.4.2.1 Configuring Accuity watchlist in EDQ

This example describes how to edit the `watch list-management.properties` run profile to allow you to download and configure the Accuity list.

To automatically download the Accuity list, set the following values in the `watch list-management.properties` run profile:

```
phase.ACY\ -\ Download.enabled = Y
```

```
phase.ACY\ -\ Stage\ reference\ lists.enabled = Y
```

To manually download the Accuity watch list using the Oracle Enterprise Data Quality (OEDQ) server, you must first set `phase.ACY\ -\ Download.enabled` and `phase.ACY\ -\ Stage\ reference\ lists.enabled = N` and click sftp://username:password@ftp.financialgo.net/PIDGWL.ZIP to connect to the WinSCP client. Enter your user name and password and download the watch list from the `config/landingarea/Accuity` directory.

If the OEDQ server is connected to the internet through a proxy server, you must provide values for the following attributes in the proxy server:

- proxy_host. For example, proxy.example.microsoft.com
- proxy_port. For example, 80
- proxy_username. For example, username
- proxy_password. For example, password

4.4.2.2 Filtering

To prepare the Accuity list without filtering, set the following value in the `watch list-management.properties` run profile:

```
phase.ACY\ -\ Prepare\ without\ filtering.enabled = Y
```

To prepare the Accuity list with filtering, set the following values in the `watch list-management.properties` run profile:

```
phase.ACY\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = Y
```

```
phase.ACY\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = Y
```

4.4.3 Private Watch List Set Up

Oracle Financial Services Customer Screening is preconfigured to work with commercially-available and government-provided watch lists. However, you can also screen data against your private watch lists. Sample private watch lists are provided in the `config/landingarea/Private` directory for individuals and entities in the `privateindividuals.csv` and `privateentities.csv` files, respectively.

> **Note**
>
> OEDQ release 12c has a base config folder and a local config folder. The base config folder is called `oedqhome` and the local config folder is called `oedqlocalhome`. The names can differ in some cases. For example, dots or underscores can be used in the names, such as `oedq_local_home`.

To screen data against a private watch list, you must first replace the data in the ready-to-use files with your data and then enable the private watch list properties in the `watch list-management.properties` run profile.

To replace the data, replace the data in the `privateindividuals.csv` and `privateentities.csv` files with your private watch list data.

> **Note**
>
> The files must be saved in UTF-8 format.

To enable the staging and preparation of the private watch list in the `watch list-management.properties` run profile, follow these steps:

1. Set `phase.PRIV\ -\ Stage\ reference\ lists.enabled = Y` to move your private watch list data to the staging tables.
2. Set `phase.PRIV\ -\ Prepare\ without\ filtering.enabled = Y` to prepare the private watch list without filtering.
3. Set `phase.PRIV\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = Y` and `phase.PRIV\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = Y` to prepare the private watch list with filtering.

4.5 Showing the Hidden Watch List Staged Data or Snapshots in the Server Console Interface

The following staged data and snapshots are hidden in the Server Console interface by default:

- Watch list snapshots
- Intermediate filtered watch list staged data
- Centralized Reference Data staged data or snapshots

To show this data, set the corresponding visibility property value in the run profile to Y.

For example, to view all Accuity watch list snapshots generated during Watch list Management, set the following properties in the `watch list-management.properties` run profile. The run profile is available in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory when you log in to the WinSCP server.

```
stageddata.ACY\Sources.visible = Y

stageddata.ACY_All.visible = Y

stageddata.ACY_Sources.visible = Y
```

4.6 Analyzing Watch List Data

Customer Screening has a process called Data Quality (DQ) that checks the quality of the downloaded watch list data which is later used for screening. This process can be run independently of the watch list screening process.

4.6.1 Analyzing Data Quality

Before you analyze your watch list data, follow these steps:

1. Ensure that your data is loaded into FCDM and the `watch list-screening` project has the correct database parameters.
2. Run the `CS_EDQ_Watch list_Analyze` job. The job checks your watch list data for any quality issues that affect have a negative impact on the screening process.

To analyze the data for watch lists, set the following properties in the `watch list-management.properties` run profile:

> **Note**
>
> The attributes shown are for the Accuity watch list. You must set the corresponding properties for the watch list for which you want to analyze data.

- `phase.DQ\ -\ Stage\ ACY\ reference\ lists.enabled = Y`
- `phase.DQ\ -\ ACY\ reference\ data\ quality\ analysis.enabled = Y`
- `stageddata.DQ\ ACY\ -\ Invalid\ Standard\ Country\ in\ Accuity\ Nation- ality\ to\ Standard\ Country.visible = Y`
- `stageddata.DQ\ ACY\ -\ Missing\ Source\ in\ Accuity\ Source\ Risk\ Scores\ Reference\ Data.visible = Y`
- `stageddata.DQ\ ACY\ -\ Obsolete\ Source\ in\ Accuity\ Source\ Risk\ Scores\ Reference\ Data.visible = Y`

4.7 Configuring Match Rules and Clusters for Customers and External Entities

You can configure match rules and clusters by adding a property value to the `customer-screening.properties` and `external-entity-screening.properties` run profiles.

For example, to disable the **Exact name only rule**, that is, `[I010O]`, for batch and real-time sanctions screening, add the following property value in the `customer-screening.properties` and `external-entity-screening.properties` run profiles:

```
phase.*.process.*.[I010O]\ Exact\ name\ only.san_rule_enabled = false
```

The * character denotes a wildcard, which indicates that the following rule applies to all phases and processes. If the `[I010O]` rule is disabled for batch screening only, the following is the new property value:

```
phase.Batch\ screening.process.*.[I010O]\ Exact\ name\ only.san_rule_enabled =
false
```

> **Note**
>
> The property value is case-sensitive.

For information on the match rules and clusters used in Customer Screening, see the Oracle Financial Services Customer Screening Matching Guide.

4.8 Real-Time and Batch Screening Set Up

By default, real-time and batch screening is enabled for SAN (sanctioned), PEP (Politically Exposed Persons), and EDD (Enhanced Due Diligence) records. This is controlled by the real-time and batch screening properties in the `customer-screening.properties`, `Customer-Screening-real- time.properties`, and `external-entity-screening.properties` run profiles. You can use these run profiles to enable or disable real-time or batch screening for all records or a specific record type.

For example, to run real-time screening for PEP and EDD individual and entity records, disable the following property values in the `customer-screening.properties` and `external-entity-screening.properties` run profiles:

```
phase.Start\ Batch\ Screening.enabled = N
```

```
phase.Real-time\ Screening.process.Individual\ Real-time\ Screening.san_enabled =
N
```

```
phase.Real-time\ Screening.process.Entity\ Real-time\ Screening.san_enabled = N
```

Ensure that all other real-time screening properties are set to **Y**.

To enable the Set Event Decision for the Case Analyst, map the `RT DECISION ACCESS` function to the Case Analyst role.

4.9 Extracting the Output of Matches into CSV Files

Customer Screening identifies possible relationships or matches between individuals and entities in your customer data and the external entities on watch lists. These matches form the basis of the cases that are investigated in Enterprise Case Management. When you perform batch screening and move these matches into the Customer Screening data layer, you can extract the output into the.csv files. This is useful if you want to use Customer Screening to identify the matches or if you want to review the matches using another case management system.

To extract the output of the matches into the `.csv` files, set the following values in the Batch Screening Setup section of the `customer-screening.properties` and `external-entity-screening.properties` run profiles. The run profiles are available in the `<domain_name>/edq/ oedq.local.home/runprofiles/` directory in the WinSCP server.

```
phase.*.process.*.output_relationships = Y
```

```
phase.Export\ Batch\ Relationships.enabled = Y
```

When you run Customer Screening with these run profile parameters enabled, two files are created:

- relns-ent-batch.csv. This file holds the match data for entities.
- relns-ind-batch.csv. This file holds the match data for individuals.

4.10 Filtering Watch List Data

The following sections provide information about how to enable watch list filtering, configure watch list filtering, how to use primary filters, secondary filters, linked records, and how to screen all watch list records.

4.10.1 Enabling Watch List Filtering

To enable filtering for a specific watch list, set the `Prepare with Filtering` phase in the appropriate run profile to **Y**, and the `Prepare Without Filtering` phase to **N**. For more information, see the example provided in Setting Filtering Options in the Run Profiles.

4.10.2 Configuring Watch List Filtering

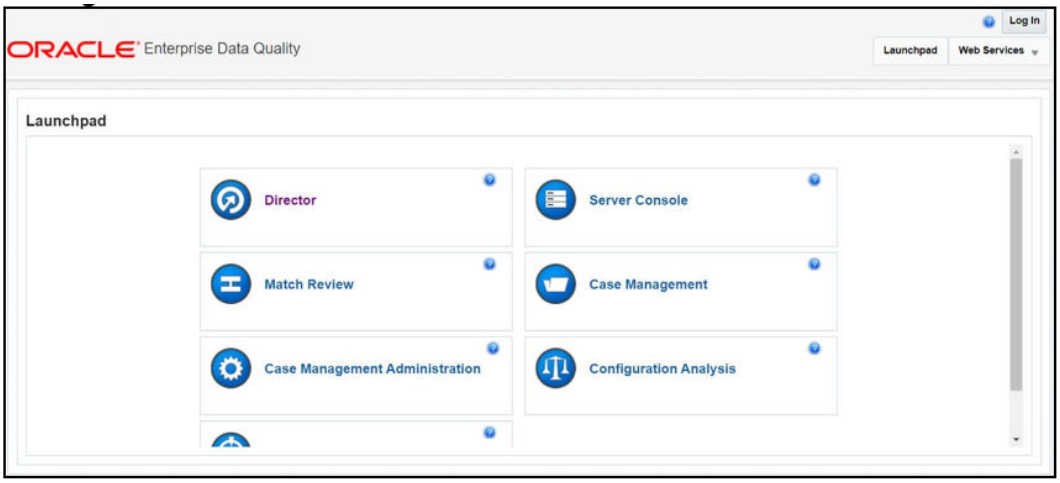
Watch List filtering is controlled by configuring reference data in the watch list projects.

> **Note**
>
> 1. The reference data sets in the Watch list Management and Customer-Screening projects are identical. This is to support installations that require filtering at different stages. For example, if a company wants to initially filter the prepared watch list data and then run several screening projects to filter specific parts of the data.
> 2. Once data is filtered out from the watch list, it is not possible to view the filtered data in another project. If, for example, all entities are filtered out in the Watch list Management project, then the Customer-Screening project will not display the entities in the screening results.

The first level of filtering is controlled by editing the following filters in the Watch list Management project:

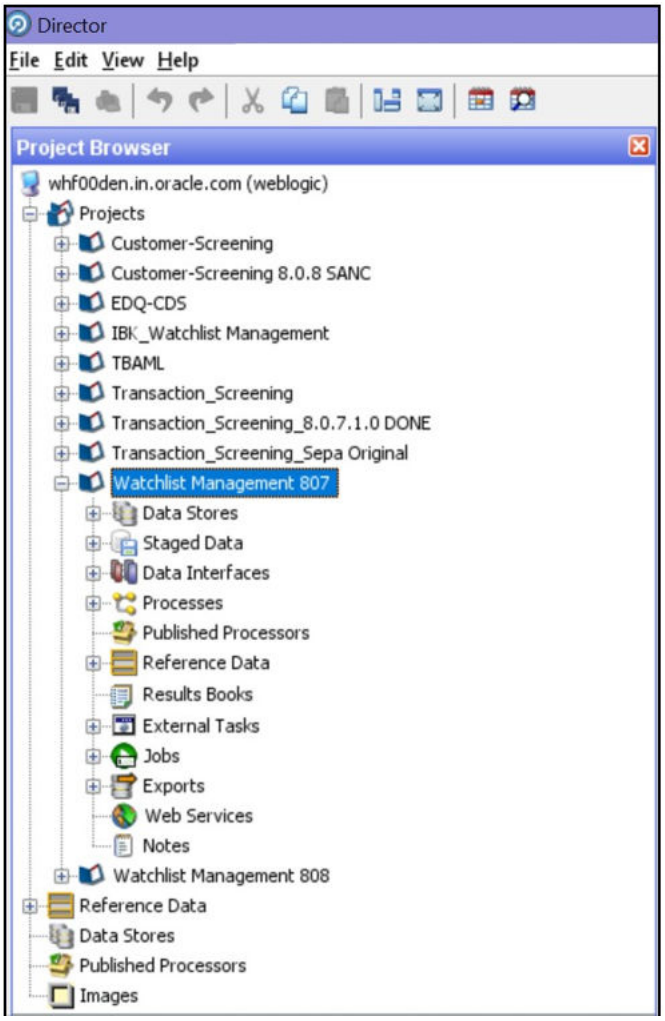
1. Go to the EDQ URL and open the **Director** menu. The **Director** Landing page appears.

Figure 4-9 Director Menu in EDQ



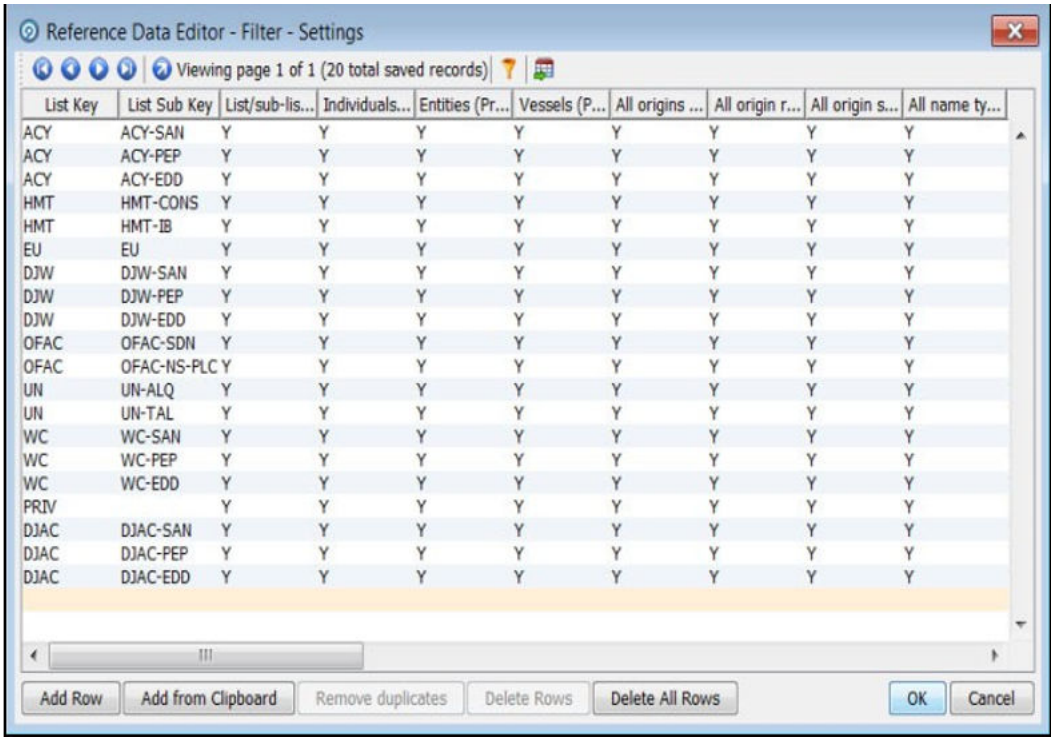
2. In the **Director** landing page, expand the **Watch list Management** project in the **Project Browser** pane.

Figure 4-10 Project Browser pane



3. Expand the **Reference Data** node and open **Filter-Settings**. The **Reference Data Editor – Filter-Settings** window appears.

Figure 4-11 Reference Data Editor–Filter-Settings window



All the reference data filters except the Linked Profiles filter is set to Y by default. Unless these settings are changed, no actual filtering is performed on the watch list data. In the filter settings, a value of Y indicates that all records are included, that is, no filters are applied.

Watch list filtering falls into four categories:

- By list and list subkey
- By list record origin characteristics
- By list profile record characteristics
- By linked profiles

For more information, see the example provided in Setting Primary Filters and Linked Profile Filters in the Watch list Management Project.

4.10.3 Primary Filters, Secondary Filters, and Filters for Linked Profiles

Primary filters are filters that are used to display all profiles that match the criteria specified. Filters for linked profiles are used to display profiles that are linked to the primary filter.

> **Note**
>
> You can filter linked profiles only for the World-Check and Dow Jones watch lists.

An example of a primary filter is a filter that is configured to capture all sanctions data. For the primary filter, a filter is configured for the related PEP data.

Secondary filters are applied to filter data that is displayed for linked profiles. For example, the secondary filter for PEP data is occupation or nationality.

Primary and secondary filters are set in one project (`Watch list Management/Customer-Screening`), and secondary filters are set in another project (`Watch list Management/Customer- Screening`).

4.10.4 Setting Multiple Values for Primary and Secondary Filters

Further configurations must display the following records:

- Origins
- Origin Regions
- Origin Statuses
- Primary and Secondary Name Qualities
- Primary and Secondary Name Types
- Primary and Secondary PEP Classifications

To filter data using one or more of these options, set the relevant value in the `Filter-Settings reference data` to **N**, and then make further changes to the corresponding reference data. When you set the value in the `Filter-Settings reference data` to **N**, only the records that match these values are included.

For example, if you set the value of the `All name qualities (Primary)?` filter to **N**, then you can determine which name qualities must be included for each watch list in the `Filter-Primary Name Qualities` reference data. Suppose you include a row for high-quality names in the EU watch list, but you do not include rows for medium-quality and low-quality names in this watch list, then only records with high-quality names are included in the watch list data.

> **Note**
>
> Some reference data sets are prepopulated with rows that usually contain data which is supplied by each watch list provider and can be viewed in the `Watch List Management` project. For example, to view all possible stop keywords for World-Check data, open the WC Keyword reference data in the Watch list Management project as mentioned in the following section.

4.10.4.1 Example:Filtering World-Check Data

This example describes the configurations which must be done to use primary and linked profile filters in the World-Check watch list in the `Watch list Management` project and how to set secondary filters in the `Customer-Screening` project.

The following tasks are described:

- How to enable filtering in the `watch list-management.properties` run profile. For more information on enabling filtering, see Setting Filtering Options in the Run Profiles.
- How to configure the primary filters and enable the filters for linked profiles in the `Watch list Management` project to return the active records for sanctioned individuals originating

from the EU list. For more information, see Setting Primary Filters and Linked Profile Filters in the Watch list Management Project.

- How to configure the secondary filters in the `Customer-Screening` project to filter out all the Linked Profiles of deceased individuals. For more information, see Setting Secondary Filters in the Customer Screening Project.

4.10.4.1.1 Setting Filtering Options in the Run Profiles

In the `watch list-management.properties` run profile, set the `World-Check` filtering phases as follows. This file is available in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory in the WinSCP server.

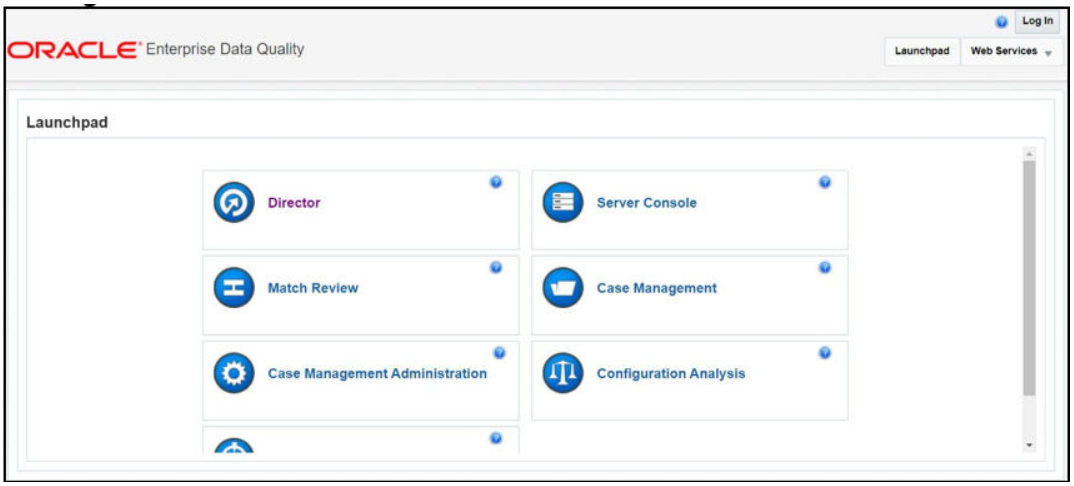
- `phase.WC\ -\ Prepare\ without\ filtering.enabled = N`
- `phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = Y`
- `phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = Y`
- `phase.WC\ -\ Load\ without\ filtering.enabled = N`
- `phase.WC\ -\ Load\ with\ filtering\ (Part\ 1).enabled = Y`
- `phase.WC\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y`

4.10.4.1.2 Setting Primary Filters and Linked Profile Filters in the Watch List Management Project

Follow these steps to set primary filters and linked profiles in the project:

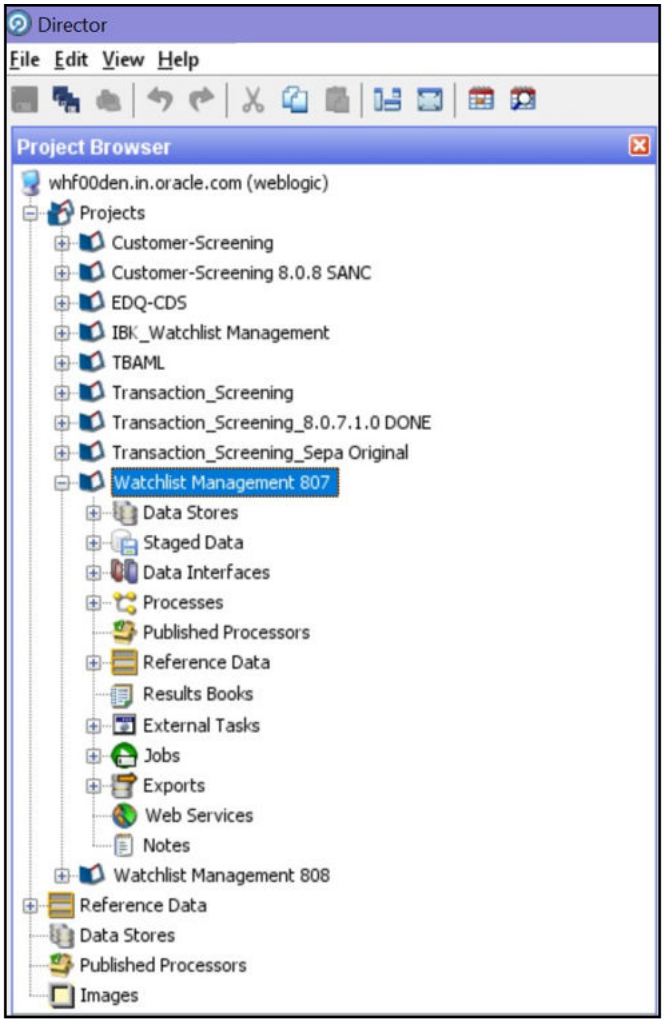
1. Go to the EDQ URL and open the **Director** menu. The **Director** Landing page appears.

Figure 4-12 Reference Data Filters



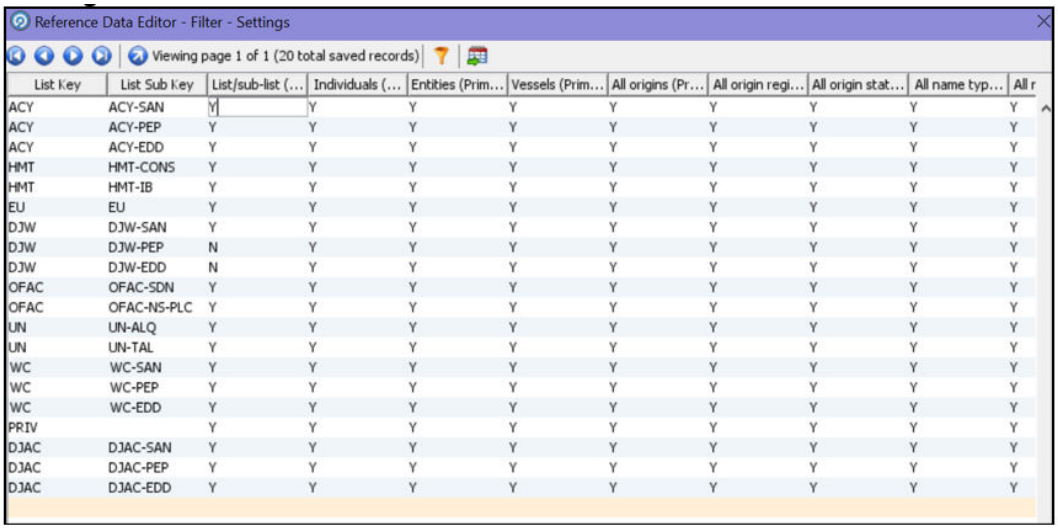
2. In the **Director** Landing page, expand the **Watch List Management** project in the Project Browser pane.

Figure 4-13 Reference Data Filters pane



3. Expand the **Reference Data** node and open **Filter-Settings**. The **Reference Data Editor – Filter-Settings** window appears.

Figure 4-14 Reference Data Filters



List Key	List Sub Key	List/sub-list (...	Individuals (...	Entities (Prim...	Vessels (Prim...	All origins (Pr...	All origin regi...	All origin stat...	All name typ...	All r
ACY	ACY-SAN	Y	Y	Y	Y	Y	Y	Y	Y	Y
ACY	ACY-PEP	Y	Y	Y	Y	Y	Y	Y	Y	Y
ACY	ACY-EDD	Y	Y	Y	Y	Y	Y	Y	Y	Y
HMT	HMT-CONS	Y	Y	Y	Y	Y	Y	Y	Y	Y
HMT	HMT-IB	Y	Y	Y	Y	Y	Y	Y	Y	Y
EU	EU	Y	Y	Y	Y	Y	Y	Y	Y	Y
DJW	DJW-SAN	Y	Y	Y	Y	Y	Y	Y	Y	Y
DJW	DJW-PEP	N	Y	Y	Y	Y	Y	Y	Y	Y
DJW	DJW-EDD	N	Y	Y	Y	Y	Y	Y	Y	Y
OFAC	OFAC-SDN	Y	Y	Y	Y	Y	Y	Y	Y	Y
OFAC	OFAC-NS-PLC	Y	Y	Y	Y	Y	Y	Y	Y	Y
UN	UN-ALQ	Y	Y	Y	Y	Y	Y	Y	Y	Y
UN	UN-TAL	Y	Y	Y	Y	Y	Y	Y	Y	Y
WC	WC-SAN	Y	Y	Y	Y	Y	Y	Y	Y	Y
WC	WC-PEP	Y	Y	Y	Y	Y	Y	Y	Y	Y
WC	WC-EDD	Y	Y	Y	Y	Y	Y	Y	Y	Y
PRIV		Y	Y	Y	Y	Y	Y	Y	Y	Y
DJAC	DJAC-SAN	Y	Y	Y	Y	Y	Y	Y	Y	Y
DJAC	DJAC-PEP	Y	Y	Y	Y	Y	Y	Y	Y	Y
DJAC	DJAC-EDD	Y	Y	Y	Y	Y	Y	Y	Y	Y

4. In the **Reference Data Editor – Filter-Settings** window, configure the following parameters. Double-click a value to update it.
   a. Set the List/sub-list (Primary?) Value in the WC-SAN row to **Y**.
   b. Set the Entities (Primary)? Value in the WC-SAN row to **N**.
   c. Set the Inactive (Primary)? Value in the WC-SAN row to **N**.
   d. Set the All Origins (Primary)? Value in the WC-SAN row to **N**.
   e. Set all other values in the WC-SAN row to **Y**.
   f. Add a new row with the following values:
      i. List Key-WC
      ii. List Sub Key-WC-SAN
      iii. Origin-EU
   g. Set the Linked Profiles? Value in the WC-SAN row to **Y**.
5. Click **OK** to close the window and save your changes.

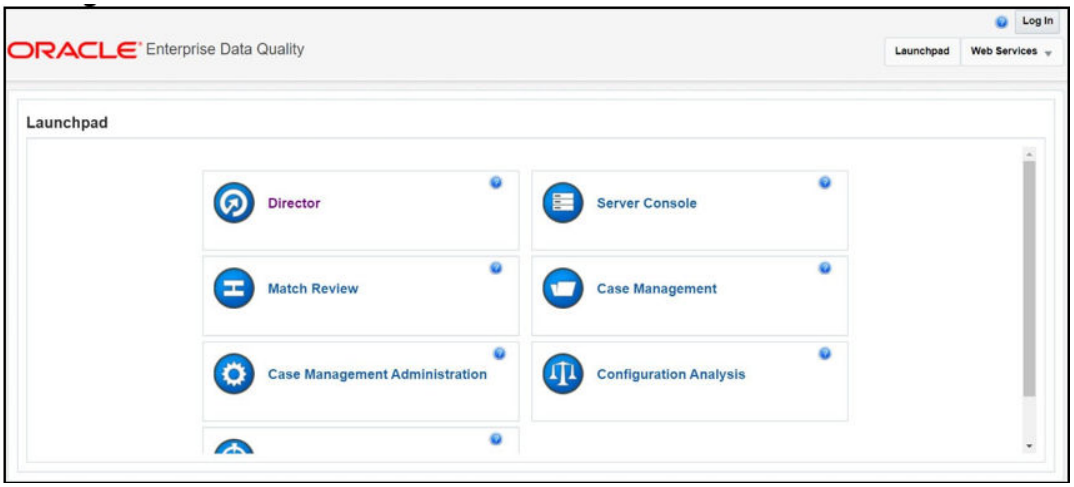
4.10.4.1.3 Setting Secondary Filters in the Customer Screening Project

Follow these steps to set secondary filters in the project:

1. Go to the EDQ URL and open the **Director** menu.

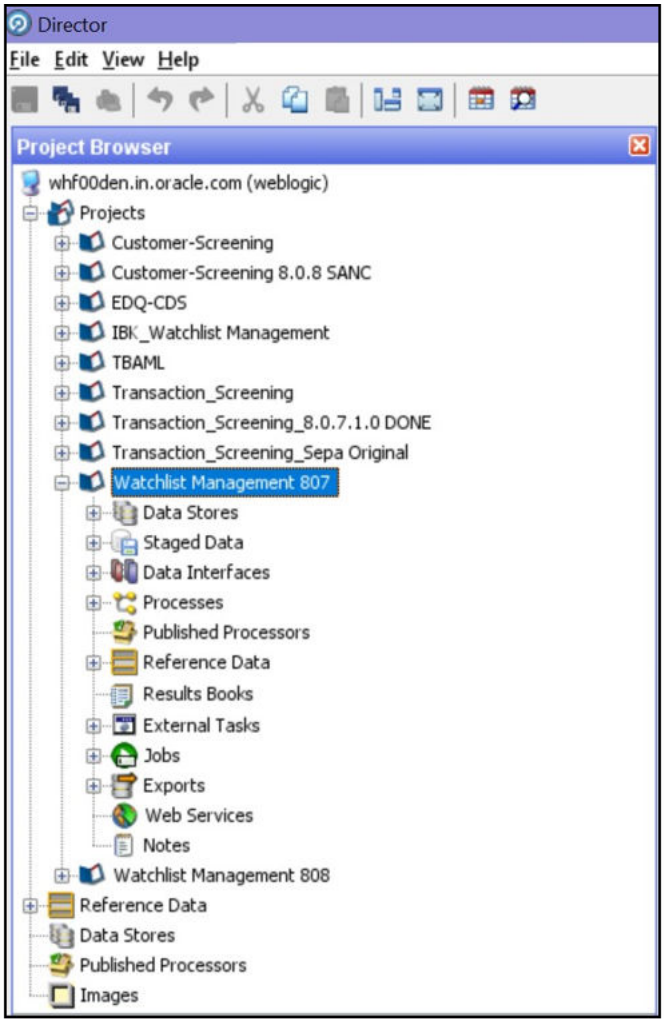
   The **Director** Landing page is displayed.

Figure 4-15 Reference Data Filters



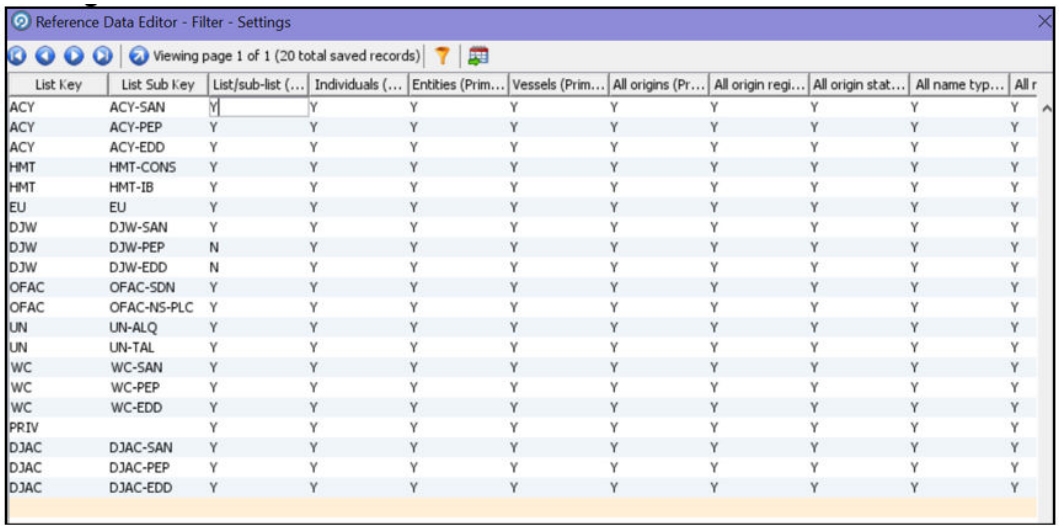
2. In the **Director** Landing page, expand the **Watch List Management** project in the **Project Browser** pane.

Figure 4-16 Reference Data Filters pane.



3. Expand the **Reference Data** node and open **Filter-Settings**. The **Reference Data Editor – Filter-Settings** window is displayed.

Figure 4-17 Reference Data Filters



4. In the **Reference Data Editor – Filter-Settings** window, Set the `Deceased (Secondary)?` value in the `WC-SAN` row to **N**.
5. Click **OK** to close the window and save your changes.

4.10.5 Screening All Sanctions Data

By default, data is routed from the `Watch List Management` project to the different screening processes depending on their record type, which can be Sanctions (SAN), Politically Exposed Persons (PEP), or Enhanced Due Diligence (EDD) records. This allows different rules to be applied according to the risk appetite of the record that is being screened.

However, if you want to use the same screening logic for all watch list records and do not want to maintain separate rulesets, you can move all watch list records to the SAN screening processes. To do this, set `phase.*.process.*.Screen\ all\ as\ SAN?` value in the `customer-screening.properties = Y`. This file is located in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory in the WinSCP server.

4.10.6 Match Persistence and Flag Keys

Customer Screening parses all customer records against all watch list records daily. This allows new alerts to be created due to changes in either the customer or the watch list data. When there is no change to the customer or the watch list record and the match is identical to a previously generated relationship, no new alerts are created.

Many attributes can change on a customer or watch list record but not all changes result in a new alert. These attributes are controlled based on the flag key value.

> **Note**
>
> If a new alias name that matches the customer record is added to a watch list, then this results in a new alert.

An example of a flag key is `date of birth`. Some potential matches are eliminated because the value the customer has provided and the value in the watch list records are different. So, if the value changes, then any potential matches related to the `date of birth` must be re-reviewed. An example of a field that is not included in the flag key is `account balance`. This value changes frequently and does not impact the match decision. Flag keys are set in individual match processes, and a hash value is generated which is used for comparison.

> **Note**
>
> The order of fields in the flag key is important. If the order changes, this will result in a new alert.

4.11 Risk Scoring in Watch Lists

Customer Screening includes a feature to estimate the relative risk of doing business with a given entity or individual. For each watch list, a risk score is calculated for an individual or entity based on various attributes such as country of residence, operating country, and associated regime. The risk scores for watch lists are available in the reference data tables for

the specific watch list. For more information, see Appendix B: Reference Data Tables for Watch Lists.

> **Note**
>
> The risk scores must be evaluated and tuned by a risk and compliance expert with knowledge of your business requirements and the relevant legislation.

4.11.1 Adjusting the Risk Scores

Customer Screening calculates a risk score and a Politically Exposed Person (PEP) risk score for every alert created during screening. The risk score is a relative measure of the risk posed by an individual or entity out of a maximum score of 100. The PEP risk score identifies the relative risk of the individual or entity when the individual or entity is considered as a PEP. Since the risk score can be different from the PEP risk score, the same algorithm is used to derive the risk score and PEP risk score but the underlying scores and weightings on which the calculations are based are different.

The overall risk score of a potential match is calculated as a weighted average of the risk scores generated for the watch list, customer, and external entity records in the match. The risk scores for the watch list, customer, and external entity records are calculated as a weighted average of the risk scores of the contributing risk elements. A risk element is a data field, such as Country of Operation or Occupation, and a risk score is assigned to the risk elements based on its value.

You can adjust the following attributes to customize the overall risk score:

- Risk scores and relative weightings of the risk elements.
- Relative weight of the watch list risk score, customer risk score, and external entity risk score.
- Reference data tables of the specific watch list used in the screening process.

4.11.2 Editing the Risk Element Scores

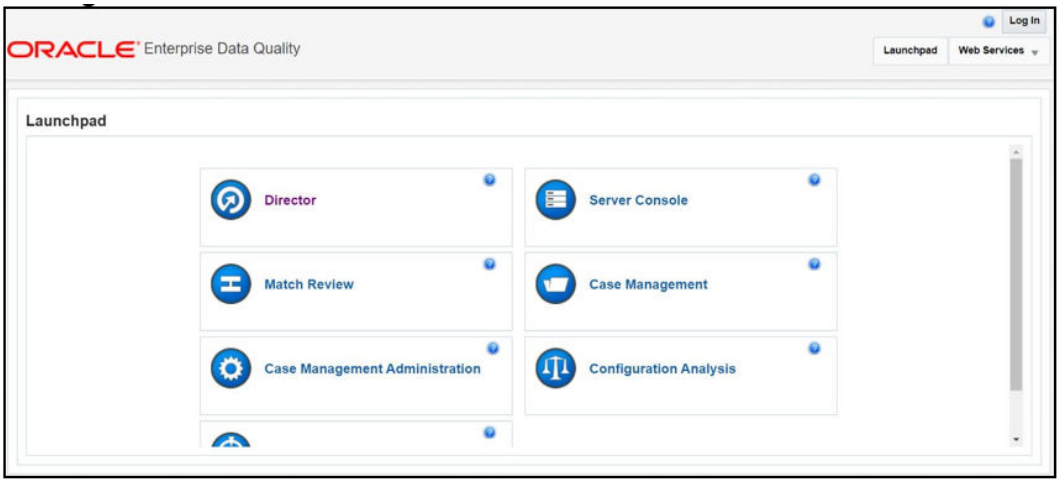
You can adjust the risk element scores by editing the risk element in Enterprise Data Management (EDQ). The risk elements that are considered during the risk score calculation depend on the fields that are present in the watch list or customer record.

4.11.2.1 Preparing the Accuity Watchlist

The following steps explain how to edit the risk element scores for the Accuity watch list:

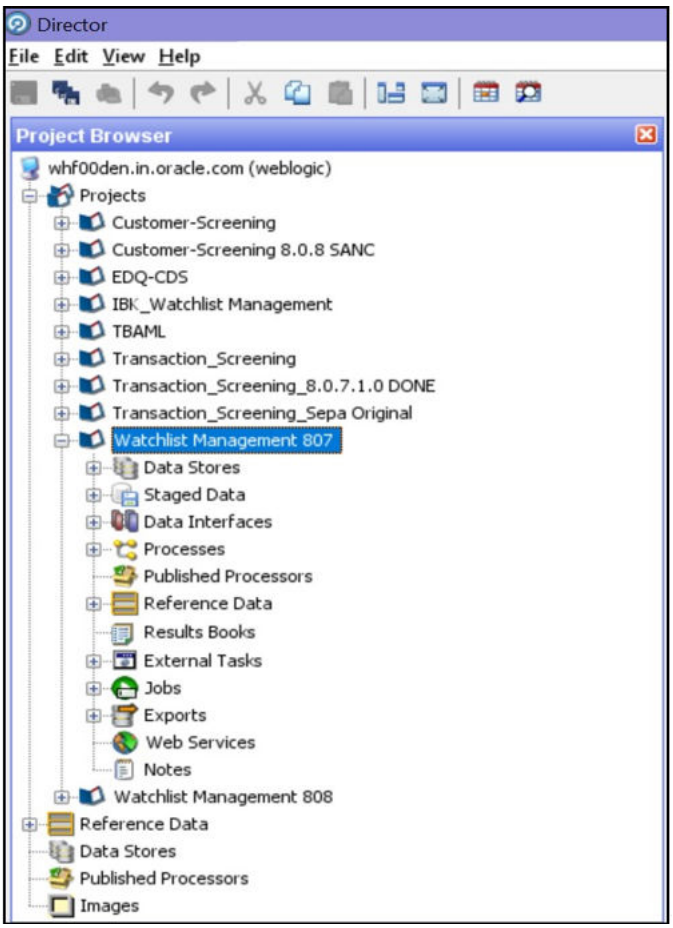
1. Go to the EDQ URL and open the **Director** menu. The **Director** Landing page is displayed.

Figure 4-18 Director Menu in EDQ

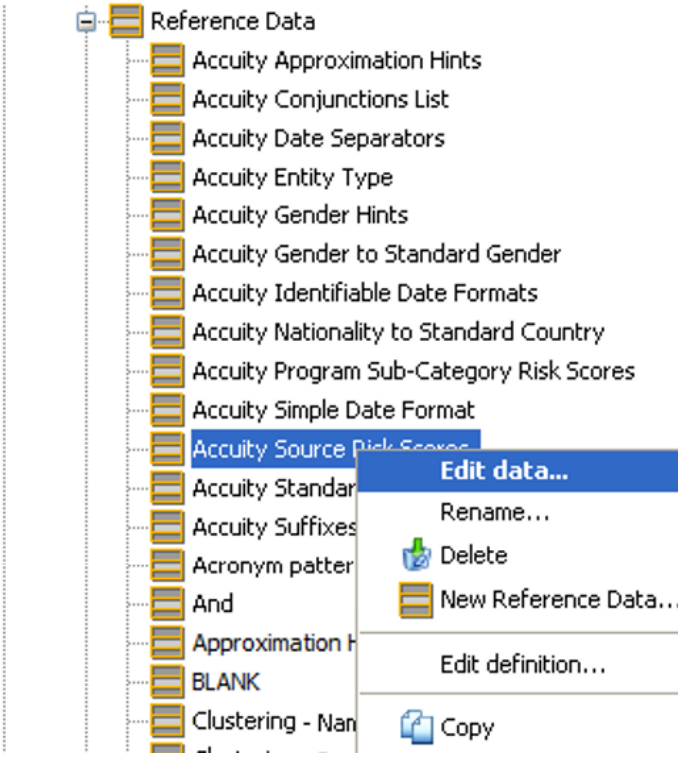


2. In the **Director** Landing page, expand the **Watch list Management** project in the **Project Browser** pane.

Figure 4-19 Project Browser pane

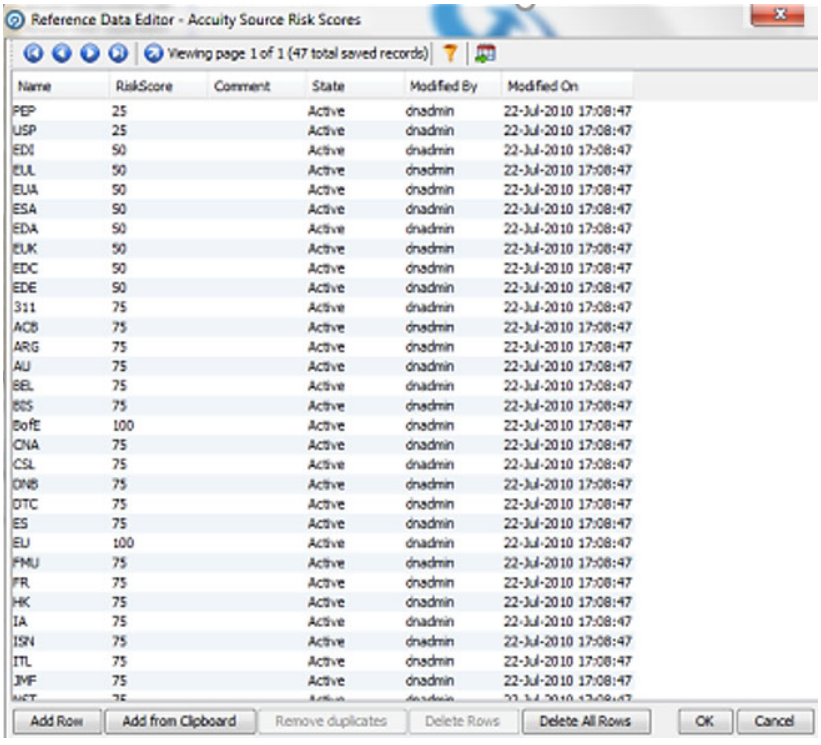


3. Expand the **Reference Data** node.
4. Right-click **Accuity Source Risk Scores** and select **Edit** data.



5. In the **Reference Data Editor – Accuity Source Risk Scores** window, the risk score appears in editable mode.

Figure 4-20 Reference Data Filters for Accuity



> **Note**
>
> If you edit the risk scores, you must rerun the `Download, Prepare, Filter and Export All Lists` jobs in the `Watch list Management` project and the `MAIN` job in the `Customer- Screening` project in EDQ. Until this is done, the generated matches will not show the new risk scores. For more information on how to view the jobs, see Analyzing the Data Quality of Customer Data and External Entity.

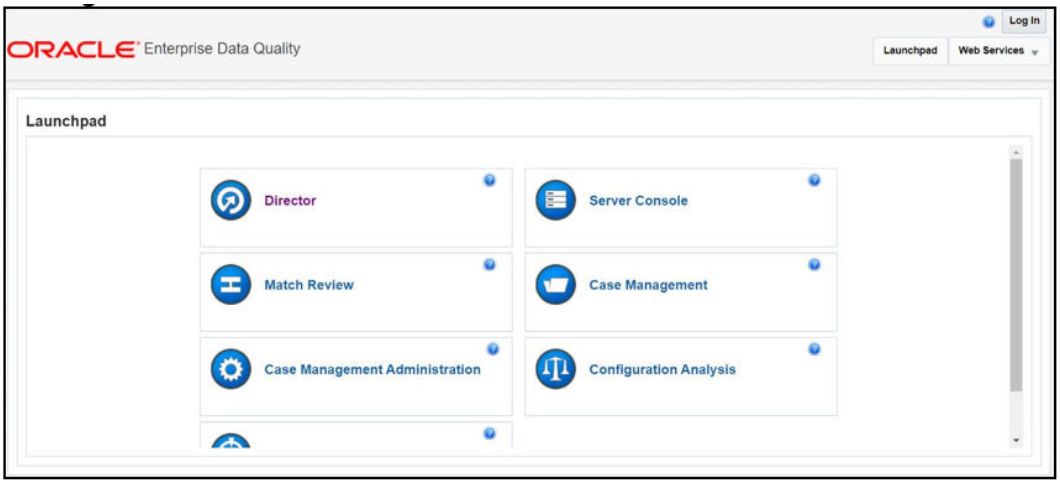
4.11.2.2 Editing the Risk Element Weightings

You can edit the default weightings assigned to each risk element in the **Reference Data Editor – Risk – Risk Element Weightings** window. This reference data set specifies which fields in that record contribute to the risk score calculation for each type of record and to what degree (weightage).

The following steps explain how to view the risk element weightings for all watch lists:

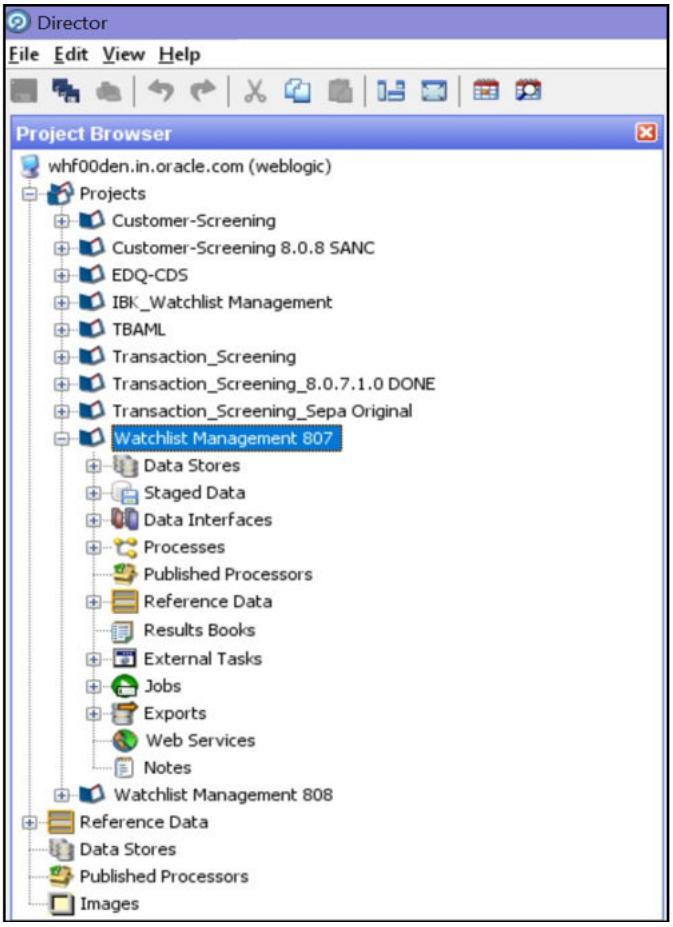
1. Go to the EDQ URL and open the **Director** menu. The **Director** Landing page is displayed.

Figure 4-21 Director Menu in EDQ



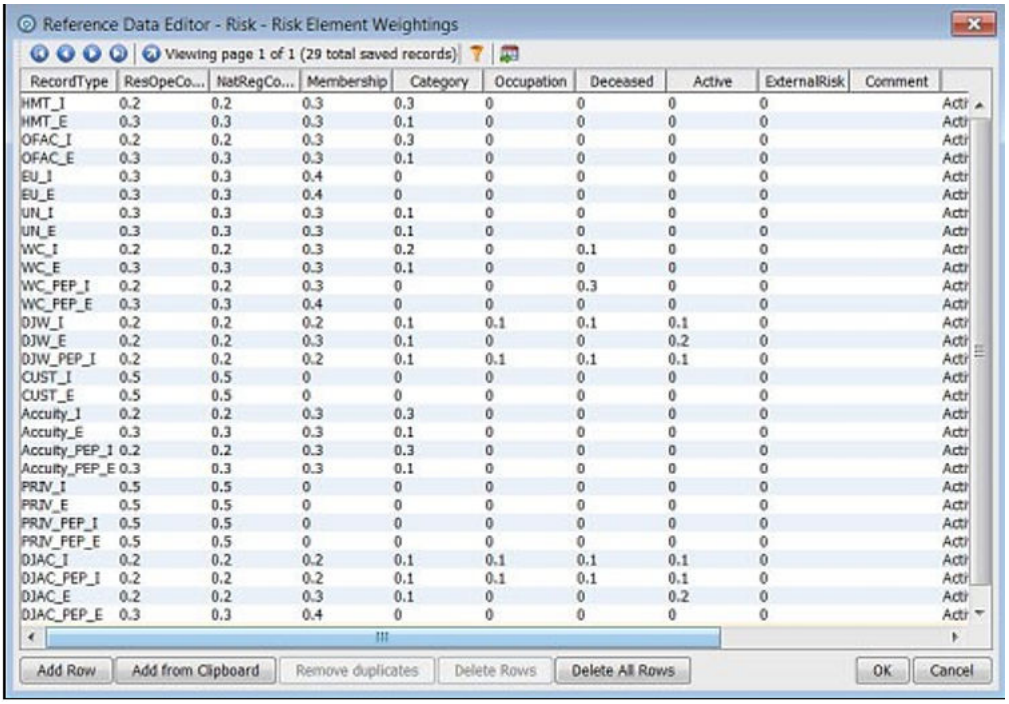
2. In the **Director** Landing page, expand the **Watch list Management** project in the **Project Browser** pane.

Figure 4-22 Project Browser pane



3. Expand the **Reference Data** node.
4. Right-click **Risk- Risk Element Weightings** and select **Edit** data.

Figure 4-23 Reference Data Filters for Risk Element Weightings



The format for the value in the **RecordType** column is the watch list and a suffix specifying whether the record represents an individual (`_I`) or an entity (`_E`). For example, `HMT_I`. Customer data have a record type of `CUST_I` for individual records and `CUST_E` for entity records.

The higher the weighting number, the more the corresponding risk element contributes to the overall risk score. The weighting scores for each row must add up to 1.

The overall risk score calculation for a record containing n elements is as follows:

Risk Score = E1w1 + E2w2 + …+ Enwn/W1+W2+ W3…..+Wn (which has valid E risk element)

E1, E2, E3, till En stand for scores for risk element.

For example, country code, residency code, nationality code, and so.

W1, W2, W3 till Wn stand for the element weightage from the above reference data. Where the risk element score for element x is represented by Ex and the weighting for element x is represented by wx.

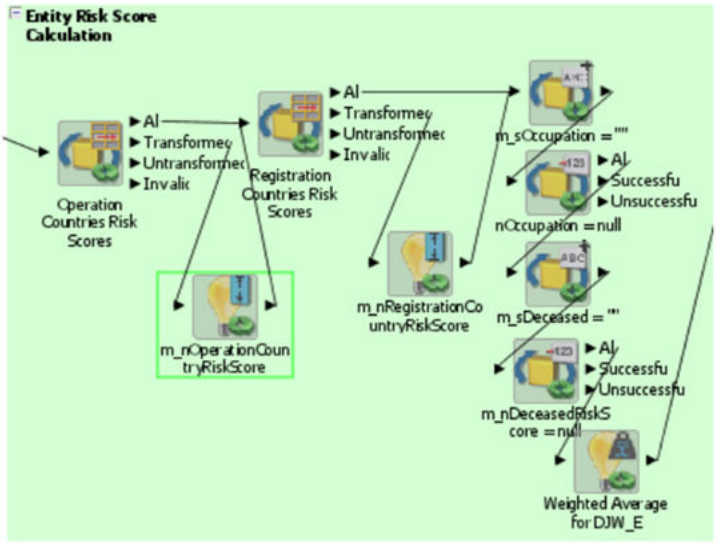
The total of all weightings must add up to 1, that is, (w1 + w2 + …+ wn = 1)

> **Note**
>
> If there is no data for a risk element, it must not be included in the risk score calculation.

The following parameters are considered for DJW and WC:

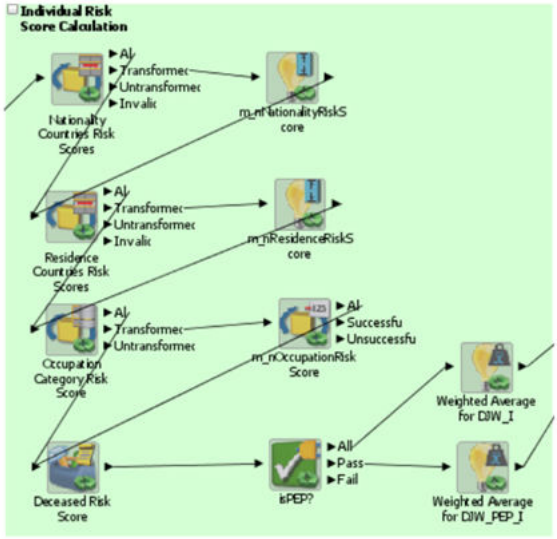
DJW ENT

Figure 4-24 DJW ENT



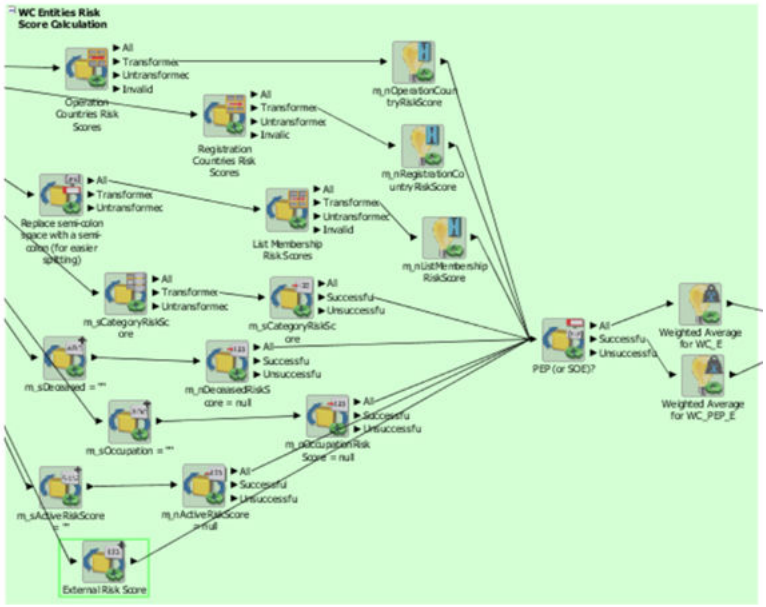
DJW IND

Figure 4-25 DJW IND



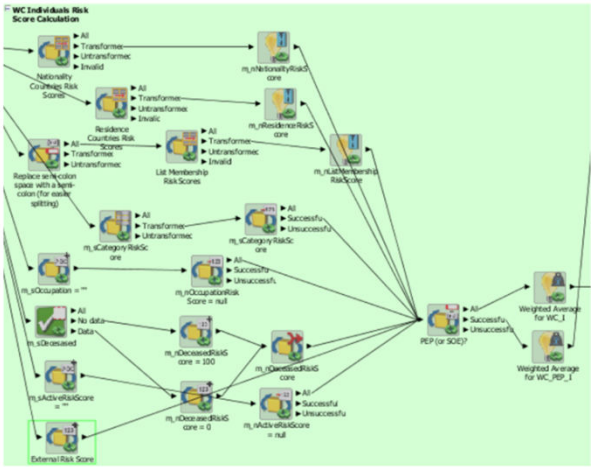
WC ENT

Figure 4-26 WC ENT



WC IND

Figure 4-27 WC IND



4.12 Scheduling the Customer Screening Run Job

To execute a Customer Screening Run job, follow these steps:

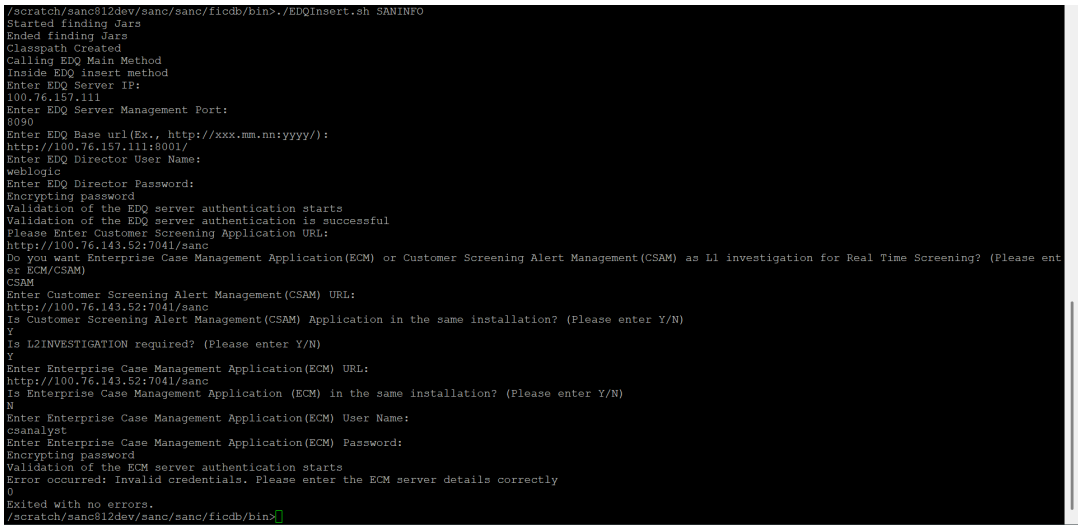
1. Navigate to the `FCI_DB_HOME/bin` directory.
2. Execute the command `/EDQInsert.sh <INFODOM NAME>`.

   This step is used to register the EDQ server details. You must replace the INFODOM NAME placeholder with your domain name.
3. Enter the following details in the console where the command is run:

- EDQ Server IP
- EDQ Server Management Port (JMX port number). This value must be 8090.
- Enter EDQ Base URL (for example - http://xxx.mm.nn:yyyy/)
- EDQ Server User Name
- EDQ Password details

> **Note**
>
> If any of the authentication details entered is incorrect, the system displays error message.

Figure 4-28 EDQ Details



4. Create and authorize a new ECM user who has no case privileges. For example, `CSConnect`. For information on how to create or add and authorize a user, see the *User Administrator* section in the Oracle Financial Services Analytical Applications Infrastructure User Guide.

> **Note**
>
> In the first login as a new user, you are prompted to change the password.

5. Execute the command `/EDQInsert.sh <INFODOM NAME>` again only if you are doing a pack-on-pack installation of Enterprise Case Management (ECM) on Sanctions and the ECM URL is unavailable. An entry is made in the ATOMIC schema in the `cs_appln_params` table.
6. Copy the following run profiles from the `<domain_name>/edq/oedq.local.home / runprofiles/` directory in the WinSCP server to the `FIC_DB_HOME/conf` directory:
   - `watch list-management.properties`
   - `customer-screening.properties`
   - `external-entity-screening.properties`

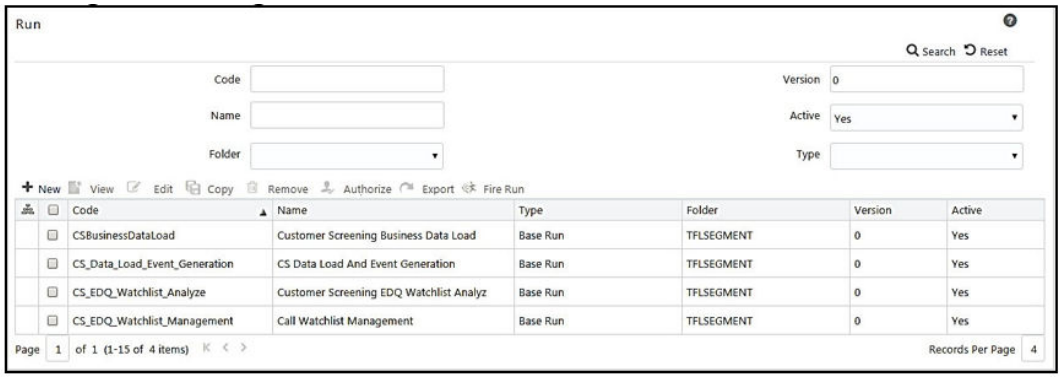
- `customer-screening-real-time.properties`

7. Load the stage table data for the customer-related tables. For more information, see Loading Data.
8. In the Run page, select the `CS_Data_Load_Event_Generation` run and click **Fire Run**. The batches must be run in the order mentioned in the following table. It is not mandatory to run all the batches.

Table 4-2 Sequence of Batches to be Run

Sequence	Batch Name	Description
1	CS_EDQ_Watchlist_Management	This job is used to run the watch list management project and start real-time screening in EDQ based on the run profile parameters. This job must be run daily.
2	CS_EDQ_Watch list_Analyze	This job is used to check the data quality of the downloaded watch list.
3	CSBusinessDataLoad	This job is used to load data from the staging tables to the business tables.
4	CS_Data_Load_Event_Generation	This job is used to match customer data with the downloaded watch list data and to generate alerts.
5	Oracle_CS_Zipper_Processing	This job will move the data from the source database to the consolidated database and create an alert based on the Customer. **NOTE:** The Oracle_CS_Zipper_Processing batch is only applicable in the L1 Investigation.

Figure 4-29 Run page



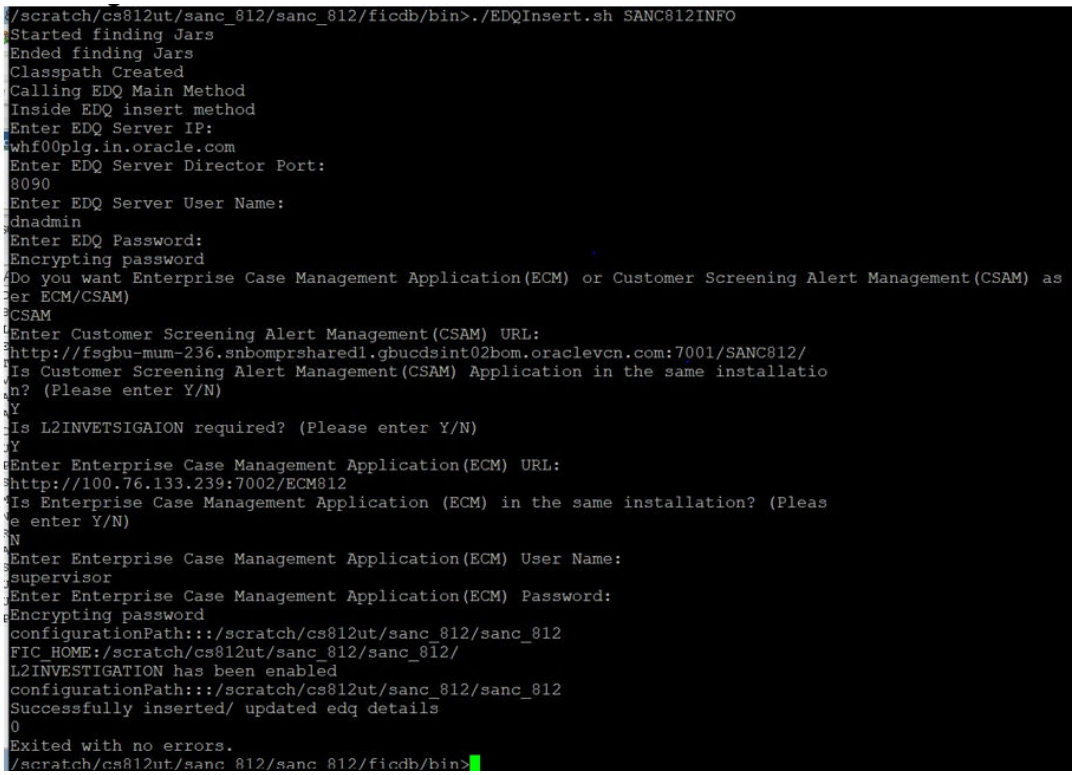
4.13 Enabling L2 Investigation and OAS for Customer Screening

To enable L2 Investigation for Customer Screening follow these steps:

1. Navigate to the `FCI_DB_HOME/bin` directory.
2. Execute the command `/EDQInsert.sh <INFODOM NAME>`.

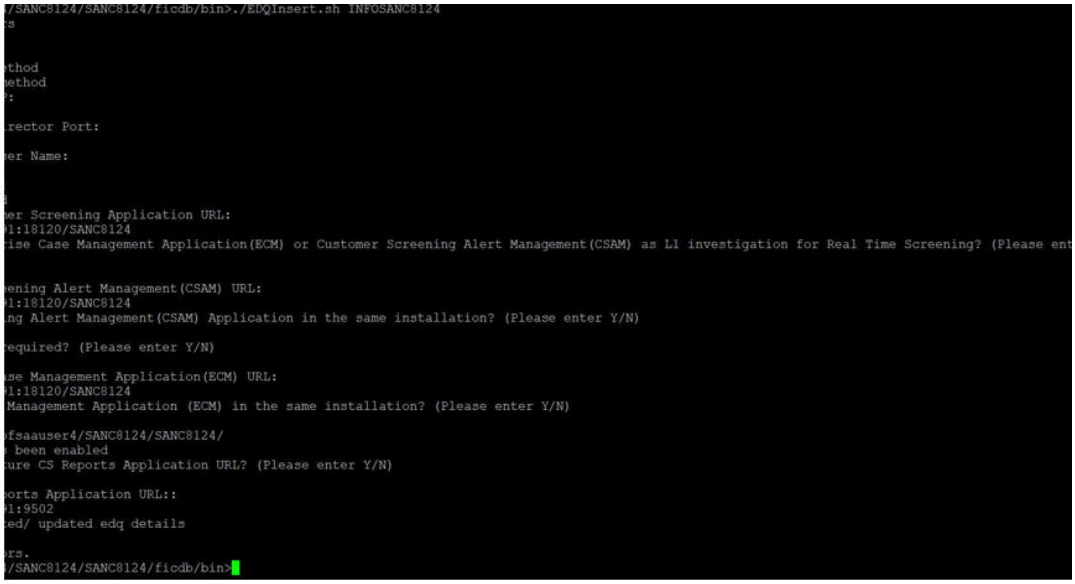
   This step is used to register the EDQ server details. You must replace the INFODOM NAME placeholder with your domain name.
3. Enter the following details in the console where the command is run:
   - EDQ Server IP
   - EDQ Server Direct Port number (JMX port number). This value must be 8090.
   - EDQ Server User Name
   - EDQ Password details

Figure 4-30 EDQ Details



4. Enter the input as CSAM for the L1 investigation and then press **Enter**.
5. Enter the Customer Screening URL and then press **Enter**.
6. Enter **Y** if the Customer Screening installed in the same installation or else **N** and then press **Enter**.
7. Enter **Y** to enable the L2 Investigation or else **N** and then press **Enter**.
8. Enter **Y** if Case Management is installed on the same installation of Customer Screening or else **N**.

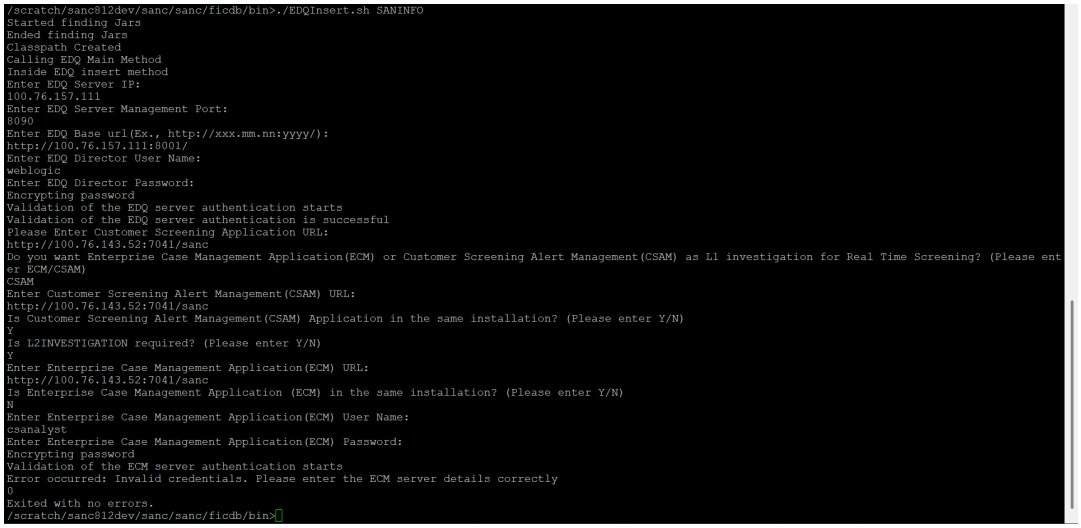
Figure 4-31 EDQ Details



9. If the input for the above step 8 is **N**, provide the User Name and Password of the Case Management.
10. Do you want to capture CS Reports Application URL? **(Enter Y/N) Y**
    - EDQ Server IP
    - EDQ Server Management Port (JMX port number). This value must be 8090.
    - Enter EDQ Base URL (for example - http://xxx.mm.nn:yyyy/)
    - EDQ Server User Name
    - EDQ Password details

> **Note**
>
> If any of the authentication details entered is incorrect, the system displays error message.

Figure 4-32 EDQ Details



11. Enter CS Reports Application URL: http://xxx.xx.166.91:9502

> **Note**
>
> The above URL is the Analytics URL.

4.14 Loading Data

This section explains how to load customer data from staging tables to the business table.

The following are the types of data loading:

- Loading Data into the Customer Tables (Full Load)
- Loading Data into the Customer Tables (Delta Load)

4.14.1 Loading Data into the Customer Tables (Full Load)

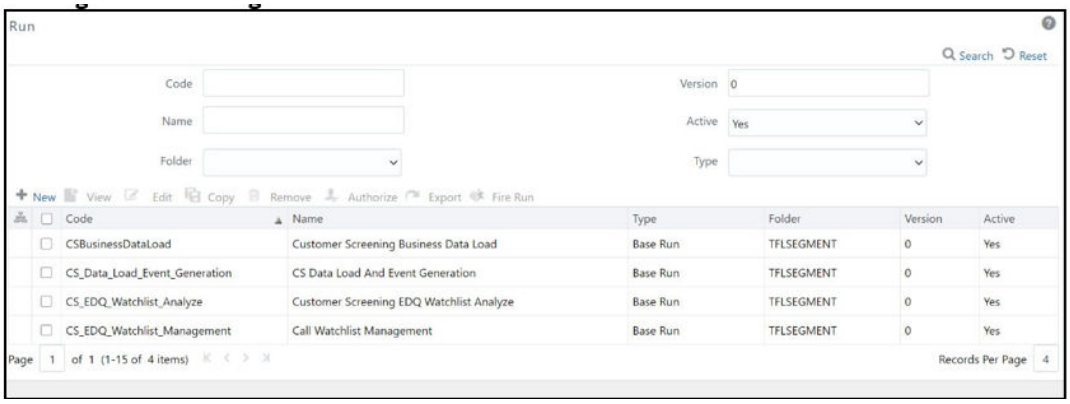
The full load allows you to move the complete list of data from the staging table to the business table.

To load data into the Customer tables, follow these steps:

1. Log on to the Customer Screening application.
2. Click **Common Tasks**, then click **Rule Run Framework**, and then click **Run**.

   The Run page appears.

Figure 4-33 Run page



3. In the Run page, select the `CSBusinessDataLoad` checkbox and click **Fire Run**. Select the Date and click **OK**.

4.14.2 Loading Data into the Customer Tables (Delta Load)

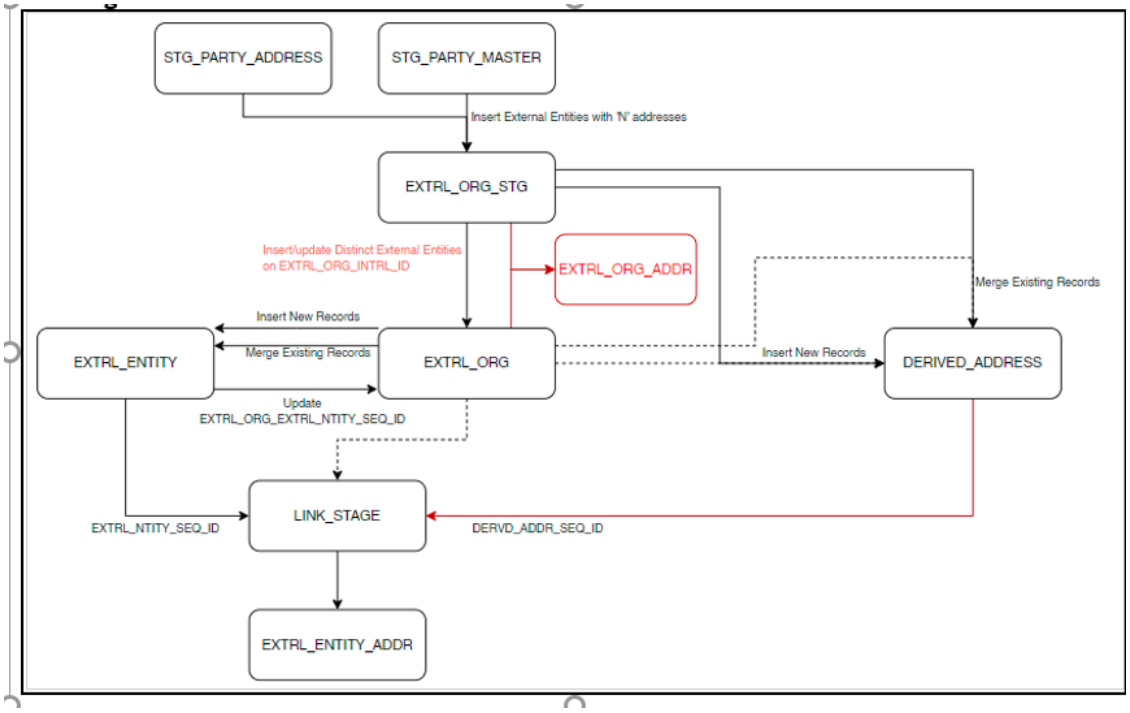
The delta load allows you to move only the changed or enhanced data from the staging table to the business table.

If any customer data is changed in stage data only those data is moved in business. Based upon the date you run the batch.

For example, if any new entry has come for the same customer ID on a different date. Only those customer details are pushed to the business table.

The following workflow explains the external entity data movement from stage tables to business tables.

Figure 4-34 Delta Load Workflow

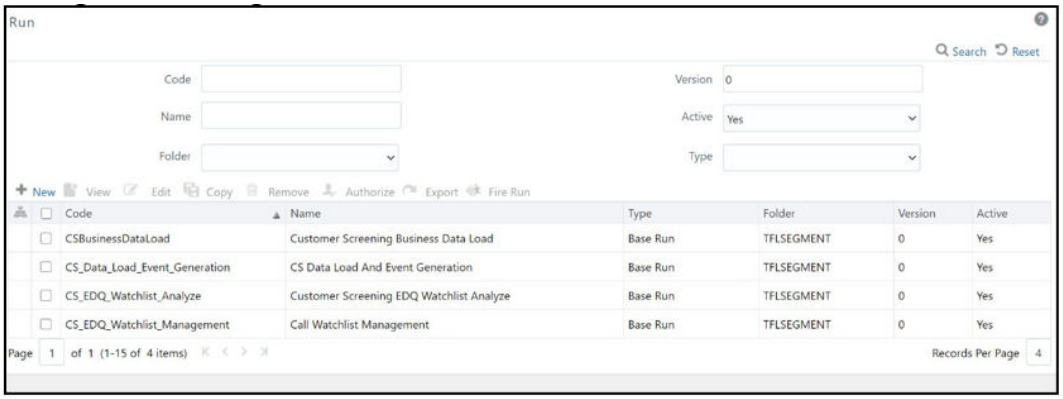


To load data into the Customer tables, follow these steps:

1. Log on to the Customer Screening application.
2. Click Common Tasks, then click Rule Run Framework, and then click Run.

   The Run page is displayed.

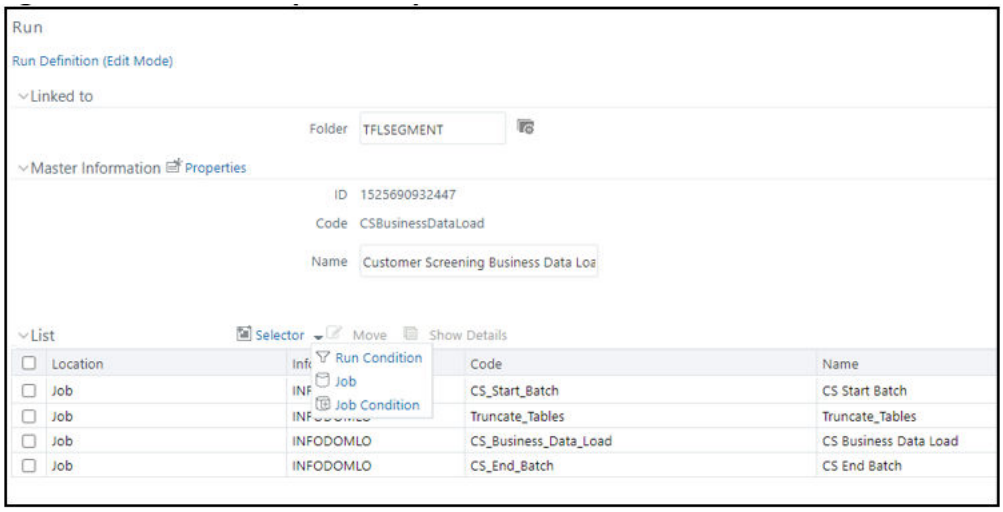
Figure 4-35 Run page



3. In the **Run** page, select the `CSBusinessDataLoad` checkbox and click **Edit**.

   The **Run** page is displayed in edit mode.

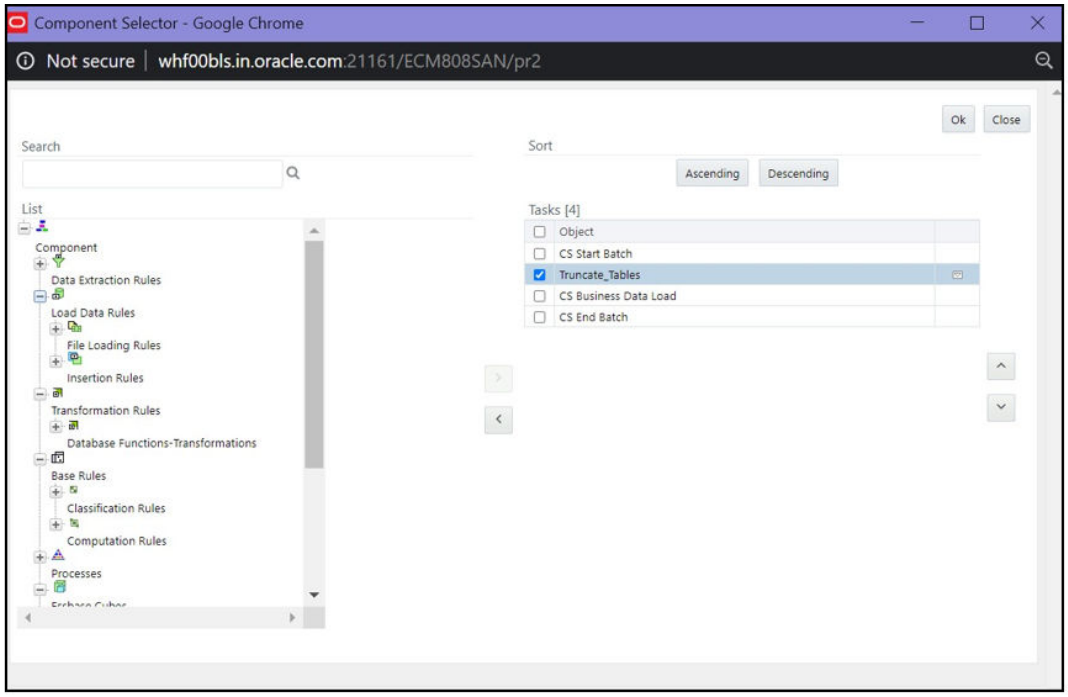
Figure 4-36 Run Definition page (Edit mode)



4. Click **Selector** and then select **Job**.

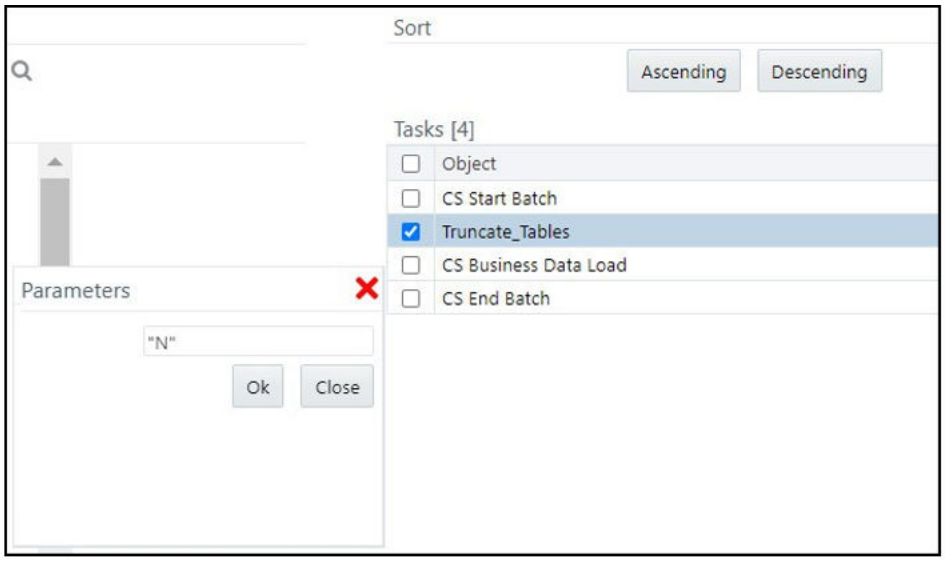
   The **Component Selector** window is displayed.
5. Select the `Truncate_Tables` task and then click **drop-down list**.

Figure 4-37 Component Selector Window



6. Change the parameter value to **N** and click **OK** to close the **Parameters** window.

Figure 4-38 Parameters window



> **Note**
>
> By default it is **"Y"**, if delta mode to be supported, update from **"Y"** to **"D"**.

7. Click **OK** to close the **Component Selector** window.

8. Click **Next**.
9. Click **Save**.

4.14.3 Creating and Running Parallel Batches

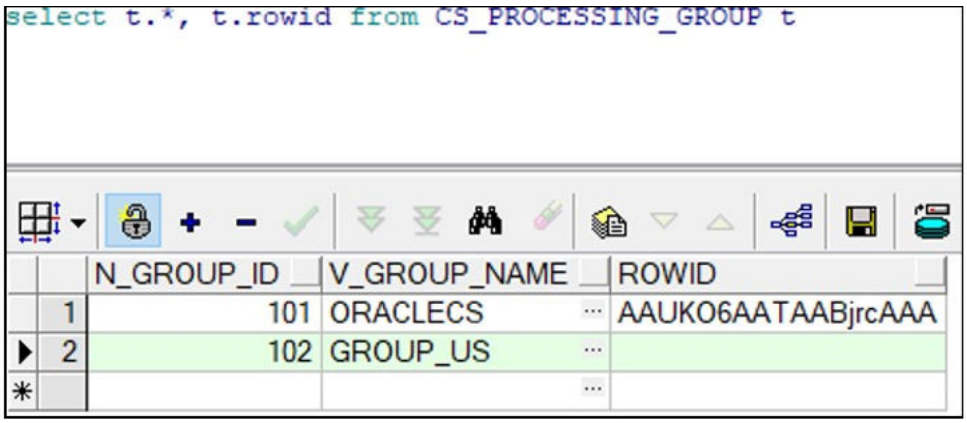
Parallel batches can be run in CS if you want to run batches with different jurisdictions at the same time. To run parallel batches, run the `CS_Data_Load_Event_Generation` task for each jurisdiction.

4.14.3.1 Creating a Process

To create a process, follow these steps:

1. Make an entry in the `cs_processing_group` table in the `N_GROUP_ID` and `V_GROUP_NAME` columns. For example, `102` and `GROUP_US`.

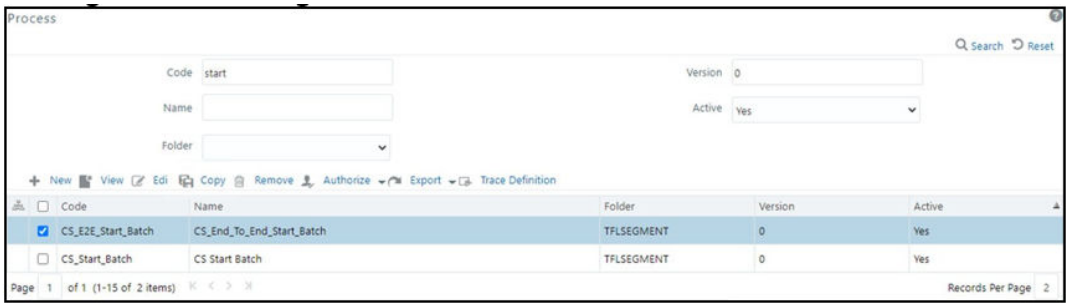
Figure 4-39 Developer window



2. Log on to the Customer Screening application.
3. Click **Common Tasks**, then click **Rule Run Framework**, and then click **Process**.

   The **Process** page is displayed.
4. Search for Start in the Code field and select CS_E2E_Start_Batch.

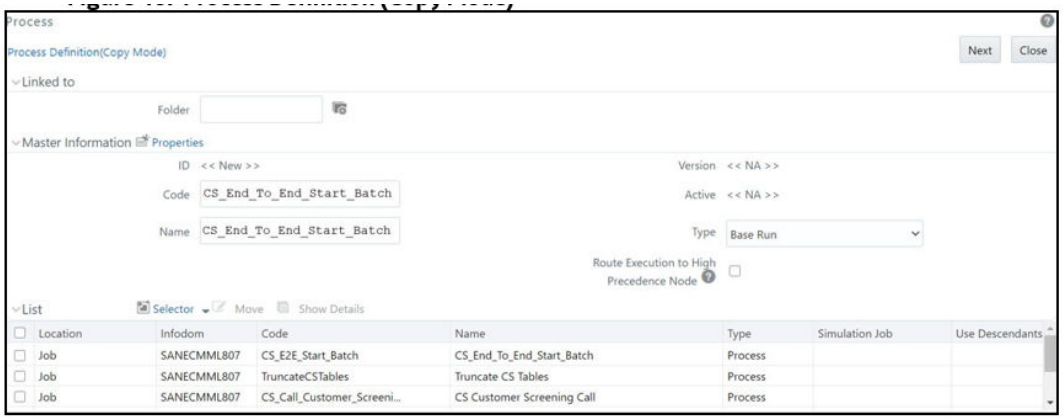
Figure 4-40 Process page



5. Click **Copy**.

   The **Process** page opens in Copy mode.

Figure 4-41 Process Definition (Copy Mode)

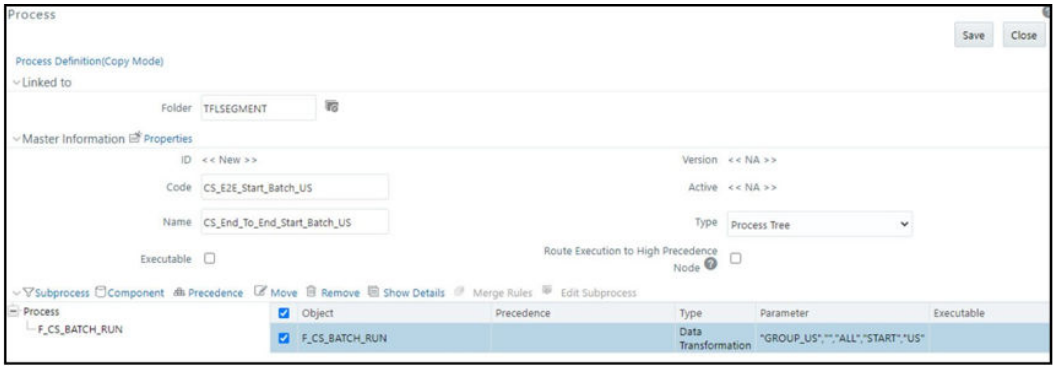


6. In the **Folder** field, click **Folder** and then select **TFLSEGMENT**.

Figure 4-42 Folder Selector

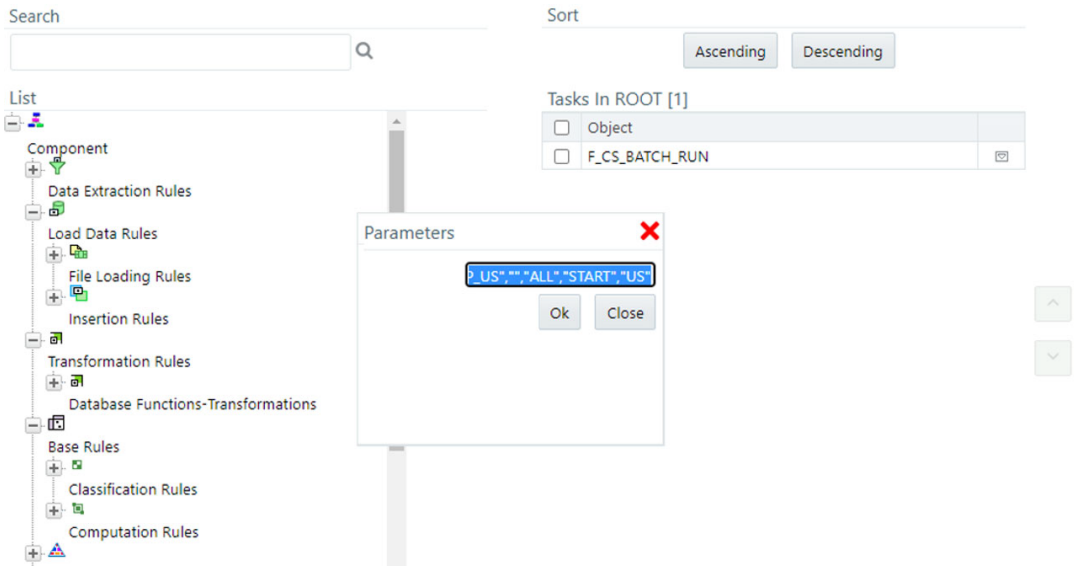
7. In the Name field, change the job name to include the Jurisdiction Code. For example, `CS_Data_Load_Event_Generation_US`.
8. Select `F_CS_BATCH_RUN`.

Figure 4-43 Process Definition (Copy Mode)



9. Select Component.
10. In the **Parameters** window, select the `F_CS_BATCH_RUN` task and then click **drop-down list**. Change the parameter `ORACLECS` to the entry made in the `cs_processing_group` table and the parameter `CS` to the Jurisdiction Code. For example, `"GROUP_US","","ALL","START","US"`.

Figure 4-44 Component Selector window



11. Click **OK** to close the **Parameters** window.
12. Click **OK**.
13. Click **Save**.
14. Search for *End* in the **Code** field and select `CS_End_To_End_End_Batch`.
15. Click **Copy**.

    The Run Page opens in **Copy** mode.
16. In the **Folder** field, first click **Folder** and then select **TFLSEGMENT**.
17. In the **Name** field, change the job name to include the Jurisdiction Code. For example, `CS_Data_Load_Event_Generation_US`.
18. Select `F_CS_BATCH_RUN`.
19. Select **Component**.
20. In the **Parameter** field, change the parameter `ORACLECS` to the entry made in the `cs_processing_group` table. For example, `GROUP_US`, and the parameter `CS` to the Jurisdiction Code, for example, `US`.
21. Click **OK**.
22. Click **OK**.
23. Click **Save**.

    A confirmation message is displayed. The new parameter is now displayed in the **Run** page.

> **Note**
>
> In the example shown, the new processing batch name has been changed from `CS` to `US`. If this change is not made, no data is loaded in the tables.

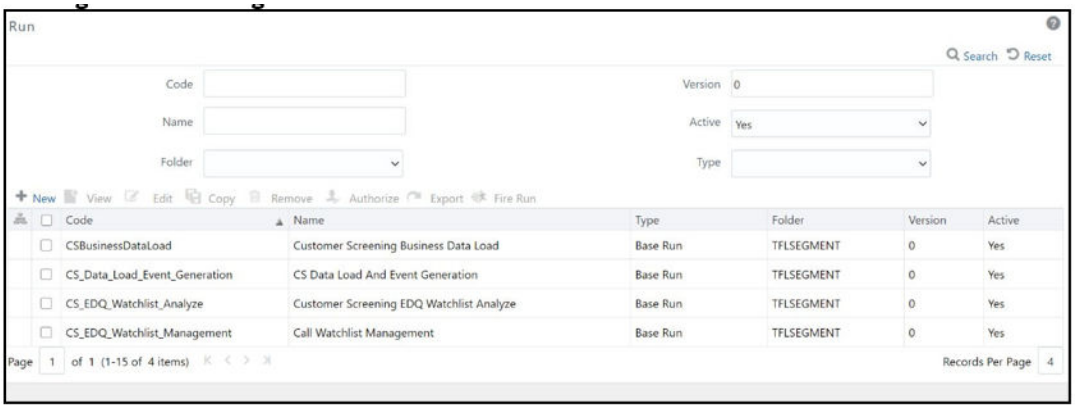
4.14.3.2 Creating a Run

To create a run, follow these steps:

1. Log on to the Customer Screening application.
2. Click **Common Tasks**, then click **Rule Run Framework**, and then click **Run**.

   The **Run** page is displayed.

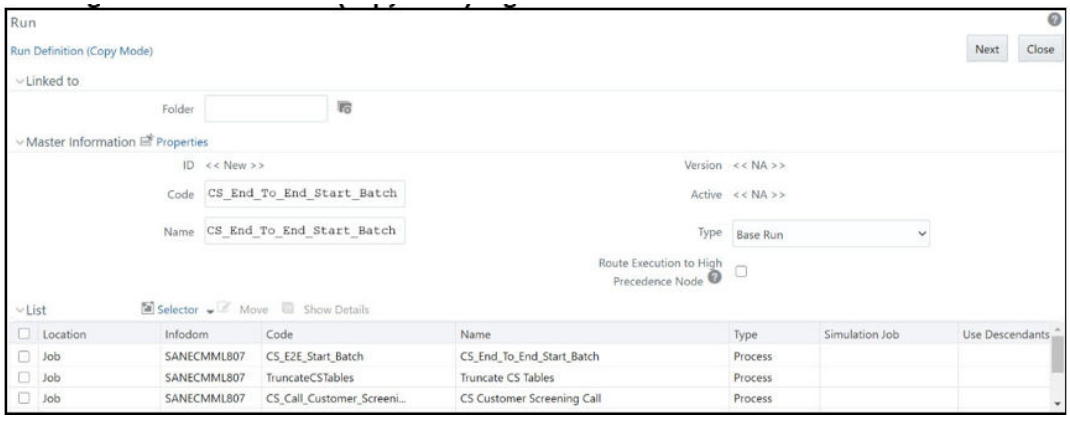
Figure 4-45 Run page



3. Search for *Start* in the **Code** field and select `CS_End_To_End_Start_Batch`.
4. Click **Copy**.

   The **Run** page opens in *Copy* mode.

Figure 4-46 Run Definition (Copy Mode) page



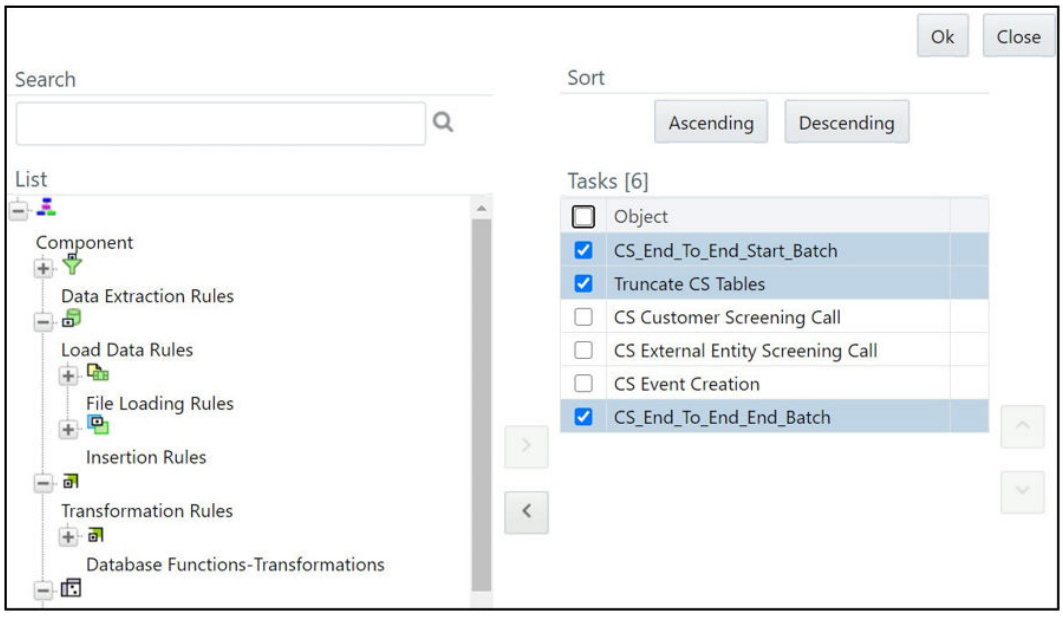
5. In the **Folder** field, click **Folder** and then select **TFLSEGMENT**.

Figure 4-47 Folder Selector

6. In the **Name** field, change the job name to include the Jurisdiction Code. For example, `CS_Data_Load_Event_Generation_US`.
7. Click **Selector** list and select **Job**.
8. In the **Component Selector** page, first select the `CS_End_To_End_Start_Batch`, `CS_End_To_End_End_Batch`, and `Truncate CS Tables tasks`(in that order) from the **Tasks** table and then click to move them to the **List** table.

   The tasks are moved to the **Processes** node.

Figure 4-48 Component Selector



> **Note**
>
> Ensure that you remove the `Truncate CS tables` job to prevent the removal of data. If, by mistake, you run the `Truncate CS tables` job, you can run the `CSBusinessDataLoad` job to reload data in the table.

9. Replace these tasks with the task created in Step 17, that is, `CS_Data_Load_Event_Generation_US`.

If you do not make this change, no data is loaded in the tables.

10. Click **OK**.
11. Click **OK**.
12. Click **Save**.

    The new job is displayed in the **Run** page.

> **Note**
>
> These steps must also be done in the ECM setup. The processes and runs created in Customer Screening create alerts, and the processes and runs created in ECM fetch the alerts. Cases are generated from these alerts. An example of a process created for ECM is `Oracle_CS_Event_Processing` and an example of a run created for ECM is `Oracle_CS_Event_Processing_US`.

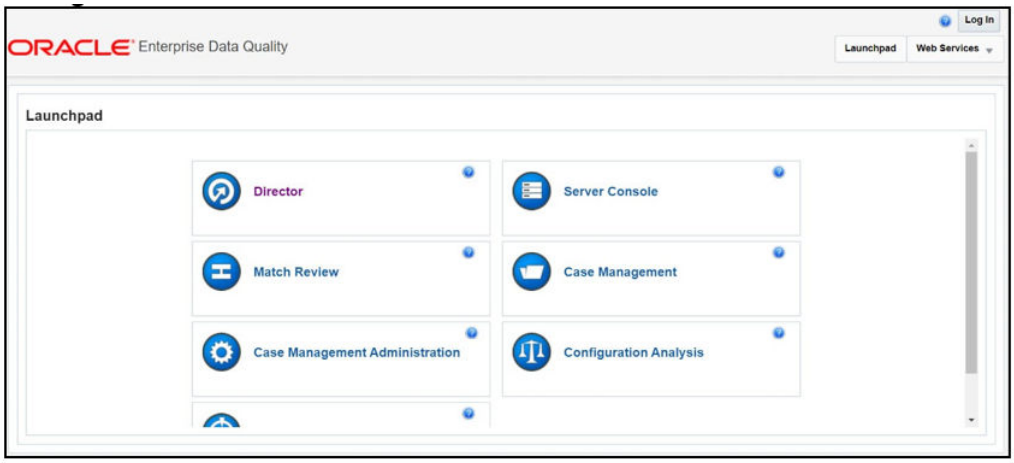
4.15 Configurations for General Data Protection Regulation (GDPR)

GDPR is a set of data protection rules. The main aim of GDPR is to give control to individuals over their data.

To enable GDPR, perform the following configurations:

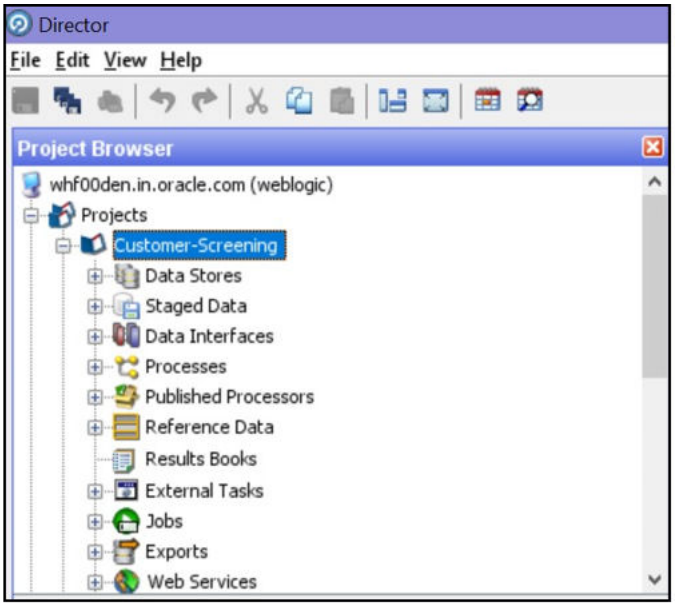
1. Create a user who will do the GDPR configurations in the same database, for example, GDPR.
2. Assign the `OFS_NOSEC_DATA` privilege to the user by executing the following grant: `GRANT OFS_NOSEC_DATA to GDPR`.
3. Follow these steps to connect to the user:
   a. Create a synonym called cs_customer for the user by executing the following command: CREATE PUBLIC SYNONYM cs_customer FOR {dbname}.cs_customer {dbname} is the user for whom the CUST data and GDPR is applied.
   Go to the EDQ URL and open the **Director** menu. The **Director** landing page is displayed.

Figure 4-49 Director Menu in EDQ



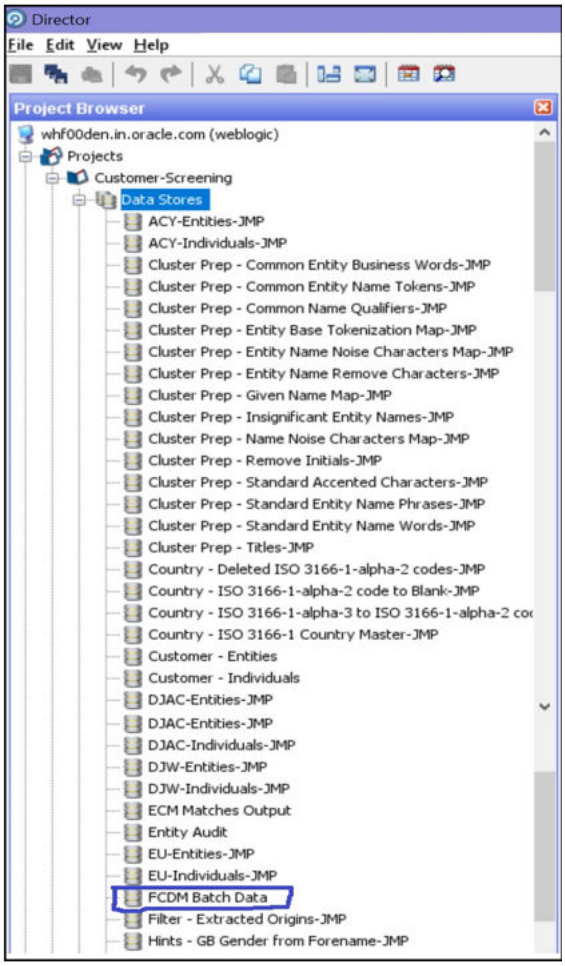
b. In the **Director** landing page, expand the **Customer-Screening** project in the **Project Browser** pane.

Figure 4-50 Project Browser pane



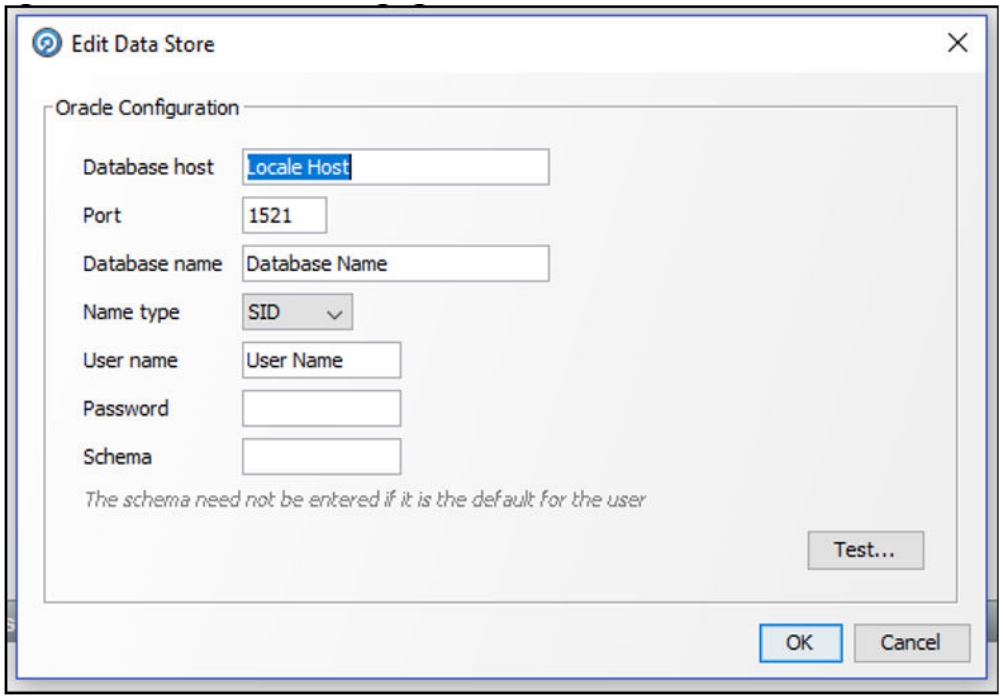
c. Expand the **Data Stores** node and open **FCDM Batch Data**. The **Edit Data Store** window is displayed.

Figure 4-51 Edit Data Store window



d. In the **Edit Data Store** window, enter the **Database host**, **Port**, **Database name**, **User name**, and **Password**.

Figure 4-52 Edit Data Store for Staging Database Connection



The GDPR configurations are now enabled for the GDPR user. You can view the applicable data in the CUST table.

4.16 Optional Configurations

This section describes about the optional configurations you can perform.

4.16.1 Data Quality Check

- To run the Data Quality (DQ) check, set the following values in the `watch list-management.properties` file. This file is located in the `<domain_name>/edq/oedq.local.home/ runprofiles/` directory in the WinSCP server.
  - `phase.DQ\ -\ Stage\ DJW\ reference\ lists.enabled = Y`
  - `phase.DQ\ -\ DJW\ reference\ data\ quality\ analysis.enabled = Y`
  - `stageddata.DQ\ DJW\ -\ Invalid\ Standard\ Country\ in\ DJ\ Country\ to\ Standard\ Country.visible = Y`
  - `stageddata.DQ\ DJW\ -\ Missing\ Category\ in\ DJW\ SI\ Category.visi- ble = Y`
  - `stageddata.DQ\ DJW\ -\ Missing\ Category\ in\ DJW\ SI\ Category\ Description.visible = Y`
  - `stageddata.DQ\ DJW\ -\ Missing\ DJW\ Country\ in\ DJ\ Country\ to\ Standard\ Country.visible = Y`
  - `stageddata.DQ\ DJW\ -\ Missing\ Name\ in\ DJW\ List\ Provider\ Reference\ Data.visible`

  - stageddata.DQ\ DJW\ -\ Missing\ Occupation\ Name\ in\ DJW\ Occupa- tion\ Category.visible
  - stageddata.DQ\ DJW\ -\ Obsolete\ Category\ in\ DJW\ SI\ Category.visible
  - stageddata.DQ\ DJW\ -\ Obsolete\ Category\ in\ DJW\ SI\ Category\ Description.visible
  - stageddata.DQ\ DJW\ -\ Obsolete\ DJW\ Country\ in\ DJW\ Country\ to\ Standard\ Country.visible
  - stageddata.DQ\ DJW\ -\ Obsolete\ Name\ in\ DJW\ List\ Provider\ Ref- erence\ Data.visible
  - stageddata.DQ\ DJW\ -\ Obsolete\ Occupation\ Name\ in\ DJW\ Occupa- tion\ Category.visible

- To move data from the Windows batch file to the Linux shell script, follow these steps in the `watch list-management.properties` file:
  - Comment out `phase.DJW\ -\ Download.externaltasks.Download\ Dow\ Jones\ Watch list.command = download-djw.bat`
  - Uncomment `phase.DJW\ -\ Download.externaltasks.Download\ Dow\ Jones\ Watch list.command = download-djw.sh`

4.16.2 Sorting Real-Time Watchlist Details

The order of Watchlist details displayed on the UI for Real-Time Screening alerts in CSAM or Case in ECM can be configured in this table:

`cs_rt_watchlistdetails_order`

The Order can be defined for Individual and Entity separately.

> **Note**
>
> If you want to insert any new field in between the order list, make sure `N_ORDER` column is properly sorted.

This change gets reflected in the following UIs:

- On click of Watchlist ID in Real-time Screening UI
- Watchlist Details in Alert Details page in CSAM
- Watchlist Details in Case Details page in ECM

4.17 Application Level Configuration

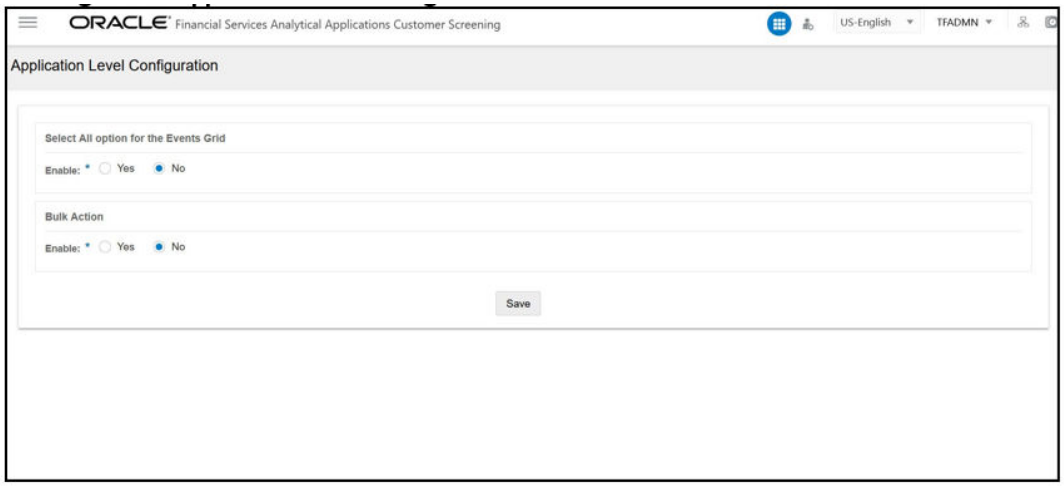
Use the Application Level Parameter Configuration tab to configure the parameters for the Customer Screening application, such as enabling or disabling the Select All option feature and enabling or disabling **Bulk Action** feature.

To configure the parameter using the CS application, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Customer Screening** Landing page.
2. Click **Application Level Configuration** in the Navigation List Available at the LHS.

The **Application Level Configuration** screen is displayed.

Figure 4-53 Application Level Configuration screen



3. Select **Yes** to enable the **Select All** option and select **No** to disable the Select All option in the Event table in Alert list details and click **Save**. For more information on alert details and event table, see Oracle Financial Services Customer Screening User Guide.
4. Select **Yes** to enable the **Bulk Action** option and select **No** to disable the **Bulk Action** option in the Alert List page and click **Save**. For more information on alert list page, see Oracle Financial Services Customer Screening User Guide.

> **Note**
>
> To display the bulk action in the Alert list page, function code must be mapped to the user group and the flag must be enabled.

4.17.1 Configuring Select All Option for the Events Table

You can configure the Select All option using Atomic Schema.

To configure Select All check box for the event table, follow these steps:

1. Access the Atomic Schema and access the `CS_APPLN_PARAMS` table.
2. For the `ZCS_SELECT_ALL` attribute enter the `PARAMETER_VALUE` value as **Y** to enable the **Select All** check box in the event table for the match summary. Enter **N** to disable the **Select All** check box.

4.17.2 Configuring Bulk Action Feature for the Alert List

You can configure the Bulk Action feature using Atomic Schema.

To display the bulk action button in the alert list page, follow the below steps:

1. Access the Atomic Schema and access the `CS_APPLN_PARAMS` table.
2. For the `ZCS_ENBL_BULK_ACTION` attribute enter the `PARAMETER_VALUE` value as **Y** to enable the **Bulk Action** button in the alert list page. Enter **N** to disable the **Bulk Action** button.

Optional: You can configure to display the alert decision for the bulk action. To enable or disable the Alert Decision in Bulk Action follow the below steps:

a. Access the Atomic Schema and access the `FCC_ZCS_ALERT_ACTIONS_DIM` table.

b. For the `F_IS_BULKACTION_ENABLE` attribute enter the `PARAMETER_VALUE` value as **Y** to enable or enter **N** to disable the alert decision in bulk action. By Default the value is **Y**.

4.18 Populating Country Code

To populate the country code, follow the subsequent steps:

1. Populate the `KDD_COUNTRY` table using the below query. This query will select the data from `STG_COUNTRY_MASTER` and insert into `KDD_COUNTRY` table:

```
INSERT INTO kdd_country (country_id, country_cd, country_nm, country_desc)
WITH country_data AS (SELECT DISTINCT v_iso_country_cd, v_country_name,
v_country_desc FROM stg_country_master WHERE TO_DATE(fic_mis_date, 'DD-Mon-
YY') = TO_DATE(?, 'DD-Mon-YY')) SELECT cm_geography_seq.nextval,
v_iso_country_cd, v_country_name, v_country_desc FROM country_data WHERE NOT
EXISTS (SELECT 1 FROM kdd_country kc WHERE kc.country_cd =
country_data.v_iso_country_cd);
```

2. Populate the `KDD_COUNTRY_TL` table using the below query. This query will select the data from `STG_COUNTRY_MASTER` and insert into `KDD_COUNTRY_TL` table:

```
INSERT INTO kdd_country_tl(v_locale_cd, country_id, country_cd, country_nm,
country_desc,v_source_locale)

SELECT 'en_us',country_id,country_cd,country_nm,country_desc,'en_us' FROM
kdd_country;
```

4.19 Addition of Extra Fields in Customer Details section

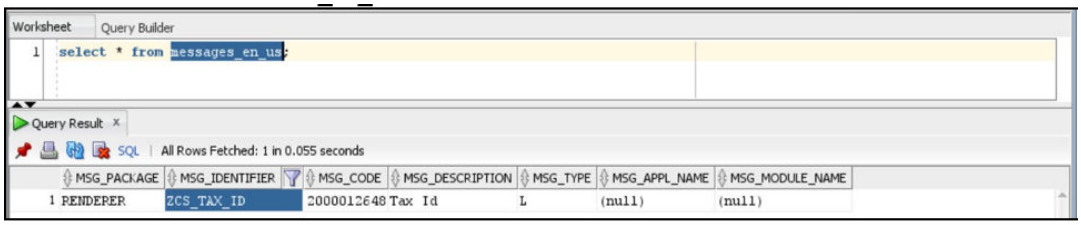
You can add extra fields for comparison in the Customer Details section of the Alert Details page and configure the fields to display in the Customer Details main page UI.

To add extra fields in Alert Details page UI follow the subsequent steps:

1. From the `FCC_ZCS_CUST` table select a field name to display in Customer Details section.
2. Create an entry in `MESSAGES_EN_US` table for the selected field name.

   For example, for `TAX_ID` field create an entry with message identifier as `ZCS_TAX_ID` in `MESSAGES_EN_US` table.

Figure 4-54 MESSAGE_EN_US table



3. After successful addition of field entry in the `MESSAGES_EN_US` table restart the server.
4. Rename field name by removing the underscore and converting the name from upper to lower case.

For example, rename from `TAX_ID` to `taxid`.

Check and validate that the Renamed field name exist in CS API response.

Following is a sample Customer Details API response:


```
[{"custId":"E000312","custaddeddate":"2010-09-
23","incdate":null,"custtype":"ORG","marriedstatus":null,"citizenship":n
ull,"asset":null,"fullname":null,"firstname":null,"middlename":null,"las
tname":null,"originalname":"Brookson (g)
Limited","aliasname":null,"sourceofwealth":null,"dob":null,"age":null,"r
esidencecode":null,"countryofbirth":null,"country":null,"publicprivate":
null,"foriegnpublicoff":null,"dpt":null,"compensateflag":null,"employeme
ntstatus":null,"creditrating":null,"workforfi":null,"creditscore":null,"
employername":null,"retirementyear":null,"custSeqId":"5331","jurisdictio
n":"Default","busdmn":"DEFAULT","datadumpdt":"2023-03-06
10:29:56","srccustseqid":"740","fnclprfllastupdtdt":null,"taxid":"TX_789
10","taxidfrmtcd":null,"annlincmbaseam":null,"netwrthbaseam":null,"lqdne
twrthbaseam":null,"eqtyknldgcd":null,"bndknldgcd":null,"optnknldgcd":nul
l,"ovrallknldgcd":null,"ovrallexpcd":null,"eqtyexpyrqt":null,"bndexpyrqt
":null,"optnexpyrqt":null,"annleqtytrdqt":null,"annlbndtrdqt":null,"annl
optntrdqt":null,"avgeqtytrdam":null,"avgbndtrdam":null,"avgoptntrdam":nu
ll,"suffnm":null,"titlnm":null,"form407fl":null,"ctzshpcntry1cd":null,"c
tzshpcntry2cd":null,"ocptnnm":null,"ageyrct":null,"ctzshpstatcd":null,"s
rcsyscd":null,"orglglstruccd":null,"pwdlastchgdt":null,"mplyrinduscd":nu
ll,"jobtitlnm":null,"cstm1dt":null,"cstm2dt":null,"cstm3dt":null,"cstm1r
l":null,"cstm2rl":null,"cstm3rl":null,"cstm1tx":null,"cstm2tx":null,"cst
m3tx":null,"totacctct":null,"custefctvrisknb":"0","cstm4tx":null,"cstm5t
x":null,"fnclinstnidtypecd":null,"fnclinstnid":null,"instnseqid":null,"c
ustlistrisknb":null,"custlistsrccd":null,"custmatchtx":null,"custmatchty
pecd":null,"custbusrisknb":"0","custgeorisknb":"0","cstmrisk1nb":"0","cs
tmrisk2nb":"0","daytrdknldgcd":null,"daytrdexpcd":null,"annlincmrptgam":
null,"netwrthrptgam":null,"lqdnetwrthrptgam":null,"prcsngbatchnm":"CS","
jrsdcncd":null,"busdmnlisttx":null,"rptgcrncycd":null,"mantascustbustype
cd":null,"custefctvriskfactrtx":null,"custpeergrpintrlid":null,"custstat
cd":"Active","taxtncntrycd":"SWIZ","custinduscd":null,"rgstntypecd":"AU" ,"alt
custid":null,"incmrngcd":null,"custgndrcd":"M","custnaicscd":null,"
maxdailyatmwdrwlam":null,"recalcitrantfl":null,"nonusctznresfl":null,"no
nusdocholderfl":null,"certlossnationfl":null,"fatcaexemptcd":null,"govtd
ocfl":null,"thrdpartycdtrptfl":null,"frgntaxrptngcertfl":null,"exceptedn
ffefl":null,"fatcaorgtypecd":null,"geojrsdcncd":null,"cpifl":null,"ultmt
instlcustintrlid":null,"cmdtyknldgcd":null,"cmdtyexpyrqt":null,"avgcmdty
trdam":null,"annlcmdtytrdqt":null,"emprlshptypecd":null,"dmcldbrchorgid" :null
,"giin":null,"giinissuedt":null,"custsubtypecd":null,"ficmisdate":" 2023-03-06
00:00:00","runskey":"102","dataorigin":"CS","applicationid":null,"branch
cd":null,"cddruleexempt":null,"cddruleexemptreason":null,"cipexcemptflag
":null,"cipexcemptreason":null,"relationshipteamcd":null,"request314":nu
ll,"stockexchgcd":null,"tickersymbol":null,"websiteurl":null}]
```


5. Go to the subsequent path and open the `Details creen.js` file.

   `<deployed-context>/CustomerScreening/js/viewmodels`

6. Search for `customeridtolabelmap` JSON object. Add a new entry inside `customeridtolabelmap` JSON object and Save it.

   For example, add the below entry for Tax ID:

   ```
   "taxid": {
   ```

```
label: CSMessageConstants.ZCS_TAX_ID,//"Tax Id",
order: 50, Displayinmain: "Y"
}
```

The entry consist of the following information:

- **Label:** Name of the field to display in the screen
- **Order:** Order of the field to display
- **Displayinmain:** Enter the value **Y** to display in the customer details main page or Enter **N** to display in the View Full Comparison page.

7. Go to the subsequent path and open the `CSMessageConstants.jsp` file.

   `<deployed-context>/CustomerScreening`

8. Create a new entry in the `CSMessageConstants.jsp` file for the field and save it.

   For example, for the `Tax_ID` field create an entry as below:

   ```
   CSMessageConstants.ZCS_TAX_ID="<%=MessageFramework.getMessageFromLocaleS
   peficCache("RENDERER.ZCS_TAX_ID", currentMsgLocale.toString())%>";
   ```

4.20 Configuring the Customer ID parameter for getting real time alerts in getAlertListForCustIdZipperCS API

If you use a customer ID other than `CustId` in RT screening request, you must change the default parameter value from `CustId` to the customized customer ID to get the RT alerts. RT alert is generated based on the customer ID value passed as an input to the API response. For API response, see OFS Customer Screening Data Interfaces Guide.

If you use the customized field for the customer ID and not configuring the value in the `CS_APPLN_PARAMS` table, you will not get RT alerts for the values passed against the customized field.

To configure the RT customer ID parameter value follow the subsequent steps:

1. Access the Atomic Schema and access the `CS_APPLN_PARAMS` table.
2. Change the `RT_CUST_ID_PARAM` parameter value from `CustId` to customized customer ID.

4.21 Configuring Bulk Action on the Events

If the bulk action on the events are configured, events are updated as per the configuration. This feature allows you to make decisions on events in bulk in accordance with the bulk action feature that is currently available for alerts on the alert list page. This feature can be enabled or disabled, and the required event decision mapping for alert decisions can be performed in the backend.

To enable or disable, and do the required decision mapping for the alert follow the subsequent steps:

1. Access the Atomic Schema and access the `FCC_ZCS_ALERT_ACTIONS_DIM` table.
2. Change the value for the following parameters:
   - `V_EVNT_UPDATE_FL`
   - `V_EVNT_DECISION_OVERRIDE_FL`

- V_EVENT_STATUS_CODE

Based on the FCC_ZCS_ALERT_ACTIONS_DIM table configuration, while performing bulk action, you must update the event status to V_EVENT_STATUS_CODE value for that particular action.

The event decision will only override when the V_EVNT_DECISION_OVERRIDE_FL is enabled as **Y**. If V_EVNT_DECISION_OVERRIDE_FL value is **N**, then the Events in the Pending status are updated.

Use Case 1:

When the V_EVNT_UPDATE_FL value is **N**, the events inside the alert are not updated.

Use Case 2:

When the V_EVNT_UPDATE_FL value is **Y**, then the system will check whether the V_EVNT_DECISION_OVERRIDE_FL is enabled or not.

- The V_EVNT_DECISION_OVERRIDE_FL value is **N**: Event decision status will not be overwritten.
- The V_EVNT_DECISION_OVERRIDE_FL value is **Y**: Event decision status will be overwritten with V_EVENT_STATUS_CODE value.

4.22 Splitting the Alerts Based on the Event Type Configuration

You can split the alerts by event type rather than group them in one alert. Based on the matches generated, separate alerts are created for SAN, PEP, and EDD.

To configure the alert splitting based on the event type, follow the subsequent steps:

1. Access the Atomic Schema and access the CS_APPLN_PARAMS table.
2. Change the ZCS_SPLIT_ALERT_TYPE parameter value as follows:
   - **Y** to enable the split alert function.
   - **N** to disable the split alert function.

4.23 Merging the Events based on the Watchlist ID for CS Alerts

To configure the merging the events based on parameters, follow the subsequent steps:

1. Access the Atomic Schema and access the CS_APPLN_PARAMS table.
2. For the CS_EVNT_GRPNG_ATTRS parameter, enter the value based on which we want to merge the events.

   Out Of the Box (By Default), the values are "ListKey, ListSubKey, ListRecordType, and ListId". We can customize them based on our requirement.

4.24 Configuring Batch Audit Trial

Configuring the batch audit trail provides traceability and transparency for batch operations within the system. This enables compliance monitoring, supports internal reviews, and facilitates easy extraction of audit reports for regulatory or business needs.

To configure the batch audit trail, follow the steps:

1. Access the Atomic Schema and open the CS_APPLN_PARAMS table.
2. Enable the batch audit trail by setting the CS_BATCH_AUDIT parameter to 'Y'.

When the CS Data Load And Event Generation batch is executed, it triggers the CSBatchAudit task. This task internally calls F_POPULATE_BATCH_DATA_AUDIT, which inserts data into the following audit tables:

- CS_CUST_AUDIT (All the customer attributes screened for EDQ)
- CS_EE_AUDIT (All the external entity attributes screened for EDQ)
- CS_MATCHES_AUDIT (All the matches data from EDQ)
- CS_WATCHLIST_AUDIT (All the matched watchlist data from EDQ)
- CS_UNSCREENED_CUSTDATA (All the unscreened data will be stored here):

Customers or external entities without names are not screened by default. To enable screening for these unnamed records, set the following property to Y in both customer-screening.properties and external-entity-screening.properties:

3. After batch processing is completed, generate screened data reports:
4. Navigate to FIC_HOME/CS-OAS-Report-Queries.
5. Choose from the following sample SQL files based on your reporting needs:
   - ZIPPER_ALERT_EE_AUDIT.sql — External Entities (Zipper alerts)
   - ZIPPER_ALERT_CUST_AUDIT.sql — Customer Data (Zipper alerts)
   - ECM_CASE_EE_AUDIT.sql — External Entities (ECM case)
   - ECM_CASE_CUST_AUDIT.sql — Customer (ECM case)

   Select a sample query and customize it as needed for your requirements, then execute it in the Atomic schema to generate the desired report.

5

Integrations with Enterprise Case Management

Customer Screening uses the Enterprise Case Management (ECM) application to investigate and manage cases generated by the matching process in Customer Screening.

The following sections describe the default case types and workflows provided with **Oracle Financial Services Enterprise Case Management**. For more information, see Oracle Financial Services Enterprise Case Management Admin Guide.

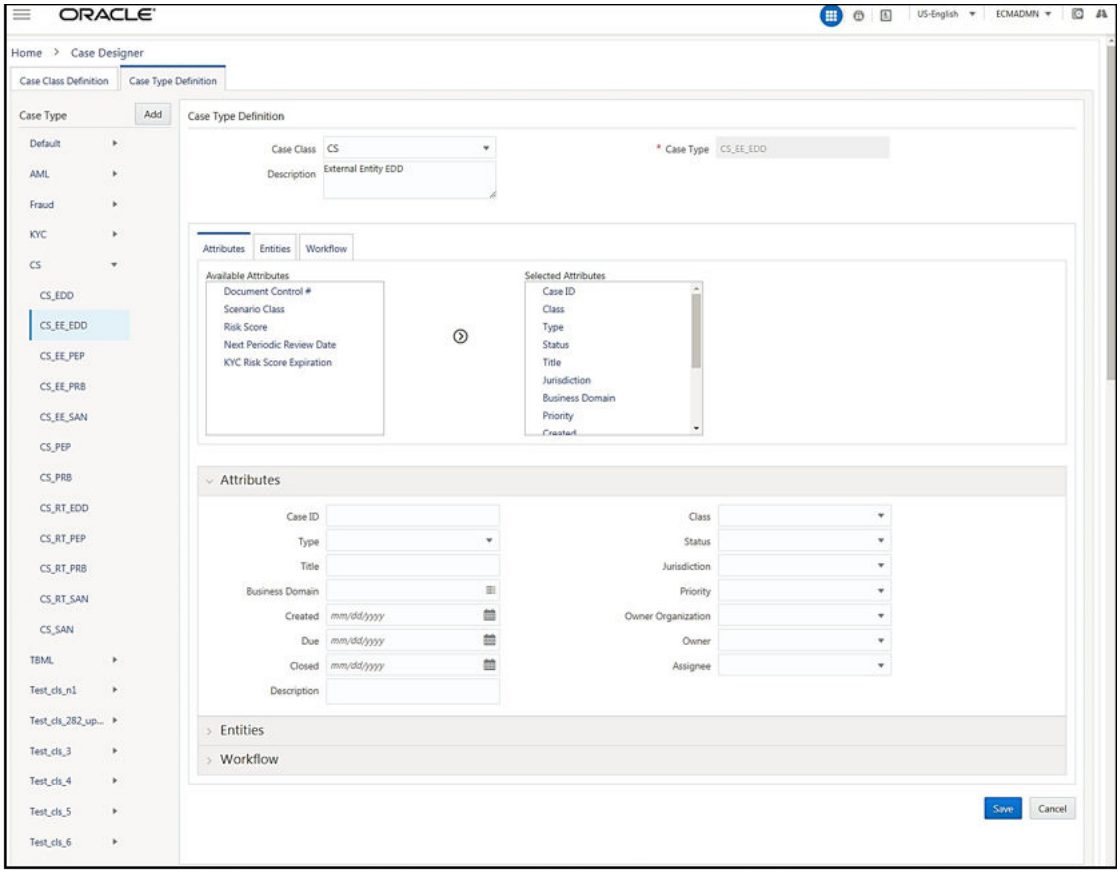
5.1 Case Class in ECM

For Customer Screening Application, the following case classes have been added in the Oracle Financial Services Enterprise Case Management Application:

- CS
- CS_EE
- CS_RT

To add new case classes, follow the steps in the **Adding Case Class** section in the Oracle Financial Services Enterprise Case Management Admin Guide.

Figure 5-1 Case Designer page



5.2 Case Types under Case Class

The following case types are created for the CS Case Class:

- **CS_EDD**: Enhanced Due Diligence (EDD)
- **CS_PRB**: Prohibition (PRB)
- **CS_SAN**: Sanctions (SAN)
- **CS_EE_EDD**: Enhanced Due Diligence (EDD) for External Entity Screening
- **CS_EE_PEP**: Politically Exposed Person (PEP) for External Entity Screening
- **CS_EE_PRB**: Prohibition (PRB) for External Entity Screening
- **CS_EE_SAN**: Sanctions (SAN) for External Entity Screening
- **CS_PEP**: Politically Exposed Person (PEP)
- **CS_RT_EDD**: Enhanced Due Diligence (EDD) for Real-Time Screening
- **CS_RT_PEP**: Politically Exposed Person (PEP) for Real-Time Screening
- **CS_RT_PRB**: Prohibition (PRB) for Real-Time Screening
- **CS_RT_SAN**: Sanctions (SAN) for Real-Time Screening

For each Case Type, default Entities are mapped. If additional Entities are required, see the **Adding Optional Entities to the Case Type** section in Oracle Financial Services Enterprise Case Management Admin Guide.

5.3 Case Correlation, Linked Cases, and Searching for Cases

After the Customer Screening batch is run, alerts are correlated into cases based on the watch list record type. More than one case can be generated for a single alert, one each for Sanctions (SAN), Country Prohibitions (PRB), Politically Exposed Persons (PEP), and Enhanced Due Diligence (EDD).

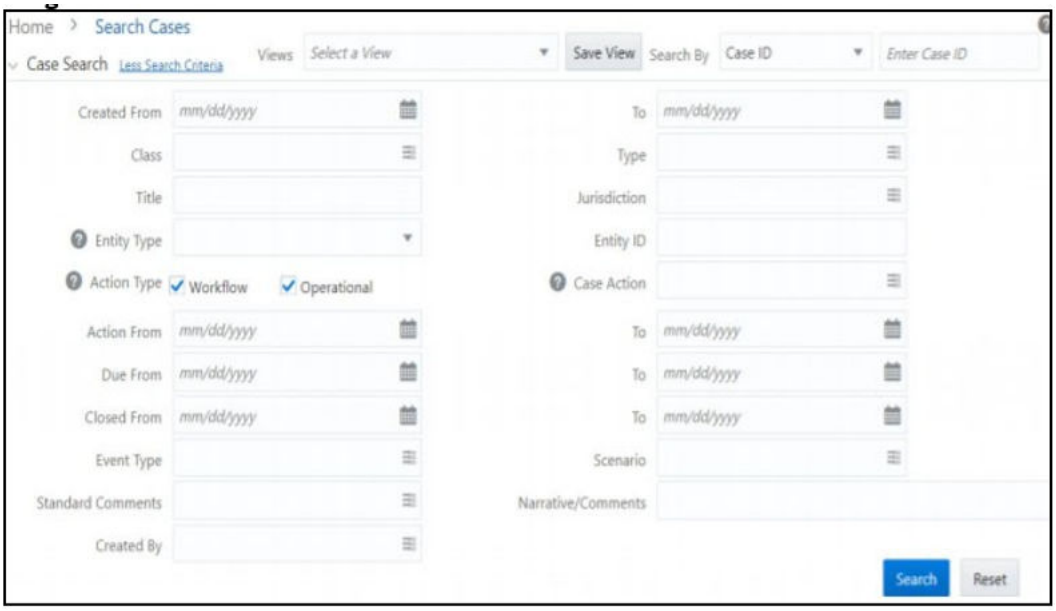
You can view the case which is linked with the case being investigated. The following image shows the fields:

Figure 5-2 Link Cases window

You can configure the correlation rules for an alert in the Correlation tab, or view the cases linked to the case being investigated in the Relationship tab. For more information, see the Using Operational Data tabs section in Oracle Financial Services Enterprise Case Management User Guide.

There are certain ready-to-use Customer Screening case type search criteria. They can be viewed in the Search Cases tab in ECM. For more information, see the Searching Cases section in Oracle Financial Services Enterprise Case Management User Guide.

Figure 5-3 Search Cases window



5.4 Creating Workflows for Case Types

Each of the Sanctions (SAN), Country Prohibitions (PRB), Politically Exposed Persons (PEP), and Enhanced Due Diligence (EDD) cases go through a workflow. The SAN and PRB cases have the same ready-to-use workflow, and the PEP and EDD cases have the same workflow.

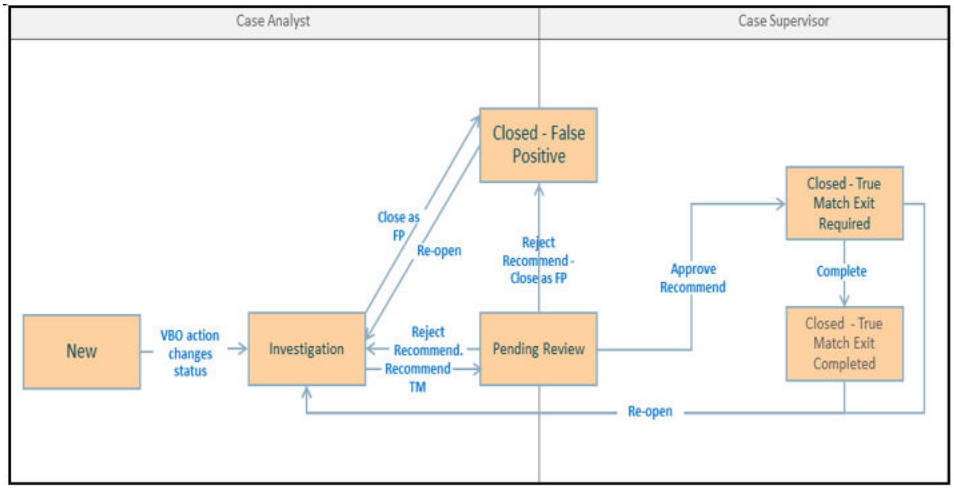
5.5 Workflow Diagrams

The following diagrams represent the workflows for the Sanctions (SAN), Politically Exposed Persons (PEP), Country Prohibition (PRB), or Enhanced Due Diligence (EDD) records:

5.5.1 SAN and PRB Workflow

The workflow for the Sanctions and country prohibition records are as follows:

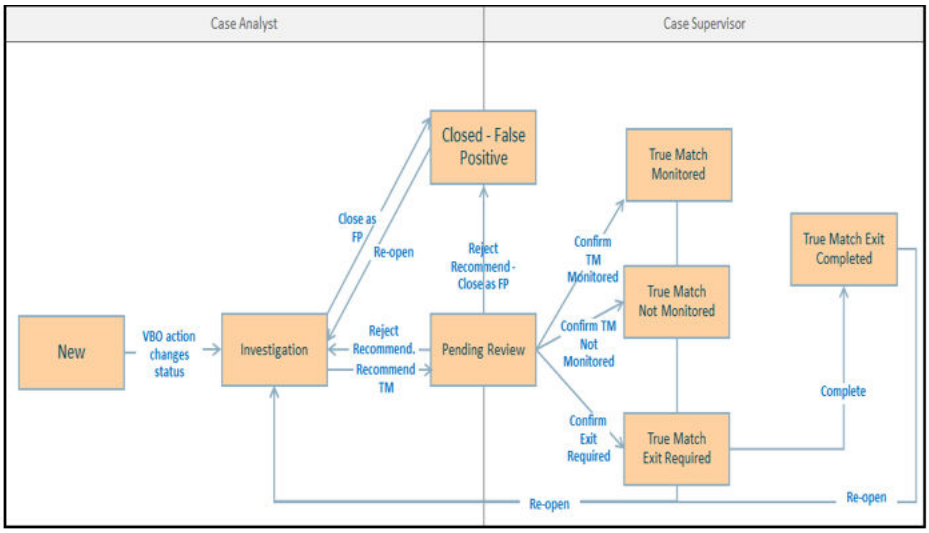
Figure 5-4 SAN and PRB Workflow



5.5.2 PEP and EDD Workflow

The workflow for the Politically Exposed Persons and Enhanced Due Diligence records are as follows:

Figure 5-5 PEP and EDD Workflow

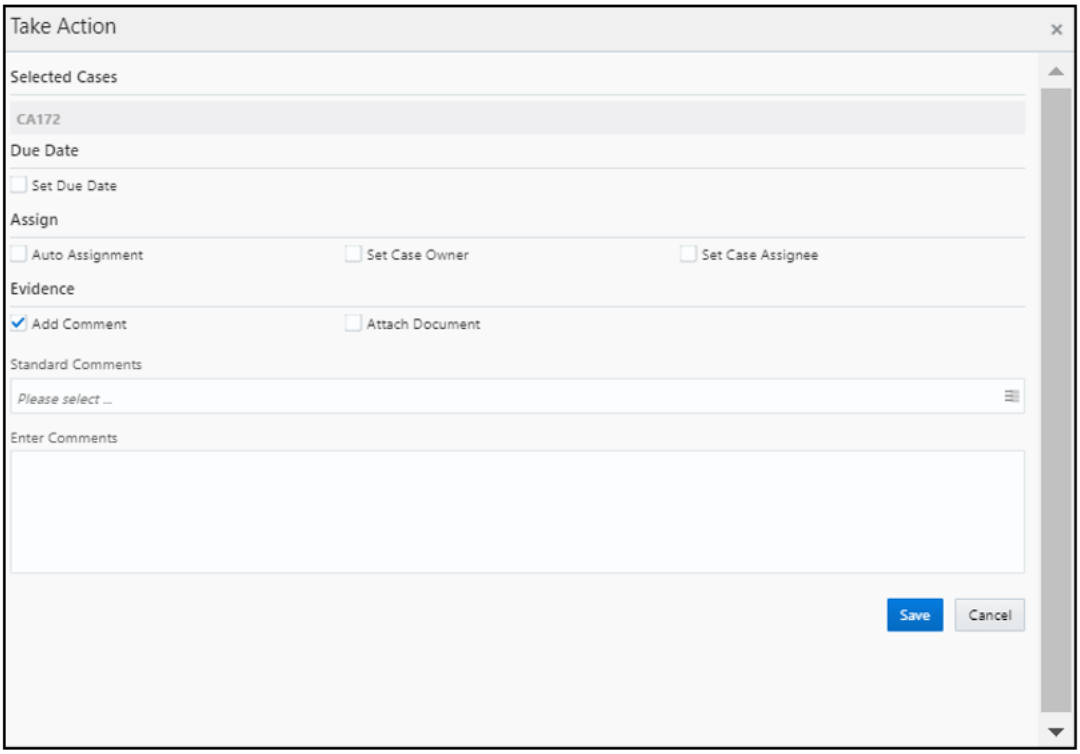


5.6 Taking Actions on Customer Screening-related Cases

You can take an action on a case depending on the workflow status, case type, and user. You can also add a comment and attach a document To take an action on a case, see the **Using Take Action window** section in Oracle Financial Services Enterprise Case Management User Guide.

The following figure shows a sample of an EDD workflow that has a Pending Review status and Supervisor user.

Figure 5-6 Take Action window



> **Note**
>
> When a match decision is taken for an alert, you can make the comments mandatory or optional.
>
> - To make comments mandatory, set the values of the `REQ_CMNT_FL` column in the `KDD_ACTION` table to **Y**. Run `select t.action_cd,t.action_nm from kdd_action t` and update the value. You cannot take an action until you provide a comment.
> - To make comments optional, set the values of the `REQ_CMNT_FL` column in the `KDD_ACTION` table to **N**. You can take an action even if you do not provide a comment.

5.7 Setting Thresholds for Case Priorities

The case priority is based on the case type and risk score. You can set the case priority in the `FCC_CASE_PRIORITY` table. By default, if you do not set the case priority, it is set to **High**.

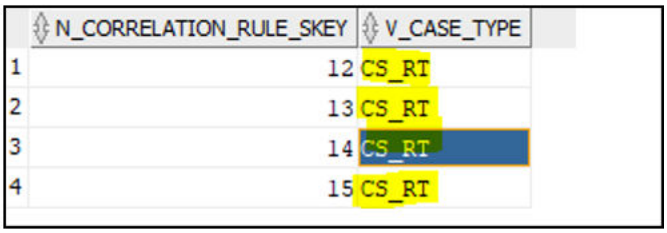
5.8 Merging Case Types

Alerts are correlated into cases based on the watch list record type when you run the Customer Screening batch. The record types Sanctions (SAN), Country Prohibitions (PRB), Politically Exposed Persons (PEP), and Enhanced Due Diligence (EDD) are merged under a single case ID based on the configuration.

To merge ECM case types follow the below steps:

1. Create new case type under case the class CS in ECM from Case Designer. For example consider the case type CS_RT. Map the entities and workflow from the user interface while creating the case type. See the **Managing Case Designer** section in Oracle Financial Services Enterprise Case Management Admin Guide.
2. Update the entries 12, 13, 14, and 15 in the FCC_CORRELATION_CASE_TYPE_MAP table with new case type CS_RT created in step 1.

Figure 5-7 FCC_CORRELATION_CASE_TYPE_MAP table

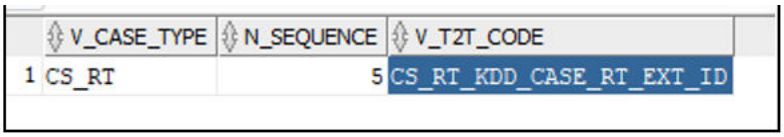


	N_CORRELATION_RULE_SKEY	V_CASE_TYPE
1	12	CS_RT
2	13	CS_RT
3	14	CS_RT
4	15	CS_RT

```
update FCC_CORRELATION_CASE_TYPE_MAP set v_case_type = 'CS_RT' where
N_CORRELATION_RULE_SKEY in (12,13,14,15);
```

3. Add a new entry in the FCC_RT_EVENTTYPE_PTC table for the newly created case type CS_RT.

Figure 5-8 FCC_RT_EVENTTYPE_PTC table

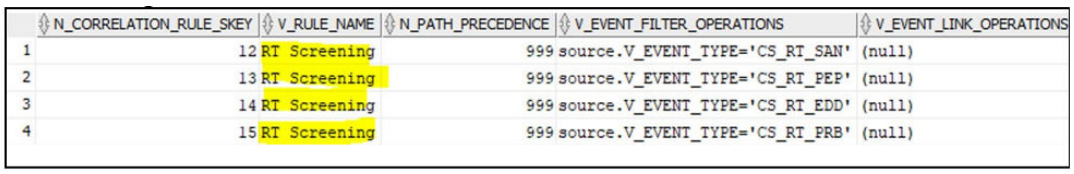


	V_CASE_TYPE	N_SEQUENCE	V_T2T_CODE
1	CS_RT	5	CS_RT_KDD_CASE_RT_EXT_ID

```
insert into FCC_RT_EVENTTYPE_PTC select 'CS_RT',
'5','CS_RT_KDD_CASE_RT_EXT_ID' from FCC_RT_EVENTTYPE_PTC where V_CASE_TYPE =
'CS_RT_SAN';
```

4. Update the entries 12, 13, 14, and 15 in FCC_CORRELATION_RULE table to reflect the new title for the case type CS_RT.

Figure 5-9 FCC_CORRELATION_RULE table

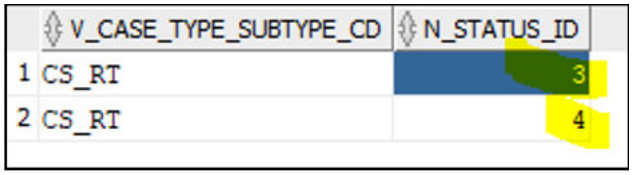


	N_CORRELATION_RULE_SKEY	V_RULE_NAME	N_PATH_PRECEDENCE	V_EVENT_FILTER_OPERATIONS	V_EVENT_LINK_OPERATIONS
1	12	RT Screening	999	source.V_EVENT_TYPE='CS_RT_SAN'	(null)
2	13	RT Screening	999	source.V_EVENT_TYPE='CS_RT_PEP'	(null)
3	14	RT Screening	999	source.V_EVENT_TYPE='CS_RT_EDD'	(null)
4	15	RT Screening	999	source.V_EVENT_TYPE='CS_RT_PRB'	(null)

```
update FCC_CORRELATION_RULE set V_RULE_NAME = 'RealTime Screening' where
N_CORRELATION_RULE_SKEY in (12,13,14,15);
```

5. In the Case Summary page, insert the status ID entries in the FCC_CASETYPE_EVENT_STATUS_MAP table for the new case type CS_RT to get the event decisions in the Set Event Decision window.

Figure 5-10 FCC_CASETYPE_EVENT_STATUS_MAP table

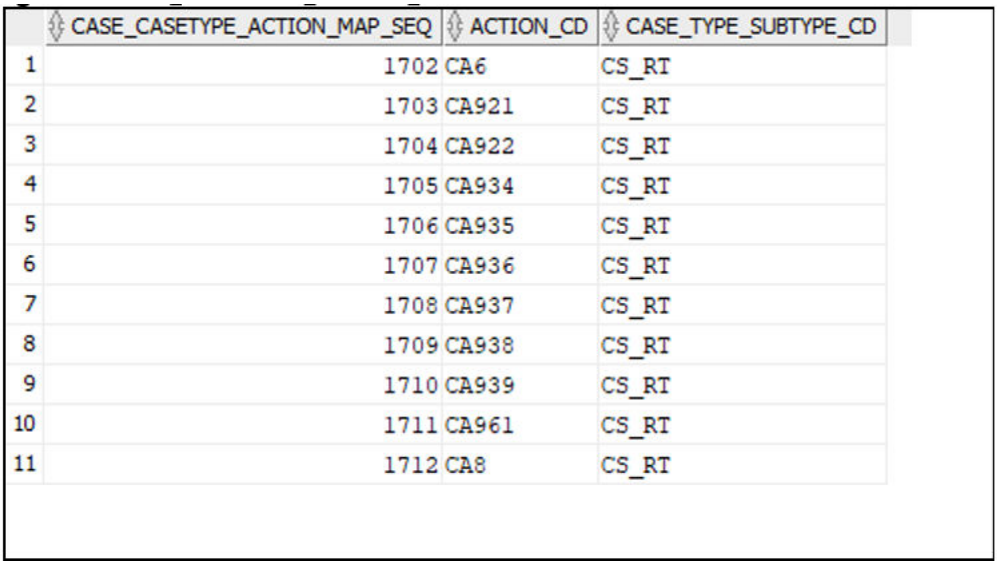


	V_CASE_TYPE_SUBTYPE_CD	N_STATUS_ID
1	CS_RT	3
2	CS_RT	4

```
insert into FCC_CASETYPE_EVENT_STATUS_MAP select 'CS_RT', n_status_id from
FCC_CASETYPE_EVENT_STATUS_MAP where V_CASE_TYPE_SUBTYPE_CD = 'CS_RT_SAN';
```

6. To get the details in Take Action Pop-up window, insert the below entries in the KDD_CASETYPE_ACTION_MAP-SEQ table for the new case type CS_RT.

Figure 5-11 KDD_CASETYPE_ACTION_MAP-SEQ table



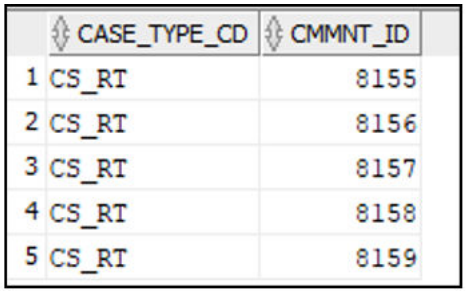
	CASE_CASETYPE_ACTION_MAP_SEQ	ACTION_CD	CASE_TYPE_SUBTYPE_CD
1	1702	CA6	CS_RT
2	1703	CA921	CS_RT
3	1704	CA922	CS_RT
4	1705	CA934	CS_RT
5	1706	CA935	CS_RT
6	1707	CA936	CS_RT
7	1708	CA937	CS_RT
8	1709	CA938	CS_RT
9	1710	CA939	CS_RT
10	1711	CA961	CS_RT
11	1712	CA8	CS_RT

```
Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA6','CS_RT');

Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA921','CS_RT');

Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA922','CS_RT');
```

```
Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA934','CS_RT');

Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA935','CS_RT');

Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA936','CS_RT');

Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA937','CS_RT');

Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA938','CS_RT');

Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA939','CS_RT');

Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA961','CS_RT');

Insert into KDD_CASETYPE_ACTION_MAP
(CASE_CASETYPE_ACTION_MAP_SEQ,ACTION_CD,CASE_TYPE_SUBTYPE_CD) values ((select
max(CASE_CASETYPE_ACTION_MAP_SEQ) from kdd_casetype_action_map)
+1,'CA8','CS_RT');
```

7. To get the values in standard comments drop down, insert below entries in `KDD_CASE_TYPE_CMMNT` table for the new case type `CS_RT`.

Figure 5-12 KDD_CASE_TYPE_CMMNT table

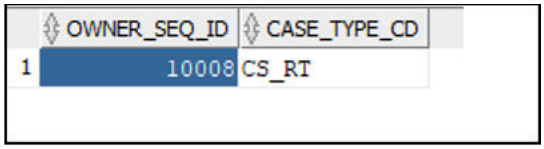


	CASE_TYPE_CD	CMMNT_ID
1	CS_RT	8155
2	CS_RT	8156
3	CS_RT	8157
4	CS_RT	8158
5	CS_RT	8159

```
insert into kdd_case_type_cmmnt select 'CS_RT', CMMNT_ID from
kdd_case_type_cmmnt where CASE_TYPE_CD = 'CS_RT_SAN';
```

8. Map the OWNER_SEQ_ID table entry with the new case type CS_RT created in the KDD_REVIEW_OWNER_CASE_TYPE table and restart the server.

Figure 5-13 OWNER_SEQ_ID table



	OWNER_SEQ_ID	CASE_TYPE_CD
1	10008	CS_RT

```
INSERT INTO KDD_REVIEW_OWNER_CASE_TYPE (OWNER_SEQ_ID, CASE_TYPE_CD) VALUES
($OWNER_SEQ_ID$, 'CS_RT')
```

6
Real-Time Screening

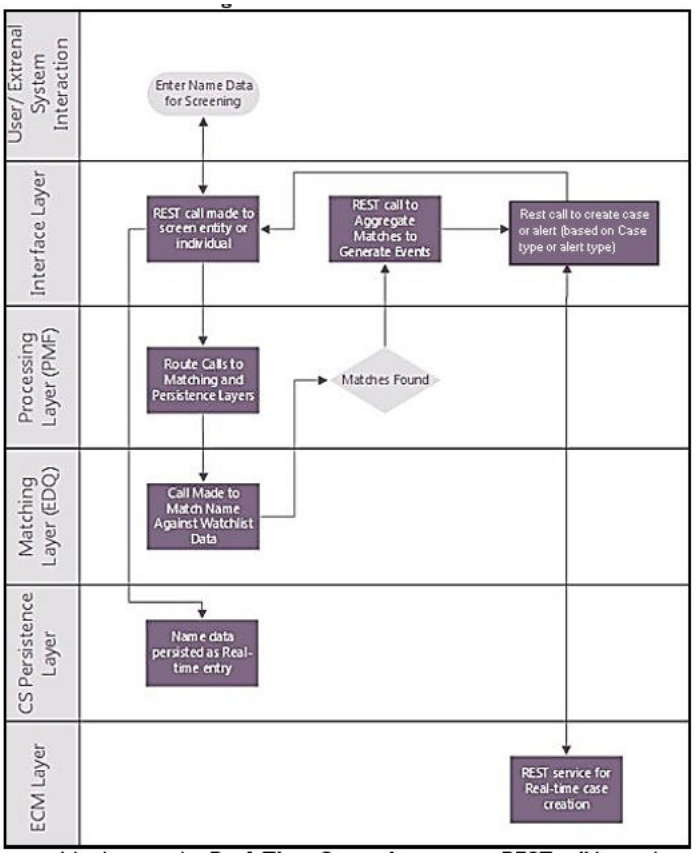
There are two ways to perform screening in the Customer Screening application: Real-Time Screening and batch screening.

Real-Time Screening is the screening of individuals and entities that occur when you enter data in the Real-Time Screening page and click Scan (Analyst & Supervisor) and Scan & Investigate (Analyst & Supervisor) to see the screening results and details of Alert generation or Case creation. You can also view the Alert details or Case details from screening results. For more information, see File Upload. To enable scan & Investigate, map the role Scan & Investigate to CSRTGRP group.

Batch Screening is the screening of individuals and entities that occur when you run the Batch Screening job. Before you run the job, you must first configure the **Enterprise Data Quality** (Director) details and then prepare and analyze the customer screening and external entity data in the **Financial Crime Data Model** (FCDM). For more information, see Running the Batch Screening Job.

The following image shows the different components involved during the Real-time screening process:

Figure 6-1 Real-Time Screening Workflow



After you provide data on the **Real-Time Screening** page, a REST call is made to the individual or entity being screened in the real-time screening user interface. The call is then routed to the **Enterprise Data Quality** (EDQ) system through the **Process Modelling Framework** (PMF) application. The information is then matched against the watch list data. Data is also persisted as external entities in the `FCT_RTSCR_REQUEST` table.

If a match is found, the matches are aggregated. The aggregated matches are used to create alerts and cases for external entities in **Financial Crime Data Model** (FCDM) and **Analytical Application Infrastructure** (AAI) and generate responses in PMF. The alerts or cases are displayed in the **Case Summary** page in L1 Alert Management or Enterprise Case Management (ECM) for investigation.

> **Note**
>
> - Real-time screening can be performed only when the realtime screening job in EDQ is running.
> - To cancel the real-time screening process, select **Shutdown web services** in the **Cancel Individual Realtime Screening web services** dialog box.
> - The Real-time access group must only be mapped to the case supervisor or the case analyst users and must not be mapped to the admin user.

6.1 Configuring the EDQ URL

The Configuring the EDQ URL section describes the detailed process to configure the EDQ URL in Real- Time Screening with Customer Screening Alert Management (CSAM) and Enterprise Case Management (ECM) in the server.

To configure the EDQ URL for Real-time screening, follow these steps:

1. Navigate to the `FCI_DB_HOME/bin` directory.
2. Execute the command `/EDQInsert.sh <INFODOM NAME>`. This step is used to register the EDQ server details. You must replace the `INFODOM NAME` placeholder with your domain name.
3. Enter the following details in the console where the command is run:
   - **EDQ server IP**: An example of the EDQ URL is `<Host Name>:Port`. Replace this with your EDQ server's URL.
   - **EDQ Server Direct Port Number**: This is the JMX port number. This value must be 8090.
   - **EDQ Server User Name**: An example of the EDQ server user name is `weblogic`. Replace this with your EDQ server's user name.
   - **EDQ Password**: An example of the EDQ password is `weblogic1`. Replace this with your EDQ server's password.
4. Enter `CSAM` for alert management if the Customer Screening Alert Management (CSAM) is as L1 investigation for Real Time Screening.
5. If the Customer Screening Alert Management application is in the same server.

Figure 6-2 Configure the EDQ URL in Real-time Screening with Customer Screening Alert Management (CSAM) in the same Server

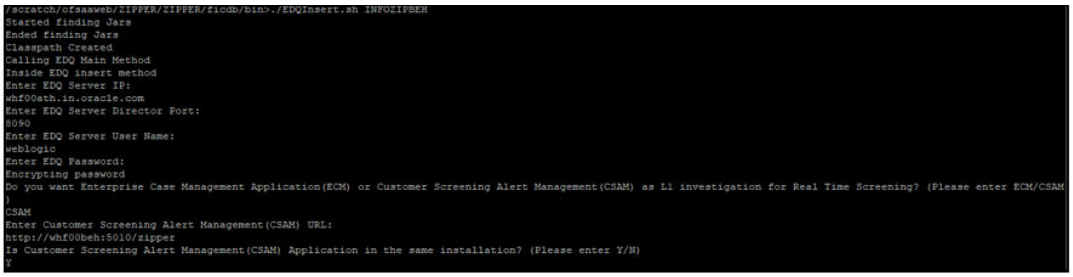
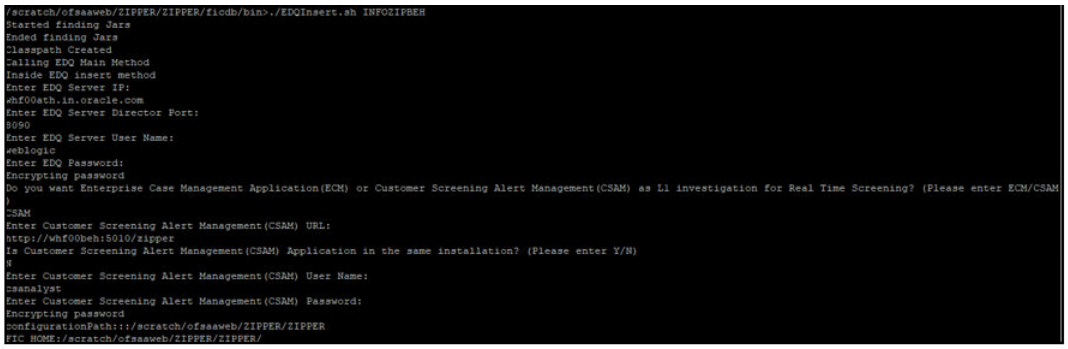


Figure 6-3 Configure the EDQ URL in Real-time Screening with Customer Screening Alert Management (CSAM) in different Server



6. Enter `ECM` for case creation if the Enterprise Case Management (ECM) is as L1 investigation for Real Time Screening.

   a. If the Enterprise Case Management application is in the same server.

Figure 6-4 Configure the EDQ URL in Real-time Screening with Enterprise Case Management (ECM) in the same Server

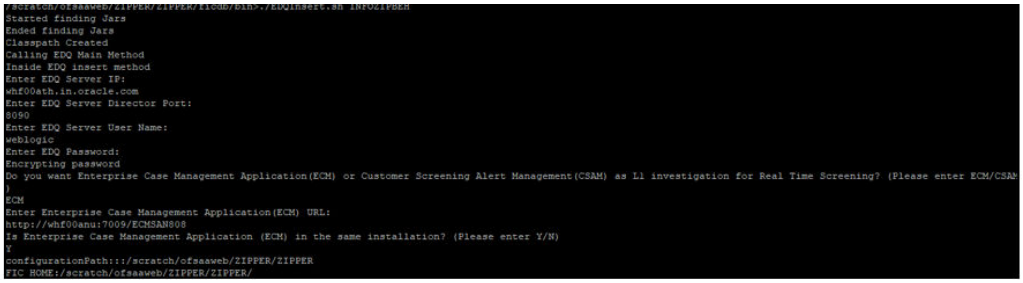
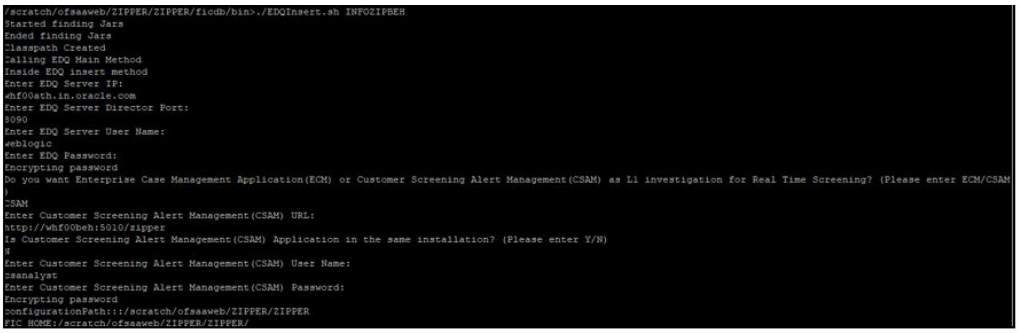


Figure 6-5 Configure the EDQ URL in Real-time Screening with Enterprise Case Management (ECM) in the different Server



7. Configure the EDQ URL in the CONFIG schema. To do this, run the following script and replace the placeholders in the `v_method_name` and `v_param_1` columns with the EDQ URL, EDQ user name, and EDQ password, respectively:

```
select t.*,t.rowid from aai_wf_application_api_b t where t.v_process_id='CSRT'
and t.v_app_api_id in ('1521535704140','1521535760435')
```

6.2 Screening Watch List Records in Real-Time

Real-Time Screening is the screening of individuals and entities that occur when you enter data in the Real-Time Screening page and click Scan (Analyst & Supervisor) and Scan & Investigate (Analyst & Supervisor) to see the screening results and details of Alert generation or Case creation. You can also view the Alert details or Case details from screening results.

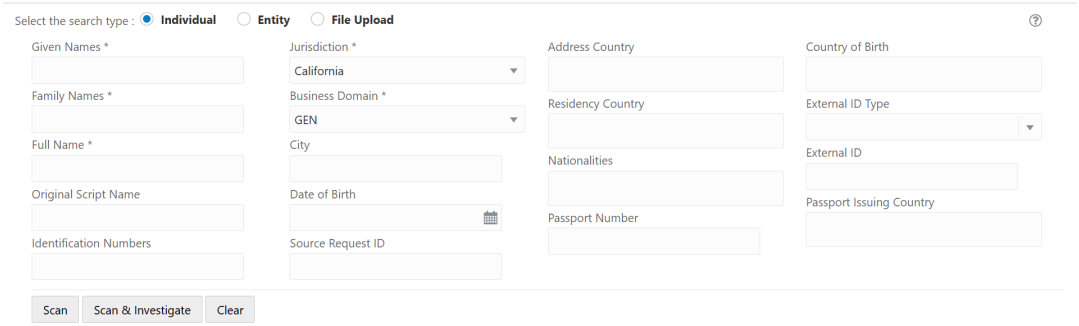
> **Note**
>
> Creating an Alert or Case is configurable. The Alert or Case will be generated when you select **CSAM** or **ECM**, respectively, while configuring EDQ URL. For more details, see Configuring the EDQ URL section.

6.2.1 Real-Time Screening for Individuals and Entities

To screen watch list records, follow these steps:

1. Log on to the Customer Screening application.
2. Click **Real-Time Screening** is displayed.

Figure 6-6 Real-Time Screening page

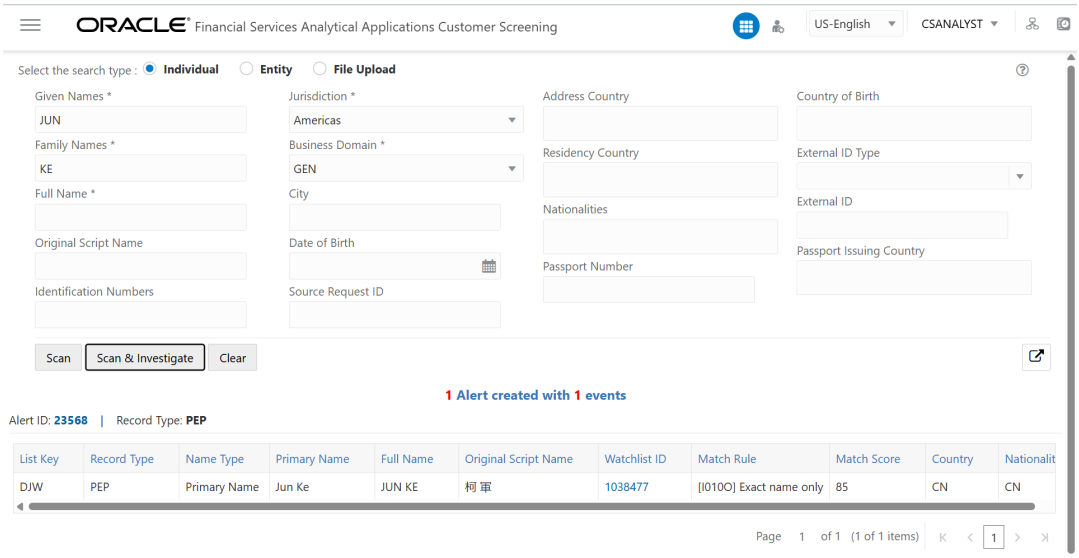


3. In the **Real-Time Screening** page, select the search type as **Individual** or **Entity**.

> **Note**
>
> - When L1 Investigation is CSAM, the `fcc_zcs_security_attr_grp_map` table must be populated to populate the business domain and jurisdiction.
> - When L1 Investigation is ECM, the ECM security mapper batch must be executed to populate the business domain and jurisdiction.

4. The following fields appear if the search type is **Individual**.

Figure 6-7 Individual Search Type



Enter/Select values for the Individual Search Type fields:

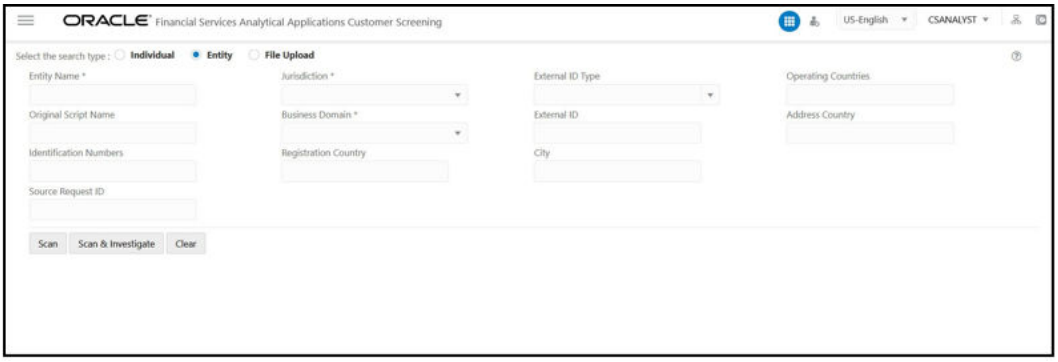
- Given Names
- Jurisdiction
- Business Domain
- Family Names
- Full Name
- Address Country
- Country of Birth
- Residency Country
- External ID Type
- Original Script Name
- City
- Nationalities
- External ID

- Date of Birth
- Passport Number
- Passport Issuing Country
- Identification Numbers
- Source Request ID

> **Note**
>
> - The combination of Given Name and Family Name or Full Name or Original Script Name or Passport Number along with Jurisdiction and Business Domain must provide to scan
> - The Source request ID is used to reconfigure and suppress the duplication of RT screening and Batch screening generated cases. For more information see Suppression of Alerts.

5. The following fields appear if the search type is Entity.

Figure 6-8 Entity Search Type



Provide details in the following mandatory fields:

- Entity Name
- Jurisdiction
- Business Domain
- Address Country
- Operating Countries
- Registration Country
- External ID Type
- Original Script Name
- City
- External ID
- Identification Numbers

- Source Request ID

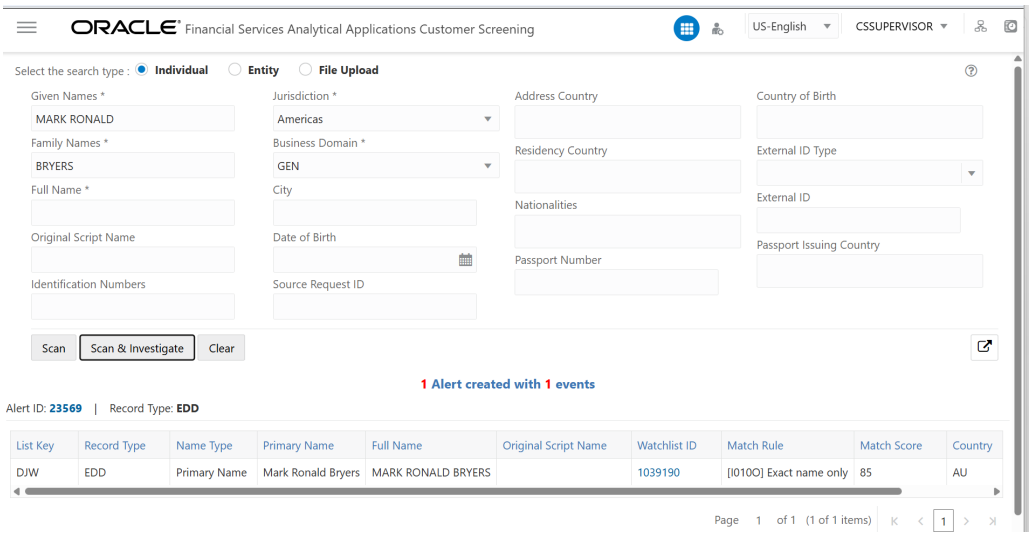
> **Note**
>
> - The combination of Entity Name or Original Script Name along with Jurisdiction and Business Domain must be provided to Scan.
> - The Source request ID is used to reconfigure and suppress the duplication of RT screening and Batch screening generated cases. For more information see Suppression of Alerts.

6. Perform the following for **Individual** or **Entity**:
7. Click **Scan**.

   The screened watch list records are displayed.

   a. **For Analyst & Supervisor:**
   Click **Scan**. The screened watch list records are displayed without creating an Alert in the L1 Investigation or case in ECM.

Figure 6-9 Scanning Real-time Screening Records table



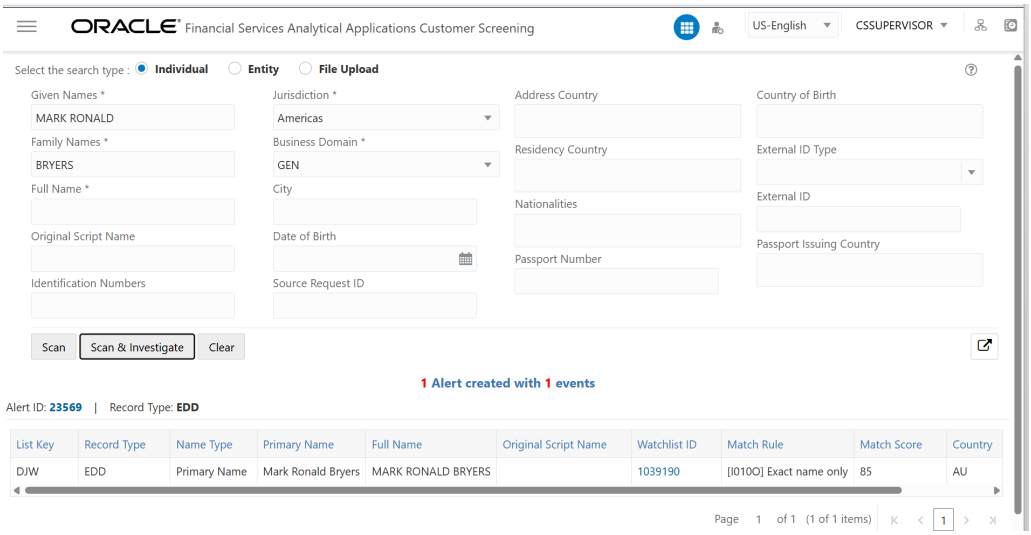
   b. **For Analyst & Supervisor:**
   Click **Scan**.

   It displays the screened watch list records.

   Click **Scan & Investigate**. It generates an alert in the L1 Investigation or case in ECM based on the configurations.

   The alert ID or Case ID results are displayed.

Figure 6-10 Scanning Real-time Screening – Individual (Supervisor)

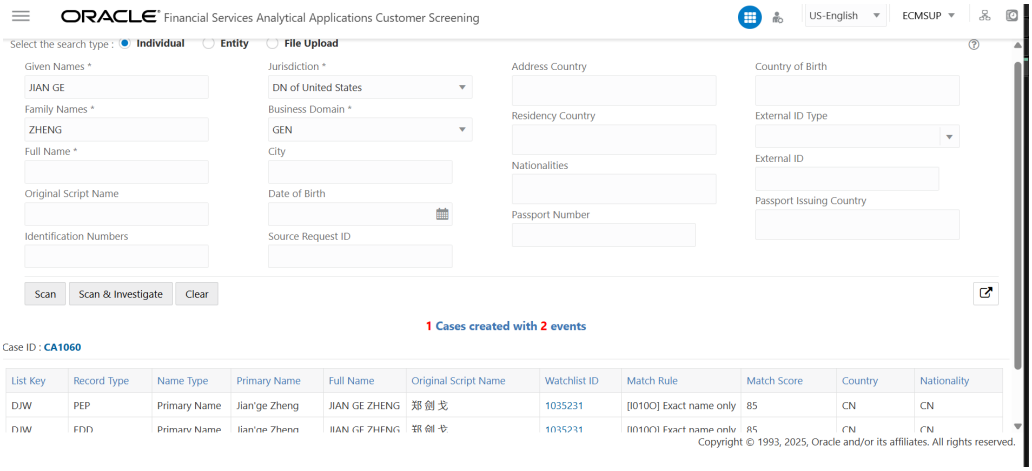


You can define and merge all the different events or record type under the same case type based on the highest priority event type.

To merge different event types or record type in the same case ID, you must access the Atomic Schema and access the **CS_appln_params** table and change the `ECM_MERGE_EVENT_TYPE` parameter value from **N** to **Y**. See Merging Case Types for more information.

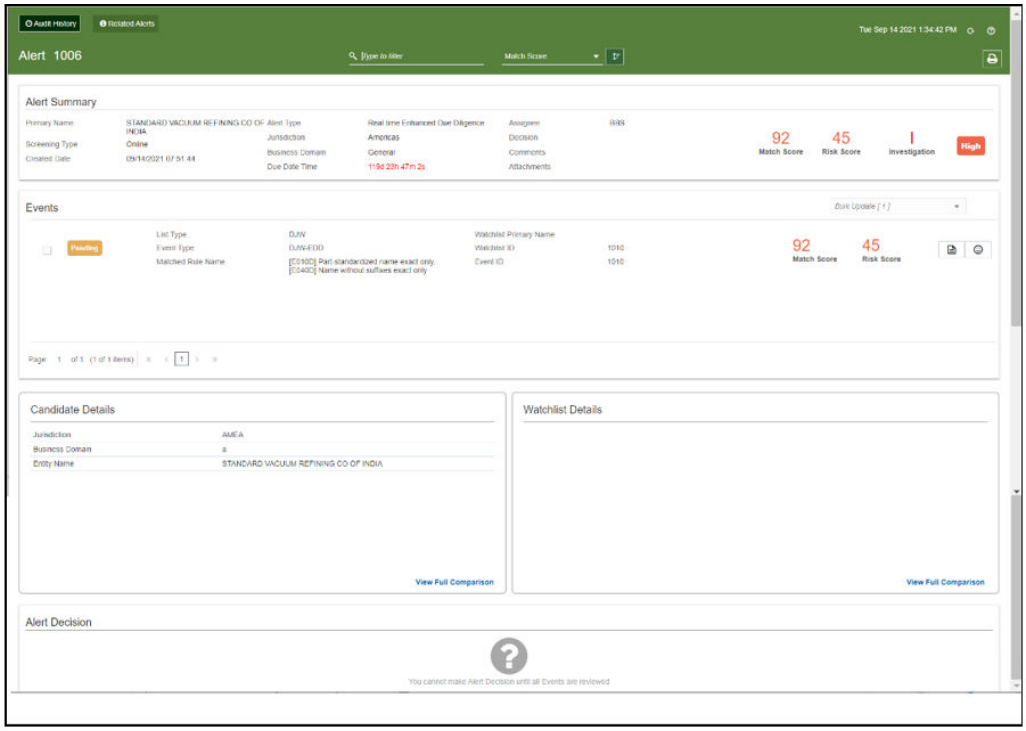
> **Note**
>
> By default, `ECM_MERGE_EVENT_TYPE` parameter value is **N**.

Figure 6-11 Merging Different Event Types in Same Case – Individual (Supervisor)



c. You can view generated alert ID or Case ID in the results and click Alert ID or Case ID to view the Alert Details or Case Details page respectively.

Figure 6-12 Alert Details



8. Click **Clear** to clear the field data and re-enter.

6.2.1.1 Field Descriptions

The Field Descriptions are as follows:

- **Given Name**: Enter the first name of the Individual.
- **Entity Name**: Enter the entity name.
- **Family Name**: Enter the family name of the Individual.
- **Family Name**: Full Name of the Individual for Screening.
- **Jurisdiction**: Select the Jurisdiction to which the Individual or Entity belongs.
- **Business Domain**: Select the business domain to which the Individual or Entity belongs. You can also provide details in the following optional fields:
- **Address Country**: Enter the current address of the Individual or Entity.
- **Country of Birth**: Enter the country code in which the individual was born or the Entity orig- inated. This field is applicable only when you select the search type as Individual.
- **Residency Country**: Enter the country code of residence of the Individual or Entity. This field is applicable only when you select the search type as Individual.
- **Operating Countries**: Enter the country codes the Entity operates in. To add more than one country code, add a comma between the countries. For example, the US, IN. This field is applicable only when you select the search type as Entity.
- **Registration Country**: Enter the country code the Entity is registered in. This field is applica- ble only when you select the search type as Entity.
- **External ID Type**: Select the external ID type of the Individual or Entity.
- **External Type**: Select the external type of Entity.

- **Original Script Name**: Enter the Individual or Entity's name in the original script if the script is a non-Latin script.
- **City**: Enter the city of residence of the Individual or Entity.
- **Nationalities**: Enter the nationality country code of the Individual. This field is applicable only when you select the search type as Individual.
- **External ID**: Enter the external ID unique to the Individual or Entity.
- **Date of Birth**: Enter the Date of birth of the Individual. This field is applicable only when you select the search type as Individual.
- **Passport Number**: Enter the passport number of the Individual.
- **Passport Issuing Country**: Enter the country code in which the passport is issued.
- **Identification Numbers**: Enter the identification numbers of the Individual or Entity.
- **Operating Countries**: Enter the operating country code of the Entity.

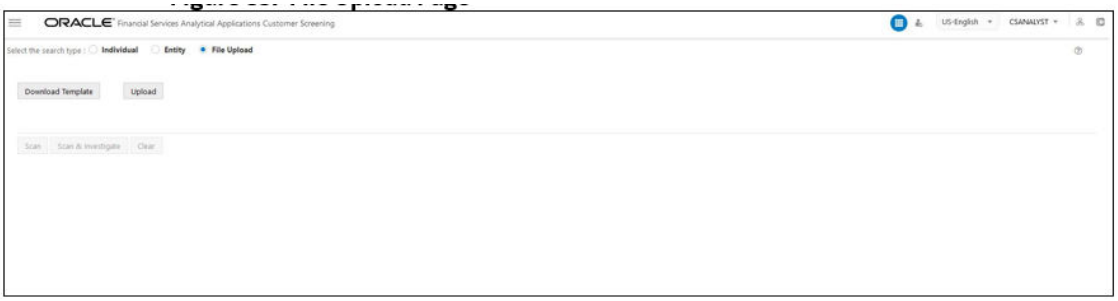
6.2.2 File Upload

File Upload facilitates bulk screening and process Realtime screening data without compromising quality or time. File upload is suitable for institutions that need to review a large number of customers. This allows instant results for multiple searches at once without having to conduct the search one by one. This data search saves time and allows the user to focus on entities that pose the highest risk to the institution.

The results of the screening can be downloaded from the system for internal use. The bulk screening result is very detailed and allows the user to see the results for each customer, including those who do not pose any risk.

For more information on File Upload screening and creating Alert or Case, see file upload section in Oracle Financial Services Customer Screening User Guide.

Figure 6-13 File Upload page



6.2.2.1 Configuring Multi-Thread Count

You can configure the thread count for the Scan or Scan & Investigate operation. A thread is a unit of execution on concurrent programming. Multi-threading is a technique that allows a processor to execute many tasks of one process at the same time.

To Configure the thread count follow the subsequent steps:

1. Access the `cs-realtime.properties` file in the following path:

   ```
   Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/ applications/
   SAN812.ear/SAN812.war/WEB-INF/classes
   ```

2. Change the `rt.excel.upload.multithread.count` value to desired value.

6.2.2.2 Merging an Event

You can define and merge all the different events or record type under the same case type based on the highest priority event type. To merge different event types or record type in the same case ID follow the subsequent steps:

1. Access the Atomic Schema and access the `CS_APPLN_PARAMS` table.
2. Change the `ECM_MERGE_EVENT_TYPE` parameter value from **N** to **Y**. By default, `ECM_MERGE_EVENT_TYPE` parameter value is **N**. See Merging Case Types for more information.

6.2.2.3 Configuring Response Count in the Results

The candidate response count limit to display the request result section in the UI is configurable.

To configure the response display limit follow the subsequent steps:

1. Access the Atomic Schema and access the `CS_APPLN_PARAMS` table.
2. Change the parameter value for the `MAX_REQ_DISPLAY_NO` parameter to the required value.

   The following images show the File Upload response result for Scan & Investigate with response count limit configured as 20 and more than 20, respectively.

Figure 6-14 Scan Response for Less than 20 Request

Figure 6-15 Scan Response for More than 20 Request

6.3 Running the Real-Time Screening Job

To source the data from the Financial Crime Data Model (FCDM) and run the FCDM data preparation process, disable the **MAIN_RT** real-time screening job phase and enable the FCDM job phases in the `customer screening-real time.properties` and `external-entity-screening.properties` run profiles. These files are available in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory in the WinSCP server. `phase.Start\ Real-time\ Screening.enabled = Y #`

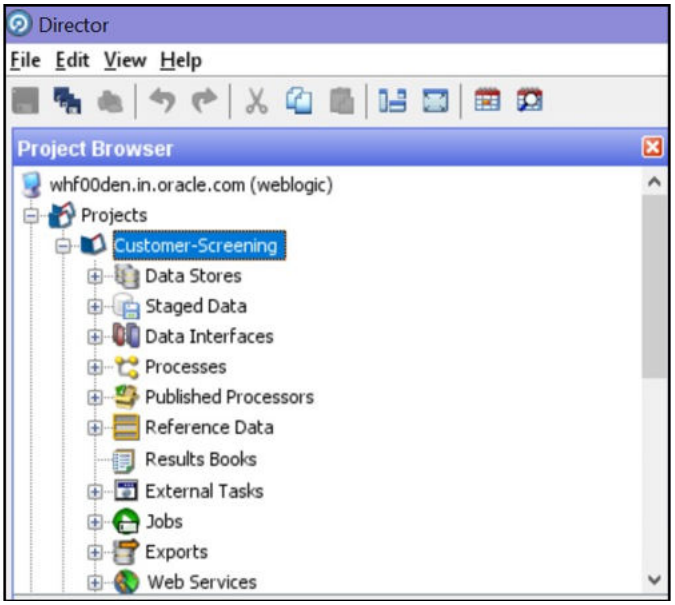
```
Control single real-time screening types

phase.Real-time\ Screening.process.Individual\ Real-time\ Screening.san_enabled = Y

phase.Real-time\ Screening.process.Individual\ Real-time\ Screening.pep_enabled = Y

phase.Real-time\ Screening.process.Individual\ Real-time\ Screening.edd_enabled = Y

phase.Real-time\ Screening.process.Entity\ Real-time\ Screening.san_enabled = Y

phase.Real-time\ Screening.process.Entity\ Real-time\ Screening.pep_enabled = Y

phase.Real-time\ Screening.process.Entity\ Real-time\ Screening.edd_enabled = Y
```

6.4 Adding a New Field in a Webservice

Currently, you can only search for the ready-to-use web service fields in the Real-time screening user interface. If you want to add a custom field to an existing web service, for example, full name, you must enter the field name in the applicable web service node and add the field to the applicable process. To do this, follow these steps:

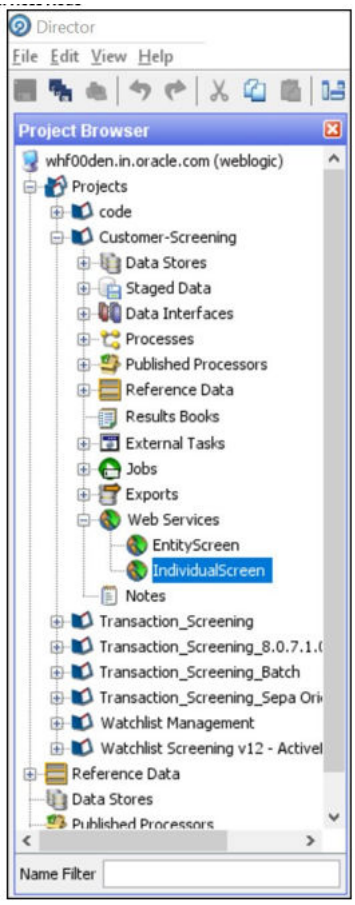
1. In the **Director** Landing page, expand the **Customer-Screening** project in the **Project Browser** pane.

Figure 6-16 Project Browser pane



2. Expand the **Web Services** node and double-click the **IndividualScreen** web service.

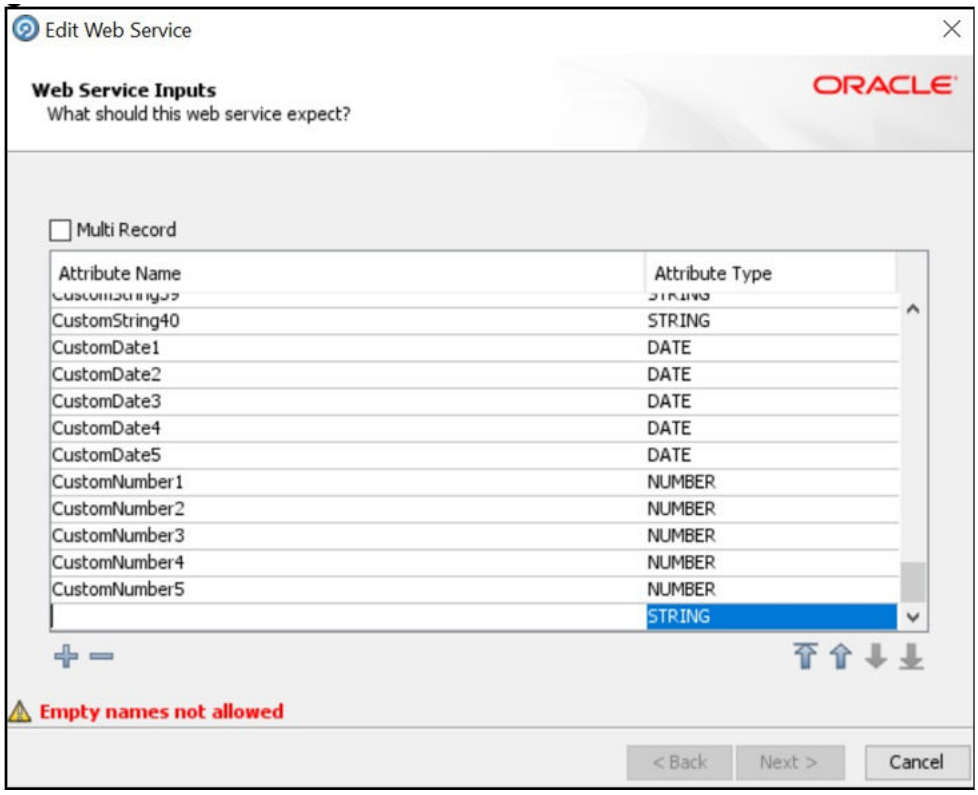
Figure 6-17 Web Services Node



3. Click the **Plus** icon in the **Web Service Inputs** window.

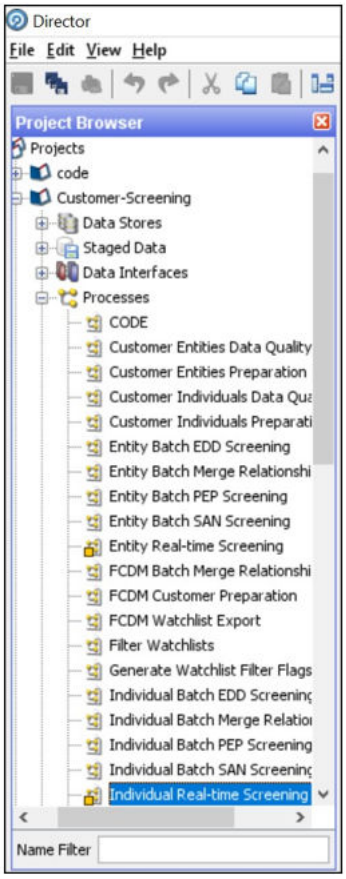
A new row is displayed in the table.

Figure 6-18 Edit Web Service window



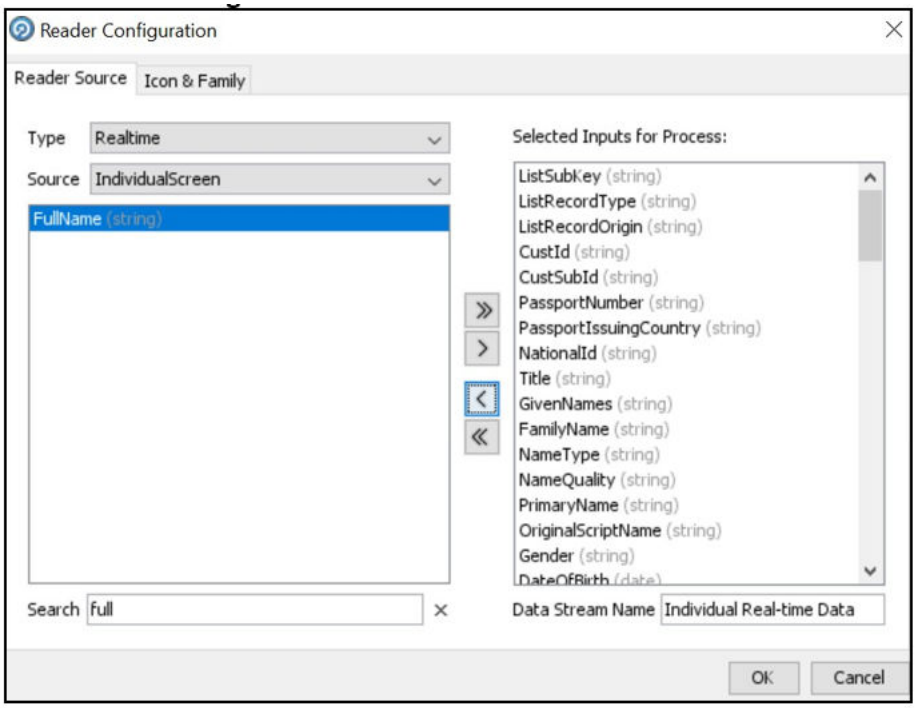
4. Enter the name of the column, for example, **FullName**, and click anywhere inside the table to enable the **Next** button.
5. Click **Next** until you view the Finish button, and click **Finish**.
6. In the **Customer-Screening** project, expand the **Processes** node and double-click the **Individual Real time Screening** process.

Figure 6-19 Processes Node



7. Click the **Individual Real-time Data** process icon in the **Individual Real-time Screening** window.
8. Search for **FullName** in the **Reader Configuration** window.

Figure 6-20 Reader Configuration window



9. Select **FullName** and select the **Remove** icon to move it to **Selected Inputs for Process**.
10. Click **OK**.

    After you add the new field, you must integrate it with the Real-time screening user interface to display it in the user interface. To do this, follow these steps:

    a. Open the RTScreening.html file from the `<Installed Sanctions Path>/js/views` directory. For example, ECM808SAN.war path }/realTimeScreening/js/views. For example, `ECM808SAN.war path }/realTimeScreening/js/views`.

    b. Add a new Entry similar to externalID and Change the external ID placeholders to FullName:
    ```
    <oj-label for =”text-input”>fullName</oj-label>

    <oj-input-text id=”fullName” value=”{{FullName}}”></oj-input-text>
    ```

    c. Copy the code with the new value.

    d. Open the RTScreening.js file from the `<Installed Sanctions Path>/js/viewModels` directory. For example, `ECM808SAN.war path }/realTimeScreening/js/viewModels`.

    e. Update the placeholder within `‘’` with the copied code with the same syntax as given in the id in the html file in the `self.Clear` function:
    ```
    Document.getElementById(“FullName”).value = ‘’;
    ```

    f. Update the placeholder within ‘’ with the copied code with the same syntax as given in the id in the html file in the `self.Clear` function:
    ```
    Document.getElementById(“FullName”).value = ‘’;
    ```

    g. Update the placeholder within “” with the copied code with the same syntax as given in the id in the html file in the `self. IndividualScreenObject` array `FullName:””`

h. In ViewModel(), Add a new entry similar to externalID and update externalId placeholder with the FullName. For example, self. fullname = `ko.observable(CSRTMessageConstants.CS_RT_FULL_NAME);)`

i. In self.clearAll, Add a new entry similar to externalId and update the externalID placeholder with the FullName. For example, `document.getElementById("fullName").value = ''`

j. In individualidtolabelmap, Add a new entry similar to externalId and updated externalId placeholder with the FullName. For example `"FullName": { "label" : self.fullName() },`

k. Add an entry for the fullName in the var `IndividualArrayCols`. For example,

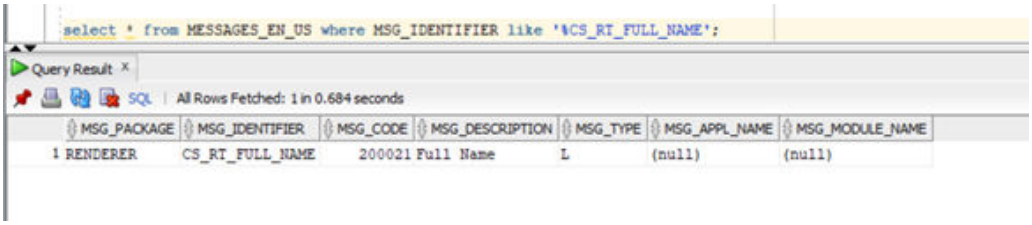
```
[{
"headerText": self.fullname(),
"field": "ListFullName",
"style": "width:11%",
"headerClassName": "oj-sm-only-hide tableHeader",
"className": "oj-sm-only-hide"
},
```

l. Open `CSRTMessageConstants.jsp` file from the `/js/views` directory. For example, `ECM808SAN.war path }/realTimeScreening`.
Add an entry similar to externalId and update. For example,

```
CSRTMessageConstants.CS_RT_FULL_NAME="<%=MessageFramework.getMessageFrom
 LocaleSpeficCache("RENDERER.CS_RT_FULL_NAME",
currentMsgLocale.toString())%>";
```

m. Add an entry in MESSAGES_EN_US table for the selected field name as below. For example,

Figure 6-21 MESSAGES_EN_U



7

Batch Screening

The following diagram describes the data movement from Customer Screening to Enterprise Case Management (ECM) during the batch screening process.

Figure 7-1 Batch Screening Workflow

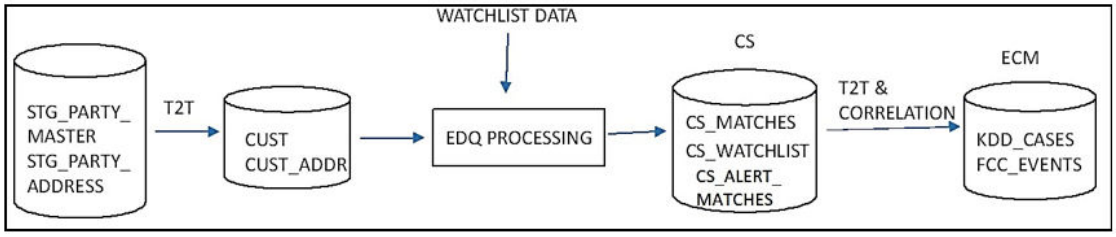
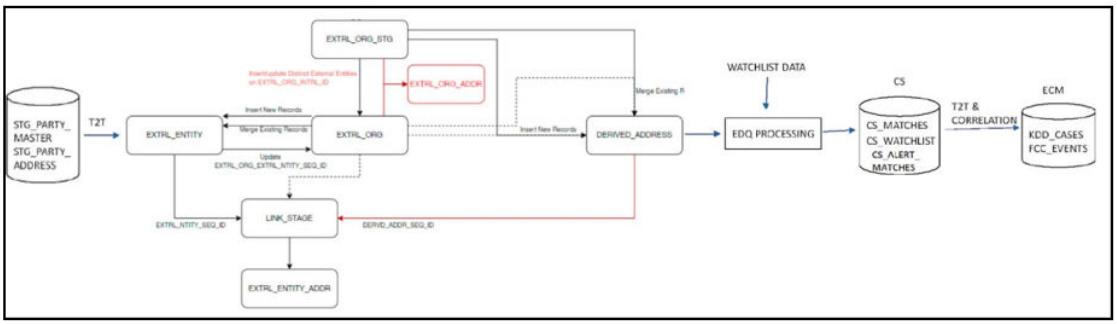


Figure 7-2 Batch Screening Workflow with EXTRNL_ORG table



The data movement in the workflow is as follows:

1. Data is moved from the `STG_PARTY_MASTER`, `STG_PARTY_ADDRESS`, `STG_CASA`, `STG_LOAN_CONTRACTS`, `STG_PARTY_ACCOUNT_ROLE_MAP`, `STG_PARTY_ROLE_MAP`, `STG_TD_CONTRACTS`, `STG_TRADING_ACCOUNT`, and `STG_PARTY_OTHER_NAMES` tables to the `CUST`, `CUST_ADDR`, `ACCT`, `CUST_NAME` and other associated customer tables using the Table-to- Table (T2T) mode.
   Data is moved from the `STG_PARTY_MASTER`, `STG_PARTY_ADDRESS`, `STG_CASA`, `STG_LOAN_CONTRACTS`, `STG_PARTY_ACCOUNT_ROLE_MAP`, `STG_PARTY_ROLE_MAP`, `STG_TD_CONTRACTS`, `STG_TRADING_ACCOUNT`, and `STG_PARTY_OTHER_NAMES` tables to the `EXTRL_ENTITY`, `EXTRL_ORG`, `EXTRL_ORG_STG`, `EXTRL_ORG_ADDR`, `LINK_STAGE`, `EXTRL_ENTITY_ADDR`, `DERIVED_ADDRESS`, `ACCT`, `CUST_NAME` and other associated customer tables using the Table-to-Table (T2T) mode. See batch screening workflow with `EXTRNL_ORG` table.
2. The watch list data is downloaded from the `watch list-management` project in EDQ. The watch list data is matched with the data in the `CUST` and `CUST_ADDR` tables in the `Customer-Screening` project.

3. The matches are loaded into the CS_MATCHES table and the corresponding watch list data is loaded into the CS_WATCHLIST table.
4. Data from the CS_MATCHES_HIST table is generated as alerts in the CS_ALERTS and CS_ALERTS_MATCHES tables.

> **Note**
>
> a. The CS_MATCHES_HIST table contains all the matches made. Each time screening is run, the CS_MATCHES table is compared to the CS_MATCHES_HIST table and any new or updated matches are added to the CS_MATCHES_HIST table. This creates a new alert.
>
> b. Every time you run the Customer-Screening project, data is cleared from the CS_MATCHES table.

5. Data is correlated and loaded into the KDD_CASES and FCC_EVENTS tables in ECM.

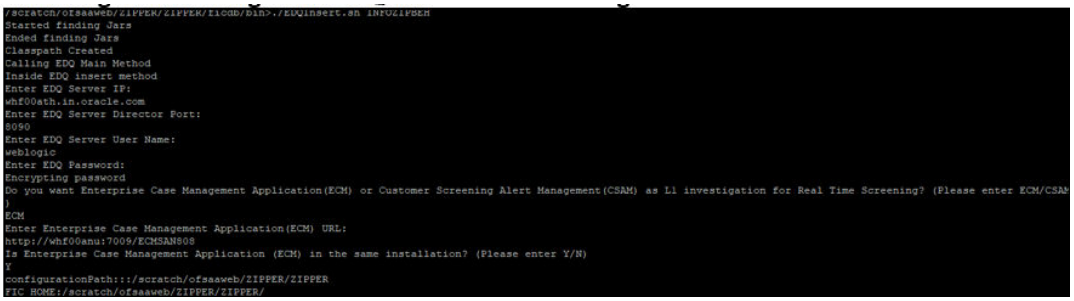
7.1 Configuring the EDQ URL

To configure the EDQ URL for batch screening, follow these steps:

1. Navigate to the FCI_DB_HOME/bin directory.
2. Execute the command /EDQInsert.sh <INFODOM NAME>.

   This step is used to register the EDQ server details. You must replace the INFODOM NAME placeholder with your domain name.
3. Enter the following details in the console where the command is run:
   - **EDQ Server IP:** An example of the EDQ URL is http://whf00bte.in.oracle.com:7008/ edq. Replace this with your EDQ server's URL.
   - **EDQ Server Direct Port Number:** This is the JMX port number. This value must be 8090.
   - **EDQ Server User Name:** An example of the EDQ server user name is weblogic. Replace this with your EDQ server's user name.
   - **EDQ Password:** An example of the EDQ password is weblogic1. Replace this with your EDQ server's password.

Figure 7-3 Configure the EDQ URL in Batch Screening



4. Configure the EDQ URL in the CONFIG schema. To do this, run the following script and replace the placeholders in the v_method_name and v_param_1 columns with the EDQ URL, EDQ user name, and EDQ password, respectively:

```
select t.*,t.rowid from aai_wf_application_api_b t where t.v_process_id='CSRT'
and t.v_app_api_id in ('1521535704140','1521535760435')
```

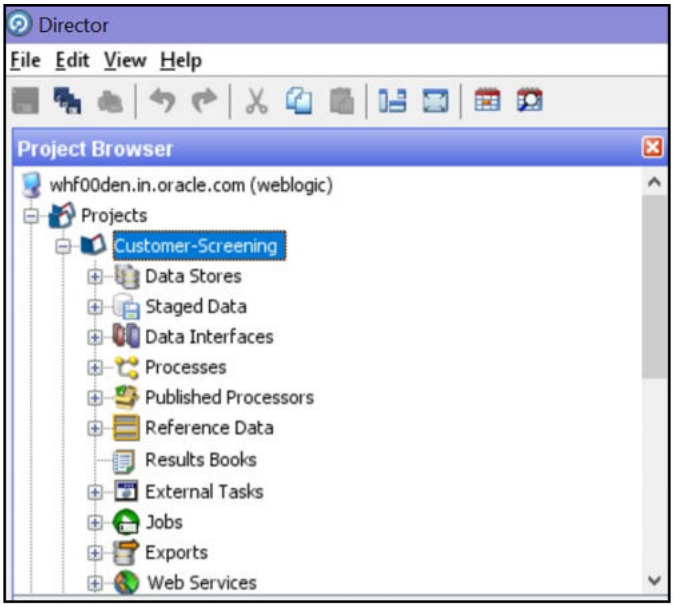
7.2 Staging Database Connection Details

To run the customer screening jobs using the Financial Crime Data Model (FCDM) as a source of customer and external entity data, you must add the connection details of the staging database into which FCDM will place the data to be screened in EDQ.

To set the connection details for customer and external entity data, follow these steps:

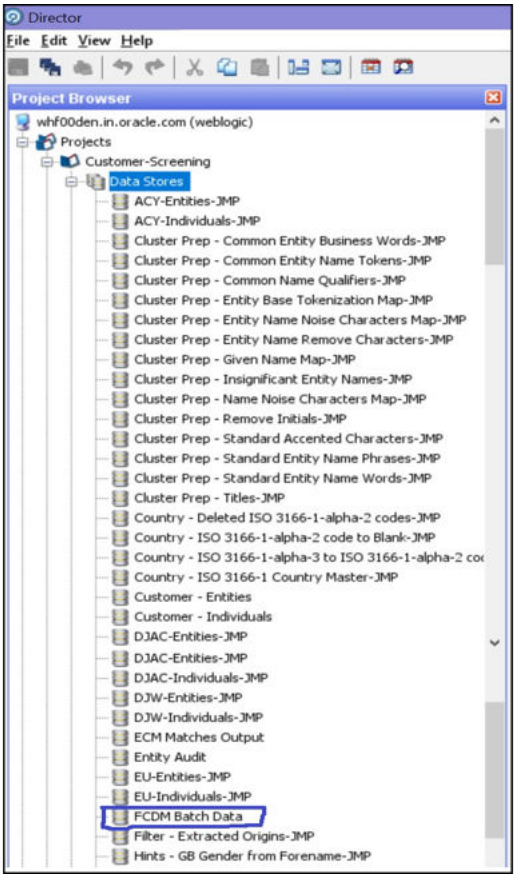
1. Go to the EDQ URL and open the **Director** menu.
2. In the **Director** Landing page, expand the **Customer-Screening** project in the **Project Browser** pane.

Figure 7-4 Project Browser pane



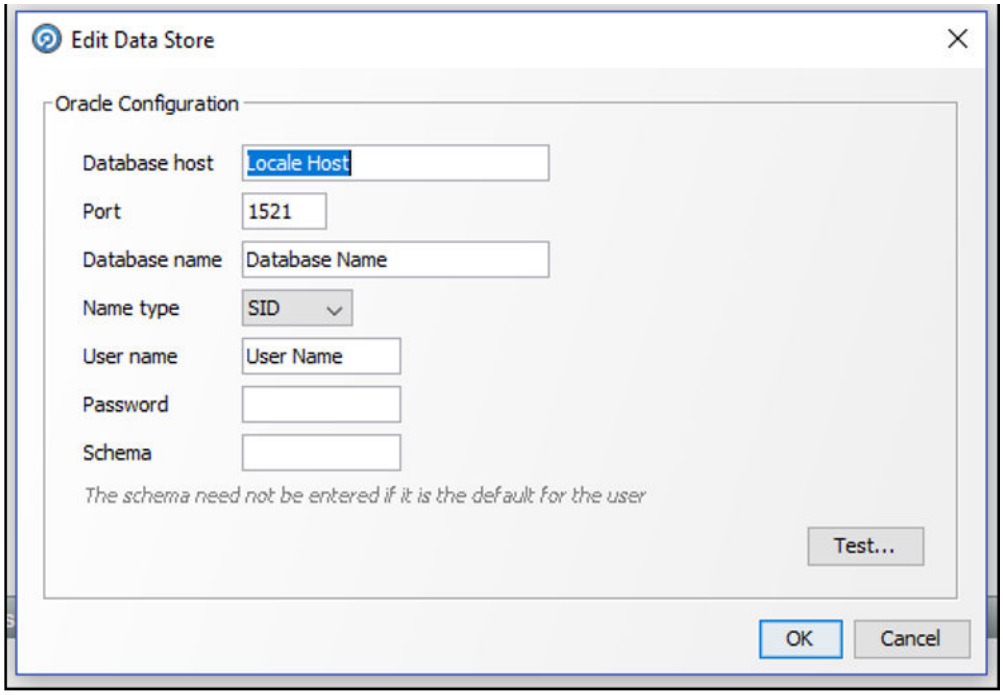
3. Expand the **Data Stores** node and open **FCDM Batch Data**. The **Edit Data Store** window appears.

Figure 7-5 Data Stores Node



4. In the **Edit Data Store** window, enter the database host, database name, user name, and password.

Figure 7-6 Edit Data Store for Staging Database Connection



Note

a. OEDQ release 12c has a base config folder and a local config folder. The base config folder is called `oedqhome` and the local config folder is called `oedqlocalhome`. The names may differ in some cases. For example, dots or underscores may be inserted in the names, such as `oedq_local_home`.

b. It is not necessary to enter the schema name if the user name mentioned is the schema owner.

c. The parameters can be passed as externalized values in the `runopsjob` command.

7.3 Enabling Customer and External Entity Tables

The FCDM Integration section of the `customer-screening.properties` and `external.entity.properties` run profile contains the following parameters. These files are available in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory in the WinSCP server.

- `phase.Batch\ Screening\ FCDM.enabled`
- `phase.Snapshot\ External\ Entity\ Data.enabled`

To enable screening of the customer table, set `phase.Batch\ Screening\ FCDM.enabled` to **Y** and `phase.Snapshot\ External\ Entity\ Data.enabled` to **N**.

To enable screening of the external entity table, set `phase.Batch\ Screening\ FCDM`.enabled to **N** and `phase.Snapshot\ External\ Entity\ Data.enabled` to **Y**.

7.4 Data Preparation in FCDM

Before you prepare data for individuals and entities, there is an FCDM-specific data preparation process which needs to be performed. This process performs the following transformations:

- Splits records into individuals and entities based on Customer Type Code
- Creates additional rows of data for aliases
- Creates name attributes compatible with CDI
- Derives gender and year of birth for individuals

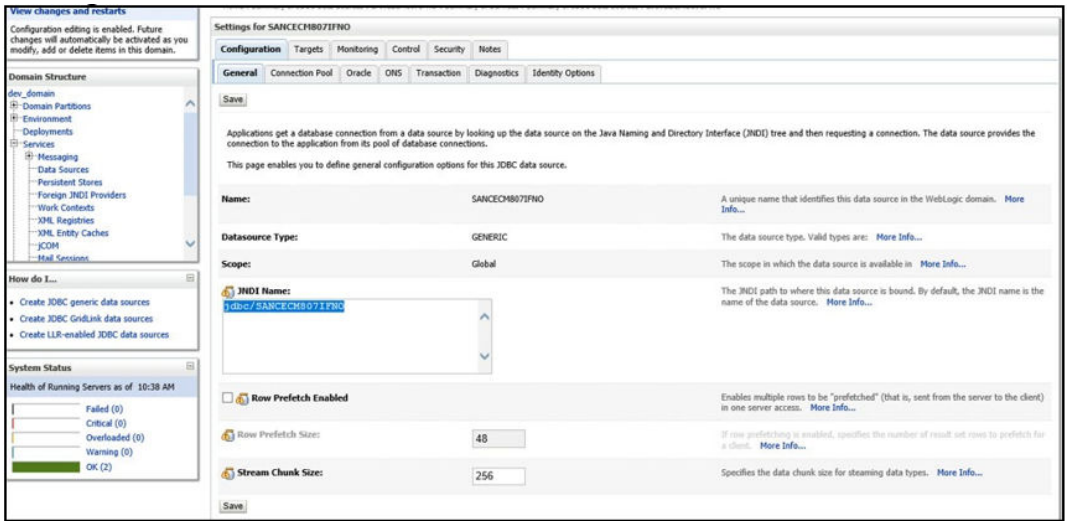
> **Note**
>
> The FCDM Data Preparation job is built on expected population of data in FCDM. This must be validated for each specific implementation and the process adapted if required.

7.4.1 Establishing a JDBC Database Connection using WebLogic

To set up a database connection using the WebLogic server, follow these steps:

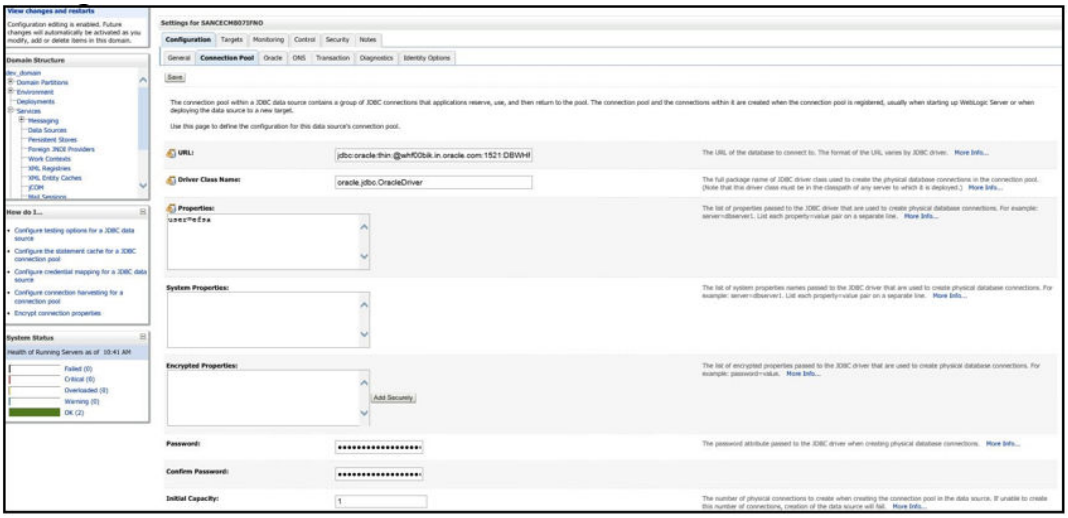
1. In the WebLogic server, provide the name of the JNDI directory in the **JNDI Name** field in the **General** subtab of the **Configurations** tab.

Figure 7-7 JNDI Name



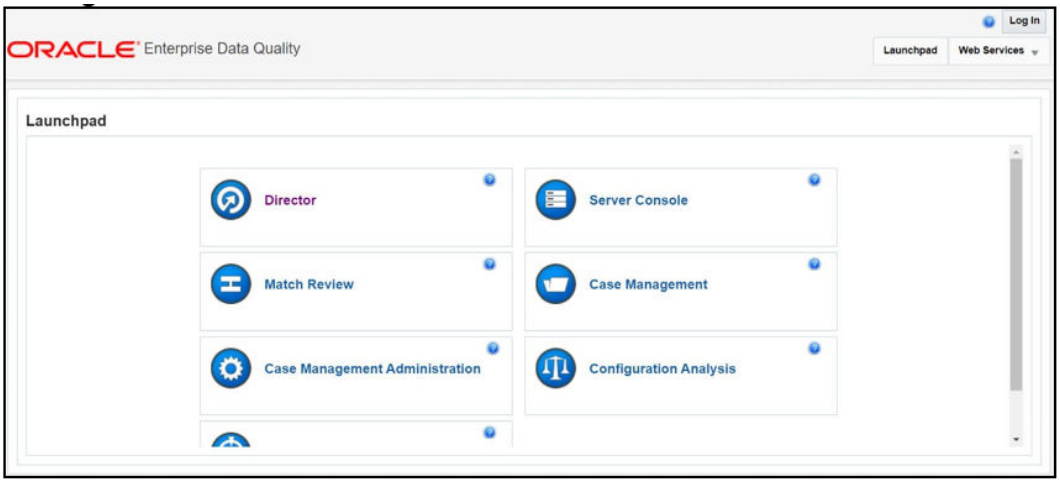
2. In the **Connection Pool** subtab, provide the connection details of the JDBC URL. Enter the JDBC URL in the **URL** field and the class name of the JDBC driver in the **Driver Class Name** field.

Figure 7-8 JDBC URL and Driver



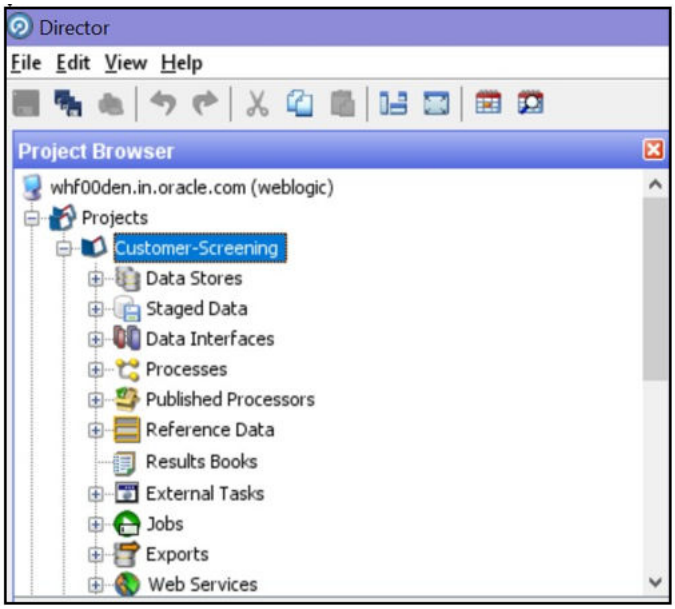
3. Go to the EDQ URL and open the **Director** menu. The **Director** Landing page appears.

Figure 7-9 Director Menu in EDQ



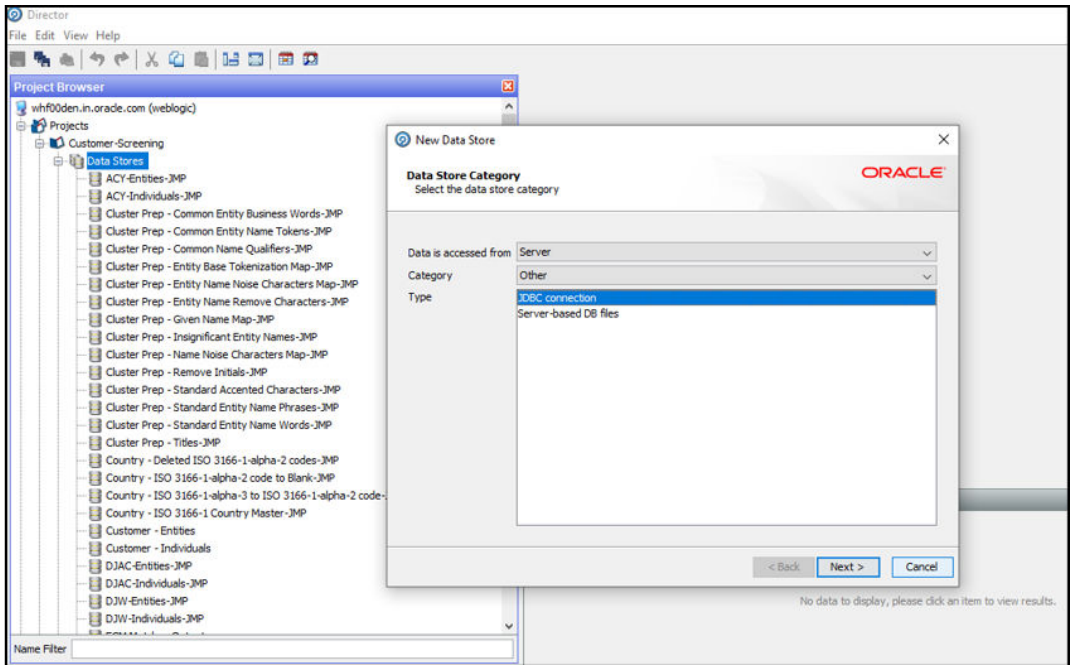
4. In the **Director** Landing page, expand the **Customer-Screening** project in the **Project Browser** pane.

Figure 7-10 Project Browser pane



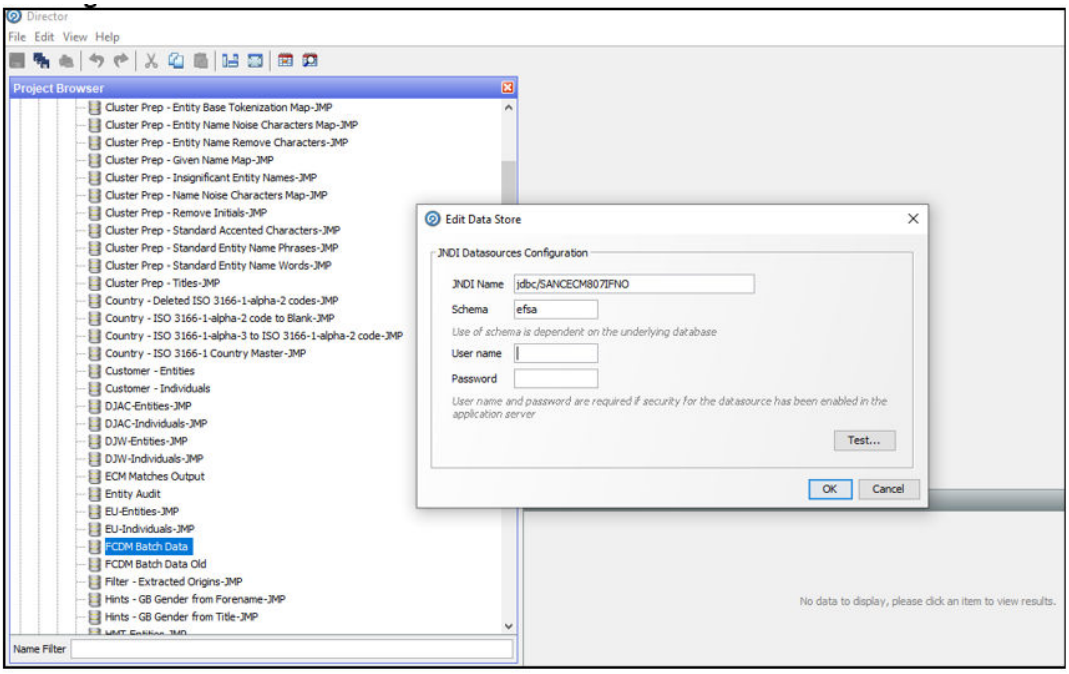
5. In the **Project Browser** pane, right-click **Data Stores** under the Customer-Screening project and then select **New Data Store**.

Figure 7-11 New Data Store



6. In the **New Data Store** window, select the type as **JDBC Connection** and click **Next**.

Figure 7-12 Edit Data Store



7. In the **Edit Data Store** window, enter the JDBC connection details.
8. Click **OK**.

   You have now created a JDBC database connection.

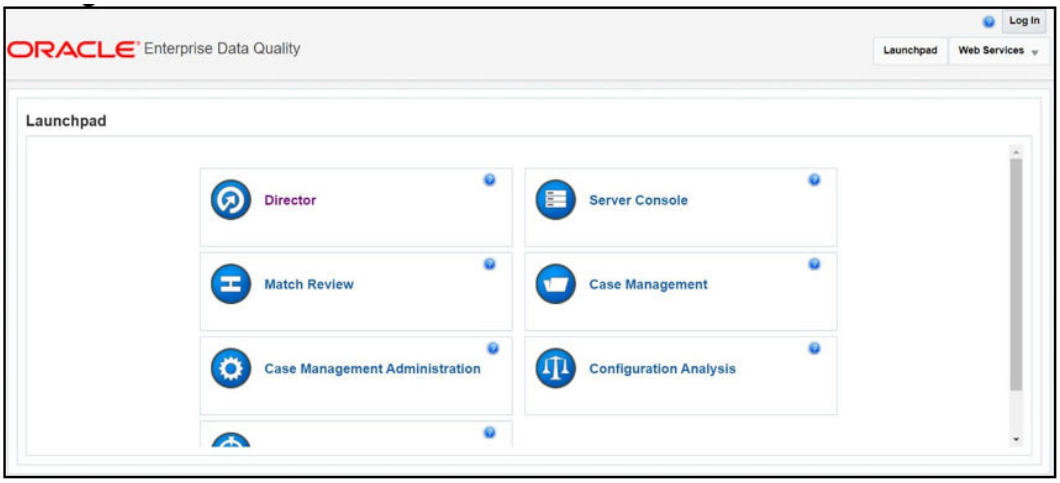
7.5 Analyzing the Data Quality of Customer Data and External Entity

Customer Screening is integrated with a Data Quality (DQ) check process which checks the quality of data in FCDM for screening. This process is run independently of the screening process and identifies potential issues with the customer and external entity data quality that can affect the screening efficiency. Run the Analyze FCDM Customer Data Quality job to analyze the data quality. This job checks data for any quality issues that can affect the screening efficiency.

To analyze the customer data, follow these steps:

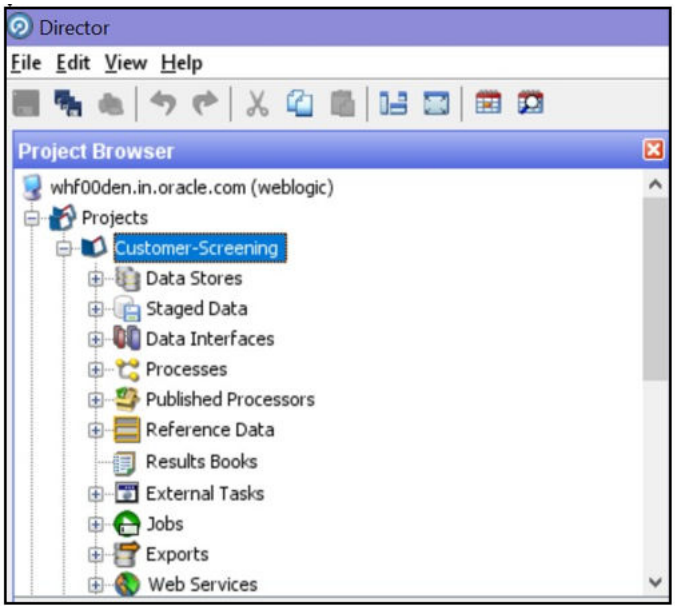
1. Ensure that data is loaded into FCDM and the **Customer-Screening** project has the correct database parameters.
2. Go to the EDQ URL and open the **Director** menu.

Figure 7-13 Director menu in EDQ



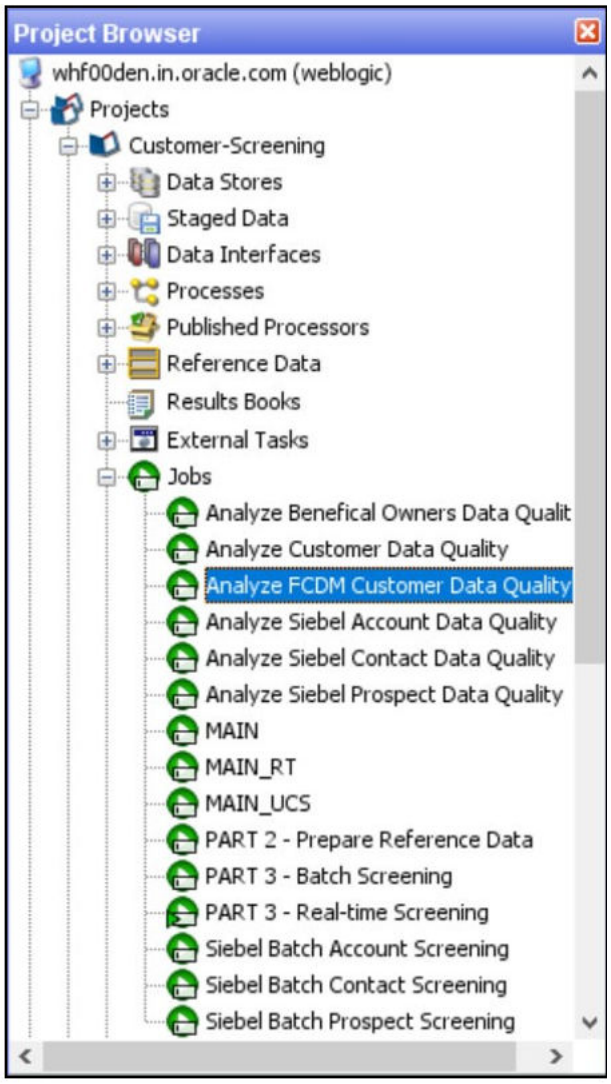
3. In the **Director** Landing page, expand the **Customer-Screening** project in the **Project Browser** pane.

Figure 7-14 Project Browser pane



4. Expand the **Jobs** node.
5. Right-click the `Analyze FCDM Customer Data Quality` job and click **Run**.

Figure 7-15 Jobs Node

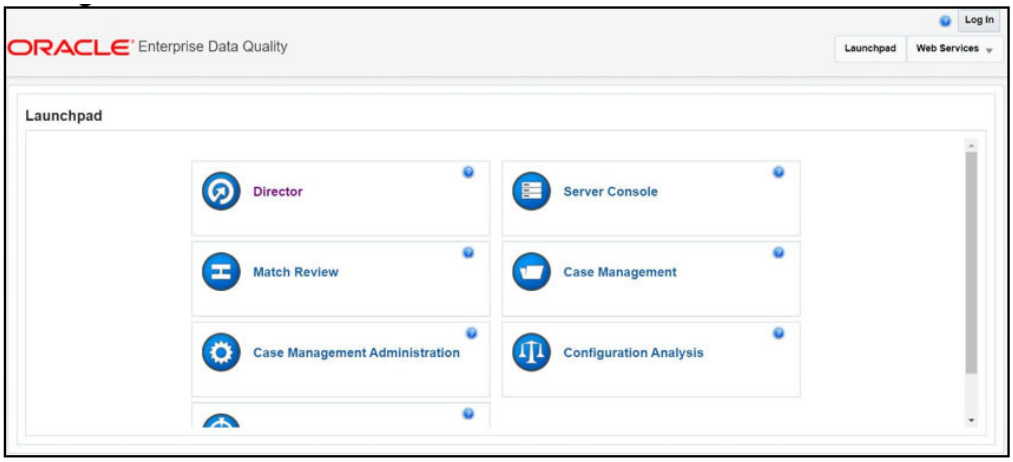


To analyze the external entity data, follow these steps:

a. Ensure that data is loaded into FCDM and the **Watch list Management** project has the correct database parameters.

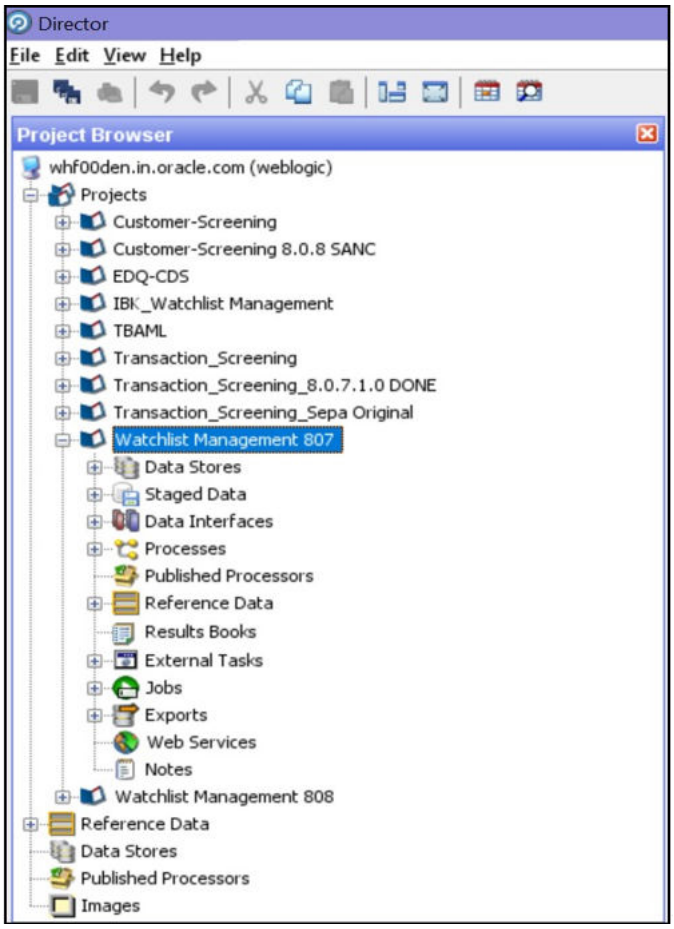
b. Go to the EDQ URL and open the **Director** menu.

Figure 7-16 Director Menu in EDQ



c. In the **Director** Landing page, expand the **Watch list Management** project in the **Project Browser** pane.

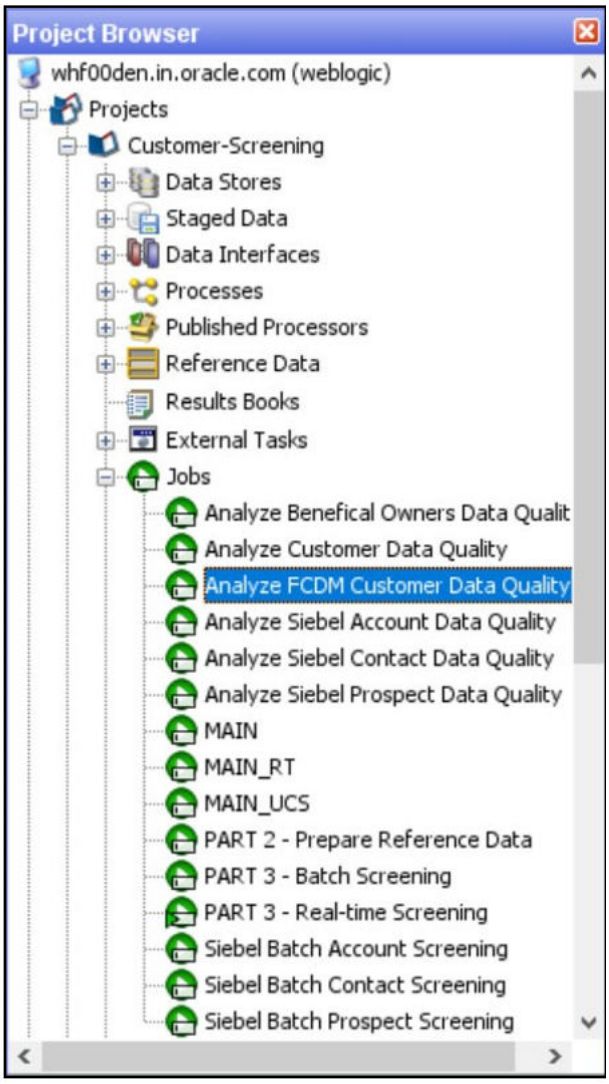
Figure 7-17 Project Browser pane



d. Expand the **Jobs** node.

e. Right-click the `Analyze FCDM Customer Data Quality` job and click **Run**.

Figure 7-18 Jobs Node



7.5.1 Data Quality Errors

For each Data Quality (DQ) error, a severity code is assigned, and it corresponds to the likely impact the issue will have on screening efficiency. The error codes and the associated messages that are displayed are based on the data analysis are shown in the following table:

Table 7-1 Severity Codes Assigned to Data Quality Errors

Severity Code	DataQuality Error
1	Severedata error which prevents screening.
2	Invaliddata which will limit the effectiveness of screening.
3	Missingdata which will limit the effectiveness of screening.

Table 7-1 (Cont.) Severity Codes Assigned to Data Quality Errors

Severity Code	DataQuality Error
4	Invalid data which does not affect screening. Errors in this categorywill not affect the output of the match processor but can cause issues when manually evaluating any potential matches that are raised.

The data quality check analyzes each row of data. If the analysis of any row results in a severity code of 1, it is rejected by the screening process. This is because there is a lack of data in the core attributes used by the screening process, and so screening cannot be performed.

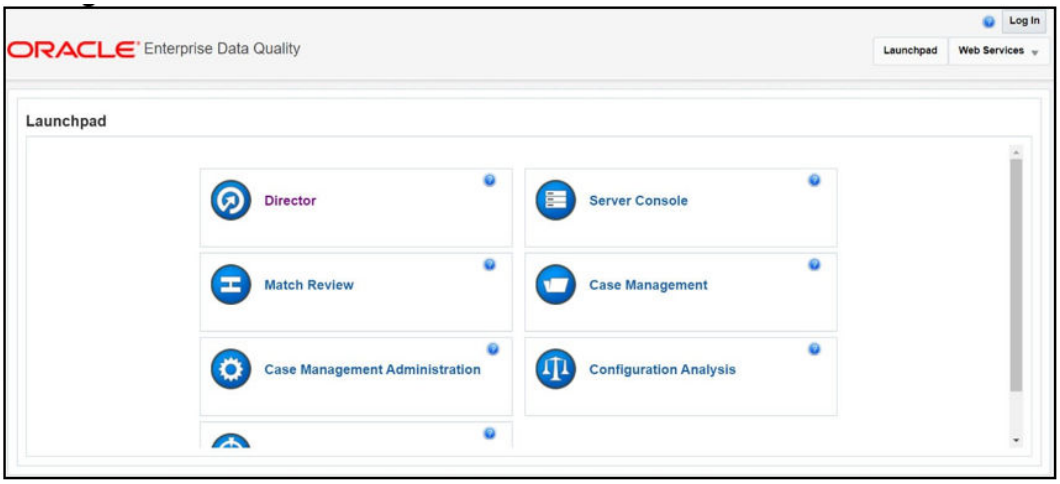
The screening processes load data that cannot be screened into the `CUST_Individuals_Invalid staged data` or the `CUST_Entities_Invalid staged data` tables for the individual and external entity records, respectively. The error codes associated with each row are also stored in the database.

7.6 Extract Transform Load (ETL) Database Connection Details

After screening is run, relationships (matches) and watch list records are exported to the Customer Screening database, and this data is sent to ECM based on the connections configured in the data store. To set the ETL database connection details, follow these steps

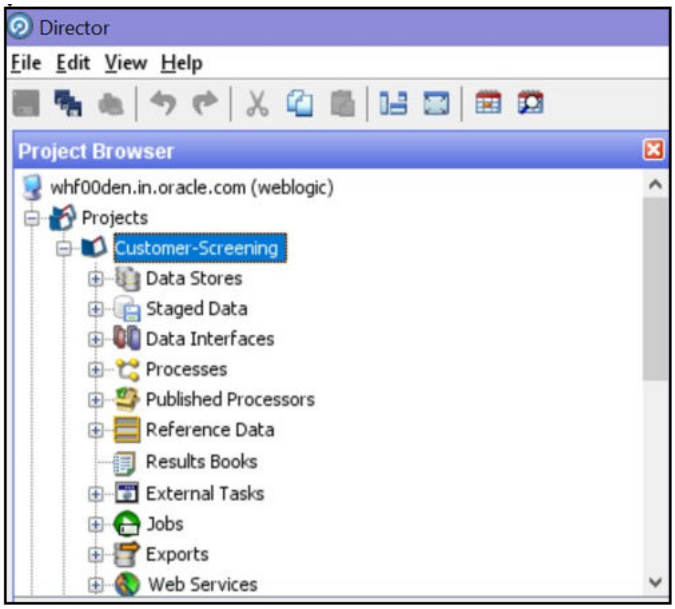
1. Go to the EDQ URL and open the **Director** menu.

Figure 7-19 Director menu in EDQ



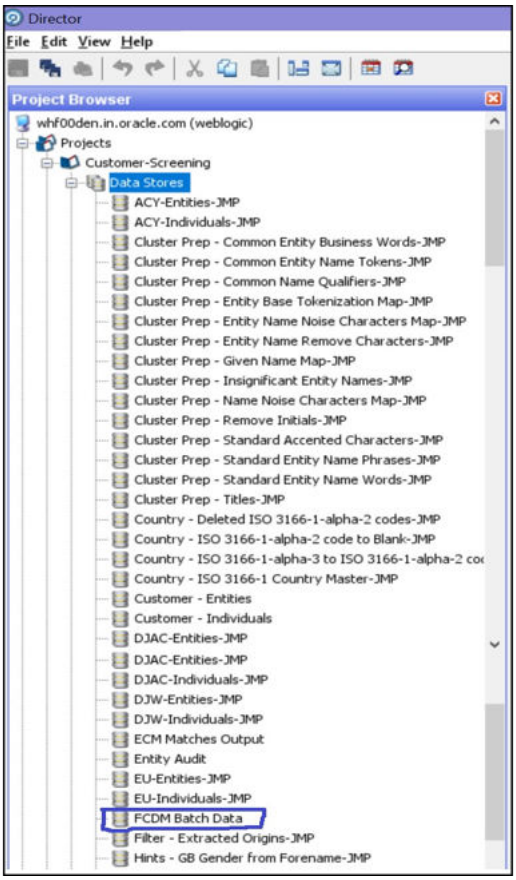
2. In the **Director** Landing page, expand the **Customer-Screening** project in the **Project Browser** pane.

Figure 7-20 Project Browser pane



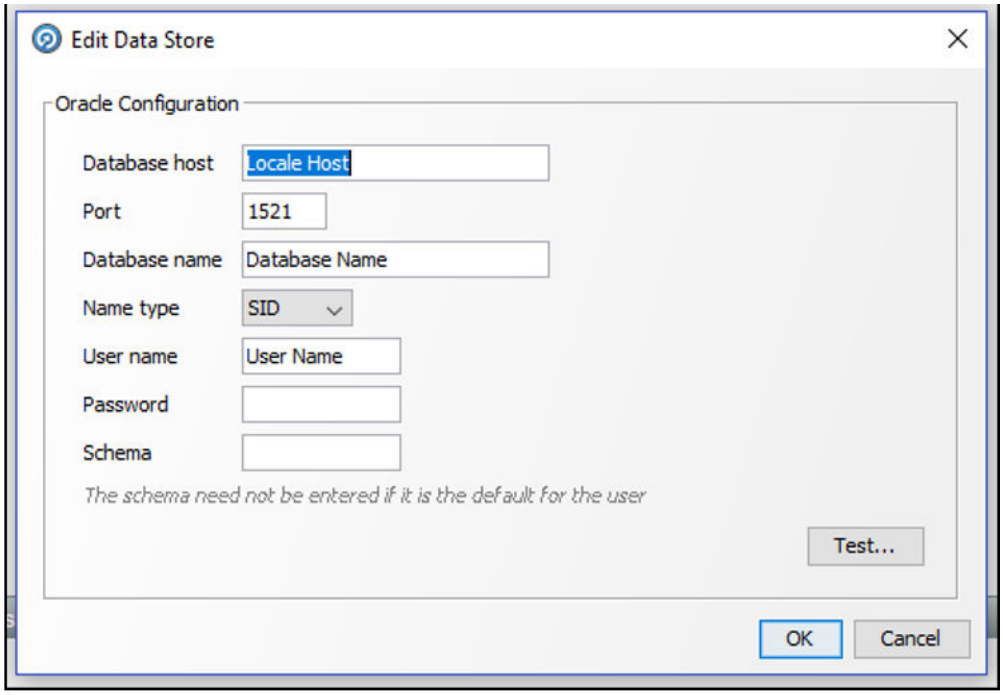
3. Expand the **Data Stores** node and open **FCDM Batch Data**. The **Edit Data Store** window appears.

Figure 7-21 Data Stores Node



4. In the **Edit Data Store** window, enter the database host, database name, user name, and password.

Figure 7-22 Edit Data Store for Staging Database Connection



> **Note**
>
> a. OEDQ release 12c has a base config folder and a local config folder. The base config folder is called `oedqhome` and the local config folder is called `oedqlocalhome`. The names may differ in some cases. For example, dots or underscores may be inserted in the names, such as `oedq_local_home`.
>
> b. It is not necessary to enter the schema name if the user name mentioned is the schema owner.
>
> c. The parameters can be passed as externalized values in the `runopsjob` command.

7.7 Running the Batch Screening Job

To source the data from the Financial Crime Data Model (FCDM) and run the FCDM data preparation process, disable the **MAIN** batch screening job phase and enable the FCDM version in the `customer screening.properties` and `external-entity-screening.properties` run profiles:

```
# Globally turns on/off batch screening types phase.Batch\ Screening.enabled = N
phase.Batch\ Screening\ FCDM.enabled = Y
```

To export the data to the Customer Screening database these job phases must also be enabled:

```
phase.ECM\ Export\ Matches.enabled = Y

phase.ECM\ Export\ Watch list.enabled = Y
```

7.8 Generating Alerts

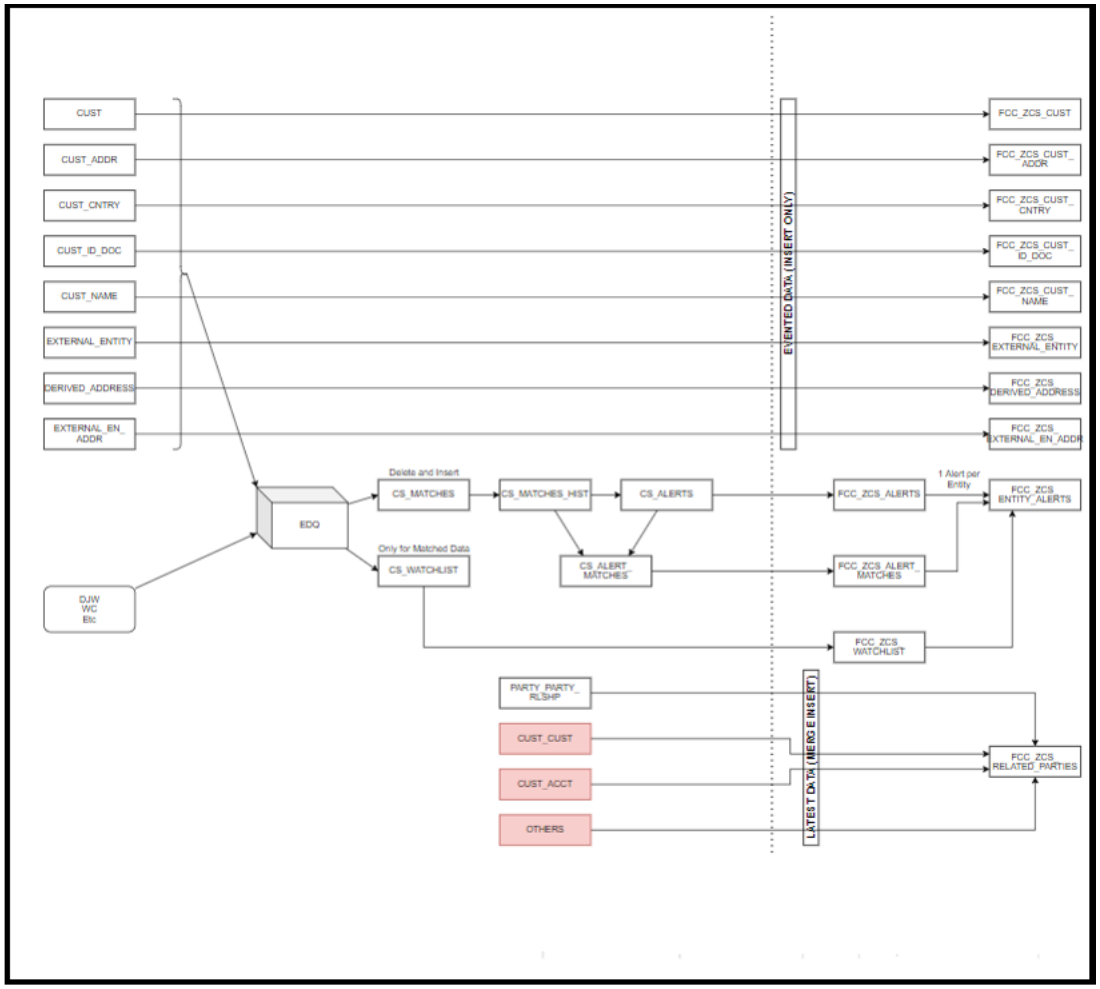
This job will move the alerts data displayed in the L1 Investigation for Alert Management from different origins in the source database to the consolidated database.

The Customer and Watchlist data will be screened in Enterprise Date Quality (EDQ) server. If any Customer data is matched with Watchlist Data, then the events are created. Based on the Customer, the alerts are generated.

If any customer data is changed in source data, only that data is moved in the consolidated database. Based upon the date, you run the batch.

The following workflow explains the data movement from the source database to the consolidated database.

Figure 7-23 Generating Alerts Workflow

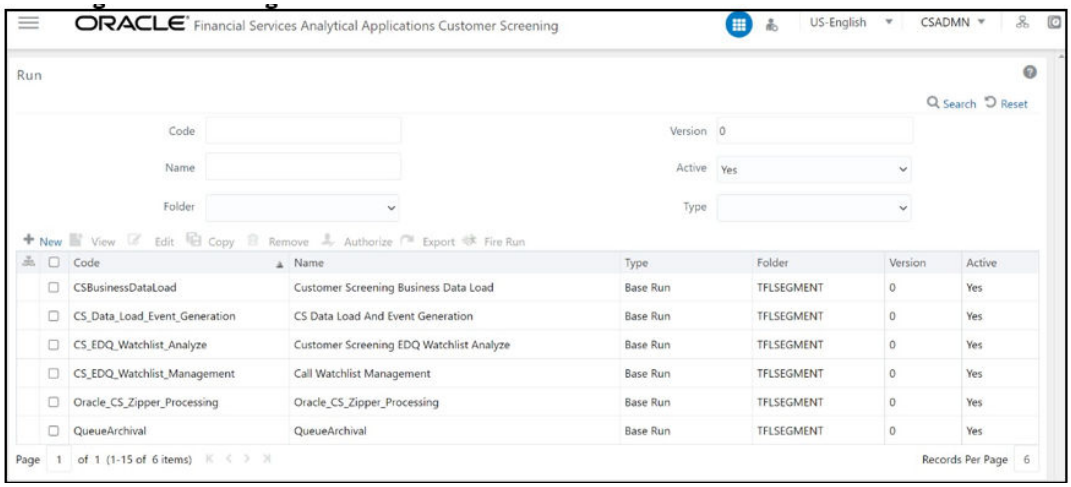


To run the batch to move data from the source database to the consolidated database, follow these steps:

1. Log in to the Customer Screening application.
2. Click **Common Tasks** list of common tasks displayed. Then click **Rule Run Framework**, and then click **Run**.

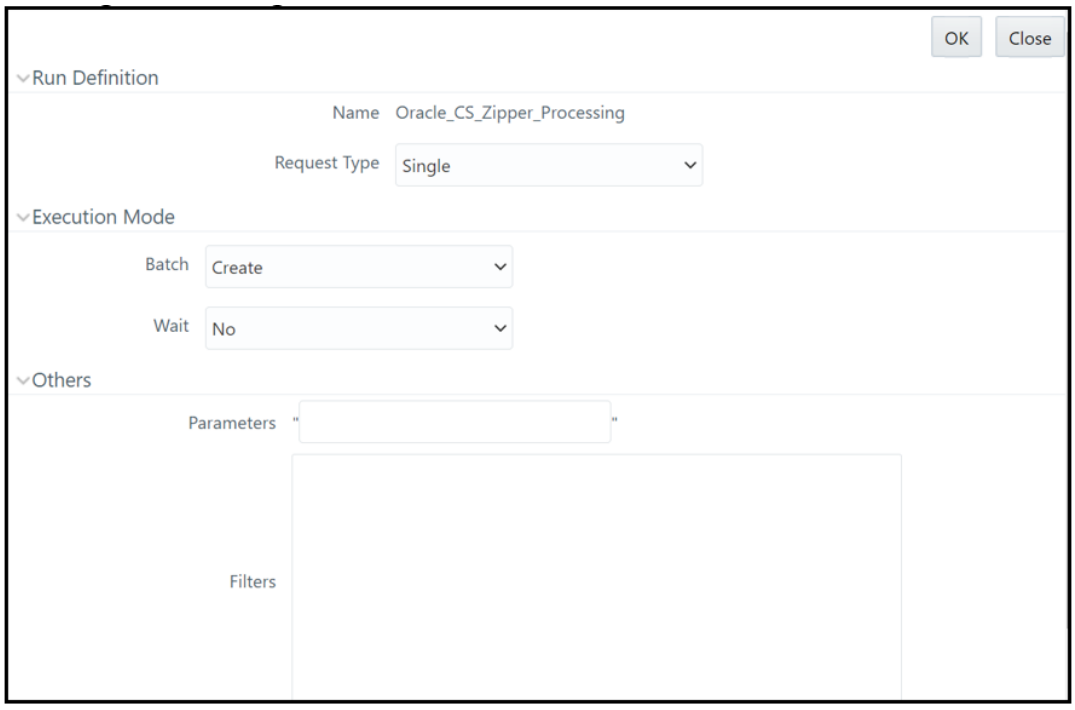
   The **Run** page is displayed.

Figure 7-24 Run page



3. In the **Run** page, select the `Oracle_CS_Zipper_Processing` checkbox and click **Fire Run**.

Figure 7-25 Run page



4. In the **Run Definition** section, select **Request Type** from the drop-down list.
5. In the **Execution Mode** section, select the Batch value as **Create** to create the batch or select **Create & Execute** to create the batch and execute it.

a. If you select Execution Mode as Create & Execute, then select **MIS Date**.

6. Select the Wait as **No** if you want to create or create & execute the batch without any delay or select **Yes** and enter the duration value in seconds.
7. In the **Others** section, enter the **Parameters** and **Filters**, if required.

7.9 Suppression of Alerts

This reconfigurability allows you to suppress the duplication of RT and Batch CS cases.

For any RT Screening, a new Real-time case is created. A new case is created for Batch Screening only if the customer matches with Watchlist information based on the rule configuration.

The subsequent batch runs will not create a new CS case against the customer until and unless any hash key attribute is changed on the customer or watchlist side.

To configure the Alert Suppression follow the these steps:

1. Access the Atomic Schema and access the CS_appln_params table. Change the parameter value from N to Y for ALERT_SUPRRESSION parameter name.

> **Note**
>
> By default, the ALERT_SUPRRESSION parameter value is **N**.

2. The request ID for the respective customer name from the real-time screening must be copied for a match or scan.
3. Enter the copied request ID in the `V_ORIG_PARTY_ID` field in the `STG_PARTY_MASTER` table.

> **Note**
>
> The suppression of alerts is only applicable for CS batch alerts and not applicable for RT case.

7.10 Configuring Additional Columns on the Alert List page

This configurability allows you to add additional column(s) on the Alert Search and List page and view additional information.

It also provides configurability to execute the customized query to fetch the data in the columns against each Alert ID and shows the new columns in the Columns drop-down list while saving the view.

To add a column on the Search and List page and filters, follow these steps:

1. Add an entry in this table "FCC_SANC_LIST_PAGE_CONFIG" to configure a new value in the column drop-down section for FCC_ZCS_ENTITY_ALERTS.

   See fcc_sanc_list_page_config.xlsx file with sample entries for Case ID and Watchlist primary name.

> **Note**
>
> Add an entry only for the DEFAULT view. "TABLE_NAME" column must have 'FCC_ZCS_ENTITY_ALERTS' value "COLUMN_NAME" column must have actual column name value in the parent table like V_CASE_ID, WATCHLIST_PRIMARY_NAME, and so on.

2. Add an entry in this table "FCC_SAN_LIST_CONFIG" to configure a new value in the filter search section for CS_LIST_FILTER.

   See fcc_san_list_config.xlsx file with sample entries for Case ID and Watchlist primary name.

3. Add an entry in this table "FCC_SAN_LIST_CONFIG_TL" to configure a new value in the filter search section.

   See fcc_san_list_config_tl.xlsx file with sample entries for Case ID and Watchlist primary name.

> **Note**
>
> N_CONFIG_ID column value in this table must match with N_CONFIG_ID value in "fcc_san_list_config" table.

4. Update "v_query" column in this table "FCC_SANC_LIST_PAGE_QUERY_CONF" where "V_QUERY_IDENTIFIER" column value is 'CS_ALERT_LIST_GRID', with the new column details in select query to get the data for new column.
5. **(Optional step):** If you are trying to configure the column from the existing listed tables in the query. If not, follow the below step, Update "v_query" column in this table "FCC_SANC_LIST_PAGE_QUERY_CONF" where "V_QUERY_IDENTIFIER " column value is 'CS_ALERT_LIST_COUNT' with the new column details in select query to get the updated count value.
6. Now insert the below script in the config schema where application is installed. Make an entry into messages_en_us table with MSG_IDENTIFIER column value starting with 'ZCS_'and BUSINESS_DISPLAY_NAME column value given in FCC_SANC_LIST_PAGE_CONFIG table. MSG_DESCRIPTION value should be the name which should be displayed on the UI.

> **Note**
>
> If there is any space exist's in BUSINESS_DISPLAY_NAME column value replace with underscore('_').For Example: If BUSINESS_DISPLAY_NAME column value is Alert ID then the MSG_IDENTIFIER column value should be like ZCS_Alert_ID. After insertion please restart the server.

7. Next open the CSMessageConstants.jsp file from the <Installed Sanctions Path>/ Customer Screening Directory. For example, ECM808SAN.war path }/CustomerScreening

   Add the below line:

   CSMessageConstants.MSG_IDENTIFIER = "%=MessageFramework.getMessageFromLocaleSpeficCache("RENDERER.MSG_IDENTIFIER", currentMsgLocale.toString())%>"; Search for alertListColMap and add the below line: alertListColMap.set(MSG_IDENTIFIER,CSMessageConstants.MSG_IDENTIFIER);

> **Note**
>
> Replace MSG_IDENTIFIER with the actual Value which is inserted into messages_en_us table in the above step.

7.11 Configuring Additional Columns on the Related Alerts Page

This configurability allows you to add additional column(s) on the Related Alerts page and view additional information.

It also provides configurability to execute the customized query to fetch the data in the columns against each Alert ID.

To add a column on the Related Alerts page and filters, follow these steps:

1. In Atomic Schema, for the table FCC_SANC_LIST_PAGE_QUERY_CONF, find the query present in the column V_QUERY for V_QUERY_IDENTIFIER = 'CS_RELATED_ALERTS'.
2. In the above query, check if the column to be added in related alerts page, is present or not.
3. If present, note down the column name (or alias name, if present). If not present, add necessary changes in the sql, and note down it's column name (or alias name, if given).
4. Open the AuditScreen.js from the below path in deployed area.../<DEPLOYED_WAR>/CustomerScreening/js/viewModels.
5. Search by the 'self.auditcolumnArray = ko.observableArray([{' in the above page where params.data.moduleName == "Related Alerts" is present as condition check.
6. Add a new json object for header details for the new column to be added just like the exisitng ones.
7. In the newly added json object for header details, for headerText field, provide appropriate value from CSMessageConstants.jsp which will be shown as column name in related alerts page.
8. If there is no appropriate entry present in CSMessageConstants.jsp, create a new one by giving entry in messages_en_us table and CSMessageConstants.jsp.
9. Restart server (only if the step 8 is executed).
10. Clear browser cache (if js file is changed).
11. Re-login and check the related alerts page.

7.12 Steps to customize the set of special characters to be allowed in the input of Primary Name field in Search Filter of List Page

Follow these steps to customize the set of special characters to be allowed in the input of Primary Name field in Search Filter of List page:

1. In Atomic Schema, for the table FCC_SAN_LIST_CONFIG, find the value in the column V_REGEX_EXPR for V_PARAM_NAME = 'CS_LIST_FILTER'
2. The value contains all the special characters allowed for the Primary Name field's input for the Search Filter of the List page.

3. Add/Remove the special character(s) which is(are) needed to be allowed/restricted.
4. Once the column value is updated, reload the list page menu.

8
OWS Migration

The existing Oracle Watchlist Screening (OWS) customer data must be migrated to Oracle Financial Services Customer Screening (OFS CS).

The OWS User Application provides Watchlist Management for a number of free and commercial watchlists and has default matching rules for Entity and Individual Sanctions and Politically Exposed Persons (PEPs) and for Country Prohibitions. For more information on OWS, see Oracle Watchlist Screening Implementation Guide.

Oracle clients using OWS must migrate the customer data from OWS to OFS CS while the OWS-related components and processes continue. Migrating the data from the OWS to CS provides continued functionality to the existing OWS clients without any data loss. OWS and CS share the same functionality except for the output.

Following customer data are migrated from OWS to CS during the migration process:

- Closed Cases
- Alerts
- Watchlist data associated with Case or Alert
- Customer data associated with Case or Alert
- Comments and Attachments

The following data are not migrated from OWS to CS during the migration process:

- The OWS Workflow is not migrated.
- The EDQ rules are not migrated.
- In EDQ, the new projects will be a CS project. Any customization done on the OWS project must be done on the CS project.

If a new alert is generated for the customer and watchlist, it will be generated as a new alert, and you can view the migrated closed or resolved cases and their corresponding details. You cannot reopen a migrated case from OWS in CS.

> **Note**
>
> - Migrating the customer data from OWS to OFS CS is a one-time activity.
> - EDQ version 12.2.1.4.0 must be installed.

8.1 Post Implementation Steps for Data Migration from OWS to CS

Follow the subsequent steps to migrate/import customer data from OWS to OFS CS after installing the Sanction Application Pack:

1. Create a DBLINK from the Sanctions Atomic Schema to the Enterprise Data Quality (EDQ) Config Schema. DBLINK act as a connection between the sanctions atomic schema and EDQ Config Schema.

   Sample DBLINK format:

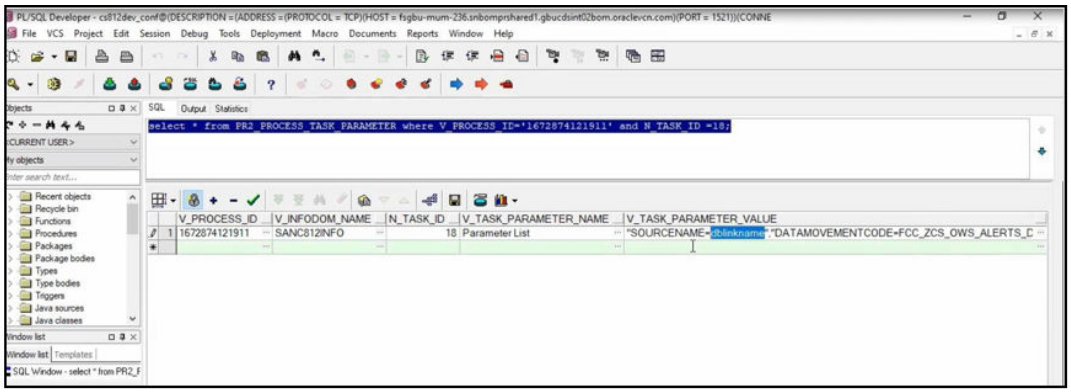
   ```
   CREATE DATABASE LINK {dblinkname} CONNECT TO {edqconfiguser} IDENTIFIED BY
   {password} USING '(DESCRIPTION =(ADDRESS =(PROTOCOL = TCP)(HOST =
   {DBServername})(PORT = {portnumber}))(CONNECT_DATA =(SERVER = DEDICATED)
   (SERVICE_NAME = {servicename})))';
   ```

2. Login into Sanction Config Schema.
3. Run the following script in the Config Schema.

   ```
   select * from PR2_PROCESS_TASK_PARAMETER where V_PROCESS_ID='1672874121911'
   and N_TASK_ID =18;
   ```

4. After running the script, in the `PR2_PROCESS_TASK_PARAMETER` table, update the DBLINK name in the `V_TASK_PARAMETER_VALUE` column with the DBLINK name created in step 1. See the below screen.

Figure 8-1 PR2_PROCESS_TASK_PARAMETER table

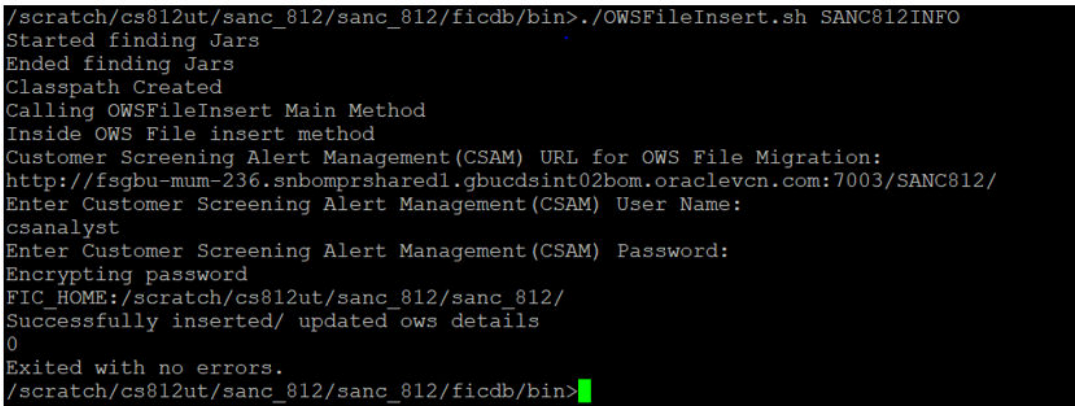


5. To move the file data from OWS Server to the CS server, you need to run the OWSFileInsert.sh, which is present in `ficdb/bin` path.

   If you run the `OWSFileInsert.sh` shell script, it will be inserted in to the `CS_APPLN_PARAMS` table.

   Once the entries for the `OWS_CS_URL` attribute are done in `CS_APPLN_PARAMS`, if you run the OWS Migration batch from the Run Screen, the OWS File Migration task will read the details from `CS_APPLN_PARAMS` table and move the files from OWS Server to CS server.

Figure 8-2 OWSFileInsert.sh shell script



6. Go to the `fichome` folder in the Sanctions server.

   Sample file path:

   `/scratch/ofsaabuild/BUILD_HOME/8.1.2.4.0/OFS_CMBT/packs/OFS_SANC/dist_GENERIC/OFS_SANC/build/partial/fichome`

7. Open the OWSMIGRATION folder.
8. Open DXI folder.

   The following files are available in the DXI folder:

   - OWSCS case migration utility.dxi
   - OWS_CS_Case_Migration.properties 9.

9. Move the `OWSCS case migration utility.dxi` and `OWS_CS_Case_Migration.properties` file to local directory.
10. Upload the `OWSCS case migration utility.dxi` file to the EDQ application from the local directory.

    For more information on Importing the OFS Customer Screening Projects, see Oracle Financial Services Sanctions Pack Installation and Configuration Guide.

11. Upload the `OWS_CS_Case_Migration.properties` file to the following path in the EDQ server:

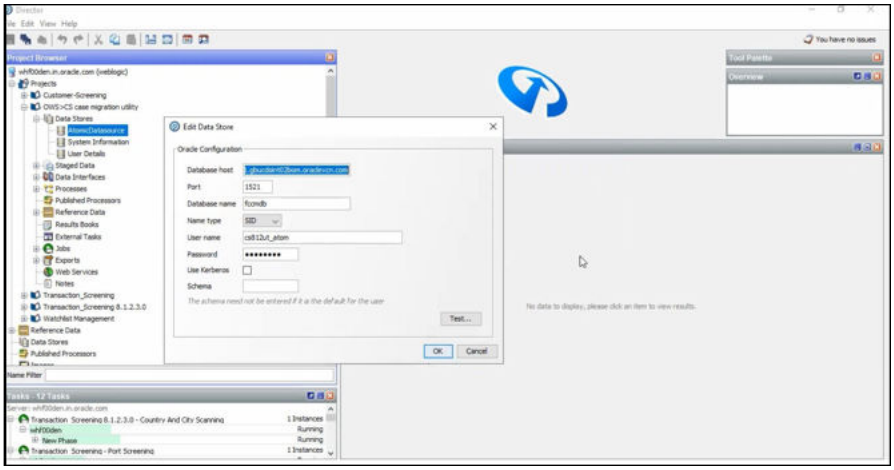
    `/scratch/devuser/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/edq/0edq.local.home/runprofiles`

12. After uploading the DXI file to the EDQ application. Open the DXI from EDQ director and select the **Data Stores** folder the Project Browser.
13. Click **AtomicDatasource**.

    The **Edit Data Store** window is displayed.

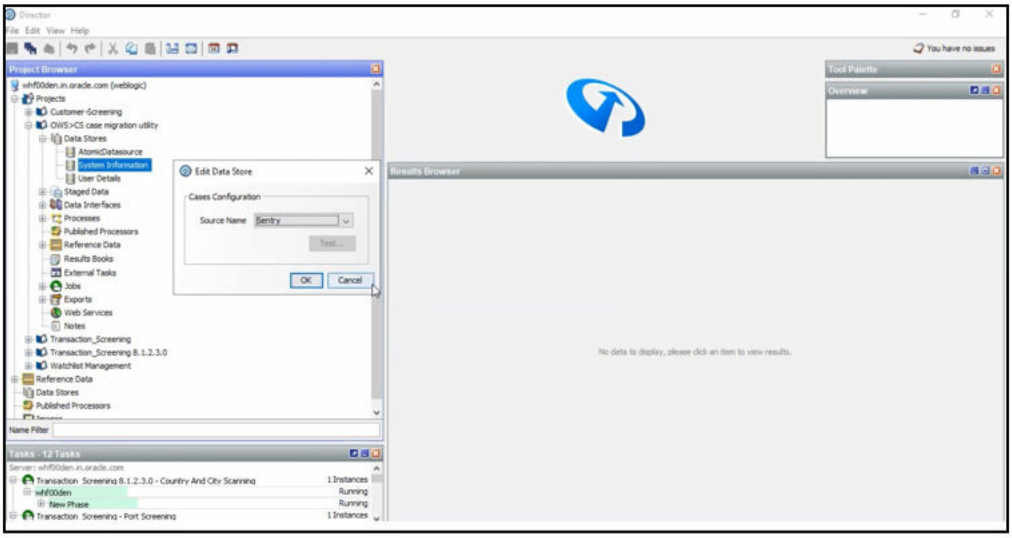
14. Update the sanctions data base details in the Edit Data Store configuration window and click **OK**.

Figure 8-3 Edit Data Store



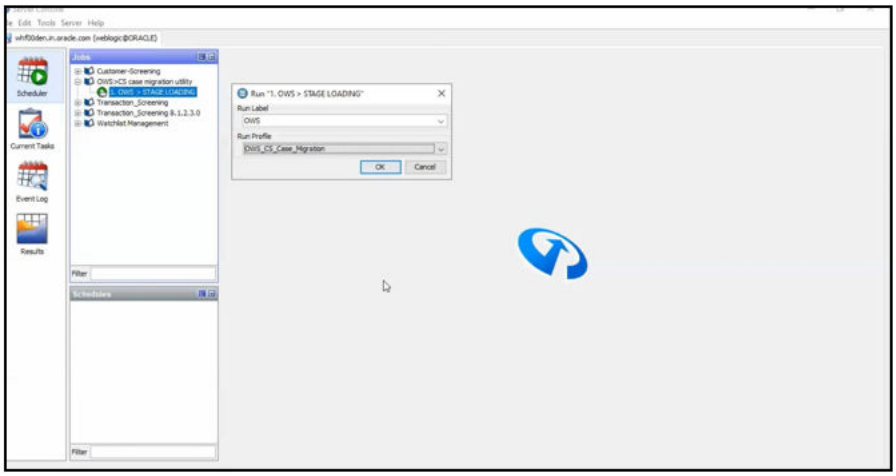
15. Click **System Information** in the **Data Stores** folder and select **Sentry** as source name.

Figure 8-4 System Information page



16. Go to the EDQ server and login to the Server Console from the Launchpad menu.
17. Select **OWS>CS case migration utility** folder in the Server Console page.
18. Run **OWS > STAGE LOADING** by using the `OWS_CS_Case_Migration.properties` file by Right-clicking **OWS > STAGE LOADING**.
19. Select **OWS_CS_Case_Migration** from the Run Profile drop-down and click **Ok** to run the project. With the execution, the results will be populated inside a temporary setup table.

Figure 8-5 Server Console page



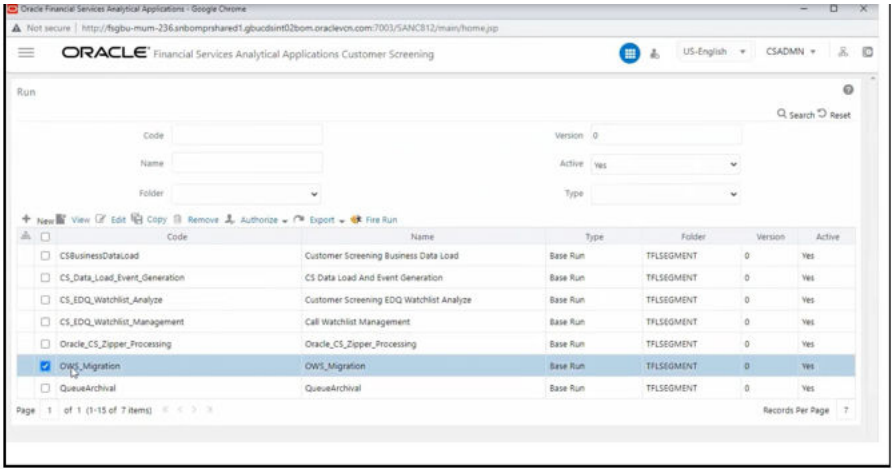
> **Note**
>
> If there is a break or failure in running the OWS > STAGE LOADING, truncate the following tables and re-run step 17.
>
> - `OWS_CS_CASE_ATTACHMENTS;`
> - `OWS_CS_CASE_COMMENTS;`
> - `OWS_CS_CASE_HISTORY;`
> - `OWS_CS_CASE_MASTER;`
> - `OWS_CS_CASE_ISSUES;`
> - `OWS_CS_CASE_RELATION;`
> - `OWS_CS_COUNTRY_PRHB;`
> - `OWS_CS_ENTITY_WL_DATA;`
> - `OWS_CS_ENT_CUST_DATA;`
> - `OWS_CS_IND_CUST_DATA;`
> - `OWS_CS_IND_WL_DATA;`
> - `OWS_CS_IND_CUST_ISSUES;`
> - `OWS_CS_ENT_CUST_ISSUES;`

20. After running the job, log in to Oracle Financial Services Customer Screening (OFS CS) application.
21. Click **Common Tasks**, then click **Rule Run Framework**, and then click **Run**.

    The **Run** page is displayed.
22. In the **Run** page, select the `OWS_Migartion` check box from the table and click **Fire Run**.

    The **Fire Run** page is displayed.

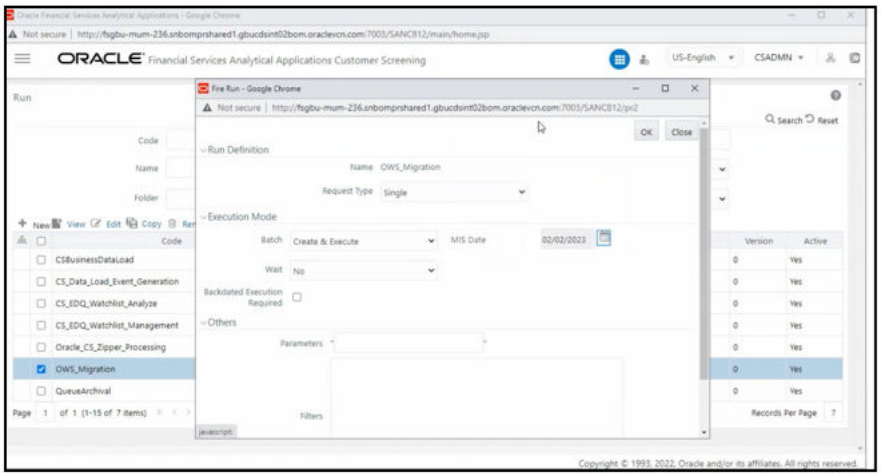
Figure 8-6 Run page



23. Select **single** as the **Request Type** in the Run Definition section.
24. Select the Batch value as **Create & Execute** and select the MIS Date in the Execution Mode section.
25. Select Wait as **No** to create & execute the batch without any delay.
26. Click **Ok** to execute the OWS_Migration batch.

    A message is displayed after successful batch execution. Click **Close** to go back to the Run page.

Figure 8-7 Fire Run page



After the successful execution, the OWS data will get migrated to CS and alert will be generated in the Customer Screening Alert List if there are matches. For more information on Alert List, see Alerts for Migrated OWS Watchlist data section in OFS Customer Screening User Guide.

8.2 Monitoring the migrated OWS batch ID in OFSAA

After the batch is executed, you can view the batch details on the Batch Monitor page.

To view the batch details follow the subsequent steps:

1. To access the Batch Monitor page, click Operations, and then click Batch Monitor. The Batch Monitor page has details of all batches. The batch you have executed is the last in the Batch Details list.
2. Select the **Batch ID**.
3. Select the **MIS or Information Date**.

   After you select the **MIS Date**, the **Batch ID** is displayed in the **Batch Run ID** field.
4. Select **Batch Run ID**.
5. Click **Start Monitoring**.

   The task details associated with the batch appears in the **Task Details** section. You can also view and export the event logs for the batch in the **Event Log** section.

> **Note**
>
> If the batch run fails, you must run the following scripts and start a new batch:
>
> - `delete from fcc_zcs_cust where JRSDCN_CD='D';`
> - `delete from fcc_zcs_cust_addr where ZCS_CUST_SEQ_ID in (select ZCS_CUST_SEQ_ID from fcc_zcs_cust where JRSDCN_CD='D');`
> - `delete from fcc_ZCS_CUST_ID_DOC where JRSDCN_CD='D';`
> - `delete from FCC_ZCS_RT_ENTITY where ext_id_type ='OWS_ENT';`
> - `delete from FCC_ZCS_RT_ENTITY where ext_id_type ='OWS_IND';`
> - `delete from fcc_ZCS_WATCHLIST where WATCHLIST_SUB_ID is not null;`
> - `delete from fcc_ZCS_WATCHLIST where WATCHLIST_KEY='PRHB';`
> - `delete from FCC_ZCS_ENTITY_ALERTS where JRSDCN_CD='D';`
> - `delete from fcc_zcs_alerts where JRSDCN_CD='D';`
> - `delete from FCC_ZCS_ALERT_MATCHES where JRSDCN_CD='D';`
> - `delete from FCC_ZCS_ENTITY_ALERTS_AUDIT where V_UPDATED_BY = 'Director Administrator';`
> - `delete from OWS_CS_CASE_ATTACHMENTS;`

9 Simulation

The OFS customer Screening Simulation feature allows the user to test new configurations in a sandbox environment and compare the results with the existing set-up by integrating with the OFS Compliance Studio Application. This allows the user to replicate and test the screening process without impacting the production environment. The Sandbox workspace created will allow the user to define a suitable dataset based on the production and the available test data. You can extract the data, filter it, and plug it into a visualization tool.

You can create multiple workspaces, each with its own EDQ rules. To view the changes in the simulation data for a deeper analysis, you can use the data extraction feature. You can run multiple simulations and compare the results using data extraction.

For information about installation and configuration of Compliance Studio Application, see Oracle Financial Services Compliance Studio Installation Guide.

For the subsequent information, see Oracle Financial Services Compliance Studio User Guide.

- Accessing the OFS Compliance Studio Application
- Using the Application UI
- Mapping User Groups
- Access the Workspace Dashboard Window
- Using the OFS Compliance Studio Application
- Using Workspaces
- Managing Workspace
- Managing Model Pipelines

9.1 CS Data Process Flow

The process flow for building Customer Screening models in Compliance Studio involves the configuring, creation Sandboxes and the creation of Models mapped to the Sandboxes. You can use these CS models to perform model visualizations and test for the outcomes. You can then publish a model into production and make it available to users after you have determined that the models and the parameters used to construct the models meet the requirements of your business logic.

Figure 9-1 Simulation Process Flow

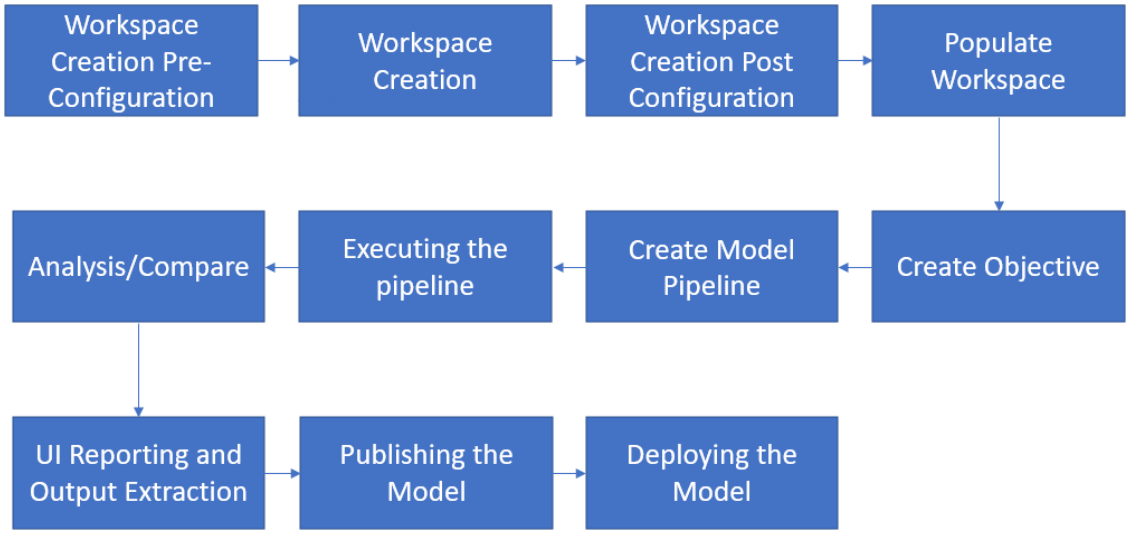
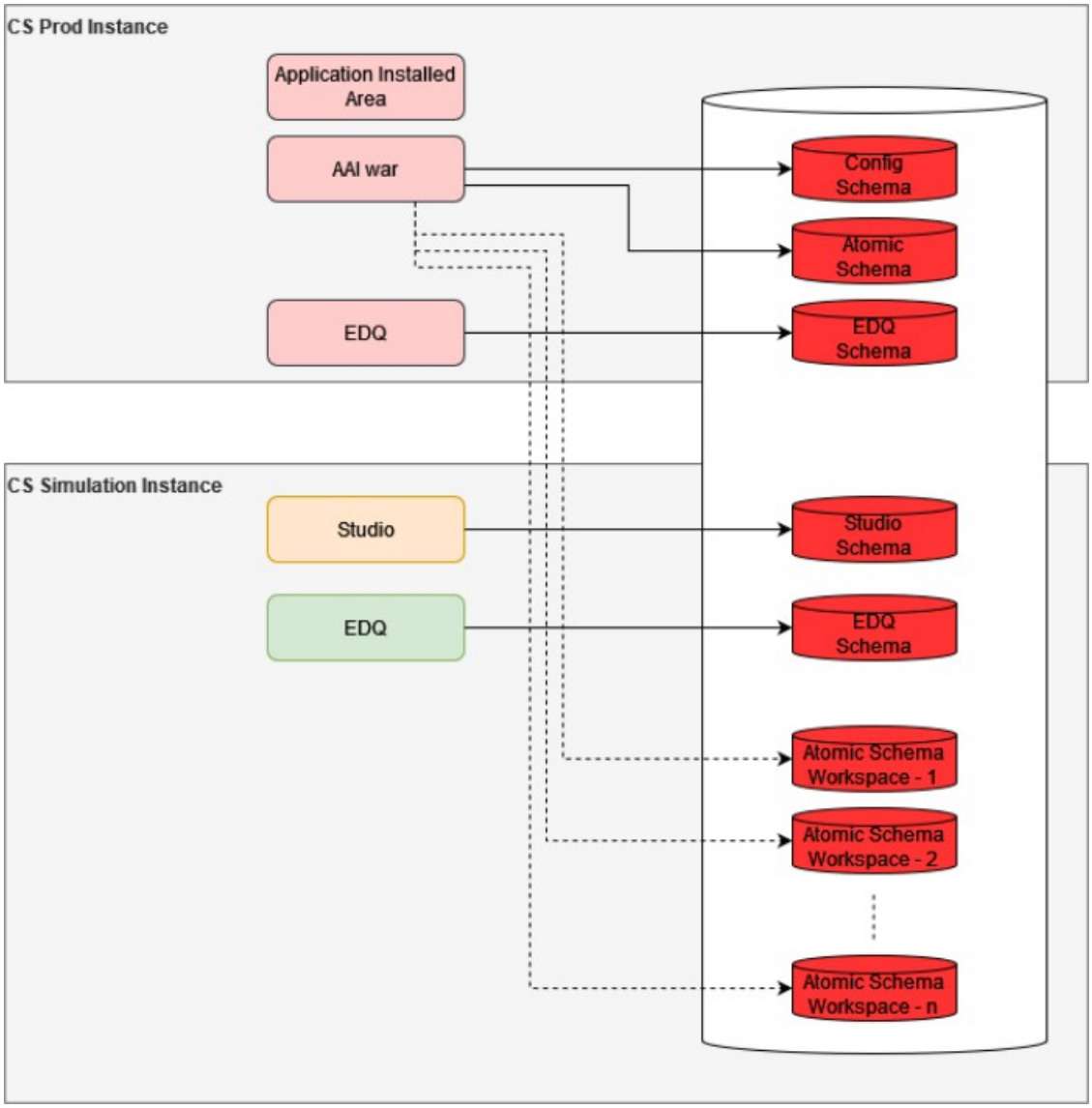


Figure 9-2 CS Data Flow



9.2 Integrating With Compliance Studio

OFS Compliance Studio is an advanced analytics application that supercharges anti-financial crime programs for better customer due diligence, transaction monitoring, and investigations by leveraging the latest innovations in artificial intelligence, open-source technologies, and data management. It combines Oracle's Parallel Graph Analytics (PGX), Machine Learning for AML, Entity Resolution, and notebook-based code development and enables Contextual Investigations in one platform with complete and robust model management and governance functionality. For More Information on Compliance Studio, see Oracle Financial Services Compliance Studio User Guide.

Topics:

- Workspace Creation Pre-Requisite
- Workspace Creation Pre-Configuration

- Workspace Creation
- Workspace Creation Post-Configuration

9.2.1 Workspace Creation Pre-Requisite

Following are the pre-requisites for workspace creation:

1. Create User tablespace in simulation database by executing below script as sysdba user:

   ```
   CREATE TABLESPACE AIF_USER_TS DATAFILE '<DATAFILE PATH>/
   aif_user_data_tablespace.dbf' SIZE 1G REUSE AUTOEXTEND ON NEXT 500M
   MAXSIZE UNLIMITED;
   ```

   DATAFILE PATH example: `/scratch/oraofss/app/oradata`

2. Perform the Zippelin Interpreter Configuration in Compliance Studio UI. See Appendix R: Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMIT in Python Interpreter.
3. Create Instance Token for Production and Simulation in Sanctions Application. See Appendix F: Configurations for the Bearer Token.

9.2.2 Workspace Creation Pre-Configuration

Execute the following steps in the same order to integrate the CS data with OFS Compliance Studio application:

1. Create Database Schema for the new workspace
2. Add the schema to wallet in the Compliance Studio Setup
3. Add the infodom in Weblogic Console
4. Display the OFSAA Environment Menu in Compliance Studio UI
5. Registering the OFSAA Environment Details
6. Procedure to Create PPK File
7. Different ways of PPK File Registration
8. Configuring the Data Source

Create Database Schema for the new workspace

Follow the subsequent steps to configuring new Database schema:

1. Create a new database schema in the sys user. To create the new schema, run the below script as sysdba user:

   ```
   CREATE USER <NEW SIM USER> IDENTIFIED BY <NEW SCHEMA PASSWORD> DEFAULT
   TABLESPACE
   AIF_USER_TS TEMPORARY TABLESPACE TEMP QUOTA UNLIMITED ON AIF_USER_TS;
   grant create SESSION to <NEW SIM USER>;
   grant create PROCEDURE to <NEW SIM USER>;
   grant create SEQUENCE to <NEW SIM USER>;
   grant create TABLE to <NEW SIM USER>;
   grant create TRIGGER to <NEW SIM USER>;
   grant create VIEW to <NEW SIM USER>;
   grant create MATERIALIZED VIEW to <NEW SIM USER>;
   grant select on SYS.V_$PARAMETER to <NEW SIM USER>;
   ```

```
grant create SYNONYM to <NEW SIM USER>;
grant select on sys.v_$parameter to <NEW SIM USER>;
grant select on sys.dba_free_space to <NEW SIM USER>;
grant select on sys.dba_tables to <NEW SIM USER>;
grant select on sys.Dba_tab_columns to <NEW SIM USER>;
grant create RULE to <NEW SIM USER>;
grant create any trigger to <NEW SIM USER>;
grant drop any trigger to <NEW SIM USER>;
grant select on SYS.DBA_RECYCLEBIN to <NEW SIM USER>;
grant connect, resource, dba to #new_user#;
grant execute on dbms_crypto to <NEW SIM USER>;
grant execute on <SIM CONFIG SCHEMA>.checkenvfordataredaction to <NEW
SIM USER>;
grant select on <SIM CONFIG SCHEMA>.PR2_FIRERUN_FILTER to <NEW SIM
USER>;
grant select on <SIM CONFIG SCHEMA>.pr2_run_object to <NEW SIM USER>;
grant select on <SIM CONFIG SCHEMA>.pr2_run_object_member to <NEW SIM
USER>;
grant select on <SIM CONFIG SCHEMA>.pr2_run_map to <NEW SIM USER>;
grant select on <SIM CONFIG SCHEMA>.PR2_FILTERS to <NEW SIM USER>;
grant select on <SIM CONFIG SCHEMA>.pr2_run_execution_b to <NEW SIM
USER>;
grant select on <SIM CONFIG SCHEMA>.pr2_run_execution_filter to <NEW SIM
USER>;
grant select on <SIM CONFIG SCHEMA>.configuration to <NEW SIM USER>;
grant select on <SIM CONFIG SCHEMA>.aai_wf_filter_exec_map to <NEW SIM
USER>;
```

2. Run the below sql statements in newly created user:

> **Note**
>
> Replace <NEW INFODOM> with the actual infodom within the single quotes.

```
CREATE SYNONYM pr2_firerun_filter FOR <SIM CONFIG
SCHEMA>.pr2_firerun_filter;
CREATE OR REPLACE SYNONYM checkenvfordataredaction FOR <SIM CONFIG
SCHEMA>.checkenvfordataredaction;
CREATE OR REPLACE SYNONYM cssms_role_mast FOR <SIM CONFIG
SCHEMA>.cssms_role_mast;
CREATE OR REPLACE SYNONYM cssms_group_role_map FOR <SIM CONFIG
SCHEMA>.cssms_group_role_map;
CREATE OR REPLACE SYNONYM cssms_usr_group_map_view FOR <SIM COA@NFIG
SCHEMA>.cssms_usr_group_map_view;
CREATE OR REPLACE FORCE EDITIONABLE VIEW pr2_run_object (

v_run_id,v_infodom_name,v_object_unique_name,v_object_type_code,v_object_lo
cation_code,n_object_order,v_task_ref_unique_name,

v_task_type_code,v_task_sub_type_code,v_task_ref_1_name,v_task_ref_1_value,
v_task_ref_2_name,v_task_ref_2_value,v_task_ref_3_name,
    v_task_ref_3_value,v_task_ref_4_name,v_task_ref_4_value
) AS
    SELECT
```

```
v_run_id,v_infodom_name,v_object_unique_name,v_object_type_code,v_object_lo
cation_code,n_object_order,v_task_ref_unique_name,v_task_type_code,
v_task_sub_type_code,v_task_ref_1_name,v_task_ref_1_value,v_task_ref_2_name
,v_task_ref_2_value,v_task_ref_3_name,v_task_ref_3_value,
v_task_ref_4_name,v_task_ref_4_value

    FROM
        <SIM CONFIG SCHEMA>.pr2_run_object pro
    WHERE
        pro.v_infodom_name = <NEW INFODOM>;
CREATE OR REPLACE FORCE EDITIONABLE VIEW pr2_run_object_member (

v_run_id,v_infodom_name,v_object_unique_name,v_member_unique_name,v_member_
type_code,n_member_order
) AS
    SELECT

v_run_id,v_infodom_name,v_object_unique_name,v_member_unique_name,v_member_
type_code,n_member_order
    FROM
        <SIM CONFIG SCHEMA>.pr2_run_object_member prom
    WHERE
        prom.v_infodom_name = <NEW INFODOM>;
CREATE OR REPLACE FORCE EDITIONABLE VIEW pr2_run_map (

v_run_id,v_infodom_name,v_task_ref_unique_name,v_object_unique_name,v_membe
r_unique_name
) AS
    SELECT

v_run_id,v_infodom_name,v_task_ref_unique_name,v_object_unique_name,v_membe
r_unique_name
    FROM
        <SIM CONFIG SCHEMA>.pr2_run_map prm
    WHERE
        prm.v_infodom_name = <NEW INFODOM>;
CREATE OR REPLACE FORCE EDITIONABLE VIEW pr2_filters (

f_is_rrf,v_dsn_name,v_execution_id,v_task_id,v_component_code,n_run_skey,v_
run_code,v_rule_code,v_filter
) AS
    SELECT

filters.f_is_rrf,filters.v_dsn_name,filters.v_execution_id,filters.v_task_i
d,filters.v_component_code,filters.n_run_skey,filters.v_run_code,
filters.v_rule_code,filters.v_filter
    FROM
             (
            SELECT
                'RRF'                   AS f_is_rrf,
                pref.v_infodom_name     AS v_dsn_name,
                pref.v_run_execution_id AS v_execution_id,
                pref.v_task_id          AS v_task_id,
                pref.v_process_id       AS v_component_code,
                pref.n_run_skey         AS n_run_skey,
                preb.v_run_id           AS v_run_code,
```

```
                    pref.v_rule_id          AS v_rule_code,
                    '('
                    ||
                    CASE
                        WHEN pref.v_process_filter IS NULL THEN
                                '7=7'
                        ELSE
                            pref.v_process_filter
                    END
                    || ')'
                    || ' AND '
                    || '('
                    ||
                    CASE
                        WHEN pref.v_run_filter IS NULL THEN
                                '8=8'
                        ELSE
                            pref.v_run_filter
                    END
                    || ')'
                    || ' AND '
                    || '('
                    ||
                    CASE
                        WHEN pff.v_run_filter IS NULL THEN
                                '9=9'
                        ELSE
                            pff.v_run_filter
                    END
                    || ')'                  AS v_filter
                FROM
                    <SIM CONFIG SCHEMA>.pr2_run_execution_b      preb
                    LEFT OUTER JOIN <SIM CONFIG
SCHEMA>.pr2_firerun_filter       pff ON pff.v_run_execution_id =
preb.v_run_execution_id
                                                                        AND
pff.v_infodom_name = preb.v_infodom_name
                    JOIN <SIM CONFIG SCHEMA>.pr2_run_execution_filter pref ON
pref.v_run_execution_id = preb.v_run_execution_id
                                                                      AND
pref.v_infodom_name = preb.v_infodom_name
                WHERE
                    preb.v_infodom_name = <NEW INFODOM>
                UNION ALL
                SELECT
                    'PR2' AS f_is_rrf,v_dsn_name,v_execution_id,NULL  AS
v_task_id,v_component_code,n_run_skey,v_run_code,v_rule_code,v_filter
                FROM
                    <SIM CONFIG SCHEMA>.pr2_filters pf
                WHERE
                    pf.v_dsn_name = <NEW INFODOM>
            ) filters
            JOIN <SIM CONFIG SCHEMA>.configuration ON upper(paramvalue) =
upper(f_is_rrf)
        WHERE
            paramname = 'F_IS_RRF'
```

```
    UNION ALL
    SELECT

awfem.f_is_rrf,awfem.v_dsn_name,awfem.v_execution_id,awfem.v_task_id,awfem.
v_component_code,awfem.n_run_skey,awfem.v_run_code,
awfem.v_rule_code,awfem.v_filter
    FROM
        <SIM CONFIG SCHEMA>.aai_wf_filter_exec_map awfem;

CREATE SYNONYM AAI_WF_REQUEST_QUEUE_HIST FOR
<SIM CONFIG SCHEMA>.AAI_WF_REQUEST_QUEUE_HIST;
CREATE SYNONYM AAI_WF_REQUEST_QUEUE FOR
<SIM CONFIG SCHEMA>.AAI_WF_REQUEST_QUEUE;
CREATE SYNONYM AAI_WF_REQUEST_PARAMETER FOR
<SIM CONFIG SCHEMA>.AAI_WF_REQUEST_PARAMETER;
CREATE SYNONYM AAI_WF_REQUEST_PARAMETER_HIST FOR
<SIM CONFIG SCHEMA>.AAI_WF_REQUEST_PARAMETER_HIST;
create or replace type array_varchar as VARRAY(200) OF VARCHAR2(50);
```

Add the schema to wallet in the Compliance Studio Setup

Follow the subsequent steps to add the schema to the wallet:

1. Add the database schema credentials in the wallet using the following command:

   ```
   mkstore -wrl <WALLET LOCATION> -createCredential <NEW SCHEMA>_alias <NEW
   SCHEMA>
   ```

2. After you run the command, a prompt is displayed. Enter the password `<NEW SCHEMA PASSWORD>` associated with the database user account in the prompt. You are the prompted to re-enter the password and the wallet password that you entered during wallet creation.
3. Update the tnsnames.ora file to include the following entry.

   ```
   <NEW SCHEMA>_alias = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL
   = TCP)(HOST = <<IP ADDRESS>>)(PORT = <<PORT NUMBER>>)) ) (CONNECT_DATA =
   (SERVICE_NAME = <<SERVICE NAME>>) ) )
   ```

4. Repeat the above steps for Production Database Schema if not added.

For more information, see Oracle Wallet documentation to create/manage wallets. Refer to the Compliance Studio Installation Guide to locate the wallet location.

Add the infodom in Weblogic Console

To add the infodom in WebLogic console follow the subsequent steps:

1. Login into WebLogic console.
2. Go to **Services**.
3. Click **Data Sources**.
4. Click on **New** button and add Data Source name as `<<Simulation Infodom>>` and JNDI Name as `jdbc/<<Simulation Infodom>>` for the newdatabase schema details.

> **Note**
>
> - <<Simulation Infodom>> must have 11 characters.
> - <<Simulation Infodom>> name used while creating the work space.

Configure the infodom in tnsnames.ora in Simulation Sanctions Setup

To enter the new schema details in the tnsnames.ora file, see the below sample template:

```
<<NEW SCHEMA>> =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = <<IP ADDRESS>>)(PORT = <<PORT
NUMBER>>))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = <<SERVICE NAME>>)
    )
  )

<<Simulation Infodom>> =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = <<IP ADDRESS>>)(PORT = <<PORT
NUMBER>>))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = <<SERVICE NAME>>)
    )
  )
```

To enter the new infodom details in the weblogic server, see Configure Multi Data Sources section in OFS Sanctions Pack Installation and Configuration Guide

Display the OFSAA Environment Menu in Compliance Studio UI

To display OFSAA Environment in the UI follow the subsequent steps:

1. Click the **User** Icon right top corner.
2. Click **Identity Management**. The Identity Management window is displayed. For more information on Identity Management, see OFS Admin Console User Guide.
3. Click **Groups**. The Groups window is displayed.
4. Select **Workspace Administrator** from the list to display the Group Details page.
5. Select **Mapped Roles** tab. The Mapped Roles window is displayed.
6. Click **New Mapping**. The Unmapped Roles window is displayed.
7. Click **Authorization View**.
8. Search for OFSAA Environment Menu Access, and select **OFSAA Environment Menu Access**.
9. Click Authorize to display **OFSAA Environment** in the UI.

Registering the OFSAA Environment Details

To Register the OFSAA Environment details, follow the subsequent steps:

1. Click the **User** Icon and select the **OFSAA Environment** from the list.
2. Click **Register Environment**. The OFSAA Environment page is displayed.
3. Click **Register Environment** to register the new CS Environment.

> **Note**
>
> You must Register Environment for Production and Simulation.

4. Provide the input for the following fields:
   - **Name**: Name of the environment Must be minimum 5 characters and maximum 20 characters
   - **Description**: Description for the environment
   - **Type**: Select either simulation or production
   - **Properties**: Select the key and enter the corresponding value. For information on Key and corresponding values, see *OFSAA Production Environment Key and ValueKey* table and *OFSAA Simulation Environment Key and Values* table.
   - **Authentication Type**: To register FIC Server and EDQ Server details follow these steps:
     There are **three Authentication** types:
     a. Password Authentication
     b. Putty Private Key Authentication
     c. Putty Private Key with Passphrase Authentication

Figure 9-3 Password Authentication

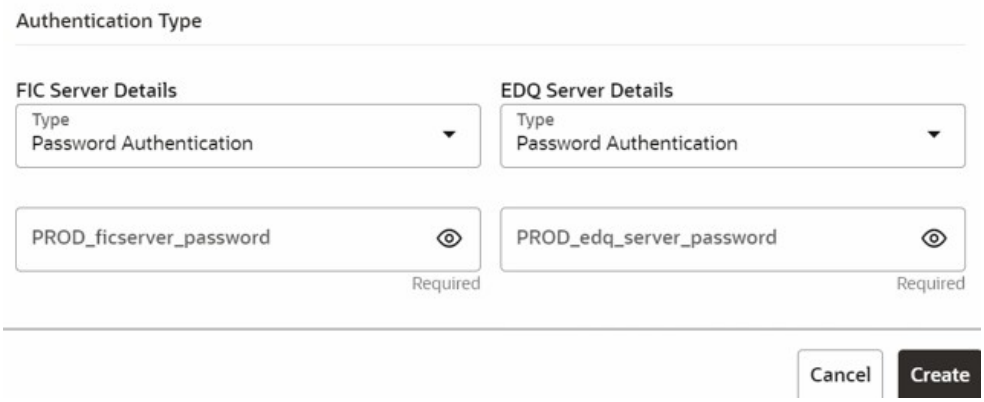


Figure 9-4 Putty Private Key Authentication

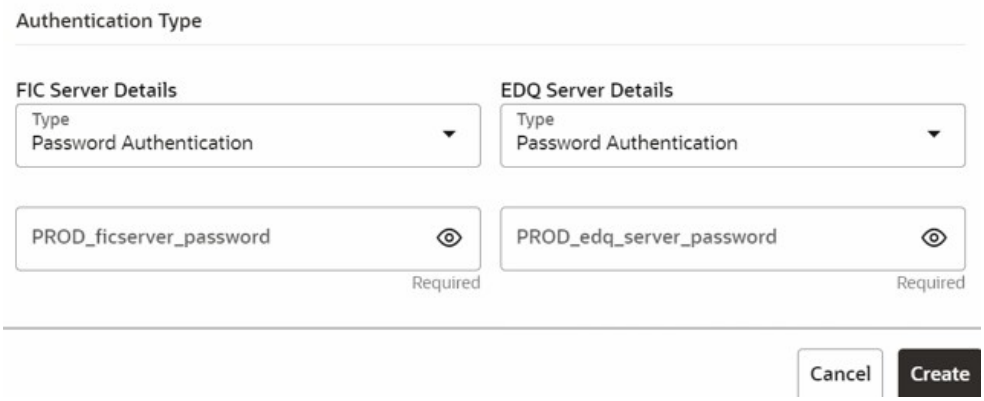
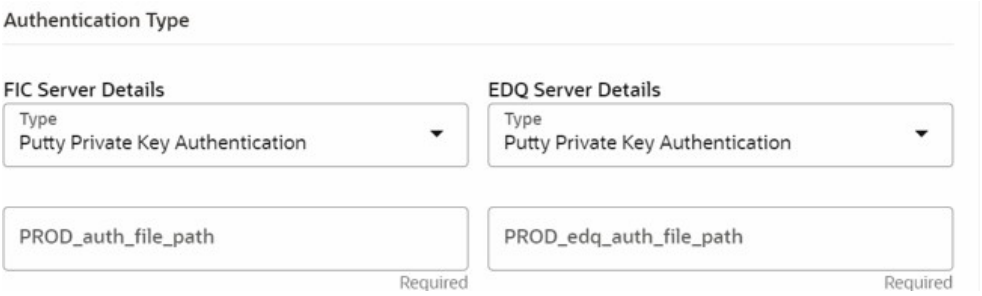


Figure 9-5 Putty Private Key with Passphrase Authentication



> **Note**
>
> We have to register with any one of the three authentication types in OFSAA Registration.

5. Click **Create**.
OFSAA Production Environment Key and ValueKey table and *OFSAA Simulation Environment Key and Values* table provides information about Key and Values for OFSAA Environment Registration.

Table 9-1 OFSAA Production Environment Key and ValueKey

Key	Description
PROD_baseUrl	Sanctions application base URL. (Example:`http://host name>:<port>/ <context- name>`)
PROD_app_id	Application ID (Example:OFS_CS)
PROD_infodom	infodom ID (Example: SANC812INFO)
PROD_ficserver_hostname	Server IP address where ftpshare is located
PROD_ficserver_username	ficserver user name
PROD_ficserver_password	ficserver password

Table 9-1 (Cont.) OFSAA Production Environment Key and ValueKey

Key	Description
PROD_ftpshare_path	ftpshare path (Example:`/scratch/sanc812/sanc/ftpshare`)
PROD_edq_server_hostname	EDQ server host name
PROD_edq_server_username	EDQ server user name
PROD_edq_server_password	EDQ server password
PROD_edq_runprofiles_path	EDQ run profiles path(Example: `/scratch/ofsaaapp/EDQ/Middleware/Oracle_Home/user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/runprofiles/`)
PROD_edq_autorun_directory	EDQ Autorun directory (Example: `/scratch/ofsaaapp/EDQ/Middleware/Oracle_Home/user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/autorun/`)
PROD_edq_exportproject_directory	EDQ export project directory (Example: /scratch/ofsaaapp/test/CS/Export/)
PROD_edq_jshell_jar_directory	EDQ jshell and jar directory (Example: /scratch/ofsaaapp/EDQ/Middleware/Oracle_Home/edq/oracle.edq/)
PROD_edq_management_port	EDQ management port ID
PROD_edq_director_username	EDQ director user name
PROD_edq_director_password	EDQ director password
PROD_edq_landingarea_path	EDQ landing area path (Example: `/scratch/ofsaaapp/EDQ/Middleware/Oracle_Home/user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/landingarea/`)
PROD_edq_project_name	EDQ project name (Example: Customer_Screening, Watchlist_Management)
PROD_instanceName	Instance name (Example: SIMULATION)
PROD_instanceAccessToken	Instance access token ID
PROD_edq_baseUrl	EDQ base URL (Example: `http://host name>:<port>`)
PROD_ficdb_path	ficdb directory
PROD_auth_file_path	FIC Server Private Key File Path (Refer section 9.2.2.8)
PROD_edq_auth_file_path	EDQ Server Private Key File Path (Refer section 9.2.2.8)
PROD_auth_passphrase	Password for FIC Server Private Key File
PROD_edq_auth_passphrase	Password for EDQ Server Private Key File

Table 9-2 OFSAA Simulation Environment Key and Values

Key	Description
SIM_baseUrl	Sanction application Base URL (Example: http://host name>:<port>/<context-name>)
SIM_ficserver_hostname	ficserver host name

Table 9-2 (Cont.) OFSAA Simulation Environment Key and Values

Key	Description
SIM_ficserver_username	ficserver user name
SIM_ficserver_password	ficserver password
SIM_ftpshare_path	ftpshare path (Example: /scratch/tf812dev/san_812/ftpshare)
SIM_edq_server_hostname	EDQ server host name
SIM_edq_server_username	EDQ server user name
SIM_edq_server_password	EDQ server password
SIM_edq_autorun_directory	EDQ auto run directory (Example: `/scratch/ofsaaapp/EDQ/Middleware/Oracle_Home/user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/autorun/`)
SIM_edq_importproject_directory	EDQ import project directory (Example: /scratch/ofsaaapp/test/CS/Import/)
SIM_edq_jshell_jar_directory	EDQ jshell and jar directory (Example: /scratch/ofsaaapp/EDQ/Middleware/Oracle_Home/edq/oracle.edq/)
SIM_edq_management_port	EDQ management port
SIM_edq_director_username	EDQ director username
SIM_edq_director_password	EDQ director_password
SIM_edq_landingarea_path	EDQ landingarea_path (Example: `/scratch/ofsaaapp/Oracle/Middleware/Oracle_Home/ user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/landingarea/`)
SIM_instanceAccessToken	Instance access token ID
SIM_instanceName	Instance Name
SIM_sys_admin_user	System admin user ID
SIM_sys_auth_user	System authentication user ID
SIM_edq_baseUrl	EDQ base URL (Example: `http://host name>:<port>`)
SIM_edq_runprofiles_path	EDQ run profiles path (Example: `/scratch/ofsaaapp/EDQ/Middleware/Oracle_Home/user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/runprofiles/`)
SIM_ficdb_path	ficdb directory
SIM_auth_file_path	FIC Server Private Key File Path (Refer section 9.2.2.8)
SIM_edq_auth_file_path	EDQ Server Private Key File Path (Refer section 9.2.2.8)
SIM_auth_passphrase	Password for FIC Server Private Key File
SIM_edq_auth_passphrase	Password for EDQ Server Private Key File

Procedure to Create PPK File

Open the putty session and run the below command:

ssh-keygen -t rsa -C "username@hostname"

Replace username & hostname with respective server details.

For reference, see below screenshot:

Figure 9-6 Procedure to Create PPK File

Different ways of PPK File Registration

1. Once the PPK file is generated it will create both private Key and public Key.
2. Place the public key inside authorized keys file present in ssh folder. Now verify once connecting to winscp using the Private Key file.
   In OFSAA Registration we can either give in any one of the following ways.

   Method 1:

   a. Create the PPK file individually in FIC server and EDQ server.
   b. Now move the PPK file generated to the simulation OFSAA FIC server deployed area. Note the path of the file here.
   c. Now register this path in the OFSAA registration for keys like PROD_auth_file_path,PROD_edq_auth_file_path,SIM_auth_file_path,SIM_edq_auth_file_pat h.

   Method 2:

   a. Create the PPK file only in simulation OFSAA FIC server alone.
   b. Now place the public key inside authorized keys file across different servers like PROD FIC Server, SIM FIC Server, PROD EDQ Server & SIM EDQ Server.
   c. Now place the PPK in the deployed area of the SIM OFSAA FIC server. Note the path of the file here.
   d. Now register this path in the OFSAA registration for all the keys like PROD_auth_file_path,PROD_edq_auth_file_path,SIM_auth_file_path,SIM_edq_auth_file_pat h.

Configuring the Data Source

The Data Source allows you to manage the Data Schemas registered with the OFS Compliance Studio application. The Data Source Summary window shows the list of Data Schemas registered with OFS Compliance Studio. These Data Schemas can be used either for workspace or for sourcing data.

To view the Data Source details, click **Action** icon next to corresponding Workspace and select **View**.

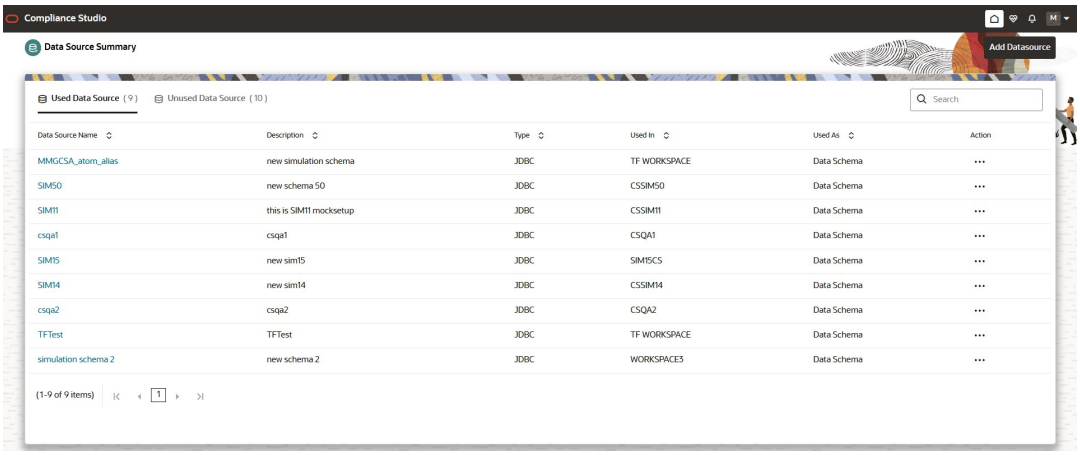
After Pre-configuration procedures you must add new data source in the compliance studio application.

> **Note**
>
> Add the production schema data source from where the data will be moved to the Simulation schema.

Follow the subsequent steps to add the new data source:

1. Click the **User** Icon.
2. Click **Data Source**. The **Data Source** page is displayed.
3. Click **Add Data Source** and enter the value for the following fields:
   - Data Source Name: Enter the workspace schema name.
   - Description: Enter the description of database connection.
   - Type: Enter the type of the database connection.
   - Database Type: Select the Database Type as Oracle.
   - Wallet Alias: Enter the Wallet Alias. This value should be same as configured using Oracle Wallet (`<NEW SCHEMA>_alias`)
   - Table Owner: Enter the table owner name (`<NEW SCHEMA>`).
4. Click **Test Connection** to check the status of the connection.
5. Click **Create** to create the Data Source or Click **Cancel** to skip the changes.

Figure 9-7 Data Source Summary Page



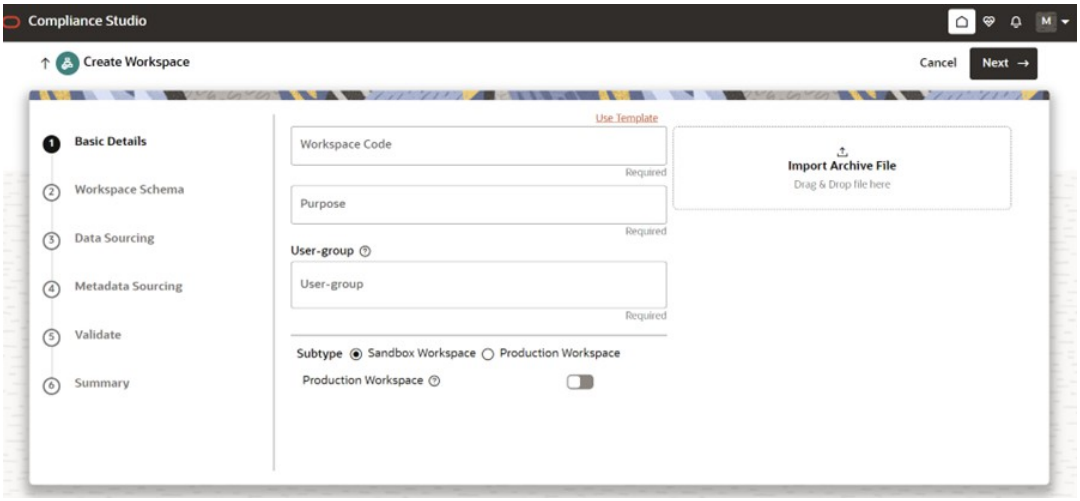
9.2.3 Workspace Creation

The Workspace creation requires entry of the source of dataset, validation, and deployment.

To create a Workspace, follow the subsequent steps:

1. Navigate to **Workspace Summary** page. The page displays workspace records in a table.
2. Click **Add Workspace**. The **Create Workspace** page is displayed.

Figure 9-8 Create Workspace



> **Note**
>
> The window displays a progress indicator at the left that indicates the active window where you are entering details. Click **Previous** to go back a step and click **Next** to go to the next step.

Use the pre-configured template to load the data base and metadata objects to the workspace.

To use the pre-configured template, follow the subsequent steps:

1. Click **Use template**. Use template pop up window is displayed.
2. Select `CSWorkspaceTemplate.zip` from the library drop-down. The Update schema mapping is displayed.
3. Select the following target schema field details:
   - New Data Schema: Enter/select the newly created schema ID.
   - New Data Source Name: Enter/select the production data source name.
4. Click **Update** to load the pre-configured template. Click **Cancel** to close the window. The following steps show the various phases from workspace creation to deployment:
   a. Configuring Basic Details
   b. Configuring Workspace Schema
   c. Configuring Metadata Sourcing
   d. Validating Workspace
   e. Displaying Summary

Configuring Basic Details

To configure the basic details follow the subsequent steps:

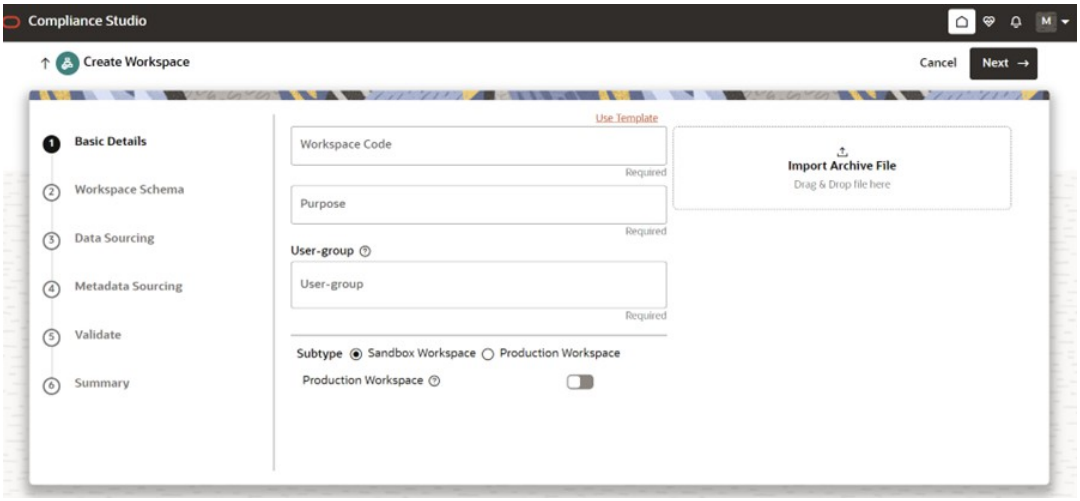
1. Enter the value for the fields displayed in the Basic Details table.
2. Click **Next** to open the next page.

> **Note**
>
> The field drop down values are populated based on the registration in the OFSAA Environment and the template.

Table 9-3 Basic Details

Fields	Description
Workspace Code	Enter the code of the workspace. This field is limited to 20 characters.
Purpose	Enter he purpose of the creation of the Workspace.
User group	Click the user group field to display a list of User-group values. Select the required value. • Modeling Approver • Modeling Reviewer • Modeling User
Type	Select the type of Workspace as Modeling or Simulation.
Sub Type	If you have selected Modeling, select the subtype of Workspace as Sandbox Workspace or Production Workspace.
Application Type	Select Customer Screening
Production	The CS Production drop down value will be populated as a result of registering the OFSAA Environment Details.
Simulation	The CS Simulation drop down value will be populated as a result of registering the OFSAA Environment Details.
Simulation Infodom	Enter Infodom name (<<Simulation Infodom>>).
Simulation User Group Code	Enter the User Group Code. This field is limited to 20 characters.
Simulation User ID	Enter the User ID. This field is limited to 20 characters.
Simulation User Password	Enter the User Password.
Simulation DB Server	Enter the Simulation fic server IP address.
Simulation DB Schema name	Enter simulation Schema name (<NEW SCHEMA>).
Simulation DB Password	Enter the password (<NEWSCHEMA PASS-WORD>).
Simulation Jdbc Connection String	Enter the connection Sting (Example: <oracle-driver>@<hostipadress>:<dbport>/<servicen- ame>).

Figure 9-9 Create Workspace



Configuring Workspace Schema

Select the schema operation and enter connection details. No configuration required if you are using the template.

Configuring Data Sourcing

The schema type selected in the previous step requires the definition of database objects to be used for model creation. The data sourcing step of Workspace provisioning allows the select tables from Hive-based data sources from which data has to be pulled into the Oracle-based Workspace data schema.

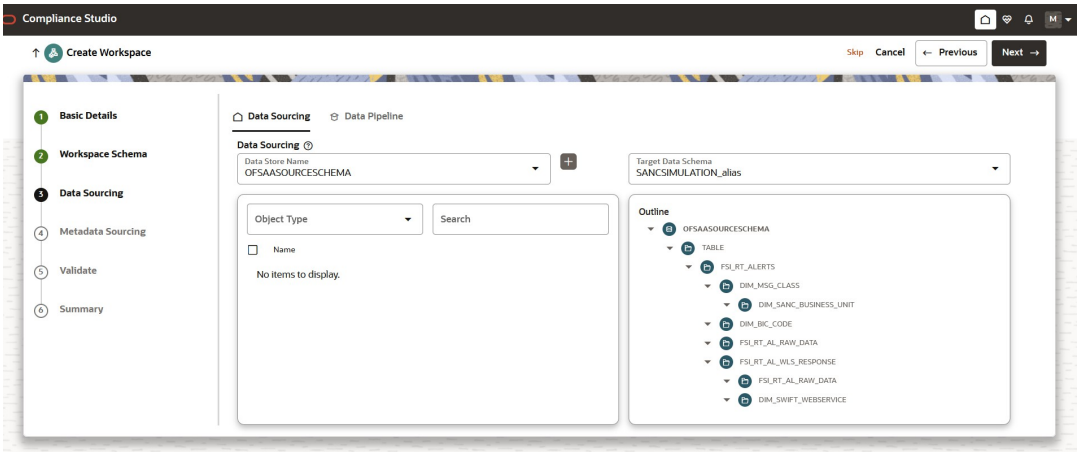
In case any of the selected tables are not present in the target schema, those tables are included in the failed objects count in the workspace provisioning summary.

As a part of using the template, all the CS specific data sourcing objects are available by default.

If you are not using the template, follow the subsequent steps and enter the value manually to configure the Data Sourcing:

1. Select a **Data Source** from the Data Source Name drop-down list.
2. Select the **Target Data Schema**.
3. Select the object type and corresponding object names from the drop down list.
4. Click **Previous** to go back a step and click **Next** to go to the next step.

Figure 9-10 Data Sourcing



Configuring Metadata Sourcing

The Metadata Sourcing is a stage during Workspace provisioning to allow seeding of metadata like scheduler batches at the time of workspace provisioning.

To configure Metadata Sourcing, select the CS specific schema from the Object Type drop-down list and corresponding available objects.

As a part of using the template, all the CS specific metadata sourcing objects are available by default.

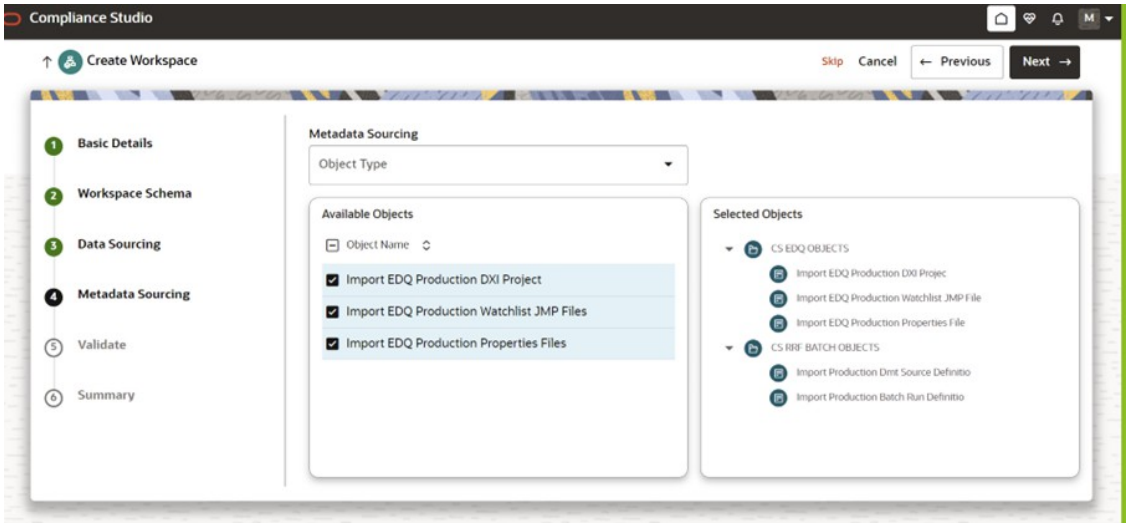
If you are not using the template, following the *Metadata Sourcing Object Type* and Names table and select the metadata objects manually.

Click **Previous** to go back a step and click **Next** to go to the next step.

Table 9-4 Metadata Sourcing Object Type and Names

Object Type	Object Name
CSEDQ OBJECTS	Import EDQ Production DXI Project
-	Import EDQ Production Watchlist JMP Files
-	Import EDQ Production Properties Files
CSRRF BATCH OBJECTS	Import Production Dmt Source Definition
-	Import Production Batch Run Definition

Figure 9-11 Metadata Sourcing



Once all the meta data objects are successful, perform the Mandatory Configuration for imported EDQ project.

Validating Workspace

The **Validate** pane displays a preview of the configuration values entered in the previous panes. Click **Previous** to go back a step and click **Next** to go to the next step.

Displaying Summary

The **Summary** pane displays the status of the workspace creation. Click Download to download the deployment report.

9.2.4 Workspace Creation Post-Configuration

Do the subsequent configuration in the CS application after the Workspace creation.

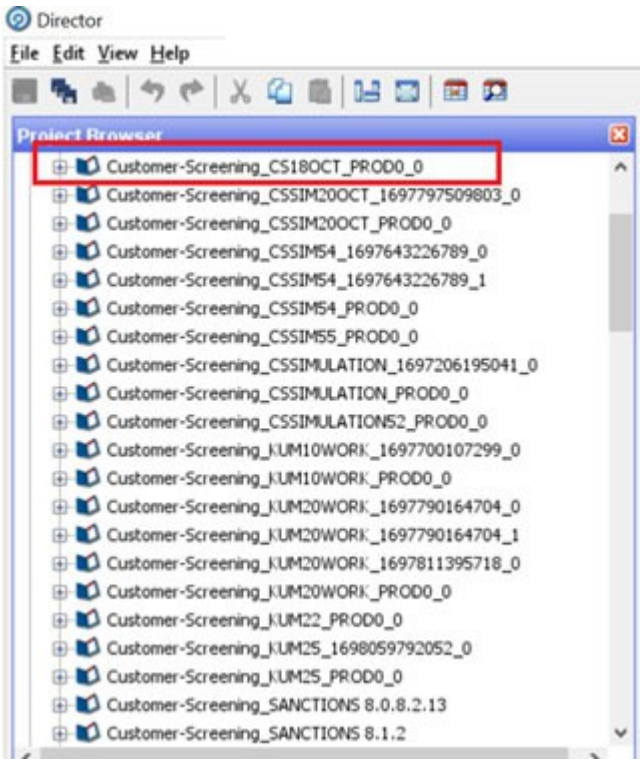
Mandatory Configuration for imported EDQ project

This is a one-time manual activity that must be done once the EDQ dxi project is transferred from production to the Simulation EDQ director.

Follow the subsequent steps:

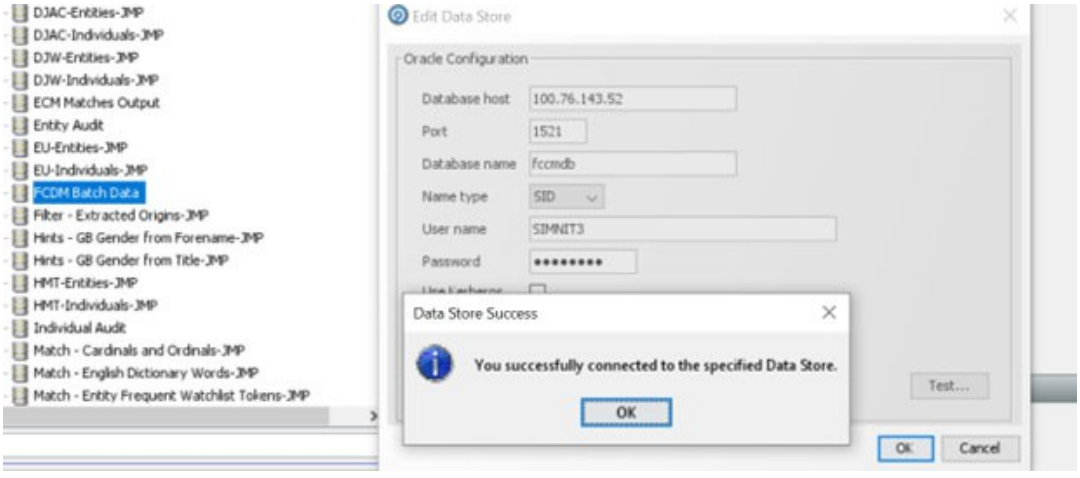
1. Go to the EDQ project in the simulation EDQ director.

Figure 9-12 EDQ Director



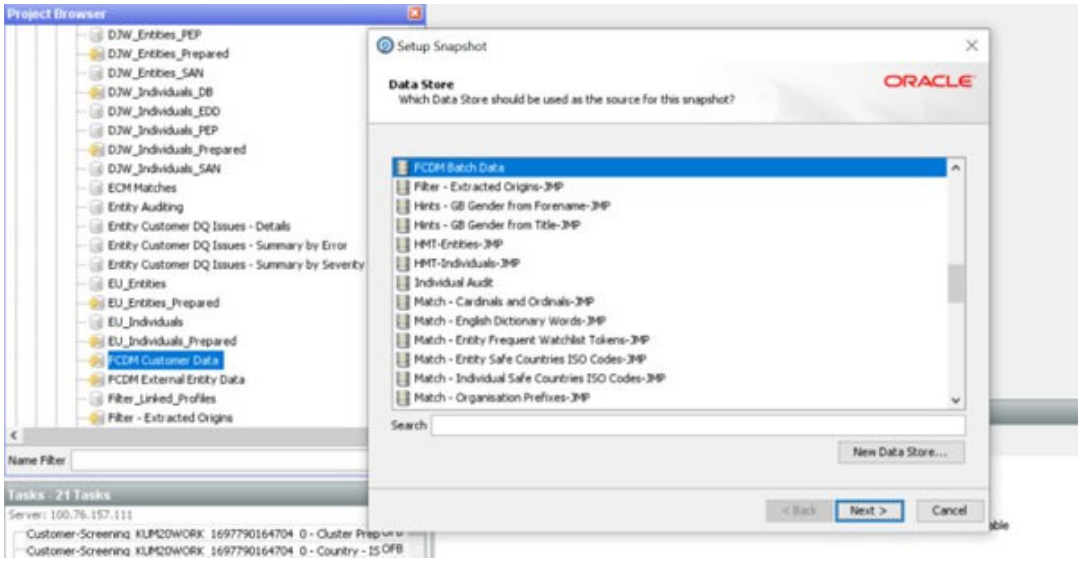
2. Click **Data Stores** and click **FCDM Batch Data**. The Edit Data Store window is displayed.
3. Give the simulation database details and click **Test** to connect to the specific Data Store.
4. Click **Ok**.

Figure 9-13 Edit Data Store Window



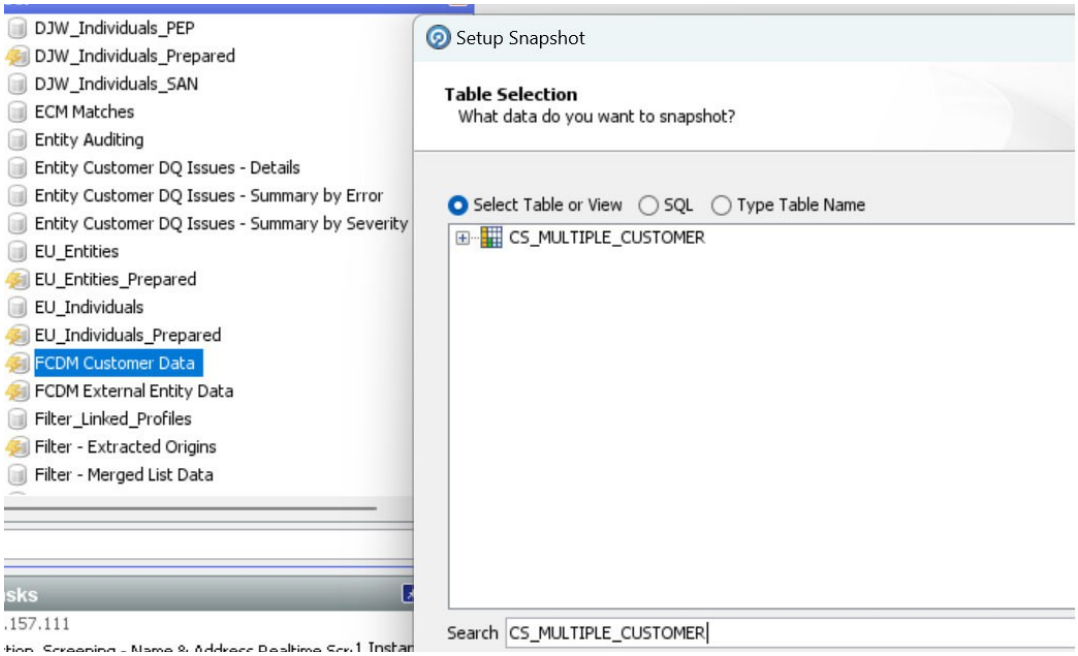
5. Click Simulation EDQ project **Staged Data** and click on **FCDM Customer Data**. The data Store window is displayed.

Figure 9-14 Data Store Window



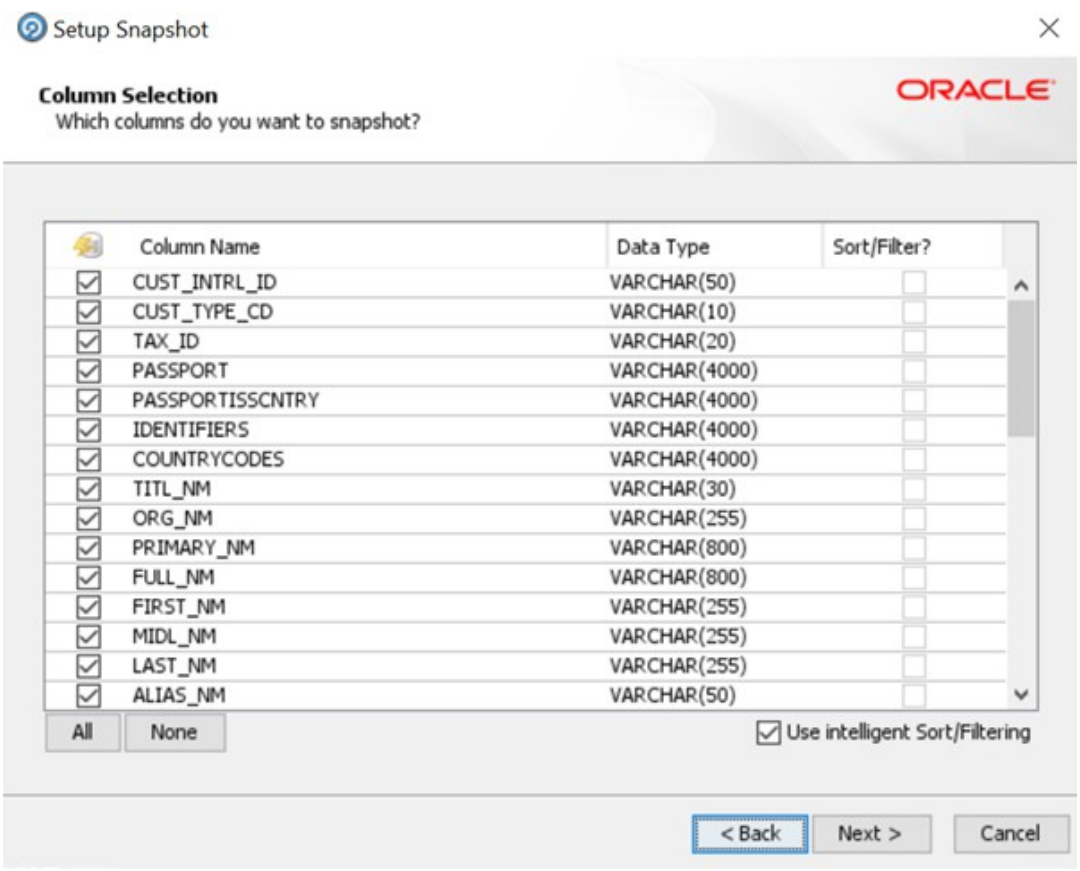
6. Click **Next**. The Table Selection window is displayed.

Figure 9-15 Table Selection Window



7. Select the table or view and click Next. The Column Selection window is displayed.

Figure 9-16 Column Selection



8. Search for `cs_multiple_customer` and select `cs_multiple_customer`.
9. Click **Next**. The Snapshot Name window is displayed.
10. Click **Finish** to save the updates.

Importing Workspace Metadata for ML4AML for the created Workspace

1. Login to Compliance Studio installed UNIX Machine.
2. Navigate to the following path: `/deployed/ml4aml/bin`
3. Execute the following UNIX command once, against the schema used in the current Sandbox workspace:`./importWorkspaceSQL.sh -w <NEW_SCHEMA>_alias`

> **Note**
>
> `<NEW SCHEMA>` is the placeholder to be replaced with the actual value used to create the workspace.

9.3 Managing a Workspace

The workspace displays a menu for Models and an application configuration and model creation sub-menu. For more information on the subsequent topics, see Managing Workspaces section in Oracle Financial Services Compliance Studio User Guide.

- Launching a Workspace

- Viewing the Workspace
- Editing the Workspace
- Deleting the Workspace
- Downloading the Workspace

9.3.1 Populating the Workspace

The workspace is populated with data from source data schema to target data schema. When you are creating a workspace the table definitions are created. The Data movement from production to simulation happens when you populate the screen.

To populate the Workspace, follow these steps:

1. Navigate to the **Workspace Summary** page.
   The page displays Workspace records in a table.
2. Click Action  next to corresponding Workspace and select Populate Workspace to populate the Workspace  with data from source data schema to target data schema in the Populate Workspace window.
3. You ca use the pre-configured template to auto populate the field values and filters. click Use Template and select `CSJurisdictionFilterTemplate.zip` file from the library list to auto populate the values.

   > **Note**
   >
   > You must replace the SQL Filter (`$JRSDCN_CD$`) value with the jurisdiction.

4. You can enter the field values manually. For reference, see the Populate Workspace table.

Figure 9-17 Populate Workspace Window

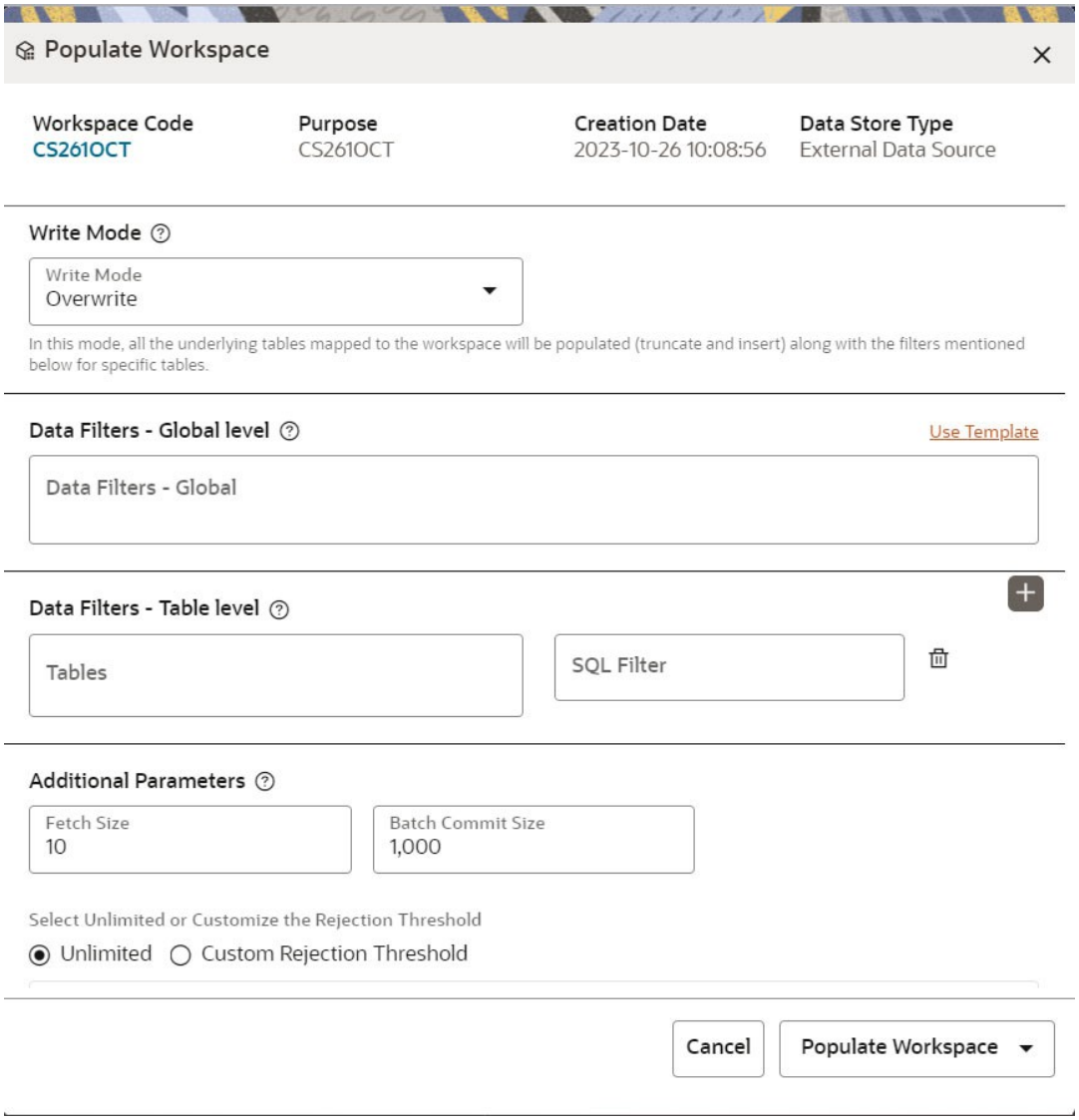


Table 9-5 Populate Workspace

Field	Description
Workspace Code	The code of the Workspace.
Purpose	The description for the Workspace.
Creation Date	The date on which the Workspace was created.
Data Source Type	The source of data. The value can be the OFSAA Data Schema or an external data source.
Data Filter - Global	Enter the data filter that needs to be applied on all the tables selected for data sourcing. For example: If MISDATE is equal to Today, then it is applied to all tables (wherever it is available) for selected Data Sources during population. If this field is not found (MISDATE) in the tables, it is not updated.

Table 9-5 (Cont.) Populate Workspace

Field	Description
Data Filter - Table level	Provide the data filters individually on the tables here. **NOTE:**You can provide multiple table names for the same SQL filter. For example, there are two tables called Student and Employee in the target data source, and below filters are applied: • MISDATE as Today for Student and Employee tables • ID as 1 for Student table Then,Student table will be populated with MISDATE and ID filters and Employee table will be populated with only MISDATE filter. Global Filters will not be applicable for those tables on which filters have been applied individually. If the same table name is provided in more than one rows here, then filter condition is generated as a conjunction of all the provided filters.
-	
Fetch Size	Enter the Fetch size of JDBC properties for data upload
Batch Commit Size	Enter the Batch Commit size of JDBC properties for data upload
Write Mode	Populate the workspace in **append**mode.
Rejection Threshold	Following two options are available: • Custom Rejection Threshold Enter the maximum of number of inserts that may fail for any of the selected tables. You can provide the maximum number of inserts that can fail while loading data to a given table from all the sources. In case of threshold breach, all the inserts into the particular target schema will be rolled back. However, it will continue with populating the next target schema. • Unlimited Here,all the errors will be ignored during the data population.
Data Load	Available options are SELECTIVE and ALL. Use ALL for first time data population

5. Click **Populate Workspace** to start the process.

You can create the batch using Create Batch, or create and execute using Create and Execute Batch option. On selecting either of these options, a workspace population task gets added to the batch.

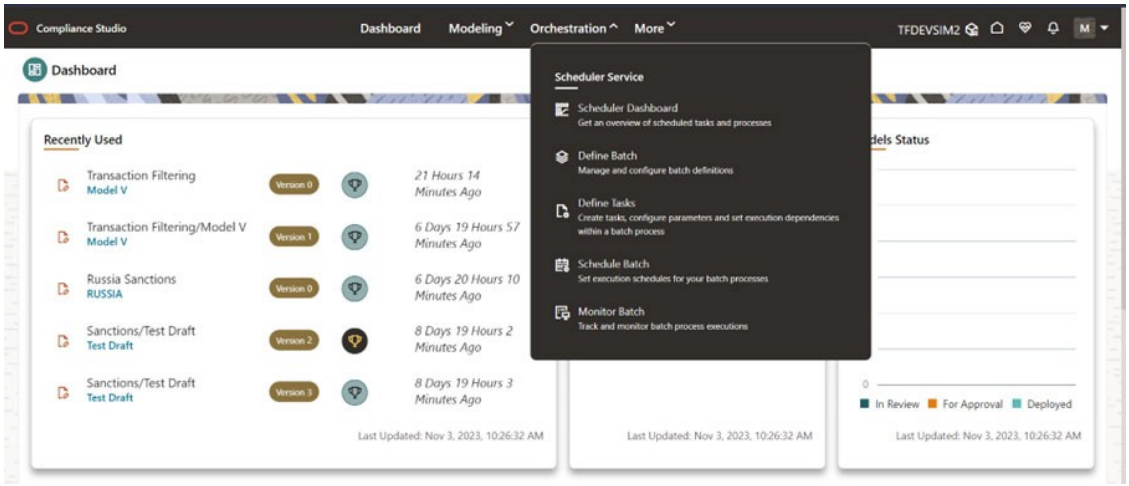
> **Note**
>
> You may require approval from an approver to populate the workspace.

- When you select Create and Execute Batch option, it allows you to create batch and triggers the batch as well.
- When you select 'Create Batch' option, it allows you to prepare the batch and then execute or schedule the batch at a later time through Scheduler Service window.

The Workspace population task execution can be tracked in the 'Monitor Batch' window. For more information on Scheduler Service and Workspace population task execution, see Oracle Financial Services Compliance Studio User Guide.

> **Note**
>
> - You can only run the workspace population for once.
> - Any table that is deselected from the data sourcing definition will **NOT** be dropped.

Figure 9-18 Accessing Scheduler Service from Dashboard



9.4 Managing Model Pipelines

Model Pipeline allows you to create and publish models based on the workspaces created from datasets in the database. The published models are then deployed in production to be consumed by users. For the subsequent information on model pipelines, see Managing Model Pipelines section in Oracle Financial Services Compliance Studio User Guide.

- Prerequisites
- Access the Workspace Dashboard Window
- Accessing the Model Pipelines
- Reviewing, Approving Model
- Import a Workspace Model Data into a New Model
- Import/Export Models
- Using View Models
- Editing Models

- Deleting Objectives and Draft Models
- Creating Seeded Models

9.4.1 Creating a Model

Model creation and deployment undergoes a workflow of Model Governance where the following types of users in the system have privileges that restrict the activities, they can do in the model creation and deployment workflow.

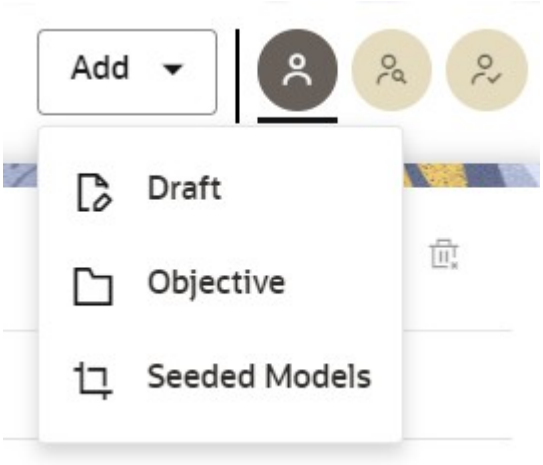
Creating Objective (Folders)

Create folders called Objectives within which you can create Models.

To create an Objective, follow these steps:

1. Click Launch Workspace next to corresponding Workspace to Launch Workspace and display the **Dashboard** window with application configuration and model creation menu.
2. In the Mega menu, click **Modeling** and select **Pipelines** from the drop down to display the **Model Pipeline** window.
3. Click **Add** and select **Objective** from the list to display the **Objective Details** dialog box.

Figure 9-19 Select Objective from Add



4. Enter details in Objective **Name** and **Description** fields in the Add **Objective** dialog box.
5. Click **Save**.

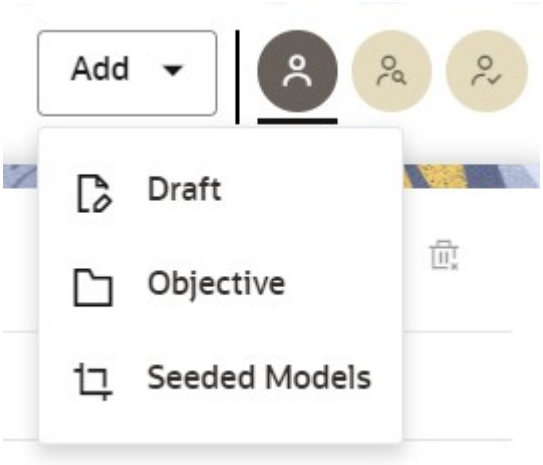
Creating Draft Models Using Seeded Model

Create Models that are classified as draft models. These models will be reviewed before being sent for Scoring.

To create a draft Model, follow these steps:

1. Click Launch Workspace next to corresponding Workspace to Launch Workspace and display the **Dashboard** window with application configuration and model creation menu.
2. Open the Objective.
3. Click **Add** and select **Draft** from the list to display the **Add Draft** dialog box.

Figure 9-20 Select Objective from Add



4. **Create New Model** is the default setting in the **Model Details** dialog box.
To create a new model, follow these steps:

   a. Click **Use Template**.

   b. Select the CS Simulation zip file from the templates. The available CS templates are:

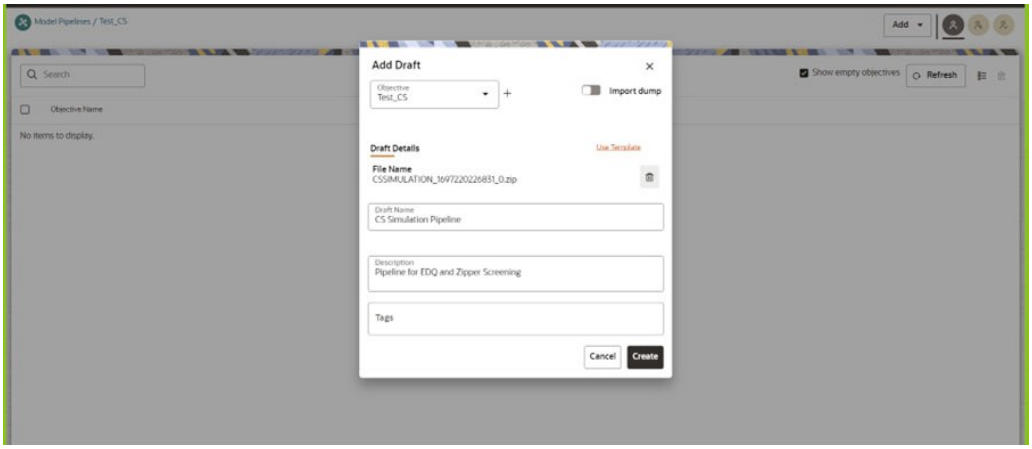
      - CSWLSIMULATION_1697221476336_0.zip (CS Watchlist Screening pipeline, see *CS Watchlist Screening Pipeline* Figure)
      - CSSIMULATION_1697220226831_0.zip (CS Simulation pipeline, see *CS Simulation Pipeline* figure)
      - CSNOPRODSIMULATION_1701856523642_0.zip (Customer Screening Staged Data Simulation Pipeline)

Table 9-6 CS Pipeline and Associated Widgets

Pipeline	Widgets
CSSIMULATION_1697220226831_0	Customer Screening Batch EDQ
-	Data Load Event Generation Batch
-	L1Alert Generation Batch
-	CS Simulation Statistics
-	CS Simulation Results
-	CS Production Results
CSWLSIMULATION_1697221476336_0	Watchlist Management Batch EDQ
-	Watchlist Management Batch
CSNOPRODSIMULATION_1701856523642_0	Business Data Load Batch
-	Customer Screening Batch EDQ
-	Data Load Event Generation Batch
-	L1Alert Generation Batch
-	CS Simulation Statistics
-	CS Simulation Results

   c. Enter details for Draft Name and Description.

Figure 9-21 Model Details - Create New Model



d. Enter a tag in the **Tags** field.

e. Click **Create**. a model pipeline will be created from the template.

To clone the objects for Batch EDQ and Batch RRF Widgets, follow the subsequent steps:

a. Navigate to the **Design Pipeline** page.

b. From the pipeline canvas double click on the widget to open the widget details screen on the right side.

c. In the widget screen under the Custom Parameters tab, click **Copy** to open the **Clone Objects** Window.

d. Select the source model ID from the **Clone Objects** Window and select the version from which you want to clone the widget.

> **Note**
>
> Select the model ID as PROD. For the Batch EDQ widget, the model ID is PRODi (Example: PROD0, PROD1) based on the input in the `PROD_edq_project_name` Key.

e. Click **Copy**. The CS Widget clone process begins. Once the cloning is completed, the current model ID and version will automatically be populated in the widget screen.

f. Click **Save** to save the widget.

Cloning a Model

You can pick any published model and clone the contents to a new draft in the same objective or clone the content to the current parent draft. The cloned draft can be edited and used further. Audit Trail window also captures the clone information.

To clone the model details, follow these steps:

1. Open a Published Model in Pipeline Designer.
2. Select **Clone to new Draft** to Re-image parent draft with current.

9.5 Model Pipeline

Modeling refers to the process of designing a prototype based on a structured data model for statistical analysis and for simulating actual events and functions. A user with access to the Workspace can create or modify models in a workspace. Model versions are preserved in the Workspace, along with execution and output histories. Once a model has been validated in the Workspace and considered fit for use, modelers can request to push the Model into the production environment.

The following sections are available on the Model Pipeline window:

- Pipeline
- Dashboard
- Notebook
- Simulations
- Execution History
- Compare

9.5.1 Pipeline

A pipeline is an embedded data processing engine that runs inside the application to filter, transform, and migrate data on-the-fly. Pipelines are a set of data processing elements called widgets connected in series, where the output of one widget is the input to the next element. Use the Pipeline canvas to create the model and execute the pipeline using widgets.

To create a paragraph using pipeline, follow these steps:

1. Navigate to the **Pipeline Designer** page. Pipeline Canvas is displayed.
2. Click on the Connector  to display the widgets.
3. Select Customer Screening from the list.
4. Select a widget and add the widget to the pipeline canvas. For information on widgets, see the *CS Pipeline Widgets* table.
5. From the pipeline canvas double click on the widget to open the widget details screen on the right side.
6. In the widget screen under the Custom Parameters tab, click **Copy** to open the **Clone Objects** Window.
7. Select the source model ID from the **Clone Objects** Window and select the version from which you want to clone the widget.

> **Note**
>
> Select the model ID as PROD. For the Batch EDQ widget, the model ID is PRODi (Example: PROD0, PROD1) based on the input in the `PROD_edq_project_name` Key.

8. Click **Copy**. The CS Widget clone process begins. Once the cloning is completed, the current model ID and version will automatically be populated in the widget screen.

> **Note**
>
> Cloning of Watchlist-Management and Customer-Screening project should not be configured in the same pipeline.

9. Click **Save** to save the widget.
10. Click **Add** the next widget and repeat from step 2 to step 8.

Figure 9-22 CS Simulation Pipeline

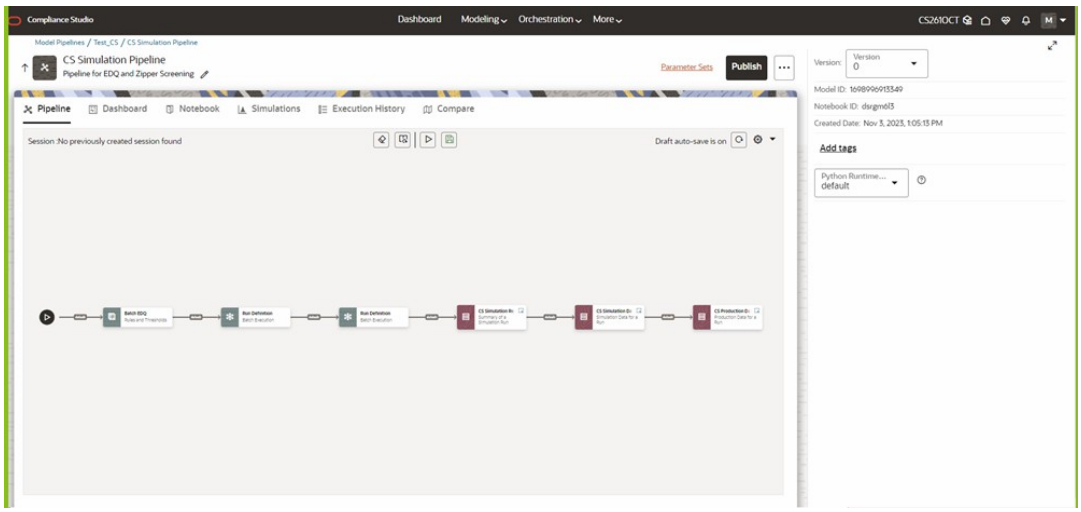


Figure 9-23 CS Watchlist Screening Pipeline

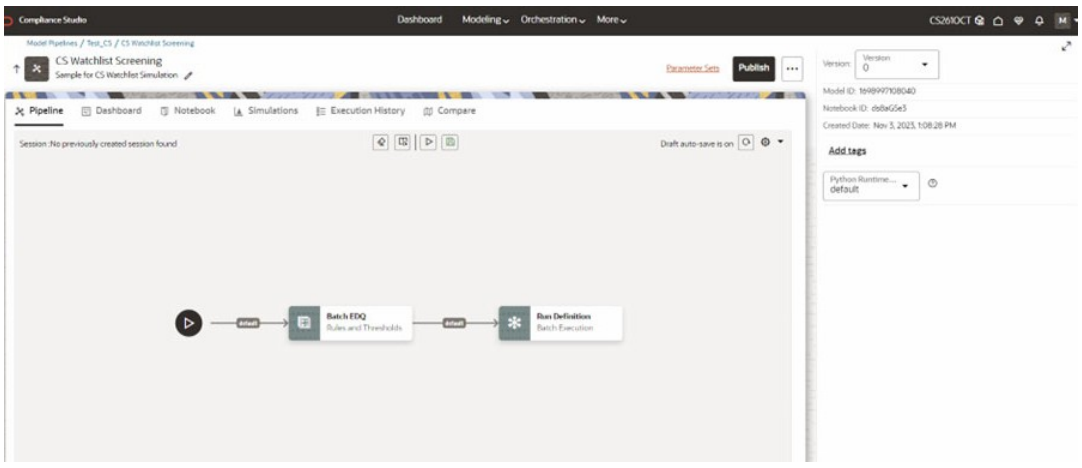


Figure 9-24 Customer Screening Staged Data Simulation Pipeline

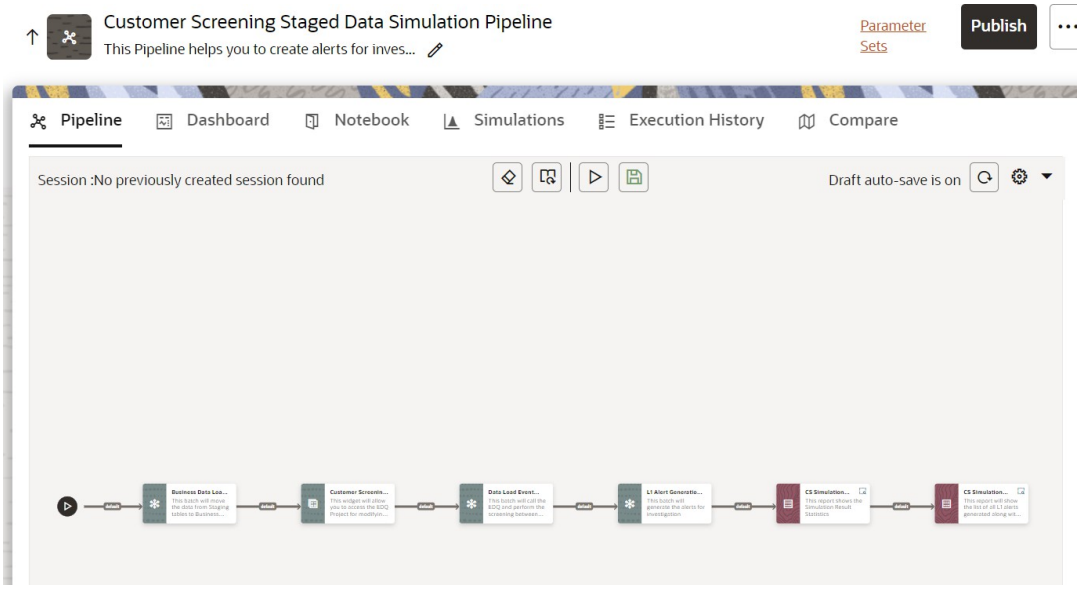


Table 9-7 CS Pipeline Widgets

Widget	Description
Customer Screening Batch EDQ	This widget will allow you to access the EDQ Project for modifying the matching configurations.
Data Load Event Generation Batch	This batch will call the EDQ and perform the screening between Customer and Watchlist data to generate the matches in simulation schema.
L1Alert Generation Batch	This batch will generate the alerts for investigation.
CS Simulation Statistics	This report shows comparison between Production Results and Simulation Results for the same input
CS Simulation Results	This report shows the list of all L1 alerts generated along with the events for a Simulation Run.
CS Production Results	This report shows the list of all L1 alerts generated along with the events in Production Environment for the same input.
Watchlist Management Batch EDQ	This widget will allow you to access the EDQ Project for modifying the watchlist configurations.
Watchlist Management Batch	This batch will call the EDQ and load the watchlist data.
Business Data Load Batch	This batch will move the data from Staging tables to Business tables.
Customer Screening Batch EDQ	This widget will allow you to access the EDQ Project for modifying the matching configurations.
Data Load Event Generation Batch	This batch will call the EDQ and perform the screening between Customer and Watchlist data to generate the matches in simulation schema.

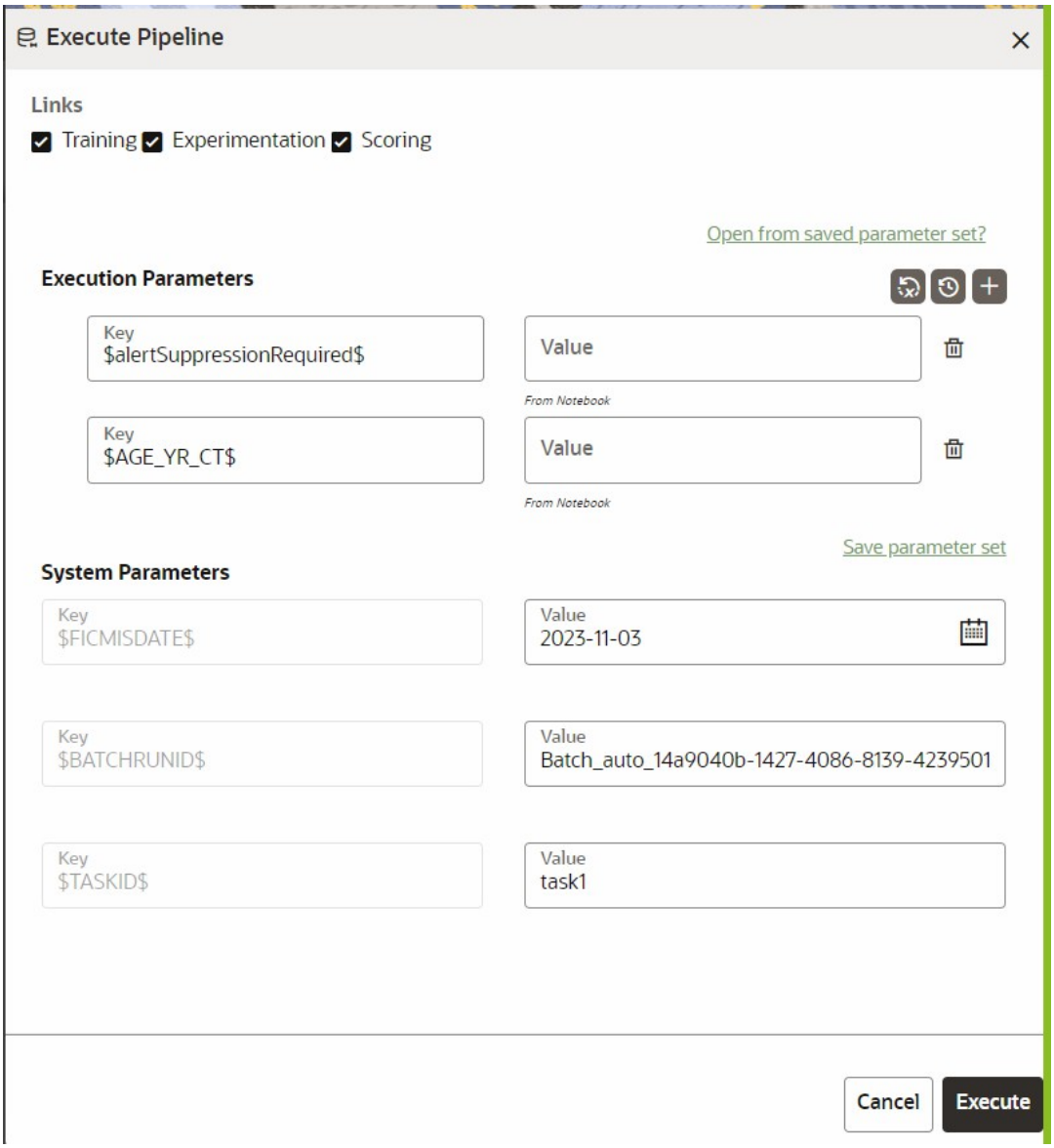
Table 9-7 (Cont.) CS Pipeline Widgets

Widget	Description
L1Alert Generation Batch	This batch will generate the alerts for investigation.
CS Simulation Statistics	This report shows the Simulation Result Statistics.
CS Simulation Results	This report will show the list of all L1 alerts generated along with the events for a Simulation Run.

To execute the pipeline follow the subsequent steps:

1. Click execute  . Execute Pipeline window is displayed.

Figure 9-25 Execute Pipeline



2. Click **Open from saved Parameter set?** to import the template.
3. If your not importing the template enter Enter the execution Key and Value manually.

> **Note**
>
> Select the flow, which you want to execute Scoring, Training, and Experimentation. It displays all the keys defined for all the paragraphs in the notebook with a placeholder for providing the values.

4. You can add new parameters using Add  .

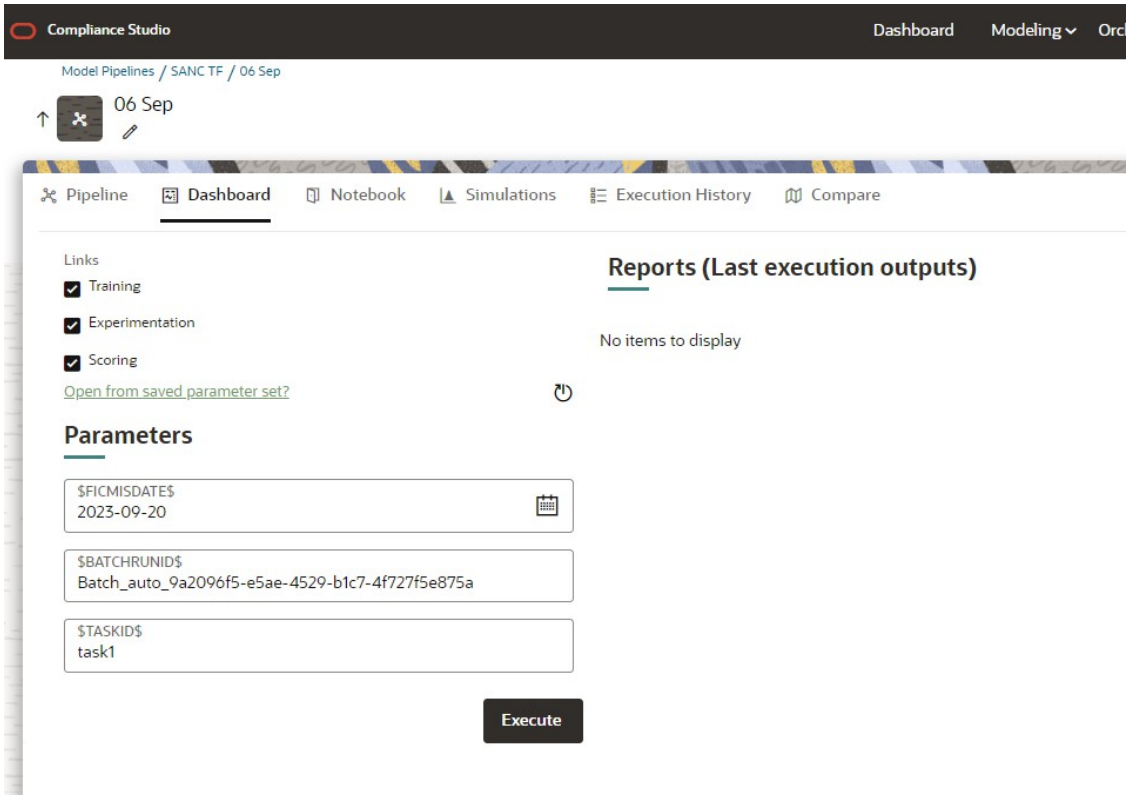
> **Note**
>
> If the parameter is not defined in the notebook, it will not be used for the execution. In case of multi select, if there are common parameters among the chosen scenarios, it will take the value based on the order of selection. that is first chosen scenario parameter will be taken.

5. But if open from saved scenarios again (not on single go), then already added will get replaced by the newly added (same as what existed)
6. Execution is performed based on selected link types. It filters out all the not required/ unused parameters. And, all the unused parameters for the current execution are displayed with a warning  . To view the only required parameters, click **Show only required** link.
7. Click Reset  to reset the entered data.
8. Click Delete  to delete the entered Key and Value.
9. Click **Execute** to initiate the execution. The widgets in pipelines are executed sequentially and you can see  icon on each widget for a successful execution. For individual widget execution details click the widget and click **View Details**.

9.5.2 Dashboard

The Dashboard of the Pipeline Designer allows you to execute shows the execution output of the Model.

Figure 9-26 Dashboard Tab

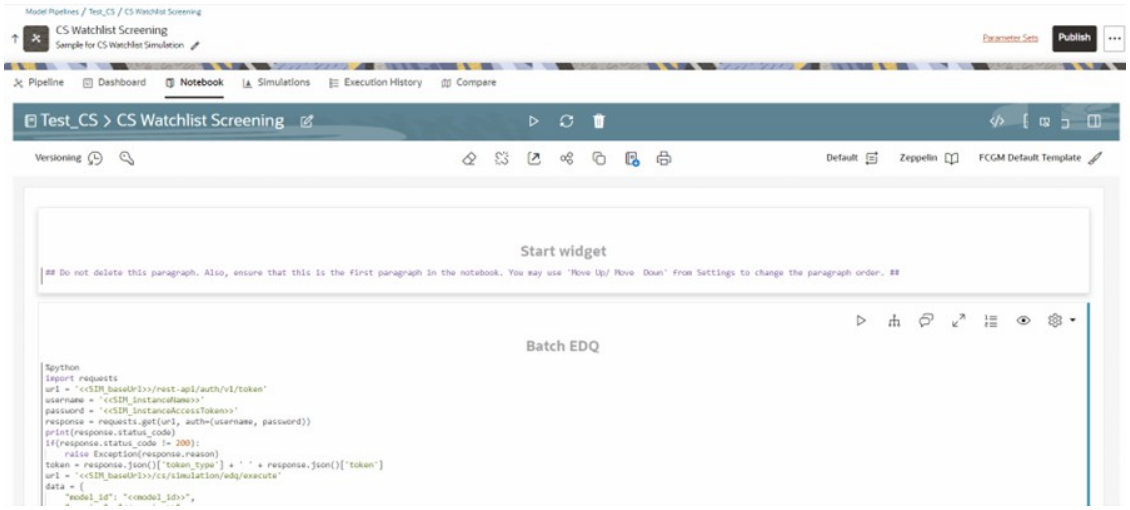


9.5.3 Notebook

Navigate to Notebook tab to view the paragraphs. You can run, invalidate session, edit, add, and export the notebook in the Notebook tab.

> **Note**
>
> By default the code is not displayed in the UI. To display code in the UI, click the visibility icon and select code.

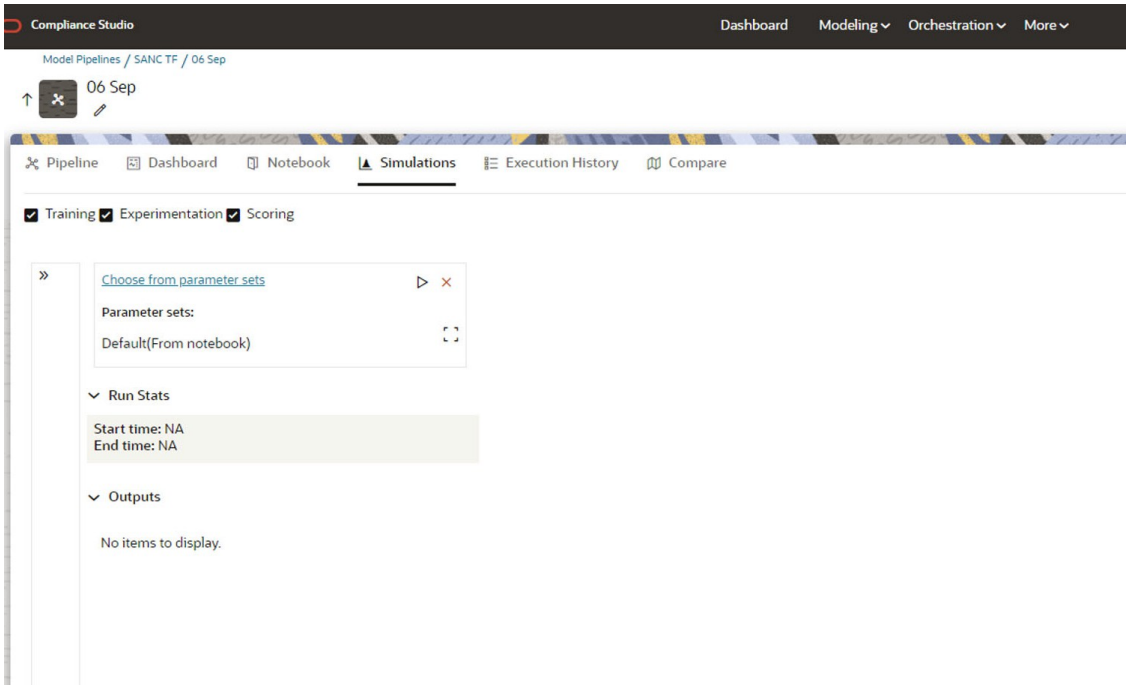
Figure 9-27 Notebook Tab



9.5.4 Simulations

The simulation flow allows for iterative execution along that path with input drivers (variables) that are passed through a parameter set. You can either create a new parameter set or use the existing parameter set and execute it from this tab.

Figure 9-28 Simulation Tab

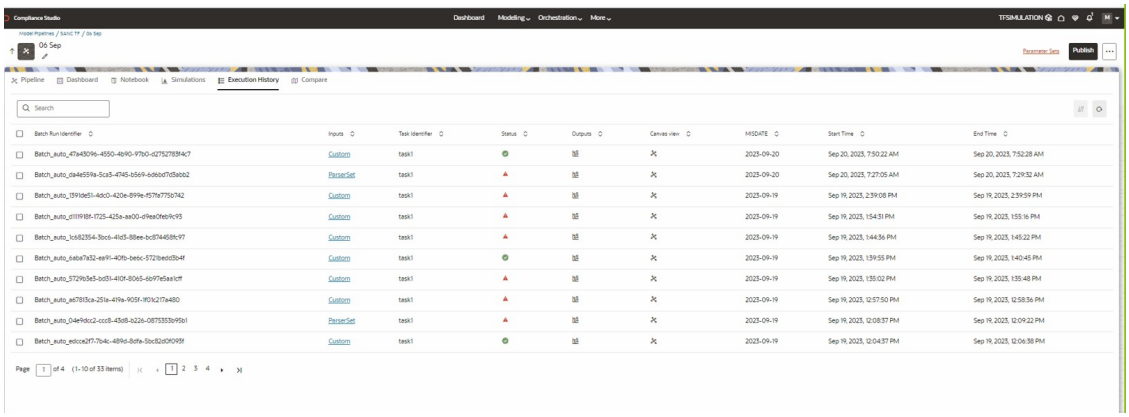


9.5.5 Execution History

This section of Pipeline Designer shows the history of the executions of the current pipeline. You can view the list of executions, check the report for the corresponding simulation run, and

extract the report. You can compare multiple executions by selecting multiple executions and click on Compare icon.

Figure 9-29 Execution History Tab



To download the report follow the subsequent steps:

1. Click the output icon for the respective batch. Output Details Page is displayed. Following Output report tiles are displayed
   - Start Widget
   - CS Specific widget
   - Report Widget
2. From the Report Widget tile click the download icon to download the report in the text file format.

> **Note**
>
> You must open the extracted report file in Excel or drag and drop the file in Excel to view the Simulation output.

Figure 9-30 Report Extraction Tile

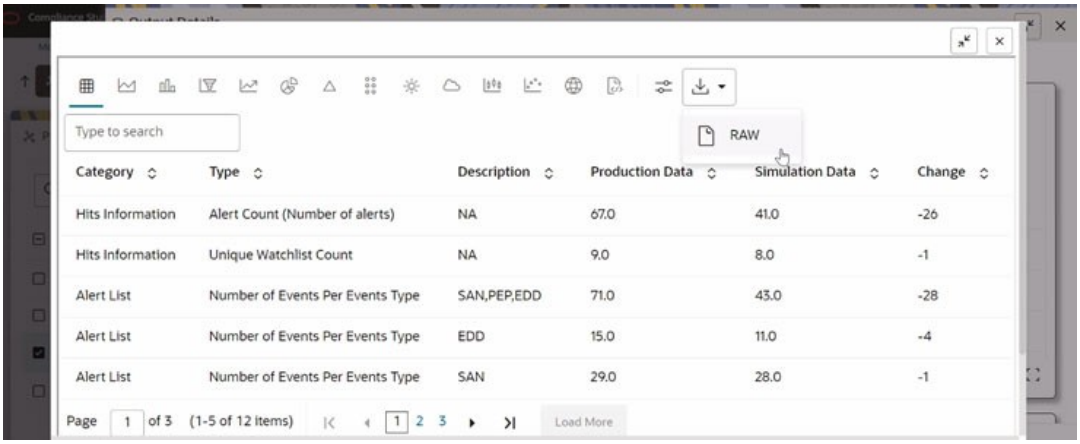


Figure 9-31 Extracted Output Sample

Category	Type	Description	Production Data	Simulation Data	Change
Hits Information	Number of Alerts in each web service	Name and Address	2	1	-1
Hits Information	Number of Alerts in each web service	Narrative	5	2	-3
Hits Information	Alert Count (no of Ierts)	NA	5	2	-3
Hits Information	Unique WL Count	NA	4	1	-3
Hits Information	No of Events Per Events Type - TF	SAN	100	102	2
Hits Information	No of Events Per Events Type - CS	SAN, EDD, PEP	100	75	-25
Hits Information	No of Events Per Events Type - CS	SAN	50	7	-43
Hits Information	No of Events Per Events Type - CS	EDD	10	8	-2
Hits Information	No of Events Per Events Type - CS	PEP	10	2	-8
Hits Information	Exemption Recommendation TF	Total Events Exempted	30	5	-25
Hits Information	Exemption Recommendation TF	Total Events Exempted - Narrative	7	3	-4
Hits Information	Exemption Recommendation TF	Total Events Exempted - Name	3	2	-1
Hits Information	Exemption Recommendation TF	Total Events Not Exempted	10	12	2
Hits Information	Exemption Recommendation TF	Total Events Not Exempted - Narrative			
Hits Information	Exemption Recommendation TF	Total Events Not Exempted - Name			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against SAN	5	10	5
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against PEP	3	3	0
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against EDD			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against PRB			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of alert have hits against SAN & PEP & EDD & PRB			
Hits Ratio	Ratio of alerts generated between 2 changes TF On	% of Zipper alert have hits against SAN	100	150	1
Alert List	No of alerts per jurisdiction (Juris Name)	Germany	10	5	-5
Alert List	No of alerts per jurisdiction (Juris Name)	India	5	2	-3
Alert List	No of alerts per biz domain (dom Name)	Domain A	10	5	-5
Alert List	No of alerts per biz domain (dom Name)	Domain B	5	10	5
Alert List	No of alerts per Message Type/ tag	MT10159a	200	50	-150
Alert List	No of Hits Generated Per Customer Type, CS	Individual	7000	8000	1000
Alert List	No of Hits Generated Per Customer Type, CS	Entity (organisation)	8000	7000	-1000
Alert List	No of Hits Generated Per WL Entity Type, TF	Individual	8000	7000	-1000
Alert List	No of Hits Generated Per WL Entity Type, TF	Entity (organisation)	8000	7000	-1000

Compare

The Compare option allows you to compare the executions with champion model.

To compare, follow these steps:

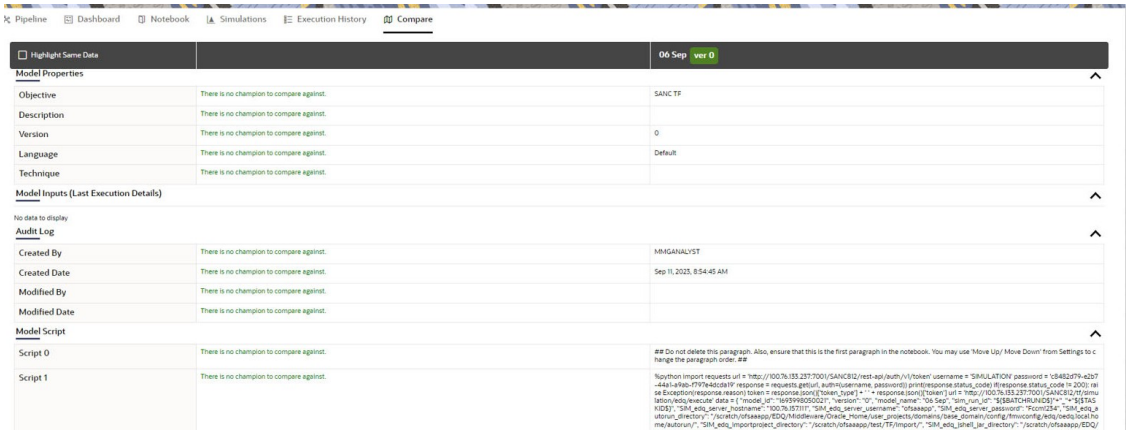
1. Navigate to Execution Summary window.
2. Select the executions using the corresponding check-boxes.
3. Click Compare

The Execution Comparison window is displayed.

The Window shows the following comparison details:

- Model Properties
- Model Input (Last Execution Details)
- Audit Log
- Model Script
- Model Output (Last Execution Outputs)

Figure 9-32 Compare Tab



9.5.6 Report Extraction

You can view the output of the executions from all the tabs of the model pipeline. Execution History tab allows you to download the execution output to the local system. For more information, see Execution History.

> **Note**
>
> - You must open the report text file in excel or drag and drop in excel to view the output.
> - If the execution output is truncated, update the Zeppelin interpreter output limit. For more information, see Appendix R: Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMIT in Python Interpreter.

Figure 9-33 Extracted Output Sample

Category	Type	Description	Production Data	Simulation Data	Change
Hits Information	Number of Alerts in each web service	Name and Address	2	1	-1
Hits Information	Number of Alerts in each web service	Narrative	5	2	-3
Hits Information	Alert Count (no of Ierts)	NA	5	2	-3
Hits Information	Unique WL Count	NA	4	1	-3
Hits Information	No of Events Per Events Type - TF	SAN	100	102	2
Hits Information	No of Events Per Events Type - CS	SAN, EDD, PEP	100	75	-25
Hits Information	No of Events Per Events Type - CS	SAN	50	7	-43
Hits Information	No of Events Per Events Type - CS	EDD	10	8	-2
Hits Information	No of Events Per Events Type - CS	PEP	10	2	-8
Hits Information	Exemption Recommendation TF	Total Events Exempted	30	5	-25
Hits Information	Exemption Recommendation TF	Total Events Exempted - Narrative	7	3	-4
Hits Information	Exemption Recommendation TF	Total Events Exempted - Name	3	2	-1
Hits Information	Exemption Recommendation TF	Total Events Not Exempted	10	12	2
Hits Information	Exemption Recommendation TF	Total Events Not Exempted - Narrative			
Hits Information	Exemption Recommendation TF	Total Events Not Exempted - Name			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against SAN	5	10	5
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against PEP	3	3	0
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against EDD			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against PRB			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of alert have hits against SAN & PEP & EDD & PRB			
Hits Ratio	Ratio of alerts generated between 2 changes TF On	% of Zipper alert have hits against SAN	100	150	1
Alert List	No of alerts per jurisdiction (Juris Name)	Germany	10	5	-5
Alert List	No of alerts per jurisdiction (Juris Name)	India	5	2	-3
Alert List	No of alerts per biz domain (dom Name)	Domain A	10	5	-5
Alert List	No of alerts per biz domain (dom Name)	Domain B	5	10	5
Alert List	No of alerts per Message Type/ tag	MT101 59a	200	50	-150
Alert List	No of Hits Generated Per Customer Type, CS	Individual	7000	8000	1000
Alert List	No of Hits Generated Per Customer Type, CS	Entity (organisation)	8000	7000	-1000
Alert List	No of Hits Generated Per WL Entity Type, TF	Individual	8000	7000	-1000
Alert List	No of Hits Generated Per WL Entity Type, TF	Entity (organisation)	8000	7000	-1000

9.5.7 Publishing a Pipeline

If your satisfied with the results of the execution you can publish the pipeline. Publish the pipeline will backup the current model pipeline with non editable mode. To publish the pipeline, follow these steps:

1. Click Launch Workspace  next to corresponding Workspace to Launch Workspace and display the **Dashboard** window with application configuration and model creation menu.
2. In the Mega menu, click **Modeling** and select **Pipelines**  from the drop down to display the **Model Pipeline** window.
3. Select the Objective from the list. The publish canvas is displayed.
4. Click **Publish**. Publish Pipeline pop-up is displayed.
5. Enter the field details. See the following Publish Pipeline table.

Table 9-8 Publish Pipeline

Field or Icon	Description
Model Name	The field displays the name of the Model. Modify the name if required.
Model Description	The field displays the description for the Model. Enter or modify the description if required.
Technique	Enter the registered technique to use.

Table 9-8 (Cont.) Publish Pipeline

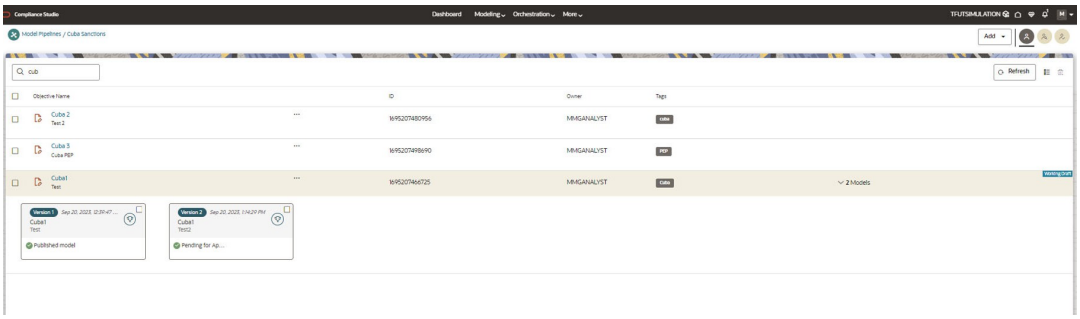
Field or Icon	Description
Run Version	Select a rub version.
Variable Mapping	The table displays the OFSAA variables and data sets used in the creation of the Training Model.
Script	The table displays the Paragraphs created in the Training Model. Select the Paragraphs that you want to use to create the Scoring Model. Track Output - Select this to track the output of the paragraph.

6. Select the required configuration and click **Publish**to publish the pipeline or click **Cancel**to go back to previous page.

To view the published model follow the subsequent steps:

1. Navigate to **Model Pipeline** page.
2. Click **Models** in-line with the Object Name. published models are displayed.

Figure 9-34 Published Model



The published models are then deployed in production to be consumed by users. The iterations of comparison between various models lead to the elimination of undesired models and the filter of a few robust ones that can be considered for deployment in production. Modelers then use their better judgment to consolidate their choice and fix on one model - the champion model. The champion model is also called the scoring model or the actual model in this document.

9.5.8 Deploying the Model

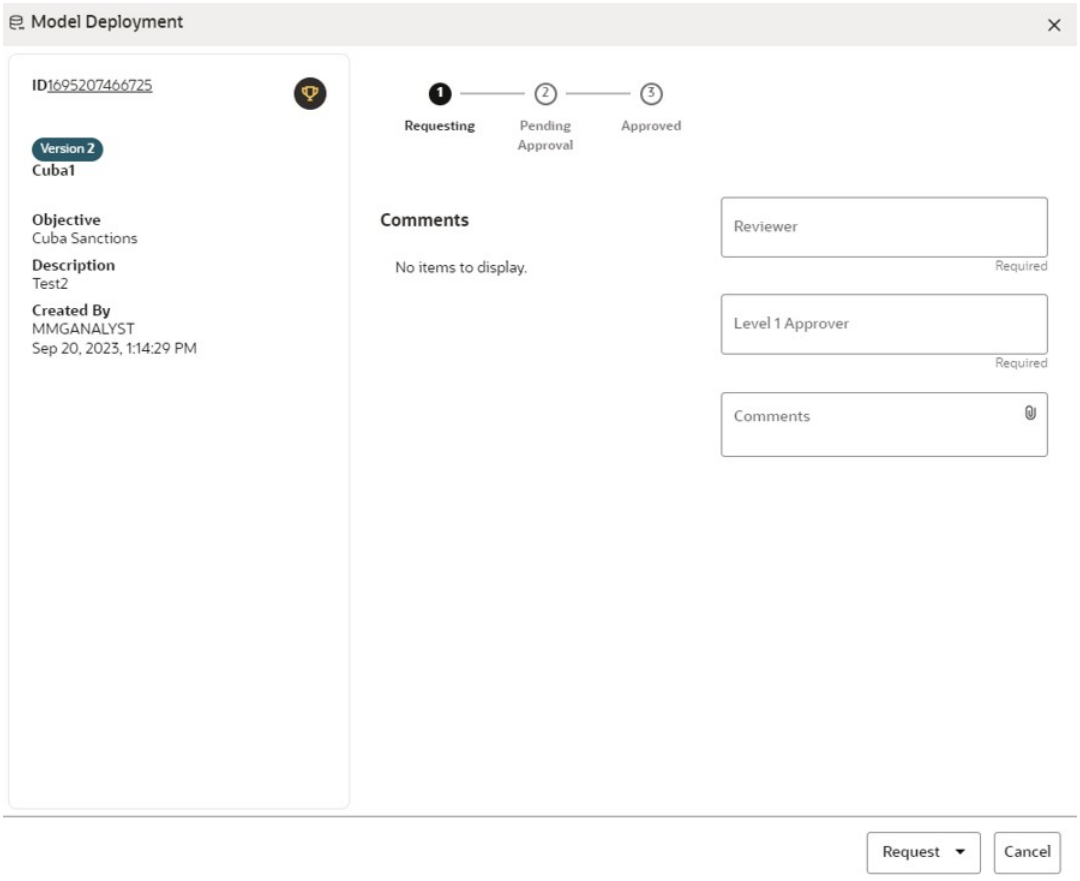
You can promote the published model to production by deploying the Model. For the subsequent information, see Oracle Financial Services Compliance Studio User Guide.

- Understanding Model Governance
- Request Model Acceptance
- Review Models and Move to Approve or Reject
- Approve Models and Promote to Production
- Deploying Models in Production and Make it a Global Champion
- Executing Models using Scheduler Service

To deploy the model follow the subsequent steps:

1. Click Launch Workspace  next to corresponding Workspace to Launch Workspace and display the **Dashboard** window with application configuration and model creation menu.
2. In the Mega menu, click **Modeling** and select **Pipelines**  from the drop down to display the **Model Pipeline** window.
3. Select the Objective name from the list and select the published Model.
4. Click  to view the Model Deployment screen.

Figure 9-35 Model Deployment Window



5. Select the value for the following fields:
   - Reviewer
   - Level 1 Approver
   - Comments
6. Click **Request** and select **Model Acceptance** action.
7. Click **Cancel** to cancel the model Deployment.

> **Note**
>
> For each workspace there can be only one champion model.

9.5.9 Audit Trail

For information on using audit trail, see Oracle Financial Services Compliance Studio User Guide.

10

ML Integration with Customer Screening

Oracle's customer screening process generates alerts that indicate whether an entity or individual matches with an entity in any global sanctions lists.. The matches are dependent on the quality of input data and match configurations. However, the system typically generates a large volume of false positive alerts. To minimize the efforts of analysts, machine learning capability helps in the automatic disposition of events.

The Machine Learning (ML) integration with OFS customer Screening feature allows the user to enhance its compliance capabilities. ML models employ various techniques to aid the compliance users in adjudication of matches, reducing false positives, and enabling more efficient identification of potential risks. This integration allows organizations to streamline their compliance workflows, improve productivity, and maintain robust defenses against financial crimes. it enables compliance professionals to take quicker and accurate decisions.

This chapter provides step-by-step instructions to integrate ML with customer screening.

10.1 Prerequisites

1. Apply the latest sanctions 8.1.2.9.0 version (See Oracle Financial Services Sanctions Pack Installation Guide) and studio 8.1.2.9.0 version (See OFS Compliance Studio Installation Guide) .
2. Perform the following procedures mentioned in the ***Sanctions Event Scoring*** section in the OFS Compliance Studio Administration and Configuration Guide.
   a. Prerequisites for Creating Production Workspace
   b. Creating Production Workspace

   > **Note**
   >
   > Here Production OFSAA infodom name and workspace name must be same.

   c. Prerequisites for Creating Sandbox Workspace
   d. Creating Sandbox Workspace
   e. Populating Sandbox Workspace
   f. Importing Workspace Metadata
   g. Batch Framework for Sanctions Event Scoring
   h. Execute Batch
   i. Monitor Batch
3. Perform the following procedures mentioned in the Sanctions Event Scoring chapter in the latest OFS Compliance Studio Use Case Guide.
   a. Prerequisites
   b. Admin Notebook Activity

> **Note**
>
> While creating model groups using metadata (see *Metadata to Create Model Group(s)* section), create model groups separately for **Entity** and **Individual** in the **V_CUST_RECORD_TYPE_DESC** metadata.

c. Import Packages

d. Create Instance for Sanctions Event Scoring Class

e. Create Definition for Model

f. Get Current Definition Details

g. Create Sanctions Event Scoring Model

Summary of the steps you followed:

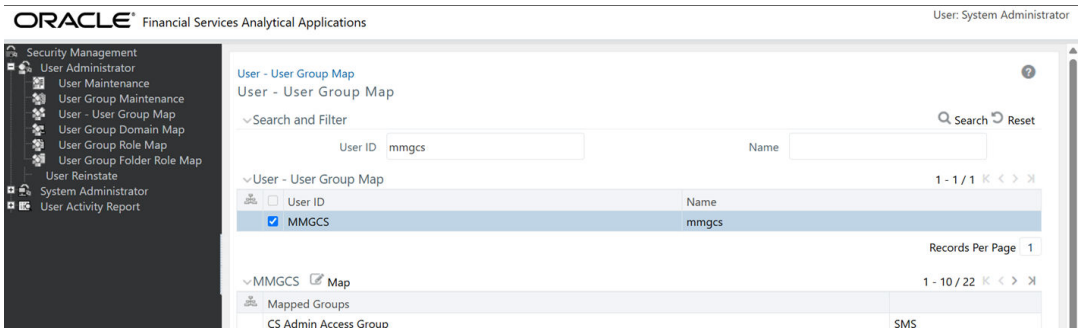
1. Created a production workspace and sandbox workspace.
2. In sand box workspace, you populated the data and ran the `importWorkspaceSQL.sh` and `importNotebooksSES.sh` file.
3. While segmentation of the data, you created model groups separately for Entity and Individual in the `V_CUST_RECORD_TYPE_DESC` metadata.
4. You trained the model and deployed into the production.

10.2 Configuration

Once model is trained and deployed into production, you need to perform the following configuration in the production sanctions OFSAA application to ML integration for the batches.

1. Create a same user in the OFSAA app as in Compliance Studio with CS Admin Access group.

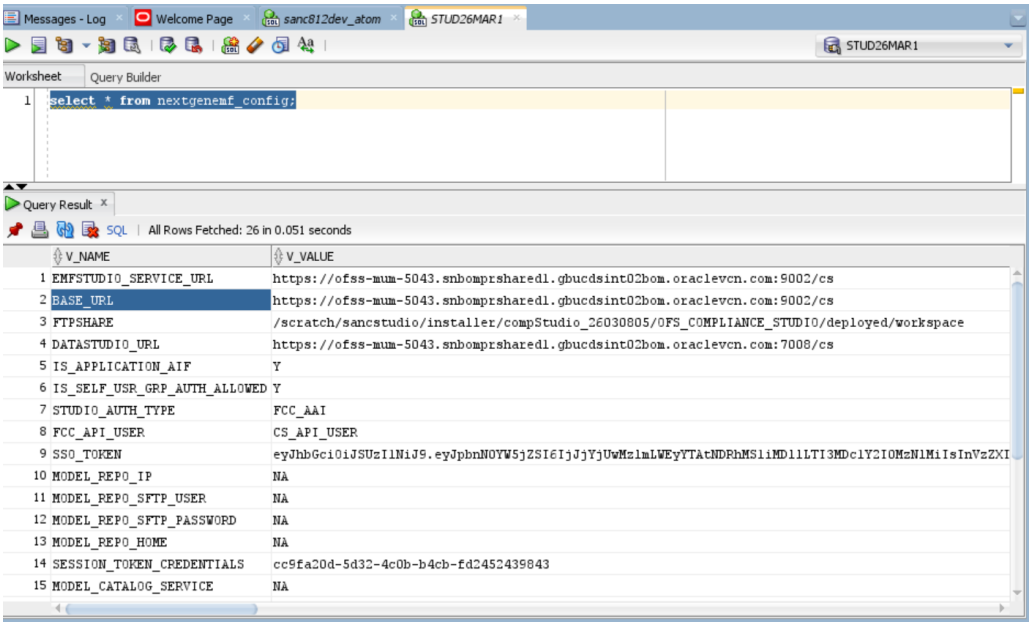
Figure 10-1 User Administrator group



2. Update `MMG_SERVICE_URL` in the `nextgenemf_config` table with the `BASE_URL` value of the `nextgenemf_config` table present in the **compliance studio schema**.

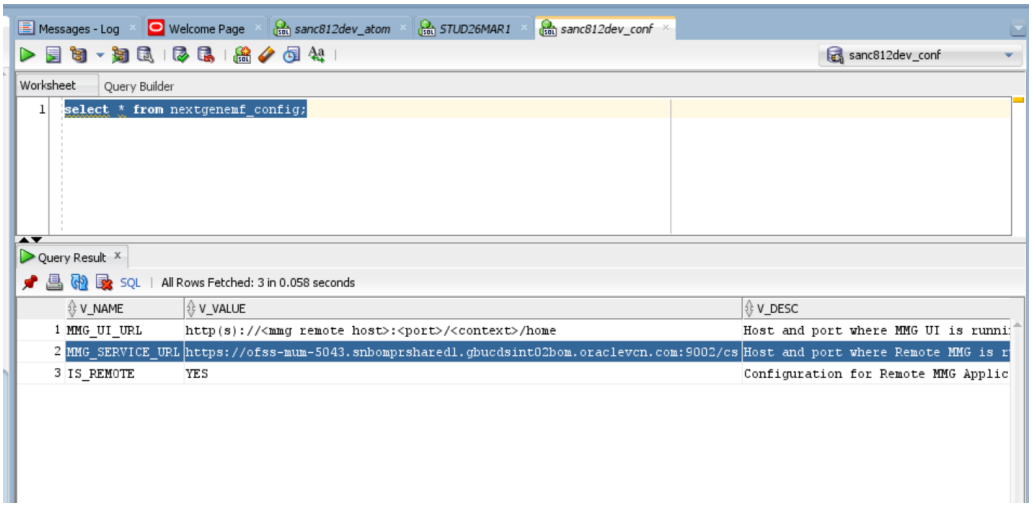
   a. On **compliance studio schema**, open the `nextgenemf_config` table and copy the `BASE_URL`.

Figure 10-2 The Base URL on the Compliance studio schema



b. On **Sanctions Schema**, open the `nextgenemf_config` table and paste `BASE_URL` value to the `MMG_SERVICE_URL` value.

Figure 10-3 The MMG Service URL on the Sanctions Schema



3. Import the compliance studio_server certificate to sanctions java key store path.

   a. Navigate to `<COMPLIANCE_STUDIO_INSTALLATION_PATH>/mmg-home/mmg-studio/ conf` path, copy the `studio_server.cer` certification and paste it into sanctions OFSAA server.

   b. Run the below command to replace the placeholders:

```
keytool -importcert -keystore <JAVA_HOME>/lib/security/cacerts -
storepass changeit -alias studio_ml -file <studio_certificate_path>/
studio_server.cer
```

> **Note**
>
> Use the `studio_ml` as the alias name while creating the certificate.

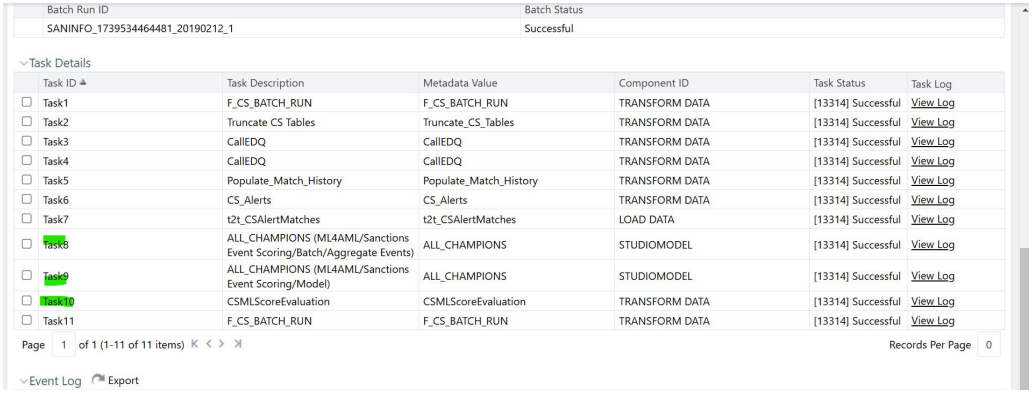
4. Following three ML Process are introduced in our batches:

   a. **CS_ML_Batch_Process**: This process internally calls the Compliance Studio production workspace, Aggregate events Task, and ML Scoring Task.
   For more information refer to the Batch Framework for Sanctions Event Scoring section in the OFS Compliance Studio Administration and Configuration Guide

   The OOB for this process, you need to configure manually after **CS Event Creation process** and before the **CS ML Score Evaluation** process.

   b. **CS_ML_Score_Evaluation**: This process calls the `F_EVALUATE_CS_ML_EVENT_SCORE` function to update the `v_status_code` column in the `CS_ALERTS table` to either **ML Closed** or **ML Escalated** based on the ML auto action threshold settings, and it will also add entries to the `CS_ALERTS_ML_AUDIT` table.
   The Out of Box (OOB) process, this preset in the CS DATA LOAD GENERATION BATCH before the **CS_End_To_End_End_Batch** process.

Figure 10-4 ML process batches successful screen in Data Load Event Generation Batch

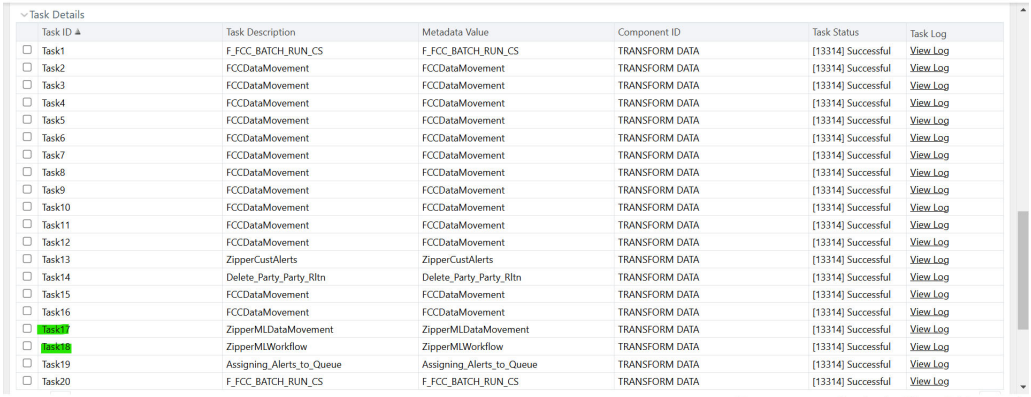


   c. **Zipper ML Process**: It contains two tasks, such as **ZipperMLDataMovement & ZipperMLWorkflow**.
   The **ZipperMLDataMovement** process calls the `F_POPULATE_ZCS_ML_EVNT_DTLS` function to add events score data into the `fcc_cs_ml_evnt_score` and `fcc_cs_ml_evnt_score_dtls` tables.

   The **ZipperMLWorkflow** process calls the `F_CS_ML_WORKFLOW_TRIGGER` function. This function changes the alerts status to either **ML Closed** or **ML Escalated**.

   The OOB for this process is provided in Oracle CS Zipper Processing batch and it is present just before the Assign alerts to queue tasks.

Figure 10-5 Zipper ML process successful screen in Oracle_CS_Zipper_Processing Batch



Task Details

Task ID	Task Description	Metadata Value	Component ID	Task Status	Task Log
Task1	F_FCC_BATCH_RUN_CS	F_FCC_BATCH_RUN_CS	TRANSFORM DATA	[13314] Successful	View Log
Task2	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task3	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task4	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task5	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task6	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task7	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task8	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task9	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task10	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task11	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task12	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task13	ZipperCustAlerts	ZipperCustAlerts	TRANSFORM DATA	[13314] Successful	View Log
Task14	Delete_Party_Party_Rltn	Delete_Party_Party_Rltn	TRANSFORM DATA	[13314] Successful	View Log
Task15	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task16	FCCDataMovement	FCCDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task17	ZipperMLDataMovement	ZipperMLDataMovement	TRANSFORM DATA	[13314] Successful	View Log
Task18	ZipperMLWorkflow	ZipperMLWorkflow	TRANSFORM DATA	[13314] Successful	View Log
Task19	Assigning_Alerts_to_Queue	Assigning_Alerts_to_Queue	TRANSFORM DATA	[13314] Successful	View Log
Task20	F_FCC_BATCH_RUN_CS	F_FCC_BATCH_RUN_CS	TRANSFORM DATA	[13314] Successful	View Log

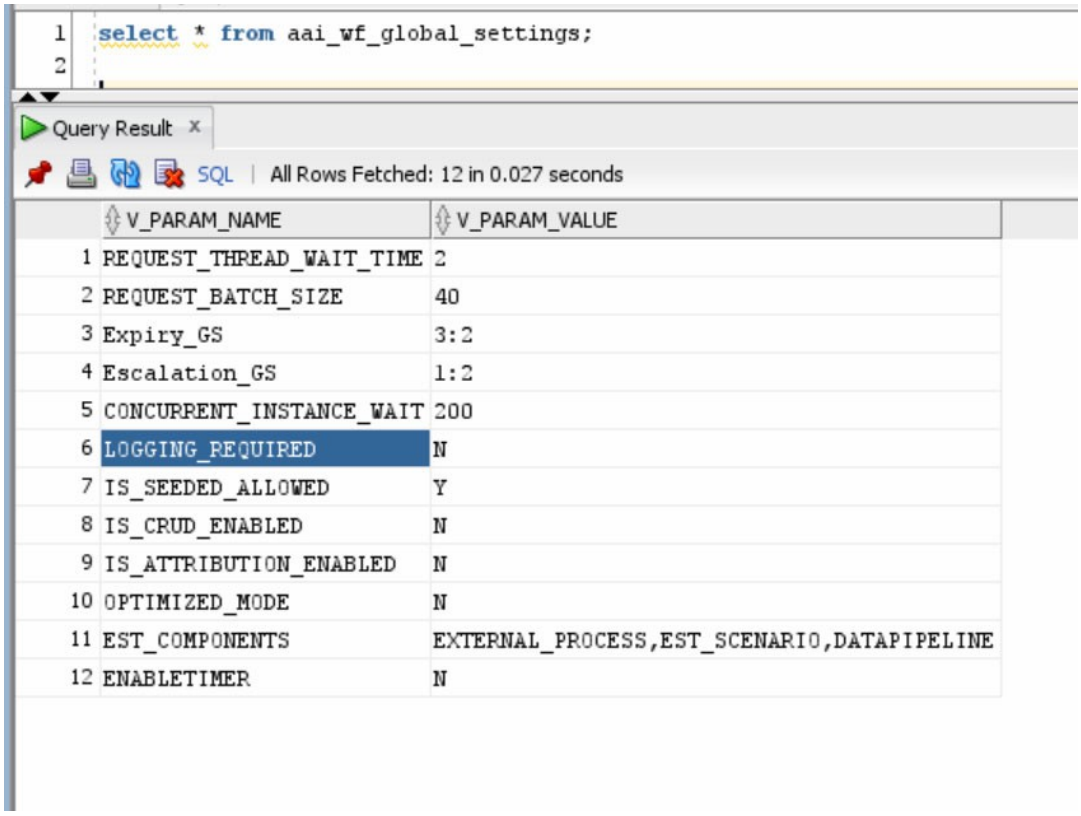
Note

- If any one of the event is in **Pending Review**, the alert status is updated as **New.**
- If all the events in alert are **ML auto closed**, the alert status is updated as **ML Closed**.
- If any one of the event is **ML escalated**, and no other event is in **Pending Review**, the alert status is updated as **ML Escalated**

5. In the Config Schema, Configure the `aai_wf_global_settings` as suggested below:

```
CONCURRENT_INSTANCE_WAIT=200
REQUEST_BATCH_SIZE=40
REQUEST_THREAD_WAIT_TIME=2
LOGGING_REQUIRED=N
```

Figure 10-6 The aai_wf_global_settings screen



	V_PARAM_NAME	V_PARAM_VALUE
1	REQUEST_THREAD_WAIT_TIME	2
2	REQUEST_BATCH_SIZE	40
3	Expiry_GS	3:2
4	Escalation_GS	1:2
5	CONCURRENT_INSTANCE_WAIT	200
6	LOGGING_REQUIRED	N
7	IS_SEEDED_ALLOWED	Y
8	IS_CRUD_ENABLED	N
9	IS_ATTRIBUTION_ENABLED	N
10	OPTIMIZED_MODE	N
11	EST_COMPONENTS	EXTERNAL_PROCESS,EST_SCENARIO,DATAPIPELINE
12	ENABLETIMER	N

6. Once all the configuration steps are done, you can run the Data load event generation and Oracle CS Zipper processing batch.

> **Note**
>
> Model training input data is available in the `ML4AML_SES_EVENT_INPUT` table. For more information, see the ***Sanctions Event Scoring*** section in the OFS Compliance Studio Administration and Configuration Guide and OFS Compliance Studio Use Case Guides.

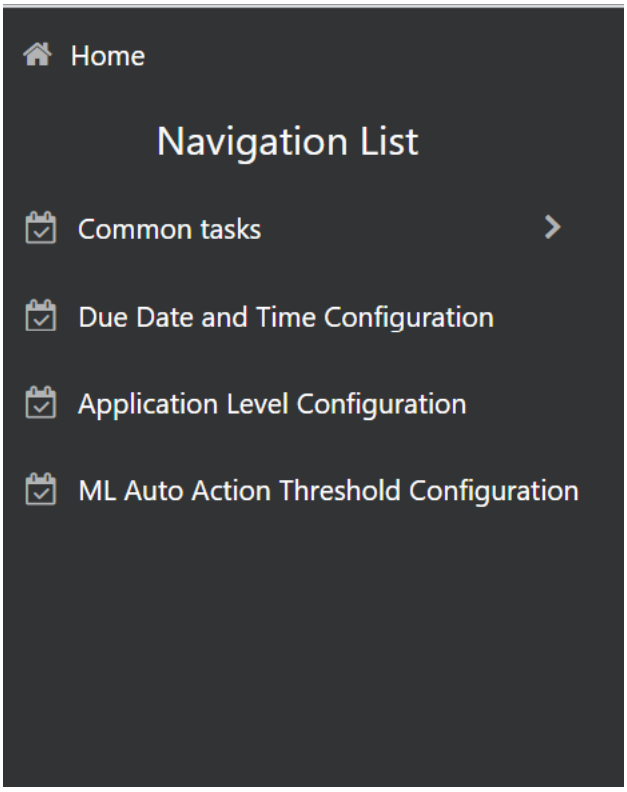
10.3 ML Auto Action Threshold Configuration

Use the ML Auto Action Threshold Configuration tab to configure the parameters for the Customer Screening application, such as enabling or disabling the threshold configuration for the **ML Auto Close/Auto Escalate Feature** .

To configure the parameter using the CS application, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Customer Screening** landing page.
2. Click **ML Auto Action Threshold Configuration** in the Navigation List Available at the LHS.

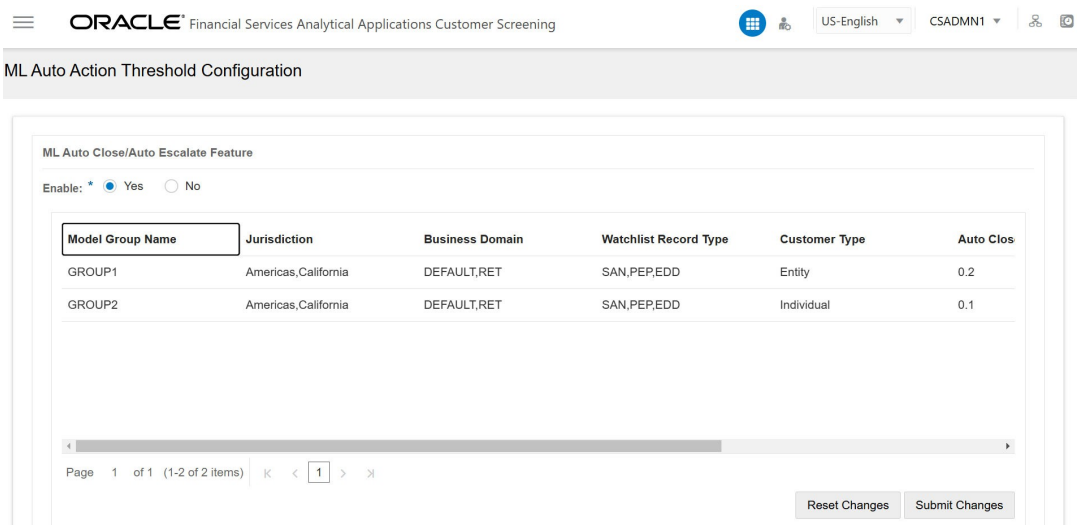
Figure 10-7 Navigation



The **ML Auto Action Threshold Configuration** Screen is Displayed.

3. Select **Yes** to enable the **ML Auto Close/Auto Escalate Feature** option. The list of models deployed in the production appears.

Figure 10-8 ML Auto Action Threshold Configuration screen

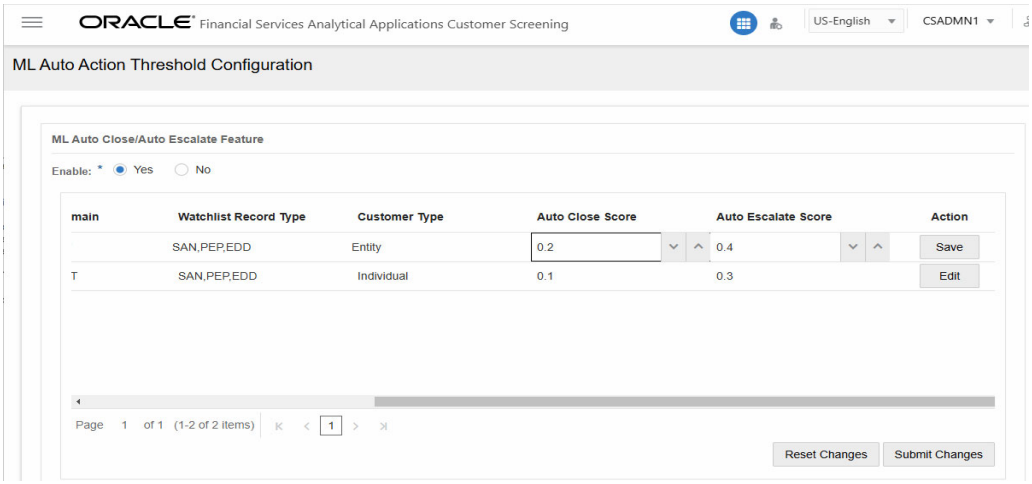


a. Click the **Edit** option for respective model.

b. Enter the **Auto Closure Score** and **Auto Escalate Score** fields.

> **Note**
>
> If any events ML score is **less than or equal** to threshold configured for auto closed score, the alert status is updated as **ML Closed**.
>
> If any events ML score is **greater than or equal** to threshold configured for auto escalated score, the alert status is updated as **ML Escalated**.
>
> If any events ML score is greater than threshold configured for auto closed score and less than auto escalated score threshold, the alert status updated as **New**.

Figure 10-9 The ML Auto Action Threshold Configuration screen score



c. Click **Save**.

d. Click **Submit Changes**.

4. Select No to disable the **ML Auto Close/Auto Escalate Feature** option for the ML Alerts in Alert list details and click **Submit Changes**.

For more information on alert details and event table, see Oracle Financial Services Customer Screening User Guide.

> **Note**
>
> To reset the configuration to default, click **Reset Changes**.

A

Screening Non-Latin Character Sets

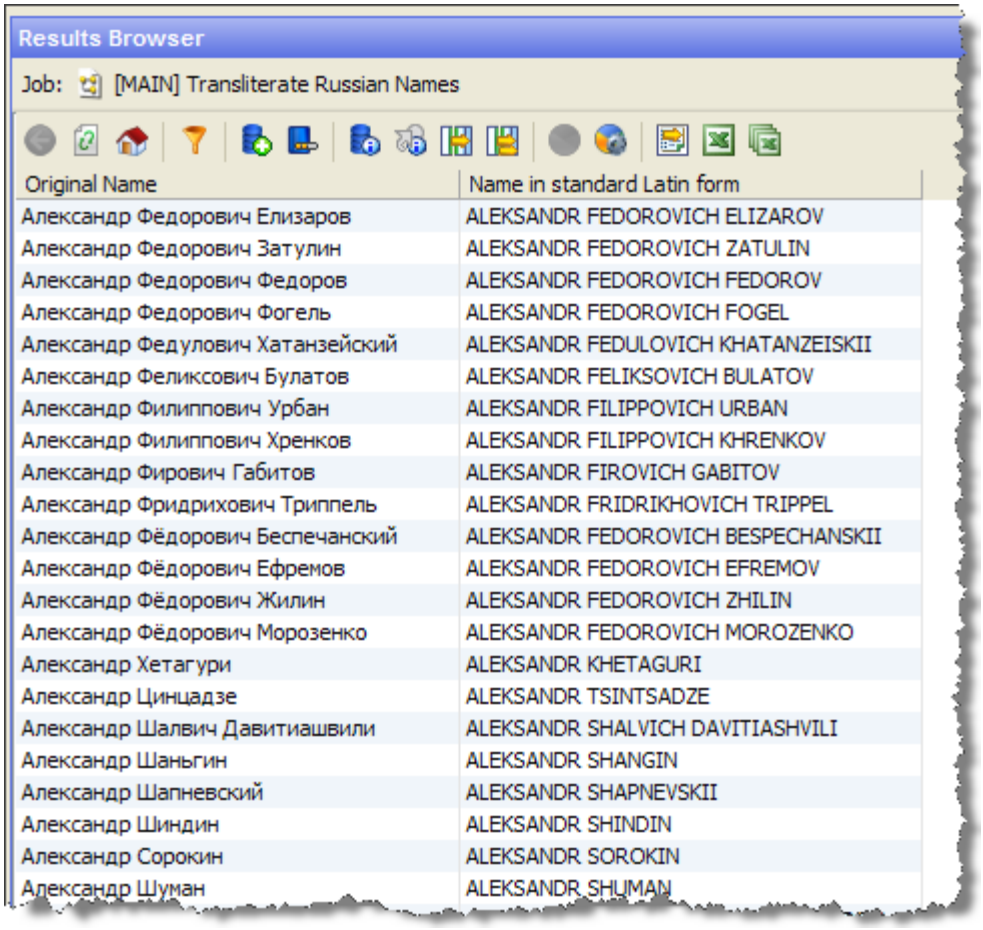
The reference data sources supported by Customer Screening are all provided in the Latin character set, and some in the original scripts. The screening process can also be used with non-Latin data. Non-Latin data can be screened against the Latin reference data sources which are supported by performing transliteration of data from the non-Latin character set to the Latin character set.

Non-Latin customer data can be screened against non-Latin reference data without any changes to the product, although certain fuzzy text matching algorithms may not be as effective when used to match data with the non-Latin character set. Text is processed on a left-to-right basis.

> **Note**
>
> You may have to install additional language packs to display non-Latin data. For more information, contact My Oracle Support (MOS).

The following screenshot shows the transliteration of Cyrillic to the Latin character set:

Figure A-1 Non-Latin Character Set



Original Name	Name in standard Latin form
Александр Федорович Елизаров	ALEKSANDR FEDOROVICH ELIZAROV
Александр Федорович Затулин	ALEKSANDR FEDOROVICH ZATULIN
Александр Федорович Федоров	ALEKSANDR FEDOROVICH FEDOROV
Александр Федорович Фогель	ALEKSANDR FEDOROVICH FOGEL
Александр Федулович Хатанзейский	ALEKSANDR FEDULOVICH KHATANZEISKII
Александр Феликсович Булатов	ALEKSANDR FELIKSOVICH BULATOV
Александр Филиппович Урбан	ALEKSANDR FILIPPOVICH URBAN
Александр Филиппович Хренков	ALEKSANDR FILIPPOVICH KHRENKOV
Александр Фирович Габитов	ALEKSANDR FIROVICH GABITOV
Александр Фридрихович Триппель	ALEKSANDR FRIDRIKHOVICH TRIPPEL
Александр Фёдорович Беспечанский	ALEKSANDR FEDOROVICH BESPECHANSKII
Александр Фёдорович Ефремов	ALEKSANDR FEDOROVICH EFREMOV
Александр Фёдорович Жилин	ALEKSANDR FEDOROVICH ZHILIN
Александр Фёдорович Морозенко	ALEKSANDR FEDOROVICH MOROZENKO
Александр Хетагури	ALEKSANDR KHETAGURI
Александр Цинцадзе	ALEKSANDR TSINTSADZE
Александр Шалвич Давитиашвили	ALEKSANDR SHALVICH DAVITIASHVILI
Александр Шаньгин	ALEKSANDR SHANGIN
Александр Шапневский	ALEKSANDR SHAPNEVSKII
Александр Шиндин	ALEKSANDR SHINDIN
Александр Сорокин	ALEKSANDR SOROKIN
Александр Шуман	ALEKSANDR SHUMAN

Original Script Matching

To match the original script data against reference data, follow these steps:

1. Prepare customer and external entity data such that non-Latin names are populated in the Original Script Name fields.
2. Enable Original Script Name match rules and clusters.

For more information, see the Oracle Financial Services Customer Data Interfaces Guides.

> **Note**
>
> You must make changes to the FCDM Customer Preparation process to support original script matching. For more information, contact My Oracle Support (MOS).

B

Reference Data Tables for Watch Lists

This appendix lists the reference data tables which are available in Customer Screening. These tables contain data that is used to calculate the risk scores and PEP risk scores. The reference data tables are stored in the `Watch list Management` project.

Table B-1 Reference Data Tables for Watch Lists

Screening Process or Watch List	Reference Data Table Used
Multiple screening processes	The following reference data table contains risk score values used by multiple screening processes: • Risk - ISO 3166-1 Country to Risk Score (used by the look up Risk- ISO 3166-1-alpha-2 code to Risk Score) is used to derive a risk score from a country code
Country prohibition screening process	The following reference data tables contain risk score values used in the country prohibition screening process: • Country Prohibitions - Entities • Country Prohibitions - Individuals
DowJones watch list (DJW)	The following reference data tables contain risk score values used when calculating risk scores for the Dow Jones watch list records: • DJW Occupation Category • DJW List Provider Risk Scores • DJW SI Category Description • DJW SI Category
DowJones Anti-Corruption (DJAC) watch list	The following reference data tables contain risk score values used when calculating risk scores for the Dow Jones watch list records: • DJAC Occupation Category • DJAC List Provider Risk Scores • DJAC SI Category Description
EU watch list	There are no reference data tables containing risk score values used only for calculating risk scores for the EU watch list records.
HM Treasury watch list	The `HMT Regime` reference data table contains risk score values used when calculating risk scores for the HM Treasury watch list records.
OFAC watch list	The `OFACSDN Program` reference data table contains risk score values used when calculating risk scores for the OFAC watch list records.
UN watch list	The `UN List Type` reference data table contains risk score values used when calculating risk scores for the UN watch list records.

Table B-1 (Cont.) Reference Data Tables for Watch Lists

Screening Process or Watch List	Reference Data Table Used
World-Check(WC) watch list	The following reference data tables contain risk score values used when calculating risk scores for the World-Check watch list records: • WC Category • WC Keyword (used by the lookup WC Keyword - Risk Score Lookup)
Accuity watch list	The following reference data tables contain risk score values used when calculating risk scores for the Accuity watch list records: • Accuity Program Sub-Category Risk Scores • Accuity Source Risk Scores
NA	The `Risk– Risk Element Weighting` reference data table contains the weightings used when calculating a record risk score from the various contributing elements.

C

Pre-configured Watch List Information

This appendix contains details of each of the pre-configured watch lists that can be used by Customer Screening.

HM Treasury Watch List

The HM Treasury publishes a sanctions list that can be used for screening in Customer Screening. The sanctions list provides a consolidated list of targets listed by the United Nations, European Union, and the United Kingdom under legislation relating to current financial sanctions regimes. For more information, visit the HM Treasury website.

Customer Screening uses the watch list in a semi-colon delimited form. Click the following link to download the `.csv` file.

https://ofsistorage.blob.core.windows.net/publishlive/ConList.csv

OFAC Watch List

The US Treasury's Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. For more information, visit the Treasury website.

Customer Screening supports the OFAC Specially Designated Nationals and OFAC Consolidated Sanctions watch lists.

The OFAC Specially Designated Nationals (SDN) watch list must be downloaded in three parts:

https://www.treasury.gov/ofac/downloads/sdn.csv

https://www.treasury.gov/ofac/downloads/add.csv

https://www.treasury.gov/ofac/downloads/alt.csv

The OFAC Consolidated Sanctions List watch list must be downloaded in three parts:

https://www.treasury.gov/ofac/downloads/consolidated/cons_prim.csv

https://www.treasury.gov/ofac/downloads/consolidated/cons_add.csv

https://www.treasury.gov/ofac/downloads/consolidated/cons_alt.csv

EU Watch List

The European Union applies sanctions or restrictive measures to achieve certain objectives as mentioned in the Common Foreign and Security Policy (CFSP) and defined in Article 11 of the Treaty on the European Union. The European Commission offers a consolidated list containing the names and identification details of all persons, groups, and entities targeted by these financial restrictions. For more information, visit the European Commission website.

To download the consolidated list, follow these steps:

1. Go to https://webgate.ec.europa.eu/europeaid/fsd/fsf#!/account and create a user name and password to the site.
2. Navigate to https://webgate.ec.europa.eu/europeaid/fsd/fsf#!/files and open the settings for the crawler file.
3. Copy the URL for 1.0 XML (Based on XSD). This will be in the format `https://webgate.ec.europa.eu/europeaid/fsd/fsf/public/files/ xmlFullSanctionsList/content?token=[username]`. You must replace the `[username]` placeholder with the user name you have created.
4. Enter this URL in your run profile or download task.

UN Consolidated Watch List

The United Nations (UN) or United Nations Security Council consolidated list is a watch list that includes all individuals and entities who are subject to sanctions measures imposed by the Security Council. For more information, visit the UN Security Council website.

Download the consolidated list from https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/consolidated.xml.

C.1 Dow Jones Watch List

The Dow Jones watch list provides a subscription-based service and offers a consolidated list of PEPs (Politically Exposed Persons) and entities and individuals appearing on the various sanctions lists. For more information, visit the Dow Jones website.

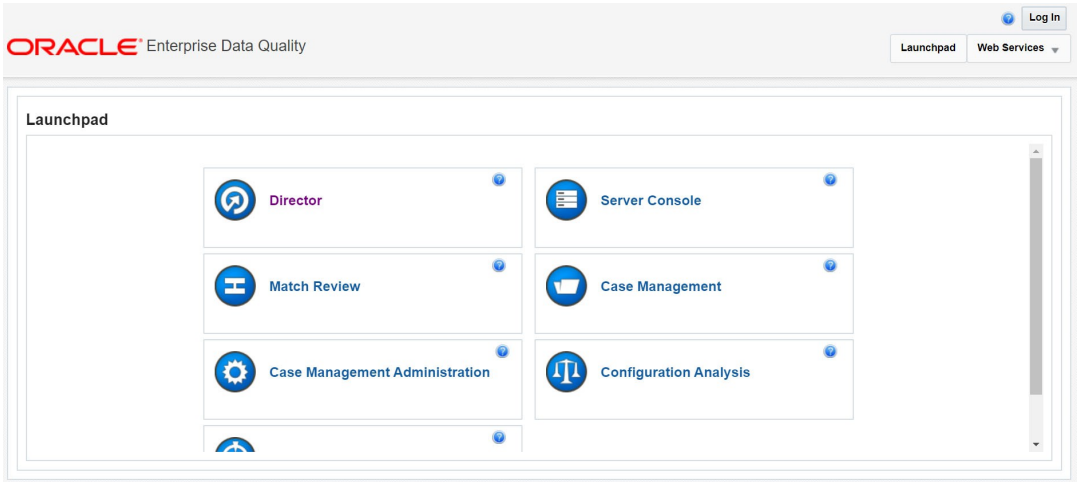
You can automate the download of the Dow Jones watch list using the following script files that are provided with Customer Screening to configure the download process:

```
download-djw.sh (for use on Unix platforms)
download-djw.bat (for use on Windows platforms)
```

The script files are used by the automated task to download the data files and copy them to the Oracle Enterprise Data Quality (OEDQ) landing area. The script files must be modified to provide the download URL and the proxy server details for your Internet connection as follows:

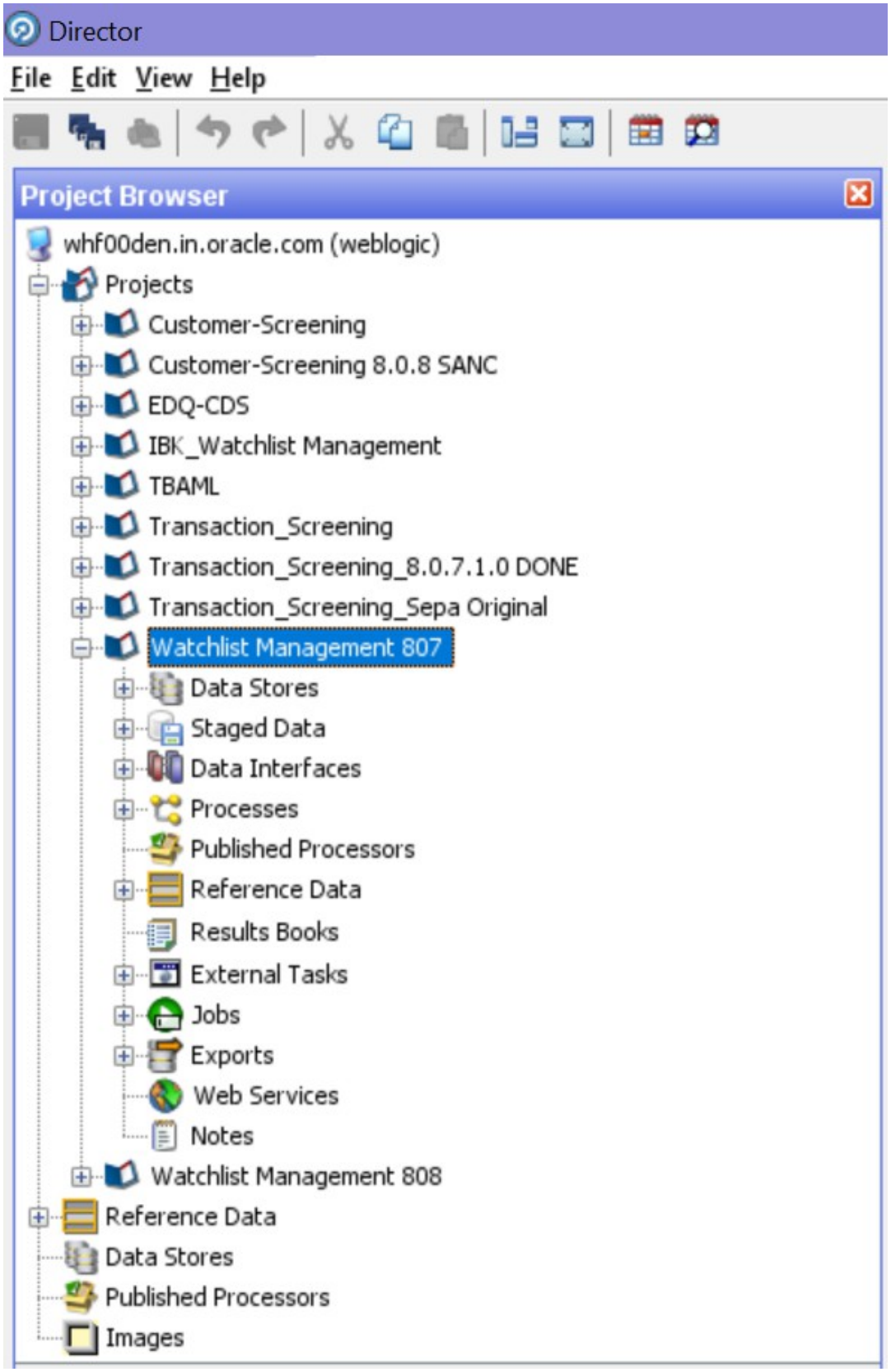
1. Go to the EDQ URL and open the **Director** menu.

Figure C-1 Director Menu in EDQ



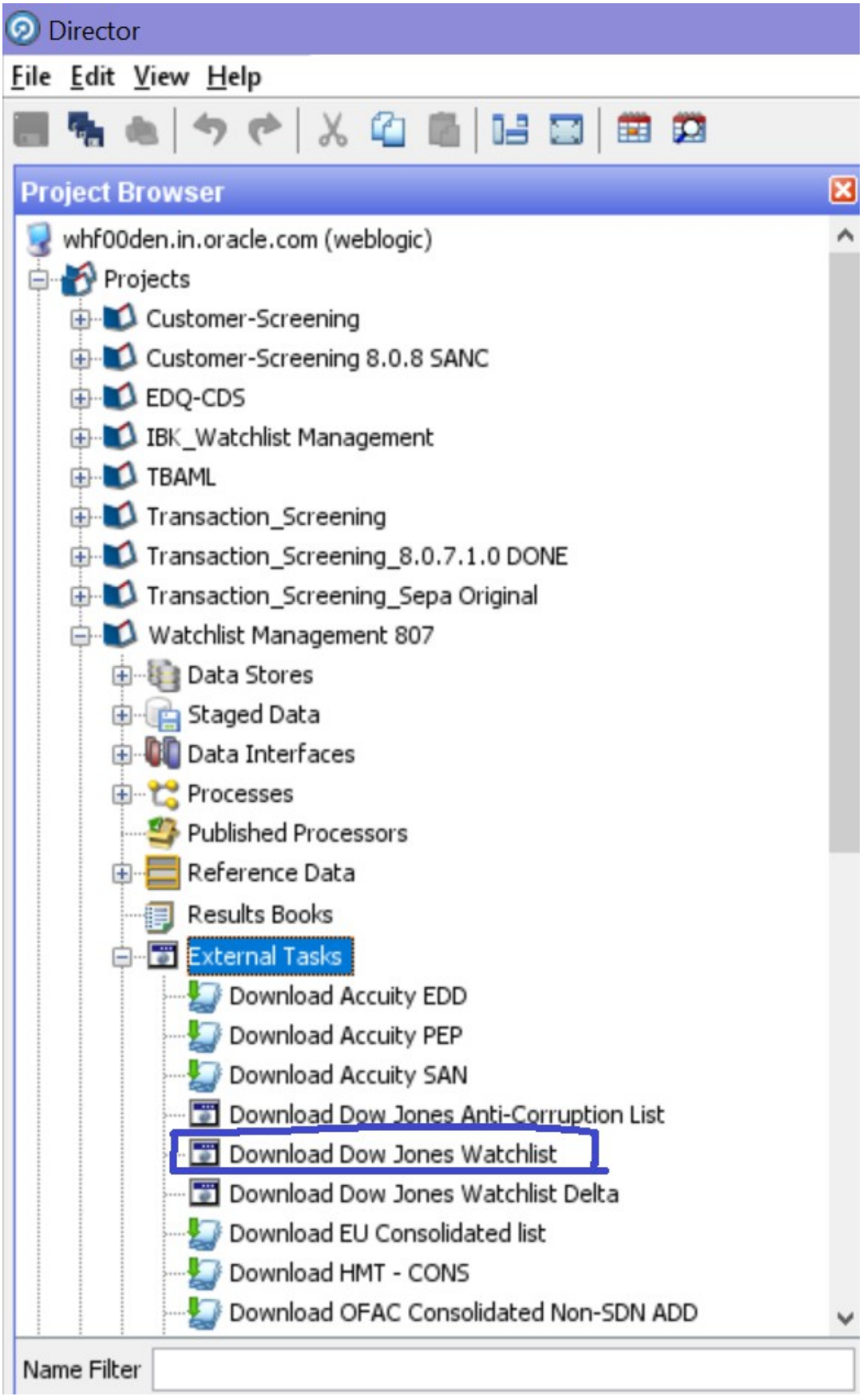
2. In the **Director** landing page, expand the **Watch list Management** project in the **Project Browser** pane.

Figure C-2 Project Browser Pane



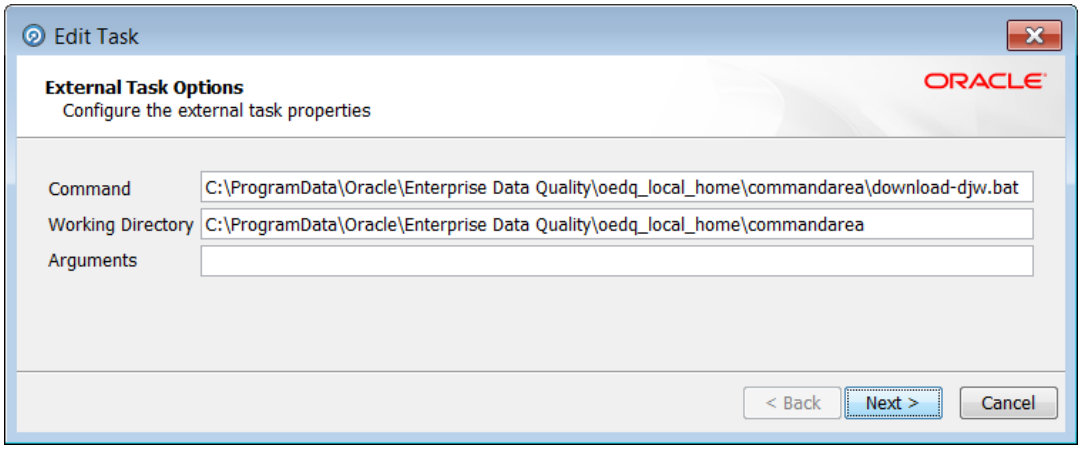
3. Expand the **External Tasks** node for the `Watch list Management` project and then double-click the **Download Dow Jones Watch list** task.

Figure C-3 External Tasks Node



4. Configure the external task to call the batch or shell file by providing the directory and related command as shown:

Figure C-4 Edit Task Window for the Dow Jones Watch List



5. Configure your `PATH` system variable to include the path to your Java installation.
6. Add the user name and password and the proxy server configuration details for Dow Jones in the batch or script file.

> **Note**
>
> In Watchlist Management Project under Reference Data, the “DJW List Provider Static”, contains the entire Dow Jones List Providers. It contains the score and the flag irrespective whether it belongs to Sanctions List or not. User has the privilege to change the flag and score based on their preference.

C.2 Dow Jones Anti-Corruption Watch List

The Dow Jones Anti-Corruption watch list provides a subscription-based service that contains information to help you assess, investigate, and monitor third-party risk with regards to the anti-corruption compliance regulation. For more information, visit the Dow Jones website.

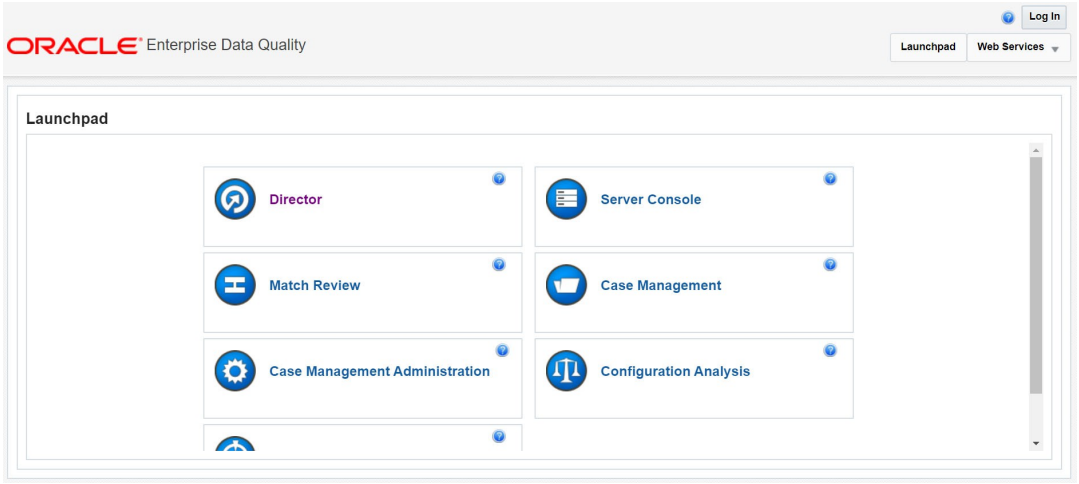
You can automate the download of the Dow Jones watch list using the following script files that are provided with Customer Screening to configure the download process:

```
download-djac.sh (for use on Unix platforms)
download-djac.bat (for use on Windows platforms)
```

The script files are used by the automated task to download the data files and copy them to the Oracle Enterprise Data Quality (OEDQ) landing area. The script files must be modified to provide the download URL and the proxy server details for your Internet connection as follows:

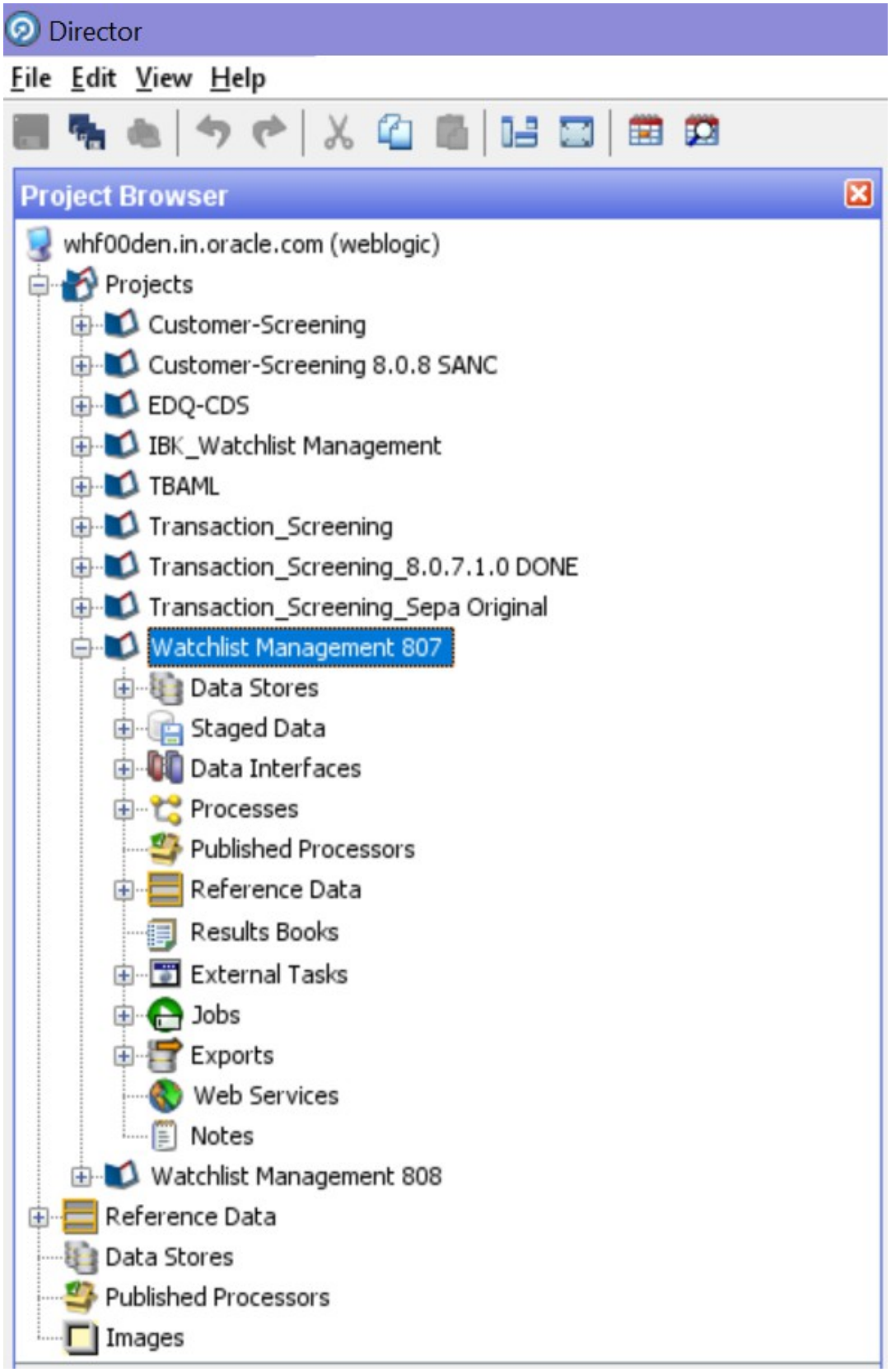
1. Go to the EDQ URL and open the **Director** menu.

Figure C-5 Director Menu in EDQ



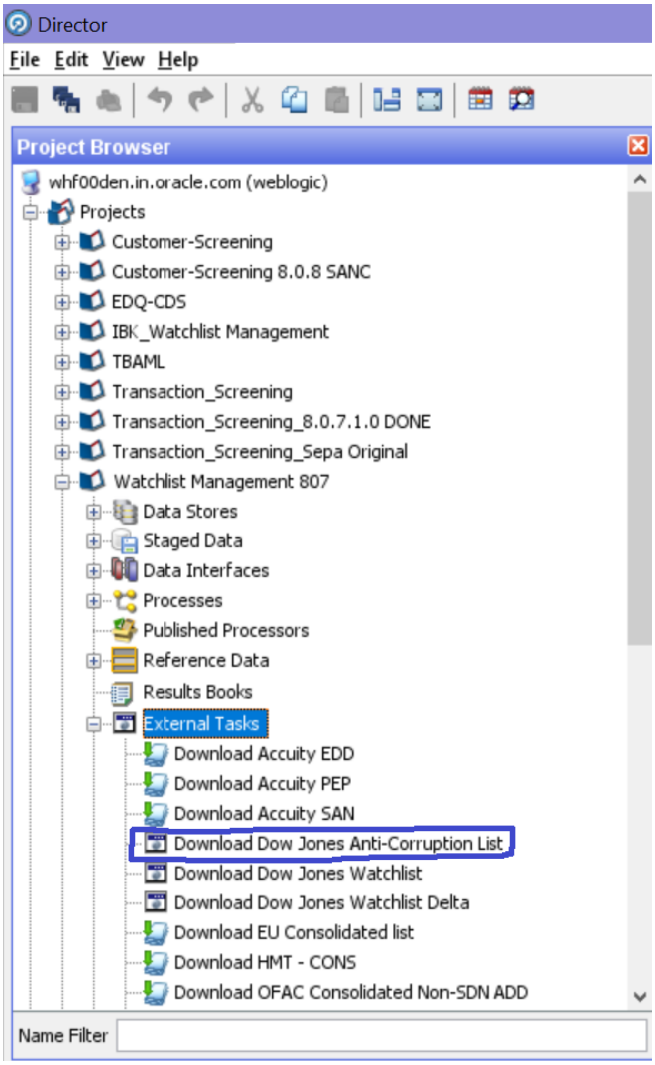
2. In the **Director** landing page, expand the **Watch list Management** project in the **Project Browser** pane.

Figure C-6 Project Browser Pane



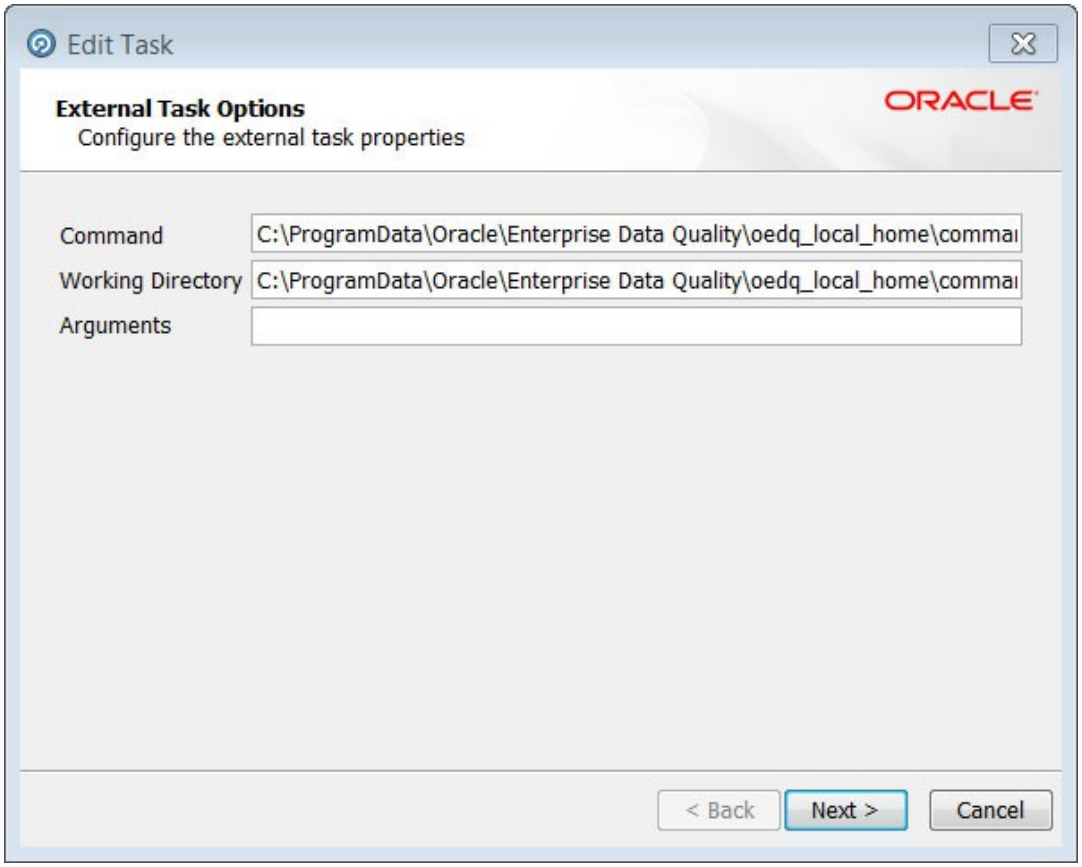
3. Expand the **External Tasks** node for the Watch list Management project and then double-click the **Download Dow Jones Anti-Corruption List** task.

Figure C-7 External Tasks Node



4. Configure the external task to call the batch or shell file by providing the directory and related command as shown:

Figure C-8 Edit Task Window for the Dow jones Anti-Corruption Watch List



5. Configure your `PATH` system variable to include the path to your Java installation.
6. Add the user name and password and the proxy server configuration details for Dow Jones Anti- Corruption in the batch or script file.

C.3 Delta Watch List Configurations for the Dow Jones Watch List

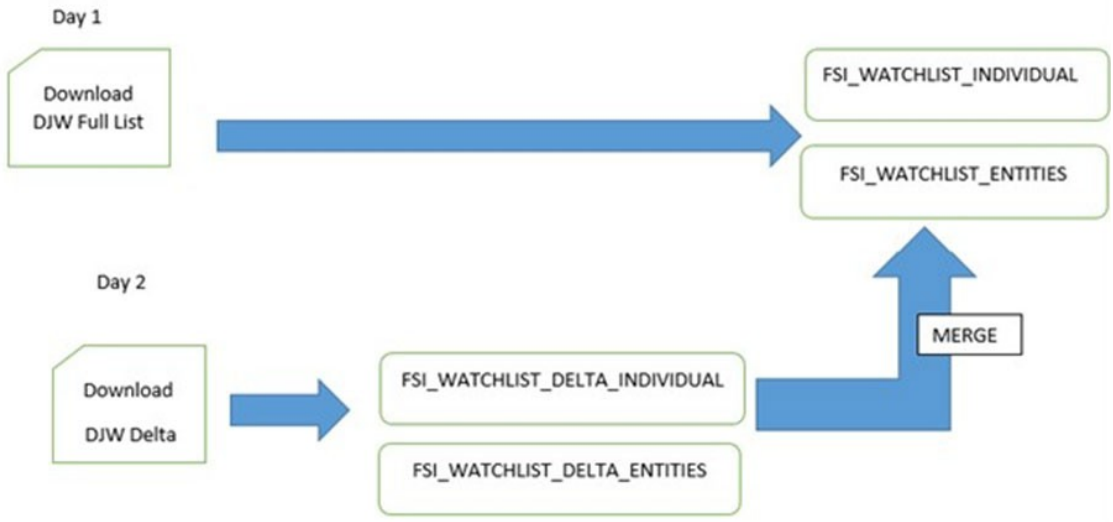
> **Note**
>
> These configurations are performed when you do not want to download the full watch list, and only want to download the delta watch list. This helps to reduce the download time and is not part of the screening process.

Customer Screening recommends that you always use the full watch list during the screening process. Due to the clustering strategy which is implemented in the screening process, you must not download the delta watch list. There are certain cases in which you must download the delta watch list files, for example, if the full watch list files are not yet available for download or if you want to save time.

Customers who download the delta watch list files must first download the full watch list files and then download the delta watch list files. The delta watch list is then merged into the full watch list before screening.

The following image shows the information flow for the delta watch list:

Figure C-9 Flow for Delta Watch List



When you download the full watch list, data is stored in the `FSI_WATCHLIST_INDIVIDUAL` and `FSI_WATCHLIST_ENTITIES` tables. When you download the delta watch list, data is first stored in the `FSI_WATCHLIST_DELTA_INDIVIDUAL` and `FSI_WATCHLIST_DELTA_ENTITIES` tables. Then, based on the value in the ACTION Flag tag in the delta watch list, it merges with the full watch list.

The ACTION flag key is a non-editable value, and can be one of the following values:

- **new**: If the value is `new`, it means that these records are new and are added to the full watch list when the delta files are merged with the full watch list.
- **chg**: If the value is `chg`, it means that these records are modified and are added to the full watch list when the delta files are merged with the full watch list.
- **del**: If the value is `del`, it means that these records are no longer active and are removed from the full watch list when the delta files are merged with the full watch list.

> **Note**
>
> You must always run the full watch list files before you run the delta watch list files. The full watch list files must be downloaded if, for example, the download of the delta watch list files has failed for multiple days. You can also run the full watch list once every week to ensure that the complete data has been processed.

Configurations for the Full and Delta Watch Lists

The following configurations must be done for both full and delta watch list updates in the `watch list-management.properties` run profile. The run profile is available in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory when you log in to the WinSCP server.

- Set `phase.Initialise\ staged\ data.enabled = N` to disable the `.jmp` file updates.

- Set `phase.Initialise\ staged\ data\ DB.enabled = Y` to initialize the database.
- Set `phase.Initilize\ Prepared\ List\ Data.enabled = N` to disable the `.jmp` file updates.
- Set `phase.Initilize\ Prepared\ List\ Data\ DB.enabled = Y` to prepare the database.

Running the Full Watch list

To run the full watch list, follow these steps:

1. Set the following properties in the `watch list-management.properties` file:
   - `phase.DJW\ -\ Download.enabled = Y.`
   - `phase.DJW\ -\ Download\ Delta.enabled = N.`
   - `phase.DJW\ -\ Stage\ reference\ lists.enabled = Y.`
   - `phase.DJW\ -\ Sanction_List_Reference.enabled = Y`
   - `phase.DJW\ -\ Keywords_Preparation.enabled = Y`
   - `phase.*.export.*.ind_table_name = FSI_WATCHLIST_INDIVIDUAL.`
   - `phase.*.export.*.entities_table_name = FSI_WATCHLIST_ENTITIES.`
2. Set the following properties in the `customer-screening.properties` file:
   - `phase.DJW\ -\ Load\ without\ filtering.enabled = N`
   - `phase.DJW\ -\ Load\ without\ filtering\ DB.enabled = Y`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 1).enabled = N`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y`
3. Set the following properties in the `customer-screening-real-time.properties` file:
   - `phase.DJW\ -\ Load\ without\ filtering.enabled = N`
   - `phase.DJW\ -\ Load\ without\ filtering\ DB.enabled = Y`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 1).enabled = N`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y`
4. Set the following properties in the `external-entity-screening.properties` file:
   - `phase.DJW\ -\ Load\ without\ filtering.enabled = N`
   - `phase.DJW\ -\ Load\ without\ filtering\ DB.enabled = Y`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 1).enabled = N`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y`

Running the Delta Watch List

To run the delta watch list, follow these steps:

1. Set the following properties in the `watch list-management.properties` file:
   - `phase.DJW\ -\ Download.enabled = N.`

- `phase.DJW\ -\ Download\ Delta.enabled = Y.`
- `phase.DJW\ -\ Stage\ reference\ lists.enabled = Y.`
- `phase.DJW\ -\ Sanction_List_Reference.enabled = Y`
- `phase.DJW\ -\ Keywords_Preparation.enabled = Y`

2. Set `phase.*.export.*.ind_table_name = FSI_WATCHLIST_DELTA_INDIVIDUAL`.
3. Set `phase.*.export.*.entities_table_name = FSI_WATCHLIST_DELTA_ENTITIES`.

Merging the Delta Watch List to the Full Watch List

To merge the delta watch list with the full watch list, set the following properties in the `watch list-management.properties` file:

- `phase.Delta\ Merge.enabled = Y.`
- `phase.Linked\ Profiles.enabled = Y.`

C.4 Delta Watch List Configurations for the World-Check Watch List

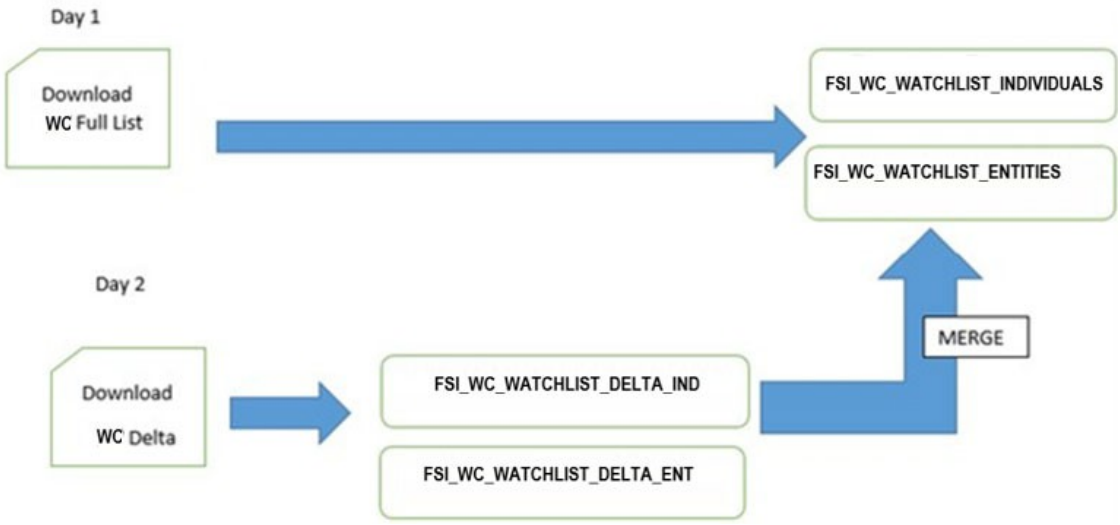
> **Note**
>
> These configurations are performed when you do not want to download the full watch list, and only want to download the delta watch list. This helps to reduce the download time and is not part of the screening process.

Customer Screening recommends that you always use the full watch list during the screening process. Due to the clustering strategy, which is implemented in the screening process, you must not download the delta watch list. There are certain cases in which you must download the delta watch list files, for example, if the full watch list files are not yet available for download or if you want to save time.

Customers who download the delta watch list files must first download the full watch list files and then download the delta watch list files. The delta watch list is then merged into the full watch list before screening.

The following image shows the information flow for the delta watch list:

Figure C-10 Flow for Delta Watch List



When you download the full watch list, data is stored in the FSI_WC_WATCHLIST_INDIVIDUALS and FSI_WC_WATCHLIST_ENTITIES tables. When you download the delta watch list, data is first stored in the FSI_WC_WATCHLIST_DELTA_IND and FSI_WC_WATCHLIST_DELTA_ENT tables. Then the data is merged into the main table. For more information, see Merging the Delta Watch List to the Full Watch List.

> **Note**
>
> You must always run the full watch list files before you run the delta watch list files. The full watch list files must be downloaded if, for example, the download of the delta watch list files has failed for multiple days. You can also run the full watch list once every week to ensure that the complete data has been processed.

Configurations for the Full and Delta Watch Lists

The following configurations must be done for both full and delta watch list updates in the `watch list-management.properties` run profile. The run profile is available in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory when you log in to the WinSCP server.

- Set `phase.Initialise\ staged\ data.enabled = N` to disable the `.jmp` file updates.
- Set `phase.Initialise\ staged\ data\ DB.enabled = Y` to initialize the database.
- Set `phase.Initilize\ Prepared\ List\ Data.enabled = N` to disable the `.jmp` file updates.
- Set `phase.Initilize\ Prepared\ List\ Data\ DB.enabled = Y` to prepare the database.

Running the Full Watch list

To run the full watch list, follow these steps:

1. Set the following properties in the `watch list-management.properties` file:

- phase.WC\ -\ Download.enabled = Y.
- phase.WC\ -\ Download\ Delta.enabled = N.
- phase.WC\ -\ Stage\ reference\ lists.enabled = Y.
- phase.*.export.*.wc_ind_table_name=FSI_WC_WATCHLIST_INDIVIDUAL §
- phase.*.export.*.wc_entities_table_name=FSI_WC_WATCHLIST_ENTITIES

To run the full watch list without filtering, set the following properties:

- phase.WC\ -\ Prepare\ without\ filtering.enabled = N
- phase.WC\ -\ Prepare\ without\ filtering\ Full\ DB.enabled = Y

To run the full watch list with filtering, set the following properties:

- phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = N
- phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = N
- phase.WC\ -\ Prepare\ with\ filtering\ Full\ DB.enabled = Y

To run the full watch list without filtering, set the following properties:

- phase.WC\ -\ Load\ without\ filtering.enabled = N
- phase.WC\ -\ Load\ without\ filtering\ DB.enabled = Y

To run the full watch list with filtering, set the following properties:

- phase.WC\ -\ Load\ with\ filtering\ (Part\ 1).enabled = N
- phase.WC\ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y
- phase.WC\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y

2. Set the following properties in the `customer-screening-real-time.properties` file:
   - phase.WC\ -\ Load\ without\ filtering.enabled = N
   - phase. WC \ -\ Load\ without\ filtering\ DB.enabled = Y
   - phase. WC \ -\ Load\ with\ filtering\ (Part\ 1).enabled = N
   - phase. WC \ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y
   - phase. WC \ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y
3. Set the following properties in the `external-entity-screening.properties` file:
   - phase. WC \ -\ Load\ without\ filtering.enabled = N
   - phase. WC \ -\ Load\ without\ filtering\ DB.enabled = Y
   - phase. WC \ -\ Load\ with\ filtering\ (Part\ 1).enabled = N
   - phase. WC \ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y
   - phase. WC \ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y

Running the Delta Watch List

To run the delta watch list, follow these steps:

1. Set the following properties in the `watch list-management.properties` file:
   - phase.WC\ -\ Download.enabled = N.
   - phase.WC\ -\ Download\ Delta.enabled = Y.

- `phase.WC\ -\ Stage\ reference\ lists.enabled = Y.`
- `phase.*.export.*.wc_ind_table_name=FSI_WC_WATCHLIST_DELTA_IND`
- `phase.*.export.*.wc_entities_table_name=FSI_WC_WATCHLIST_DELTA_ENT`

2. To run the delta watch list without filtering, set the following properties:
   - `phase.WC\ -\ Prepare\ without\ filtering.enabled = N`
   - `set phase.WC\ -\ Prepare\ without\ filtering\ Delta\ DB.enabled = Y`

   To run the delta watch list with filtering, set the following properties:
   - `phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = N`
   - `phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = N`
   - `phase.WC\ -\ Prepare\ with\ filtering\ Delta\ DB.enabled = Y`

Merging the Delta Watch List to the Full Watch List

To merge the delta watch list with the full watch list, set the following properties in the `watch list-management.properties` file:

- `phase.WC\Delta\ Merge.enabled = Y.`
- `phase.WC\Linked\ Profiles.enabled = Y.`

D

Splitting Jobs Using Multiple EDQ Servers

You can split jobs across multiple servers to reduce the time taken to process many customers, for example, one million or more.

> **Note**
>
> These steps are applicable only if you plan to use multiple EDQ servers for customer screening. If you want to use the default setup, that is, only a single EDQ server, see Scheduling the Customer Screening Run Job.

Some examples are as follows:

- If one server is used to process the watch lists and another server is used to process the entity names.
- If one server is used to process data of individuals and another server is used to process data of entities during different times of day.

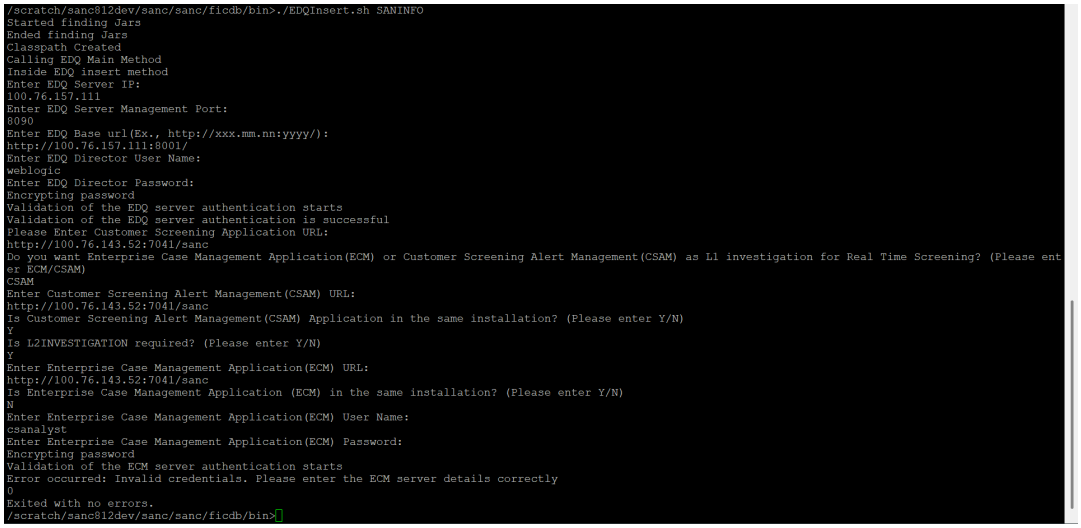
> **Note**
>
> 1. Provide the EDQ user name and password in the `cs_appln_params` table.
> 2. Run the `select * from cs_edq_servers` query in your SQL query tool to verify the server details.

To split jobs using multiple servers, follow these steps:

1. Navigate to the `FIC_DB_HOME/bin` directory.
2. Execute `./EDQServerInsert.sh <INFODOM NAME>`. This step is used to register the EDQ server details. You must replace the `INFODOM NAME` placeholder with your domain name.
3. Enter the following details in the console where the command is run:
   - EDQ Server Name
   - EDQ server IP
   - Enter EDQ Base URL (for example - http://xxx.mm.nn:yyyy/)
   - EDQ Server Direct Port number (JMX port number). This value must be 8090.
   - EDQ Server User Name
   - EDQ Password details

> **Note**
>
> If any of the authentication details entered is incorrect, the system displays error message.

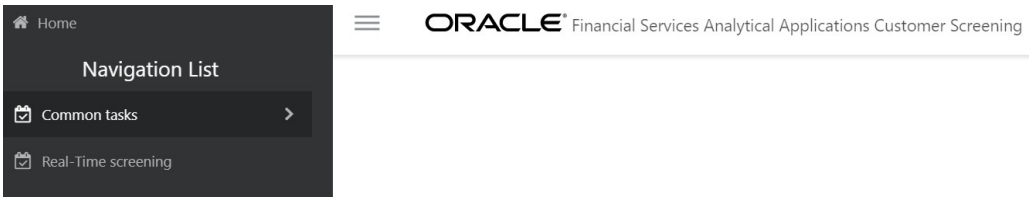
Figure D-1 EDQ Details



4. Duplicate the `CS_Data_Load_Event_Generation` batch in the **Run** page. To do this, copy the `CS_Data_Load_Event_Generation` batch and create another batch.
Follow these steps to access the Run page:

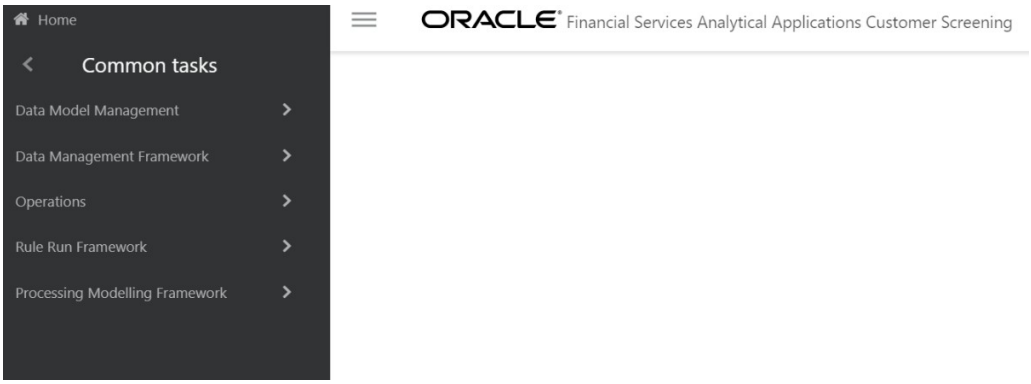
   a. Login as the administrator. The **Financial Services Analytical Applications Customer Screening** home page appears.

Figure D-2 Financial Services Analytical Applications Customer Screening Home Page



   b. Click the hamburger icon to view the Application Navigation List.

Figure D-3 Application Navigation List



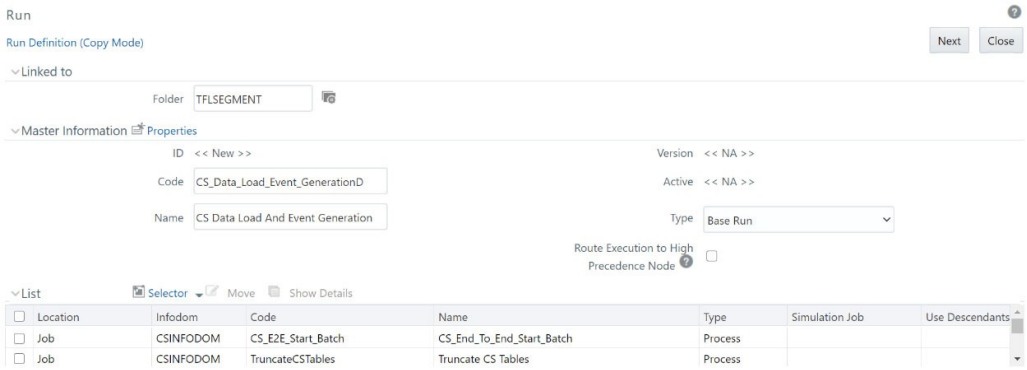
   c. From the **Application Navigation List**, select **Common Tasks**, then select **Rule Run Framework**, and then select **Run**. The **Run** page appears.

5. In the **Run** page, follow these steps to create a duplicate batch:

   a. Select the `CS_Data_Load_Event_Generation` run and click **Copy**. The **Run** page opens in copy mode.

> **Note**
>
> You must select the segment folder for the Sanctions pack in the **Folder** field to proceed.

Figure D-4 Run Page in Copy Mode



   b. Enter a new run code or alter the existing value in the **Code** field. For example, code can be `CS_Data_Load_Event_GenerationD`.

   c. Enter a new run name or alter the existing value in the Code field. For example, name can be `CS Data Load And Event Generation`.

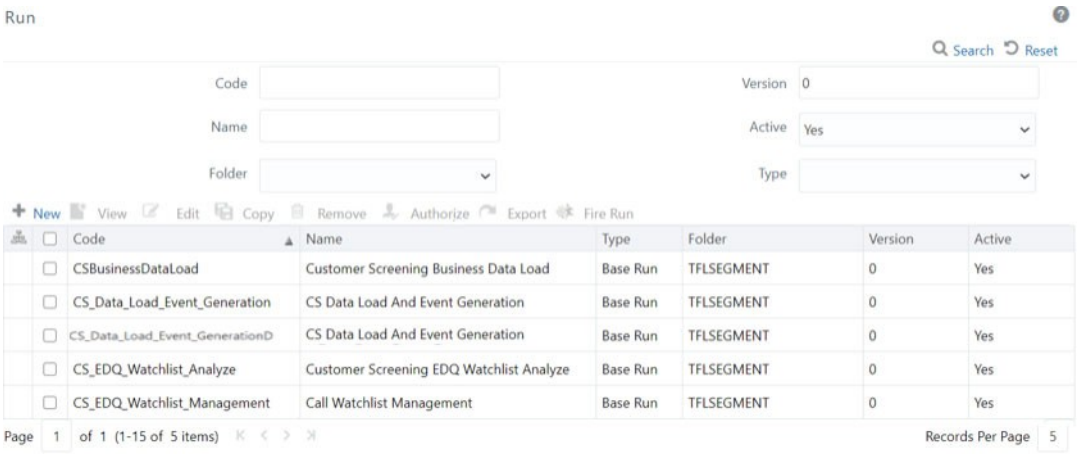
> **Note**
>
> The run name and run code values can be the same.

   d. Click **Next** to go to the next page and confirm the name.

   e. Click **Save**.

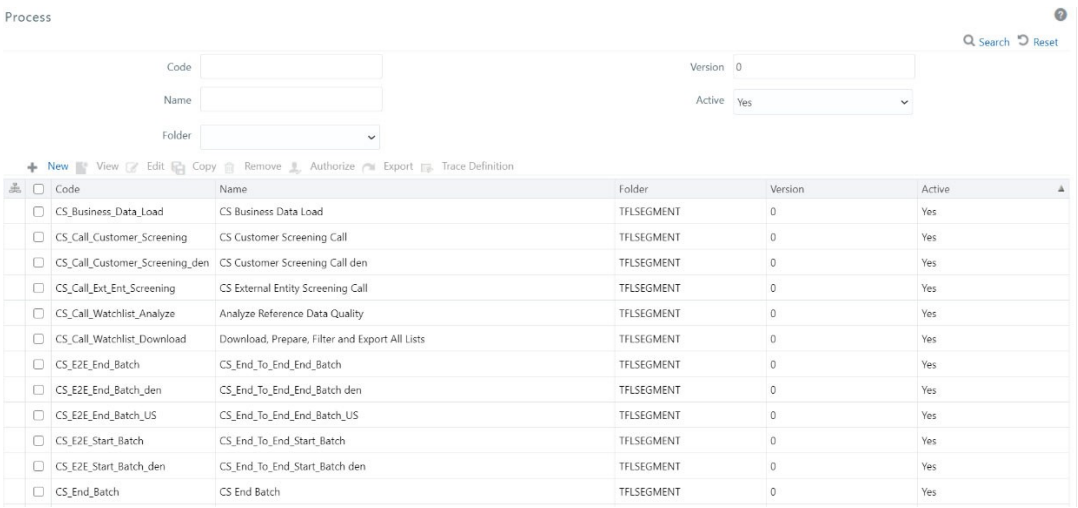
After you click **Save**, the new run name appears in the **Run** page.

Figure D-5 New Run Name in Run Page



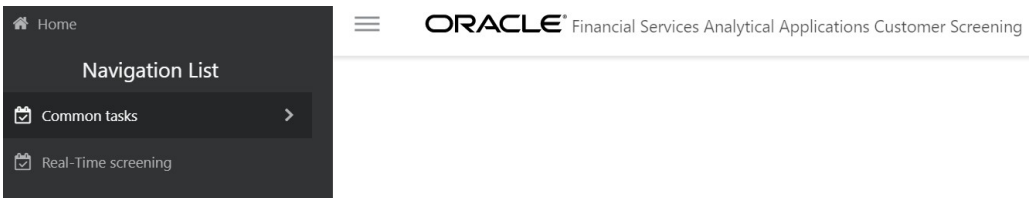
6. Duplicate the `CS_E2E_Start_Batch`, `CS_Call_Customer_Screening`, and `CS_E2E_End_Batch` processes in the **Process** page.

Figure D-6 Process Page



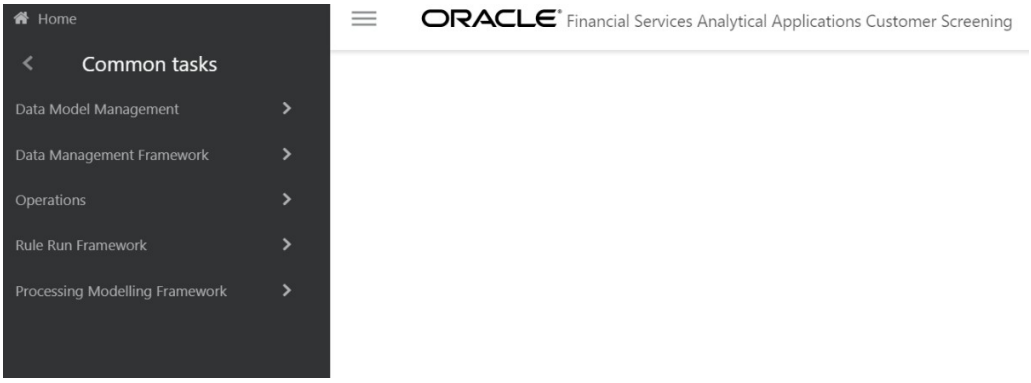
7. Follow these steps to access the **Process** page:
   a. Login as the administrator. The **Financial Services Analytical Applications Customer Screening** home page appears.

Figure D-7 Financial Services Analytical Applications Customer Screening Home Page



   b. Click the hamburger icon to view the Application Navigation List.

Figure D-8 Application Navigation List



c. From the **Application Navigation List**, select **Common Tasks**, then select **Rule Run Framework**, and then select **Process**. The **Process** page appears.

8. To duplicate each process, follow these steps:

   a. For the `CS_E2E_Start_Batch` process:

      i. In the **Process** page, select `CS_E2E_Start_Batch` and click **Copy**. The Process page opens in copy mode.

> **Note**
>
> You must select the segment folder for the Sanctions pack in the **Folder** field to proceed.

      ii. Enter a new process code in the **Code** field and a new process name in the **Name** field. You can also alter the existing process code or name. For example, `CS_E2E_Start_Batch_den`.

      iii. Click **Save**.

   b. For the `CS_Call_Customer_Screening` process:

      i. In the **Process** page, select `CS_Call_Customer_Screening` and click **Copy**. The **Process** page opens in copy mode.

      ii. Enter a new process code in the **Code** field and a new process name in the **Name** field. You can also alter the existing process code or name. For example, `CS_Call_Customer_Screening_den`.

      iii. Click **Save**.

   c. For the `CS_E2E_End_Batch` process:

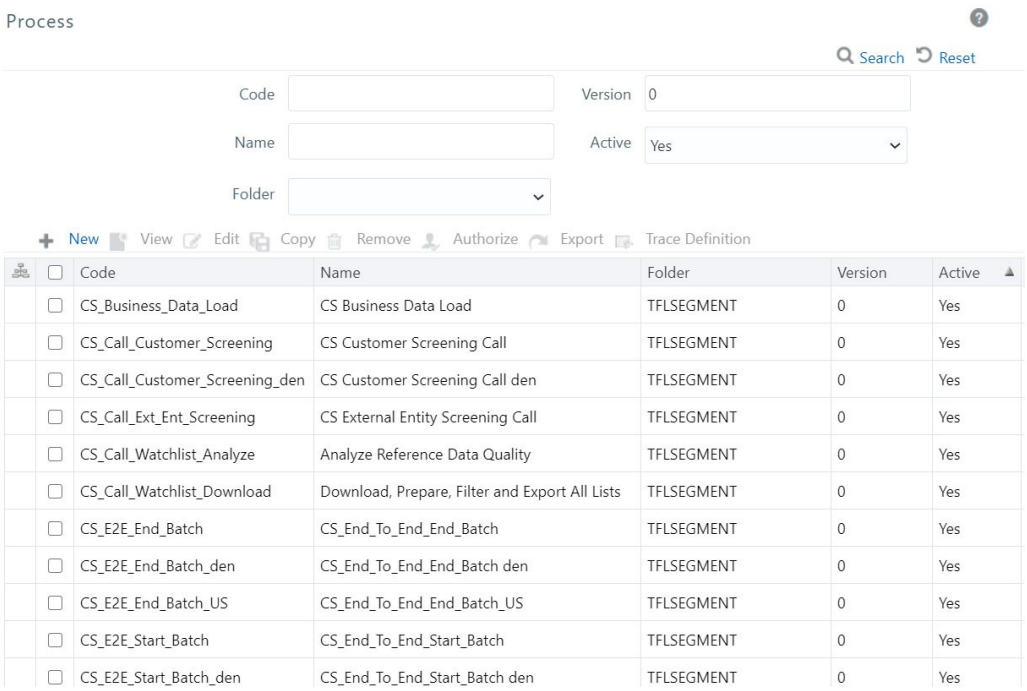
      i. In the **Process** page, select `CS_E2E_End_Batch` and click **Copy**. The Process page opens in copy mode.

      ii. Enter a new process code in the **Code** field and a new process name in the **Name** field. You can also alter the existing process code or name. For example, `CS_E2E_End_Batch_den`.

      iii. Click **Save**.

      After you click Save, the new process names appear in the Process page.

Figure D-9 New Process Names in Process Page



9. Update the group name for the `CS_E2E_Start_Batch_den` and `CS_E2E_End_Batch_den` processes. To do this, run the following query:

   ```
   select * from cs_processing_group
   ```

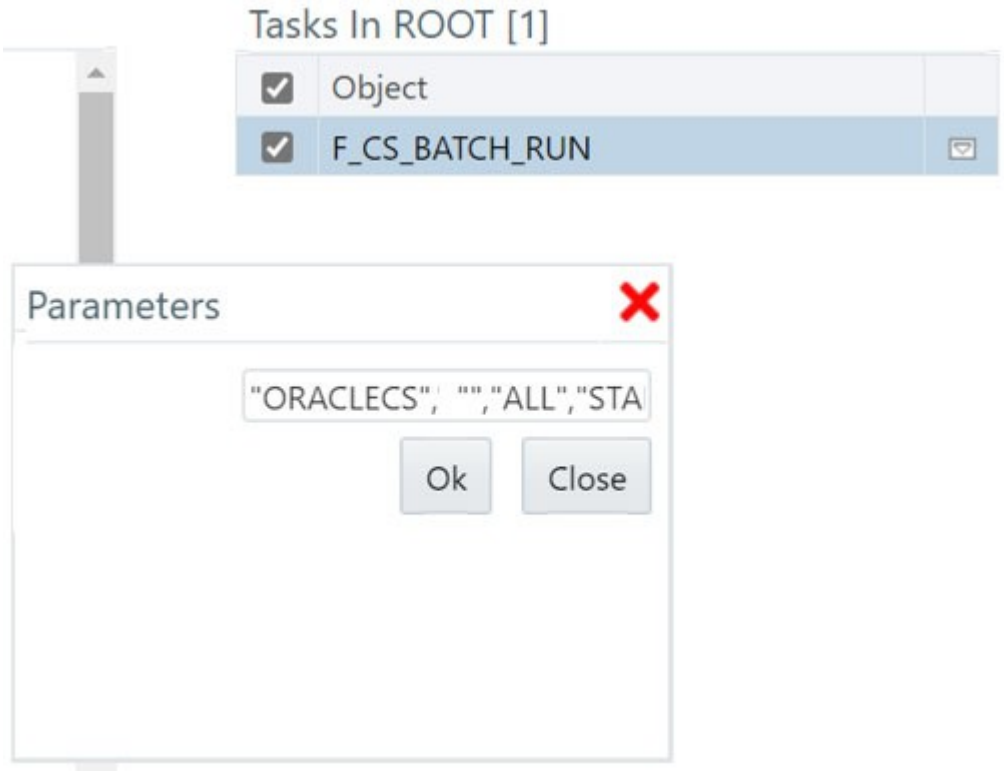
10. Change the parameter for the `CS_E2E_Start_Batch_den` process. To do this, follow these steps:

    a. Select the duplicated process created in the earlier step and click **Edit**. The **Process** page opens in edit mode.

    b. Click **Component**. The **Component Selector** window appears.

    c. Click the drop-down list in line with the **F_CS_BATCH_RUN** task. The **Parameters** window appears.

Figure D-10 Parameter for the CS_E2E_Start_Batch Process



d. Change the `ORACLECS` parameter to the applicable data origin or processing name.

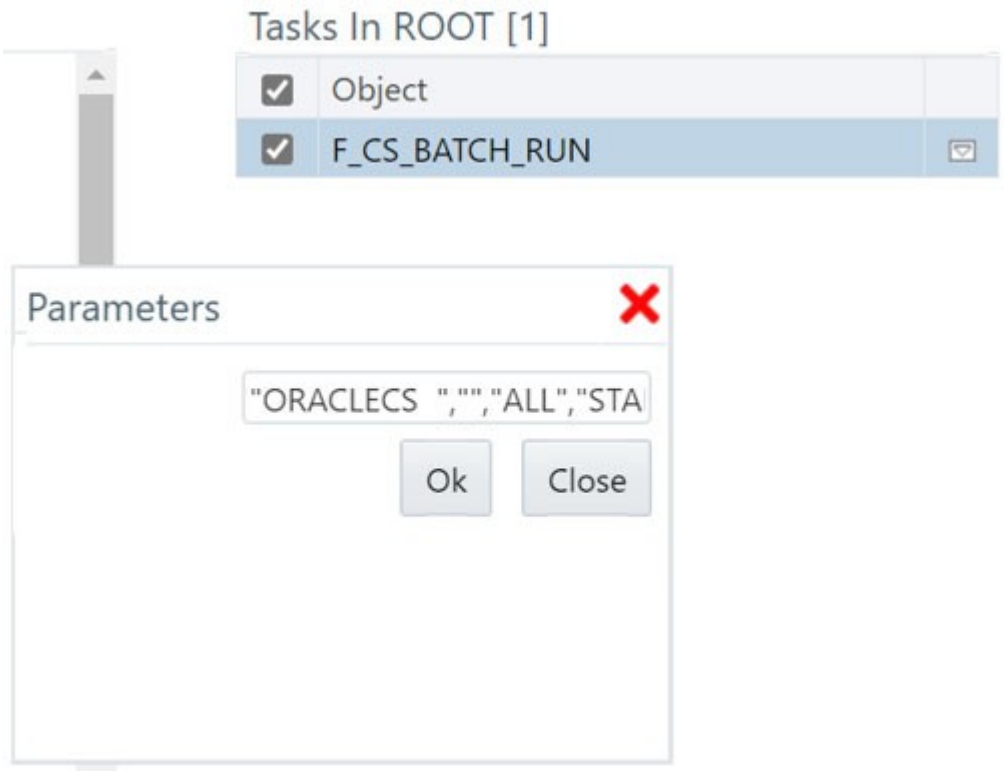
11. Change the parameter for the `CS_E2E_End_Batch_den` process. To do this, follow these steps:

    a. Select the duplicated process created in the earlier step and click **Edit**. The **Process** page opens in edit mode.

    b. Click **Component**. The **Component Selector** window appears.

    c. Select the drop-down list in line with the **F_CS_BATCH_RUN** task. The **Parameters** window appears.

Figure D-11 Parameter for the CS_E2E_End_Batch Process



d. Change the `ORACLECS` parameter to the data origin or processing name.

12. To change the parameters for the `CS_Call_Customer_Screening_den` process, follow these steps:

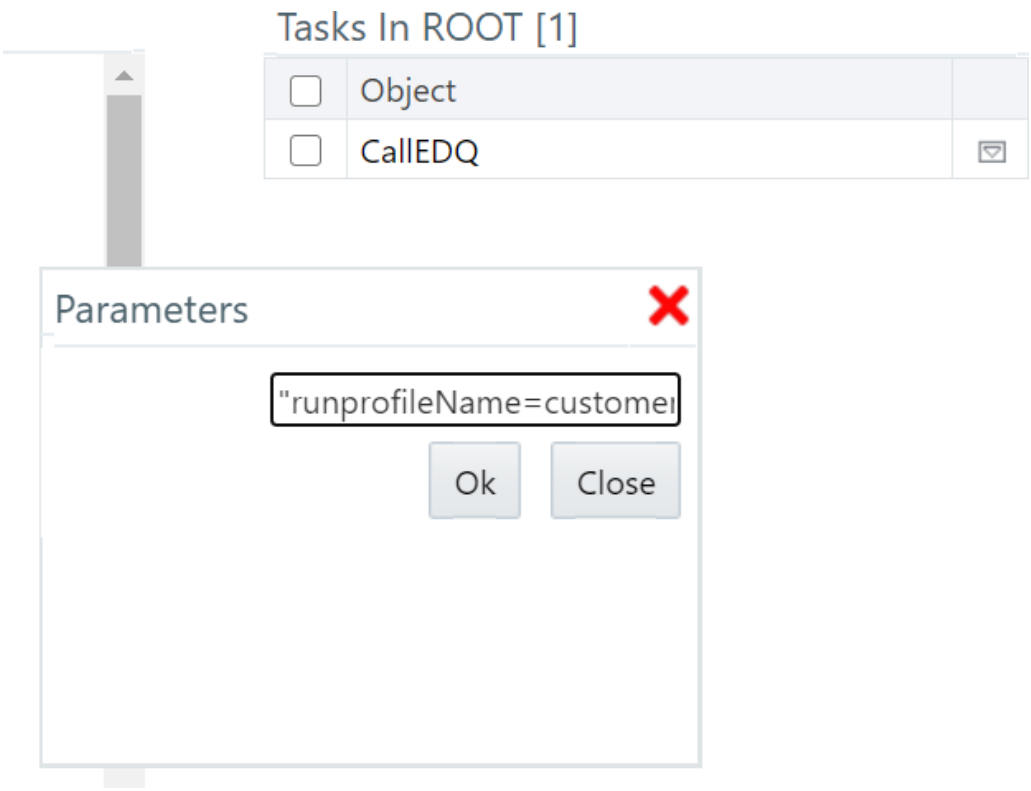
    a. Select the duplicated process created in the earlier step and click **Edit**. The Process page opens in edit mode.

    b. Click **Component**. The **Component Selector** window appears.

    c. Select the drop-down list in line with the **CallEDQ** task. The **Parameters** window appears with the following values:

```
"runprofileName=customer-
screening1.properties","RunLabel=customerscreening","
JobName=MAIN","ProjectName=Customer-
Screening","edqServerName=SERVER_2","condition=and AGE_YR_CT>20 and
BIRTH_DT <= @$~20 June 1972@$~"
```

Figure D-12 Parameters for the CS_Call_Customer_Screening_den Process



d. Change the following parameters:

   i. Run profile name
   Example: `runprofileName=customer-screening1.properties"`

   ii. EDQ server name. If you do not change the server name, it is replaced with the server name in the `cs_appln_params` table.
   Example: `"edqServerName=SERVER_2"`

   iii. Condition. By default, a single condition is provided. Use and to give more than one condition.
   Example: `"condition=and AGE_YR_CT>20 and BIRTH_DT <= @$~20 June 1972@$~"`

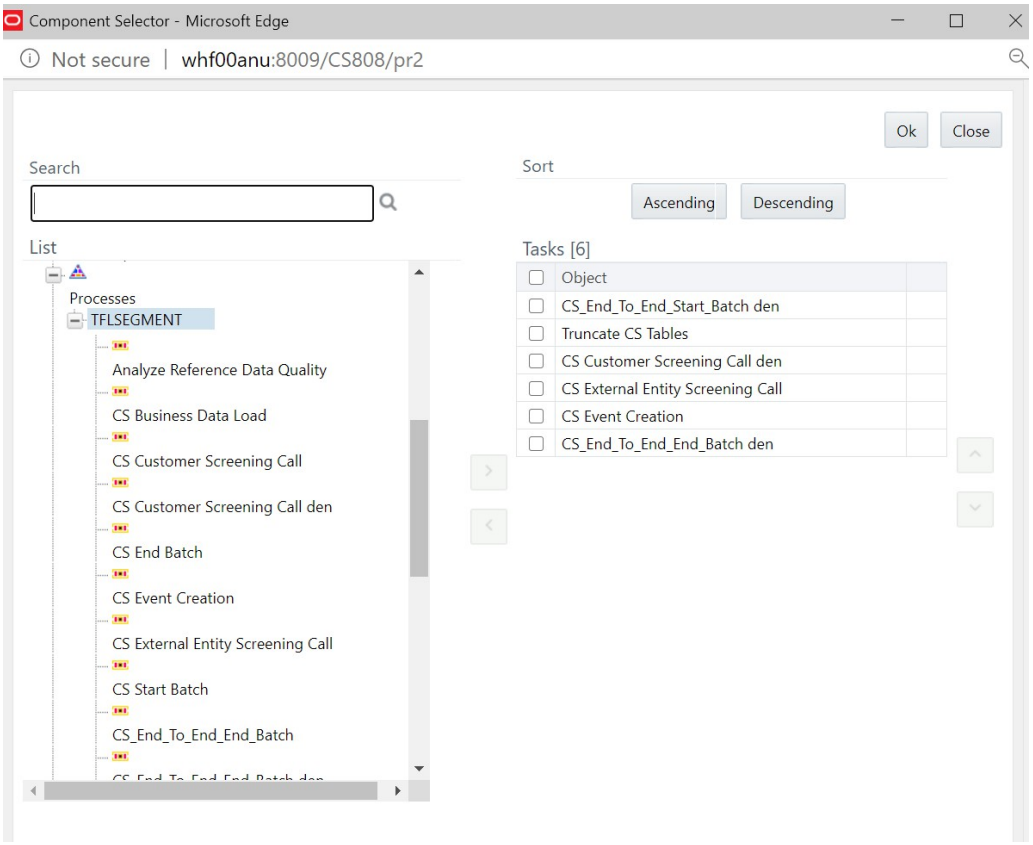
> **Note**
>
> a. It is not mandatory to provide a condition.
>
> b. Provide the expression `@$~` to use alphanumeric characters for fields such as customer birth date. For example, `"condition=and AGE_YR_CT>20 and BIRTH_DT <= @$~20 June 1972@$~"`.

13. Replace the new batches in the **Run** page. To do this, follow these steps:

   a. Select `CS_Data_L_Event_Generation_Den` and click **Edit**. The **Run** page opens in edit mode.

   b. Click the **Selector** drop-down list and select **Job**. The **Component Selector** window appears.

Figure D-13 Parameters for the CS_Call_Customer_Screening_den Process



c. In the **List** hierarchy window, expand the **Transformation Rules** node.

d. Expand the **Processes** node and then the **TFLSEGMENT** node.

e. In the **Tasks** table, select the original processes, which are `CS_End_To_End_Start_Batch`, `CS Customer Screening Call`, and `CS_End_To_End_End_Batch`. These processes must be selected one at a time.

f. Click **Move**  . The selected batches are displayed in the **TFLSEGMENT** node.

g. In the **List** table, select the new processes, which are `CS_End_To_End_Start_Batch_den`, `CS Customer Screening Call den`, and `CS_End_To_End_End_Batch_den`.

h. Click **Remove**  . The selected batches are displayed in the Tasks table.

i. Click **OK**.

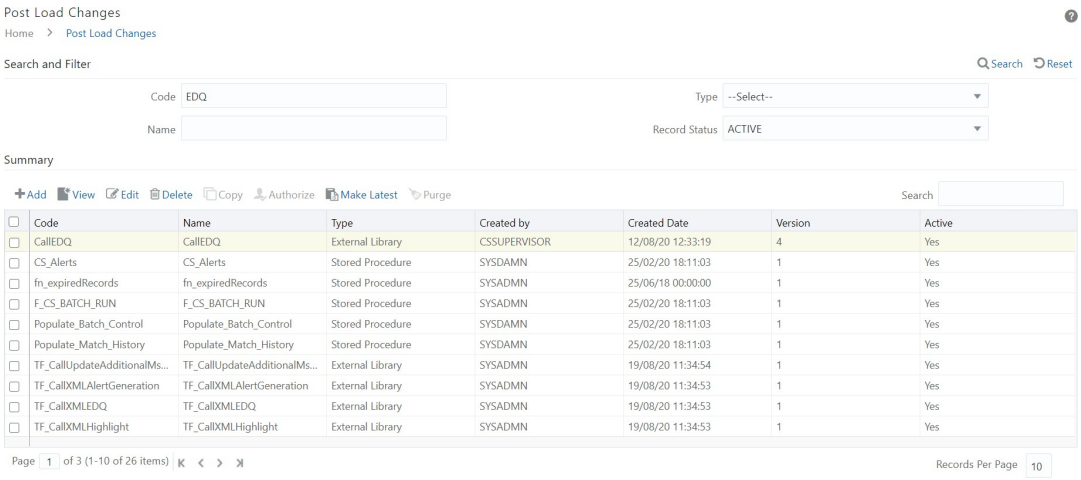
The duplicate jobs are now split across servers using the `CS_End_To_End_Start_Batch`, `CS Customer Screening Call`, and `CS_End_To_End_End_Batch` batches.

D.1 Adding Input Parameters for the CallEDQ Task

Finally, add the new EDQ server name and applicable condition as input parameters in the **Post Load Changes** page as shown in the following steps:

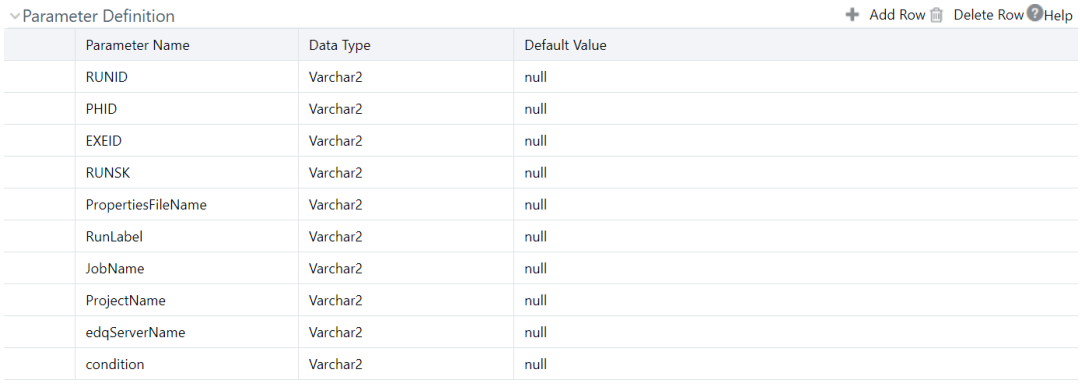
1. Click the **hamburger** icon to view the Application Navigation List.
2. From the **Application Navigation List**, select **Common Tasks**, then select **Data Management Framework**, then select **Data Management Tools**, and then select **Post Load Changes**. The **Post Load Changes** page appears.

Figure D-14 Post Load Changes Page



3. Search for Call EDQ in the **Code** field and select it.
4. Click **Edit**.
5. In the **Transformation Process Flow** section, select **Input Parameters**. The Input parameters appear in the **Parameter Definition** section.
6. Click **Add Row** to add a row. You must add two rows, one for the EDQ server name and one for the condition.

Figure D-15 Adding Input Parameters



7. Click **Finish**.
   To verify the batch execution logs for the EDQ tasks, see the `FIC_HOME/ficdb/bin/CS_EDQ_CALL log` file.

D.2 Fix for Primary Key Constraints

The Multi EDQ Screening process fails when you try to insert in the CS_WATCHLIST table, due to an interlock problem at the database level when two or more of the EDQ try to perform

an action over the same database. You will experience a unique constraint as multiple systems are trying to update the same data.

The error caused due to locking of the record is removed by a creating multiple EDQ instances and then insert data into the temporary table by running CS batch.

For example, consider five EDQ server instances. Error is caused when the five EDQ servers are loaded into the same `CS_WATCHLIST` table. To overcome the scenario, five temporary tables (`CS_WATCHLIST1, CS_WATCHLIST2, CS_WATCHLIST3, CS_WATCHLIST4`, and `CS_WATCHLIST5`) are created. Each EDQ servers are individually loaded into each watchlist table, and then the five tables are merged into the `CS_WATCHLIST` table.

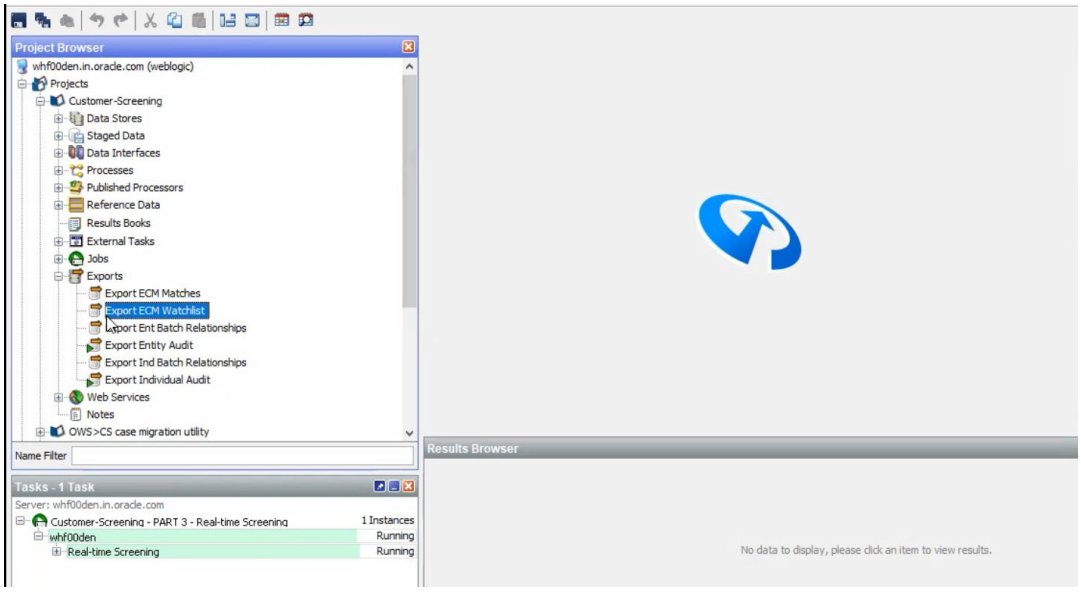
The EDQ application is pre-configured with following five watchlist tables:

- `CS_WATCHLIST1`
- `CS_WATCHLIST2`
- `CS_WATCHLIST3`
- `CS_WATCHLIST4`
- `CS_WATCHLIST5`

If you have multiple EDQ servers, follow the subsequent steps to load the EDQ server to the watchlist table:

1. Log into the EDQ Application.
2. Click **Customer Screening** project from Project Browser. For more information on Importing the OFS Customer Screening Projects, see Oracle Financial Services Sanctions Pack Installation and Configuration Guide.
3. Click **Export ECM Watchlist** in the Export folder under **Customer Screening** project to open the Edit Export Definition page.

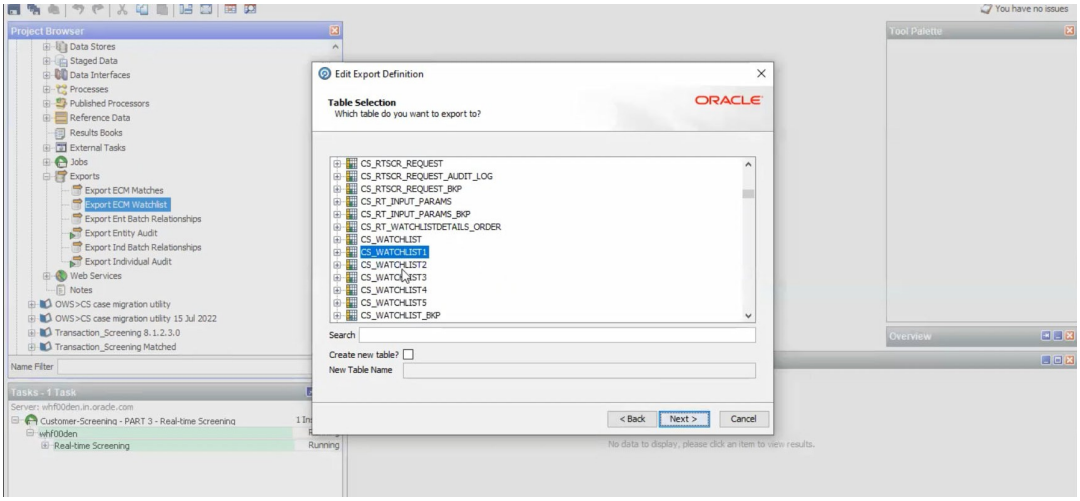
Figure D-16 Export Folder



4. Select the `ECM_Watchlist` data interface from the staged data table and click **Next** to open the data store table. `ECM_Watchlist` is the staged data that you will export.

5. Select the ECM Watchlist Output as data store from the Data Store table and click **Next** to open the Table Selection screen. ECM Watchlist Output is the data store which will be used as the target for the export.
6. In the Table Selection table by default `CS_Watchlist` table is selected. Instead of `CS_Watchlist`, select `CS_Watchlist1` and click **Next** to open Column Mapping table.

Figure D-17 Loading EDQ Server to CS_Watchlist1



7. Click **Next** in Column Mapping table and click Finish the process in Export Name screen. The EDQ server will be loaded to the `CS_Watchlist1`.
   The same procedure steps must be repeated for the remaining EDQ servers if you have multiple EDQ servers.

   Merging the table is a pre-configured procedure. The multiple watchlist table will auto populate to `CS_Watchlist`.

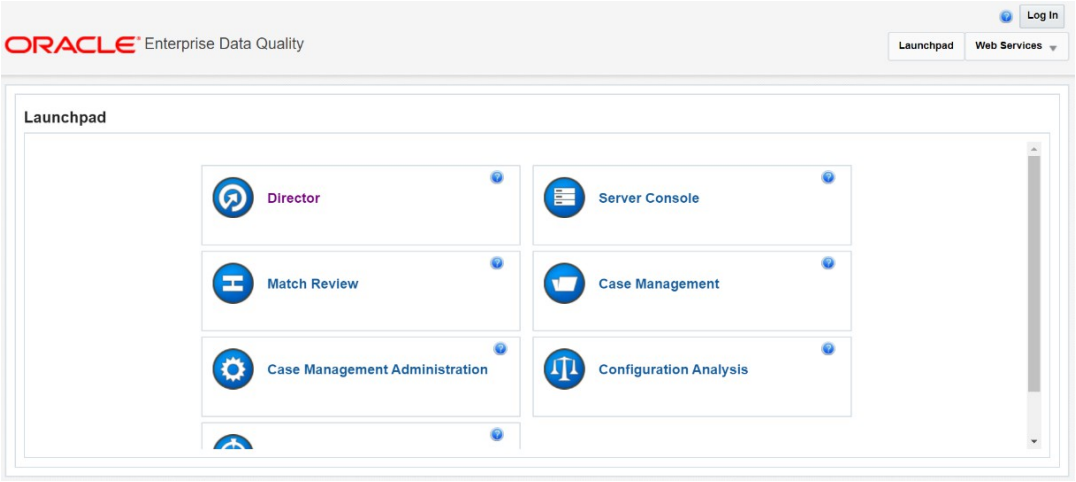
E

Viewing Snapshots of Tables in EDQ

To view a snapshot of a selected table and associated columns in the **Results Browser** pane in Enterprise Data Quality (EDQ), follow these steps:

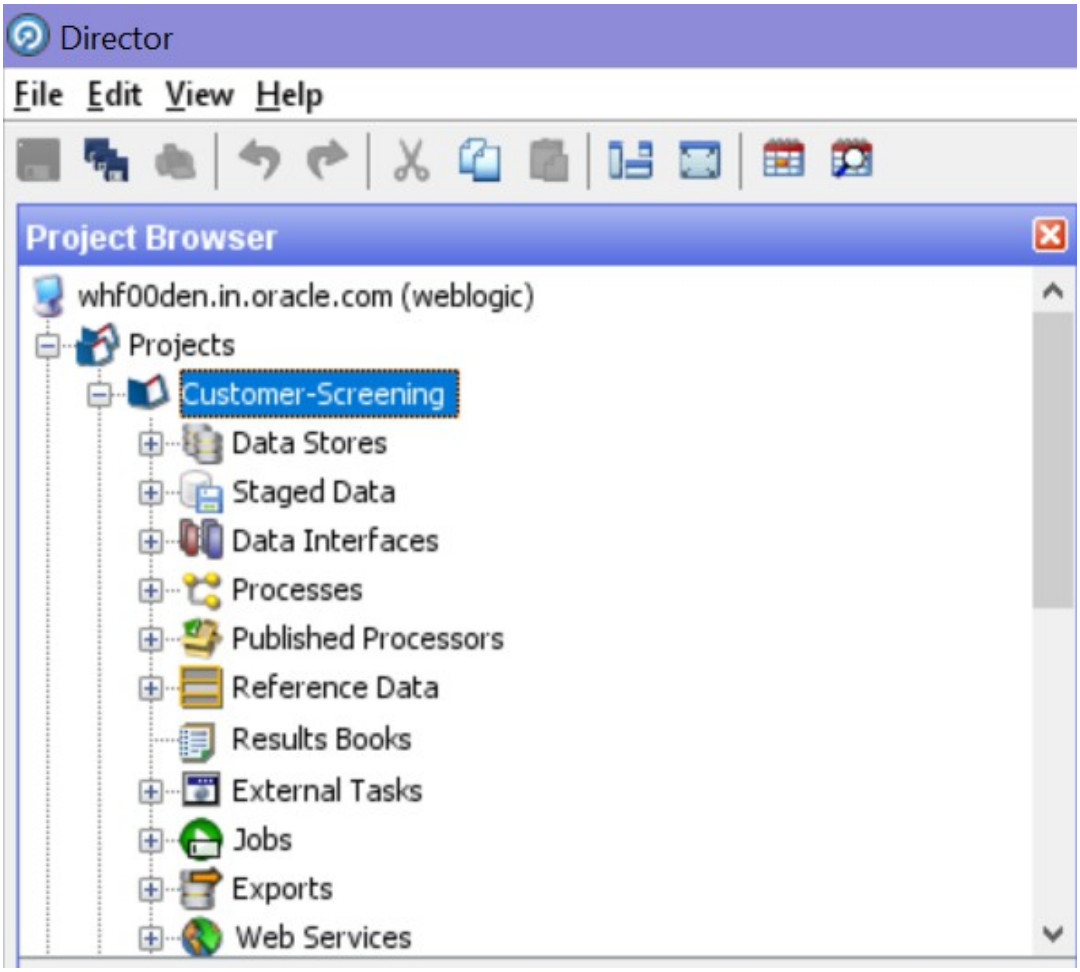
1. Go to the EDQ URL and open the **Director** menu. The **Director** landing page appears.

Figure E-1 Director Menu in EDQ



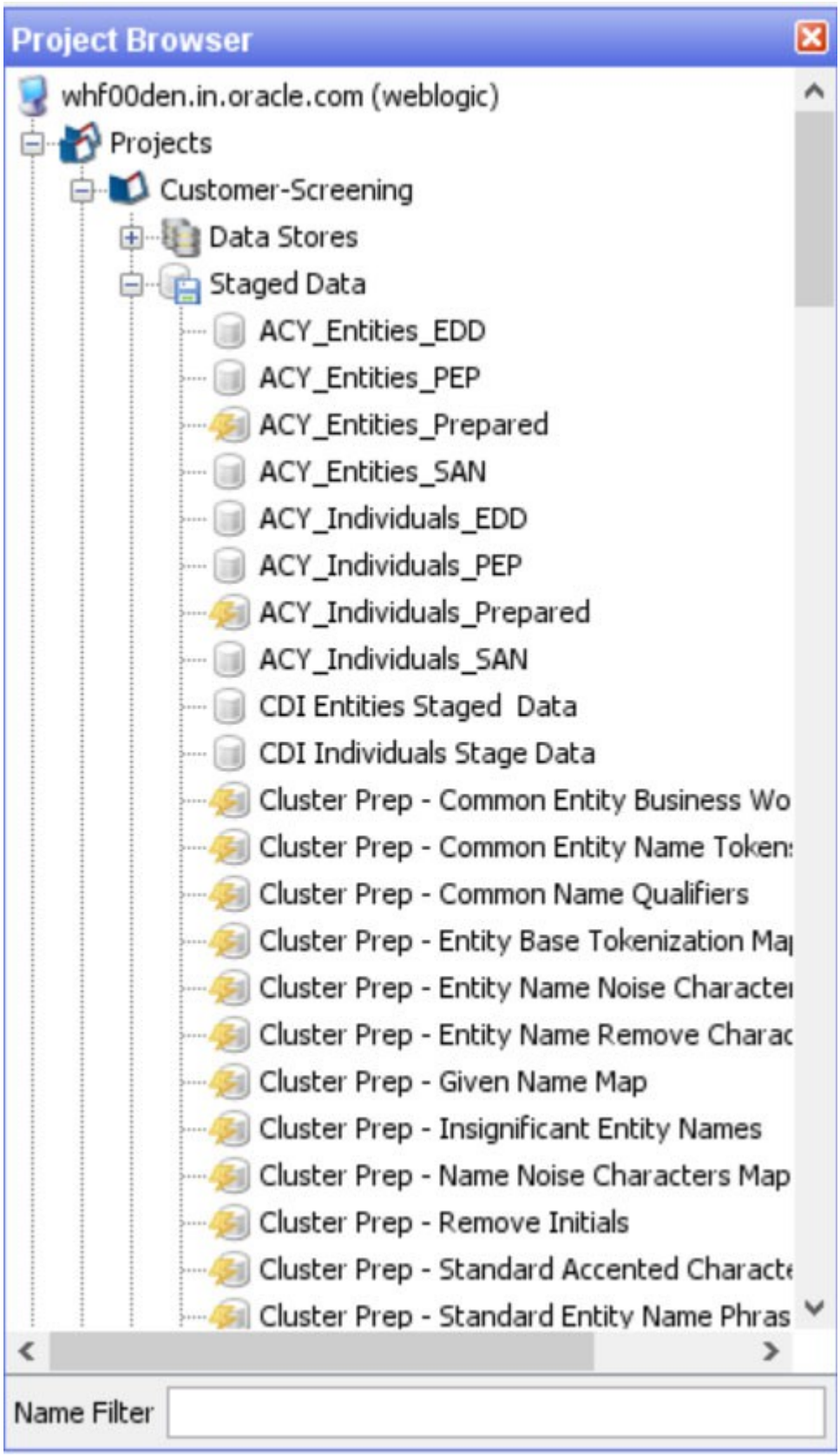
2. In the **Director** landing page, expand the **Customer-Screening** project in the **Project Browser** pane.

Figure E-2 Project Browser Pane



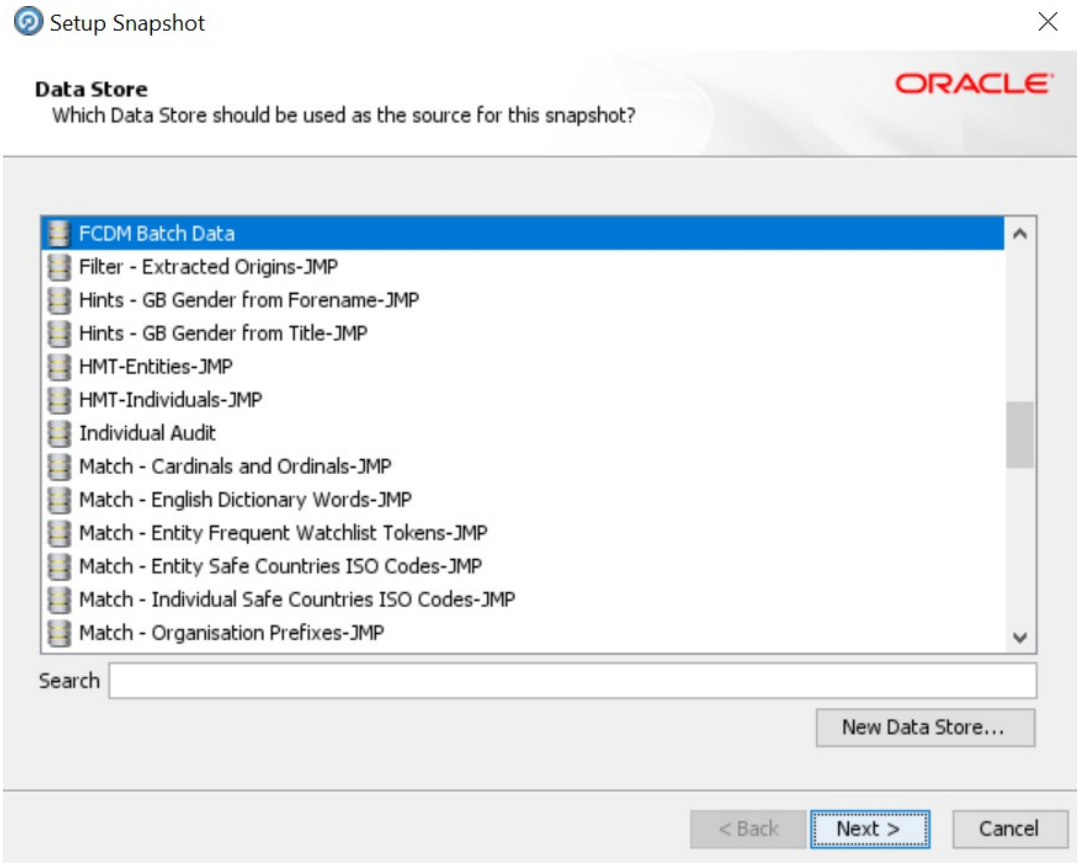
3. Expand the **Staged Data** node and double-click **FCDM Customer Data**.

Figure E-3 FCDM Customer Data Node



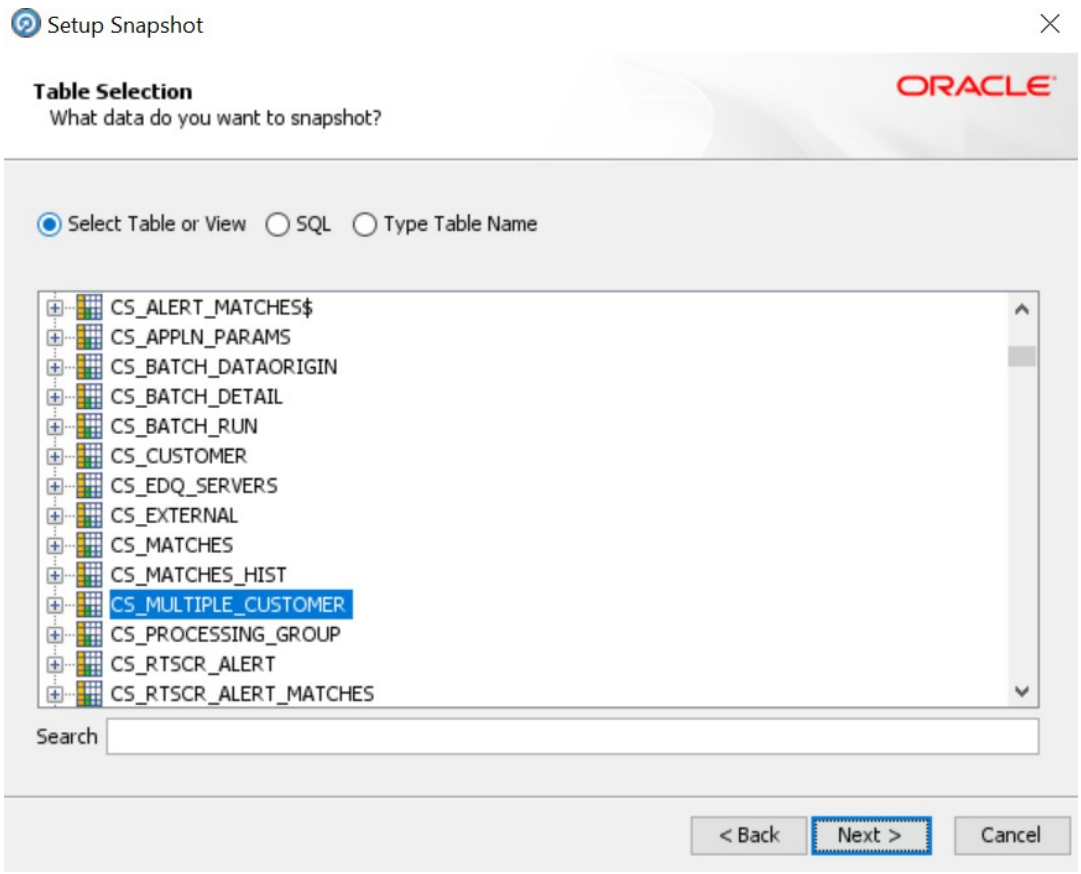
4. In the Setup Snapshot window, double-click **FCDM Batch Data**.

Figure E-4 Setup Snapshot Window



5. The default view is the SQL query. To change the view to a table view, select **Select Table** or **View**.

Figure E-5 Select Table or View



6. Click **Next** until you see the **Finish** button.
7. Click **Finish** to view a snapshot of the selected table in the **Results Browser**.

F

Configurations for the Bearer Token

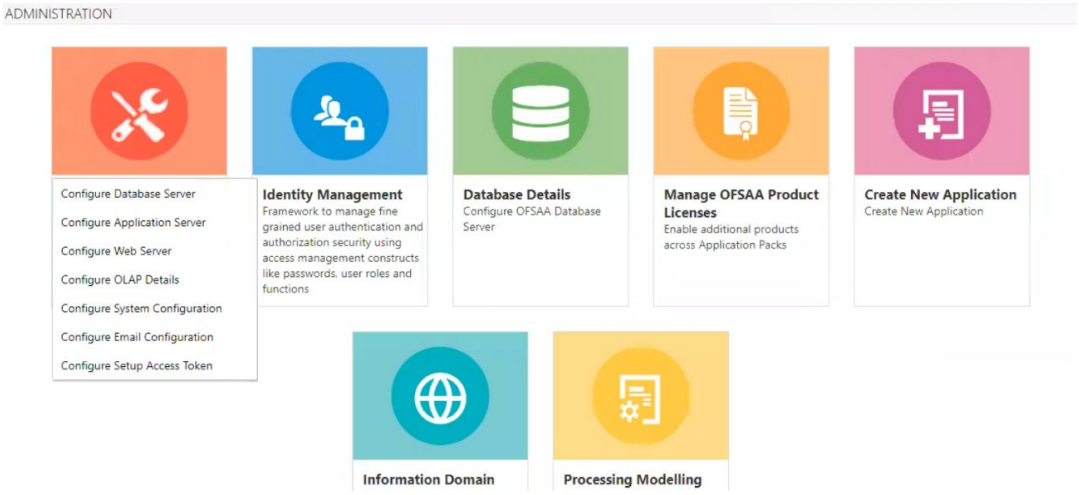
- The following section takes you through the process of generating a token and using it to get the individual or entity JSON, depending on the API request. A token is used to authorize the request.
- You can begin by generating a password for the user who sends the request. After the password is generated, generate a token to authorize this request. The default time for token expiration is 3600 seconds (1 hour) and can be changed. To change the validity, see Change Token Validity.

F.1 Generate User Password

To generate a password for the user, follow these steps:

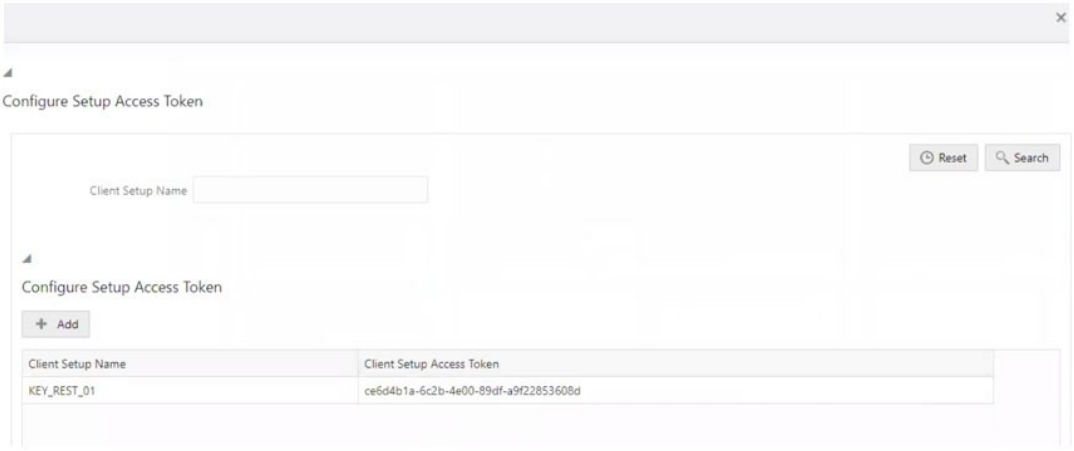
1. Log in as a system administrator.
2. Click **System Configuration** in the **Administration** page and select **Configure Setup Access Token**. The **Configure Setup Access Token** window is displayed.

Figure F-1 Administration Page



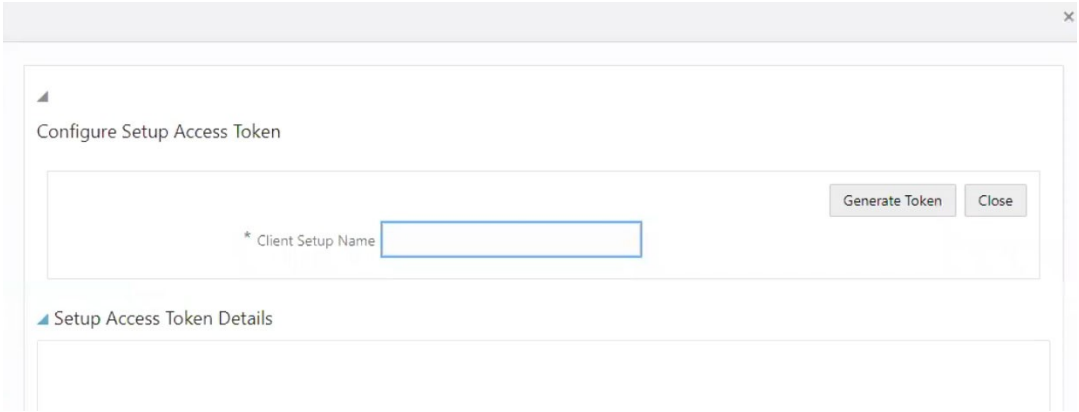
3. In the **Configure Setup Access Token** section, click **Add**. A new window is displayed.

Figure F-2 Configure Setup Access Token



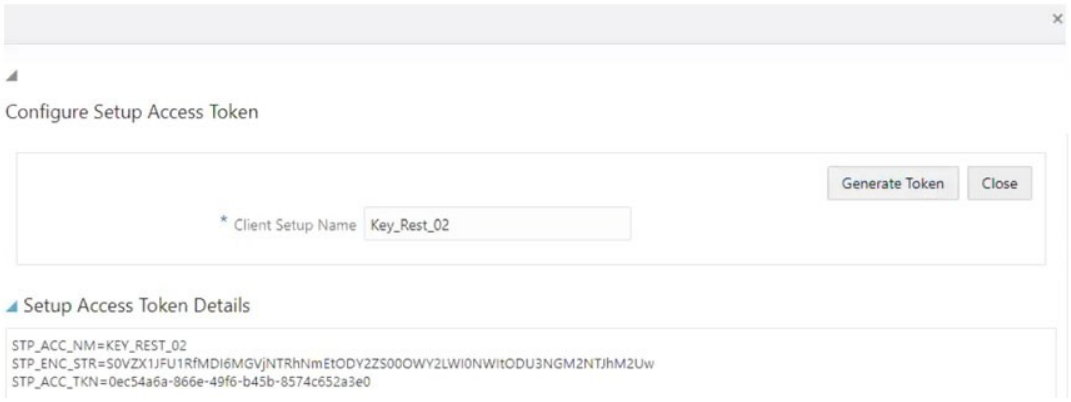
4. Enter the username in the **Client Setup Name** field and click **Generate Token**. The token is displayed in the **Setup Access Token Details** section.

Figure F-3 Generate Token Button



5. Copy and save the text generated in the **Setup Access Token Details** section.

Figure F-4 Setup Access Token Details



The **STP_ACC_NM** field displays the username. The **STP_ACC_TKN** field displays the password.

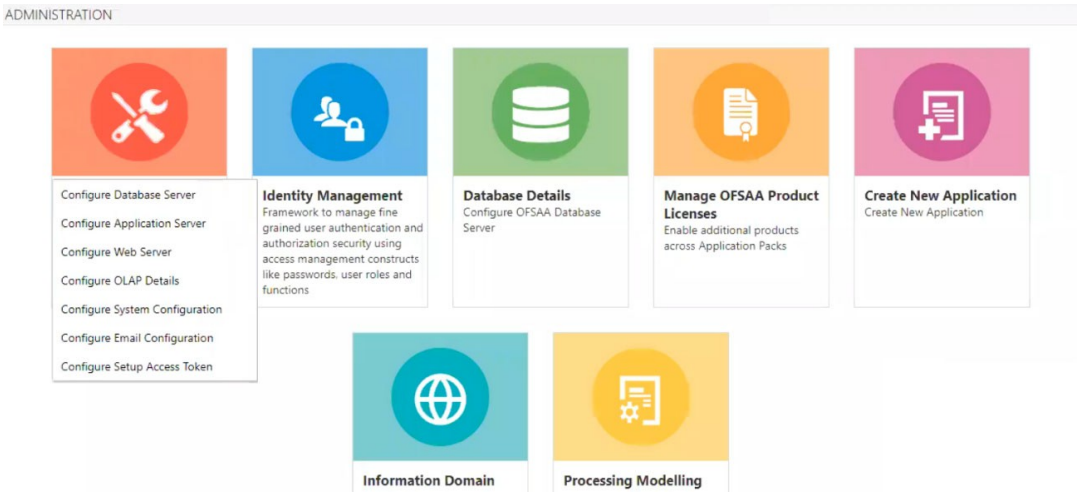
6. Click Close and log out as the system administrator.

F.2 Change Token Validity

To generate a password for the user, follow these steps:

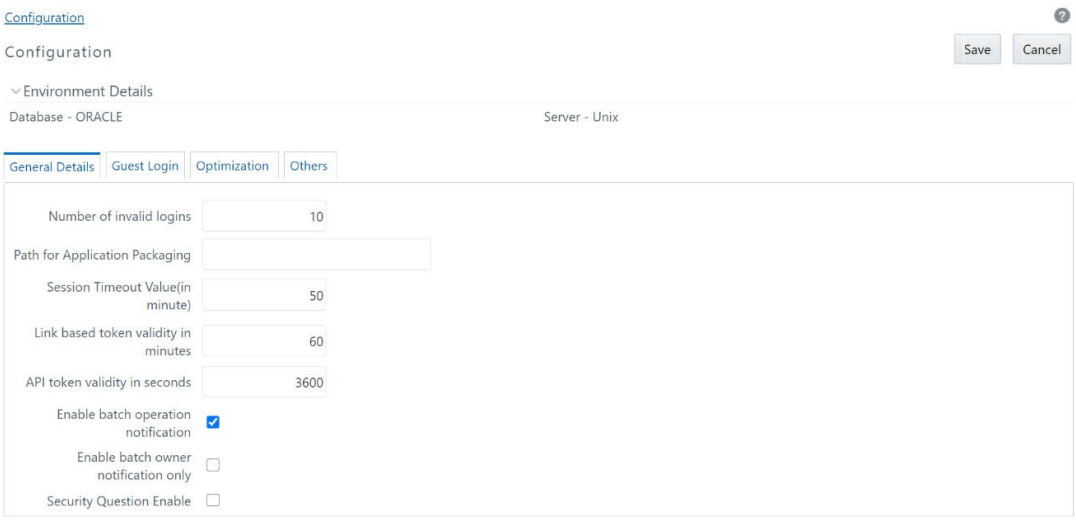
1. Log in as a system administrator.
2. Click **System Configuration** in the **Administration** page and select **Configure System Configuration**. The **Configuration** window is displayed.

Figure F-5 Administration Page



3. In the **Configuration** window, change the token validity time in the **API token validity** in seconds field.

Figure F-6 Configuration window with the API token validity in seconds field shown



4. Click **Save**.

F.3 Generate Token

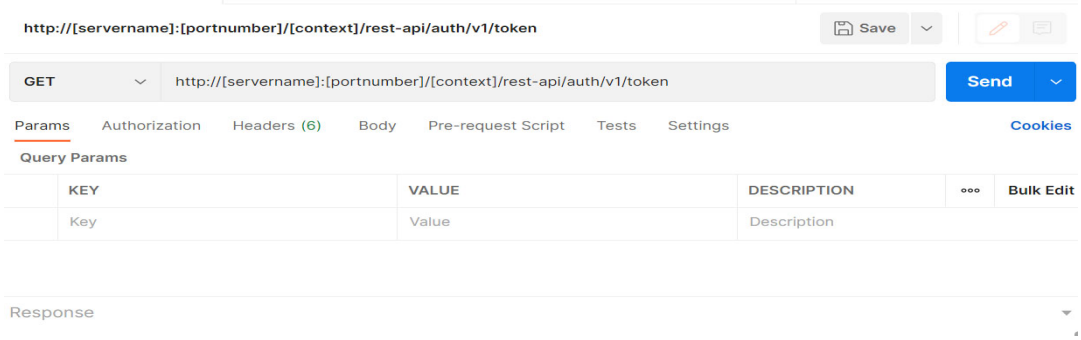
After the password is generated, you can generate the token. To generate the token, open your API client and follow these steps:

> **Note**
>
> - You may use the desktop version of the Postman client to perform these steps. Postman is an open-source, collaborative platform for API development. For more information, see Postman Docs.
> - You can also use any other API client, such as cURL. For more information, see REST APIs for Oracle Database.

1. Open the Postman client and click **Create a request**.
2. Select the request type as **GET** and enter the request URL in the following format:

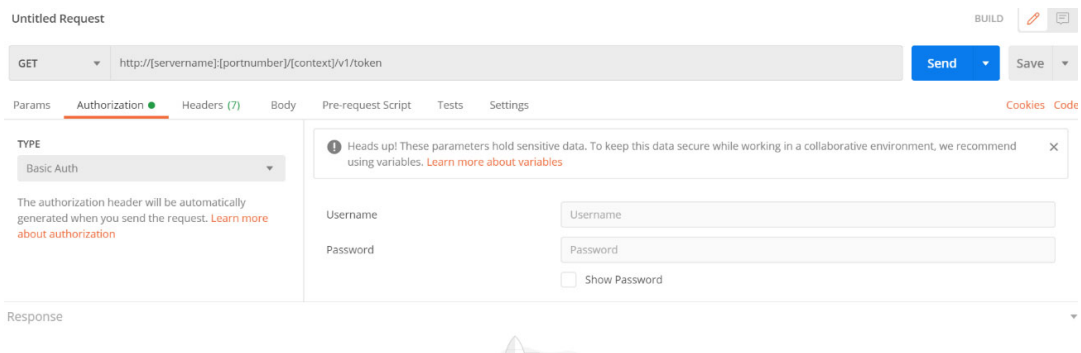
```
http://[servername]:[portnumber]/[context]/rest-api/auth/v1/token
```

Figure F-7 Request



3. Select the **Authorization** menu and then select the **TYPE** as **Basic Auth**.

Figure F-8 Authorization



4. Enter the username and password.
   The username is the value generated for the **STP_ACC_NM** attribute and the password is the value generated for the **STP_ACC_TKN** attribute.
5. Click **Send**. The token is displayed in the **Response** field.

Figure F-9 Response

F.4 Send Requests

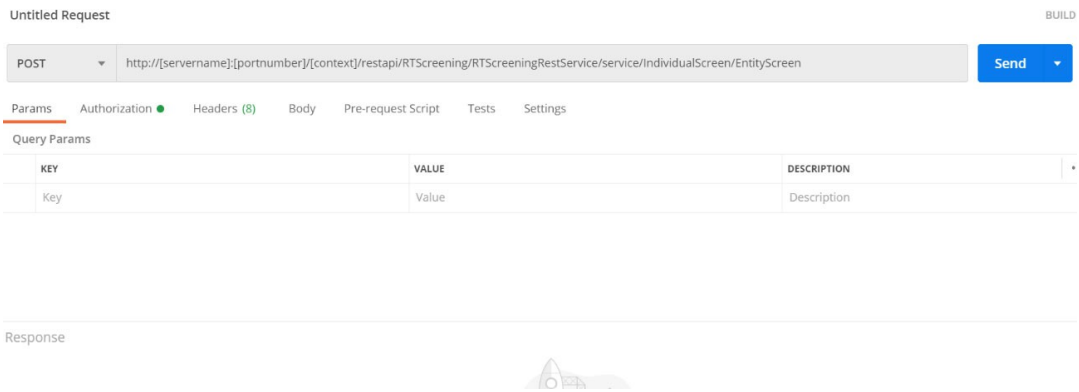
1. Requests are sent using the **POST** request feature. Use the token generated to authorize the request and pass the JSON in the correct format.

> **Note**
>
> - You may use the desktop version of the Postman client to perform these steps. Postman is an open-source, collaborative platform for API development. For more information, see Postman Docs.
> - You can also use any other API client, such as cURL. For more information, see REST APIs for Oracle Database.

2. In the Postman client, select the request type as **POST** and enter the request URL in the following format:

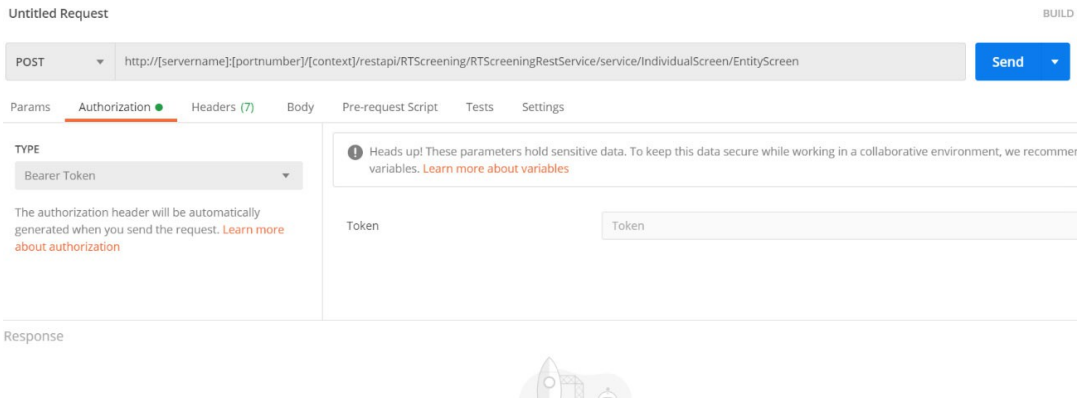
```
http://[servername]:[portnumber]/[context]/rest-api/RTScreening/
RTScreeningRestService/service/IndividualScreen/EntityScreen
```

Figure F-10 Request



3. In the **Authorization** menu, select the **TYPE** as **Bearer Token**.

Figure F-11 Authorization



4. Paste the token generated in the Token field.
5. Click **Send**. The JSON is displayed in the **Response** field. A sample JSON is shown:

```
{
            "Jurisdiction": "AMEA",
            "BusinessDomain":"d",
            "FamilyName": "HAMMAD",
            "GivenNames": "Fathi Ahmad"
            }
```

G

Error Logs

The following are the types of failures you may encounter:

- EDQ Failure
- Data Model
- Failure Batch
- Failure DM Utility Failure

EDQ Failure

If there is an EDQ failure, follow these steps.

1. Go to the following path, where the EDQ is installed.

   ```
   {domain_path}/servers/edq_server1/logs/edq/logs.
   ```

2. Open the file name (`main0.log`).
3. Rectify the errors that you find in the logs.

Data Model Failure

If there is a data model failure, follow these steps.

1. Go to the following path.

   ```
   {ftpshare_path}/{infodom}/logs.
   ```

2. Check for the latest file and rectify the error according or raise an SR to support.

Batch Failure

If there is batch failure, follow these steps.

1. Go to the following path.

   ```
   {ftpshare_path}/logs/{BatchDate}/{infodom}/TRANSFORM DATA.
   ```

2. Search for the log file with task ID. Rectify the relevant error.

DM Utility Failure

If there is DM Utility failure, follow these steps.

1. Log in to Atomic Schema and search for the table FCC_DM_AUDIT.
2. This table has all the logs for the current running batch.
3. Rectify the relevant error.

H

Out Of Box process to move Alerts from CS_ALERTS of one DB instance to FCC_ZCS_ALERTS of another DB instance

The `Oracle_CS_Zipper_Processing` run, present under the Run screen of Rule Run Framework, handles data movement from the `CS_ALERTS to FCC_ZCS_ALERTS`. It is configured to Out of Box (OOB) to move this data on the same instance.

The following are the steps to move data from one DB instance to another:

> **Note**
>
> The following configurations must be done on the instance where the Zipper UI is present.

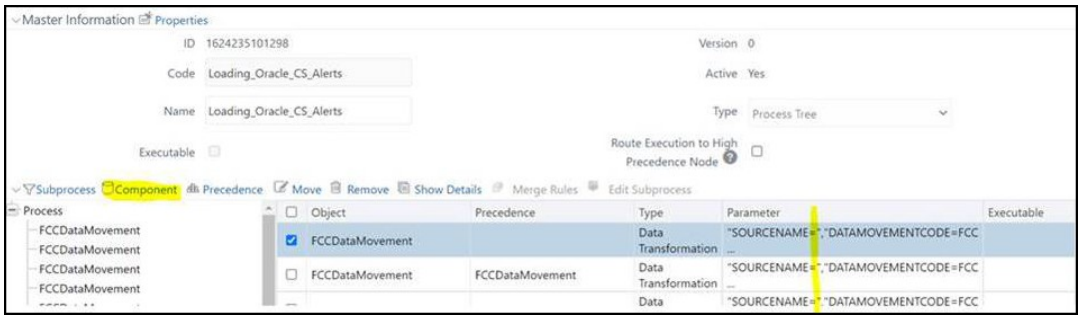
The `Oracle_CS_Zipper_Processing` run intern calls `Loading_Oracle_CS_Alerts` process, which is present under the Process screen of Rule Run Framework. This process is responsible for moving the `CS_ALERTS` data from the source system to the destination system.

1. Create a DB link in the Zipper UI database by giving the DB details of source system database details where `CS_ALERTS` are present.
2. Login with CS Admin in the Zipper UI instance and navigate to `Common Tasks > Rule Run Framework>Process`.
3. Select the check box for `Loading_Oracle_CS_Alerts` process name and click **Edit**.
4. In the process details screen, you will see that in the parameters column, `SOURCENAME` and `LOADTYPE` is value is empty by default as shown in the below screenshot. Make sure to update these parameters with the following values.
   SOURCE NAME: Enter the name of the DB link which is created in Step 1.

   LOADTYPE: Enter the value as DBLINK.

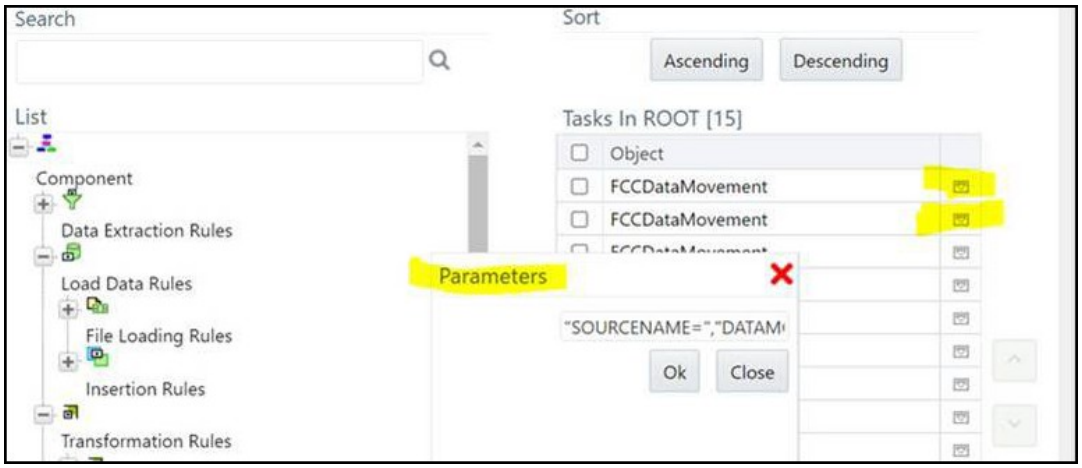
   Example:`"SOURCENAME=SOURCE1_DB_LINK_NAME","DATAMOVEMENTCODE=FCC_ZCS_CUST","LOADTYPE=DBLINK","DATAMOVEMENTOPERATION=IS"`.

Figure H-1 Master Information



5. Click the **Component** button to edit the parameters.
6. In the **Component Selector** popup, on the **TASK** in the **ROOT** section on the right side, against each `FCCDataMovement`, click the down arrow button to edit the parameters as shown in below screenshot.

Figure H-2 Component Selector



7. Give the value for `SOURCENAME` and `LOADTYPE` as suggested in Step d and click **OK** to save.
8. Update the above values mentioned in step 7 to all the `FCCDataMovement` where `SOURCENAME` and `LOADTYPE` are empty..
9. Now, if you create a batch out `Oracle_CS_Zipper_Processing` run in ZIPPER UI Instance and execute it, it will pull the `CS_ALERTS` from the source system and create a zipper alert Zipper UI instance.
   The following are the steps to pull data from multiple source systems in the zipper UI instance:
   a. Enter a DB details of source system database where CS_ALERTS are present to create a DB link in the Zipper UI database for each source system.
   b. Login as a CS Admin in the Zipper UI instance and navigate to `Common Tasks>Rule Run Framework>Process`.
   c. Select the check box for `Loading_Oracle_CS_Alerts` process name and click Copy to create a copy. Create the copies for all source systems.
   d. Now, select Individual Process and click **Edit** and follow the above steps from 4 to 7 and give the respective **SOURCENAME** value and **LOADTYPE** as DBLINK.
   e. Navigate to Common `Tasks>Rule Run Framework>Run`.
   f. Select the check box for `Oracle_CS_Zipper_Processing` run name and click Copy to create a copy.
   g. In the RUN details, enter a Folder name and give a different name for Code and Name fields.
   h. Click on the **Selector** button and then select **Job**.
   i. From the tasks section on the right side, remove the `Loading_Oracle_CS_Alerts`, map the respective process created for a particular source system, and click **OK**.
   j. Verify the **Run Details** screen to see processes are mapped correctly and proceed to finish the steps to complete copying of process.

k. Create a different run for each source system by following the above steps from Step vi to x.

l. Now, if you create a batch out individual source system runs created in ZIPPER UI Instance and execute it, it will pull the `CS_ALERTS` from the respective source system and create zipper alert in Zipper UI instance.

API to create the Alerts in the Zipper Alerts table (FCC_ZCS_ALERTS)

Multiple CS Instances are used for an ad-hoc Screening of Customer and External Entity from the Real-time Screening UI. Following are the steps to configure these systems to create zipper alerts in separate Zipper UI Instances:

1. Navigate to `##FIC_HOME##/ficdb/bin` folder of CS instance, used for ad-hoc screening of Customer and External Entity from Real-time Screening UI.
2. Execute `EDQInsert.sh` bypassing `infodom` along with it.
   Example: `./EDQInsert.sh TFLTINFO`
3. Initially, enter the EDQ server details.
4. If you want to use the **Enterprise Case Management Application (ECM)** or **Customer Screening Alert Management (CSAM)** as an L1 investigation for Real-Time Screening, enter CSAM.
5. Enter the URL of the Zipper UI instance used for Zipper alerts, and if the **Customer Screening Alert Management (CSAM)** application is in the same installation, enter **N**.
6. Enter the user name and password to access the Zipper UI instance URL.
7. Now, if you perform an ad-hoc screening of Customer and External Entity from Real-time Screening UI from CS instance, it will create zipper alerts in Zipper UI instance.
8. Follow the above steps 1 to 7 in all the multiple CS instances used for ad-hoc screening of Customer and External entity from Real-time Screening UI.

> **Note**
>
> The source systems are configured with the **Rest URL** of the CS Instance used for ad-hoc screening of Customer and External Entity from the Real-time Screening UI. In this case, it will still use the same configuration done in the above steps 1 to 7 and creates zipper alerts in the Zipper UI instance.

J

PMF Configurations for Pool of Analyst

To configure the PMF Pool of Analyst configuration to set the new statuses, follow these steps:

1. Perform the following queries and introduce new status in the following tables.
   - Select t.*,rowid from AAI_WF_STATUS_B t where t.v_app_package_id in ('OFS_CS_RT');
   - Select t.*,rowid from AAI_WF_STATUS_TL t where t.v_app_package_id in ('OFS_CS_RT');
   - Create unique v_status_id in AAI_WF_STATUS_B table and map the same in the AAI_WF_ STATUS_TL table and fill all the other columns data. This data will show in the PMF screen while mapping new status.

Figure J-1 Example 1

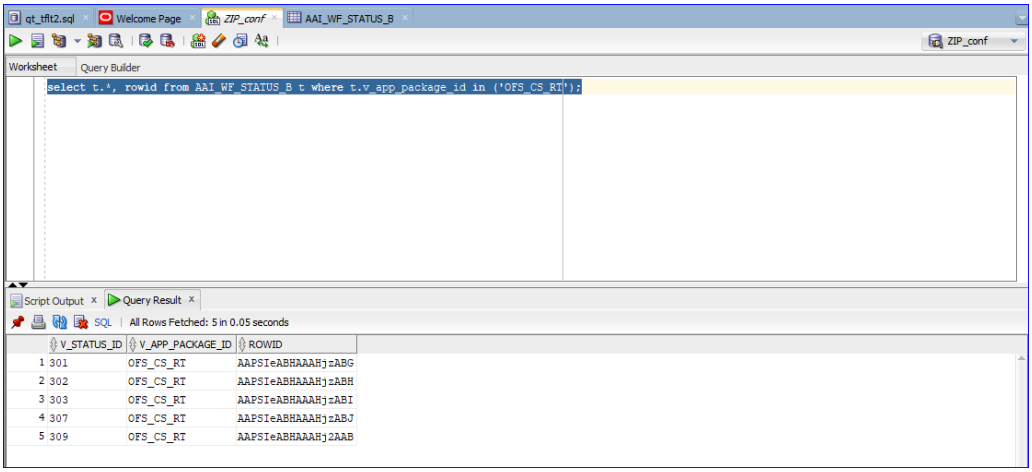
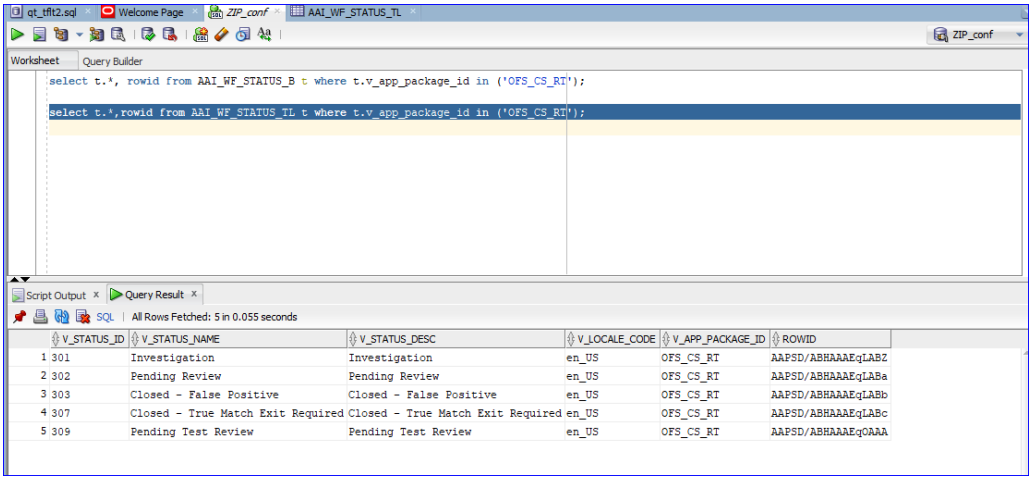


Figure J-2 Example 1 (Contd.)



2. Perform the following query and introduce new Outcome in both the following tables.
   - Select t.*, rowid from AAI_WF_OUTCOME_B t;
   - Select t.*, rowid from AAI_WF_OUTCOME_TL t;
   - Create unique outcome id in AAI_WF_OUTCOME_B table and map the same in AAI_WF_OUTCOME_ TL table and provide other columns data.

Figure J-3 Example 2

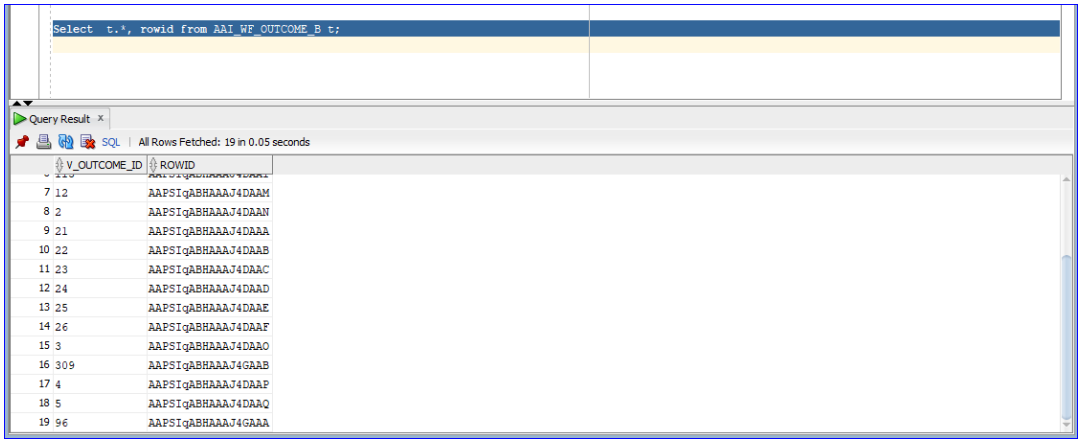
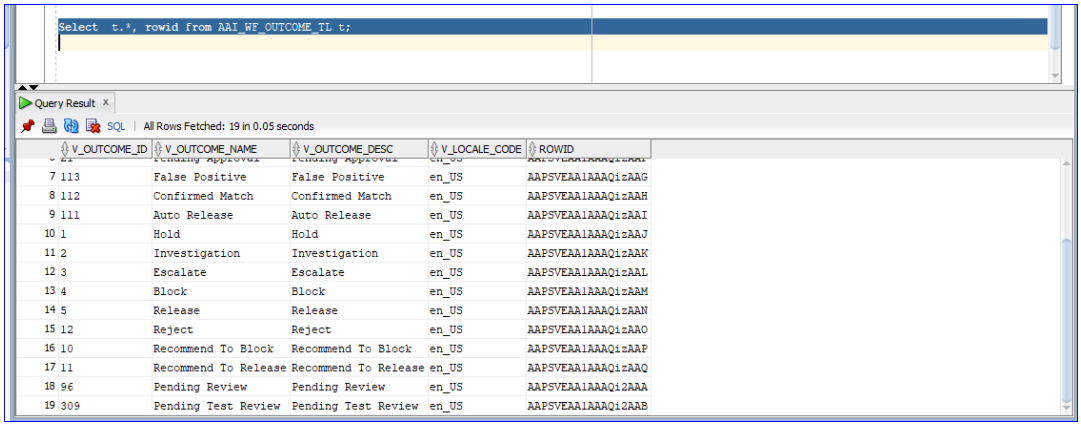


Figure J-4 Example 2(Contd.)



3. In the atomic schema, do the configuration for the following tables:
   Select t.*,rowid from FCC_ZCS_STATUS_dim t;

   Select V_STATUS_CODE, V_STATUS_CODE from fcc_zcs_status_dim;

Figure J-5 Example 3

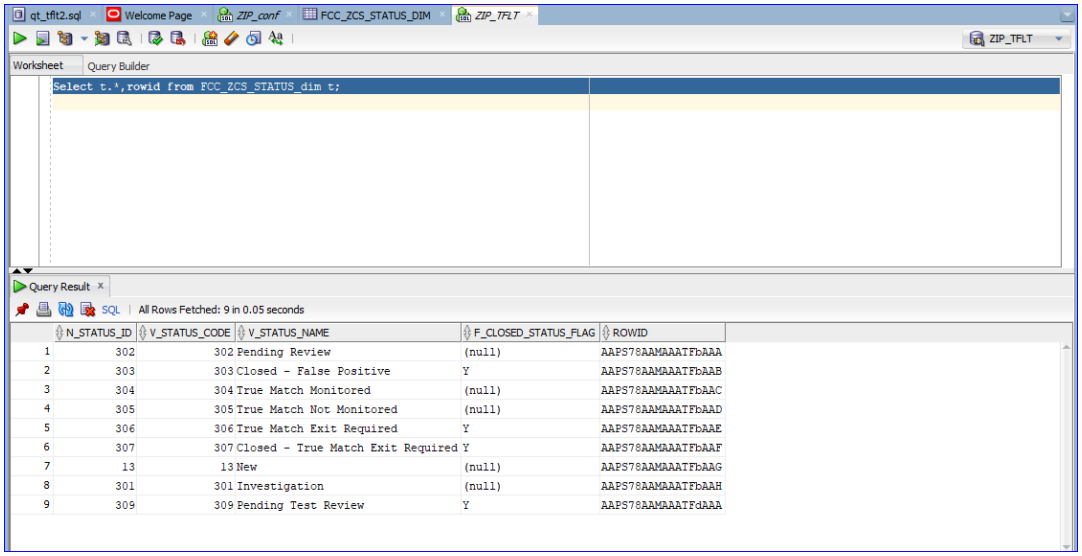
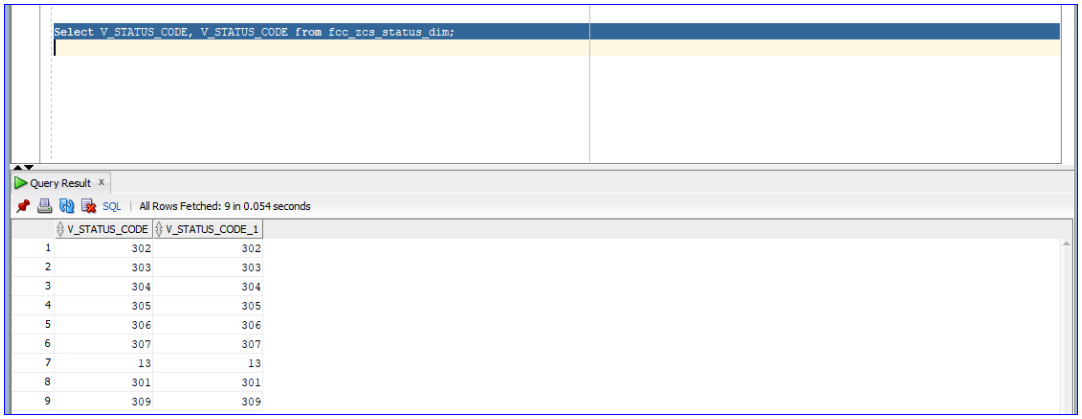


Figure J-6 Example 3 (Contd.)



4. In the following table do the security attribute mapping for the new workflow:
   Select `t.*, rowid from FCC_ZCS_SECURITY_ATTR_GRP_MAP t;`

   In the following table, add the two entries:

   Select `* from cs_appln_params;`

   For the entry `ZCS_ENBL_ANLYST_POOL`, the value must be Y and for the entry `POA_CHECK_STS_CODES`, add the status code of the newly created status.

5. Create Human task in PMF screen that you want to introduce in-between existing status or you want to introduce new status or create separate status.
   Activity

   ---------- Activity Name*

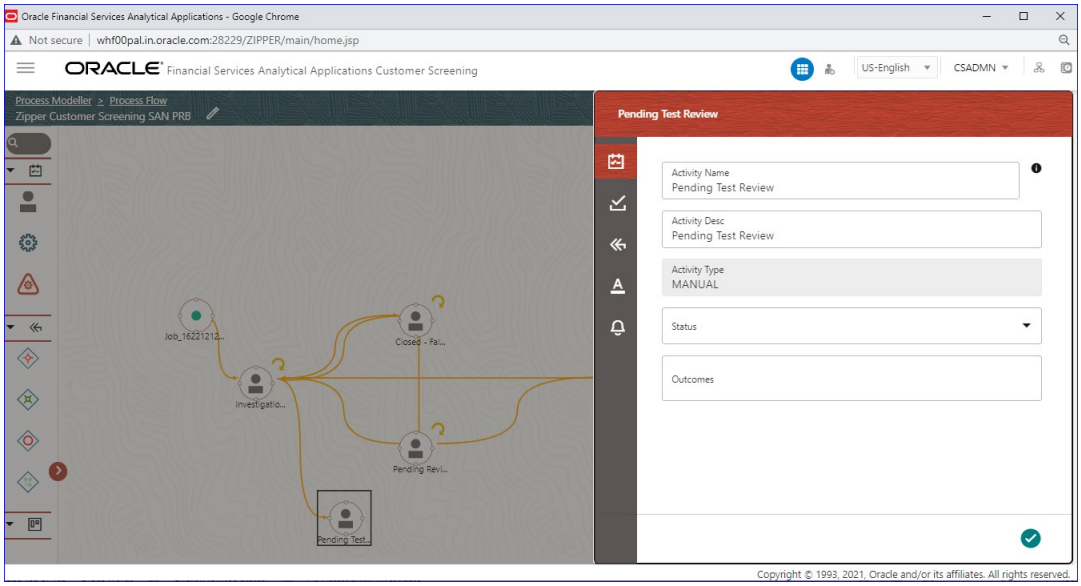
   Activity Description

   Status* - New Status Name.

   Outcomes - Where has to go (Destination Status).

Example: If we have to introduce a new status between Investigation to Pending Review, first add the new activity as shown in the following Figures (Pending Test Review).

Figure J-7 Activity Statuses



Transitions

Add ->

Transition Name - Unique Name for the particular Transition.

Connected To – Destination status.

Decision Rule - Map to decision rule for particular status.

Order - 1

Stroke – Default.

Example: First Transition between **Investigation** to **Pending Test Review** the next one between **Pending Test Review** and **Pending Review**.

Figure J-8 Edit Transaction – Pending Test Review

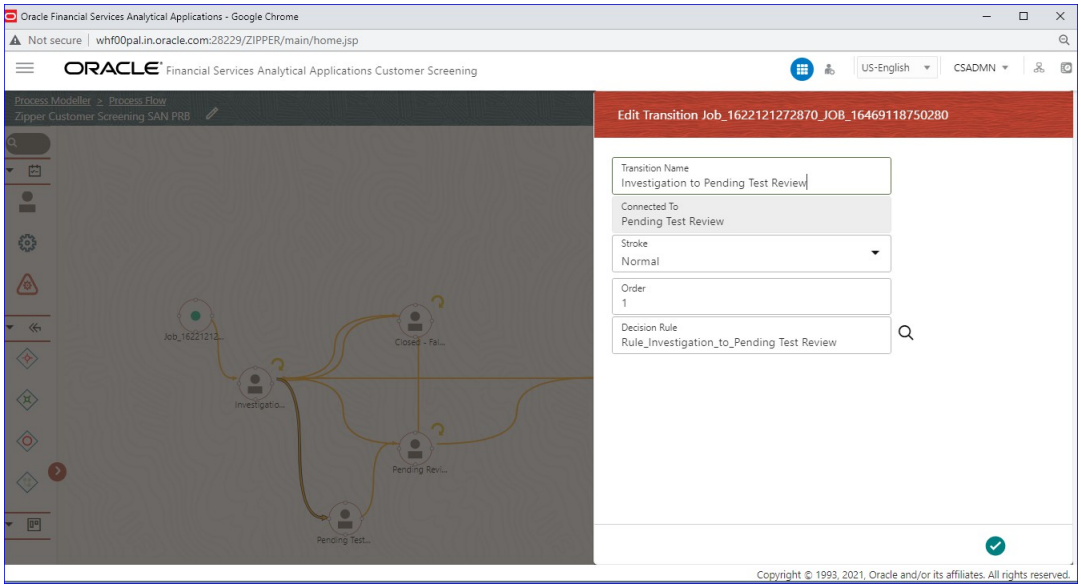
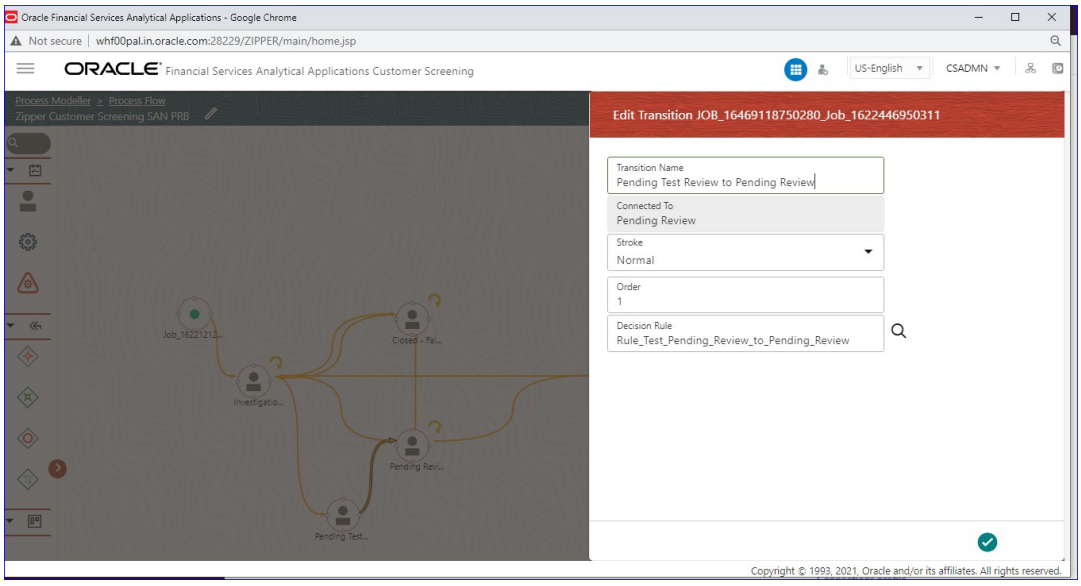


Figure J-9 Edit Transaction – Pending Review



In Transition Decision Rule Map the specified rule for the current status. Or create as per business requirement.

Example: For the decision rules, add the following 2 decision rules.

Figure J-10 Rule Details – Decision Rule 1

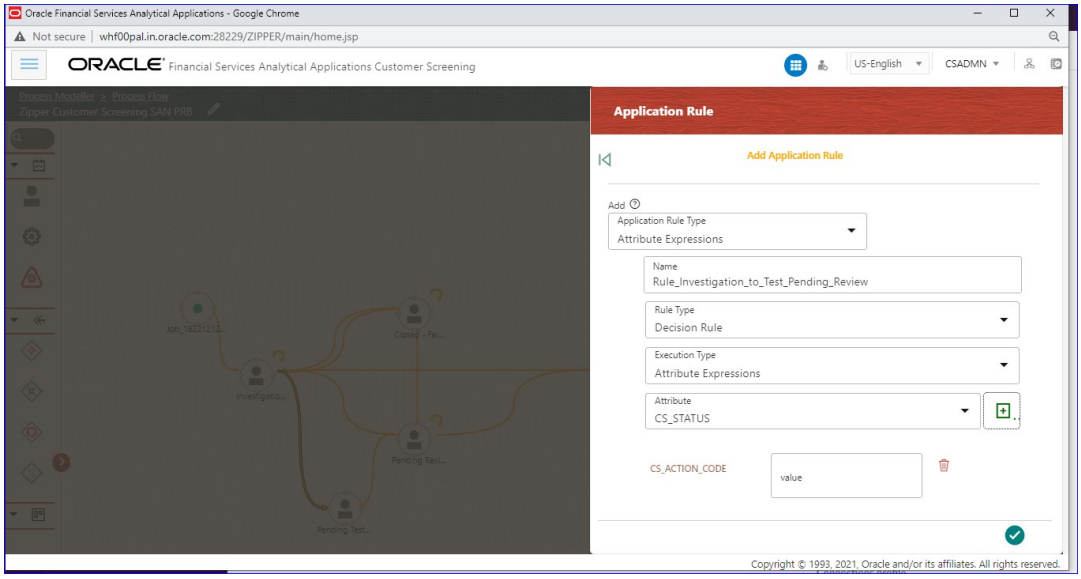


Figure J-11 Rule Details – Decision Rule 1

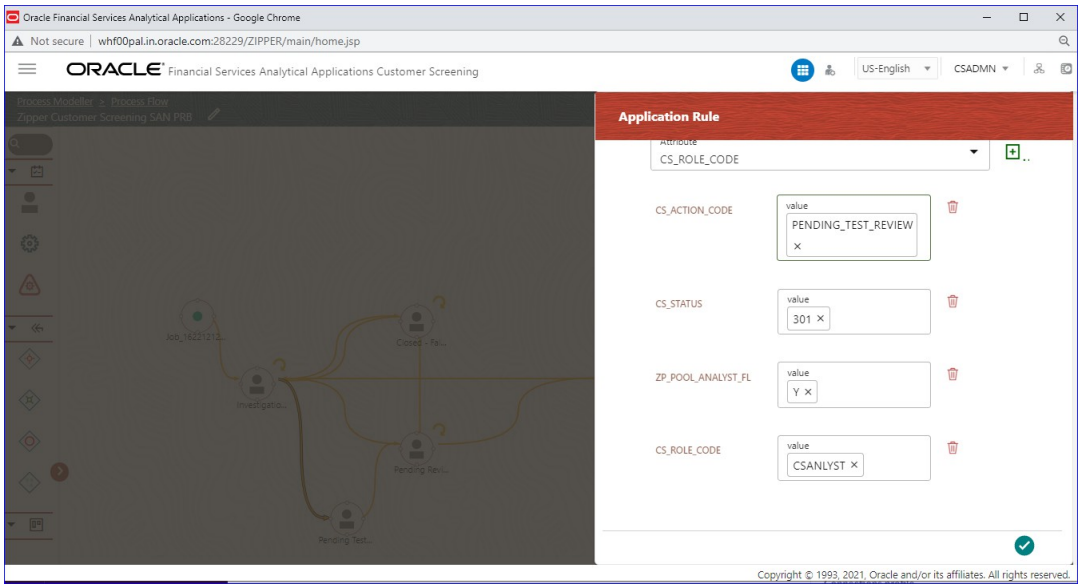


Figure J-12 Rule Details – Decision Rule 2

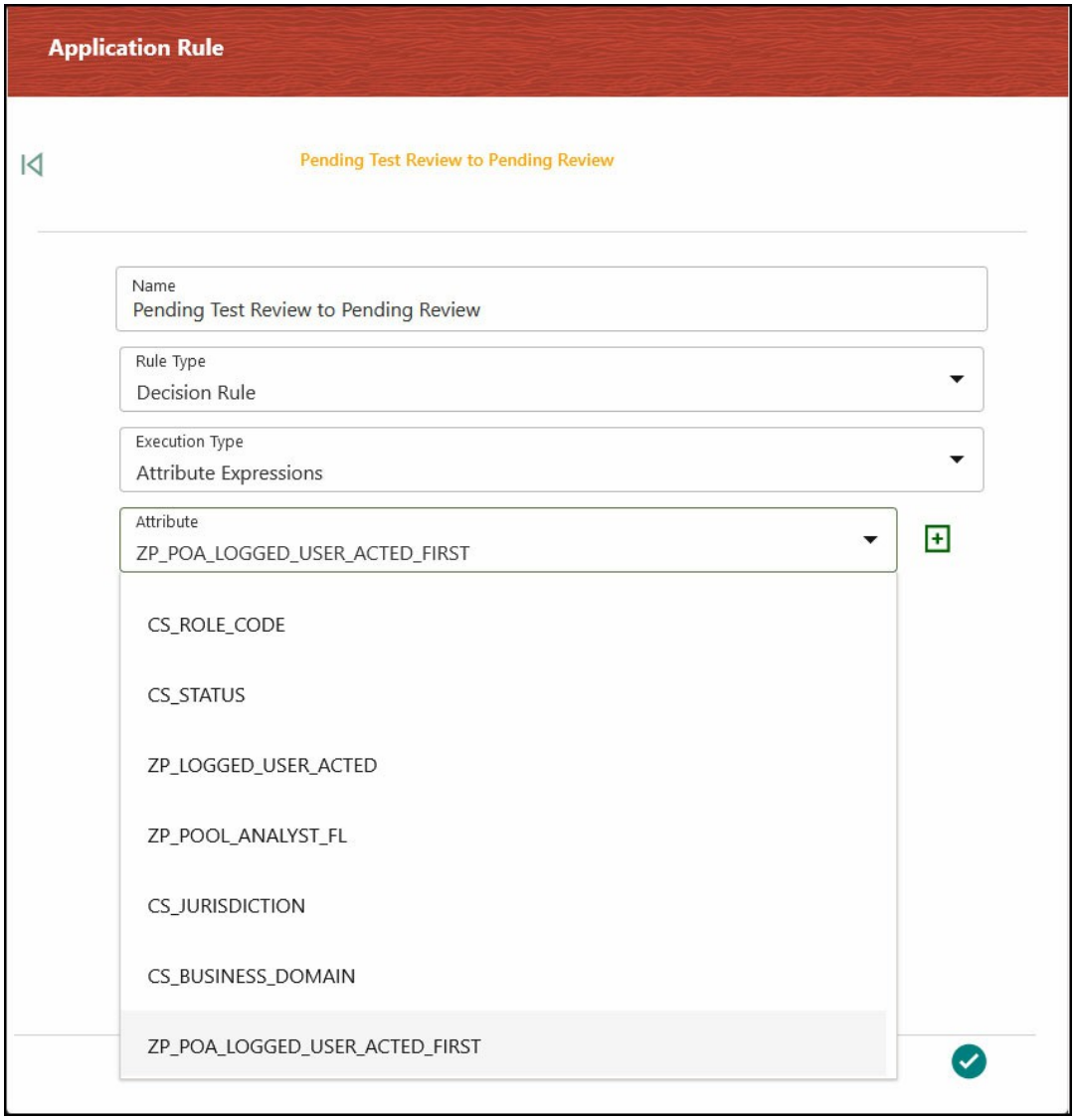
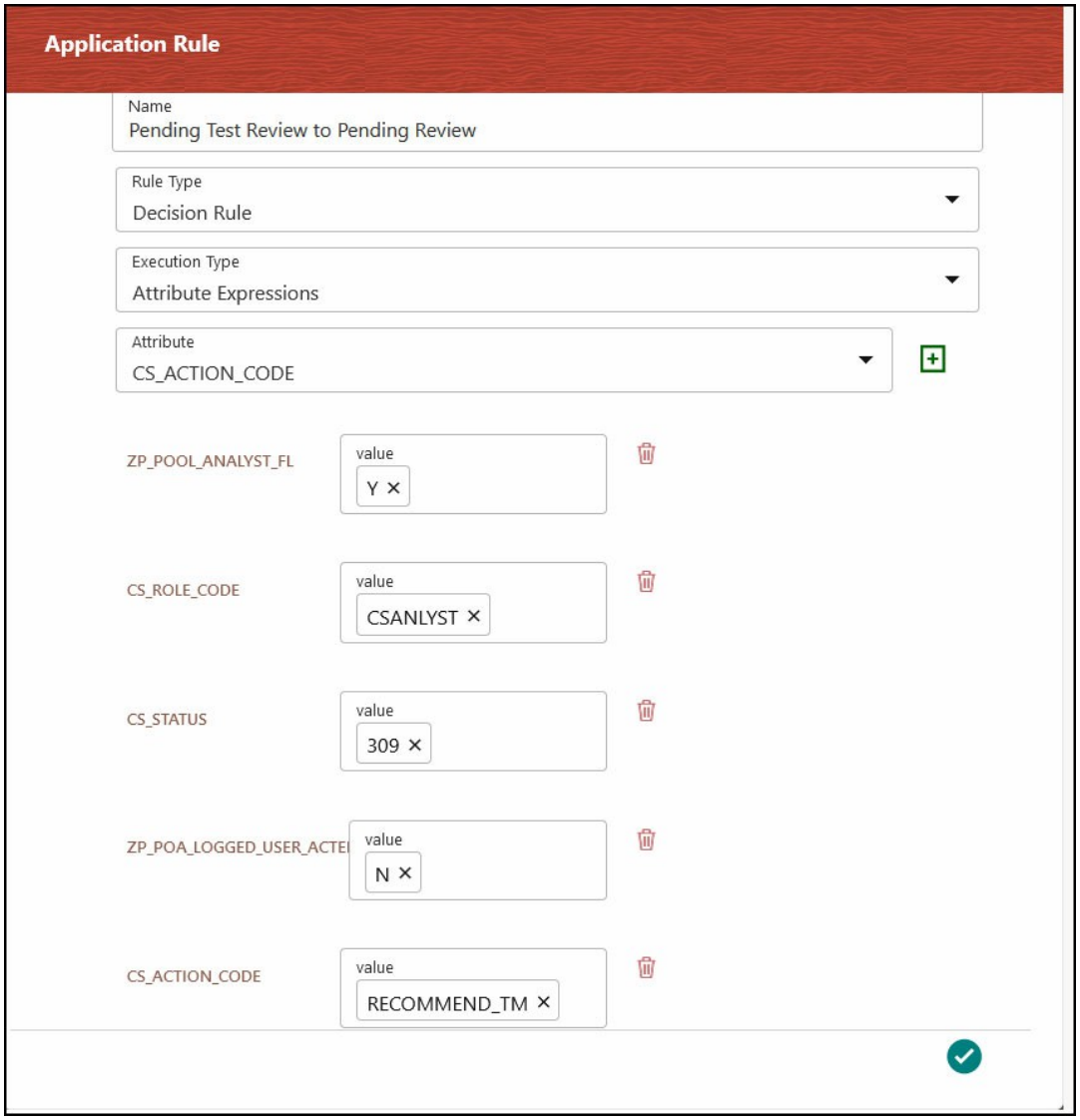


Figure J-13 Rule Details – Decision Rule 2



Edit the existing decision rule, by adding the ZP_POOL_ANALYST_FL.

J.1 List of Attributes Passed to Workflow

Table J-1 Attributes Passed to Workflow

Attributes	Description
CS_ROLE_CODE	Logged in User.
CS_STATUS	Status code.
TF_ALERTTYPE	Alert type of the message (1 or 2).
ZP_POOL_ANALYST_FL	Allowed values are Y/N based on the CS_appln_params Configuration.

Table J-1 (Cont.) Attributes Passed to Workflow

Attributes	Description
ZP_POA_LOGGED_USER_ACTE D_FIRST	If the Logged in User is the user who performed the first action on the POA status, then the value of ZP_POA_LOGGED_USER_ACTED_FIR ST is Y else it's N.

J.2 Attribute to Configure the Auto Refresh in Queue Management

Table J-2 Q_AUTO_REFRESH_TIME Attribute

Attributes	Description
Q_AUTO_REFRESH_TIME	Provide the time in milli second for the attribute in CS_APPLN_PARAMS table. By default it's 25000 i.e 25 seconds but the value is editable.

K

Invoking the PMF Workflow from backend

This appendix describes invoking the Process Modeller Framework (PMF) workflow from the backend for the alert.

Table K-1 PMF Workflow Invoking Parameters

Parameter Name	Parameter Description
Object ID	This represents the unique object ID. For Sanctions, the object ID can be alert ID or Good Guy Whitelist ID.
Object Type	This represents the object type for the object ID. For Sanctions, the object type will be **301** for alert and **302** for Good Guy Whitelist.
Infodom	This represents the name of the infodom in which Sanctions are installed.
Segment	This represents the name of the segment. For Sanctions, it will be **TFLSEGMENT**.
User ID	This represents the User ID that is triggering the workflow. Pass the value as **SYSTEM**.
Locale	This represents the locale. Pass the value as **en_US**.
Application Params	This represents the list of workflow data fields with their respective value.
Security Params	This represents the list of workflow security data fields with their respective value.

To trigger the workflow for Sanctions Alerts, follow the below code snippet.

```
DECLARE

  lv_infodom  varchar2(4000);
  lv_segment  varchar2(4000);
  TYPE alert_record_ids IS TABLE OF fsi_rt_alerts.n_grp_msg_id%TYPE;
  l_alert_record_ids alert_record_ids;
  appParams            array_varchar := array_varchar();
  secMap               array_varchar := array_varchar();
BEGIN

  appParams.extend();
  appParams(1) := 'TF_ACTION=MANUAL_CLOSE';
  appParams.extend();
  appParams(2) := 'Role=SYSTEM';
  select t.v_attribute_value1
    into lv_infodom
    from setup_rt_params t
   where t.v_param_name = 'TFLT_INFODOM';
  select t.v_attribute_value1
```

```
    into lv_segment
    from setup_rt_params t
   where t.v_param_name = 'TFLT_SEGMENT';
  select t.n_grp_msg_id bulk collect
    into l_alert_record_ids
    from fsi_rt_alerts t
   where t.n_status_cd in (1,2);
  FOR recId IN 1 .. l_alert_record_ids.COUNT loop
    startWorkflowForExpireRecord(l_alert_record_ids(recId),
                                 '301',
                                 lv_infodom,
                                 lv_segment,
                                 'SYSTEM',
                                 'en_US',
                                 appParams,
                                 secMap);
  end loop;

EXCEPTION
  WHEN OTHERS THEN
    dbms_output.put_line(SQLCODE || SQLERRM);
    ROLLBACK;
END;
```

L

Mapping the PMF Workflow for Different Jurisdiction and domain

The AAI_WF_APP_DEFINITION_MAP table in Config Schema stores the mapping of object type data to the rocess Modeller Framework (PMF) workflow that is to be used.

The AAI_WF_APP_DEFINITION_MAP table also captures the values for crucial business decisions such as jurisdiction and business domain.

To map a particular workflow to an object type for a combination of jurisdiction and business domain follow these steps:

1. Insert V_KBD_1 and V_KBD_2 columns values into the AAI_WF_APP_DEFINITION_MAP table.

   > **Note**
   >
   > V_KBD_1 represents Jurisdiction code and V_KBD_2 represents Business Domain code.

2. Restart the web server after inserting the values into AAI_WF_APP_DEFINITION_MAP table.

M

User Group Customization

When a new user group for Customer Screening is created from Oracle Financial Services Analytical Applications (OFSAA) user Interface (UI), you must insert an entry in the `CSSMS_GROUP_MAST_PACK` table manually with the product id `OFS_CS`.

N

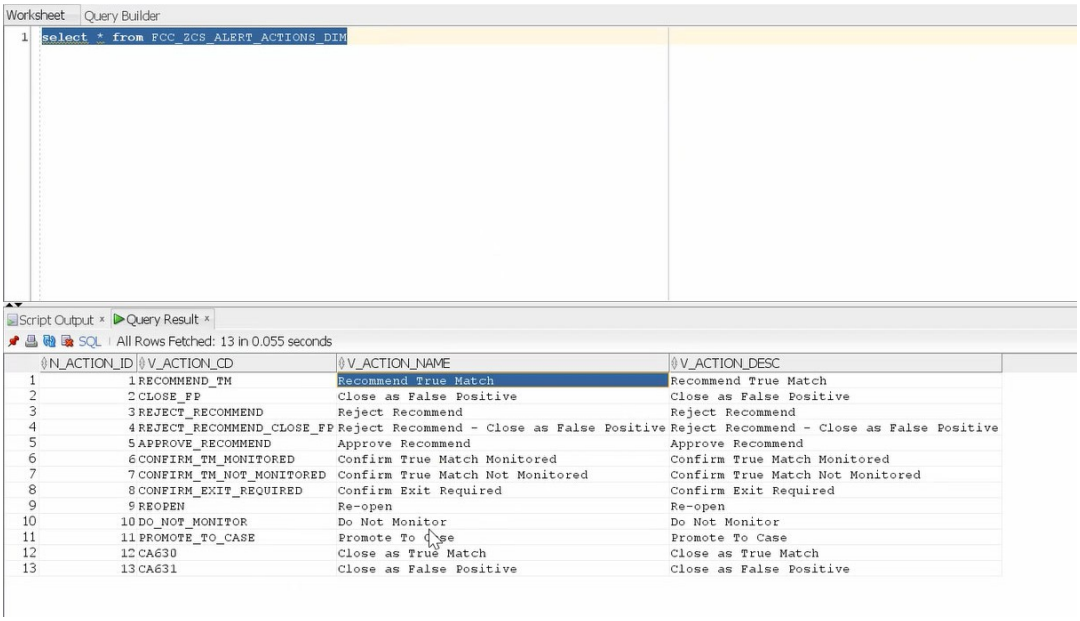
Adding New Alert Level Action and Standard Comments

To Add new Alert level action in the alert decision follow the subsequent steps:

1. Access the atomic schema in database.
2. Add new entries in the following tables:
   - `fcc_zcs_alert_actions_dim`
   - `fcc_zcs_alert_actions_tl`

   For example, to add a new alert decision, provide an entry in the `fcc_zcs_alert_actions_dim` and `fcc_zcs_alert_actions_tl` with action code, name and description.

Figure N-1 fcc_zcs_alert_actions_dim Table



	N_ACTION_ID	V_ACTION_CD	V_ACTION_NAME	V_ACTION_DESC
1	1	RECOMMEND_TM	Recommend True Match	Recommend True Match
2	2	CLOSE_FP	Close as False Positive	Close as False Positive
3	3	REJECT_RECOMMEND	Reject Recommend	Reject Recommend
4	4	REJECT_RECOMMEND_CLOSE_FP	Reject Recommend - Close as False Positive	Reject Recommend - Close as False Positive
5	5	APPROVE_RECOMMEND	Approve Recommend	Approve Recommend
6	6	CONFIRM_TM_MONITORED	Confirm True Match Monitored	Confirm True Match Monitored
7	7	CONFIRM_TM_NOT_MONITORED	Confirm True Match Not Monitored	Confirm True Match Not Monitored
8	8	CONFIRM_EXIT_REQUIRED	Confirm Exit Required	Confirm Exit Required
9	9	REOPEN	Re-open	Re-open
10	10	DO_NOT_MONITOR	Do Not Monitor	Do Not Monitor
11	11	PROMOTE_TO_CASE	Promote To Case	Promote To Case
12	12	CA630	Close as True Match	Close as True Match
13	13	CA631	Close as False Positive	Close as False Positive

3. If you require any validation for the newly added alert level action before taking action, provide an entry in the following tables:
   - `FCC_ZCS_ALERT_ACTIONS_MSG_DIM`
   - `FCC_ZCS_ALERT_ACTIONS_MSG_TL`

To add new standard comments for the alert action, follow the subsequent steps:

1. Access the atomic schema in database.
2. Add new entries in the following table:
   - For simply adding new standard comments in the application:

  - fcc_san_std_cmnts_dim
  - fcc_san_std_cmnts_tl
- For mapping a newly added standard comment to event/alert in the application:
  - fcc_san_std_cmnts_entity_map
- For mapping a newly added standard comment to an existing action in the application:
  - fcc_san_scmnts_entity_actn_map

O

CS and ECM Table Mapping for Alert Status Customization

When L2 Investigation is enabled and if there is any customization of the alert workflow (status, action, or standard comments) done to the Customer Screening (CS) dimension tables listed in the following table, then update the same data in the corresponding ECM dimension table. As a result Alert summary for the escalated case will be visible in Enterprise Case Management (ECM) application.

Table O-1 CS and ECM Dimension Tables

CS Dimension Tables	ECM Dimension Tables
FCC_ZCS_STATUS_DIM	FCC_CS_CM_STATUS_DIM
FCC_ZCS_STATUS_TL	FCC_CS_CM_STATUS_TL
FCC_ZCS_ALERT_PRIORITY_DIM	FCC_CS_CM_ALERT_PRIORITY_DIM
FCC_ZCS_ALERT_PRIORITY_TL	FCC_CS_CM_ALERT_PRIORITY_TL
FCC_ZCS_SCREENING_MODE_DIM	FCC_CS_CM_SCREENING_MODE_DIM
FCC_ZCS_SCREENING_MODE_TL	FCC_CS_CM_SCREENING_MODE_TL
FCC_ZCS_ALERT_TYPE_DIM	FCC_CS_CM_ALERT_TYPE_DIM
FCC_ZCS_ALERT_TYPE_TL	FCC_CS_CM_ALERT_TYPE_TL
FCC_SAN_ALERT_STD_CMNTS_MAP	FCC_CS_ESC_AL_STDCMNTS
FCC_SAN_STD_CMNTS_DIM	FCC_CS_CM_SAN_STD_CMNTS_DIM
FCC_SAN_STD_CMNTS_TL	FCC_CS_CM_SAN_STD_CMNTS_TL
FCC_ZCS_ALERT_ACTIONS_DIM	FCC_CS_CM_ALERT_ACTIONS_DIM
FCC_ZCS_ALERT_ACTIONS_TL	FCC_CS_CM_ALERT_ACTIONS_TL
FCC_ZCS_EVENT_STATUS_DIM	FCC_CS_CM_EVENT_STATUS_DIM
FCC_ZCS_EVENT_STATUS_TL	FCC_CS_CM_EVENT_STATUS_TL
FCC_SAN_EVENTS_STD_CMNTS_MAP	FCC_CS_ESC_EVNT_STDCMNTS
FCC_ZCS_MATCH_RULE_DIM	FCC_CS_CM_MATCH_RULE_DIM
FCC_ZCS_MTCH_RULE_ENT_ATTR_MAP	FCC_CS_CM_MTCH_RULE_ENT_ATRMAP
FCC_ZCS_ENTITY_ATTR_DIM	FCC_CS_CM_ENTITY_ATTR_DIM
FCC_ZCS_MTCH_RULE_WLS_ATTR_MAP	FCC_CS_CM_MTCH_RULE_WLS_ATRMAP
FCC_SAN_SCMNTS_ENTITY_ACTN_MAP	FCC_CSCM_SCMNTS_ENT_ACTN_MAP
FCC_SAN_STD_CMNTS_ENTITY_MAP	FCC_CSCM_STD_CMNTS_ENT_MAP

P

Configurations Required to Open ECM Case or CSAM Alert from RT Screening if RT Screening and ECM/CSAM are in Different Servers

Perform the following configuration to open Enterprise Case Management (ECM) Case or Customer Screening Alert Management (CSAM) Alert from Real-time (RT) Screening if RT Screening and ECM/CSAM are in Different Servers.

Configure REFERRER-POLICY-ENABLED

The valid `V_PROP_VALUE` values are TRUE or FALSE. The default is FALSE. Configure this value to TRUE to allow Referrer URLs.

```
MERGE INTO aai_setup_props ut
USING (
SELECT 'REFERRER-POLICY-ENABLED' AS V_PROP_NAME FROM dual
) md ON (ut.V_PROP_NAME = md.V_PROP_NAME)
WHEN NOT MATCHED THEN
INSERT (V_PROP_NAME,V_PROP_VALUE,V_PROP_TIER,V_SEEDED_BY)
VALUES ('REFERRER-POLICY-ENABLED','FALSE','WEB','AAI')
/
```

Configure ALLOWED-REFERRER-URLS

By default `V_PROP_VALUE` is set to NONE.

Configure this value to set the HOST URL (Real time CS URL) as the allowed URL in the following format:

`http://<HOST_NAME>:<PORT_NUMBER>/`

Separate the URLs with a single space. Adding the URLs without a space between them or adding two or more spaces between them results in errors.

Run the following query after replacing the <Referral-URLs> with the suitable values.

```
MERGE INTO aai_setup_props ut
USING (
SELECT 'ALLOWED-REFERRER-URLS' AS V_PROP_NAME FROM dual
) md ON (ut.V_PROP_NAME = md.V_PROP_NAME)
WHEN NOT MATCHED THEN
INSERT (V_PROP_NAME,V_PROP_VALUE,V_PROP_TIER,V_SEEDED_BY)
VALUES ('ALLOWED-REFERRER-URLS','<Referral-URLs>','WEB','AAI')
/
```

Q
Function Codes for User Groups

All actions or functions in the Customer Screening (CS) application is configured with a function code. You can define the functionalities for the particular user group by assigning the required functional code to the user group. If a function code is mapped to the user group, the functionality corresponding to the functional code is enabled in the UI.

Table Q-1 Function Codes for User Groups

Function Codes	Function Description	CSANYST	CSSUPRV	CSSNRSUPER	CSREADONLY	CSRT
CSQALLALRT	Access to View All Alerts in List Page through Queue	-	-	✓	✓	-
CSACSALLQ	Access to open any queue in Queue dashboard	-	-	✓	✓	-
CSQGET-NEXT	Access to get the next queue alerts in details page	-	-	✓	✓	-
CSQGNXTALL	Access to view all alerts from get next in queue	-	-	✓	✓	-
CSALRTASGN	Access to assign alerts when the user opens alert	✓	✓	✓	-	-
CSALRTATTH	Access to select and save attachments for an alert in List Page	✓	✓	✓	-	-
CSBLKACNT	This function gives access to Bulk Update in List Page	-	-	✓	-	-
CSADATTH	Access to select and save attachments for an alert in Details Page	✓	✓	✓	-	-

Table Q-1 (Cont.) Function Codes for User Groups

Function Codes	Function Description	CSANYST	CSSUPRV	CSSNRSUPER	CSREADONLY	CSRT
CSEVNTDEC	Access to take event level action in alert Details Page	✓	✓	✓	-	-
CSEVNTCOM	Access to add or update event level comments in alert Details Page	✓	✓	✓	-	-
CSSCN	This function gives access to Scan Button in Real Time Screening Page	✓	-	-	-	✓
CSSCNINVST	This function gives access to Scan & Investigate Button in Real Time Screening Page	✓	-	-	-	✓
CSBLKTK-ACN	Bulk Action Function Code	✓	✓	-	-	-
CSRTUP-LOAD	File Upload Function Code	✓	-	-	-	-
CSALRTSTS	Function Code to Access Alert List API for Cust Id	-	-	-	-	-

Note

If you configure any of the following function codes to a user group, you must also configure the CSALRTASGN function code to the user group as a mandatory function code:

- CSADATTH
- CSEVNTDEC
- CSEVNTCOM

R

Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMIT in Python Interpreter

An interpreter is a program that directly executes instructions written in a programming or scripting language without requiring them previously to be compiled into a machine language program. Interpreters are plug-ins that enable users to use a specific language to process data in the backend. In Compliance Studio, Interpreters are used in Notebooks to execute code in different languages. Each The interpreter has a set of adjusted and applied properties across all notebooks. For more information on Interpreter Configuration and Connectivity, see OFS Compliance Studio Administration and Configuration Guide.

Using the **zeppelin.interpreter.output.limit** field you can enter the output message limit. Any message that exceeds the limit is truncated.

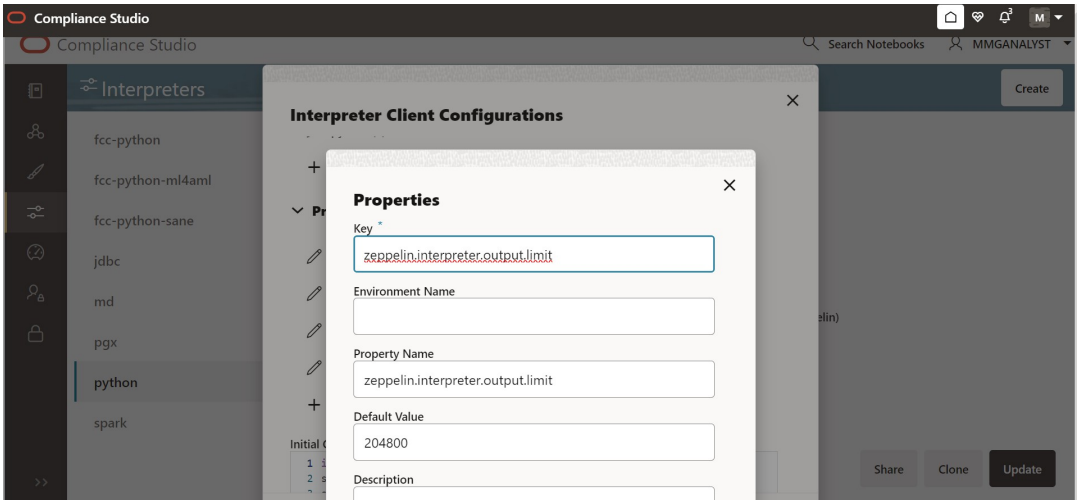
R.1 Configuring through the UI

Follow the subsequent steps to configure the **zeppelin.interpreter.output.limit** through the UI:

Using the Wizard Screen:

1. Click the **User** Icon right top corner.
2. Go to **Data Studio Options**.
3. Click **Interpreters**. The Interpreters page is displayed.
4. select the python interpreter for which you want to configure the **zeppelin.interpreter.output.limit**.
5. Select python from the LHS options.
6. Click the Wizard  Icon.
7. From the RHS side, click **oracle.datastudio.python.DsPythonInterpreter** under Interpreter Client Configurations. The Interpreter Client Configuration pop-up is displayed.
8. Under Properties, click +Properties. The Properties pop-up is displayed.
9. Fill the options as shown in following figure. Set the default value to 870400 (for 1000 records approx.).

Figure R-1 spring-postSacalert.properties file



> **Note**
>
> - Configuration using the Wizard screen is preferable to other ways of configuration.
> - If the data is more than 1000 records, update the **zeppelin.python.maxResult** in properties to the desired value and **zeppelin.interpreter.output.limit** as 870.4 x maxResult.
> - If you cannot see the **Create** and **Cancel** buttons, click on the header label of the Properties window.
> - The default value for zeppelin.interpreter.output.limit i is 102400 (in bytes)
> - Increasing the default value from 102400 bytes to an immense value will slow down the rendering of outputs of python paragraphs.

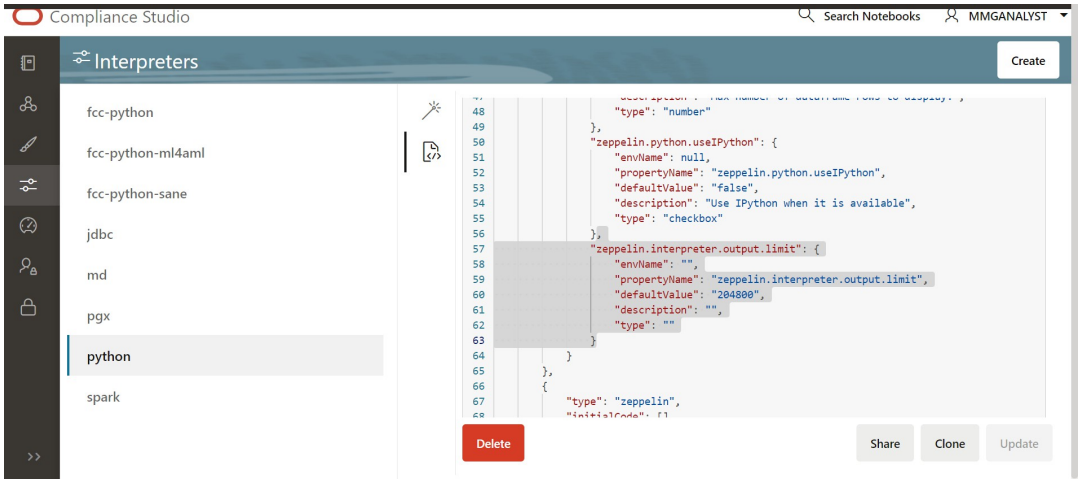
10. Click **Create**. The Interpreter Client Configuration pop-up is displayed and **zeppelin.interpreter.output.limit** is displayed under **Properties**.
11. Click **Confirm**. The Interpreter Client Configuration window is displayed.
12. Click **Update**.
13. Restart the Compliance Studio application to reflect the changes.

Configuration through JSON Screen:

1. Click the **User** Icon right top corner.
2. Go to **Data Studio Options**.
3. Click **Interpreters**. The Interpreters page is displayed.
4. select the python interpreter for which you want to configure the **zeppelin.interpreter.output.limit**.
5. Select python from the LHS options.
6. Click the Icon. The JSON configuration screen is displayed.

7. Scroll down and locate interpreterClientConfigs with className **oracle.datastudio.python.DsPythonInterpreter**. you can find the properties section with zeppelin configurations.
8. Add the **zeppelin.interpreter.output.limit.** See the following figure.

Figure R-2 JSON Screen



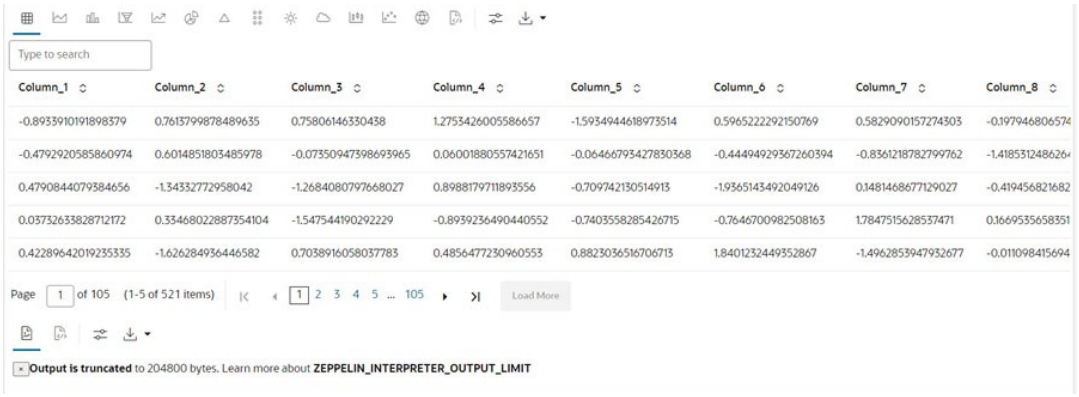
9. The update button will be enabled in the bottom right corner after the JSON modification. Click **Update**.
10. Restart the Compliance Studio application to reflect the changes.

R.2 Configuring through the Filesystem

Follow the subsequent steps to configure the zeppelin.interpreter.output.limit through the filesystem:

1. Go to the python interpreter option as pointed out in section 27.1. You can see the python interpreter listed there if you have run the MMG services before. Delete it, if you run the MMG Application for the first time on a fresh schema, then you don't need to do this step.
2. After deleting the python interpreter or if the start has not been done, go to the filesystem inside mmg-home/mmg-studio/server/builtin/interpreters, and open `python.json` in a text editor.
3. Scroll down under **interpreterClientConfigs** with className ,r**acle.datastudio.python.DsPythonInterpreter**, you will find the following properties section with Zeppelin configurations. After the last entry in properties, add the zeppelin.interpreter.output.limit using the JSON screen. See the *JSON* screen figure.
4. Save the python.json with the desired default value.
5. Restart the Compliance Studio application to reflect the changes.

Figure R-3 Output in table view



You can see the ZEPPELIN_INTERPRETER_OUTPUT_LIMIT value as a warning if the table content is more than the set default value for zeppelin.interpreter.output.limit, and accordingly, you can modify the default value for the same.

S

API to Check the Status of EDQ Job

You can check the status of the EDQ job by sending a real-time request in GET method. To execute the request, follow the subsequent steps:

1. Open Postman or a relevant tool.
2. Go to the Header tab.
3. Send a request using the GET method. The request must be in the following format:

```
http://<App_Host>:<App_Port>/EdqCheck/CheckEdqRestService/
checkEDQ?edqUrl=http://
<Edq_Host>:<Edq_Port>&projectName=<Edq_project_name>
```

Enter the following mandatory parameters in the Query Params table:

Table S-1 Query Params for Individual Screening

Key	Value
edqUrl	EdqUrl, which you want to check its health/status
projectName	**Customer-Screening**

Enter the following optional parameters in the Query Params table:

Table S-2 Query Params for Individual Screening

Key	Value
extraServiceName	<WEBSERVICE URL>
timeoutSeconds	<PlaceHolder Value>

> **Note**
>
> The Key and Value fields are case sensitive.

You will get the following sample response for a successful execution:

```
{
    "payload": [
        {
            "serviceUrl": "http://100.76.157.111:8001/edq/restws/Customer-
Screening:IndividualScreen",
            "serviceName": "IndividualScreen",
            "responseCode": 200,
            "status": "SUCCESS"
        },
        {
```

```
            "serviceUrl": "http://100.76.157.111:8001/edq/restws/Customer-
Screening:EntityScreen",
            "serviceName": "EntityScreen",
            "responseCode": 200,
            "status": "SUCCESS"
        },
        {
            "serviceUrl": "http://100.76.157.111:8001/edq/restws/Customer-
Screening:abv",
            "serviceName": "abv",
            "responseCode": 404,
            "status": "FAILED"
        }
    ],
    "message": "One of the EDQ webservices is not up and running.",
    "status": "FAILED"
}
```

T

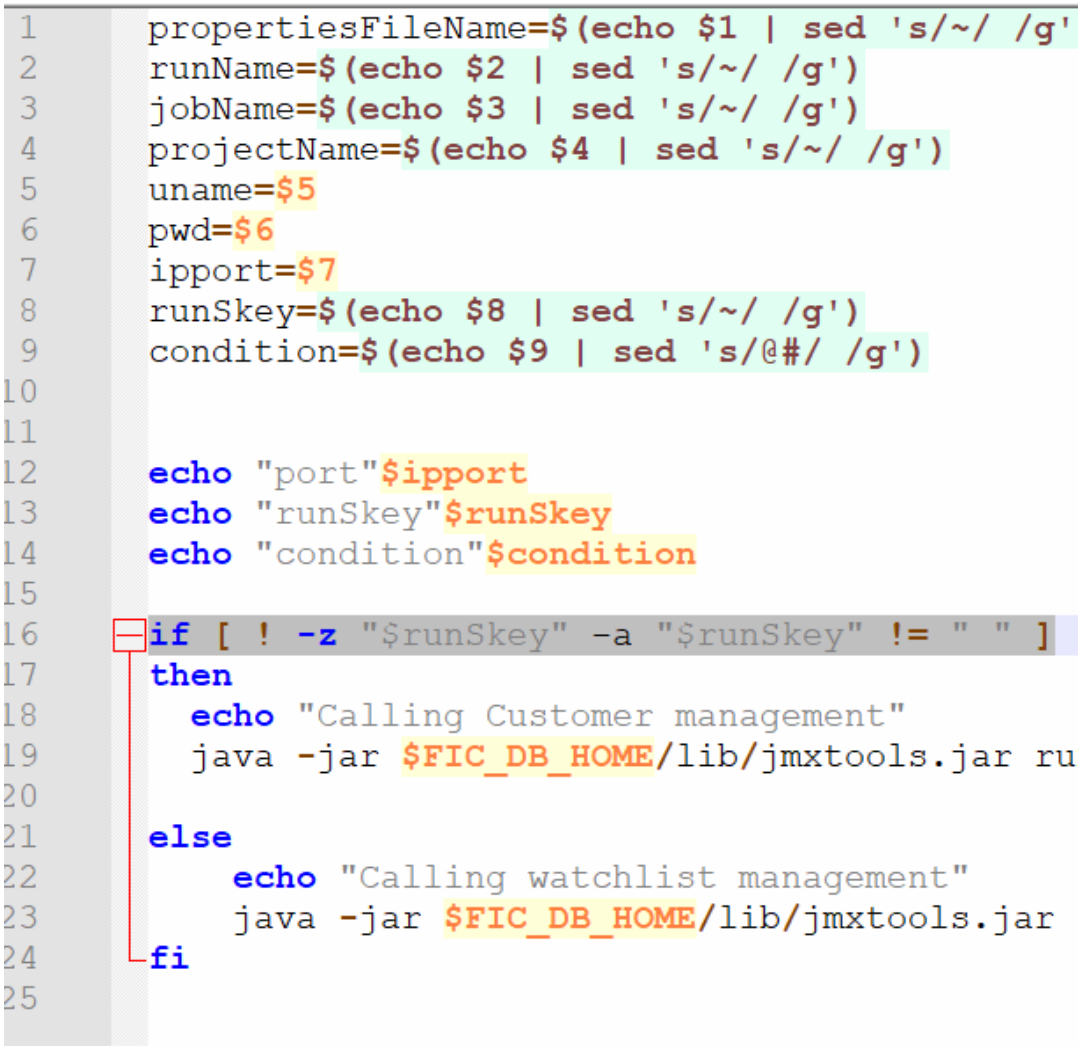
CS Matching Batch Issue with EDQ Execution

You need to remove the Java Virtual Machine environment variable from your system, if the edq task is success and still the CS Matching batch is failed.

To remove the Java Virtual Machine environment variables, follow the subsequent steps:

1. Navigate to the `##FIC_HOME##/ficdb/bin` folder, and open the `EDQExecute.sh` file.

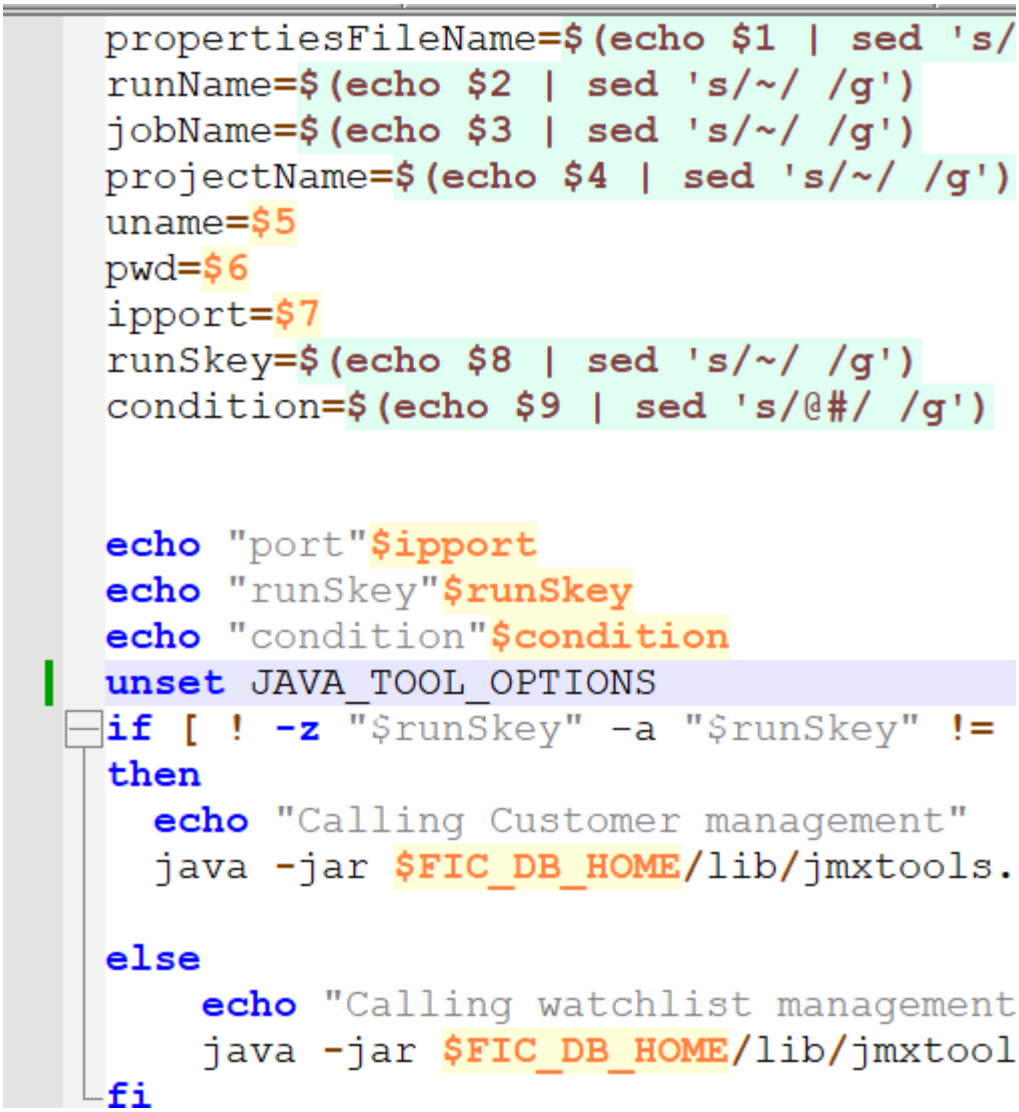
Figure T-1 EDQExcute.sh file



```
propertiesFileName=$(echo $1 | sed 's/~/ /g'
runName=$(echo $2 | sed 's/~/ /g')
jobName=$(echo $3 | sed 's/~/ /g')
projectName=$(echo $4 | sed 's/~/ /g')
uname=$5
pwd=$6
ipport=$7
runSkey=$(echo $8 | sed 's/~/ /g')
condition=$(echo $9 | sed 's/@#/ /g')


echo "port"$ipport
echo "runSkey"$runSkey
echo "condition"$condition

if [ ! -z "$runSkey" -a "$runSkey" != " " ]
then
  echo "Calling Customer management"
  java -jar $FIC_DB_HOME/lib/jmxtools.jar ru

else
    echo "Calling watchlist management"
    java -jar $FIC_DB_HOME/lib/jmxtools.jar
fi
```

2. Add the `unset JAVA_TOOL_OPTIONS` command before `if` condition.

Figure T-2 Updated EDQExcute.sh file



```
propertiesFileName=$(echo $1 | sed 's/
runName=$(echo $2 | sed 's/~/ /g')
jobName=$(echo $3 | sed 's/~/ /g')
projectName=$(echo $4 | sed 's/~/ /g')
uname=$5
pwd=$6
ipport=$7
runSkey=$(echo $8 | sed 's/~/ /g')
condition=$(echo $9 | sed 's/@#/ /g')


echo "port"$ipport
echo "runSkey"$runSkey
echo "condition"$condition
unset JAVA_TOOL_OPTIONS
if [ ! -z "$runSkey" -a "$runSkey" !=
then
  echo "Calling Customer management"
  java -jar $FIC_DB_HOME/lib/jmxtools.

else
    echo "Calling watchlist management
    java -jar $FIC_DB_HOME/lib/jmxtool
fi
```

3. Save the `EDQExecute.sh` file.
4. Re-execute the CS Matching batch.
   The CS Matching Batch runs successfully.

Glossary

Index