OFS Transaction Filtering

Administration Guide

Release 8.0.7.0.0

August 2020

E91799-01

ORACLE
Financial Services

ORACLE®

OFS Transaction Filtering Administration Guide

Copyright © 2021 Oracle and/or its affiliates. All rights reserved.

For information on third party licenses, see here.

Document Control

Table 1: Document Control

Version Number	Revision Date	Change Log
8.0.7.1.2	November 2020	• Added the notification for overdue alerts. • Added the configurations needed to ensure that the US NACHA batch runs successfully. • Added new message types for US NACHA in the *Message Categories and Message Types* appendix.
8.0.7.0.36	October 2020	• Added two new fields, *Jurisdiction and Business Domain*, in the *<Message Type> Screening Configuration Window* section in the *Configuring the SWIFT Message Parameters* chapter. •
8.0.7.0.29	June 2020	Added a section for running the SWIFT migration utility in the *General Configurations* chapter.
8.0.7.0.28	May 2020	Added the message types for US NACHA (message types 1 and 2 in the table) in the *Message Categories and Message Types* appendix.
8.0.7.0.27	April 2020	• Added the message types for Fedwire (message types 1 and 2 in the table) in the *Message Categories and Message Types* appendix. • Added a section for configuring Fedwire message parameters in the *Configuring the Fedwire Message Parameters* chapter.
8.0.7.0.23	March 2020	• Added the message types for SWIFT (message types 9 to 79 in the table) in *Appendix F: Message Categories and Message Types*. • Added values to be updated for the `V_ATTRIBUTE_VALUE1` value in the *Configuring the Host Port and Context Name* section in the *General Configurations* chapter.

Version Number	Revision Date	Change Log
8.0.7.0.22	February 2020	• Added the message types for ISO20022 (message types 1 and 2 in the table) in *Appendix F: Message Categories and Message Types*. • Added a chapter for configuring ISO20022 message parameters. • Updated steps for running the SWIFT migration utility in the *General Configurations* chapter. • Updated the *Introduction* section in the *About Oracle Financial Services Transaction Filtering* chapter. • Added information on the `transaction-screening.properties` and `transaction-screening-batch.properties` files in the *Transaction Screening Setup* section in the *Enterprise Data Quality (EDQ)* chapter.
8.0.7.0.20	January 2020	• Added a section, *Version Control*, in the *General Configurations* chapter. • Added a section on how to assign a message automatically to a user in the *General Configurations* chapter. • Added a section for setting the message cut-off time in the *General Configurations* chapter. • Added a section for setting the priority for a message category in the *General Configurations* chapter.
8.0.7.0.17	January 2020	Audit tables were added.
8.0.7.0.15	December 2019	Updated steps for running the purge utility in the *General Configurations* chapter.
8.0.7.0.14	November 2019	• Updated the text in the *Creating a JSON for the 3xx, 5xx, and 6xx Message Types* section in the *Creating a JSON* chapter. • Added information for the UTF-8 message formats in the *Configuring the SWIFT Message Parameters* chapter. • Added a note to explain how to repeat sequences in the *Adding or Updating a New Message Type* section in the *Configuring the SWIFT Message Parameters* chapter. • Updated the description for the Generic Business Data field to include information for the new sequences added in the *Configuring the SWIFT Message Parameters* chapter. • Added information for the Jurisdiction field in the Message and Screening Configurations window in the *Configuring the SWIFT Message Parameters* chapter.

Version Number	Revision Date	Change Log
8.0.7.0.6	May 2019	Added an Appendix, *Time Zone Configuration*, which contains information on the time zone configurations required for each country.
8.0.7.0.5	May 2019	Added an Appendix, *Delta Watch List Configurations*, to provide instructions on how to download the delta watch list data.
8.0.7.0.2	May 2019	Updated the *Process Modeller Framework (PMF) Configurability* appendix.
8.0.7.0.1	February 2019	Updated an Appendix, *Process Modeller Framework (PMF) Configurability*, to provide instructions on how to configure the PMF workflow.
8.0.7.0.0	January 2019	• Added the tables in which reference data is available in the Prohibition Screening section in the *General Configurations* chapter. • Updated the EDQ Configuration Process Flow steps to include the command area paths in the *EDQ Configurations* chapter.

Table of Contents

1   About This Guide

This guide provides comprehensive instructions for system administration and the daily operations and maintenance of Oracle Financial Services Transaction Filtering. The logical architecture provides details of the Transaction Filtering process for a better understanding of the pre-configured application, which allows you to make site-specific enhancements using OFSAAI.

1.1   Who Should Use This Guide

This *Administration Guide* is designed for use by the Implementation Consultants and System Administrators. Their roles and responsibilities, as they operate within Oracle Financial Services Transaction Filtering, include the following:

- **Implementation Consultant**: Installs and configures Oracle Financial Services Transaction Filtering at a specific deployment site. The Implementation Consultant also installs and upgrades any additional Oracle Financial Services solution sets and requires access to deployment-specific configuration information (For example, machine names and port numbers).

- **System Administrator**: Configures, maintains, and adjusts the system, and is usually an employee of a specific Oracle customer. The System Administrator maintains user accounts and roles, configures the EDQ, archives data, loads data feeds, and performs post-processing tasks.

1.2   How This Guide is Organized

The *Oracle Financial Services Transaction Filtering Administration Guide* includes the following chapters:

- About Oracle Financial Services Transaction Filtering provides a brief overview of the Oracle Financial Services Transaction Filtering (OFS TF) application.

- Getting Started explains common elements of the interface, includes instructions on how to configure your system, access Transaction Filtering, and exit the application.

- Managing User Administration provides information on the user administration of the Oracle Financial Services Transaction Filtering application.

- General Configurations describes how to configure the SWIFT (Society for Worldwide Interbank Financial Telecommunication) message and screening parameters, run the migration utility, run the Purge utility, and do Version Control for messages in the Oracle Financial Services Transaction Filtering application.

- Configuring the Fedwire Message Parameters describes how to configure the Fedwire message parameters.

- Configuring the SWIFT Message Parameters describes how to configure the SWIFT message parameters.

- Configurations for the ISO20022 Message Parameters describe how to configure the ISO20022 message parameters and run the ISO20022 batch.

- Configurations for the US NACHA Batch Process describes how to configure the US NACHA batch.

- Enterprise Data Quality (EDQ) Configurations describes how to configure the EDQ parameters.

- Configuring Risk Scoring Rules describes how to configure business rules in the Inline Processing Engine (IPE).

- Creating a JSON describes how to create a JSON (JavaScript Object Notation) for SWIFT messages with sequences and SWIFT messages without sequences.

- Appendix A: Watch Lists mentions the details of each of the pre-configured watch lists that can be used by Oracle Transaction Filtering.

- Appendix B: System Audit Logging Information contains information on the logs related to the Debug and Info log files.

- Appendix C: Process Modeller Framework (PMF) Configurability describes how to configure the Process Monitor Facility (PMF) workflow.

- Appendix D: Time Zone Configuration describes how to set the time zone for a user.

- Appendix E: Delta Watch List Configurations describes how to run and download the delta updates.

- Appendix F: Message Categories and Message Types shows the different message types available for the SWIFT, Fedwire, ISO 20022, and US NACHA message types.

1.3   Where to Find More Information

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

- User Guide

- Installation and Configuration Guide

- Matching Guide

- Reporting Guide

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

1.4   Conventions Used in this Guide

The following table mentions the conventions used in this guide.

Table 2: Conventions Used

Conventions	Meaning
Italics	- Names of books as references - Emphasis - Substitute input values
Bold	- Menu names, field names, options, button names - Commands typed at a prompt - User input

Conventions	Meaning
Monospace	- Directories and subdirectories - File names and extensions - Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text
Hyperlink	Hyperlink type indicates the links to external websites, internal document links to sections.
Asterisk (*)	Mandatory fields in User Interface
<Variable>	Substitute input value

2   About Oracle Financial Services Transaction Filtering

Oracle Financial Services Transaction Filtering is a Sanctions screening system that identifies Individuals, entities, cities, countries, goods, ports, BICs, and Stop keywords that may either be suspicious, restricted, or sanctioned with relation to a financial transaction that is processed through the TF application. The application enables you to integrate with any clearing or payment system, accept messages from the source system, and scans them against different watch lists maintained within the application to identify any suspicious data present within the message. The TF application can scan messages which are in the SWIFT, ISO20022, Fedwire, or NACHA category, or any custom format.

The OFS Transaction Filtering application is built using components of the Oracle Financial Services Analytical Applications (OFSAA) product suite. These components are Oracle Enterprise Data Quality (OEDQ) and Inline Processing Engine (IPE).

Financial Institutions are required to comply with regulations from different authorities. Some of them are as follows:

- USA PATRIOT Act
- U.S. Treasury's Office of Foreign Assets Control (OFAC), USA
- Office of the Superintendent of Financial Institutions (OSFI), Canada
- Financial Action Task Force (on Money Laundering) (FATF/GAFI)
- EU Commission
- Country-specific authorities

While the regulations can differ between countries, the spirit of regulatory intervention is uniform, and that is to hold financial institutions responsible and accountable if they have been a party, intentionally or unintentionally, to a criminal or terrorist-related transaction.

Sanctions include the withholding of diplomatic recognition, the boycotting of athletic and cultural events, and the sequestering of the property of citizens of the sanctioned country. However, the forms of sanctions that attract the most attention and are likely to have the greatest impact are composed of various restrictions on international trade, financial flows, or the movement of people.

Transaction Filtering against government-regulated watch lists and internal watch lists is a key compliance requirement for financial institutions across the globe. At the turn of the century, Financial Institutions (FIs) were expected to identify customers who were either sanctioned or who lived in sanctioned countries and identify any transactions which were associated with these customers. FIs are now expected to also identify any suspicious dealings and parties involved in the transaction, and more recently identify information that is deliberately hidden or removed.

The TF application delivers a strong, effective filter that identifies all sanctioned individuals or entities with true positives and exploits all available information (internal and external) to reduce false positives and therefore minimizes the operational impact on FIs.

2.1 Transaction Filtering Workflow

The following image describes the Transaction Filtering workflow.

Figure 1: Transaction Filtering Workflow
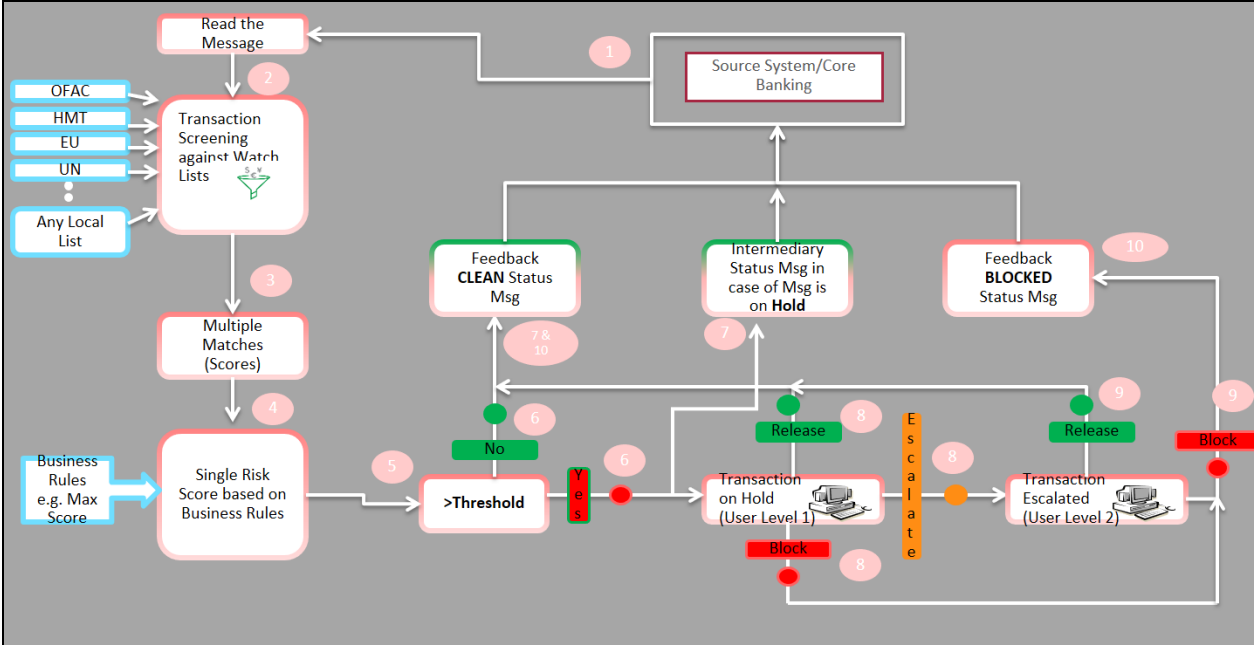
The application first receives a message from the payment system and scans it against the watch lists, then provides a risk score for the message. If no suspicious data is found during screening, then the TF application sends a feedback message with the status CLEAN back to the payment system through the message queue. If suspicious data is found during screening, then the message is sent to an Analyst who investigates it using the TF User Interface. Feedback is sent to the payment system through a message queue, which indicates that the message is on hold. The Analyst reviews the message, which is the first level of review and decides to release, block, or escalate the message. Based on the decision, the system sends a feedback message, either CLEAN or BLOCKED, to the payment system for the reviewed message.

If the four-eyes workflow is enabled, then the Analyst can additionally Recommend to Release, Recommend to Block, or escalate the message to the Supervisor. If the Analyst escalates the message, then the message is sent to the Supervisor, which is the second level of review. The Supervisor can block or release the message and add comments. For a four-eyes workflow, the Supervisor can Release, Block, or Reject the message. You can view the associated matched data of a message from the Match Summary section. You can also view the risk score details from the Risk Summary section. Both these sections are present in the Investigation User Interface.

3   Getting Started

This chapter provides step-by-step instructions to log in to the Transaction Filtering System and different features of the Oracle Financial Services Analytical Applications (OFSAA) Application page.

3.1   Accessing the Oracle Financial Services Analytical Applications (OFSAA) Page

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

> **NOTE**   After the first login, you will be prompted to change your password.

To access the **Oracle Financial Services Analytical Applications** page, follow these steps:
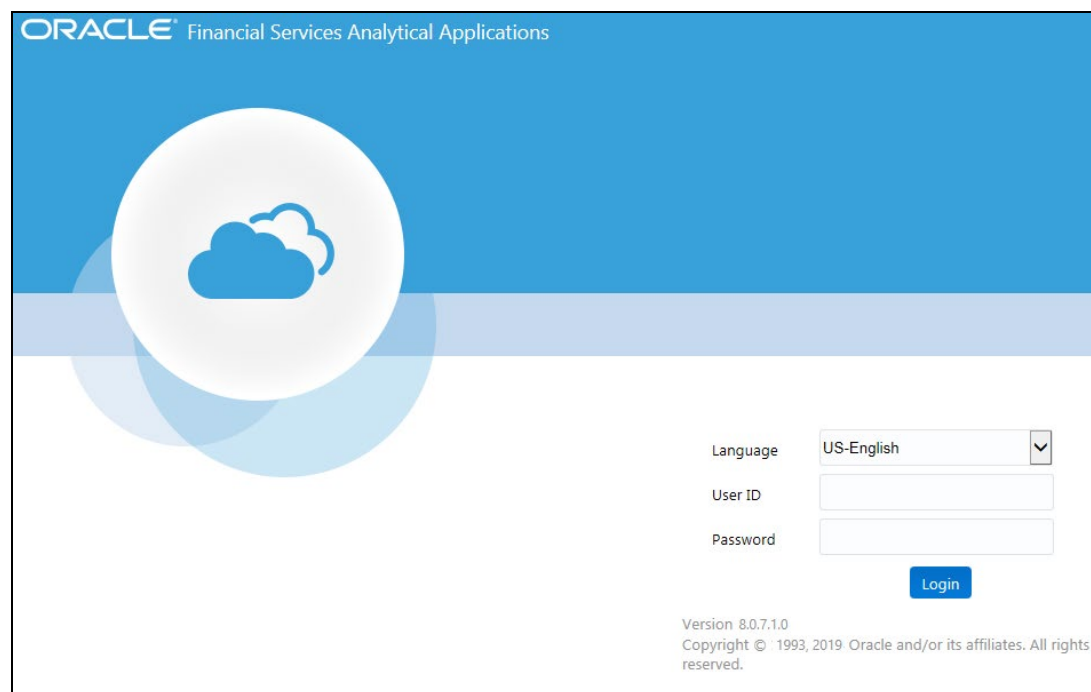
1. Enter the URL into your browser using the following format:

   ```
   <scheme/ protocol>://<ip address/ hostname>:<port>/<context-
   name>/login.jsp
   ```

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

   The **Oracle Financial Services Analytical Applications** login page is displayed.

   Figure 2: Oracle Financial Services Analytical Applications 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 Transactions Filtering** page is displayed.

Figure 3: Financial Services Analytical Applications Transactions Filtering Page
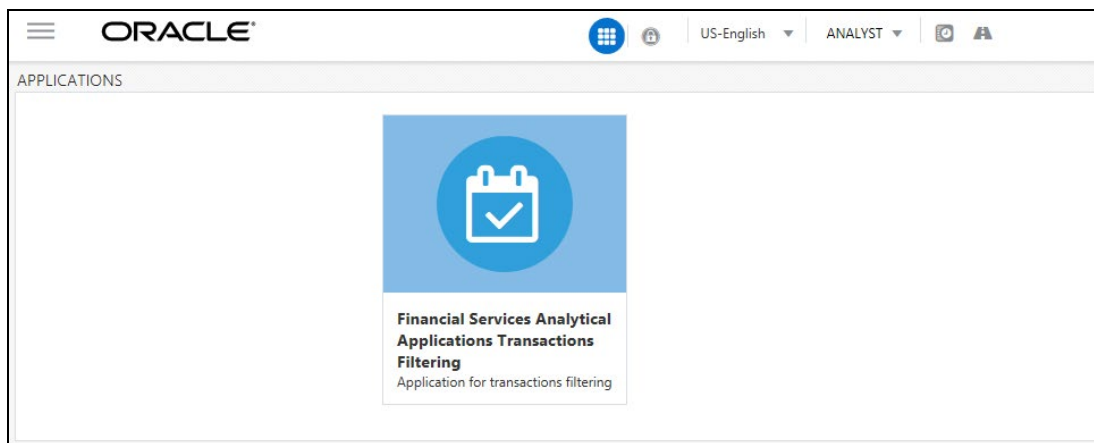
To view the **Financial Services Analytical Applications Transactions Filtering** home page, click **Calendar** .

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

From the **Oracle Financial Services Analytical Applications** page, you can access the menus for the different message configurations. You can change the default transaction currency from USD to another currency in the **Process Modeller** page and view the **Good Guy Summary** page, which has details related to the records added in the good guy list.

3.2.1 Transaction Filtering Admin Menu

The **Transaction Filtering Admin** menu allows the system administrator to configure the application-level parameters, good guy matching parameters, the cut-off time for messages, and assignment type for a message (manual or automatic). For more information, see General Configurations.

To view the menu, follow these steps:

1. Click **Financial Services Sanctions Pack**.

Figure 4: Financial Services Sanctions Pack Menu
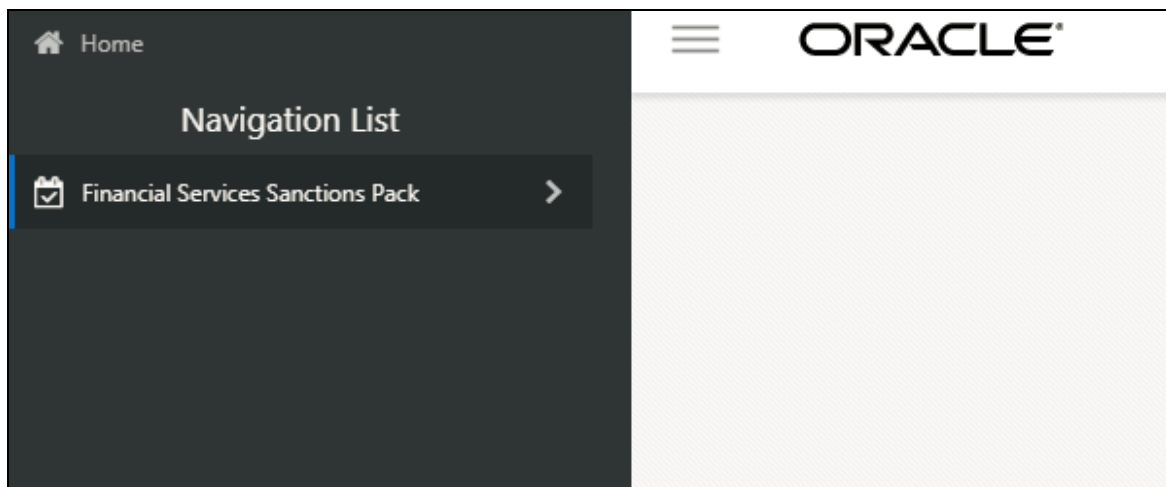
2. Click **Transaction Filtering Admin**. The *Configuration Screen* displays.

Figure 5: Transaction Filtering Admin Sub-menu
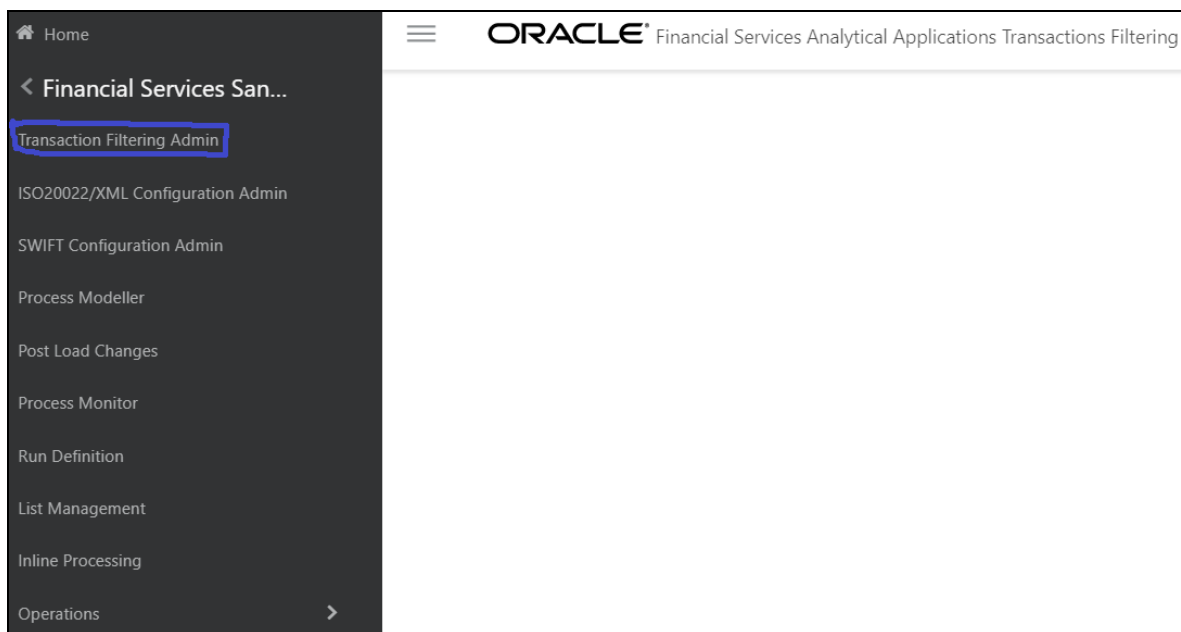
3.2.2 ISO20022 Configuration Admin Menu

The **ISO20022/XML Configuration Admin** menu allows the system administrator to configure the ISO20022 parser parameters. For more information, see Configurations for the ISO20022 Message Parameters.

To view the menu, follow these steps:

1. Click **Financial Services Sanctions Pack**.

   Figure 6: Financial Services Sanctions Pack Menu
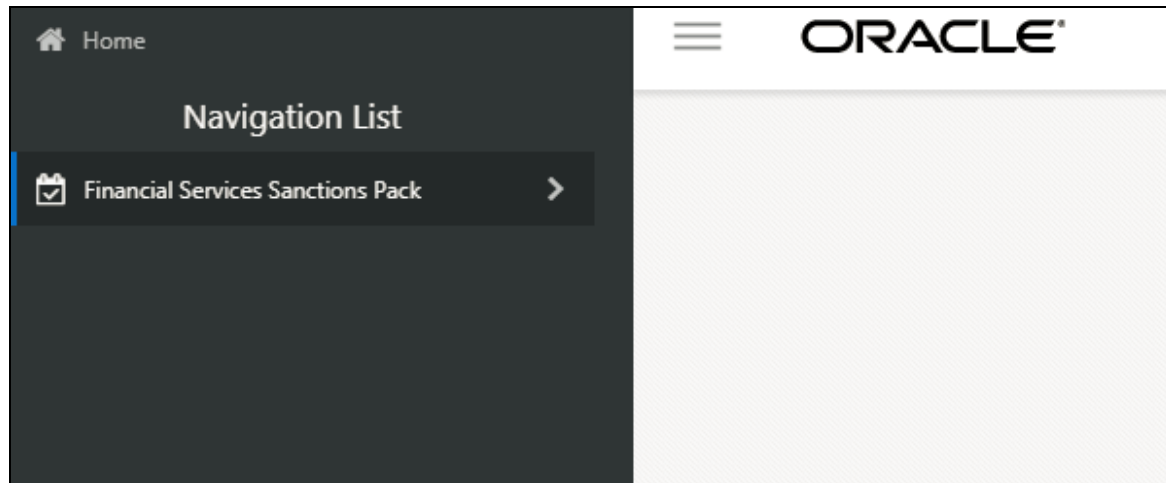
2. Click **ISO20022/XML Configuration Admin.** The *Configuration Screen* displays.

   Figure 7: ISO20022/XML Configuration Admin Sub-menu
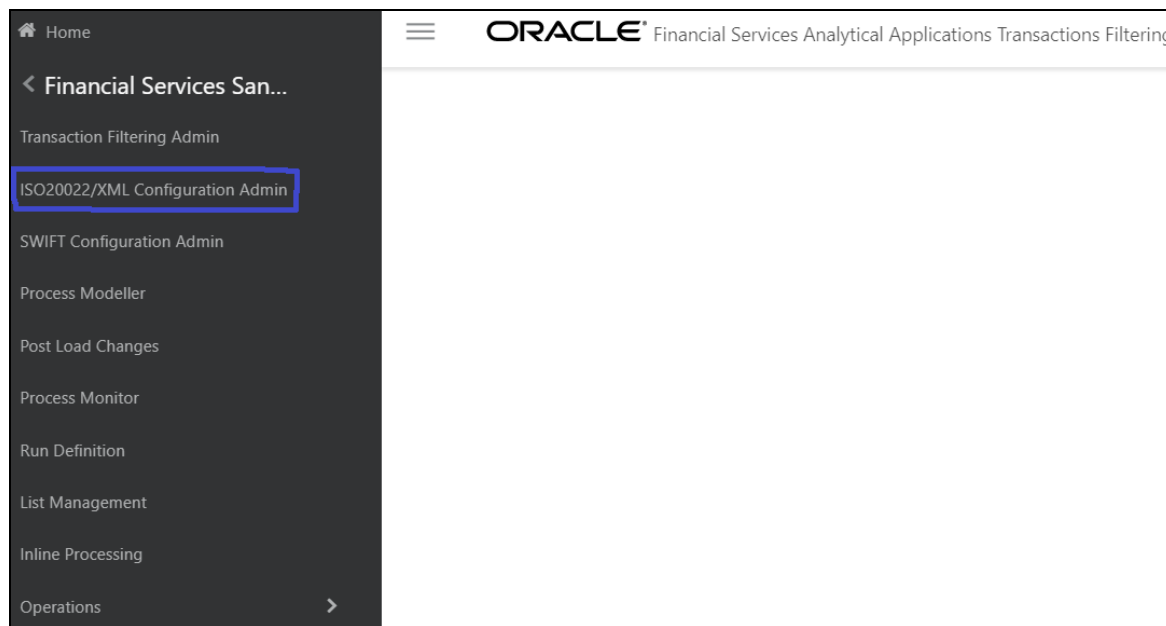
3.2.3 SWIFT Configuration Admin Menu

The **SWIFT Configuration Admin** menu allows the system administrator to configure the SWIFT parser parameters. For more information, see General Configurations.

To view the menu, follow these steps:

1. Click **Financial Services Sanctions Pack**.

   Figure 8: Financial Services Sanctions Pack Menu
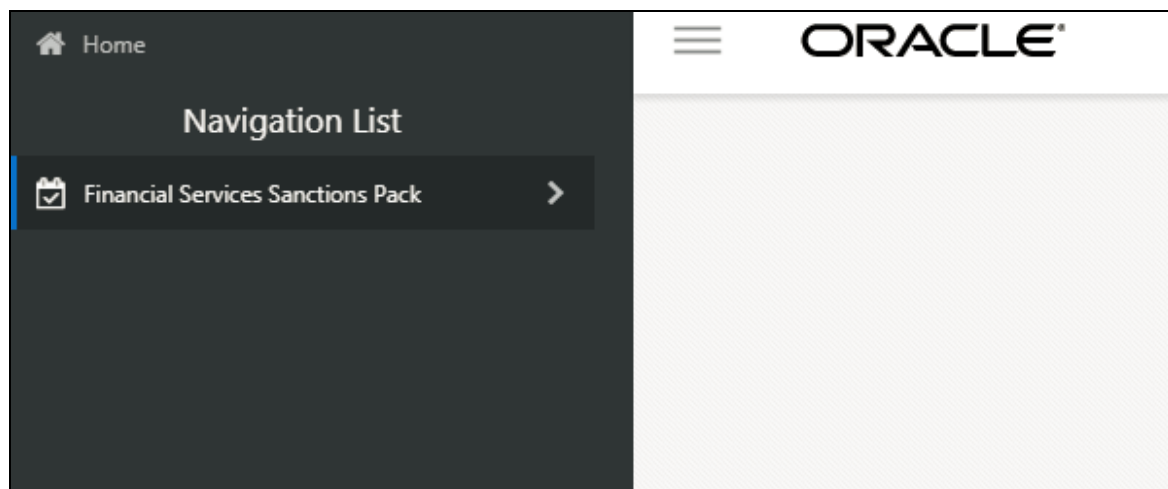
2. Click **SWIFT Configuration Admin.** The *Configuration Screen* displays.

   Figure 9: SWIFT Configuration Admin Sub-menu
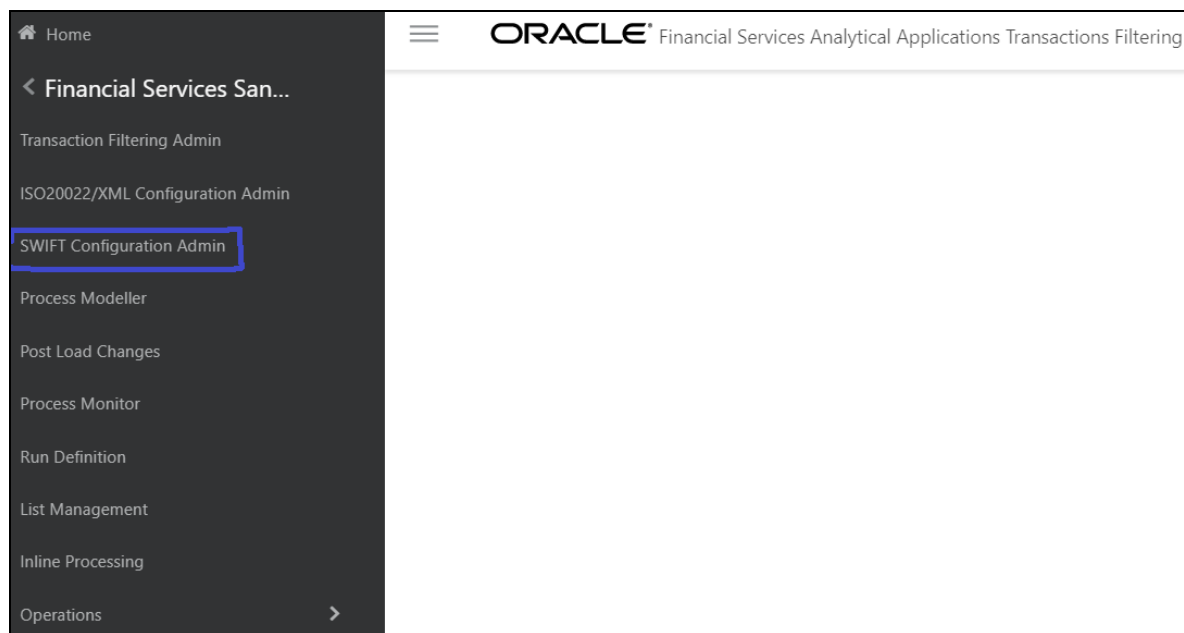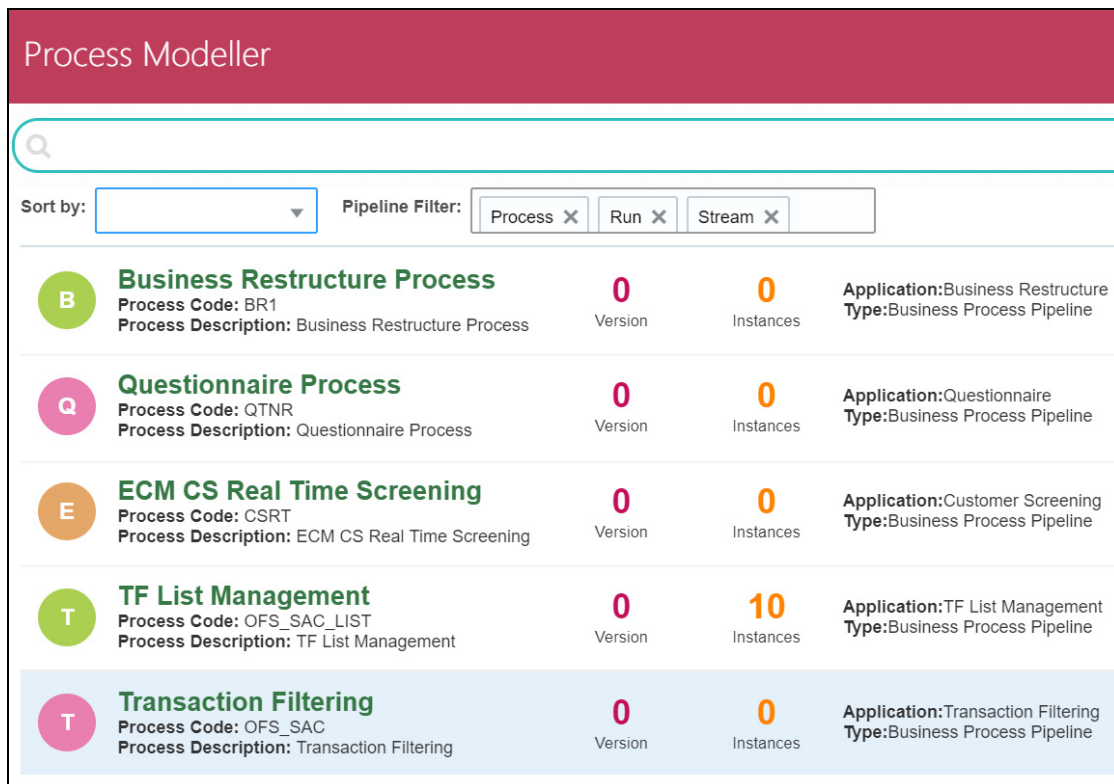
3.2.4 Process Modeller Menu

The **Process Modeller** menu allows the System Administrator to provide the security and operational framework required for the Infrastructure.

You can view the PMF process flow for the standard, four-eyes, and good guy workflows. For more information on the workflows, see the **Transaction Filtering WorkFlows** section in the Oracle Financial Services Transaction Filtering User Guide.

To view the ready-to-use PMF flows, click **Process Modeller**. The **Process Modeller** page is displayed.

Figure 10: Process Modeller Page

To expand the window, click **Navigation Menu** .

3.2.4.1   Configuring the Transaction Currency

You can change the default transaction currency (USD) to another currency. To configure the currency, follow these steps:

1. On the **Process Modeller** page, click the **Application Rule** subtab.

Figure 11: Application Rule Subtab

Select	Rule Name	Rule Type	Implementation Type
○	Sup_Access_Attr_Rule	DecisionRule	Attribute Expression
○	Analyst_Access_Attr_Rule	DecisionRule	Attribute Expression
○	Default	DecisionRule	SQL
○	Outcome Approve	DecisionRule	Outcome
○	Outcome Reject	DecisionRule	Outcome
○	Outcome Submit	DecisionRule	Outcome
○	Hold_Outcome	DecisionRule	Outcome
○	Assigned_Outcome	DecisionRule	Outcome
○	Escalate_Outcome	DecisionRule	Outcome
○	Release_Outcome	DecisionRule	Outcome
○	Block_Outcome	DecisionRule	Outcome
○	R_to_Release_Outcome	DecisionRule	Attribute Expression
○	R_to_Block_Outcome	DecisionRule	Attribute Expression

(Tabs: Process Flow | Definition | **Application Rule** | DataFields. Toolbar: Add ▾ | Edit | Delete)

2. To change the currency for a released transaction, select **R_to_Release_Outcome**. To change the currency for a blocked transaction, select **R_to_Block_Outcome**.

3. Click **Edit**.

4. Click inside the **TF_Currency** drop-down list and select the required currency.

5. Click **Save**.

3.2.5 FEDWIRE Configuration Admin Menu

The **FEDWIRE Configuration Admin** menu allows the system administrator to configure the Fedwire parser parameters. For more information, see General Configurations.

To view the menu, follow these steps:

1. Click **Financial Services Sanctions Pack**.

   Figure 12: Financial Services Sanctions Pack Menu
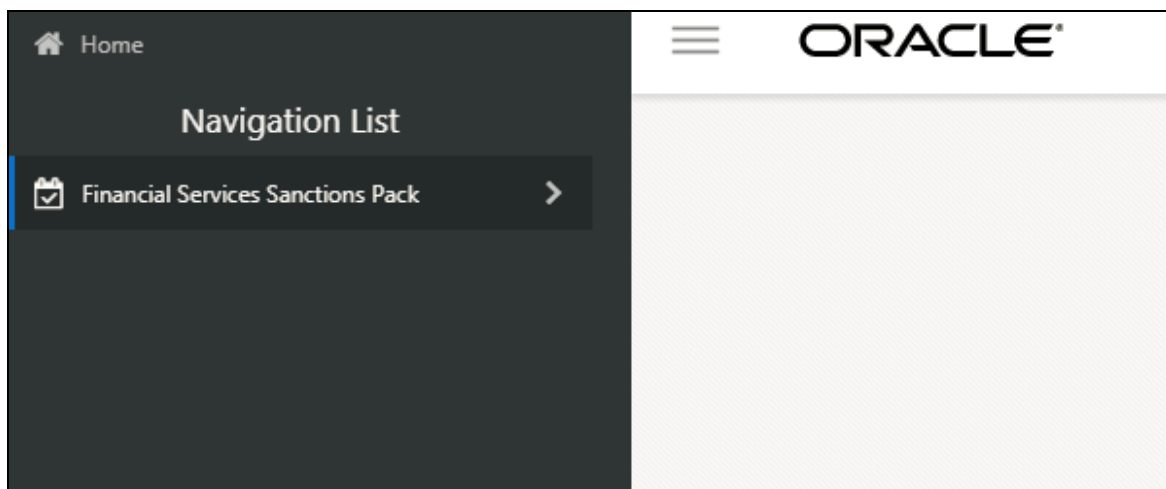
2. Click **FEDWIRE Configuration Admin.** The **Configuration Screen** is displayed.

   Figure 13: FEDWIRE Configuration Admin Sub-menu
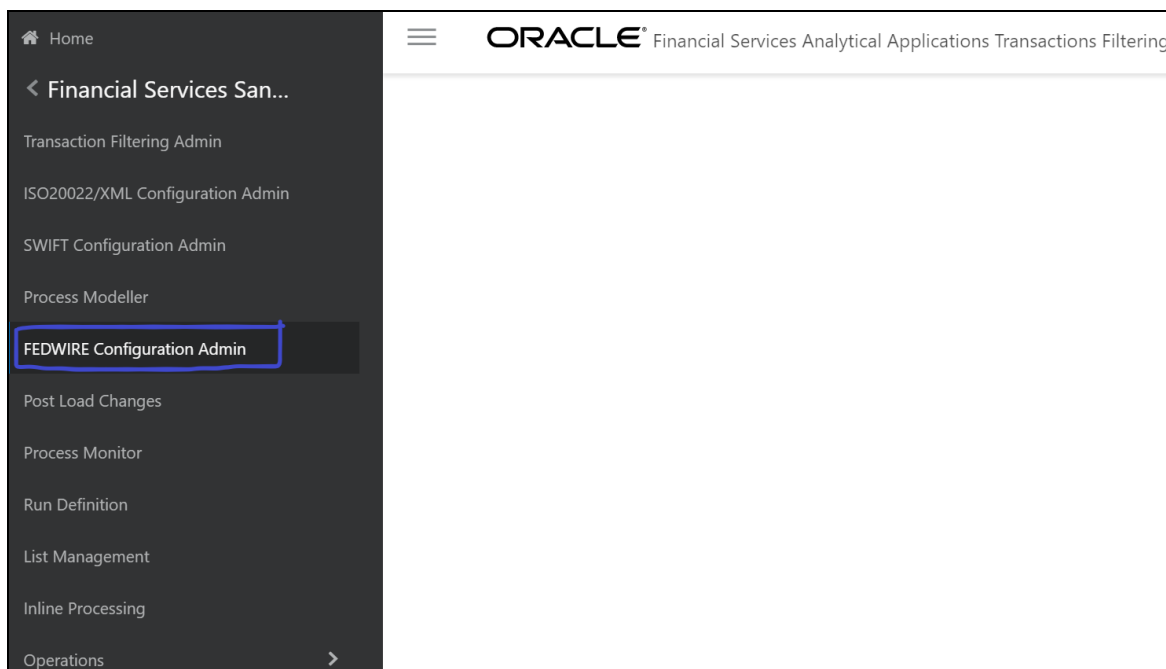
3.2.6 Process Monitor Menu

The **Process Monitor** menu allows the System Administrator to configure the workflow for a process. To do this, click **Process Monitor**. The **Process Monitor** page is displayed.

Figure 14: Process Monitor Menu Page

To expand the window, click **Navigation Menu** ▭.

3.2.7 Run Definition Menu

The **Run Definition** menu allows the system administrator to run the batches for the message formats.

To run the batches, follow these steps:

1. Click **Financial Services Sanctions Pack**.

   Figure 15: Financial Services Sanctions Pack Menu
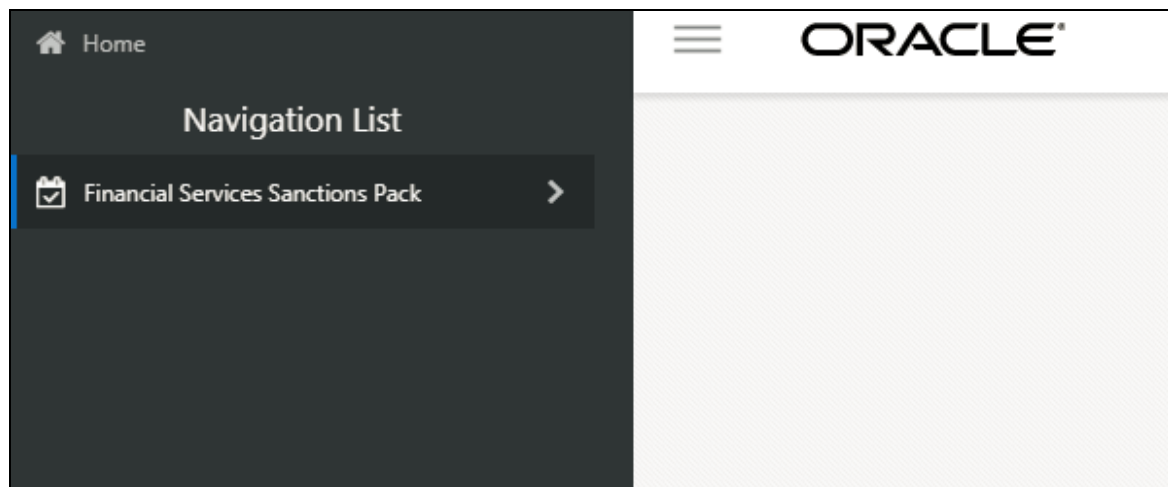
2. Click **Run Definition.** The **Run** page is displayed.

   Figure 16: Transaction Filtering Admin Sub-menu
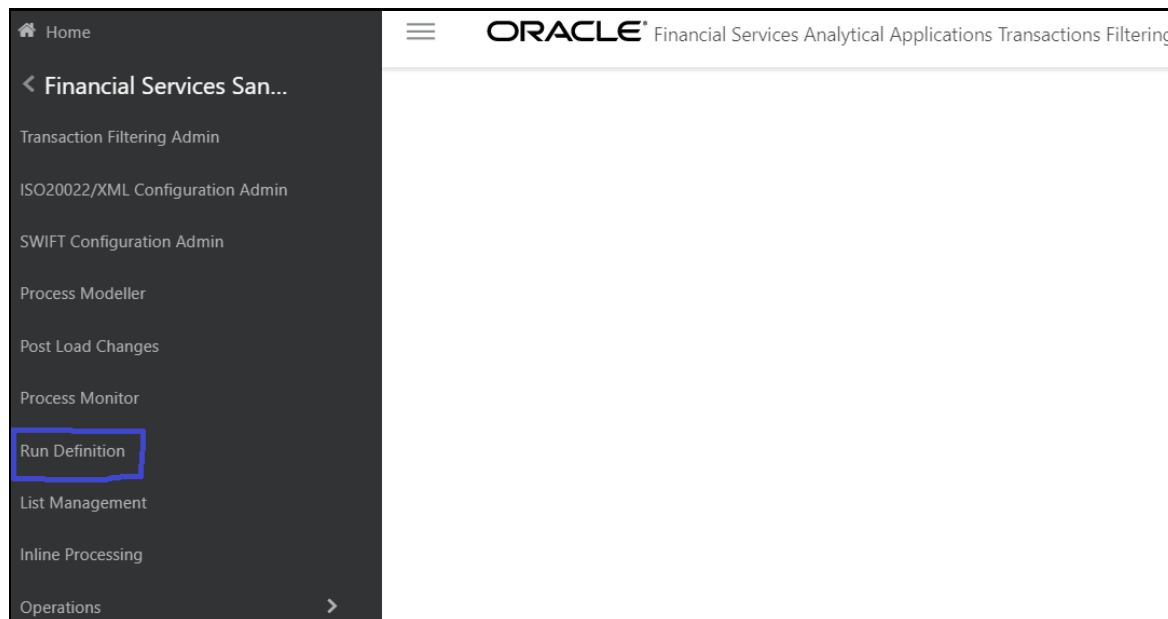
3.2.8   List Management Menu

The **List Management** menu allows the system administrator to view the **Good Guy Summary** page. For more information on the **Good Guy Summary** page, see the **Good Guy Summary** section in the Oracle Financial Services Transaction Filtering User Guide.

To view the page, follow these steps:

1. Click **Financial Services Sanctions Pack**.

    Figure 17: Financial Services Sanctions Pack Menu
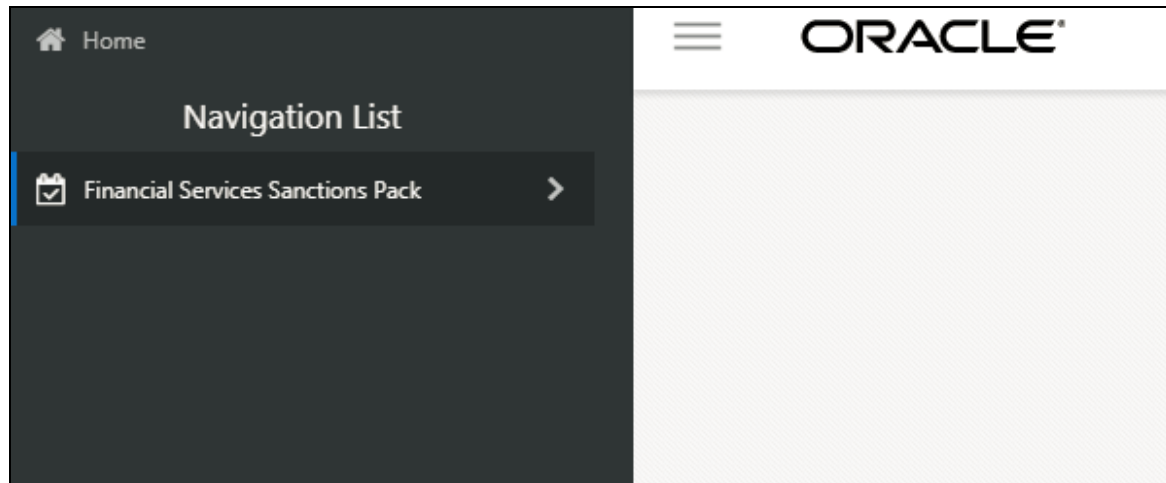
2. Click **List Management.** The **Good Guy Summary** page is displayed.

    Figure 18: List Management Sub-menu
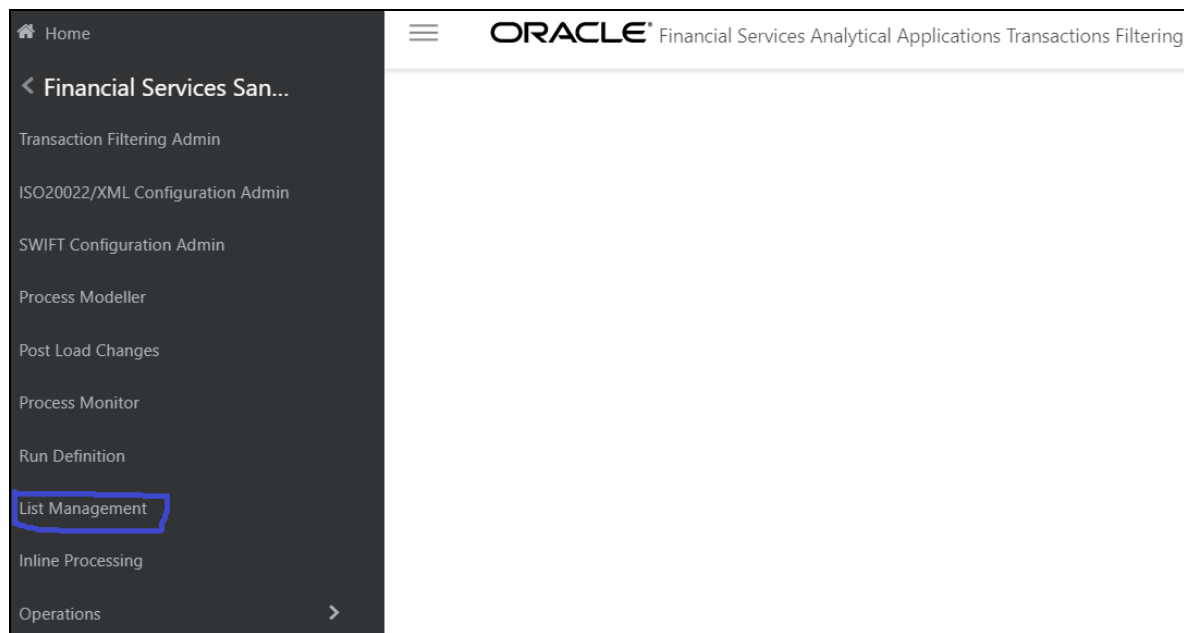
3.2.9 Inline Processing Menu

The **Inline Processing** menu allows the System Administrator to view and configure the details related to Inline Processing Engine (IPE). For more information, see Configuring Risk Scoring Rules.

To view the **Inline Processing** page, follow these steps:

1. Click **Financial Services Sanctions Pack**.

   Figure 19: Financial Services Sanctions Pack Menu
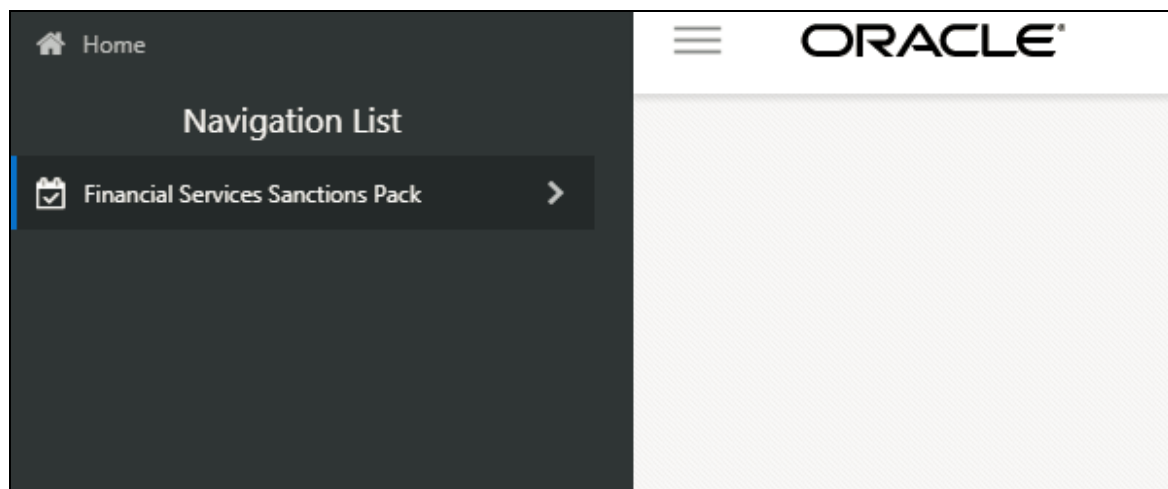
2. Click **Inline Processing.** The **Inline Processing** page is displayed.

   Figure 20: Inline Processing Sub-menu
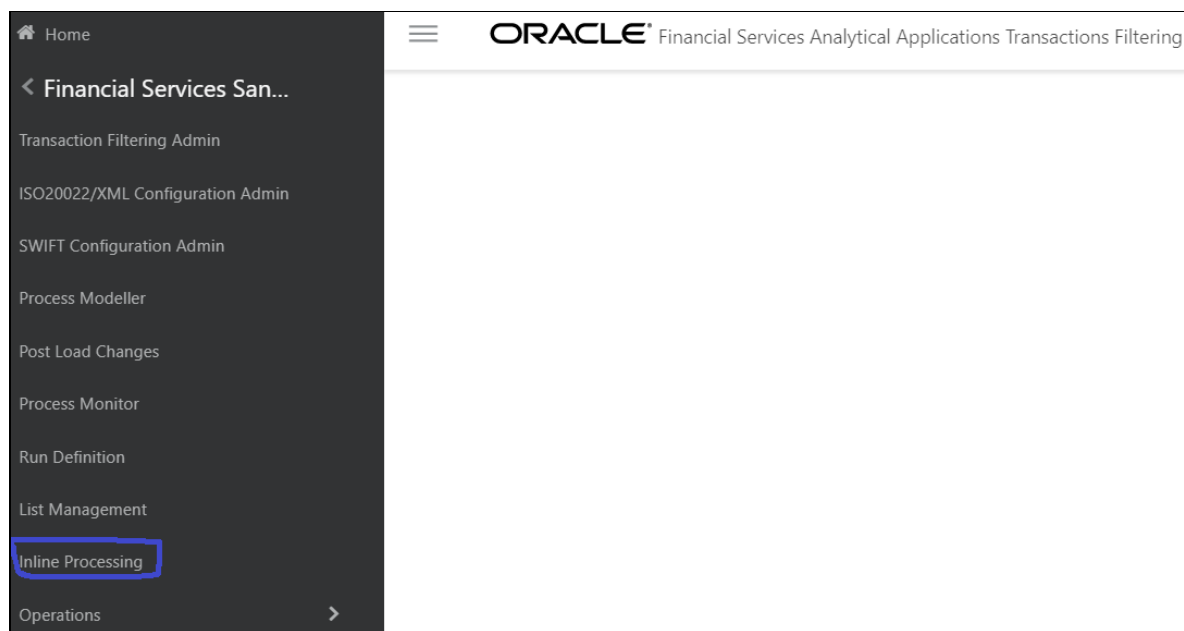
3.3 Troubleshooting Your Display

If you experience problems logging into Oracle Financial Services Transaction Filtering or with your display, the browser settings may be incompatible with running OFSAA applications. The following sections provide instructions for setting your Web display options for OFSAA applications

3.3.1 Enabling JavaScript

This section describes how to enable JavaScript.

To enable JavaScript, 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, select **all options**.

6. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

3.3.2 Enabling Cookies

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

3.3.3 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 adjust your Temporary Internet File settings, follow these steps:

1. Navigate to the **Tools** menu.

2. Click **Internet Options**. The **Internet Options** dialog box is displayed.

3. On the **General** tab, click **Settings**. The **Settings** dialog box is displayed.

4. Click **Every visit to the page**.

5. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

3.3.4 Enabling File Downloads

This section describes how to enable file downloads.

To enable file downloads, 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. Under the **Downloads** section, ensure that **Enable** is selected for all options.

6. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

3.3.5 Setting Printing Options

This section explains how to enable printing background colors and images.

To enable this option, follow these steps:

1. Navigate to the **Tools** menu.

2. Click **Internet Options**. The **Internet Options** dialog box is displayed.

3. Click the **Advanced** tab. In the **Settings** list.

4. Under the **Printing** setting, 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.

3.3.6 Enabling the Pop-Up Blocker

You may have trouble running the Oracle Financial Services Transaction Filtering application when the IE Pop-up Blocker is enabled. It is recommended to add the URL of the application to the **Allowed** *Sites* in the Pop-up Blocker Settings in the **IE Internet Options** menu.

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**. The Settings are enabled.

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.

3.3.7 Setting Preferences

Use the Preferences section to enables you to set your OFSAA home page.

To access this section, follow these steps:

1. In the **Financial Services Analytical Applications Transactions Filtering** page, select **Preferences** from the user name drop-down list. The **Preferences** page is displayed.

Figure 21: 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 M/dd/yyyy.

4. Click **Save** to save your preferences.

4   Managing User Administration

This chapter provides instructions for performing the user administration of Oracle Financial Services (OFS) Transaction Filtering.

4.1   About User Administration

User administration involves creating and managing users and providing access rights based on their roles. This section discusses the following:

- Administrator permissions
- Creating roles and granting and authorizing a user

4.2   Managing User Administration

The following sections provide information on how to create and authorize a user and map the users to user groups in the Transaction Filtering application.

The following table lists the various actions and associated descriptions of the user administration process flow:

Table 3: User Administration

Action	Description
Creating and Authorizing a User	Create a user. This involves providing a user name, user designation, and the dates between which the user is active in the system.
Mapping a User with a User Group	Map a user to a user group. This enables the user to have certain privileges that the mapped user group has.

4.2.1.1   Creating and Authorizing a User

The sysadmn user creates a user and the sysauth user authorizes a user in the Transaction Filtering application. For more information on creating and authorizing a user, see the Oracle Financial Services Analytical Applications Infrastructure User Guide.

4.2.1.2   Mapping a User with a User Group

This section explains how to map Users and User Groups. The user has access to privileges as per the role. The sysadm user maps a user to a user group in the Transaction Filtering application. The following table describes the predefined User Roles and corresponding User Groups.

Table 4: User Group-Role Mapping

Role	Group Name	User Group Code
Administrator	Transaction Filtering Analyst Group	TFLTADMINISTATORGRP
Analyst	Transaction Filtering Supervisor Group	TFLTANALYSTGRP

Role	Group Name	User Group Code
Supervisor	Transaction Filtering Administrator Group	TFLTSUPERVISORGRP

For each role, you can configure the time zones that apply to them. For information on the time zone values, see Time Zone Configuration.

5   General Configurations

The following sections provide information on how to configure the application and message and screening parameters, configure the transaction workflow to accommodate the four-eyes principle and the good guy component, define the cut-off time for the message workflow (including investigations), set a priority for a message category, define the assignment type for messages (manual or automatic), run the purge and migration utilities, add a good guy record, view the different emails generated based on the transaction status, segregate the alerts based on jurisdictions and business domains, and do version control for SWIFT messages, ISO20022 messages, and IPE.

5.1   Configuring the Application Level Parameters

Use the **Application Level Parameter Configuration** tab to configure the parameters for the Transaction Filtering (TF) application, such as enabling or disabling the four-eyes workflow, define the parameters that must be matched during the good guy workflow, define the cut-off period required to complete the entire transaction workflow, and assign messages manually or automatically.

To configure the parameters, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** home page.

2. Click **Transaction Filtering Admin**. The **Application Level Parameter Configuration** is displayed.

    Figure 22: Application Level Parameter Configuration Tab

3. In the **Audit** section, select **Yes** to view the Debug details or select **No** to view the Info details.

If you select **Yes**, then all the steps are logged in the system irrespective of the value in the **Status** column. If you select **No**, then only those steps for which the value is **Y** in the **Status** column are logged in the system.

NOTE	For more information on the values in the *Status* column, see System Audit Logging Information.

4. In the **4 Eyes** section, select **Yes** to enable the four-eyes workflow and select **No** to disable the four-eyes workflow.

5. In the **EDQ** section, provide the following values:

   ▪ **EDQ URL** in the following format:

   `<http>: <Hostname of the server in which EDQ is installed>: Port Number`

   ▪ **EDQ UserName**: The default username is displayed. You can update the username if required.

   ▪ **EDQ PassWord**: The default password is displayed. You can update the password if required.

   ▪ **EDQ webservice status username**

   ▪ **EDQ webservice status password**

6. In the **FEEDBACK** section, enter the URL where we need to post messages for HOLD, RELEASE, CLEAN, BLOCK in the feedback queue in the **FEEDBACK URL** field.

7. In the UI section, provide the time period after which the system refreshes the notification (false positive) count in the Transaction Filtering window.

NOTE	• The time period is in milliseconds.
	• The notification count is reset to zero every day at midnight.

8. Click **Save**. The following confirmation message is displayed**: Records Updated Successfully**.

5.2   Configuring the Good Guy Matching Parameters

The parameters shown here are applicable only when the good guy workflow is enabled. The TF application checks if there is a match or not for every parameter which is enabled, and if there is a match, the record is added to the good guy list. For more information on the good guy workflow, see the **Managing Transaction Filtering** chapter in the Oracle Financial Services Transaction Filtering User Guide.

To enable or disable the good guy parameters, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** home page.

2. Click **Transaction Filtering Admin** and then click the **Good Guy Matching Configuration** tab.

Figure 23: Good Guy Matching Configuration Tab

The record name must be matched, so it is mandatory to set the value in the **Record Name** to **Yes**. If you do not set it to **Yes**, an error message, "**The record name should be set as Yes mandatorily**." is displayed.

5.3   Configuring the Cut-Off Parameters for Alerts

Use the **Cut-Off Configuration** window to set a cut-off time for the investigator to complete the alert investigation. You can either set a single cut-off time for all alerts or set different cut-off times for each alert based on multiple conditions such as message category, message type, jurisdiction, business domain, currency, amount range, message priority, and message direction.

> **NOTE**   The cut-off time must be defined in HH:MM:SS format.

To set a single cut-off time for all alerts, define the cut-off time in the **Cut-Off Time** field and then select **Any** in the condition fields which have drop-down values. Do not enter a value in the **Currency** and **Amount** fields.

To set different cut-off times based on specific values, define the cut-off time in the **Cut-Off Time** field and then select one or more values in the condition fields. Here, you can enter a value in the **Currency** and **Amount** fields. For more information, see step 6.

> **NOTE** If you set different cut-off times, ensure that you define the conditions in such a way that the cut-off time defined for a specific set of conditions does not overwrite the cut-off time defined for another set of conditions.

When the cut-off time is set for an alert, the alert displays the time in *green* in the Investigation User Interface until the cut-off time is passed. After the cut-off time is passed, that is, the alert becomes overdue and is not investigated within the defined cut-off time, then the alert displays the time in *red* in the Investigation User Interface. For information on the Investigation User Interface, see the Oracle Financial Services Transaction Filtering User Guide.

You can set an automatic action to be taken by the system if the alert is not investigated within the defined cut-off time using the **Auto Action Parameter** field (this is an optional step). For example, if you select **Escalate**, then the alert is escalated to the Supervisor after the cut-off time is passed. You can also set a notification to be sent for overdue alerts as soon as the cut-off time is passed for an alert to any user role, for example, to a supervisor. For more information, see the Generating Email for Different Statuses section.

To set the cut-off time, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** home page.

2. Click **Transaction Filtering Admin** and then click the **Cut-Off Configuration** tab.

Figure 24: Cut-Off Configuration Tab

3. Enter the cut-off time in `HH:MM:SS` format. This is the time period by when the alert must be closed by the investigator.

4. Select an automatic action for an alert that is overdue. You can do one of the following:

   ▪ Recommend to block the transaction

- Block the transaction

- Recommend to release the transaction

- Release the transaction

- Escalate the transaction

5. Select **Yes** to enable a specific combination, else select **No**.

6. To create a combination, use the following conditions. This is an optional step.

- **Message Category**: Select the message category used for the transaction. You can also select **Any** to indicate that regardless of the message category, the cut-off time is enabled for the combination. If you select **Any**, you cannot select a message type.

- **Message Types**: Select a message type for the message category. You can also select **All** to indicate that the cut-off time is enabled for all message types.

> **NOTE**   If you have selected the message type as **All** for a configuration, you cannot select a specific message type using the same configuration. If you do, then the configuration with the **All** value overwrites the configuration with the message type value.

- **Jurisdiction**: Select the jurisdiction/geography if the defined cut-off time must apply to only this jurisdiction. You can also select **All** to select all jurisdictions/geographies.

- **Business Domain**: Select the business domain if the defined cut-off time must apply to only this business domain. You can also select **All** to select all business domains.

- **Currency**: Enter the ISO currency code of the currency used for the transaction.

- **Amount**: Select the amount range used in the transaction.

- **Priority**: Set a specific alert priority or select **Any** to indicate that the alert can have any priority.

- **Message Direction**: Select INBOUND for transactions that are coming into your account and select OUTBOUND for transactions that are going out of your account. You can also select **Any** to select any message direction.

After you select the values in the required fields, you can do the following:

Table 5: General Actions

To...	Do this...
Add a configuration	Click **Add**. The values appear in a tabular format.
Update a configuration	Select the configuration you want to update, update the value of one or more fields, and click **Update**. The updated value is displayed in the table.
Remove a configuration	Select the configuration you want to remove and click **Remove**. The selected configuration is removed from the table.

To...	Do this...
Clear the values of some of the fields in a configuration	Click **Clear**. You can only clear the values of the *Cut-Off Time*, *Currency*, and *Amount* fields.
Enable all configurations	Click **Enable All**.
Disable all configurations	Click **Disable All**.

> **NOTE**   After you remove a configuration, you must restart all web services.

5.4   Automatic Assignments of Alerts

The Transaction Filtering application provides two options for assigning alerts:

- **Manual assignment**: Here the user must manually assign alerts one by one using the lock button in the Investigation Use Interface.

  When you manually assign an alert, then all alerts which belong to the selected jurisdiction/business domain are displayed. You can manually assign an alert if, for example, the Analyst to whom the alert is assigned is on leave. In this case, the Supervisor moves the status of the alert from **ASSIGNED** to **HOLD** in the Investigation User Interface. The Analyst can self-assign the alert using the lock/unlock feature. For more information on the Investigation User Interface, see the **Managing Transaction Filtering** chapter in the Oracle Financial Services Transaction Filtering User Guide.

- **Automatic assignment**: Alerts are automatically assigned to the selected user role and respective user IDs. When you auto-assign an alert, the alert is automatically assigned to all users who belong to the selected role. You can use two options: load balancing or load balancing along with specific criteria, to assign the alert.

- **Retrigger functionality**: With Retrigger functionality, while posting the SWIFT/Fedwire messages, if the EDQ pointing to the application is down, the user should have the privilege to configure the message posting time with `RETRIGGER_INTERVAL_MINS` parameter in the `setup_rt_params` table under atomic schema. By default, the timer is set to 30 minutes which are customizable and can be changed (increased/decreased) as per user requirement.

> **NOTE**
> - The Transaction Filtering application assigns all new alerts to the Analyst by default.
> - Alerts cannot be assigned to a user who is mapped to the Admin role.

> **NOTE**   You cannot change the mode of assignment from automatic to manual for an alert that is already assigned. You can only select a mode of assignment for new alerts.

To configure an alert to be assigned manually or automatically, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** home page.

2. Click **Transaction Filtering Admin** and then click the **Auto Assignment Configuration** tab.

3. Select **Automatic** to auto-assign the alert to the selected role. Select **Manual** to manually assign an alert to the selected user.

   If you select **Automatic**, you can choose between **Based On Load Balancing** to select a user role or **Custom Criteria With Combination Of Load Balancing** to select a user role along with the following conditions.

   If you select **Based On Load Balancing**, all users who belong to the role are assigned the alert and the maximum capacity for each user role must be defined.

Figure 25: Auto Assignment Configuration Tab with Based on Load Balancing Selection

If you select **Custom Criteria With Combination Of Load Balancing**, you can select a user role and a specific combination of conditions. The system then applies load balancing along with these conditions, while also applying the maximum capacity defined for the users.

Figure 26: Auto Assignment Configuration Tab with Custom Criteria with Combination of Load Balancing Selected

The following conditions must be defined:

- **User Role**: Select the role to whom you want to automatically assign alerts. When you select the role, all users who belong to that role are displayed in the *User ID* field. You can assign an alert to any user except the Admin user.

- **User ID**: Select the user to whom you want to automatically assign alerts.

- **Jurisdiction**: Select the jurisdiction applicable to the combination, or select **All** to indicate that for all jurisdictions, the alert auto-assignment is enabled for the combination.

- **Business Domain**: Select the business domain applicable to the combination or select **All**.

- **Max Capacity**: Select the maximum number of alerts that can be investigated by the selected user.

- **Enable Flag**: Select **Yes** to enable the combination.

The following additional fields can be used to create a combination when you select **Custom Criteria With Combination Of Load Balancing**:

- **Message Category**: Select the message category used for the combination or select **Any** to indicate that regardless of the message category, the alert auto-assignment is enabled for the combination.

- **Message Types**: Select a message type for the message category or select **None**.

- **Match Score**: Select the match score range. If the match score is between this range, then the alert is assigned to the selected user based on the configuration.

- **Priority**: Set the message priority or select **Any**.

- **Currency**: Enter the ISO currency code of the currency used during the transaction.

- **Amount**: Select the amount range used in the transaction.

After you select the values in the required fields, you can do the following:

Table 6: General Actions

To...	Do this...
Add a configuration	Click **Add**. The values appear in a tabular format.
Update a configuration	Select the configuration you want to update, update the value of one or more fields, and click **Update**. The updated value is displayed in the table.
Remove a configuration	Select the configuration you want to remove and click **Remove**. The selected configuration is removed from the table.
Clear the values of some of the fields in a configuration	Click **Clear**. You can only clear the values of the **Currency** and **Amount** fields.
Enable all configurations	Click **Enable All**.
Disable all configurations	Click **Disable All**.

5.4.1 Configuring the Host Port and Context Name

In the `setup_rt_params` table, set the `V_ATTRIBUTE_VALUE1` value for `HOST_NAME`, `PORT` and `SANC_CONTEXT_NAME` corresponding to the `N_PARAM_IDENTIFIER value` as `55` and the `V_PARAM_NAME` value as `XML_WEB_SERVICE_BASE_URL`. It is in the following format:

`http://##HOST_NAME##:##PORT##/##SANC_CONTEXT_NAME##/SanctionsService`

Example:

http://whf00bls:8930/SAN807SEPA/SanctionsService

5.5 Setting the Priority for Messages

You can set the priority for a specific message category as **High**, **Medium**, and **Low** based on certain criteria such as the message jurisdiction, message type, and amount. The seeded message categories are **High**, **Medium**, and **Low**. To add other priority types, do an inner join of the `V_ATTRIBUTE_VALUE1` column with the `DIM_ALERT_PRIORITY_TYPE` table.

The ready-to-use application extracts some of the key fields of the message into the `FSI_RT_AL_MSG_TAG` table.

If you want to use any field to define the priority, write an SQL query in the `V_ATTRIBUTE_VALUE1` column of the `SETUP_RT_PARAMS` table.

To define the priority for a message category, follow these steps:

1. Run the following query to view the `SETUP_RT_PARAMS` table:

   `select * from SETUP_RT_PARAMS;`

2. Search for the `MESSAGE_PRIORITY` value in the `V_PARAM_NAME` column.

3. In the `V_ATTRIBUTE_VALUE1` column, write the query or function to define the priority.

You can write functions or queries based on your criteria. It must be an inner join with the `DIM_ALERT_PRIORITY_TYPE` table. After you do an inner join, the system stores the priority for the message category.

5.6 Running the Purge Utility

Use the purge utility to maintain all data such as alerts, transactions, and reference data for a specific archival period for all involved jurisdictions. The archival period can be configured by users who have the required permissions in accordance with each legal entity policy or local data protection requirements.

To run the purge utility, follow these steps:

1. Go to the `purgeTF.sh` file in the `<installed area>/ficdb/bin/` directory and replace the `##Infodom##` placeholder with the name of your Infodom.

2. Run the purge utility from the `<installed area>/ficdb/bin/` directory using the following command:

   ```
   ./purgeTF.sh <from date in mm/dd/yyyy> <to date in mm/dd/yyyy> S/H
   ```

   `S` stands for soft delete and `H` stands for hard delete.

   For example, `./purgeTF.sh 11/11/2019 11/12/2019 S`

3. Verify the purge logs in the following directory:

   ```
   <installed area>/ficdb/log/TFpurge/ path
   ```

5.7 Adding, Editing or Deleting Good Guy Records

You can add, edit or delete a Good Guy record from the **Good Guy List Details** page.

5.7.1 Adding a Good Guy Record

Apart from adding a good guy record using the process mentioned in the **Good Guy/White List Matching** section in the [Oracle Financial Services Transaction Filtering User Guide](), you can also manually add a record to the `FCC_WHITELIST` table, for example, if the record is a trusted customer.

To add a record, follow these steps:

1. In the **Good Guy Summary** section, click **Plus** . A pop-up window is displayed.

Figure 27: Good Guy Summary Pop-up Window

2. Enter the required details.

3. Click **Save**.

5.7.2 Editing a Good Guy Record

After you add a record, you can change the jurisdiction or expiry date of the record by editing the record.

To edit the good guy record, follow these steps:

1. In the **Good Guy Summary** section, click **Actions**.

2. From the drop-down list, click **Edit**.

3. Make the necessary changes to the record.

4. Enter your reasons for editing the record.

5. Click **Save**.

5.7.2.1 Updating the Status of an Expired Alert

If the Supervisor has not worked on the alert and it is past the expiry date, you must move it to the expiry status. To do this, run the Good Guy Expiry Check batch in the Run page.

5.7.3 Deleting a Good Guy Record

You can delete a record, for example, if the record was added in error or the record must no longer be in the Good Guy table.

To delete the good guy record, follow these steps:

1. In the **Good Guy Summary** section, click **Actions**.

2. From the drop-down list, click **Delete**.

3. Enter your reasons for deleting the record.

4. Click **Save**.

The following columns in the `FCC_WHITELIST` table are used for matching. This match can be against a single column or column combinations:

- **V_ORIGIN**: This column contains the watch list name.

- **V_WHITE_ENTITY_NAME**: This column contains the watch list record name.

- **V_WHITE_NAME**: This column contains the input message name.

- **V_IDENTIFIER_CODE**: This column contains the ID of the party name present in the `V_WHITE_NAME` column and comes from the input message.

- **N_RECORD_ID**: This column contains the watch list record ID.

- **V_JURISDICTION**: This column contains the watch list jurisdiction.

- **D_EXPIRE_ON**: This column contains the date after which the record is no longer checked against the records in the `FCC_WHITELIST` table.

5.8 Generating Email for Different Statuses

An email is generated for a transaction depending on its status. The following types of emails are generated:

- Notification Email

- Task Email

-

5.8.1 Notification Email

A notification email is generated for Blocked and Released transactions and the template is as follows:

```
Subject: Notification-<id>-Issue Identified - New issue assigned to you


Hi TFSUPERVISOR,

This is to inform you that a Notification is generated for you in your inbox
for

Notification ID: <id>

Transaction Type: <Message Type>
```

```
Message Reference: <Message Reference>
Status: <Blocked/Released>
User Comments: <User comments>
Received On: 2017-07-25 12:03:19.0


Please access the below link to logon to Transaction Filtering System.
<Application URL>


Regards,
Admin
```

5.8.2 Task Email

A task email is generated for Hold and Escalated transactions and the template is as follows:

```
Subject: Taskid-<id>-Issue Identified - New issue assigned to you


Hi TFSUPERVISOR/TFANALYST,
This is to inform you that a Notification is generated for you in your inbox
for
Task ID: <id>
Transaction Type: <Message Type>
Message Reference: <Message Reference>
Status: <Hold/Escalated>
User Comments: <User comments>       applicable to escalated only
Received On: 2017-07-25 12:03:19.0


Please access the below link to logon to Transaction Filtering System.
<Application URL>


Regards,
Admin
```

5.8.3 Email for an Overdue Alert

An email is generated for an overdue alert if the alert is not closed within the cut-off time set for the alert and the template is as follows:

```
Subject: Notification-Overdue alert Identified - New issue assigned to you


Hi SUPERVISOR,
```

```
This is to inform you that a Notification Overdue alert is generated for you in
your inbox for

Transaction Type    : <Message Type>

Message Reference    : <Message Reference>

Group Message Id     : < Group Message Id >

Status  : <Hold/Escalated>

User Comments : System generated Overdue Notification

Received On   : 2020-11-02 13:16:51


Please access the below link to logon to Transaction Filtering System.
<Application URL>


Regards,

Admin
```

5.9 Configuring Operating Model - Multi-Jurisdiction and Multi-Business Unit Implementation

Alerts are segregated based on jurisdiction and business unit or line of business. You can also configure the alerts that are assigned to the users in the `tfanalytgroup` and `tfsupervisorgrp` groups.

5.9.1 Jurisdiction

Jurisdictions are used to limit user access to data in the database. The user must load all jurisdictions and associate user groups to jurisdictions in the tables as specified in Configuring Jurisdictions and Business Domains. User groups can be associated with one or more jurisdictions.

> **NOTE** All jurisdictions in the system reside in the `FCC_SWIFT_JSRDSN_MAP` table.

In the Investigation User interface system, users can view only data or alerts associated with jurisdictions to which they have access. You can use jurisdiction to divide data in the database. For example:

- **Geographical**: Division of data based on geographical boundaries, such as countries, states, and so on.
- **Organizational**: Division of data based on different legal entities that compose the client's business.
- **Other**: Combination of geographic and organizational definitions. Also, it can be customized.

The definition of jurisdiction varies from between users. For example, a user can refer to a branch BIC as jurisdiction and another user can refer to a customer ID as jurisdiction.

5.9.2 Business Unit/ Line of Business

Business domains are used to limit data access. Although the purpose is like jurisdiction, they have a different objective. The business domain is used to identify records of different business types such as Private Client versus Retail customer, or to provide more granular restrictions to data such as employee data.

If a user has access to any of the business domains that are on a business record, the user can view that record.

NOTE	All business domains in the system reside in the `FCC_SWIFT_BUS_DMN_MAP` table.

5.9.3 Configuring Jurisdictions and Business Domains

The default Sanctions groups are `tfanalytgroup` and `tfsupervisorgrp`. According to the ready-to-use product, these groups get all alerts and notifications for all jurisdictions and business domains. To configure the alerts, follow these steps:

1. Load all the jurisdictions. To do this, run the query `SELECT * FROM FCC_SWIFT_JSRDSN_MAP` and load the jurisdictions in the `V_JRSDCN_CD` column in the `FCC_SWIFT_JSRDSN_MAP` table.

   The following columns are provided to populate any additional information:

   Table 7: Columns used to provide additional information for Jurisdictions

Column	Data Type and Length
V_EXTRACTED_SWIFT_FIELD	VARCHAR2(100 CHAR)
V_JRSDCN_CD	VARCHAR2(40 CHAR)
V_CUST_COLUMN_1	VARCHAR2(4000 CHAR)
V_CUST_COLUMN_2	VARCHAR2(4000 CHAR)
V_CUST_COLUMN_3	VARCHAR2(4000 CHAR)
V_CUST_COLUMN_4	VARCHAR2(4000 CHAR)
N_CUST_COLUMN_1	NUMBER(20)
N_CUST_COLUMN_2	NUMBER(20)
N_CUST_COLUMN_3	NUMBER(20)
N_CUST_COLUMN_4	NUMBER(20)

2. Load all the business domains in the `V_BUS_DMN_CD` column in the `FCC_SWIFT_BUS_DMN_MAP` table.

   The following columns are provided to populate any additional information:

Table 8: Columns used to provide additional information for Business Domains

Column	Data Type and Length
V_EXTRACTED_SWIFT_FIELD	VARCHAR2(100 CHAR)
V_JRSDCN_CD	VARCHAR2(40 CHAR)
V_CUST_COLUMN_1	VARCHAR2(4000 CHAR)
V_CUST_COLUMN_2	VARCHAR2(4000 CHAR)
V_CUST_COLUMN_3	VARCHAR2(4000 CHAR)
V_CUST_COLUMN_4	VARCHAR2(4000 CHAR)
N_CUST_COLUMN_1	NUMBER(20)
N_CUST_COLUMN_2	NUMBER(20)
N_CUST_COLUMN_3	NUMBER(20)
N_CUST_COLUMN_4	NUMBER(20)

3. Map user groups to the appropriate jurisdiction and business domain. To do this, run the query `SELECT * FROM DOMAIN_JUR_GRP_MAP` and do the mapping in the `DOMAIN_JUR_GRP_MAP` table.

   In the case of multiple jurisdictions mapped to a single user group, create as many rows as the number of jurisdictions and add the new jurisdiction in each row for the same user group.

   In the case of multiple business domains for the same user group and same jurisdiction, create as many rows as the number of business domains and add the new business domain in each row for the same user group and jurisdiction.

4. Put the appropriate SQL query in the `Message_jurisdiction` and `Message_Business_Domain` rows to derive the jurisdiction and business domain respectively in the `Setup_Rt_Params` table.

   This step is required to define the source of jurisdiction and business domain from the message or an external source.

   The definition and source of jurisdiction and business domain are different for each customer. In this way, the Transaction Filtering application gives the flexibility to the user to pick any attribute of the message to define the jurisdiction and business domain. For example, jurisdiction can be the BIC present in block 1/block 2 of the SWIFT message or the branch ID present in the SWIFT GPI header.

   The ready-to-use application can extract some of the key fields of the message, which are available in the `fsi_rt_al_msg_tag` table. If the customer wants to use any field as a jurisdiction or business domain from this table, then an SQL query must be written in the `Setup_Rt_Param` table to extract the respective column.

   When a message is posted, the system updates the jurisdiction and business domains extracted in step 4 in the `FSI_RT_RAW_DATA` and `FSI_RT_ALERTS` tables.

5.10   Version Control

Version control for SWIFT messages, IPE, and ISO200222 is accomplished using the Import/export feature in Transaction Filtering. Say a file has been moved from one environment to another environment. Later, the file is updated. The import/export utility will create 2 separate files for each configuration. You can import both the files into the application and use a text file comparator such as *beyond compare* or a version control tool such as *SVN* to view the differences between the exported files.

Version control for EDQ follows a different process. EDQ has an inbuilt version control feature available, so you will just need to compare the `.dxi` files to view the differences.

5.10.1   Version Control for SWIFT Messages and IPE

The steps involved for SWIFT messages and IPE are the same. These steps are explained here:

1. Export the new file and save it in your local drive.

2. Import the file into the Transaction Filtering application.

    You can now compare this file with another file. Ensure that you place these files in separate folders.

5.10.2   Version Control for ISO20022

The steps involved for ISO20022 are explained here:

1. Export the new file and save it in your local drive.

2. Import the file into the Transaction Filtering application.

    You can now compare this file with another file. Ensure that you place these files in separate folders.

    If you want to restore the current version to a previous version of the file, you can delete data from all the tables, import a previously exported file that has the date you want to restore into the application, and restart the webserver. This restores the configuration of the previous version.

5.10.3   Version Control for EDQ

To use the version control feature available within EDQ, follow these steps:

1. In the EDQ application, copy the two different versions of the `.dxi` files into the **EDQ Director** menu.

2. Click **View** and select **Configuration Analysis** in the **EDQ Director** menu.

3. In the popup which appears, select the versions that you want to compare.

4. Click **Configuration**.

5. In the popup which appears, select the differences only and click **OK**.

6. In the same window, select **Start Comparison**. This gives all changes between the two files.

For more information, see Oracle Enterprise Data Quality Documentation.

5.11 Running the Config Migration Utility

Use the config migration utility to import/export SWIFT and ISO20022 message configurations from one environment to another, for example, from the development server to UAT, and subsequently to production. For information on configuring the SWIFT message parameters, see Configuring the SWIFT Message Parameters. For information on configuring the ISO20022 message parameters, see Configurations for the ISO20022 Message Parameters.

To use the utility, first export the configuration from the source environment and then import the file to the destination environment. To export the configuration, follow these steps:

1. Navigate to the `$FIC_HOME/Transaction_Processing/TF_Config_Migration_Utility/config` directory.

2. Open the `Dynamic.properties` file and update the placeholders as shown:

Table 9: Configurations required in the Dynamic.properties file when running the export file

Placeholder	Update with...
##jdbcurl##	Your JDBC URL.
##username##	The Atomic Schema user name using which you want to execute the files.
##password##	The Atomic Schema password for the user name.
##infodom##	Your Infodom name.
The following placeholder applies only to SWIFT:	
##N_SWIFT_MSG_ID##	Your SWIFT ID. This is available in the `n_sanction_swift_msg_id` column in the `dim_sanctions_swift_details` table. If you are providing multiple IDs, add the IDs separated by commas. For example, 1,2,3,4.
The following placeholder applies only to ISO20022:	
##N_XSD_CONF_ID##	Your ISO20022 ID. This is available in the `n_xsd_conf_id` column in the `fcc_tf_xml_xsd_conf` table. If you are providing multiple IDs, add the IDs separated by commas. For example, 1,2,3,4.

3. Navigate to the `TF_Config_Migration_Utlity/bin` directory and run the required command.

   - To run the export file for SWIFT, run `./export.sh SWIFT`

   - To run the export file for ISO20022, run `./export.sh SEPA`

   - To run the export file for SWIFT and ISO20022, run `./export.sh ALL`

To import the configuration, follow these steps:

1. Navigate to the `TF_Config_Migration_Utility/config` directory.

2. Open the `Dynamic.properties` file and update the placeholders as shown:

Table 10: Configurations required in the Dynamic.properties file when running the import file

Placeholder	Update with...
##jdbcurl##	Your JDBC URL.
##username##	The Atomic Schema user name using which you want to execute the files.
##password##	The Atomic Schema password for the user name.
##infodom##	Your Infodom name.
The following placeholder applies only to SWIFT:	
##SWIFT_AUDIT_COMMENTS##	Your comments related to the configurations made.
The following placeholder applies only to ISO20022:	
##N_XSD_CONF_ID##	Your ISO20022 ID. This is available in the `n_xsd_conf_id` column in the `fcc_tf_xml_xsd_conf` table. If you are providing multiple IDs, add the IDs separated by commas. For example, 1,2,3,4.

3. Navigate to the `TF_Config_Migration_Utlity/bin` directory and run the required command.

   ▪ To run the import file for SWIFT, run `./ import.sh SWIFT`

   ▪ To run the import file for ISO20022, run `./ import.sh SEPA`

   ▪ To run the import file for SWIFT and ISO20022, run `./ import.sh ALL`

5.12   Running the SWIFT Migration Utility

Use the SWIFT migration utility to import or export the SWIFT message configurations. For information on configuring the SWIFT message parameters, see [Configuring the SWIFT Message Parameters](#). The message types provided in this utility are available in the `TF_Swift_Migration_Utlity/output/MSG_TYPES` directory.

To export the configurations, follow these steps:

1. Navigate to the `TF_Swift_Migration_Generator/config` directory.

2. Open the `Dynamic.properties` file and update the placeholders as shown:

Table 11: Configurations required in the Dynamic.properties file when running the export file

Placeholder	Update with...
##jdbcurl##	Your JDBC URL.
##username##	The Atomic Schema user name using which you want to execute the files.
##password##	The Atomic Schema password for the user name.

Placeholder	Update with...
##infodom##	Your Infodom name.
The following placeholder applies only to SWIFT:	
##SWIFT_MSG_ID##	Your SWIFT ID. This is available in the `n_sanction_swift_msg_id` column in the `dim_sanctions_swift_details` table. If you are providing multiple IDs, add the IDs separated by commas. For example, 1,2,3,4.

3. Navigate to the `TF_Swift_Migration_Generator/bin` directory and run the `export.sh SWIFTMSGEXPORT MSG_TYPES` command.

   `MSG_TYPES` is the folder name of the folder to which you can export the configurations. Before you perform the export, change the folder name. For example, `Exported`.

   > **WARNING** Do not change the folder name to `MSG_TYPES`. This will overwrite the ready-to-use message types provided with the utility.

To import the configurations, follow these steps:

1. Navigate to the `FIC_HOME/Transaction_Processing/TF_Swift_Migration_Utlity/config` directory.

2. Open the `SWIFT_MSG_TYPES.txt` file and add the message types that you want to import to the `Exported` folder mentioned in the export configuration steps.

3. Open the `Dynamic.properties` file and update the placeholders as shown:

Table 12: Configurations required in the Dynamic.properties file when running the import file

Placeholder	Update with...
##jdbcurl##	Your JDBC URL.
##username##	The Atomic Schema user name using which you want to execute the files.
##password##	The Atomic Schema password for the user name.

4. Navigate to the `TF_Swift_Migration_Utlity/bin` directory and run the `import.sh SWIFTMSGIMPORT MSG_TYPES` command.

   `MSG_TYPES` is the folder name of the folder from where you can import the configurations. Before you perform the import, change the folder name. For example, `Imported`.

> **WARNING**   Do not change the folder name to `MSG_TYPES`. This will overwrite the ready-to-use message types provided with the utility.

After you complete the export and import steps, restart the web server. To verify if the message types have been successfully imported or not, check if the message types are available in the **Message Type Configuration** field in the [Message and Screening Configurations Window](#).

5.12.1   Restoring a Previous Configuration for SWIFT Messages

To restore a configuration, you must first export and then import the configuration from that environment using the SWIFT migration utility, and then restart the webserver. This restores the configuration of the previous version.

Follow these steps to restore the configuration:

1. Export the SWIFT message configuration from the environment using the SWIFT migration utility.

> **NOTE**   Ensure that you save the configuration.

2. To restore the previous version, Import the saved configuration using the SWIFT migration utility.

   When you import a message configuration, and the message already exists in the system, then the value of the `F_LATEST_IDENTIFIER` column is updated to **Y** in the `FSI_RT_SWIFT_CONF_DTLS` and `DIM_SANCTIONS_SWIFT_DETAILS` tables.

   The audit history is captured in the `FSI_RT_SWIFT_CONF_DTLS_HIST` table in the `V_HIST_DESC` column and will have the following remark: `'Configuration Updated Through Migration Utility'`.

5.13   Host Configuration

To configure the Transaction Filtering application for a host location, add the following details:

- Host name of the location
- Port number of the location
- User name and password of the location

5.14   Audit Queries

The following are the audit queries you can run to see the different audit operations:

Table 13: Audit Queries
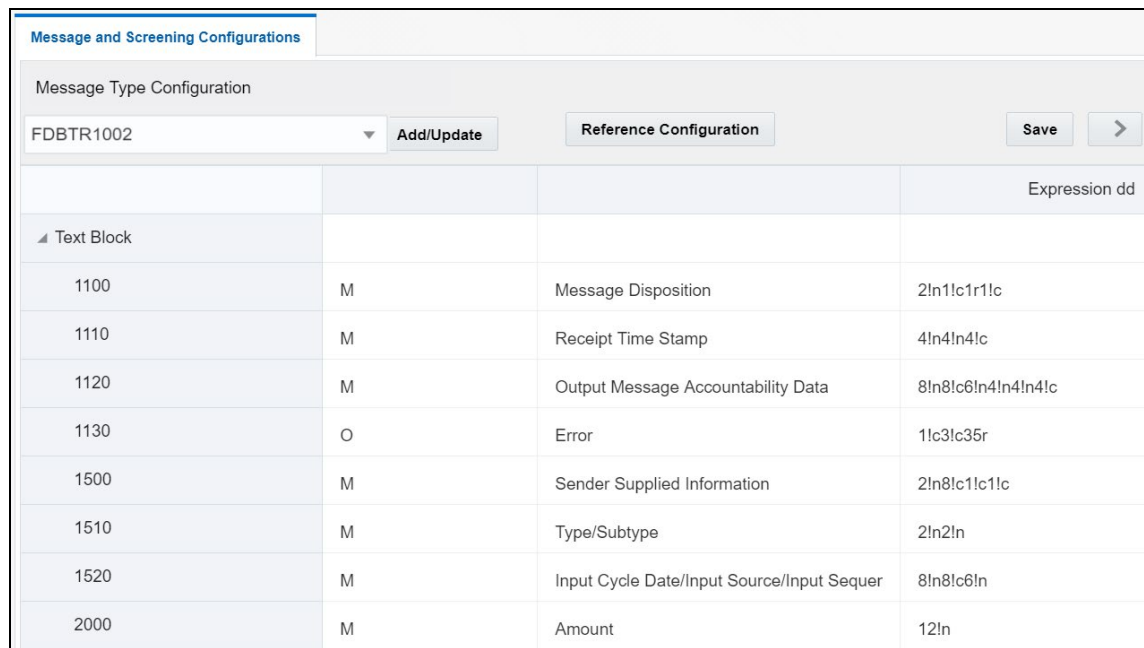
Table Name	Query	Description
`FCC_TF_XML_XSD_CONF`	Select * from `FCC_TF_XML_XSD_CONF_HIST`	Run this query to see the history of all the actions that have been performed.
`FCC_TF_XML_MSG_TAG_FLD_XPATH`	Select * from `FCC_TF_XML_MSG_TAG_FLD_XPATH_HIST`	Run this query to see the history of all the actions performed in the *XML Message Configuration* tab.
`FCC_TF_XML_SCRENG_XPATH_GRP`	Select * from `FCC_TF_XML_SCRENG_XPATH_GRP_HIST`	Run this query to see the XPath for each parent node.
`FCC_TF_XML_SCRENG_FLD_XPATH`	Select * from `FCC_TF_XML_SCRENG_FLD_XPATH_HIST`	Run this query to see the XPath for each subfield node.

6 Configuring the Fedwire Message Parameters

To configure the message and screening parameters, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** home page.

2. Click **FEDWIRE Configuration Admin**. The **Message and Screening Configurations** tab is displayed.

Figure 28: Message and Screening Configurations tab for Fedwire

Message and Screening Configurations				
Message Type Configuration				
FDBTR1002 ▼	Add/Update	Reference Configuration		Save >
				Expression dd
▲ Text Block				
1100	M	Message Disposition		2!n1!c1r1!c
1110	M	Receipt Time Stamp		4!n4!n4!c
1120	M	Output Message Accountability Data		8!n8!c6!n4!n4!n4!c
1130	O	Error		1!c3!c35r
1500	M	Sender Supplied Information		2!n8!c1!c1!c
1510	M	Type/Subtype		2!n2!n
1520	M	Input Cycle Date/Input Source/Input Sequer		8!n8!c6!n
2000	M	Amount		12!n

This tab has the following windows: Message Type Configuration window, <Message Type> Subfield Level Configuration Details window, <Message Type> Screening Configuration Window, and <Message Type> Other Field/Subfield Configuration Window.

6.1 Message Type Configuration Window

This window allows you to edit the status, field names, and expressions of the different JSON parameters in the message.

In the **Message Type Configuration** field, select the Fedwire message category.

The following image shows a sample Fedwire message:

Figure 29: Sample Fedwire Message

{1100}02P 7{1110}03082108FT01{1120}20060309B6B0072D00000103082108FT01{1500}30QWERTYUIPP{1510}1002{1520}20200317CTRFULLC000156{2000}000001234567{3100}123456789IRAN
DEVOTIONAL*{3320}IPE1030800065862{3400}123456789RIHS IVORY COASTS SOMALIA*{3500}PREMSGIDENTIFIER{3600}BTR{4000}BSIIBSYDA*SYRIA INTERNATIONAL ISLAMIC BANK
****{4100}D121149*MELLI BANKAS*Paris*FRANCE**{4200}D1234456656*MELLI BANKAS*Paris*FRANCE**{4320}TERRORIST{5000}D123456789*Wells Fargo Bank Texas National*Association 109 North San
Saba*San Antonio Texas 78207**{5100}BBOFAUS3N*COOPER&PRICE MANAGEMENT MANULIFE *PLAZA ROOM 1202-05 12TH FLOOR*THE HK,HONG
KONG**{5200}CCHIPSParticipant*Name*Address1*Address2*Address3*{6000}YOUR INVOICE OFF-0506-7450****{6100}ROUTING NO
026005322******{6200}Terrorist******{6210}LTRLETTERDETAILS******{6300}YOUR INVOICE OFF-0506-7450******{6310}LTRQWERTYUIOP******{6400}L/C NO.CR2016/151479 YR.
REF*RCL/FBDL/151479*****{6410}LTRLETTERDETAILS******{6420}CHECK123456*{6500}CHECK123456******

Each message type has a Text Block. The fields in the Text Block may change depending on the message type.

Figure 30: Message and Screening Configurations tab for Fedwire

In this figure, the first column lists all the message identifiers for the Fedwire message category. The other columns are:

- **Status**: This column mentions whether the field is Mandatory (**M**) or Optional (**O**).

- **FieldName**: This column describes the name of the given field as per Fedwire standards.

- **Expression**: This column depicts the field structure in terms of expression. For example, if the field is a data type, then the maximum length of the field is displayed.

To edit a parameter, click the parameter name. After you make the changes, click **Save**.

6.1.1 Adding or Updating a New Message Type

To add or update an existing message type, follow these steps:

1. Click **Add/Update**. The **Attachment Details** window is displayed.

2. Select the type of message that you want to add or update from the drop-down list.

Figure 31: Attachment Details Window

3. To upload an attachment, click **Choose File** [Choose File]. You can upload only one attachment at a time.

> **NOTE**   This file must be of the format .json or .txt.

4. Click **Upload**.

5. Click **Submit**. The message is displayed in the following table as *<Message Type_draft>*.

   For more information, see the **JSON Upload Configuration** section in the Oracle Financial Services Transaction Filtering Technical Integration Guide.

6.1.2 Configuring Message and Transaction References

Any message which contains message references or transaction references, or both, must be configured. To view and change the message reference or transaction reference, click **Reference Configuration**.

Figure 32: Reference Configuration Window

For the **Message Reference** field, a unique identifier must be configured at the message level for all message categories. For the Transaction Reference field, a unique identifier must be configured at the transaction level only if applicable for the specific message category.

6.2   <Message Type> Subfield Level Configuration Window

This window allows you to add a subfield to a field in the **Message Type Configuration** Window.

Figure 33: <Message Type> Subfield Level Configuration Window

1. To add a subfield, provide the required values in the fields shown in the window and click **Add**
   [Add]. Enter values in the following fields:

Table 14: Fields in the <Message Type> Subfield Level Configuration Window

Fields	Field Description
Expression Identifier	Enter a unique identifier. It must begin with an alpha character and must not contain any spaces. This is a mandatory field.
Expression Name	Enter a name for the expression. The name must be in capital letters. This is a mandatory field.
Expression Description	Enter a description for the Expression. This is a mandatory field.
Field	This field displays a complete list of fields in the drop-down for the given message type. Select the field from this drop-down field to configure the expression.
Field/Subfield Name	This field displays the respective field name or subfield options for the field that was previously selected. Select the subfield from the drop-down list.
Update button	To update an existing subfield, click the name of the subfield. After you make the changes, click **Update** [Update].
Remove button	To remove an existing subfield, click the name of the subfield and click **Remove** [Remove].
Clear button	To clear the data in these fields, click **Clear** [Clear].

You can configure the subfield in two ways:

- By configuring the **subfield level data within the option** expression: Do this if you want to configure specific data within the expression.

  For example, if 1100 has four options A, B, C, and D in the FDBTR1002 message but you want to configure BIC (Identifier Code) from option A:

```
Option A:
[/1!a][/34x]          (Party Identifier)
4!a2!a2!c[3!c]        (Identifier Code)
```

You must enter the names in the **Subfield Expression Identifier**, **Subfield Name**, and **Subfield Description** fields.

- By configuring the element level data within the subfield expression: Do this if you want to further configure any data out of the subfield.

  In this example, if you want to configure the country code for `field 57,` then you can configure `2!a` from Identifier Code expression as a country code by giving unique names in the **Subfield Expression Identifier**, **Subfield Name**, and **Subfield Description** fields.

```
Option A:
[/1!a][/34x]          (Party Identifier)
4!a 2!a 2!c[3!c]       (Identifier Code)
```

6.3   <Message Type> Screening Configuration Window
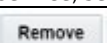
This window allows you to add, update, remove, and enable or disable a web service.

Figure 34: <Message Type> Screening Configuration Window

To view a web service, enter values in the following fields:

Table 15: Fields in the <Message Type> Screening Configuration Window

Fields	Field Description
Screening WebService	Select a screening web service from the drop-down list. This field lists all the supported matching web services in the **Transaction Filtering** application. The following web services are available: • BIC • Country and City • Goods Screening • Name and Address • Narrative or Free Text Information • Port Screening The fields for all web services except Goods Screening are as shown here. For information on the fields for Goods Screening, see Fields for Goods Web services.
Expression (ID-Name)	Select an expression identifier. When you select an expression identifier, the values are populated in the **Field** and **Field/Subfield Name** fields.
Field	Select the field name.
Field/Subfield Name	Select the subfield name. This displays the expression.
Enable	Select **Yes** to enable the web service. Select **No** to disable the web service.
Message Direction	Select INBOUND(o) and OUTBOUND(i) based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select **inbound**, else select **outbound**. If that field must be screened for both inbound and outbound, then select **ANY**.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** Add .
Update button	To update a web service, select the web service that you want to update and click **Update** Update .
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** Remove .
Enable All button	To enable all web services, click **Enable All** Enable All .
Disable All button	To disable all web services, click **Disable All** Disable All .

The fields you can use to configure the Goods web service are different from the fields you can use to configure the other web services. These fields are as shown:

Figure 35: Fields for Goods Web Services

Table 16: Fields in the Goods Web Service Window

Fields	Field Description
Expression Identifier	Select the Expression for the good.
Tag	Select the tag related to the good. Based on the tag selected, the field name is populated.
Field Name	The field name is populated based on the tag selected.
Message Direction	Select INBOUND(o) and OUTBOUND(i) based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select **inbound**, else select **outbound**. If that field must be screened for both inbound and outbound, then select **ANY**.
Enable	Select **Yes** to enable the message in a direction. Select **No** to disable the message in a direction.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** [Add].
Update button	To update a web service, select the web service that you want to update and click **Update** [Update].
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** [Remove].
Enable All button	To enable all web services, click **Enable All** [Enable All].
Disable All button	To disable all web services, click **Disable All** [Disable All].

6.3.1 Enabling or Disabling a Web Service

By default, every web service is enabled. You can change the message configuration by disabling a web service. When you do this, the selected web service is not evaluated.

To enable or disable one or more web services, replace the `[WEBSERVICE_IDS]` placeholder with the corresponding web service ID. The web services and the corresponding IDs are shown here:

Table 17: Web Services used in Transaction Filtering

Web Service	Web Service ID
Name and Address	Name and Address
BIC	BIC
Country and City	Country and City
Narrative or Free Text Information	Narrative or Free Text Information
Port Screening	Port Screening
Goods Screening	Goods Screening

To disable all the web services, replace the `[WEBSERVICE_IDS]` placeholder with 1, 2, 3, 4, 5, 6 in the following command:

```
UPDATE FSI_RT_MATCH_SERVICE SET F_ENABLED = 'N' WHERE N_WEBSERVICE_ID IN
([WEBSERVICE_IDS])
```

To enable all the web services, change **N** to **Y**.

6.3.2 Updating and Removing a Web Service

To update an existing web service, click the name of the web service. The fields are populated with the web service parameters. After you make the changes, click **Update**.

To remove an existing web service, click the name of the web service and click **Remove**.

6.3.3 Populating Data for the Trade Goods and Trade Port Web Services

Data for the Trade goods and Trade port web services are taken from a reference table. To populate data for these web services, do this:

1. In the **EDQ Director** menu, go to the **Watch List Management** project.
2. Right-click on the **Reference Data Refresh** job.
3. Click **Run**. Provide a unique run label and run profile.
4. When you run this job, the port and goods reference data are refreshed at the same time.
5. Go to the **Transaction Filtering** project.
6. Right-click on the **MAIN-Shutdown Real-time Screening** job to shut down all web services.
7. Click **Run**.
8. Right-click on the **MAIN** job to restart all web services.
9. Click **Run**.

6.4 <Message Type> Other Field/Subfield Configuration Window

This window allows you to update the other fields which you can configure in the application. It displays the list of fixed business data/names for the required fields to run the system for any given message type. You can select a business data value to mention the source for a given message type.

Figure 36: <Message Type> Other Field/Subfield Configuration Window

To update the parameter, click the parameter name. The fields are populated with the field parameters. The following fields are displayed in this window:

Table 18: Fields in the <Message Type> Other Field/Subfield Configuration Window

Fields	Field Description
Generic Business Data	This field displays the business name of the record that is selected. It is mandatory to configure this field.
	If the message contains one or more of the B, C, D, or E sequences, you must configure the field with the first tag of the sequence according to the Fedwire standard.
Message Direction	Select INBOUND(o) and OUTBOUND(i) based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select inbound, else select outbound. If that field must be screened for both inbound and outbound, then select ANY.
Expression (ID-Name)	Select an expression identifier. When you select an expression identifier, the values are populated in the Field and Field/Subfield Name fields.
Field	Select the field name.
Field/Subfield Name	Select the Subfield Name. This displays the Expression.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** Add .

Fields	Field Description
Update button	To update a web service, select the web service that you want to update and click **Update** Update .
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** Remove .

After you make the changes, click **Update**.

7   Configuring the SWIFT Message Parameters

To configure the message and screening parameters, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** home page.

2. Click **SWIFT Configuration Admin**. The **Message and Screening Configurations** tab is displayed.

Figure 37: Message and Screening Configurations Tab for SWIFT
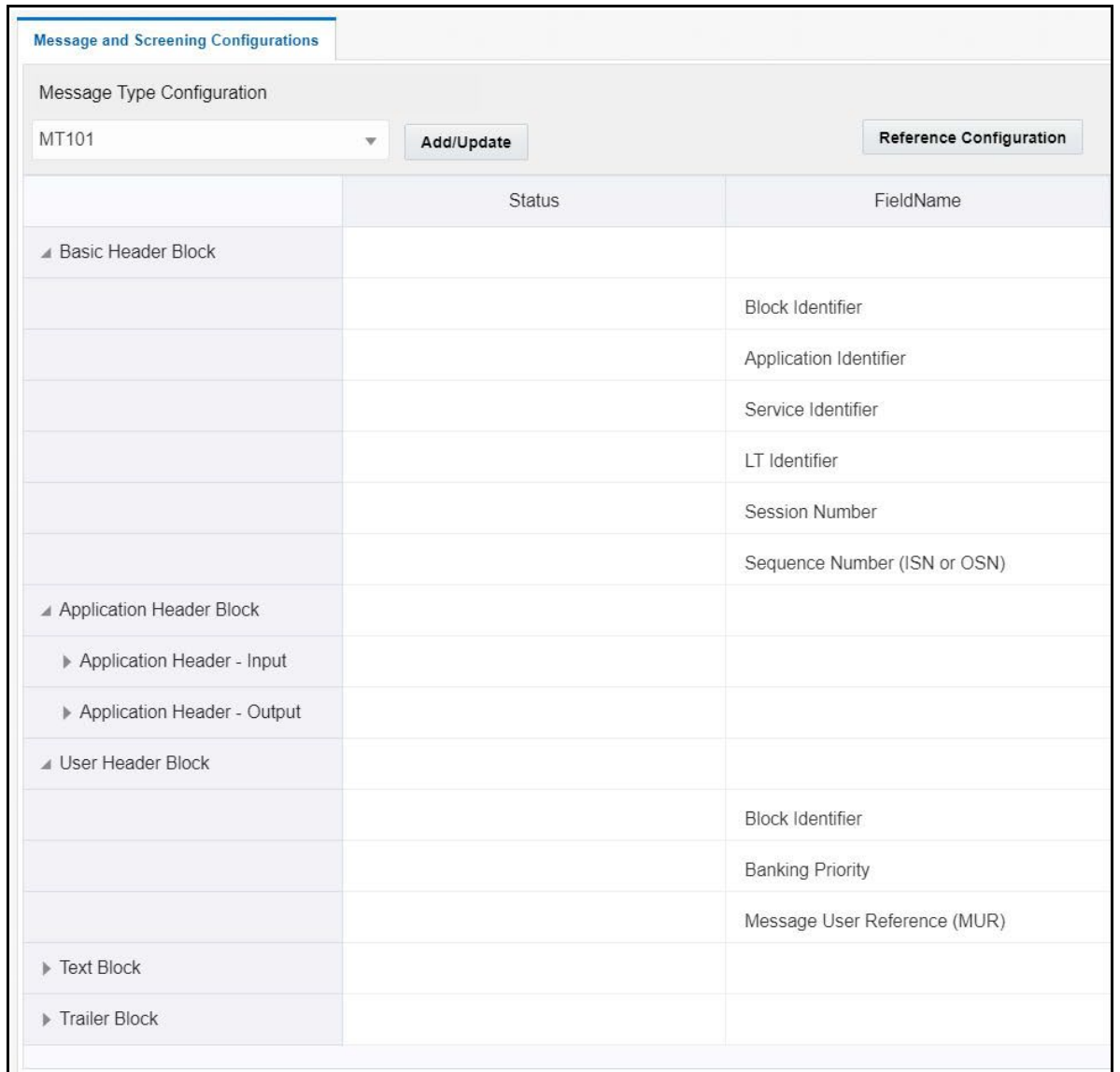
This tab has the following windows: Message Type Configuration window, <Message Type> Subfield Level Configuration Details window, <Message Type> Screening Configuration Window, and <Message Type> Other Field/Subfield Configuration Window.

7.1 Message Type Configurations Window

This window allows you to edit the status, field names, and expressions of the different JSON parameters in the message.

In the Message Type Configuration field, select the SWIFT message category. All message definitions are SWIFT 2019 compliant.

The following message types, *MTC11, MTC22, MTC33*, and *MTC44*, have been introduced for creating custom message formats, and they support UTF-8 characters. To add more custom formats, use the `dim_sanc_swift_msg_details` table. The new format must contain *MTC* and must be followed by a two-digit number.

You can also add a single line or multiple lines for Chinese characters. To add a single line, use `100k` for the expression in the configuration JSON. To add multiple lines, use `100*100k` for the expression in the configuration JSON.

Figure 38: Sample format for MTC11/MTC22/MTC33/MTC44 SWIFT message type

```
{1:F01SIIBSYDA9998525820}
{2:OC11540170801FSBKDZALAXXX1237
07812617080720718N}{4:
:20:OAC44591555/5465
:11A:参考阿斯塔
:12:Osama Bin laden
Pakistan
:13:你好
:14:印度
:15:数据
数据
数据
:16:test data
-}{5:{MAC:44544500}
{CHK:3E59F535C1E9}{PDE:}{PDE:}
```

In this example, *C11* can be either *11* or *11A* and not *111*. So, the tag can either start with two numbers or two numbers and one alphabet. The value in the *11A* tag represents `100k` in the JSON expression, and the value in the *15* tag represents `100*100k` in the JSON expression.

An example JSON is shown:

```
{
        "attr": {
          "id": "t4:2:2",
          "field": "12",
```

```
            "status": "M",

            "fieldName": "Entity Type",

            "expression": "100k",

            "regex": "",

            "editable": "Y"

        }

    },

    {

        "attr": {

            "id": "t4:2:3",

            "field": "13",

            "status": "M",

            "fieldName": "Entity Relationship",

            "expression": "100*100k",

            "regex": "",

            "editable": "Y"

        }

    },
```

Each message type has five blocks: Basic Header Block, Application Header Block, User Header Block, Text Block, and Trailer Block.

Figure 39: Message and Screening Configurations Window
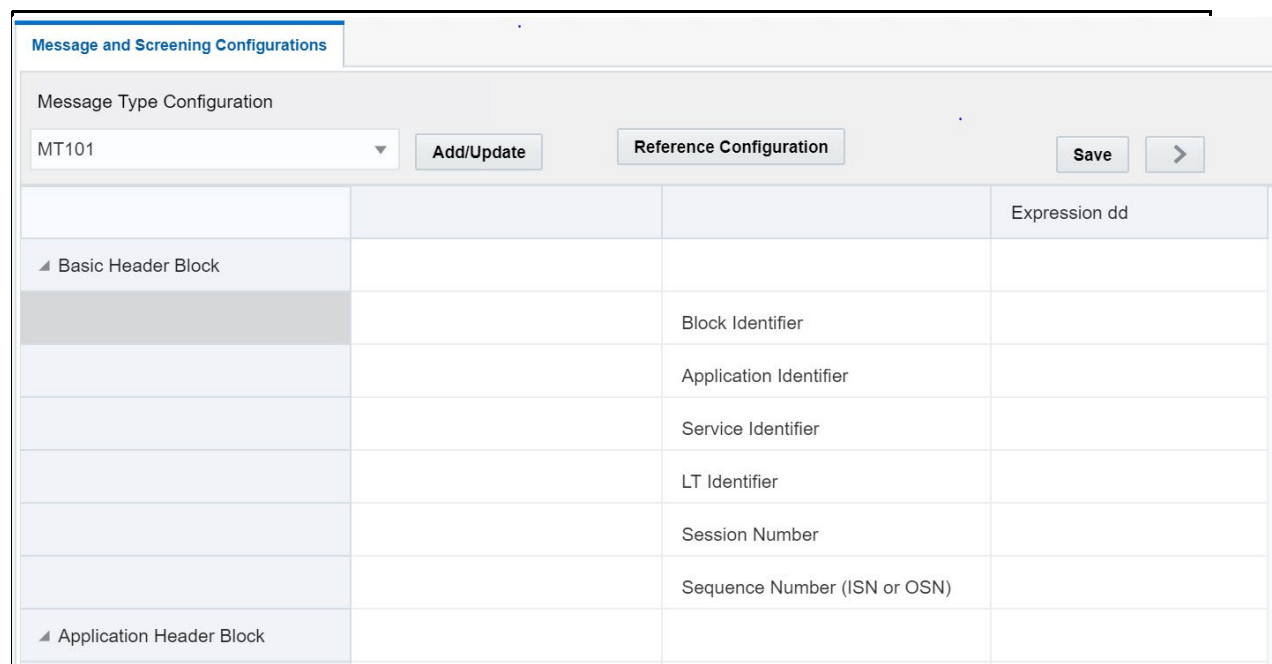
In this figure, the first column lists all the SWIFT blocks and a list of fields within each block which follows SWIFT naming standards. In this field, if a part of the sequence has multiple formats, then while uploading the JSON for the message type, update the formats within `[..]` with unique identifiers. The other columns are:

- **Status**: This column mentions whether the field is *Mandatory* (M) or *Optional* (O).

- **FieldName**: This column describes the name of the given field as per SWIFT standards.

- **Expression**: This column depicts the field structure in terms of expression. For example, if the field is a data type, then the maximum length of the field is displayed.

To edit a parameter, click the parameter name. After you make the changes, click **Save**.

7.1.1 Adding or Updating a New Message Type

To add or update an existing message type, follow these steps:

NOTE	If the SWIFT message contains sequences and the same tag repeats in both the sequences and the subsequences, then you must set the `V_REPEAT_TYPE` column to `Y` in the `dim_sanc_swift_msg_details` table before you upload a new message type. If a SWIFT message has already been uploaded, then after you set the `V_REPEAT_TYPE` column to `Y` in the `dim_sanc_swift_msg_details` table, you can click the **Save** button in the *Message Type Configuration* window.

1. Click the **Add/Update** button. The **Attachment Details** window is displayed.

2. Select the type of message that you want to add or update from the drop-down list.

Figure 40: Attachment Details Window

3. To upload an attachment, click **Choose File** [Choose File]. You can upload only one attachment at a time.

> **NOTE**   This file must be of the format `.json` or `.txt`.

4. Click **Upload**.

5. Click **Submit**. The message is displayed in the following table as *<Message Type_draft>*.

For more information, see the **JSON Upload Configuration** section in the Oracle Financial Services Transaction Filtering Technical Integration Guide.

> **NOTE**   To repeat sequences, ensure that the value in the `V_REPEAT_TYPE` column in the `dim_sanc_swift_msg_details` table is set to **Y**.

7.1.2 Configuring Message and Transaction References

Any message which contains message references or transaction references, or both, must be configured. To view and change the message reference or transaction reference, click **Reference Configuration**.

Figure 41: Reference Configuration window

For the **Message Reference** field, a unique identifier must be configured at the message level for all message categories. For the **Transaction Reference** field, a unique identifier must be configured at the transaction level only if applicable for the specific message category.

7.2 <Message Type> Subfield Level Configuration Window

This window allows you to add a subfield to a field in the **Message Type Configuration** Window.

Figure 42: <Message Type> Subfield Level Configuration Window

1. To add a subfield, provide the required values in the fields shown in the window and click **Add**
   [Add]. Enter values in the following fields:

Table 19: Fields in the <Message Type> Subfield Level Configuration Window

Fields	Field Description
Expression Identifier	Enter a unique identifier. It must begin with an alpha character and must not contain any spaces. This is a mandatory field.
Expression Name	Enter a name for the expression. The name must be in capital letters. This is a mandatory field.
Expression Description	Enter a description for the Expression. This is a mandatory field.

Fields	Field Description
Field	This field displays a complete list of fields in the drop-down for the given message type. Select the field from this drop-down field to configure the expression.
Field/Subfield Name	This field displays the respective field name or subfield options for the field that was previously selected. Select the subfield from the drop-down list.
Update button	To update an existing subfield, click the name of the subfield. After you make the changes, click **Update** Update .
Remove button	To remove an existing subfield, click the name of the subfield and click **Remove** Remove .
Clear button	To clear the data in these fields, click **Clear** Clear .

2. To update an existing subfield, click the name of the subfield. After you make the changes, click **Update**.

3. To remove an existing subfield, click the name of the subfield and click **Remove**.

4. To clear the data in these fields, click **Clear**.

You can configure the subfield in two ways:

- By configuring the **subfield level data within the option** expression: Do this if you want to configure specific data within the expression.

  For example, if `field 57` has four options `A, B, C,` and `D` in `MT103` message but you want to configure BIC (Identifier Code) from option `A`:

  ```
  Option A:
  [/1!a][/34x]          (Party Identifier)
  4!a2!a2!c[3!c]         (Identifier Code)
  ```

  You must enter the names in the **Subfield Expression Identifier**, **Subfield Name**, and **Subfield Description** fields.

- By configuring the element level data within the subfield expression: Do this if you want to further configure any data out of the subfield.

  In this example, if you want to configure the country code for `field 57,` then you can configure `2!a` from Identifier Code expression as a country code by giving unique names in the **Subfield Expression Identifier**, **Subfield Name**, and **Subfield Description** fields.

  ```
  Option A:
  [/1!a][/34x]          (Party Identifier)
  4!a 2!a 2!c[3!c]       (Identifier Code)
  ```

7.3   **<Message Type> Screening Configuration Window**

This window allows you to add, update, remove, and enable or disable a web service.

Figure 43: <Message Type> Screening Configuration Window

To view a web service, enter values in the following fields:

Table 20: Fields in the <Message Type> Screening Configuration Window

Fields	Field Description
Screening webservice	Select a screening web service from the drop-down list. This field lists all the supported matching web services in the **Transaction Filtering** application. The following web services are available: • BIC • Country and City • Goods Screening • Name and Address • Narrative or Free Text Information • Port Screening The fields for all web services except Goods Screening are as shown here. For information on the fields for Goods Screening, see Fields for Goods Web Services.
Expression (ID-Name)	Select an expression identifier. When you select an expression identifier, the values are populated in the Field and Field/Subfield Name fields.
Field	Select the field name.
Field/Subfield Name	Select the subfield name. This displays the expression.
Enable	Select **Yes** to enable the web service. Select **No** to disable the web service.

Fields	Field Description
Message Direction	Select **INBOUND(o)** and **OUTBOUND(i)** based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select **inbound**, else select **outbound**. If that field must be screened for both inbound and outbound, then select **ANY**.
Jurisdiction	Select **All** to apply the webservice for all jurisdictions or select the specific jurisdiction to apply the webservice for a specific jurisdiction. Use the `kdd_jrsdcn` table to configure the jurisdiction values. It has the following columns: • JRSDCN_CD: Values must be unique. • JRSDCN_NM: Actual jurisdiction name. • JRSDCN_DSPLY_NM: Jurisdiction name displayed in the Message and Configurations screen. • JRSDCN_DESC_TX: Optional field to add descriptions for the jurisdictions.
Business Domain	Select the applicable business domain. You can also select **All** to apply the webservice for all business domains or select **DEFAULT** to apply the webservice for the default jurisdiction. Use the `dim_kdd_bus_dmn` table to configure the business domain values. It has the following columns: • BUS_DMN_CD: Values must be unique. • BUS_DMN_DESC_TX: Optional field to add descriptions for the business domains. • BUS_DMN_DSPLY_NM: Business domain name displayed in the Message and Configurations screen. • TF_BUS_DMN_NM: Actual business domain name.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** [Add] .
Update button	To update a web service, select the web service that you want to update and click **Update** [Update] .
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** [Remove] .
Enable All button	To enable all web services, click **Enable All** [Enable All] .
Disable All button	To disable all web services, click **Disable All** [Disable All] .

The fields you can use to configure the Goods web service are different from the fields you can use to configure the other web services. These fields are as shown:

Figure 44: Fields for Goods Web Services

Table 21: Fields in the Goods Web Service Window

Fields	Field Description
Expression Identifier	Select the Expression for the good.
Tag	Select the tag related to the good. Based on the tag selected, the field name is populated.
Field Name	The field name is populated based on the tag selected.
Message Direction	Select **INBOUND(o)** and **OUTBOUND(i)** based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select **inbound**, else select **outbound**. If that field must be screened for both inbound and outbound, then select **ANY**.
Enable	Select **Yes** to enable the message in a direction. Select **No** to disable the message in a direction.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** ![Add].
Update button	To update a web service, select the web service that you want to update and click **Update** ![Update].
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** ![Remove].
Enable All button	To enable all web services, click **Enable All** ![Enable All].
Disable All button	To disable all web services, click **Disable All** ![Disable All].

7.3.1 Enabling or Disabling a Web Service

By default, every web service is enabled. You can change the message configuration by disabling a web service. When you do this, the selected web service is not evaluated.

To enable or disable one or more web services, replace the `[WEBSERVICE_IDS]` placeholder with the corresponding web service ID. The web services and the corresponding IDs are shown here:

Table 22: Web Services in Transaction Filtering

Web Service	Web Service ID
Name and Address	Name and Address
BIC	BIC
Country and City	Country and City
Narrative or Free Text Information	Narrative or Free Text Information
Port Screening	Port Screening
Goods Screening	Goods Screening

To disable all the web services, replace the `[WEBSERVICE_IDS]` placeholder with 1, 2, 3, 4, 5, 6 in the following command:

```
UPDATE FSI_RT_MATCH_SERVICE SET F_ENABLED = 'N' WHERE N_WEBSERVICE_ID IN
([WEBSERVICE_IDS])
```

To enable all the web services, change **N** to **Y**.

7.3.2 Updating and Removing a Web Service

To update an existing web service, click the name of the web service. The fields are populated with the web service parameters. After you make the changes, click **Update**.

To remove an existing web service, click the name of the web service and click **Remove**.

7.3.3 Populating Data for the Trade Goods and Trade Port Web Services

Data for the Trade goods and Trade port web services are taken from a reference table. To populate data for these web services, do this:

1. In the **EDQ Director** menu, go to the **Watch List Management** project.

2. Right-click on the **Reference Data Refresh** job.

3. Click **Run**. Provide a unique run label and run profile.

4. When you run this job, the port and goods reference data are refreshed at the same time.

5. Go to the **Transaction Filtering** project.

6. Right-click on the **MAIN-Shutdown Real-time Screening** job to shut down all web services.

7. Click **Run**.

8. Right-click on the **MAIN** job to restart all web services.

9. Click **Run**.

7.4 <Message Type> Other Field/Subfield Configuration Window

This window allows you to update the other fields which are required for the application. It displays the list of fixed business data/names for the required fields to run the system for any given message type. You can select a business data value to mention the source for a given message type.

Figure 45: <Message Type> Other Field/Subfield Configuration Window

To update the parameter, click the parameter name. The fields are populated with the field parameters. The following fields are displayed in this window :

Table 23: Fields in the <Message Type> Other Field/Subfield Configuration Window

Fields	Field Description
Generic Business Data	This field displays the Business Name of the record that is selected. It is mandatory to configure this field. If the message contains one or more of the B, C, D, or E sequences, you must configure the field with the first tag of the sequence according to the SWIFT standard.
Message Direction	Select **INBOUND(o)** and **OUTBOUND(i)** based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select **inbound**, else select **outbound**. If that field must be screened for both inbound and outbound, then select **ANY**.
Expression (ID-Name)	Select an expression identifier. When you select an expression identifier, the values are populated in the **Field** and **Field/Subfield Name** fields.
Field	Select the field name.
Field/Subfield Name	Select the Subfield Name. This displays the Expression.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** [Add].
Update button	To update a web service, select the web service that you want to update and click **Update** [Update].

Fields	Field Description
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** Remove .

After you make the changes, click **Update**.

8   Configurations for the ISO20022 Message Parameters

This chapter explains how to configure the parameters for the ISO20022 message category. The **Configuration** window allows you to view the elements associated with an `XSD` file after you upload the file. The elements are displayed in a tree structure. You must provide the transaction `XPath` before submitting the file. After the file is submitted, you can view the elements associated with a specific web service and define the `XPath` priority. This `XSD` file can be downloaded again. The **Run** page has information on the different tasks associated with the ISO20022 batch.

> | NOTE | The `XPath` of an element is the logical structure or hierarchy of the element within the `XSD` file. |
> | --- | --- |

8.1   Configuring the ISO20022 Message Parameters

To configure the ISO20022 message parameters, follow these steps:

1. On the **Financial Services Analytical Applications Transactions Filtering** home page, click **ISO20022/XML Configuration Admin**. The **Configuration** window is displayed.

Figure 46: Configuration Window - ISO20022

The Message List displays the `XSD` files associated with each message provider /scheme/message type combination. Click the link in the **Message Provider** column to view the transaction `XPaths` for the message for every screening type. You can download the `XSD` for a message by clicking

Download ![icon] in the **Download XSD** column. The `XSD` is downloaded as a zip folder; unzip the folder to view the `XSD` files.

2. To upload a new XSD file, click **Add Message**. An **Attachment Details** dialog box opens.

Figure 47: Add Message Dialog Box

3. Select the message provider and message type for the web service. If required, you can also select the message scheme. If you select a message scheme, then the message types change depending on the selected combination of the message provider and message scheme.

> | **NOTE** | The message provider, message scheme, and message type values are mapped in the `fcc_tf_xml_pro_sch_msg_map` table. |

4. To upload the parent XSD file and one or more child XSD files, click **Upload** ☐ and select the `XSD` file from your local drive. After you select the file and click **Open**, the `XSD` file name appears next to the Upload button. Select the radio button next to the primary file name and click **Upload**. A confirmation message appears, "**File uploaded successfully**." The basic elements related to the uploaded file appear in a tree view.

Figure 48: Add Message Dialog Box
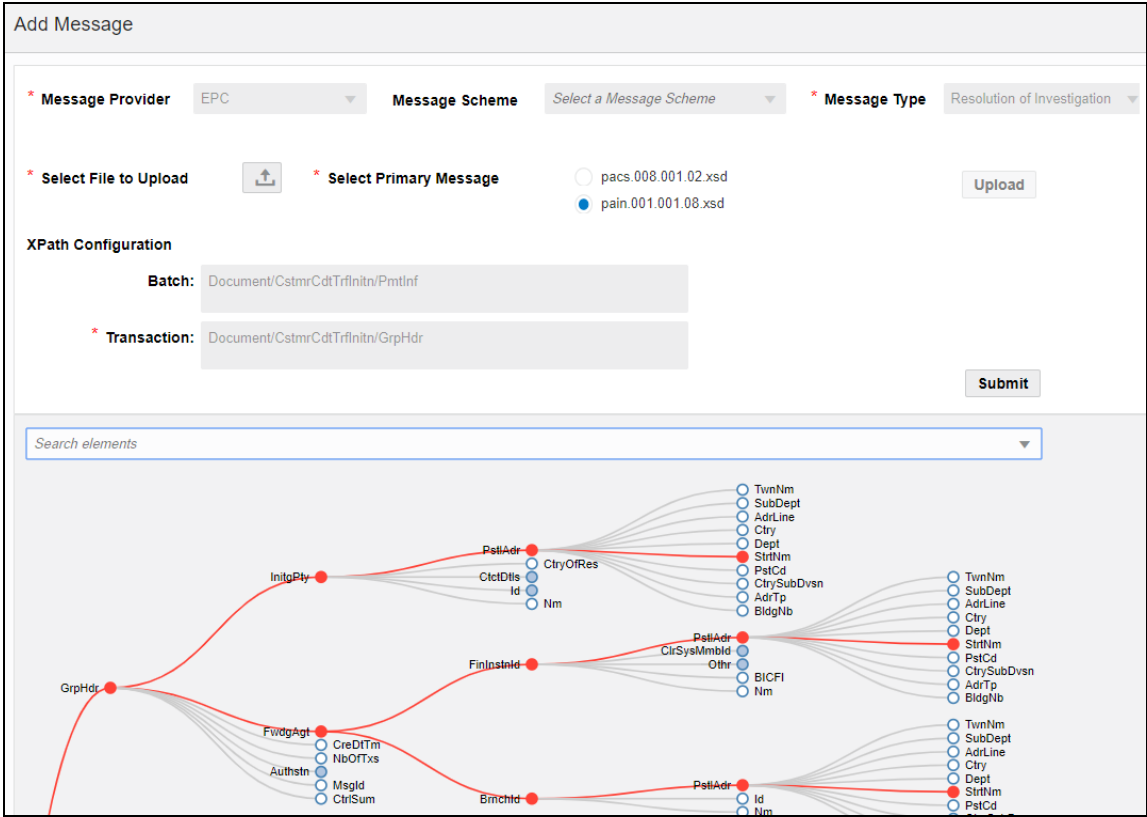
If you want to see the `XPath` of an element, select the element from the drop-down field. In the example window, the `XPath` for the `StrNm` element is highlighted in red.

To choose the `Batch XPath` or the `Transaction XPath` of the element, right-click any element node in the Tree view and click **Batch** or **Transaction** respectively. The values appear in the tree view. It is mandatory to select the **Transaction XPath Configuration** before you submit the uploaded files.

NOTE	To view the child elements for a parent element, mouse over the parent element and click the parent element in the Tree view. If **Zero** ⊙ is displayed beside the element name, it means that there are no more child elements you can drill down to.

5. Click **Submit**. The ISO20022 parameter name appears in the **Message List** section with **_Draft** attached to the parameter name.

Figure 49: Message List Window

6. To complete the configuration, click the message provider link. The **XML Screening Configuration** tab is displayed.

Figure 50: Message List Window

In this tab, you can view the details of the element `XPaths` available for the selected web service. You can also perform the following actions:

Table 24: Other Actions

To...	Do this...
Add a web service configuration	Click **Add**. The following fields appear: **Figure 51: Add a web service configuration** Select the message direction and enable or disable the web service and click **Save**. Clicking **Clear** clears any values selected. If you click **Cancel**, the fields disappear. In the Tree view, right-click any element node and click the element to view the element's `XPath`. The fields appear in the **Screening XPath Configuration List** section. **Figure 52: Add a web service configuration - tree view**
Update a web service configuration	Select the configuration you want to update and click **Update**. The fields shown in the previous row appear. Make the required changes and click **Save**. The updated values are displayed in the **Screening XPath Configuration List** section.

To...	Do this...
Remove a web service configuration	Select the configuration you want to remove and click **Remove**. The selected configuration is removed from the **Screening XPath Configuration List** section.
Enable all web service configurations	Click **Enable All**.
Disable all web service configurations	Click **Disable All**.

7. To view the message tag configurations for a field, click the **XML Message Configuration** tab.
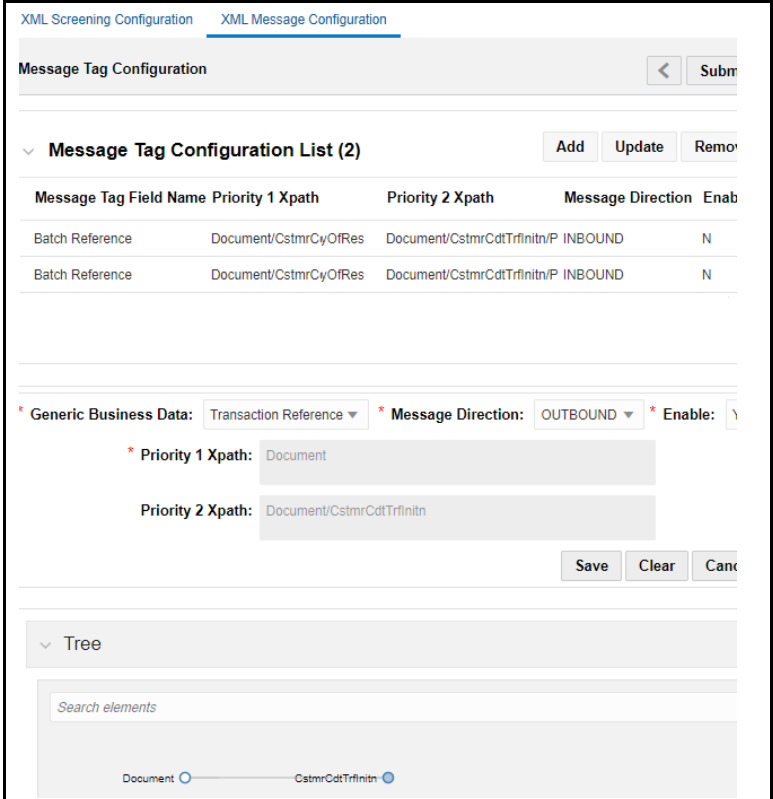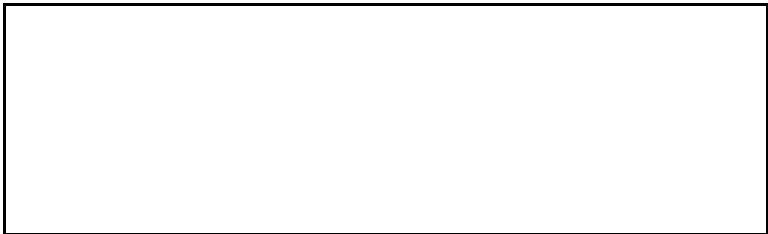
Figure 53: XML Message Configuration Tab

You can also perform the following actions:

Table 25: Other Actions

To...	Do this...
Add a message configuration	Click **Add**. The following fields appear: **Figure 54: Add a message configuration** Select the business data value, message direction, enable or disable the value, choose the **Priority 1 XPath** and **Priority 2 XPath,** and click **Save**. Clicking **Clear** clears any values selected. If you click **Cancel**, the fields disappear. In the Tree view, right-click any element node and click the element to view it's `XPath`. The fields appear in the **Message Tag Configuration List** section. **Figure 55: Add a message configuration - tree view**

To...	Do this...
Update a message configuration	Select the configuration you want to update and click **Update**. The fields shown in the previous row appear. Make the required changes and click **Save**. The updated values are displayed in the **Message Tag Configuration List** section.
Remove a message configuration	Select the configuration you want to remove and click **Remove**. The selected configuration is removed from the **Message Tag Configuration List** section.

> **NOTE** There are 53 ready-to-use business data values in the Transaction Filtering application. The business data values are available in the `DIM_TF_XML_MSG_TAG_FLD` column. You can add a new value in this column.

8. Click **Submit**. The ISO20022 parameter name is updated in the **Message List** without **_Draft**.

Figure 56: Message List Window

> **NOTE** If an earlier configuration exists with the same message version, then this configuration is disabled, and the new configuration is enabled.

8.2 Running the ISO20022 Batch

The ISO20022 messages are processed using batches. So, you must first create the following folders before you run the ISO20022 batch:

1. Create a folder for the MIS date with the folder name as `##FIC_MIS_DATE##` (the date on which we run the ISO20022 batch) in the following directory structure:

   `##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML`

   For example,
   `/scratch/fccmappchef/SANC807/ftpshare/SANCINFO/STAGE/SEPA/inputXML/2020021`
   `4`.

   `20200214` is the MIS Date folder.

2. Create two folders called `OUTBOUND` and `INBOUND` inside the MIS Date folder and create a folder called `INPUT` inside both the folders.

NOTE	All the ISO20022 XMLs must be either kept inside the `INPUT` folder inside the `OUTBOUND` folder or the `INPUT` folder inside the `INBOUND` folder based on the direction of the message XML. The ISO20022 batch takes these XMLs as input when it is run.

The directory structures for `OUTBOUND` and `INBOUND` are as follows:

`##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUTBOUND/INPUT`

`##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/INBOUND/INPUT`

For example,

- `/scratch/fccmappchef/SANC807/ftpshare/SANCINFO/STAGE/SEPA/inputXML/20200214/OUTBOUND/INPUT`

- `/scratch/fccmappchef/SANC807/ftpshare/SANCINFO/STAGE/SEPA/inputXML/20200214/INBOUND/INPUT`

After you run the ISO20022 batch, the following actions are performed:

- The `VAL_ERROR`, `PRCSNG_ERROR`, `PROCESSED`, and `FEEDBACK` folders are created as part of the batch processing.

- If any message XML fails during validation, then it is moved to the `VAL_ERROR` folder. The directory structures for `OUTBOUND` and `INBOUND` are as follows:

`##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUTBOUND/VAL_ERROR`

`##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/INBOUND/VAL_ERROR`

- If any message XML fails during the parsing process after validation, then it is moved to the `PRCSNG_ERROR` folder. The folder structures for `OUTBOUND` and `INBOUND` are as follows:

`##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUTBOUND/PRCSNG_ERROR`

`##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/INBOUND/PRCSNG_ERROR`

- If any message XML is successfully processed, then it is moved to the `PROCESSED` folder. The directory structures for `OUTBOUND` and `INBOUND` are as follows:

`##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUTBOUND/VAL_ERROR`

`##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/INBOUND/VAL_ERROR`

- After the batch is run successfully, a `##FILE_NAME##_feedback.xml` file is created for each file that is processed. The feedback is created inside the `FEEDBACK` folder. The directory structures for `OUTBOUND` and `INBOUND` are as follows:

  `##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUTBOUND/F`
  `EEDBACK`

  `##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/INBOUND/FE`
  `EDBACK`

- The logs of the batch are available in the following path:

  `##FIC_DB_HOME##/log/TF_XML`

  For example, `/scratch/fccmappchef/SANC807/SANC807/ficdb/log/TF_XML`

NOTE	When we take an action (RELEASE/BLOCK) on an alert from the Investigation User Interface, a feedback XML is recreated for the corresponding file with the name `##FILE_NAME##_feedback.xml` and the name of the previous file with the same name becomes `##FILE_NAME##_feedback_1.xml` inside the `FEEDBACK` folder. So, the `##FILE_NAME##_feedback.xml` is always the latest feedback file for a corresponding message XML.

To run the batch, follow these steps:

1. Navigate to the **Run** page. For more information, see the [Run Definition Menu](#).

   Figure 57: Run Page

2. Select the `TF_SEPA_messages_batch_process` batch and click **Fire Run**. The **Fire Run** page is displayed.

Figure 58: Fire Run Page

3. Select **Single** as the **Request Type**.

4. Select **Create & Execute** in the **Batch** field. The **MIS Date** field is displayed.

5. Select the date on which you want to execute the run. This date must be the same as the folder you create before you run the ISO20022 batch. In the example shown, since the **MIS Date** folder name is `20190913`, the date you must select is `09/13/2019`.

6. Click **OK**.

   A message "**Batch execution is in progress**" is displayed. Click **Close** to go back to the **Run** page. After the batch is executed, you can view the batch details on the **Batch Monitor** page.

   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. To run the batch, follow these steps:

   a. Select the **Batch** and the **MIS Date**. After you select the **MIS Date**, the batch ID appears in the **Batch Run ID** field.

Figure 59: Batch Monitor Page

b. Select the batch ID.

c. 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.

Figure 60: Tasks in the Batch Monitor Page

> **NOTE** If the batch run fails, you must restart the batch. In this case, the batch run ID changes.

The task details are as follows:

Table 26:Task Details

Task ID	Task Name	Task Description
Task1	TF_CallXMLParser	Parses the XML data into the pre-processing tables.
Task2	TF_CallXMLEDQ	Calls EDQ data to check if there are any matches.
Task3	Message Data Attributes	NA
Task4	TF_CallXMLRTIPopulation	Moves data from the ISO20022 configuration tables to the SWIFT configuration tables to generate OBI reports.
Task5	TF_CallXMLAlertGeneration	Creates alerts and loads data into the alert tables.
Task6	TF_CallXMLImmediateFeedbackCreation	Populates the feedback table.

Task ID	Task Name	Task Description
Task7	TF_CallXMLImmediateFeedbackFileGeneration	Generates the feedback in an XML format in the `INBOUND/feedback` directory for the date on which the run is triggered.
Task8	TF_CallXMLHighlight	Populates the highlighted column in the `fsi_rt_al_raw_data` table.
Task9	TF_CallUpdateAdditionalMsgDtls	Populates the post-processing alert table with the additional details provided for the alert.
Task10	TF_CallXMLStructuredSepa	Populates the data in the Structured Message tab in the Investigation User Interface.

8.3   Audit Queries

The following are the audit queries you can run to see the different audit operations:

Table 27:Audit Queries for ISO20022

Table Name	Query	Description
FCC_TF_XML_XSD_CONF	Select * from FCC_TF_XML_XSD_CONF_HIST	Run this query to see the history of all the actions that have been performed.
FCC_TF_XML_MSG_TAG_FLD_XPATH	Select * from FCC_TF_XML_MSG_TAG_FLD_XPATH_HIST	Run this query to see the history of all the actions performed in the **XML Message Configuration** tab.
FCC_TF_XML_SCRENG_XPATH_GRP	Select * from FCC_TF_XML_SCRENG_XPATH_GRP_HIST	Run this query to see the XPath for each parent element.
FCC_TF_XML_SCRENG_FLD_XPATH	Select * from FCC_TF_XML_SCRENG_FLD_XPATH_HIST	Run this query to see the XPath for each subfield.

9   Configurations for the US NACHA Batch Process

To configure the `TF_US_Nacha_Batch_Process` batch and to ensure successful completion, follow these steps:

1. On the **Financial Services Analytical Applications Transactions Filtering** home page, click **Financial Services Sanctions Pack**.

Figure 61: Financial Services Sanctions Pack Menu
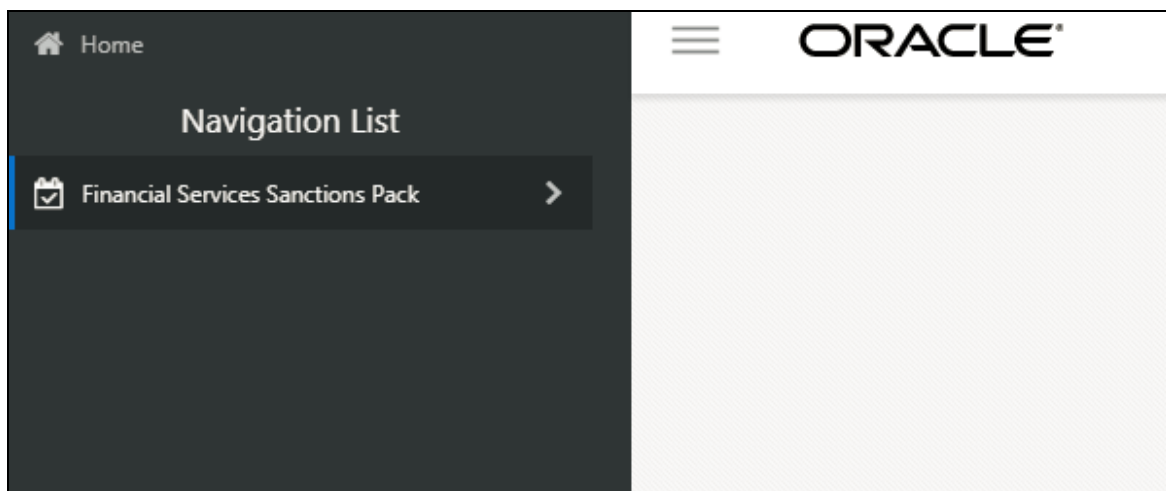
2. Click **Run Definition.** The **Run page** is displayed.

Figure 62: Run Definition Link
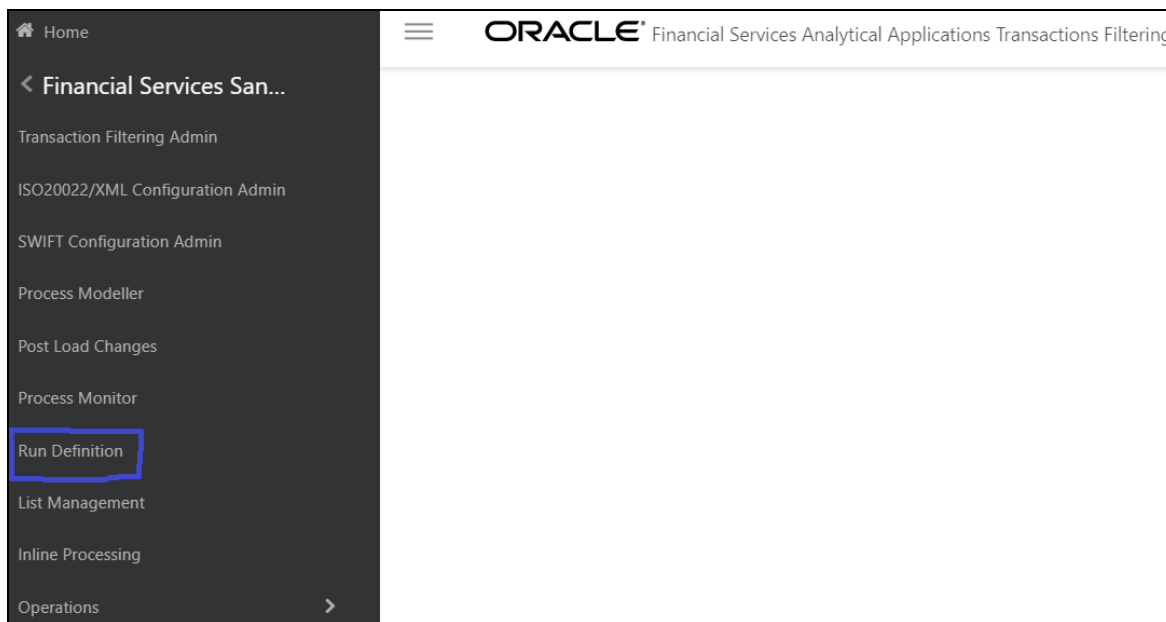
3. In the **Run** page, select the **TF_US_NACHA_Batch_Process** batch.

Figure 63: Run Page
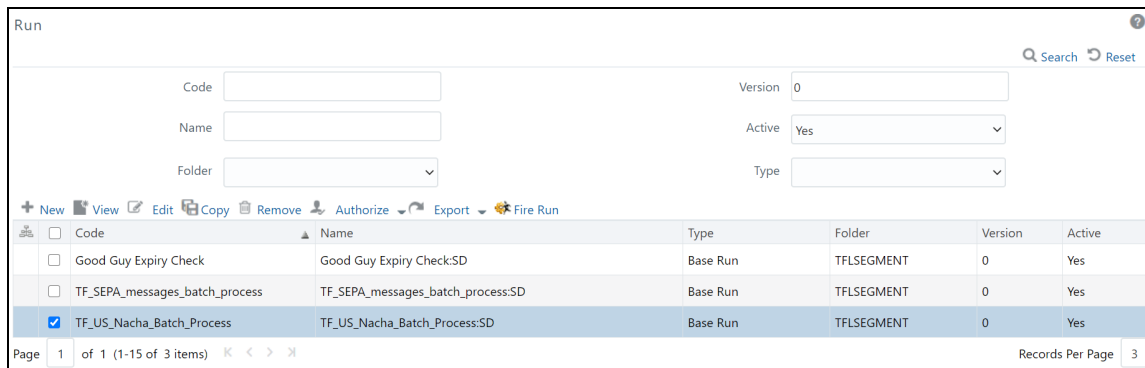
4. Click **Edit** . The **Run** page is displayed in Edit mode.

Figure 64: Run Definition (Edit Mode)
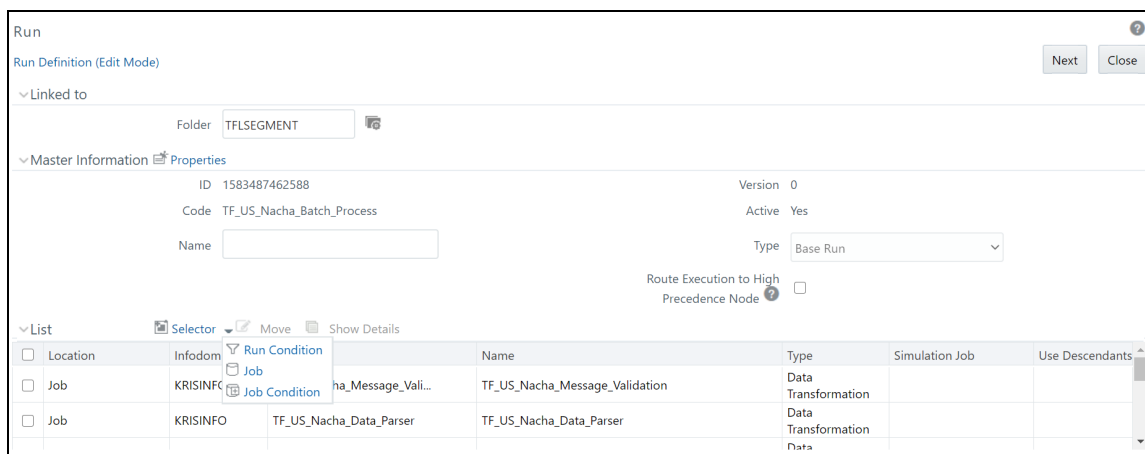
5. Click **Selector** and then click **Job** from the drop-down list. The **Component Selector** window is displayed.

Figure 65: Component Selector Window
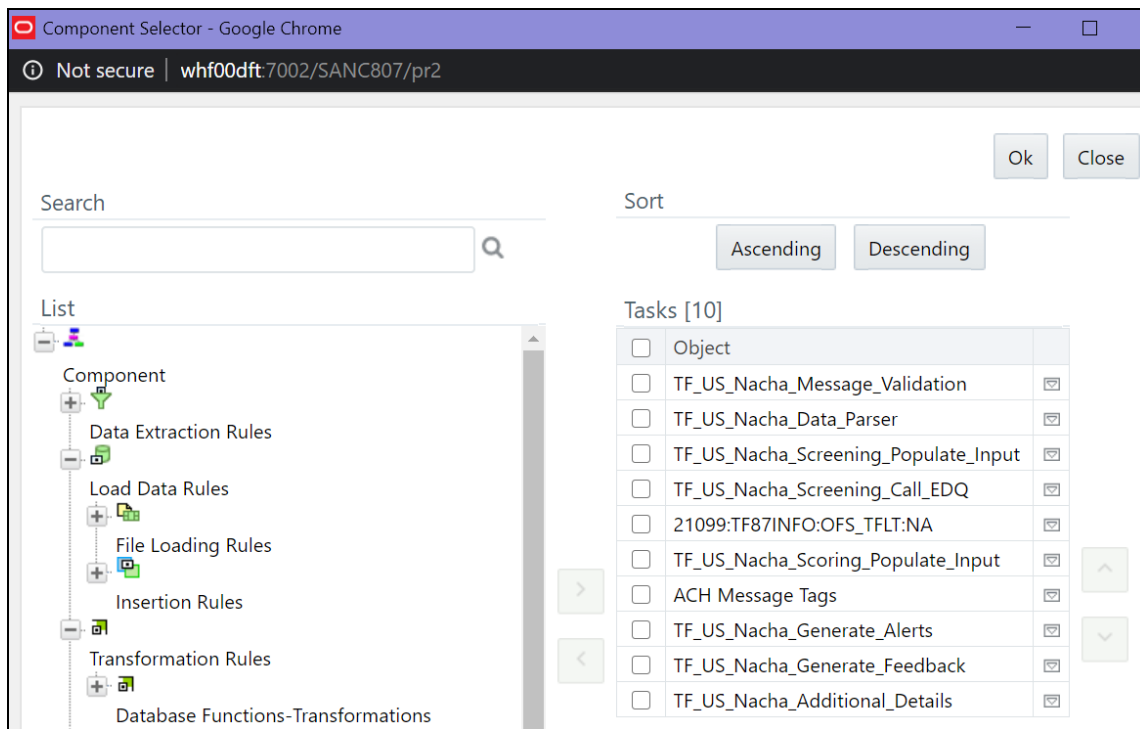
6. Deselect the `21099:TF87INFO:OFS_TFLT:NA` task.

7. Click **Ok**. The **Run** page with the **Run Definition** is displayed in Edit mode.

8. Provide a **Name** for the batch.

Figure 66: Run Definition (Edit Mode) – Batch Name
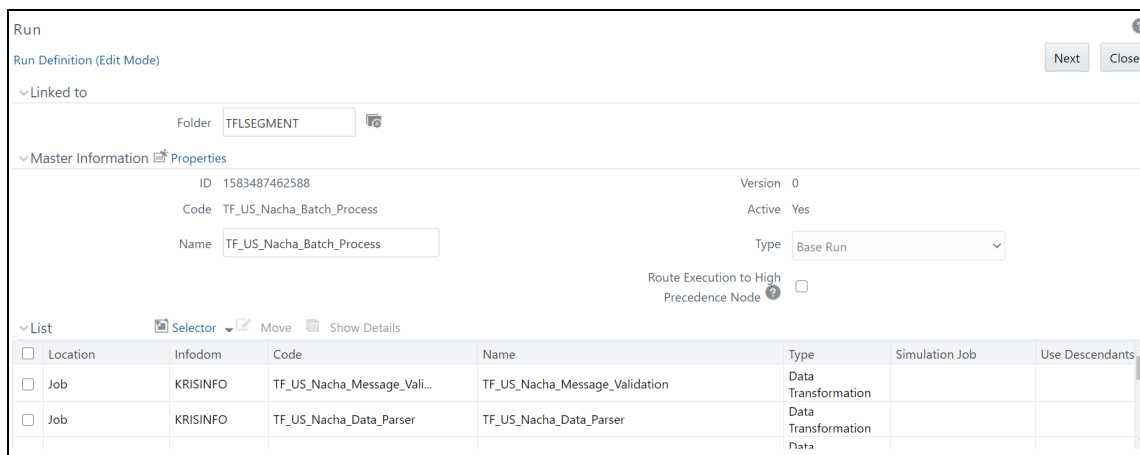
9. Click **Next**.

10. Click **Save**.

11. Click **No** in the **Run Rule Framework** dialog box.

Figure 67: Run Rule Framework Dialog Box
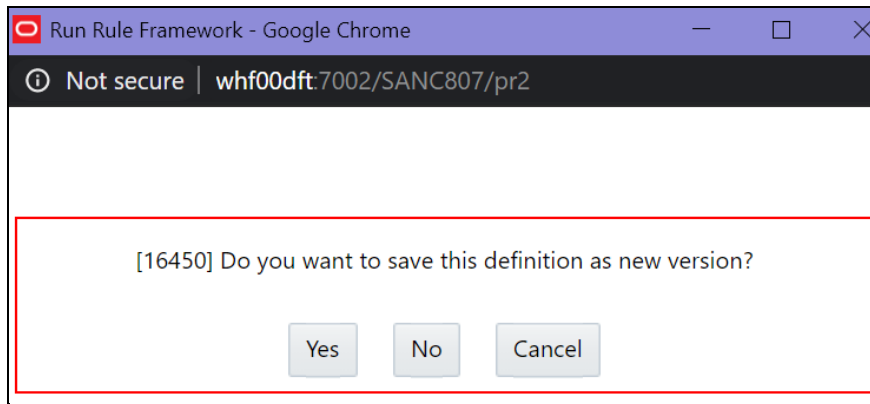
10   Enterprise Data Quality (EDQ) Configurations

The Oracle Financial Services Transactions Filtering application is built using EDQ as a platform. EDQ provides a comprehensive data quality management environment that is used to understand, improve, protect, and govern data quality. EDQ facilitates best practices such as master data management, data integration, business intelligence, and data migration initiatives. EDQ provides integrated data quality in customer relationship management and other applications.

EDQ has the following key features:

- Integrated data profiling, auditing, and cleansing and matching

- Browser-based client access

- Ability to handle all types of data (for example, customer, product, asset, financial, and operational)

- Connection to any Java Database Connectivity (JDBC) compliant data sources and targets

- Multi-user project support (Role-based access, issue tracking, process annotation, and version control)

- Representational State Transfer Architecture (REST) support for designing processes that may be exposed to external applications as a service

- Designed to process large data volumes

- A single repository to hold data along with gathered statistics and project tracking information, with shared access

- Intuitive graphical user interface designed to help you solve real-world information quality issues quickly

- Easy, data-led creation and extension of validation and transformation rules

- Fully extensible architecture allowing the insertion of any required custom processing

For more information on EDQ, see Oracle Enterprise Data Quality Documentation.

10.1   EDQ Configuration Process Flow

The following image shows the EDQ configuration process flow:
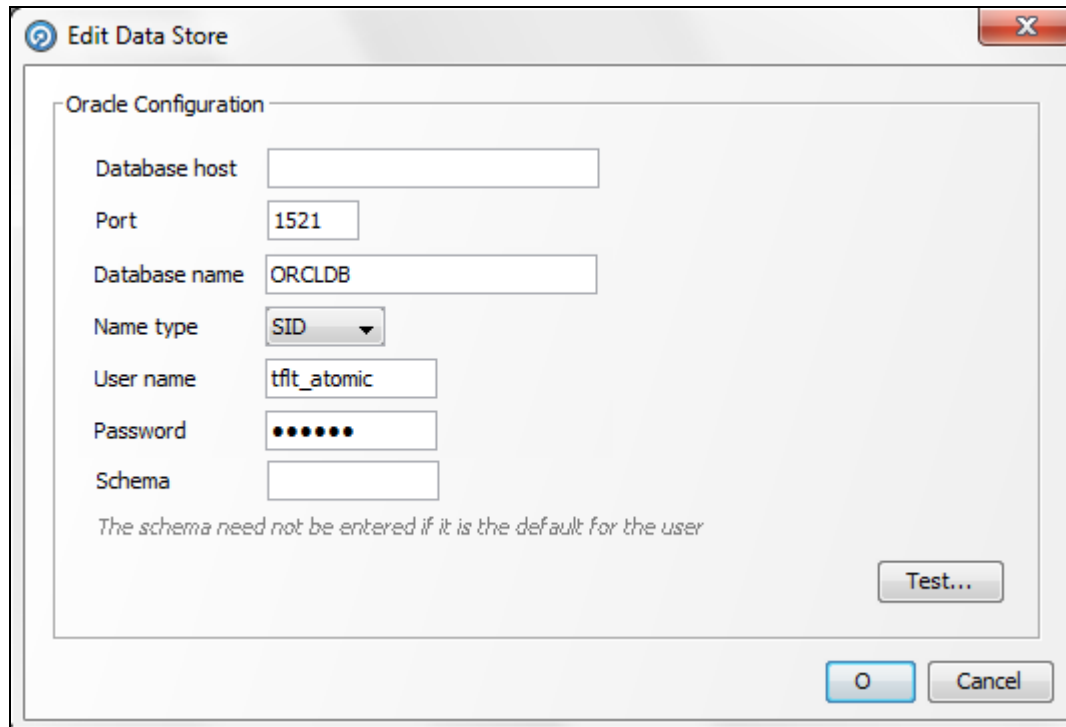
Figure 68: Enterprise Data Quality (EDQ) Configuration Steps
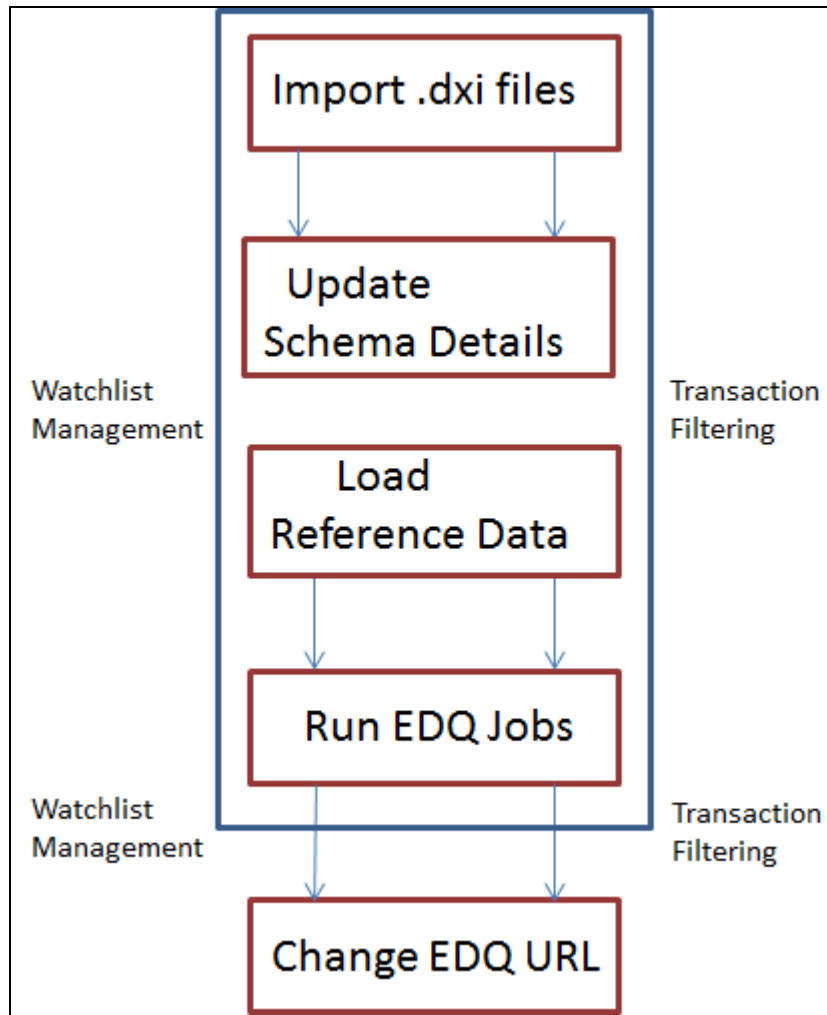
To configure EDQ, follow these steps:

1. Import the `Watchlist Management.dxi` file from the `FIC_HOME/SanctionsCommon` directory.

2. Import the `Transaction_Screening.dxi` file from the `FIC_HOME/Transaction_Processing` directory (This is for SWIFT messages only).

3. Import the `Transaction_Screening_Batch.dxi` file from the `FIC_HOME/Transaction_Processing` directory (This is for ISO20022 messages only).

4. Enter the organization-specific Atomic schema details as shown:

Figure 69: Edit Data Store Window

5. Load the Reference data. For more information on Reference data, see Viewing Reference Data for Web Services.

6. Update the command area path in the following locations:

```
Watchlist Management > External Tasks > WatchListLoadPreparedData

Transaction_Screening > External Tasks > WatchListLoadData

Transaction_Screening > External Tasks > SanctionedListRefLoadData
```

Figure 70: Edit Task Window

7. Run the following jobs under the **Watchlist Management** project:

   ▪ Analyze Reference Data Quality

   ▪ Download, Prepare, Filter and Export All Lists

   ▪ Generate StopPhrases

8. Run the **MAIN** job under the **Transaction_Screening** project.

9. Change the EDQ URL in the Transaction Filtering application. To change the EDQ URL, see Configuring the Application Level Parameters.

NOTE	The first time you set up the Transaction Filtering application, you must change the EDQ URL.

10. Configure the message and screening parameters, if required.

10.1.1 Importing the OFS Transaction Filtering Projects

For information on importing OFS Transaction Filtering projects, see the **Configuration for OFS Customer Screening and OFS Transaction Filtering** section in the Oracle Financial Services Sanctions Installation Guide.

10.1.2 Configuring Watch List Management and Transaction Filtering

The Oracle Financial Services Transaction Filtering distribution contains two run Profiles for configuring Watch List Management and screening: `watchlist-management.properties` and `watchlist-screening.properties`.

Run profiles are optional templates that specify the number of override configuration settings for externalized options when a Job is run. They offer a convenient way of saving and reusing multiple configuration overrides, rather than specifying each override as a separate argument.

Run profiles may be used when running jobs either from the Command Line Interface, using the `runopsjob` command, or in the **Server Console** User Interface.

The `watchlist-management.properties` run profile controls the following processes:

- Which watch lists are downloaded, and the configuration of the download process
- Whether filtering is applied to the watch lists or not
- Whether Data Quality Analysis is applied to the watch lists.
- Real-Time and Batch Screening set up
- Screening reference ID prefixes and suffixes
- Watch list routing
- Configuration of match rules.

> **NOTE** The properties controlling match rules are not included in the `watchlist-screening.properties` run profile by default. For more information, see Configuring Match Rules.

10.1.2.1 Preparing Watch List Data

Oracle Financial Services Transaction Filtering is pre-configured 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 Reference Data
- For information on the watch lists, see Appendix A: Watch Lists.

10.1.2.2 Setting Up Private Watch List

Oracle financial services Customer Screening is pre-configured to work with several 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 in the `privateindividuals.csv` and `privateentities.csv` files.

> **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 may differ in some cases. For example, dots or underscores may be inserted in the names, such as `oedq_local_home`.

To replace the date, follow these steps:

1. Transform your private watch list data into the format specified in the **Private List Interface** chapter in the Oracle Financial Services Data Interfaces guide.

2. Replace the data in the `privateindividuals.csv` and `privateentities.csv` files with your transformed 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 `watchlist-management.properties` Run Profile, follow these steps:

1. Move your private watch list data to the staging area by setting `phase.PRIV\ -\ Stage\ reference\ lists.enabled` to **Y**.

2. Set `phase.PRIV\ -\ Prepare\ without\ filtering.enabled` to **Y** to prepare the private watch list without filtering.

   Set `phase.PRIV\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled` and `phase.PRIV\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled` to **Y** to prepare the private watch list with filtering.

10.1.2.2.1 Showing Watch List Staged Data/Snapshots in the Server Console User Interface

Certain types of staged data and snapshots are hidden in the Server Console User Interface by default. These are:

- Watch list snapshots

- Intermediate filtered watch list staged data

- Centralized reference data staged data and snapshots

To display this data, set the corresponding visibility property value(s) in the relevant run profile to **Y**.

For example, to make all HM Treasury watch list snapshots generated during Watch List Management visible, set the following properties in the `watchlist-management.properties` run profile:

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

stageddata.ACY_All.visible = Y

stageddata.ACY_Sources.visible = Y
```

10.1.2.2.2   Configuring Match Rules

Match rules and match clusters can be configured and controlled by adding a property to the `watchlist-screening.properties` run profile.

> **NOTE** Ensure that data is available in the `ref_port_cntry` table before you begin the matching process. This table contains the port code for a port name and the corresponding port country. For more information on matching, see https://docs.oracle.com/middleware/1221/edq/user/adv_features.htm#DQUSG380.

For example, to disable the `Exact name only` rule for Batch and Real-Time Sanctions screening, add the following property to the Run Profile:

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

> **NOTE** Capitalization must be respected and characters must be escaped as required.

The `*` character denotes a wildcard and therefore specifies that the above rule applies to all phases and all processes. If disabling the rule for batch screening only, the property would read:

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

For further details on tuning match rules, see the Oracle Financial Services Transaction Filtering Matching Guide.

10.1.2.2.3   Configuring Jobs

To configure a job, it must be configured in the `properties` file and on the administration window to enable or disable the web services.

The **WatchListLoadPreparedData** process is disabled by default. To enable the process, follow these steps:

1. In the `Watchlist_Management-<patch number>` project, double-click the **Load List data from Stg to Processed table** job. All processes related to the job are displayed.

Figure 71: EDQ Director Menu
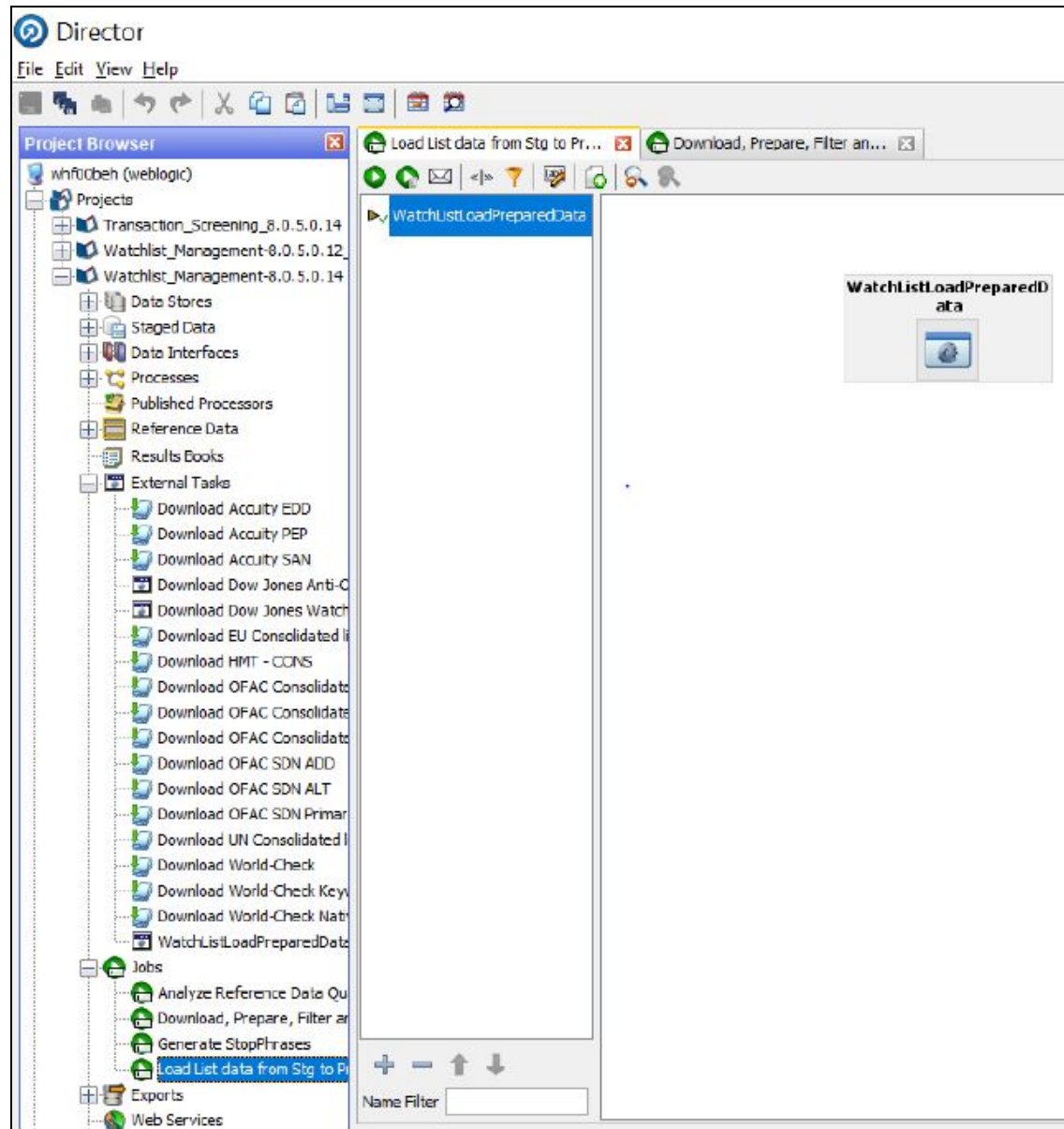
2. Right-click the **WatchListLoadPreparedData** process and click **Enable**.

10.1.2.3   Filtering Watch List Data

The following sections provide information on how to enable and configure the watch list filters.

10.1.2.3.1   Enabling Watch List Filtering

Watch list data is filtered either during List Management, Screening, or both.

To enable filtering for a specific watch list, set the `Prepare Filtering phase(s)` in the appropriate run profile to **Y**, and the `Prepare Without Filtering` phase(s) to **N**.

10.1.2.3.2   Configuring Watch List Filtering

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

NOTE	After data is filtered out, it is not possible to filter it back in. For example, if all entities are filtered out in the **Watchlist Management** project, even if the **Transaction_Screening** project is configured to include entities, they will not appear in the results data.

The top-level of filtering is controlled by editing the **Reference Data Editor - Filter - Settings** reference data.

Figure 72: Reference Data Editor - Filter - Settings Window
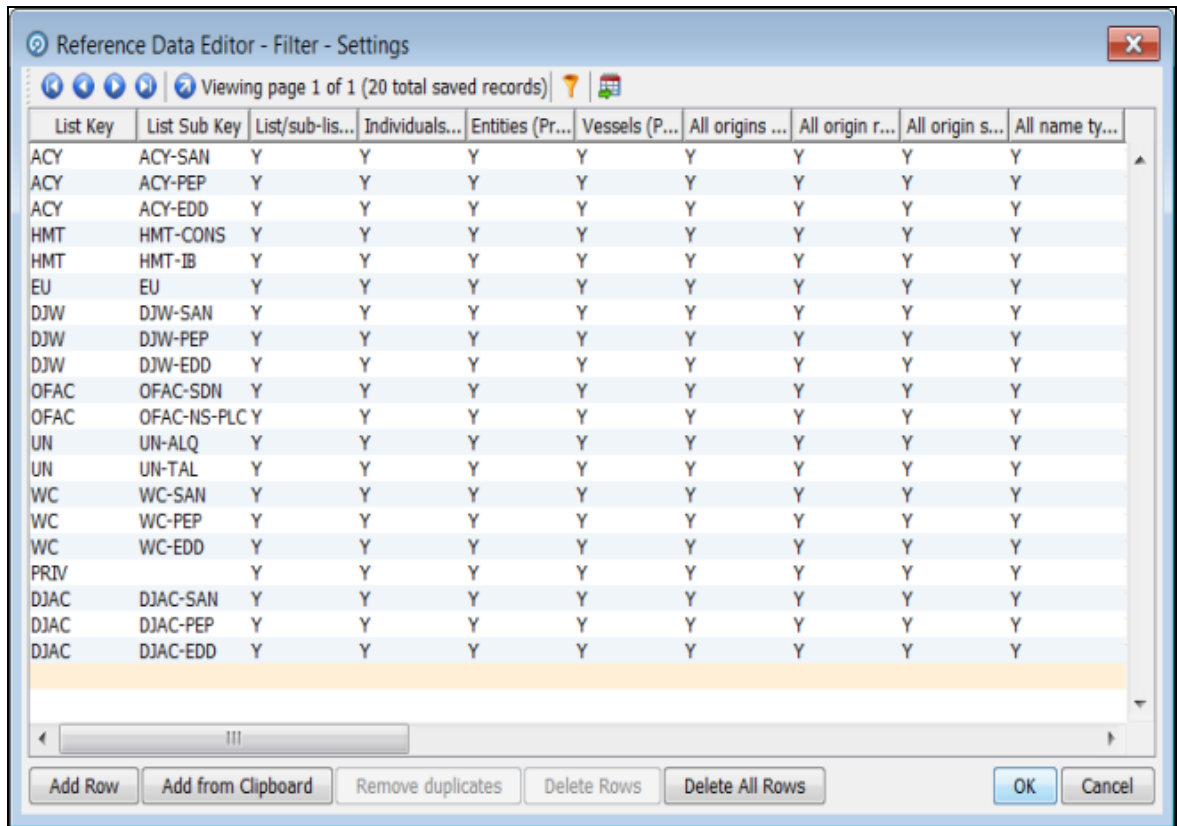
All the reference data filters are set to **Y** by default, except `Linked Profiles` which is set to **N**. No actual filtering is performed on watch list data unless these settings are changed.

NOTE	In the `Filter – Settings` reference data, a value of **Y** indicates that all records must be included - in other words, no filter must be applied.

Broadly speaking, 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.

10.1.2.3.3   Primary and Secondary Filtering, and Linked Records

- Primary filtering - These filters are used to return all profiles that match the criteria specified.

- Linked Profiles - If this value is set to **Y**, then all profiles linked to those captured by Primary filters are also captured. An example of use is a filter configured to capture all Sanctions and their related PEPs.

- Secondary filtering - These filters are applied to further filter any linked profiles that are returned.

> **NOTE**   Only the World-Check and DJW watch lists can provide Linked Profiles.

10.1.2.3.4   Setting Multiple Values for Primary and Secondary Filters

The following filter options require further configuration in additional reference data:

- Origins

- Origin Regions

- Origin Statuses

- Primary and Secondary Name Qualities

- Primary and Secondary Name Types

- Primary and Secondary PEP Classifications

To filter 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.

> **NOTE**   When you set the `Filter - Settings` reference data to **N**, only the records that match the values set in the corresponding reference data are included. For example, if you set the value of `All name qualities` to **N** in `Filter - Settings`, then you can determine which name qualities must be included for each watch list in the `Filter - Primary Name Qualities` reference data. For instance, if 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 for this watch list, then only records with high-quality names are included in the watch list.

Some of these reference data sets are pre-populated with rows, to be edited or removed as required. These rows contain data (generally, but not always) supplied by each watch list provider and are all contained within the **Watchlist Management** project.

For example, to view all possible keywords for World-Check data, open the **WC Keyword** reference data in the **Watchlist Management** project. See the following example for further details.

10.1.2.3.5   Filtering World-Check Data

This example describes configuring filtering on the World-Check Sanctions list in the **Watchlist Management** project and setting further filters in the **Transaction_Screening** project. You can also perform the following actions:

- Enable filtering in the Run Profiles

- Configure the Primary filters in the Watch List Management project to return only active records for sanctioned individuals (not entities) originating from the EU list

- Enable the filtering of Linked Profiles in the Watch List Management project

- Configure the Secondary filters in the Transaction Filtering project to further filter out all Linked Profiles of deceased individuals.

10.1.2.4   Setting Filtering options in the Run Profiles

In the `watchlist-management.properties` Run Profile, set the `World-Check filtering` phases as follows:

```
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
```

In the `watchlist-screening.properties` Run Profile, set the `World-Check filtering` phases as follows:

```
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
```

10.1.2.4.1   Setting Primary Filters and Linked Profiles in the Watchlist Management Project

To set the primary filters, follow these steps:

1. In the `Director` menu, open the `Watchlist Management` project and expand the `Reference Data` node.

2. Locate the `Filter - Settings` reference data and double-click to open it.

   Ensure the List/sub-list value in the WC-SAN row is set to **Y**.

3. Set the `Entities` value in the `WC-SAN` row to **N**.

4. Set the `Inactive` value in the `WC-SAN` row to **N**.

5. Set the `All Origins` value in the `WC-SAN` row to **N**.

   Ensure all other values in the `WC-SAN` row are set to **Y**.

6. Click **OK** to close the reference data and save changes.

7. Locate the `Filter - Origins` reference data and double-click to open it.

8. Add a new row with the following values:

   ▪ List Key - WC

   ▪ List Sub Key - WC-SAN

   ▪ Origin - EU

9. Change the `Linked Profiles` value in the `WC-SAN` row to **Y**.

10. Click **OK** to close the `Filter Settings` reference data and save changes.

10.1.2.4.2 Setting Secondary Filters in the Transaction_Screening Project

To set secondary filters, follow these steps:

1. Open the `Transaction_Screening` project, and expand the reference data link.

2. Locate the `Filter - Settings` reference data file, and double-click to open it.

3. Set the `Deceased` value in the `WC-SAN` row to **N**.

4. Click **OK** to close the reference data and save changes.

10.1.2.4.3 Screening All Data Using Sanctions Rules

By default, watch list records are routed to the different screening processes depending on their record type, that is, `SAN, PEP,` or `EDD`. This allows different rules, and hence different levels of rigor, to be applied to the list data according to risk appetite.

However, if you want to use the same screening logic for all list records, and do not want the overhead of maintaining separate rule sets, the system can be configured to reroute all list records to the SAN screening processes. To do this, set the `phase.*.process.*.Screen\ all\ as\ SAN` value in the `watchlist-screening.properties` Run Profile to **Y**.

10.1.2.5 Viewing Reference Data for Web Services

Previously, all reference data was available in EDQ. From 807 onwards, only data related to name and address is enabled in EDQ. All other reference data is available in the database in the following tables:

- Goods prohibition reference data is available in `fcc_prohibiton_goods_ref_data`

- Ports prohibition reference data is available in `fcc_port_ref_data`

- Bad BICs reference data is available in `dim_sanctioned_bic`

- Stop Keywords reference data is available in `dim_stop_keywords`

- Blacklisted Cities reference data is available in `dim_sanctioned_city`

- Blacklisted Countries reference data is available in `dim_sanctioned_country`

10.1.2.5.1 Bad BICs Reference Data

The following columns are available in the template for BICs:

- Record ID: This column displays the record serial number for the blacklisted BIC. The record ID is unique for every BIC.
- BIC: This column displays the name of the BIC.
- Details of BIC: This column displays the details of the BIC.
- Data Source: This column displays the source of the data for the BIC.
- Risk Score: This column displays the risk score for the BIC.

Sample Data for Sanctioned BICs

The following table provides examples based on BICs:

Table 28: Sample Data for Sanctioned BICs

Record ID	BIC	Data Source	Risk Score
1	SIIBSYDA	OFAC (Office of Foreign Assets Control)	85
2	FTBDKPPY	OFAC (Office of Foreign Assets Control)	90
3	DCBKKPPY	OFAC (Office of Foreign Assets Control)	85
4	ROSYRU2P	OFAC (Office of Foreign Assets Control)	90
5	INAKRU41	OFAC (Office of Foreign Assets Control)	90
6	SBBARUMM	OFAC (Office of Foreign Assets Control)	90

10.1.2.5.2   Blacklisted Cities Reference Data

The following columns are available in the template for blacklisted cities:

- Record ID: This column displays the record serial number for the blacklisted city. The record ID is unique for every city.
- Country: This column displays the name of the country of the blacklisted city.
- City: This column displays the name of the blacklisted city.
- ISO City Code: This column displays the ISO code of the blacklisted city.
- Data Source: This column displays the source of the data for the blacklisted city.
- Risk Score: This column displays the risk score for the blacklisted city.

Sample Data for Sanctioned Cities

The following table provides examples for blacklisted cities:

Table 29: Sample Data for Sanctioned Cities

Record ID	Country	City	ISO City Code	Data Source	Risk Score
1	IRAQ	ARBIL	ABL	OFAC (Office of Foreign Assets Control)	90
2	IRAQ	ABU AL FULUS	ALF	OFAC (Office of Foreign Assets Control)	90
3	IRAQ	AMARA (AL-AMARAH)	AMA	OFAC (Office of Foreign Assets Control)	85
4	IRAQ	ARAK	ARK	OFAC (Office of Foreign Assets Control)	90

10.1.2.5.3 Blacklisted Countries Reference Data

The following columns are available in the template for blacklisted countries:

- Record ID: This column displays the record serial number for the blacklisted country. The record ID is unique for every country.

- Country: This column displays the name of the blacklisted country.

- ISO Country Code: This column displays the ISO code of the blacklisted country.

- Country Synonyms: This column displays the synonyms of the blacklisted country.

- Data Source: This column displays the source of the data for the blacklisted country.

- Risk Score: This column displays the risk score for the blacklisted country.

Sample Data for Sanctioned Countries

The following table provides sample data for blacklisted countries:

Table 30: Sample Data for Sanctioned Countries

Record ID	Country	ISO Country Code	Country Synonyms	Data Source	Risk Score
1	IRAQ	IQ	IRAK, REPUBLIC OF IRAQ, AL JUMHURIYAH AL IRAQIYAH, AL IRAQ	OFAC (Office of Foreign Assets Control)	90
2	DEMOCRATIC REPUBLIC OF THE CONGO	CD	CONGO, THE DEMOCRATIC REPUBLIC OF THE	OFAC (Office of Foreign Assets Control)	90
3	AFGHANISTAN	AF	NA	ITAR (International Traffic in Arms Regulations)	85
4	ZIMBABWE	ZW	NA	ITAR (International Traffic in Arms Regulations)	90
5	CENTRAL AFRICAN REPUBLIC	CF	NA	EAR (Export Administration Regulations)	85
6	BELARUS	BY	NA	EAR (Export Administration Regulations)	80

10.1.2.5.4   Stop Keywords Reference Data

The following columns are available in the template for keywords:

- Record ID: This column displays the record serial number for the keyword.
- Stop keyword: This column displays the keyword.
- Risk Score: This column displays the risk score for the keyword.

Sample Data for Sanctioned Stop Keywords

The following table provides examples based on keywords:

Table 31: Sample Data for Sanctioned Stop Keywords

Record ID	Stop KeyWords	Risk Score
1	EXPLOSIVE	80
2	DIAMOND	90
3	TERROR	80
4	TERRORIST	85
5	ARMS	80
6	NUCLEAR	90

10.1.2.5.5   Goods Prohibition Reference Data

The following columns are available in the template for prohibited goods:

- Record ID: This column displays the record serial number for the prohibited good. The record ID is unique for every good.
- Good Code: This column displays the code of the prohibited good.
- Good Name: This column displays the name of the prohibited good.
- Good Description: This column displays the description of the prohibited good.

Sample Data for Prohibited Goods

The following table provides sample data for prohibited goods:

Table 32: Sample Data for Prohibited Goods

Record ID	Good Code	Good Name	Good Description
1	0207 43 00	Fatty livers	Fatty livers, fresh or chilled
2	0208 90 10	Ivory	CONGO, THE DEMOCRATIC REPUBLIC OF THE
3	0209 10 00	Ivory powder and waste	NA
4	3057100	Shark fins	NA
5	4302 19 40	Tiger-Cat skins	NA

10.1.2.5.6   Ports Prohibition Reference Data

The following columns are available in the template for prohibited ports:

- Record ID: This column displays the record serial number for the prohibited port. The record ID is unique for every port.

- Country: This column displays the name of the country where the prohibited port is located.
- Port Name: This column displays the name of the prohibited port.
- Port Code: This column displays the code of the prohibited port.
- Port Synonyms: This column displays the synonym of the prohibited port.

Sample Data for Prohibited Ports

The following table provides sample data for prohibited ports:

Table 33: Sample Data for Prohibited Ports

Record ID	Country	Port Name	Port Code	Port Synonyms
1	IRAN, ISLAMIC REPUBLIC OF	KHORRAMSHAHR	IR KHO	KHORRAMSHAHR Port
2	RUSSIA	Sevastopol	SMTP	Sebastopol,Port of Sevastopol
3	New Zealand	Dunedin	NZ ORR	Otago Harbour
4	New Zealand	Ravensbourne	NZ ORR	Otago Harbour

10.1.2.6   Extending Prohibition Screening

Oracle Financial Services Transaction Filtering, as delivered, allows for prohibition screening against `Nationality and Residency for Individuals` and `[country of] Operation` and `[country of] Registration for Entities`. Additional prohibition types can be added as follows:

- Create new entries in the prohibition reference data with a new Prohibition Type name, for example, "Employment Country".
- [Batch screening only] Extend the customer data preparation process to create a new attribute, for example, dnEmploymentCountryCode.
- Edit the appropriate screening process, to create the necessary match rules and clusters for the new attribute.

11   Configuring Risk Scoring Rules

This chapter provides a brief overview of configuring Risk Scoring Rules for Transaction Filtering. These rules are configured in the Inline Processing Engine (IPE). Transaction Filtering has a few ready-to-use business rules. The following steps show the pre-configured business rules and how you can create your business rules based on the requirements.

> **NOTE**   The screenshots shown for these steps are taken for existing tables. You can perform similar steps for newly added tables.

To configure rules in IPE, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** home page. For more information, see the Inline Processing Menu.

2. Click **Inline Processing**. The **Inline Processing** page is displayed.
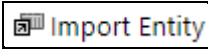
    The following window shows the **Profiles** menu. Profiles are an aggregation of information. Profiles can be based on different grouping entities (For example, account and customer) and can be filtered to only look at specific types of transactions. Profiles can also be based on time (last three months) or activity counts (last 100 transactions). For more information on Profiles, see the **Managing Profiles** chapter in the Oracle Financial Services Inline Processing Engine User Guide.

Figure 73: Profiles Menu
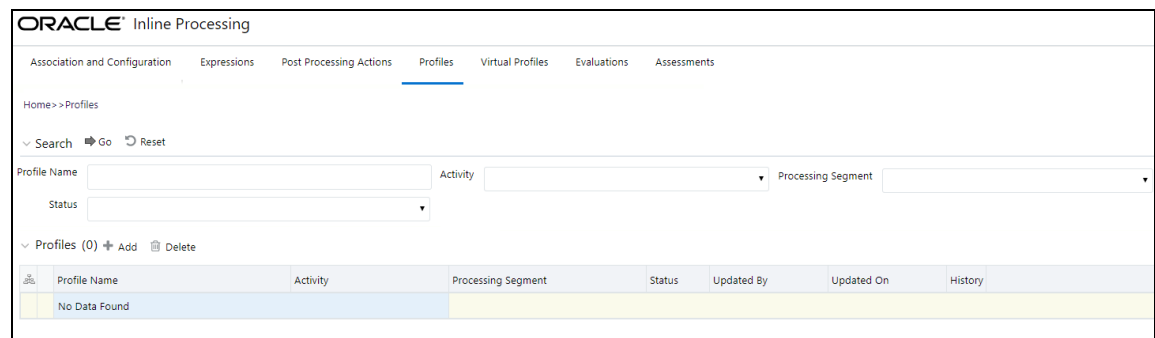
3. Import data model tables into IPE using the **Business Entities** sub-menu. A Business Entity is a virtual layer that can be added to an existing table. You can add a new business entity and search for existing business entities to modify or remove a business entity For more information on Business Entities, see the **Managing Business Entities** section in the Inline Processing Engine User Guide.

    To import a table, follow these steps:

    a. Click the **Association and Configuration** menu**,** then click the **Business Entities** sub-menu.

    b. Select the Business Entity you want to import.

    c. Click **Import Entity** [Import Entity].

Figure 74: Import Table Action

By default, all the tables defined for the entity (data model) are displayed. The Entity name is displayed in the format `<Logical Name>-<Physical Name>`.

Figure 75: Entities List

d.   Select an entity. The **Business Entity** fields are enabled. You can enter the following details:

Table 34: Business Entity Fields

Field	Description
Business Name	Enter a unique **Business Name** of the Entity. By default, the Business Name is populated as the logical name provided for the Table in the data model. The details of this field can be modified.
Entity Type	Select the **Entity Type** from the drop-down list. The following entity types are available: • **Activity**: Select a table as Activity if the data is to be processed by IPE as a part of assessment execution. To use Activity as a Reference, relevant Inline Datasets and Traversal Paths must be created. For example, if wire transactions and cash transactions are two activities, then there must be inline datasets created for them and a traversal path connecting the two. • **Reference**: Select a table as a Reference if the table has static values for IPE. Reference data cannot be processed by IPE. • **Lookup**: Select a table as Lookup if it is used as a scoring table in Evaluations. This can be used as a Reference. After a table is imported, you cannot change the entity type of the table.
Processing Segment	Select the **Processing Segment** from the multi-select drop-down list.
Set Primary Key Attribute	Select the **Primary Key Attribute** from the drop-down list. This shows all the columns of the table. This is a unique attribute of the table which is imported. It is a mandatory field. Composite Primary Keys are not supported.
Set Sequence ID Attribute	Select the sequence ID attribute from the drop-down list. Select the sequence ID attribute from the drop-down list. This field is enabled if you select **Activity** as the Entity Type.
DB Sequence Name	Enter the **DB sequence name**. A DB Sequence must be created in the Atomic Schema. The name of that Sequence must be provided in this field. This field is enabled if you select **Activity** as the Entity Type.
Set Processing Status Attribute	Select the **processing status** attribute from the drop-down list. This attribute is updated by IPE to indicate if the assessment has passed or failed. This field is enabled if you select **Activity** as the Entity Type.
Set Processing Period Attribute	Select the **processing period** attribute from the drop-down list. This attribute defines the date or time when the activity has occurred. For example, Transaction Time. This field is enabled if you select **Activity** as the Entity Type.
Score Attribute	This field is enabled ONLY if you select **Lookup** as the Entity Type. Select the **Score** Attribute from the drop-down list. This attribute can be used in evaluation scoring.

e. Click **Save**.

4. Add a business entity. To do this, follow these steps:

   a. In the **Business Entities** sub-menu, select an entity from the **Entity Name** drop-down.

   Figure 76: Entities List
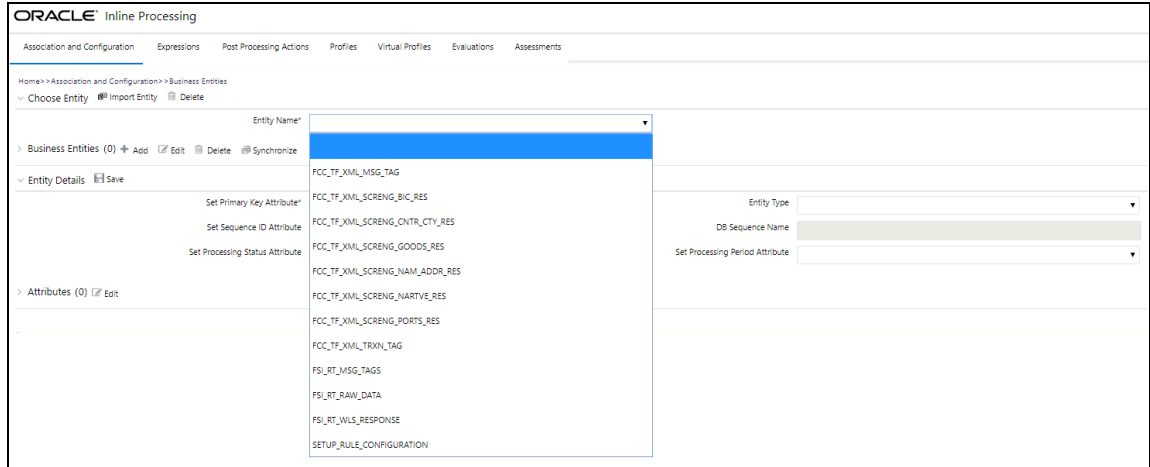
   b. Click **Add**.

5. Provide the name, processing segment, and score attribute for the business entity.

   Figure 77: Business Entity attributes

6. Click **Add**. The new parameter is added to the list of Business Entities on the **Business Entities** page.

7. Add a join in IPE from the **Inline Datasets** sub-menu in the **Association and Configuration** menu. Inline Datasets are joins between two Business Entities. When you create an Inline Dataset, you must define at least one join.

   To add a join, follow these steps:

   a. On the **Inline Datasets** page, click **Add**.

Figure 78: Inline Datasets page
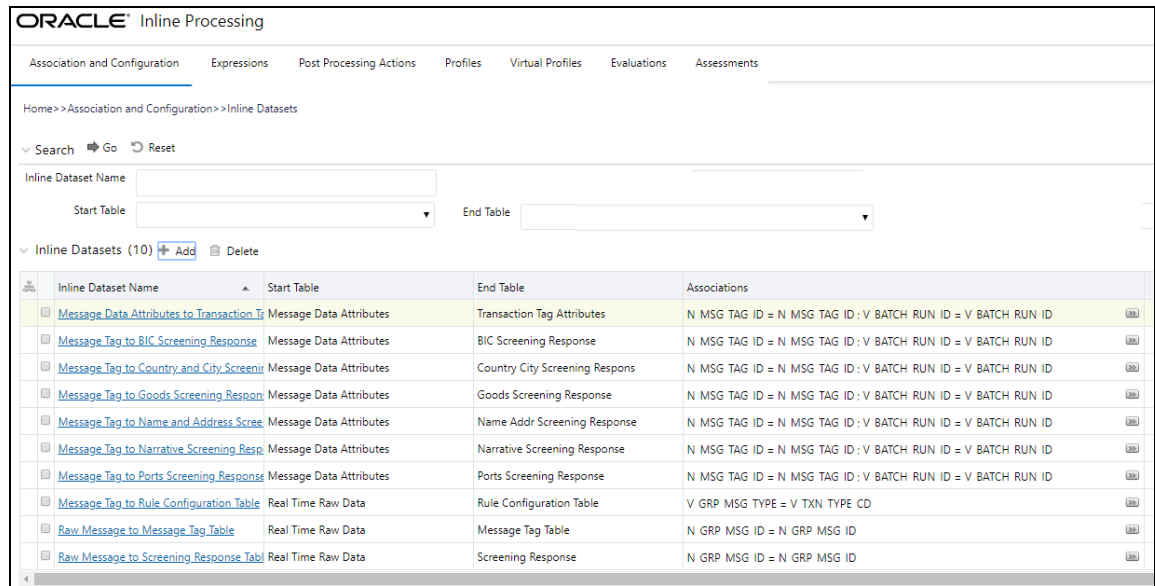
b. Enter a name for the inline dataset.

c. In the **Start Table** field, select the start table of the join.

d. In the **End Table** field, select the end table of the join.

Figure 79: Inline Datasets Attributes
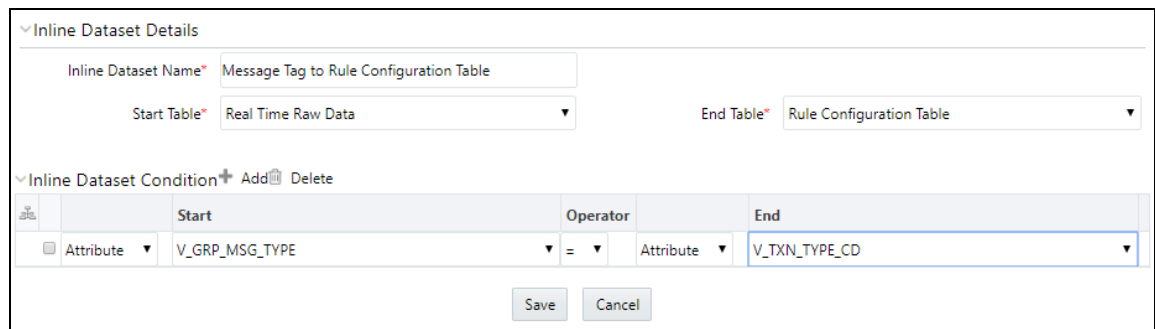
e. Click **Add**.

f. Click **Save**. The new dataset is added to the list of Inline Datasets on the **Inline Datasets** page. For more information on inline datasets, see the **Managing Inline Datasets** section in the Inline Processing Engine User Guide.

8. Add a traversal path for each join defined in the **Inline Datasets** sub-menu. Traversal paths are the paths between two or more entities. The traversal paths defined can be used to create expressions, evaluations, and profiles.

To add a traversal path, follow these steps:

a. Click the **Traversal Paths** sub-menu in the **Association and Configuration** menu.

b. On the **Traversal Paths** page, click **Add**.

Figure 80: Traversal Paths Page
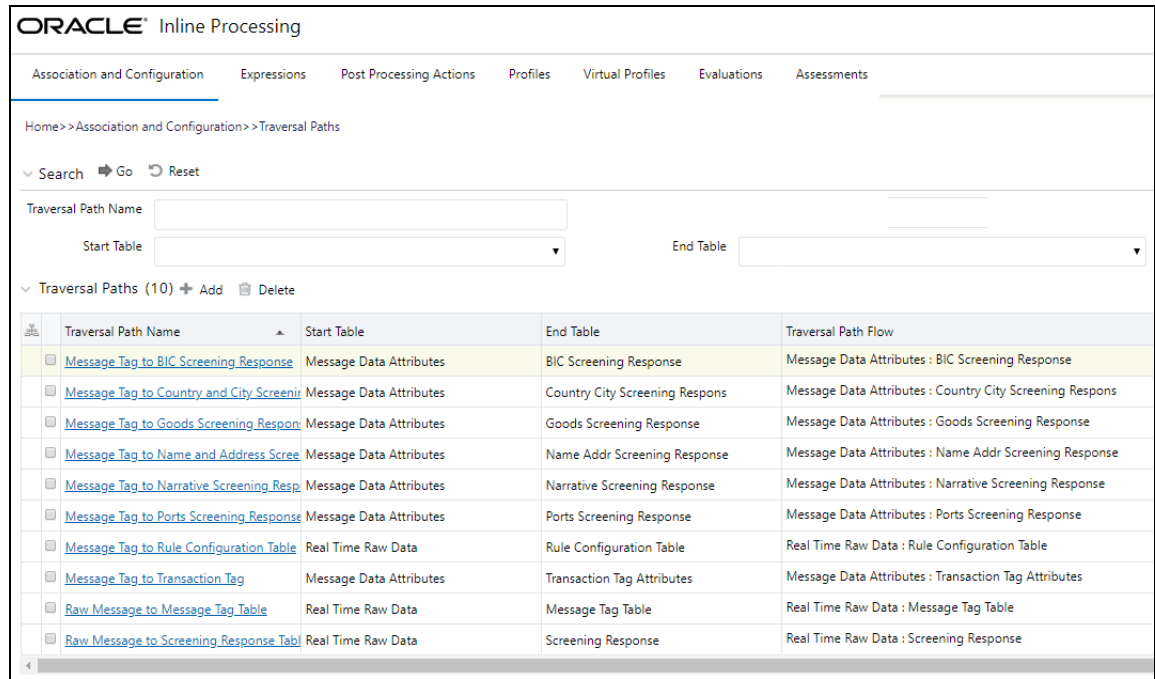
c. Enter a name for the traversal path.

d. In the **Start Table** field, select the same start table that you selected in step c.

e. In the **End Table** field, select the same end table that you selected in step d.

Figure 81: Traversal Paths Attributes
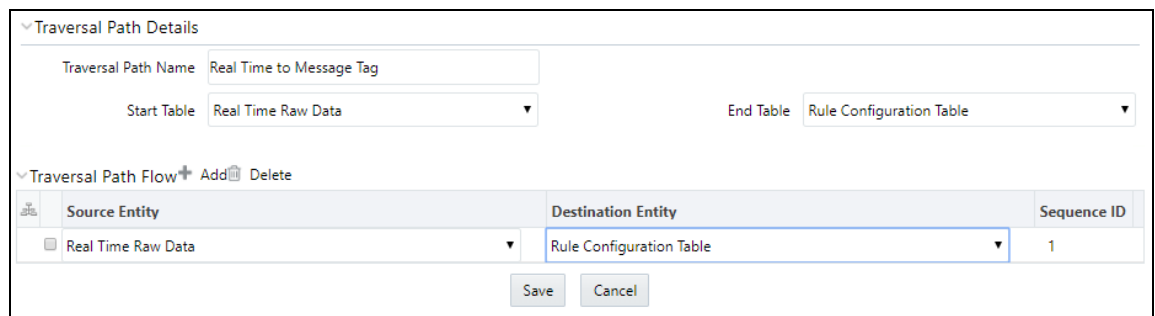
f. Click **Add**.

g. Select the values for the traversal path flow as shown in the figure.

h. Click **Save**. The new path is added to the list of traversal paths on the **Traversal Paths** page. For more information on traversal paths, see the **Managing Traversal Paths** section in the Inline Processing Engine User Guide.

9. Add an Expression on the *risk score* column of the newly created business entity which is to be scored as a risk parameter from the **Expressions** menu. An Expression is used as a filter when creating evaluations or profiles. Expressions must only be created on the activity table on which an evaluation is created.

In this example, two expressions are created. The first expression is for the column which holds the value of the new risk parameter, and the second expression is for the calculations that are needed to derive the risk score

To add an expression, follow these steps:

a. Click the **Expressions** menu.

b. On the **Expressions** page, click **Add**.

Figure 82: Expressions Page

c. For the first expression, enter a name for the expression and select the values as shown in the figure.

Figure 83: First Expression Attributes

d. Select the business entity and the business attribute where the value of the new parameter resides.

e. Click the **Save** icon. The variable is displayed on the window.

Figure 84: First Expression Displayed

f. For the second expression, enter a name for the expression and select the values as shown in the figure.

Figure 85: Second Expression Attributes

g. Click the **Save** icon. The variable is displayed.

Figure 86: Second Expression Displayed

For information on applying a function to the group or expression, see the **Managing Expressions** chapter in the Inline Processing Engine User Guide.

h. Click **Submit**. The new expression is added to the list of expressions on the **Expressions** page.

10. Add the following ready-to-use evaluations from the **Evaluations** Menu. Evaluations are logical comparisons against conditions that result in a score. For information on the conditions, see the **Managing Evaluations** section in the Inline Processing Engine User Guide.

You can define new rules according to your requirement using the expressions defined in the earlier steps.

a. **ISO20022 Risk-Currency VS Amount Threshold Evaluation**

For all filters conditions mentioned in the following table, if the filter values are met as configured then add a risk score of 20.

NOTE	• This evaluation applies to the ISO message category.
	• This score is configurable.

Table 35: ISO20022 Risk-Currency VS Amount Threshold Evaluation Filters

Sl.No	Filter Name	Filter Clause
1.	Batch ID	(Message Data Attributes:V_BATCH_RUN_ID) = BATCH RUN ID
2.	Amount	(Message Data Attributes:N_CNTRL_SUM_AMT) >= 10000
3.	Currency	(Transaction Tag Attributes:V_ CURRENCY) = 'EUR'

b. **Risk- High Risk Party Evaluation**

For all filters conditions mentioned in the following table, if the filter values are met as configured then add a risk score of 40.

Table 36: Risk- High Risk Party Evaluation Filters

Sl.No	Filter Name	Filter Clause
1.	Beneficiary Account Number	(Message Tag Table:V_BENF_ACC_NO) = (Rule Configuration Table:V_COND1)
2.	Rule Name	(Rule Configuration Table:V_RISK_RULE_CODE) = 'TF_HIGH_RSK_PARTY'
3.	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) = 'MT700'
4.	Direction	(Message Tag Table:V_DIRECTION) in (('INBOUND', 'OUTBOUND'))

c. **Risk-Currency VS Amount Threshold Evaluation**

For all filters conditions mentioned in the following table, if the filter values are met as configured then add a risk score of 25.

NOTE	This score is configurable.

Table 37: Risk-Currency VS Amount Threshold Evaluation Filters

Sl.No	Filter Name	Filter Clause
1.	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) in ('MT101', 'MT103', 'MT202COV', 'MT202')
2.	Jurisdiction	(Real Time Raw Data:V_BIC_CODE) = 'CHASUS33XXX'
3.	Direction	(Message Tag Table:V_DIRECTION) in ('INBOUND','OUTBOUND')
4.	Currency	(Message Tag Table:V_CURRENCY) = 'USD'
5.	Amount	(Message Tag Table:V_AMOUNT) >= 10000

d.   Risk-Currency VS Destination Country Evaluation

For all filters conditions mentioned in the following table, if the filter values are met as configured then add a risk score of 20.

This evaluation works with reference table `SETUP_RULE_CONFIGURATION`, which is another way of configuring evaluation or risk scoring rule. This evaluation is done using one of the lookup tables from the database. Similarly, you can add more rules using the same table where columns are generalized.

Table 38: Risk-Currency VS Destination Country Evaluation Filters

Sl.No	Filter Name	Filter Clause
1.	Currency	(Message Tag Table:V_CURRENCY) = (Rule Configuration Table:V_COND1)
2.	Destination Country	(Message Tag Table:V_DESTINATION_CNTRY) = (Rule Configuration Table:V_COND2)
3.	Direction	(Message Tag Table:V_DIRECTION) in ('INBOUND','OUTBOUND')
4.	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) = (Rule Configuration Table:V_TXN_TYPE_CD)
5.	Rule Name	(Rule Configuration Table:V_RISK_RULE_CODE) = 'TF_CCY_CTRY_RSK'

e.   Risk-High Risk Destination Country Evaluation

For all filters conditions mentioned in the following table, if the filter values are met as configured then add a risk score of 20.

NOTE	This score is configurable.

Table 39: Risk-High Risk Destination Country Evaluation Filters

Sl.No	Filter Name	Filter Clause
1.	Amount	(Message Tag Table:V_AMOUNT) >= 10000
2.	Currency	(Message Tag Table:V_CURRENCY) = 'EUR'
3.	Destination Country	(Message Tag Table:V_DESTINATION_CNTRY) in ('TH', 'PK')
4.	Direction	(Message Tag Table:V_DIRECTION) = 'OUTBOUND'
5.	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) in ('MT101', 'MT103', 'MT202COV', 'MT202')

f.   Risk-High Risk Originator Country Evaluation

For all filters conditions mentioned in the following table, if the filter values are met as configured then add a risk score of 20.

> **NOTE**   This score is configurable.

Table 40: Risk-High Risk Originator Country Evaluation Filters

Sl.No	Filter Name	Filter Clause
1.	Amount	(Message Tag Table:V_AMOUNT) >= 10000
2.	Currency	(Message Tag Table:V_CURRENCY) = 'EUR'
3.	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) in ('MT101', 'MT103', 'MT202COV', 'MT202')
4.	Direction	(Message Tag Table:V_DIRECTION) = 'INBOUND'
5.	Originator Country	(Message Tag Table:V_ORIGINATOR_CNTRY) in ('PK', 'TH')

g.   Risk-Trade Amendments Evaluation

For all filters conditions mentioned in the following table, if the filter value conditions are met as configured then add a risk score of 20.

> **NOTE**   This score is configurable.

Table 41: Risk-Trade Amendments Evaluation Filters

Sl.No	Filter Name	Filter Clause
1.	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) = 'MT707'

Sl.No	Filter Name	Filter Clause
2.	Direction	(Message Tag Table:V_DIRECTION) in (('INBOUND','OUTBOUND'))
3.	Number of Amendments	(Message Tag Table:N_NUMBER_OF_AMENDMENT) >= 5

h. Risk-WatchList Screening Evaluation

This evaluation or risk rule returns the match score generated from the matching engine. In the case of multiple matches for a given message, it returns the maximum match score. The matching rules are configured with different match scores in EDQ.

NOTE	• This evaluation applies to the SWIFT message category. • This score is configurable.

i. Watch List Score

This evaluation or risk rule watch list response score. The matching rules are configured with different match scores in EDQ.

NOTE	• This evaluation applies to the ISO message category. • This score is configurable.

Table 42: Watch List Score Filters

Sl.No	Filter Name	Filter Clause
1.	Watch List Score	(Get Max Watch List Score((Name Addr Screening Response:N_MATCH_SCORE),Goods Score,Country and City Score,BIC Score,Ports Score,Narrative Score)) > 50
2.	Batch Run ID	(Message Data Attributes:V_BATCH_RUN_ID) = :BATCH_RUN_ID

To add an evaluation, follow these steps:

a. Click the **Evaluations** menu.

b. On the **Evaluations** page, click **Add**.

Figure 87: Evaluations Page

c. Enter a name for the evaluation.

d. Select an activity for the evaluation and the **Transaction Filtering** processing segment.

Figure 88: Evaluations Attributes

e. To add a filter for the evaluation, click **Add**.

f. Select the expression as mentioned in [step f].

Figure 89: Evaluations Filters

g.   Click **Save**. The new evaluation is added to the list of evaluations on the **Evaluations** page.

11. Create an Assessment for the ready-to-use evaluations. The Assessments checks the logic of all the evaluations and consider the sum of all the Evaluations for the output score.

> | NOTE | You can adjust the risk score for any given evaluation depending on the requirement, but it must be within 40, because match rule score configuration starts with 45, and match score must always have high weightage than the individual evaluation risk score. |

The risk score is calculated at the assessment level is as follows:

- The total risk score of a message is the sum of all risk scores derived from configured evaluations or risk rules including match score.

- In the case of multiple transactions, the risk score is the sum of all risk scores derived from different evaluations across transactions.

- If the same evaluation is true for multiple transactions within a message, then the score is considered once and the maximum one is considered.

- If different evaluations are true for different transactions, then it sums up all the risk scores across transactions within a message.

To add an Assessment, follow these steps:

a.   Click the **Assessments** menu.

Figure 90: Assessments Page
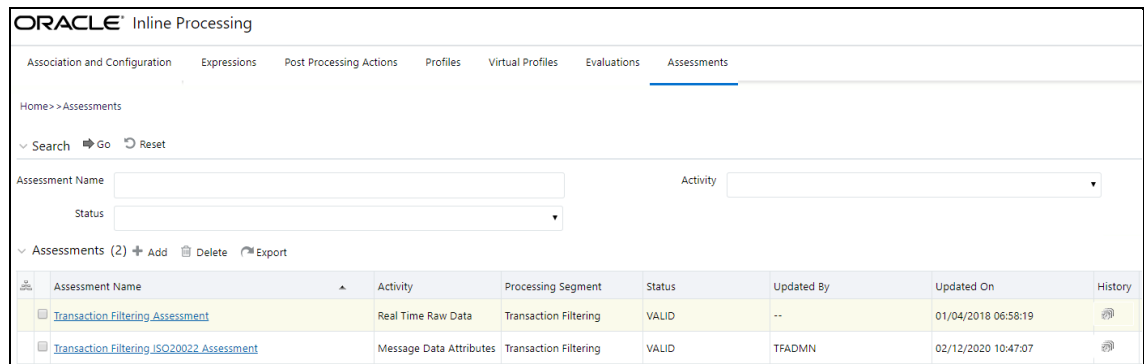
b.   On the **Assessments** page, click **Add**.

The following image shows the evaluations for the **Transaction Filtering** Assessment:

Figure 91: Assessments Attributes

The following image shows the evaluations for the **Transaction Filtering ISO20022** Assessment:

Figure 92: Sample Assessment

c. Provide the assessment name, activity, processing segment, assessment scoring method, and change description for the assessment.

d. Click **Save**. The new assessment is added to the list of assessments on the **Assessments** page. For more information on assessments, see the **Managing Assessments** section in the Inline Processing Engine User Guide.

12   Creating a JSON

Transaction Filtering allows you to add new SWIFT message types and configure the messages by uploading a JSON for a given message type followed by a few configurations using the admin UI window. A new JSON is required for each new SWIFT message type and for editing any existing message type. JSON follows SWIFT message standards given in the SWIFT document. JSON file must be `.txt` or `.json` extensions only.

This chapter provides information on how to create a JSON for SWIFT messages with sequences and SWIFT messages without sequences.

> **NOTE**   For information on how to upload a JSON, see the Adding or Updating a New Message Type section.

12.1   Structure of a JSON

The following example shows the structure of a JSON:

```
{
  "message": [
    {
      "attr": {
        "id": "t1",
        "field": "Basic Header Block",
        "status": "",
        "fieldName": "",
        "expression": "",
        "editable": "N"
      },
      "children": [
        {
          "attr": {
            "id": "t1:1",
            "field": "",
            "status": "",
            "fieldName": "Block Identifier",
            "expression": "",
            "editable": "Y",
            "size": "1"
          }
```

```
            }
        ]
    }
 ]
}
```

Each JSON must start with a *message* element. Every *message*" element is a list of *attr* elements.

Each field/tag in the JSON must be represented by *attr*. Every *attr* element in the JSON can have the following properties:

- ID: A unique value that identifies each element
- Field: Name of the element as per the Swift document, used at the parent level.
- Status: It can hold either "M" or "O" ("M" - mandatory, "O" - optional)
- FieldName: Name of the element as per the Swift document, used at child level.
- Expression: Swift expression as per the Swift document
- Editable: It can hold either "Y" or "N" ("Y" - editable in Admin UI, "N" - non-editable in Admin UI)
- Size: This property is applicable for Swift Block 1, Swift Block 2 where data is only positional, that is, there is no swift expression for the element

For example:

- The following *attr* element represents the Swift Block Name:

```
{
    "attr":
                {
                        "id":"t1",
                        "field":"Basic Header Block",
                        "status":"",
                        "fieldName":"",
                        "expression":"",
                        "editable":"N"
                }
}
```

- The following *attr* element represents the Swift Block Tag with a size property:

> **NOTE** The *expression* property must be blank for elements that are positional.

```
{
```

```
            "attr":

                      {

                            "id":"t1:1",

                            "field":"",

                            "status":"",

                            "fieldName":"Block Identifier",

                            "expression":"",

                            "editable":"Y",

                            "size":"1"

                      }

      }
```

- The following *attr* element represents the Swift Block Tag with an expression property:

```
{

    "attr":

                      {

                            "id":"t4:1:2:5:2:1",

                            "field":"",

                            "status":"",

                            "fieldName":"Party Identifier",

                            "expression":"35x",

                            "editable":"Y"

                      }

      }
```

Each *attr* element in the JSON can have one or more child attributes. Children are used as a notation to identify the children of a particular *attr* element.

```
{

  "attr": {

    "id": "t1",

    "field": "Basic Header Block",

    "status": "",

    "fieldName": "",

    "expression": "",

    "editable": "N"

  },

  "children": [
```

```
    {
      "attr": {
        "id": "t1:1",
        "field": "",
        "status": "",
        "fieldName": "Block Identifier",
        "expression": "",
        "editable": "Y",
        "size": "1"
      }
    },
    ..........
  ]
}
```

12.2 Creating JSON for SWIFT Messages with Sequences

To create a JSON, follow these steps:

1. Creating Message Elements
2. Configuring SWIFT Message Blocks

12.2.1 Creating Message Elements

To create a message element, use the following sample code:

```
{
  "message": [
  {
    Requires tags  ...
  }
  ]
}
```

12.2.2 Configuring SWIFT Message Blocks

To configure a SWIFT message block, follow these steps:

1. Configure the Basic Header Block. See Configuring the Basic Header Block.
2. Configure the Application Header Block. See Configuring the Application Header Block.
3. Configure the User Header Block. See Configuring the User Header Block.
4. Configure the Text Block. See Configuring the Text Block.

5. Configure the Trailer Block. See <u>Configuring the Trailer Block</u>.

12.2.2.1   Configuring the Basic Header Block

To configure a User Header Block, follow these steps:

1. Create an *attr* element node with `fieldName` property as the Basic Header Block and editable property as N.

2. Create a child element with the required *attr* elements that must be part of the Basic Header Block.

```
{
  "attr": {
    "id": "t1",
    "field": "Basic Header Block",
    "status": "",
    "fieldName": "",
    "expression": "",
    "editable": "N"
  },
  "children": [
    {
      "attr": {
        "id": "t1:1",
        "field": "",
        "status": "",
        "fieldName": "Block Identifier",
        "expression": "",
        "editable": "Y",
        "size": "1"
      }
    },

  ]
}
```

12.2.2.2   Configuring the Application Header Block

To configure an Application Header Block, follow these steps:

1. Create an *attr* element node with `fieldName` property as Application Header Block and editable property as **N**.

2. Create a child element with two *attr* elements with `fieldName` property as Application Header - Input and Application Header - Output and editable property as **N**.

3. Create a child element with the required *attr* elements that must be part of Application Header - Input and Application Header - Output.

```
{
  "attr": {
    "id": "t2",
    "field": "Application Header Block",
    "status": "",
    "fieldName": "",
    "expression": "",
    "editable": "N"
  },
  "children": [
    {
      "attr": {
        "id": "t2:1",
        "field": "Application Header - Input",
        "status": "",
        "fieldName": "",
        "expression": "",
        "editable": "N"
      },
      "children": [
        {
          "attr": {
            "id": "t2:1:1",
            "field": "",
            "status": "",
            "fieldName": "Block Identifier",
            "expression": "",
            "editable": "Y",
            "size": "1"
          }
        },
        ..................
      ]
    },
    {
```

```
          "attr": {
            "id": "t2:2",
            "field": "Application Header - Output",
            "status": "",
            "fieldName": "",
            "expression": "",
            "editable": "N"
          },
          "children": [
            {
              "attr": {
                "id": "t2:2:1",
                "field": "",
                "status": "",
                "fieldName": "Block Identifier",
                "expression": "",
                "editable": "Y",
                "size": "1"
              }
            },
             .................
          ]
        }
      ]
    }
```

12.2.2.3   Configuring the User Header Block

To configure a User Header Block, follow these steps:

1. Create an *attr* element node with `fieldName` property as the User Header Block and editable property as N.

2. Create a child element with the required *attr* elements that must be part of the User Header Block.

```
{
  "attr": {
    "id": "t3",
    "field": "User Header Block",
    "status": "",
    "fieldName": "",
```

```
        "expression": "",
        "editable": "N"
      },
      "children": [
        {
          "attr": {
            "id": "t3:1",
            "field": "",
            "status": "",
            "fieldName": "Block Identifier",
            "expression": "",
            "editable": "Y"
          }
        },
        ...................
      ]
    }
```

12.2.2.4   Configuring the Text Block

To configure a Text Block, follow these steps:

1. Create an *attr* element node with `fieldName` property as Text Block and editable property as **N**.

2. Create a child element with *attr* element having `fieldName` property as Sequences and editable property as **N**.

3. Create a child element with the required *attr* elements that represent individual Sequence (that is, Sequence <X>, where X can be A, B, or C) that must be part of Sequences.

```
{
  "attr": {
    "id": "t4",
    "field": "Text Block",
    "status": "",
    "fieldName": "",
    "expression": "",
    "editable": "N"
  },
  "children": [
    {
      "attr": {
        "id": "t4:1",
```

```
      "field": "Sequences",
      "status": "",
      "fieldName": "",
      "expression": "",
      "editable": "N"
    },
    "children": [
      {
        "attr": {
          "id": "t4:1:1",
          "field": "Sequence A",
          "status": "",
          "fieldName": "",
          "expression": "",
          "editable": "N"
        },
        "children": [
          {
            "attr": {
              "id": "t4:1:1:1",
              "field": "20",
              "status": "M",
              "fieldName": "Sender's Reference",
              "expression": "16x",
              "editable": "Y"
            }
          },
          ...............
        ]
      },
      {
        "attr": {
          "id": "t4:1:2",
          "field": "Sequence B",
          "status": "",
          "fieldName": "",
          "expression": "",
```

```
                              "editable": "N"
                },
                "children": [
                  {
                    "attr": {
                      "id": "t4:1:2:1",
                      "field": "21",
                      "status": "M",
                      "fieldName": "Transaction Reference",
                      "expression": "16x",
                      "editable": "Y"
                    },
                    ..............
                  }
                ]
              }
            ]
          }
        ]
      }
```

12.2.2.5   Configuring the Trailer Block

To configure the Trailer Block, follow these steps:

1. Create an *attr* element node with fieldName property as Trailer Block and editable property as **N**.

2. Create a child element with the required *attr* elements that must be part of Trailer Block.

```
{
  "attr": {
    "id": "t5",
    "field": "Trailer Block",
    "status": "",
    "fieldName": "",
    "expression": "",
    "editable": "N"
  },
  "children": [
    {
      "attr": {
```

```
      "id": "t5:1",

      "field": "CHK",

      "status": "M",

      "fieldName": "Checksum",

      "expression": "",

      "editable": "Y"

    }

  },

  ..............

  ]

}
```

12.2.3   Example of MT101 with Sequences

To see examples of MT101 with sequences, see MOS Document 2329509.1.

12.2.4   Creating a JSON for the 3xx, 5xx, and 6xx Message Types

The following sample JSONs show the JSON format for the MT3xx, MT5xx, and MT6xx message types:

12.2.4.1   Sample JSON 1

The following example contains the JSON for a message type which has the sequence displayed on the SWIFT website:

```
"attr": {

            "id": "t4:1:1",

            "field": "Sequence A",

            "status": "M",        <!--Highlighed Part---!>(Mandatory)

            "fieldName": "",

            "expression": "",

            "editable": "Y",

            "identifierTag": "16R" <!--Highlighed Part---!>(Mandatory)

                      }"children": [

            {

              "attr": {

                "id": "t4:1:1:1",

                "field": "16R",

                "status": "M",

                "fieldName": "Start of Block",

                "expression": "",
```

```
                    "editable": "Y",

                    "lov": [

                      "GENL"

                    ],


                }

              },

              {

                "attr": {

                  "id": "t4:1:1:2",

                  "field": "28E",

                  "status": "M",

                  "fieldName": "Page Number/Continuation Indicator",

                  "expression": "5n/4!c",

                  "editable": "Y",


                }

              }

                                                  ]
```

If the message contains the sequence mentioned on the SWIFT website, then you must add an identifier tag into that sequence. The identifier tag must be the tag name of the first child in that sequence. You must also provide the sequence status: if the status is Mandatory, the value must be "M", and if the status is Optional, the value must be "O".

12.2.4.2   Sample JSON 2

The following example contains the JSON for a message type which has a subsequence available under a sequence:

```
{

                "attr": {

                  "id": "t4:1:1:9",

                  "field": "Subsequence A1",

                  "status": "O",<!---Highlighted Part-----!>(Mandatory)

                  "fieldName": "",

                  "expression": "",

                  "editable": "Y",

                  "isGroup": "Y",  <!---Highlighted Part-----!>(Mandatory)

                  "isGroupIdenPresent": "Y" <!---Highlighted Part-----
!>(Mandatory)

        }
```

If a subsequence is available under a sequence, you must provide the sequence status: if the status is Mandatory, the value must be "M", and if the status is Optional, the value must be "O".

12.3 Creating JSON for SWIFT Messages without Sequences

To create a JSON, follow these steps:

1. Creating Message Elements

2. Configuring SWIFT Message Blocks

12.3.1 Creating Message Elements

To create a message element, use the following sample code:

```
{
  "message": [
  {
    Requires tags  ...
  }
  ]
}
```

12.3.2 Configuring SWIFT Message Blocks

To configure a SWIFT message block, follow these steps:

1. Configure the Basic Header Block. See Configuring the Basic Header Block.

2. Configure the Application Header Block. See Configuring the Application Header Block.

3. Configure the User Header Block. See Configuring the User Header Block.

4. Configure the Text Block. See Configuring the Text Block.

5. Configure the Trailer Block. See Configuring the Trailer Block.

12.3.2.1 Configuring the Text Block

To configure the text block, follow these steps:

1. Create an *attr* element node with `fieldName` property as Text Block and editable property as **N**.

2. Create a children element with the required *attr* elements that must be part of Text Block.

```
{
  "attr": {
    "id": "t4",
    "field": "Text Block",
    "status": "",
    "fieldName": "",
```

```
      "expression": "",
      "editable": "N"
    },
    "children": [
      {
        "attr": {
          "id": "t4:1",
          "field": "20",
          "status": "M",
          "fieldName": "Sender's Reference",
          "expression": "16x",
          "editable": "Y"
        }
      },
      ..........
    ]
}
```

12.3.3   Example of MT101 without Sequences

To see examples of MT101 with sequences, see .

12.3.4   Creating a JSON for the Nxx Message Types

The following sample JSON shows the JSON format for the N92, N95, and N96 message types:

```
{
        "attr": {
          "id": "t4:7:2",
          "field": "Additional Data",
          "status": "O",
          "fieldName": "Extra Information",
          "expression": "100*100z",
          "editable": "Y",
          "ignoreColon": "Y"
        }
    }
```

The following sample JSON shows the JSON format to add for tag 77E for the N98 message type:

```
{
```

```
            "attr": {
              "id": "t4:3",
              "field": "77E",
              "status": "",
              "fieldName": "Proprietary Message",
              "expression": "",
              "editable": "Y",
              "ignoreColon": "Y"
            },
            "children": [
              {
                "attr": {
                  "id": "t4:3:1",
                  "field": "77E",
                  "status": "M",
                  "fieldName": "",
                  "expression": "",
                  "editable": "Y",
                  "ignoreColon": "Y"
                },
                "children": [
                  {
                    "attr": {
                      "id": "t4:3:1:1",
                      "field": "",
                      "status": "",
                      "fieldName": "(Text1)",
                      "expression": "73z",
                      "editable": "Y",
                      "regex": "\\A((?<G1>[\\w|\\.|\\,|\\-
|\\(|\\)|\\/|\\=|\\'|\\+|\\:|\\?|\\!|\\\"|\\%|\\&|\\*|\\<|\\>|\\;|\\@|\\#|
]{1,73})(\\r\\n|\\n|\\r|$))"
                    }
                  },
                  {
                    "attr": {
                      "id": "t4:3:1:2",
                      "field": "",
```

```
                "status": "",
                "fieldName": "(Text2)",
                "expression": "78*78z",
                "editable": "Y",
                "regex": "\\A(?<M>((?<G1>s*[\\w|\\.|\\,|\\-
|\\(|\\))|\\/|\\=|\\'|\\+|\\:|\\?|\\!|\\\"|\\%|\\&|\\*|\\<|\\>|\\;|\\@|\\#|
]{1,78})(\\r\\n|\\n|\\r|$)){1,78})\\Z"
              }
          }
        ]
      }
    ]
  }
```

For the N98 message type, you must copy at least the mandatory fields of the original message:

```
{1:F01FSABLBBXAXXX0431806794}{2:O1952203181212BCITITMMDXXX56471423671812130747N
}{4:

:20:BILADDB25388145

:21:FEE STATEMENT

:75:00800100144503486

:32D:181217EUR1342,

:71B:/COMM/

//XXXXX ON YR CASH ACTIVITY FROM

//181101 TO 181130 AS PER OUR FEE

//STATEMENT XXXXX YOU TODAY,

//Full XXXXX XXXXXX on ISP

//Website XXXXXX to Fin.Inst.

-}{5:{MAC:44544500}{CHK:3924074D35D3}{DLM:}}{S:{SAC:}{COP:S}}
```

In the above example, the mandatory fields are:

```
:20:BILADDB25388145

:21:FEE STATEMENT

:75:00800100144503486
```

The remaining fields are optional.

12.4   Creating JSON for SWIFT messages with the List of Values (LOV) Attribute

According to SWIFT standards, if there is a tag which contains predefined codes, then we must prepare a List of Values (LOV) attribute for the SWIFT tag. The following shows a JSON with an LOV attribute:

```
{
```

```
        "attr": {
          "id": "t4:14:2:2",
          "field": "",
          "status": "",
          "fieldName": "Code",
          "expression": "14x",
          "regex": "",
          "editable": "Y",
          "lov": [
            "BY ACCEPTANCE",
            "BY DEF PAYMENT",
            "BY MIXED PYMT",
            "BY NEGOTIATION",
            "BY PAYMENT"
          ]
        }
}
```

13   Appendix A: Watch Lists

Monitoring transactions against watch lists of sanctioned individuals and companies, internal watch lists, and other commercial lists of high-risk individuals and organizations is a key compliance requirement for financial institutions worldwide. These watch lists help financial institutions identify customers who are sanctioned, live in sanctioned countries and any inbound or outbound transactions associated with these customers. The following watch lists are provided with the Transaction Filtering application:

- HM Treasury Reference Data

- OFAC Reference Data

- EU Reference Data

- UN Reference Data

- World-Check

- Dow Jones watch list

- Dow Jones Anti-Corruption List

- Accuity Reference Data

- PLI Reference Data

13.1   HM Treasury Reference Data

The HM Treasury publishes a sanctions list that can be used for screening in Transaction Filtering. The sanctions list provides a consolidated list of targets listed by the United Nations, the European Union, and the United Kingdom under legislation relating to current financial sanctions regimes.

The HM Treasury website provides more details about the list at the following location:

https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

Oracle Transaction Filtering uses the list in a semi-colon delimited form. It can be downloaded from the following location:

http://hmt-sanctions.s3.amazonaws.com/sanctionsconlist.csv

13.2   OFAC Reference Data

The US Treasury website states that 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. More details on the OFAC list can be found on the US Treasury website available at the following location:

http://www.treasury.gov/ofac/

Oracle Transaction Filtering supports two lists that are produced by OFAC. The OFAC Specially Designated Nationals (SDN) list, which is available for download in three separate parts from the following links:

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, which can be downloaded in three separate parts from the following links:

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

13.3 EU Reference Data

The European Union applies sanctions or restrictive measures in pursuit of the specific objectives of the Common Foreign and Security Policy (CFSP) as set out in Article 11 of the Treaty on 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. See the European Commission website for more details:

http://eeas.europa.eu/cfsp/sanctions/index_en.htm

To download the consolidated list:

1. Go to https://webgate.ec.europa.eu/europeaid/fsd/fsf#!/account.

2. Create an account.

3. Navigate to https://webgate.ec.europa.eu/europeaid/fsd/fsf#!/files and open show settings for crawler/robot.

4. Copy the URL for 1.0 XML (Based on XSD). This is 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.

5. Enter this URL in your run profile or download the task.

13.4 UN Reference Data

The United Nations consolidated list includes all individuals and entities subject to sanctions measures imposed by the Security Council.

Details are here:

https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

Download link is:

https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/consolidated.xml

13.5 World-Check

World-Check provides a subscription-based service, offering a consolidated list of PEPs (Politically Exposed Persons) and entities and individuals appearing on the HM Treasury, OFAC, and other world lists. Three levels of subscription are provided: Standard, Premium, and Premium+. Some features of the World-Check lists are only available to users with a higher subscription level.

To download the World-Check Premium+ feed, set values in the WC Setup section of the `watch list-management. properties` run profile as follows:

```
phase.WC\ -\ Download.enabled = Y
phase.WC\ -\ Download\ native\ aliases.enabled = Y
phase.WC\ -\ Stage\ reference\ lists.enabled = Y
phase.*.snapshot.*.use_native_aliases = 1
```

To download the Standard or Premium feeds, set values in the WC Setup section of the `watchlist-management.properties` run profile as follows:

```
phase.WC\ -\ Download.enabled = Y
phase.WC\ -\ Download\ native\ aliases.enabled = N
phase.WC\ -\ Stage\ reference\ lists.enabled = Y
phase.*.snapshot.*.use_native_aliases = 0
```

See the World-Check website for more details: https://risk.thomsonreuters.com/en/products/third-party-risk/world-check-know-your-customer.html

| **NOTE** | If your instance of Oracle Transaction Filtering uses the WebLogic application server, and you are screening against the World-Check watch list, then, to download the World-Check reference data successfully, you must add the following to the 'Server Start' arguments of your EDQ managed server: `-DUseSunHttpHandler=true`. This is only required if you are using the WebLogic application server and screening against the World-Check watch list. |

13.6   Dow Jones Watch List

Dow Jones provides a subscription-based service offering a consolidated list of PEPs (Politically Exposed Persons) and entities and individuals appearing on the various sanctions lists. See the Dow Jones website for more details:

http://www.dowjones.com/products/risk-compliance/

The Dow Jones watch list automated download task uses one of two script files that are provided with Oracle Transaction Filtering to provide further configuration of the download process. These script files are:

- `download-djw.sh` (for use on Unix platforms)
- `download-djw.bat` (for use on Windows platforms)

The script files are invoked by the automated task and will download the data files and copy them to the appropriate sub-folder of the OEDQ landing area.

13.7   Dow Jones Anti-Corruption List

Dow Jones provides a subscription-based service containing data to help you assess, investigate, and monitor third-party risk about anti-corruption compliance regulation. See the Dow Jones website for more details:

http://www.dowjones.com/products/risk-compliance/

The Dow Jones Anti-Corruption List automated download task uses one of two script files that are provided with Oracle Transaction Filtering to provide further configuration of the download process. These script files are:

- `download-djac.sh` (for use on Unix platforms)

- `download-djac.bat` (for use on Windows platforms)

The script files are invoked by the automated task and will download the data files and copy them to the appropriate sub-folder of the OEDQ landing area.

13.8   Accuity Reference Data

The Accuity Global watch list is a subscription-based service. The Accuity website states:

Accuity's proprietary collection of watch list screening databases is an aggregation of specially designated individuals and entities compiled from dozens of regulatory and enhanced due diligence lists from around the world. The global watch list provides the ideal framework for your Transaction Filtering and interdiction filtering processes.

Accuity provides its aggregated data as a set of three lists, as follows:

- The Regulatory Due Diligence (RDD) lists, covering sanctioned entities and individuals. The Accuity Group File can also be used in conjunction with this list.

- Enhanced Due Diligence (EDD) Lists, covering entities, and individuals who are not part of the regulatory sanctions lists, but whose activities may need to be monitored

- The Politically Exposed Persons (PEPs) Due Diligence Database, and covering PEPs

Any or all the lists can be downloaded and used separately or in conjunction with each other.

For more information, see http://www.accuity.com/compliance/.

13.8.1   Using the Accuity Group File

The Accuity Global watch list is created by aggregating many other lists. As such, any given individual or entity may be represented in the list by multiple entries.

The group file, GROUP.XML, provides a way to work with a data set of this type in Transaction Filtering. All records which represent the same individual or entity are collected into groups, and each group is assigned a unique group ID. The group ID is used with a prefix to indicate the fact that this is a group ID, in place of the original record identifier in Case Management. Records that are not included in a group use their original Accuity record ID, with a different prefix to indicate that they are single records.

| NOTE | The group file only applies to Transaction Filtering. That is, only entities and individuals on the Regulatory Due Diligence (RDD) Lists are included in the group file. |

The group file allows case generation to be centered around real-world individuals, rather than separate watch list records. Groups are used by default. To change this, open **Accuity Data Store** in the **Watch List Management** project and deselect the **Use groups** option.

Figure 93: Edit Data Store Window
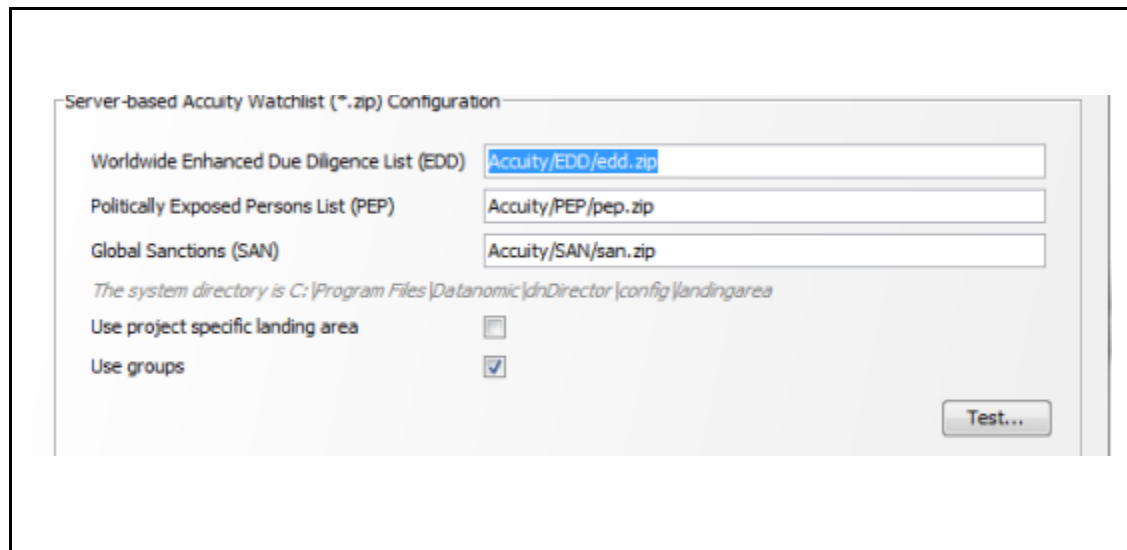
If you choose to use the group file but it is not present in your downloaded data, an error is generated.

13.8.2   New Alerts Resulting from Use of the Group File

Using the group file causes the original list ID for an entry to be replaced with the appropriate group ID. The list ID is used in the alert key, so changes to the list ID will result in new alerts being raised for existing, known relationships. There are two main scenarios in which this may occur:

Individuals or entities are moved into, out of, or between groups by Accuity, new alerts are generated for existing relationships.

| NOTE | Use of the group file may result in new alerts being raised for existing relationships if the group file structure is changed by Accuity. There is at present no way to circumvent this issue. |

The Use Groups setting is changed after cases and alerts have already been generated. The setting for the Use Groups option must be selected during the implementation phase of the project. After screening has started, it must not be changed unless necessary. Changing this setting is likely to result in duplication of existing alerts with a new alert ID.

13.9 PLI Reference Data

This section describes the structure of the `.csv` files used in the Private List Interface (PLI).

Private watch list data are provided in two `.csv` (comma-separated value) files; `privateindividuals.csv` and `privateentities.csv`. These files come with a pre-defined structure and set of validation rules. On installation, these files are populated with sample private watch list data, which must be replaced with your data, once it has been transformed into the required format.

NOTE	• It is recommended that you keep a copy of the sample private watch list files, as they can be used to verify the correct functioning of your installation on a known data set.
	• The files must be saved in UTF-8 format.

Three types of attributes are used in the PLI for screening:

Mandatory attributes: These attributes are tagged in the PLI tables with the *[Mandatory attribute]* tag and are mandatory for screening.

Recommended attributes: These attributes are used in matching, typically to either eliminate false positive matches that may occur if the mandatory fields alone were used or to reinforce the likelihood of a possible match. They are tagged in the PLI tables with the *[Recommended attribute]* tag.

Optional attributes: These attributes are not used in matching. Information provided in these fields may be of use in processes downstream of the match process.

13.9.1 Individual Private Watch List Input Attributes

This section lists the PLI fields used for individuals. In addition to the prescribed fields, fifty customizable input attributes are available for individual private watch lists, out of which forty are string attributes, five are date attributes and five are number attributes. They are available for any additional inputs required by your private watch list.

The following table lists the individual PLI fields in order, the data format expected for each field, and notes on their use in screening:

Table 43: Individual Private Watch List Input Attributes

Field Name	Expected Data Format	Notes
ListSubKey	String	This field is used to identify the source list of the watch list record (for example, Private List, Accounting Private List, Financial Private List, and so on). It is included in the alert key.
ListRecordType	String	NA

Field Name	Expected Data Format	Notes
ListRecordOrigin	String	This field is used to record the provenance of a record when it is part of a consolidated list.
ListRecordId	String	*[Mandatory attribute]* This attribute is not used as part of the matching process, but it must be populated with a unique identifier.
PassportNumber	String	This is an optional field that may be used to capture the passport numbers of customers or individuals for use in the review process. Passport numbers are not used in the default screening rules.
NationalId	String	This is an optional field that may be used to capture customer National IDs which are known for use in the review process. The National IDs of customers and individuals must not use in the default screening rules.
Title	String	This field must contain the titles of customers or individuals (such as Mr/Mrs/Dr/Herr/Monsieur). It is used to derive gender values where gender is not already stated and is used during the review process. Avoid putting titles in the name fields.
FullName	String	*[Mandatory attribute]* The individual matching process is based primarily on the name supplied for the individual. Either a full name, a pair of given and family names, or an original script name must be submitted to the screening process for screening to proceed.
GivenName	String	
FamilyName	String	
NameType	String	This is an optional field used in the review process only. Multiple names may exist for the same person. The Name Type, therefore, denotes if the name is the primary name of the listed party, or an additional name (such as an Alias, or Alternate Spelling). If two Private list records were derived from a single source with multiple names (such as Mrs. Louise Wilson née Hammond being split into two records, Louise Wilson and Louise Hammond) you may wish to denote one as the primary name and one as a maiden or alias name.

Field Name	Expected Data Format	Notes
NameQuality	String	This field may be assigned a value of *Low*, *Medium,* or *High* to indicate the quality of the individual name. High is used for Primary names and specified good/high-quality aliases.
PrimaryName	String	For alias records, this field indicates the main name for that record.
OriginalScriptName	String	*[Mandatory attribute]* The individual matching process is based primarily on the name supplied for the individual. Either a full name, a pair of given and family names, or an original script name must be submitted to the screening process for screening to proceed. If you populate the Original Script Name, then you will also need to enable two facets of Match processor configuration that are disabled by default: the Original Script Name Cluster and some or all of the Match Rules that include Original script name in their name. To adapt the Match Processor configuration, you will need to open the Transaction screening project within the Director user interface and make the changes to every process used during the Transaction Filtering installation.
Gender	String	The value supplied must be either 'M' or 'F'. The gender is not used directly in the matching process, but optionally, the value of the Gender field can be used by the elimination rules to eliminate poor matches.
Occupation	String	This is an optional field that may be used to eliminate records with "safe" occupations, in the review process and risk scoring. Note that customer occupations are not matched against list occupations using the default screening rules.
DateofBirth	String, representing a date, in the format 'YYYYMMDD'; day, month, and year are required.	*[Recommended attribute]* Birth date information can be used in matching to identify particularly strong matches or to eliminate matches that are too weak.
YearofBirth	String, in the format 'YYYY'.	NA
Deceased Flag	String	If populated, this optional field must contain either **Y** or **N**.

Field Name	Expected Data Format	Notes
DeceasedDate	String, representing a date, in the format 'YYYYMMDD'.	If populated, this optional field must contain either the current date or a date in the past.
Address1	String	These are optional fields that may be used in the review process.
Address2	String	
Address3	String	
Address4	String	
City	String	*[Recommended attribute]* City data is used to strengthen potential match information.
State	String	
Postal Code	String	
AddressCountryCode	String; ISO 2-character country code.	*[Recommended attribute]* Address country data is used to strengthen potential match information.
ResidencyCountryCode	String; ISO 2-character country code.	*[Recommended attribute]* The country of residence can be used in optional country prohibition screening.
CountryOfBirthCode	String; ISO 2-character country code.	NA
NationalityCountryCodes	String; comma separated list of ISO 2-character country codes.	*[Recommended attribute]* The nationality can be used in optional country prohibition screening.
ProfileHyperlink	String; a hyperlink to an Internet or intranet resource for the record.	This field may contain a hyperlink to an Internet or intranet resource that can provide reviewers with additional information about the individual.
RiskScore	Number, between 0 and 100	This field is included where the risk score for a customer is calculated externally.
RiskScorePEP	Number, between 0 and 100	A number indicating the relative 'riskiness' of the Individual, considered as a PEP. The risk score is expressed as an integer between 1 and 100, with Higher numbers indicating a higher risk.
AddedDate	String, representing a date, in the format 'YYYYMMDD'	These are optional fields for use in the review process.
LastUpdatedDate	String, representing a date, in the format 'YYYYMMDD'	

Field Name	Expected Data Format	Notes
DataConfidenceScore	Number, between 0 and 100	
DataConfidenceComment	String	
InactiveFlag	String	If populated, this optional field must contain either **Y** or **N.**
InactiveSinceDate	String, representing a date, in the format 'YYYYMMDD'	If populated, this optional field must contain either the current date or a date in the past.
PEPclassification	String	This field can be used to indicate the type of PEP (for example, whether the individual is part of an international organization or government, and at what level). It can be used to filter watch list records and is primarily used by the World-Check watch list, but could be used by a private watch list if required.
customString1 to customString40	String	Fifty custom fields are provided in the private list data interface for individuals. Forty of these are intended to hold string data, five hold dates, and five numeric data.
customDate1 to customDate5		
customNumber1 to customNumber5		The interface file is a comma-separated value (`.csv`) file, and so all fields intrinsically contain strings. However, during the processing of Private watch lists, the custom date and number fields are checked to ensure that they include appropriate data, and warning messages are provided as output if they do not.

13.9.2   Entity Private Watch List Input (PLI) Attributes

This section lists the PLI fields used for entities. In addition to the prescribed fields, fifty customizable input attributes are available for individual private watch lists, out of which forty are string attributes, five are date attributes and five are number attributes. They are available for any additional inputs required by your private watch list.

The following table lists the individual PLI fields in order, the data format expected for each field, and notes on their use in screening:

Table 44: Entity Private Watch List Input Attributes

Field Name	Expected Data Format	Notes
ListSubKey	String	This field is used to identify the source list of the watch list record (for example, Private List, Accounting Private List, Financial Private List, and so on). It is included in the alert key.
ListRecordType	String	*[Mandatory attribute]*This field is used when filtering alerts, to determine whether the record is a sanctions or PEP record. It must contain a value of SAN, PEP, or a combination of these values. If you want to include a combination of values, the values must be comma-separated and enclosed by double quotation marks. For example: "SAN, PEP".
ListRecordOrigin	String	This field is used to record the provenance of a record when it is part of a consolidated list.
ListRecordId	String	*[Mandatory attribute]* This attribute is not used as part of the matching process, but it must be populated with a unique identifier.
RegistrationNumber	String	This is an optional field that may be used to capture entity registration numbers which are known for use in the review process. Note that entity registration numbers are not used for matching in the default screening rules.
EntityName	String	*[Mandatory attribute]* The entity matching process is based primarily on the name supplied for the entity. An entity name or original script name must be submitted to the screening process for screening to proceed.

Field Name	Expected Data Format	Notes
NameType	String	This is an optional field used in the review process only. Multiple names may exist for the same person. The Name Type, therefore, denotes if the name is the primary name of the listed party, or an additional name (such as an Alias, or Alternate Spelling). If two private list records were derived from a single source with multiple names (such as Mrs. Louise Wilson née Hammond being split into two records, Louise Wilson and Louise Hammond) you may wish to denote one as the primary name and one as a maiden or alias name.
NameQuality	String	This field may be assigned a value of Low, Medium, or High to indicate the quality of the individual name. High is used for Primary names and specified good/high-quality aliases.
PrimaryName	String	For alias records, this field indicates the main name for that record.
OriginalScriptName	String	*[Mandatory attribute]* The individual matching process is based primarily on the name supplied for the individual. Either a full name, a pair of given and family names, or an original script name must be submitted to the screening process for screening to proceed. If you populate the Original Script Name, then you will also need to enable two facets of Match processor configuration that are disabled by default. The Original Script Name Cluster and some or all the Match Rules that include Original script name in their name. To adapt the Match Processor configuration, you will need to open the Transaction screening project within the Director user interface and make the changes to every process used during the Transaction Filtering installation.
AliasIsAcronym	String	If this field is set to **Y**, this flags an alias as an acronym as opposed to a full entity name. Leaving the field blank or setting it to any other value does not affect (that is, an alias is a full entity name). This flag is used during matching.

Field Name	Expected Data Format	Notes
VesselIndicator	String	This field must be set to Y if the entity is a vessel (a ship). It must be left empty or set to **N** if the entity is not a vessel.
VesselInfo	String	If the entity is a vessel, you can populate this field with information about it: for example, its call sign, type, tonnage, owner, flag, and so on.
Address1	String	These are optional fields that may be used in the review process.
Address2	String	
Address3	String	
Address4	String	
City	String	*[Recommended attribute]* City data is used to strengthen potential match information.
State	String	
Postal Code	String	
AddressCountryCode	String; ISO 2-character country code.	*[Recommended attribute]* Address country data is used to strengthen potential match information.
ResidencyCountryCode	String; ISO 2-character country code.	*[Recommended attribute]* The entity's registration country can be used in optional country prohibition screening.
OperatingCountryCodes	String; ISO 2-character country code.	*[Recommended attribute]* Any of the entity's operating countries can be used in optional country prohibition screening.
ProfileHyperlink	String; a hyperlink to an Internet or intranet resource for the record.	This field may contain a hyperlink to an Internet or intranet resource that can provide reviewers with additional information about the individual.
RiskScore	Number, between 0 and 100	This field is included where the risk score for a customer is calculated externally.
RiskScorePEP	Number, between 0 and 100	A number indicating the relative 'riskiness' of the individual, considered as a PEP. The risk score is expressed as an integer between 1 and 100, with higher numbers indicating a higher risk.
AddedDate	String, representing a date, in the format 'YYYYMMDD'	These are optional fields for use in the review process.
LastUpdatedDate	String, representing a date, in the format 'YYYYMMDD'	

Field Name	Expected Data Format	Notes
DataConfidenceScore	Number, between 0 and 100	
DataConfidenceComment	String	
InactiveFlag	String	If populated, this optional field must contain either **Y** or **N**.
InactiveSinceDate	String, representing a date, in the format 'YYYYMMDD'	If populated, this optional field must contain either the current date or a date in the past.
PEPclassification	String	This field can be used to indicate the type of PEP (for example, whether the individual is part of an international organization or government, and at what level). It can be used to filter watch list records and is primarily used by the World-Check watch list, but could be used by a private watch list if required.
customString1 to customString40	String	Fifty custom fields are provided in the private list data interface for individuals. Forty of these are intended to hold string data, five hold dates, and five numeric data.
customDate1 to customDate5	String, representing a date, in the format 'YYYYMMDD'	The interface file is a comma-separated value (`.csv`) file, and so all fields intrinsically contain strings. However, during the processing of Private watch lists, the custom date and number fields are checked to ensure that they include appropriate data, and warning messages are provided as output if they do not.
customNumber1 to customNumber5	Number	

14   Appendix B: System Audit Logging Information

This appendix contains information on the logs related to the Debug and Info log files.

14.1   Activities for System Audit

The following table contains information related to the system audit activities:

Table 45: Activities for System Audit

Activity Identifier	Activity Name	Activity Sequence
1	Raw Message Processing	1
2	Message Parser Processing	2
3	watch list Processing	3
4	Alert Manager Processing	4
5	Hold	5
6	Assigned	6
7	Escalated	7
8	Recommend to Block	8
9	Block	9
10	Recommend to Release	10
11	Release	11
12	Reject	12

14.2   Steps for System Audit Activities

The following table contains information related to the steps for the system audit activities:

Table 46: Steps for System Audit Activities

Step Identifier	Activity Name	Step Name	Step Sequence	Status
1	Raw Message Processing	Record the receipt of the raw message	1	Y
2	Raw Message Processing	Raw Message persisted into structure table	2	N
3	Message Parser Processing	Raw Message parsed	1	N

Step Identifier	Activity Name	Step Name	Step Sequence	Status
4	Message Parser Processing	Parsed Raw Message persisted into structure table	2	N
5	watch list Processing	Matching data prepared	1	N
6	watch list Processing	Matching Engine Invoked	2	Y
7	watch list Processing	Scoring Engine Invoked	3	Y
8	watch list Processing	Scoring performed	4	Y
9	watch list Processing	Response Received	5	Y
10	watch list Processing	Response persisted	6	N
11	Alert Manager Processing	Transaction Hold	1	N
12	Alert Manager Processing	Alert Persisted	2	N
13	Hold	Hold Transaction Workflow Invoked	1	Y
14	Hold	Hold Transaction Workflow completed	2	Y
15	Assigned	Assigned Transaction Workflow Invoked	1	Y
16	Assigned	Assigned Transaction Workflow completed	2	Y
17	Escalate	Escalated Transaction Workflow Invoked	1	Y
18	Escalate	Escalated Transaction Workflow completed	2	Y
19	Recommend to Block	NA	NA	NA

| Step Identifier	Activity Name	Step Name	Step Sequence	Status
20	Block	Blocked Transaction Workflow Invoked	1	Y
21	Block	Blocked Transaction Workflow completed	2	Y
22	Recommend to Release			
23	Release	Released Transaction Workflow Invoked	1	Y
24	Release	Released Transaction Workflow completed	2	Y
25	Reject	NA	NA	NA

15 Appendix C: Process Modeller Framework (PMF) Configurability

This appendix contains information on the steps required to configure the ready-to-use Process Modeller Framework (PMF) workflow. On the **Process Modeller** page, click the transaction that you want to configure and follow the steps in the following sequence. For information on how to access the **Process Modeller** page, see the Process Modeller Menu.

15.1 Configuring the Human Task in the PMF Page

To configure all human tasks on the **PMF** page, follow these steps:

1. Navigate to the **Process Flow** subtab in the **Process Modeller** tab. The **PMF** page is displayed.

2. Drag and drop **Human Task** on to the PMF page. For information on all components available, see the **Components for Designing Your Process Flow** chapter in the Oracle Financial Services Analytical Applications Infrastructure Process Modelling Framework (PMF) Orchestration Guide.

3. Double-click **Human Task**.

4. In the Activity dialog, provide the following information:

    ▪ A unique activity name in the **Activity Name** field. After you provide a name, it appears after the icon on the **PMF** page.

    ▪ The activity description in the **Activity Description** field.

    ▪ The current status of the transaction in the **Status** field.

    ▪ The next status of the transaction in the **Outcomes** field.

5. Click **Transitions** and then click **Add**.

    ▪ In the **Add New Transition** dialog, provide the following information:

    ▪ A unique transition name in the **Transition Name** field.

    ▪ The destination status of the transaction in the **Connected To** field.

    ▪ The execution or decision rule for a status in the **Decision Rule** field. Here you need to map the specific rule to the current status or create the rule according to the business requirement.

    ▪ The order of the transaction in the **Order** field.

    You can also configure the fields in the **Action and Notifications** subtabs. For more information, see the **Action Tab for Creating Tasks/Notification** section in the Oracle Financial Services Analytical Applications Infrastructure Process Modelling Framework (PMF) Orchestration Guide.

15.1.1 Mapping the Transaction Statuses and Transaction Outcomes

After you provide the new transaction status and outcome in step 4, you need to map the values in the required tables to update the value on the **PMF** page.

To update the status on the **PMF** page, populate the following status in the Config schema:

1. Run `select * from AAI_WF_STATUS_B t` where t.v_app_package_id = 'OFS_SAC' and `select * from AAI_WF_STATUS_TL` where t.v_app_package_id = 'OFS_SAC' queries.

2. In the `AAI_WF_STATUS_B` table, populate a unique entry in the `v_status_id` column for each new status and map the same entry in the `AAI_WF_STATUS_TL` table for a column. For example, populate the entry `OFS_SAC` in the `v_app_package_id` column.

3. When you map the new status, it appears on the PMF page.

   ▪ Ensure that data is provided in all required columns in the `AAI_WF_STATUS_TL` table.

   ▪ When doing the mapping in any other configuration tables, ensure that you provide the same status that is mentioned in the `v_status_name` column in the `AAI_WF_STATUS_TL` table.

To update the outcome on the PMF page, populate the following status in the Config schema:

1. Run the `select * from AAI_WF_OUTCOME_B t` and where t.v_app_package_id = 'OFS_SAC' queries.

2. In the `AAI_WF_OUTCOME_B` table, populate a unique outcome ID in the `v_outcome_id` column for each new status and map the same entry in the `AAI_WF_OUTCOME_TL` table.

   ▪ Ensure that data is provided in all required columns in the `AAI_WF_OUTCOME_TL` table.

   ▪ When doing the mapping in any other configuration tables, ensure that you provide the same status that is mentioned in the `AAI_WF_OUTCOME_TL` table.

   ▪ After you complete the above steps, refresh the application and web servers.

15.2 Adding Data Fields for the PMF Status

To add a new data field for each new status, for example, `TF_BLOCKED_NEW`, click the **Data Fields** subtab in the **Process Modeller** page and click **Add**. For information on the fields, see the **Data Fields** section in the [Oracle Financial Services Analytical Applications Infrastructure Process Modelling Framework (PMF) Orchestration Guide](#).

> | **NOTE** | If the data field name contains more than one word, give an underscore (_) between each word. The name will not be valid if you provide a space between each word. |

You can also edit an existing data field, follow these steps:

1. Select the radio button of the data field that you want to edit.

2. Click **Edit**.

15.3 Adding Application Rules for the PMF Status

To add a new application rule for each new status, for example, `RB_TO_Block_New`, click the **Application Rule** subtab in the **Process Modeller** page and click **Add**. For information on the fields, see the **Application Rules** section in the [Oracle Financial Services Analytical Applications Infrastructure Process Modelling Framework (PMF) Orchestration Guide](#).

15.3.1 Mapping Rule Types to Application Rules

If you select a new rule type for the application rule, you must then map it to the rule.

To map a rule, run the `select * from aai_aom_app_comp_attr_mapping` query.

If a static rule is present with n_static_grp_id = 501, then run the `select * from AAI_AOM_STATIC` query.

15.3.2 Mapping User Groups to Application Rules

If you have also mapped a new user group to the rule, then you need to map the entry in the `DOMAIN_JUR_GRP_MAP` table. After you map the user group to the rule, run the `select * from DOMAIN_JUR_GRP_MAP` query to update the `DOMAIN_JUR_GRP_MAP` table.

The steps required to create a new user group are available in [Creating New User Groups](#). For more information, see the **User Administrator** section in the [Oracle Financial Services Analytical Applications Infrastructure User Guide](#).

15.4 Configurations Required for the Audit Tables

Before you update the tables, you need to first provide a unique value in the `n_activity_id` column in the `SETUP_RT_AUD_ACTIVITY` table and then provide the same value in the `n_activity_id` column in the `SETUP_RT_AUD_STEPS` table.

After this is done, run the `select * from SETUP_RT_AUD_ACTIVITY` query to update the `SETUP_RT_AUD_ACTIVITY` table and run the `select * from SETUP_RT_AUD_STEPS` query to update the `SETUP_RT_AUD_STEPS` table.

After the tables are updated, provide two entries, 1 and 2, in the `n_step_sequence` column in the `SETUP_RT_AUD_STEPS` table.

> **NOTE** The value provided in the `v_status_name` column in the `AAI_WF_STATUS_TL` table must be a combination of one of the following values:
> - The value provided in `v_sanction_status_name` in `dim_sanctions_status` table and the name of the transaction workflow invoked for entry 1.
> - The value provided in `v_sanction_status_name` in `dim_sanctions_status` table and the name of the transaction workflow completed for entry 2.

15.5 Configurations Required for the setup_rt_params Table

To configure the table in the ATOMIC schema, follow these steps:

1. Provide the function code in the `v_attribute_value1` column where `v_attribute_name1 = 'TF_ FUNCTION_CODES'`.

2. Provide the status codes according to the `v_attribute_name1` value in the `v_attribute_value1` column where `v_attribute_name1 = 'TF_FUNCTION_AND_STATUS_CODES'`.

3. Provide all status codes in the `v_attribute_value1` column against each function code in the `v_attribute_name1` column. This displays the dynamic status filter.

4. Provide the code for each status to be displayed to the user for that function code in the `v_attribute_value1` column.

5. Provide the code for each status to be displayed to the user in the *Transaction Summary* window in the `v_attribute_value2` column.

6. Provide the code for each action that must be displayed to the user for that transaction in the `v_attribute_value3` column.

7. To create an order for the transactions, follow these steps:

   a. Provide `TF_USERWORKFLOWCLAUSE` in the `v_param_name` column.

   b. Provide `TF_ORDERBY_PRECEDENCE` in the `v_attribute_name1` column.

   c. Provide `TF_ORDERBY_FUNCCODE` in the `v_attribute_name2` column.

   d. Provide the function code for which you want to do the order in the `v_attribute_value2` column. For example, use `TFLTANYSE` for the analyst user.

   e. Provide `TF_ORDERBY_CLAUSES` in the `v_attribute_name3` column.

   f. Provide the order by query in the `v_attribute_value3` column. For example, see the value for the `TFLTANYSE` function code.

15.6 Configurations Required for the dim_sanctions_status Table

To configure the table in the ATOMIC schema, follow these steps:

1. Create a unique value for the new PMF status in the `n_sanction_status_code` column. This value must be the same in the `AAI_WF_STATUS_B` and `AAI_WF_STATUS_TL` columns. For more information, see Configurations Required for the Audit Tables.

2. Provide the activity name as mentioned in step 4 of the Configuring the Human Task in the PMF Page section in the `v_remarks` column.

3. Provide a unique data field value in the `v_applicable_params` column where `n_sanction_staus_key = 101` (ApplicationParams) and `n_sanction_staus_key = 202` (PMFParams).

4. To update the image path for the alert status, update the `v_sanction_status_img_path` value.

5. To update the image path for the list of actions, update the `v_sanction_dropdown_img_path` value.

6. To configure the action status:

   a. Provide the value `StatusActon` if a status action must be fired.

    b. Provide the value `PendingTrxnsCount` if the count of pending transactions is required for a particular action.

    c. Provide the value `PendingTrxnsSuspiciousCountAndStatusActon` if the count of pending transactions and count of pending suspicious transactions are both required.

7. In the `v_data_field` column, give the same data field created in the PMF page data field section.

8. Update the `v_owner_update` column in the `fsi_rt_alerts` table if the owner must be updated.

9. Provide the audit message in the `v_audit_msg` column. This value must be the same as the value provided in the `v_sanction_status_name` column. For more information, see <u>Configurations Required for the Audit Tables</u>.

> **NOTE**   For a new status, the `v_applicable_params` column must be left blank.

15.7   Creating New User Groups

To add a new user group, follow these steps:

1. Create a function.

2. Create a role.

3. Map the function to the role.

4. Create a user.

5. Map the user to a user group and a role.

6. Map the user to a user group and a domain.

7. Map the user to a user group.

15.8   Other Configurations

The user group is now created. After it is created, follow these steps:

1. Map the group in the `domain_jur_grp_map` table.

2. Login to the Config schema.

3. Run the `select * from cssms_folder_function_map` query.

4. Add the new function to the `Transaction Filter` folder (TransactionFiltering `TFLTADMIN`).

5. Run the `select t.v_access_code,t.v_menu_id from aai_menu_b t  where t.v_menu_id in('OFS_TFLTSCRN','OFS_TFLT')` query.

6. Add the new function in the `v_access_code` column.

7. To map the new function, add an entry in the `v_access_code` column in the `aai_menu_b` table by running a query with the entry mentioned in the following format: `select * from aai_menu_b t where t.v_menu_id like '%OFS_TFLT%';` query.

8. To map the function to a folder, run a query with the function mentioned in the following format:

```
select * from cssms_folder_function_map p where p.v_function_code like
'%TF%'; query.
```

16   Appendix D: Time Zone Configuration

This appendix contains information on the expected user input to set up the time zone preference for any user in the database. You can configure the time zone for each user ID.

If no time zone is specified for a user, the default time zone is the time zone specified in the user's browser.

To update the time zone for a user, follow these steps:

1. Run the following script:

```
select * from AAI_USR_PREFERENCE_DETAIL t where t.v_preference_id =
'TIME_ZONE';
```

2. Update the time zone name in the following `V_PREFERENCE_VALUE` column:

Table 47: User IDs for Time Zones

V_USER_ID	V_PREFERENCE_ID	V_PREFERENCE_VALUE
Administrator	TIME_ZONE	Asia/Kolkata
Analyst	TIME_ZONE	Africa/Abidjan
Supervisor	TIME_ZONE	Africa/Accra

The following table shows the country code and the respective time zone name. The following country codes listed here are only for reference. For each country code, the respective time zone name must be used to update the time zone.

Table 48: Country Codes for Time Zones

Country Code	Time Zone Name
CI	Africa/Abidjan
GH	Africa/Accra
ET	Africa/Addis_Ababa
DZ	Africa/Algiers
ER	Africa/Asmara
ML	Africa/Bamako
CF	Africa/Bangui
GM	Africa/Banjul
GW	Africa/Bissau
MW	Africa/Blantyre
CG	Africa/Brazzaville
BI	Africa/Bujumbura

Country Code	Time Zone Name
EG	Africa/Cairo
MA	Africa/Casablanca
ES	Africa/Ceuta
GN	Africa/Conakry
SN	Africa/Dakar
TZ	Africa/Dar_es_Salaam
DJ	Africa/Djibouti
CM	Africa/Douala
EH	Africa/El_Aaiun
SL	Africa/Freetown
BW	Africa/Gaborone
ZW	Africa/Zimbabwe
ZA	Africa/Johannesburg
SS	Africa/Juba
UG	Africa/Kampala
SD	Africa/Khartoum
RW	Africa/Kigali
CD	Africa/Kinshasa
NG	Africa/Lagos
GA	Africa/Libreville
TG	Africa/Lome
AO	Africa/Luanda
CD	Africa/Lubumbashi
ZM	Africa/Lusaka
GQ	Africa/Malabo
MZ	Africa/Maputo
LS	Africa/Maseru
SZ	Africa/Mbabane
SO	Africa/Mogadishu
LR	Africa/Monrovia
KE	Africa/Nairobi
TD	Africa/Ndjamena
NE	Africa/Niamey

Country Code	Time Zone Name
MR	Africa/Nouakchott
BF	Africa/Ouagadougou
BJ	Africa/Porto-Novo
ST	Africa/Sao_Tome
CI	Africa/Timbuktu
LY	Africa/Tripoli
TN	Africa/Tunis
NA	Africa/Windhoek
US	America/Adak
	America/Anchorage
	America/Boise
	America/Chicago
	America/Denver
	America/Detroit
	America/Indianapolis
	America/Knox
	America/Marengo
	America/Petersburg
	America/Tell_City
	America/Vevay
	America/Vincennes
	America/Winamac
	America/Juneau
	America/Louisville
	America/Monticello
	America/Los_Angeles
	America/Menominee
	America/Metlakatla
	America/New_York
	America/Nome
	America/Beulah
	America/Center
	America/New_Salem

Country Code	Time Zone Name
	America/Phoenix
	America/Sitka
	America/Yakutat
	America/Honolulu
AI	America/Anguilla
AG	America/Antigua
AR	America/Buenos_Aires
	America/Catamarca
	America/Cordoba
	America/Jujuy
	America/La_Rioja
	America/Mendoza
	America/Rio_Gallegos
	America/Salta
	America/San_Juan
	America/San_Luis
	America/Tucuman
	America/Ushuaia
AW	America/Aruba
PY	America/Asuncion
CA	America/Atikokan
	America/Blanc-Sablon
	America/Cambridge_Bay
	America/Creston
	America/Dawson
	America/Dawson_Creek
	America/Edmonton
	America/Fort_Nelson
	America/Glace_Bay
	America/Goose_Bay
	America/Halifax
	America/Inuvik
	America/Iqaluit

Country Code	Time Zone Name
	America/Moncton
	America/Nipigon
	America/Pangnirtung
	America/Rainy_River
	America/Rankin_Inlet
	America/Regina
	America/Resolute
	America/St_Johns
	America/Swift_Current
	America/Thunder_Bay
	America/Toronto
	America/Vancouver
	America/Whitehorse
	America/Winnipeg
	America/Yellowknife
BR	America/Araguaina
	America/Bahia
	America/Belem
	America/Boa_Vista
	America/Campo_Grande
	America/Cuiaba
	America/Eirunepe
	America/Fortaleza
	America/Maceio
	America/Manaus
	America/Noronha
	America/Porto_Velho
	America/Recife
	America/Rio_Branco
	America/Santarem
	America/Sao_Paulo
MX	America/Bahia_Banderas
	America/Cancun

Country Code	Time Zone Name
	America/Chihuahua
	America/Hermosillo
	America/Matamoros
	America/Mazatlan
	America/Merida
	America/Mexico_City
	America/Monterrey
	America/Ojinaga
	America/Tijuana
BB	America/Barbados
BZ	America/Belize
CO	America/Bogata
VE	America/Caracas
GF	America/Cayenne
KY	America/Cayman
CR	America/Costa_Rica
CW	America/Curacao
GL	America/Danmarkshavn
	America/Godthab
	America/Scoresbysund
	America/Thule
DM	America/Dominica
SV	America/El_Salvador
TC	America/Grand_Turk
GD	America/Grenada
GP	America/Guadeloupe
GT	America/Guatemala
EC	America/Guayaquil
GY	America/Guyana
CU	America/Havana
JM	America/Jamaica
BQ	America/Kralendijk
BO	America/La_Paz

Country Code	Time Zone Name
PE	America/Lima
SX	America/Lower_Princes
NI	America/Managua
MF	America/Marigot
MQ	America/Martinique
PM	America/Miquelon
UY	America/Montevideo
MS	America/Montserrat
BS	America/Nassau
PA	America/Panama
SR	America/Paramaribo
TT	America/Port_of_Spain
HT	America/Port-au-Prince
PR	America/Puerto_Rico
CL	America/Punta_Arenas
	America/Santiago
	America/Easter
DO	America/Santo_Domingo
BL	America/St_Barthelemy
KN	America/St_Kitts
LC	America/St_ Lucia
VI	America/St_Thomas
VC	America/St_Vincent
HN	America/Tegucigalpa
VG	America/Tortola
AQ	Antarctica/Casey
	Antarctica/Davis
	Antarctica/DumontDurville
	Antarctica/Mawson
	Antarctica/McMurdo
	Antarctica/Palmer
	Antarctica/Rothera
	Antarctica/Syowa

Country Code	Time Zone Name
	Antarctica/Troll
	Antarctica/Vostok
SJ	Arctic/Longyearbyen
YE	Asia/Aden
KZ	Asia/Almaty
	Asia/Aqtau
	Asia/Aqtobe
	Asia/Atyrau
	Asia/Oral
	Asia/Qyzylorda
JO	Asia/Amman
TM	Asia/Ashgabat
IQ	Asia/Baghdad
BH	Asia/Bahrain
AZ	Asia/Baku
TH	Asia/Bangkok
RU	Asia/Anadyr
	Asia/Barnaul
	Asia/Chita
	Asia/Irkutsk
	Asia/Kamchatka
	Asia/Khandyga
	Asia/Krasnoyarsk
	Asia/Magadan
	Asia/Novokuznetsk
	Asia/Novosibirsk
	Asia/Omsk
	Asia/Sakhalin
	Asia/Srednekolymsk
	Asia/Tomsk
	Asia/Ust-Nera
	Asia/Vladivostok
	Asia/Yakutsk

Country Code	Time Zone Name
	Asia/Yekaterinburg
	Europe/Astrakhan
	Europe/Kaliningrad
	Europe/Kirov
	Europe/Moscow
	Europe/Samara
	Europe/Saratov
	Europe/Ulyanovsk
	Europe/Volgograd
LB	Asia/Beirut
KG	Asia/Bishkek
BN	Asia/Brunei
MN	Asia/Choibalsan
	Asia/Hovd
	Asia/Ulaanbaatar
LK	Asia/Colombo
SY	Asia/Damascus
BD	Asia/Dhaka
TL	Asia/Dili
AE	Asia/Dubai
TJ	Asia/Dushanbe
CY	Asia/Famagusta
PS	Asia/Gaza
VN	Asia/Ho_Chi_Minh
HK	Asia/Hong_Kong
ID	Asia/Jakarta
	Asia/Jayapura
	Asia/Makassar
	Asia/Pontianak
IL	Asia/Jerusalem
AF	Asia/Kabul
PK	Asia/Karachi
NP	Asia/Kathmandu

Country Code	Time Zone Name
IN	Asia/Kolkata
MY	Asia/Kuala_Lumpur
	Asia/Kuching
KW	Asia/Kuwait
MO	Asia/Macau
PH	Asia/Manila
OM	Asia/Muscat
KH	Asia/Phnom_Penh
KP	Asia/Pyongyang
QA	Asia/Qatar
MM	Asia/Rangoon
	Asia/Yangon
SA	Asia/Riyadh
UZ	Asia/Samarkand
	Asia/Tashkent
KR	Asia/Seoul
CN	Asia/Shanghai
	Asia/Urumqi
SG	Asia/Singapore
TW	Asia/Taipei
GE	Asia/Tbilisi
IR	Asia/Tehran
BT	Asia/Thimphu
JP	Asia/Tokyo
LA	Asia/Vientiane
AM	Asia/Yerevan
PT	Atlantic/Azores
	Atlantic/Madeira
BM	Atlantic/Bermuda
ES	Atlantic/Canary
CV	Atlantic/Cape_Verde
FO	Atlantic/Faroe
IS	Atlantic/Reykjavik

Country Code	Time Zone Name
GS	Atlantic/South_Georgia
SH	Atlantic/St_Helena
FK	Atlantic/Stanley
AU	Australia/Adelaide
	Australia/Brisbane
	Australia/Broken_Hill
	Australia/Canberra
	Australia/Currie
	Australia/Darwin
	Australia/Eucla
	Australia/Hobart
	Australia/Lindeman
	Australia/Lord_Howe
	Australia/Melbourne
	Australia/Perth
	Australia/Sydney
	Australia/Yancowinna
NL	Europe/Amsterdam
AD	Europe/Andorra
GR	Europe/Athens
GB	Europe/Belfast
RS	Europe/Belgrade
DE	Europe/Berlin
SK	Europe/Bratislava
BE	Europe/Brussels
RO	Europe/Bucharest
HU	Europe/Budapest
DE	Europe/Busingen
MD	Europe/Chisinau
DK	Europe/Copenhagen
IE	Europe/Dublin
GI	Europe/Gibraltar
GG	Europe/Guernsey

Country Code	Time Zone Name
FI	Europe/Helsinki
IM	Europe/Isle_of_Man
TR	Europe/Istanbul
JE	Europe/Jersey
UA	Europe/Kiev
PT	Europe/Lisbon
SI	Europe/Ljubljana
GB	Europe/London
LU	Europe/Luxembourg
ES	Europe/Madrid
MT	Europe/Malta
AX	Europe/Mariehamn
BY	Europe/Minsk
MC	Europe/Monaco
CY	Europe/Nicosia
NO	Europe/Oslo
FR	Europe/Paris
ME	Europe/Podgorica
CZ	Europe/Prague
LV	Europe/Riga
IT	Europe/Rome
SM	Europe/San_Marino
BA	Europe/Sarajevo
UA	Europe/Simferopol
	Europe/Uzhgorod
MK	Europe/Skopje
BG	Europe/Sofia
SE	Europe/Stockholm
EE	Europe/Tallinn
AL	Europe/Tirane
MD	Europe/Tiraspol
LI	Europe/Vaduz
VA	Europe/Vatican

Country Code	Time Zone Name
AT	Europe/Vienna
LT	Europe/Vilnius
PL	Europe/Warsaw
HR	Europe/Zagreb
CH	Europe/Zurich
MG	Indian/Antananarivo
IO	Indian/Chagos
CX	Indian/Christmas
CC	Indian/Cocos
KM	Indian/Comoro
TF	Indian/Kerguelen
SC	Indian/Mahe
MV	Indian/Maldives
MU	Indian/Mauritius
YT	Indian/Mayotte
RE	Indian/Reunion
WS	Pacific/Apia
NZ	Pacific/Auckland
NZ	Pacific/Chatham
PG	Pacific/Bougainville
FM	Pacific/Chuuk
CL	Pacific/Easter
VU	Pacific/Efate
TK	Pacific/Fakaofo
FJ	Pacific/Fiji
TV	Pacific/Funafuti
EC	Pacific/Galapagos
PF	Pacific/Gambier
PF	Pacific/Marquesas
PF	Pacific/Tahiti
SB	Pacific/Guadalcanal
GU	Pacific/Guam
US	Pacific/Honolulu

Country Code	Time Zone Name
KI	Pacific/Enderbury
KI	Pacific/Kiritimati
KI	Pacific/Tarawa
FM	Pacific/Kosrae
MH	Pacific/Majuro
UM	Pacific/Midway
UM	Pacific/Wake
NR	Pacific/Nauru
NU	Pacific/Niue
NF	Pacific/Norfolk
NC	Pacific/Noumea
AS	Pacific/Pago_Pago
PW	Pacific/Palau
PN	Pacific/Pitcairn
FM	Pacific/Pohnpei
PG	Pacific/Port_Moresby
CK	Pacific/Rarotonga
MP	Pacific/Saipan
	Pacific/Samoa
TO	Pacific/Tongatapu
WF	Pacific/Wallis

# 17   Appendix E: Delta Watch List Configurations

Transaction Filtering uses the full watchlist during the screening process. It is not required to perform delta screening due to the clustering strategy which is implemented in the screening process.

Although using the full watchlist is recommended, some customers may need to download and process watchlist delta files, either due to the time zone in when the files are made available or the time taken to download the files.

Customers who download and process the watch list delta files must first do so and then combine them with the previous full watchlists before screening the files through the database. The full list data is available in the `FSI_WATCHLIST_INDIVIDUAL` and `FSI_WATCHLIST_ENTITIES` tables, and the delta updates are available in the `FSI_WATCHLIST_DELTA_INDIVIDUAL` and `FSI_WATCHLIST_DELTA_ENTITIES` tables.

The following image shows the information flow for delta updates:

Figure 94: Delta Updates Flow
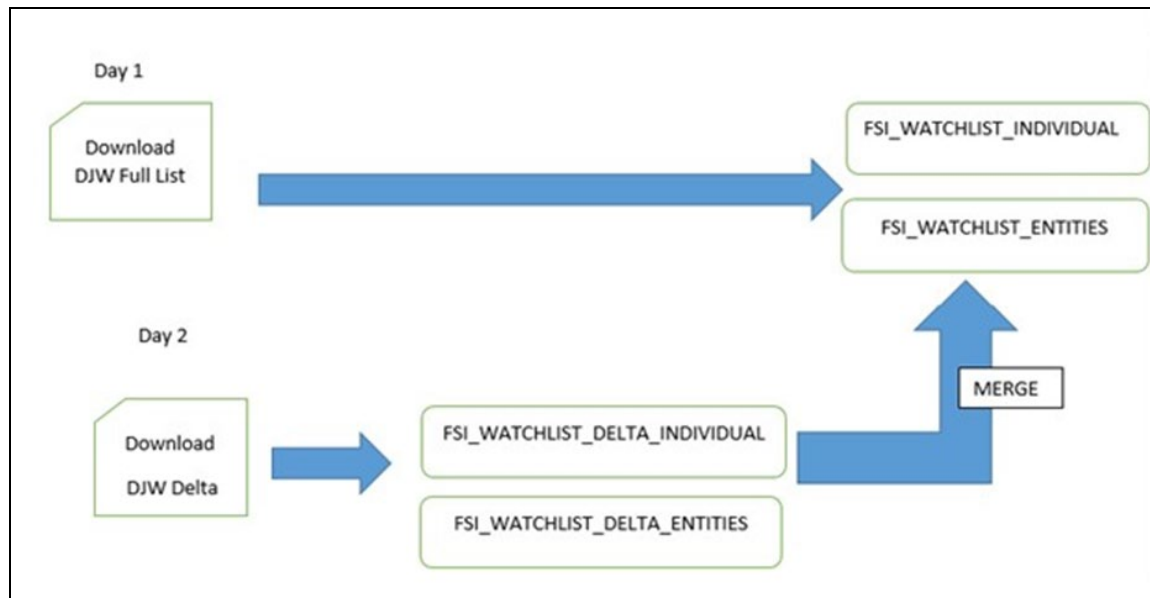
- The following watchlist management jobs are used for the full list and the delta list:
  — Analyze Reference Data Quality
  — Download, Prepare, Filter, and Export All Lists
  — Generate StopPhrases
- The following watchlist management job is used for the full list:
  — Load List data from Stg to Processed table
- The following Transaction Filtering job is used for the full list and the delta list:
  — Main

Before you run the delta watchlist files, ensure that you run the full watchlist files. You can run the delta watch list files if, for example, the delta downloads have failed for multiple days or the filter criteria are changed. You can also run the delta watch list once every week to ensure that the complete data has been processed.

To run the full watch list updates, follow these steps:

1. Navigate to the `EDQ_Run_Profile_FOLDER` directory.

2. Edit the following `watchlist-management - TF.properties` file:

   - To run the watch list file without filtering, set `phase.DJW\ -\ Prepare\ without\ filtering\ DB.enabled` to **Y**.

   - To run the watch list file with filtering, set `phase.DJW\ -\ Prepare\ with\ filtering\ DB.enabled` to **Y**.

   - Set `phase.*.export.*.ind_table_name` to `FSI_WATCHLIST_INDIVIDUAL`.

   - Set `phase.*.export.*.entities_table_name` to `FSI_WATCHLIST_ENTITIES`.

3. To enable the DJAC DJW watch list, that is, export the full list to the database:

   - Set `phase.Dow_Jones_Import1_Full_DB.enabled` to **Y**.

   - To download the delta updates, set `phase.Dow_Jones_Import1_Full_DB.enabled` to **N**.

   - Set `phase.Dow_Jones_Import2_Full_DB.enabled` to **Y**.

   - To download the delta updates, set `phase.Dow_Jones_Import2_Full_DB.enabled` to **N**.

   - Set `phase.Dow_Jones_Import3_Full_DB.enabled` to **Y**.

   - To download the delta updates, set `phase.Dow_Jones_Import3_Full_DB.enabled` to **N**.

4. To enable the watch list external task, set `phase.WatchListLoadPreparedData.enabled` to **Y**.

5. To enable the external task and execute the transaction full list, follow these steps:

   - Set `phase.WatchListLoadData.enabled` to **Y**.

   - Set `phase.SanctionedListRefLoadData.enabled` to **N**.

   - Set `phase.WatchListLoadDeltaData.enabled` to **Y**.

To run the delta updates, follows these steps:

1. Navigate to the `EDQ_Run_Profile_FOLDER` directory.

2. Edit the following attributes in the `watchlist-management - TF.properties` file:

   - To run the watch list file without filtering, set `phase.DJW\ -\ Prepare\ without\ filtering\ DB.enabled` to **N.**

   - To run the watch list file with filtering, set `phase.DJW\ -\ Prepare\ with\ filtering\ DB.enabled` to **N.**

   - To merge the delta updates with the full list, follows these steps:

     — Set phase.Delta\ Merge.enabled to **Y**.

     — Set phase.Linked\ Profiles.enabled to **Y**.

- Set `phase.*.export.*.ind_table_name` to `FSI_WATCHLIST_INDIVIDUAL`.

- Set `phase.*.export.*.entities_table_name` to `FSI_WATCHLIST_ENTITIES`.

3. To enable the DJAC DJW watch list, that is, export the full list to the database:

- Set `phase.Dow_Jones_Import1_Delta_DB.enabled` to **Y**.

- Set `phase.Dow_Jones_Import2_Delta_DB.enabled` to **Y**.

- Set `phase.Dow_Jones_Import3_Delta_DB.enabled` to **Y**.

4. To enable the watch list external task, set `phase.WatchListLoadPreparedData.enabled` to **Y**.

5. To enable the external task and execute the transaction full list, follows these steps:

- Set `phase.WatchListLoadData.enabled` to **Y**.

- Set `phase.SanctionedListRefLoadData.enabled` to **N**.

- Set `phase.WatchListLoadDeltaData.enabled` to **Y**.

18   Appendix F: Message Categories and Message Types

A user of the Transaction Filtering application can use the following message categories:

- SWIFT Message Types
- ISO20022 Message Types
- Fedwire Message Types
- US NACHA Message Types

Each message category has different message types defined. The following tables list the message categories and associated message types. To know the patch number in which the specific message category was added, see Document Control.

For SWIFT, the message types 1 to 8 are the ready-to-use message types that can be used when you log in. The other message types must be imported manually using the SWIFT migration utility.

For ISO20022, Fedwire, and US NACHA, the message types shown in the tables are the ready-to-use message types.

Table 49: SWIFT Message Types

1	MT101	2	MT103	3	MT202	4	MT202COV
5	MT700	6	MT701	7	MT707	8	MT110
9	MT671	10	MT791	11	MT606	12	MT296
13	MT299	14	MT790	15	MT599	16	MT295
17	MT796	18	MT769	19	MT591	20	MT292
21	MT795	22	MT768	23	MT590	24	MT291
25	MT607	26	MT767	27	MT536	28	MT290
29	MT298	30	MT760	31	MT499	32	MT210
33	MT999	34	MT756	35	MT498	36	MT199
37	MT998	38	MT754	39	MT496	40	MT198
41	MT996	42	MT752	43	MT495	44	MT196
45	MT995	46	MT750	47	MT492	48	MT195
49	MT950	50	MT747	51	MT491	52	MT192
53	MT910	54	MT742	55	MT490	56	MT191
57	MT899	58	MT734	59	MT455	60	MT190
61	MT896	62	MT730	63	MT412	64	MT112
65	MT895	66	MT721	67	MT410	68	MT111

69	MT802	70	MT720	71	MT400	72	MT105
73	MT799	74	MT711	75	MT399	76	MT103STP
77	MT798	78	MT699	79	MT300		

Table 50: ISO20022 Message Types

1	ISO pain.001.001.08	2	ISO pain.001.001.08

Table 51: Fedwire Message Types

1	BTR1002	2	CTR1000

Table 52: US NACHA Message Types

1	IAT	2	CTX	3	BOC	4	RCK
5	POP	6	WEB	7	CCD	8	TEL
9	PPD	10	ARC	11	ICE		

OFSAAI Support

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

Send Us Your Comments

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

- Did you find any errors?

- Is the information clearly presented?

- Do you need more information? If so, where?

- Are the examples correct? Do you need more examples?

- What features did you like most about this manual?

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

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