Oracle Financial Services Transaction Filtering

Administration Guide

Release 8.0.5.0.0

October 2017

E91799-01

OFS Transaction Filtering Administration Guide

Document Control

Table 1: Document Control

Version Number	Revision Date	Change Log
8.0.5	October 2017	Created the Administration Guide.
8.0.5.0.2	January 2018	Added the DJAC, DJW, and WC as new watchlists and content for each watchlist, note for the false-positive counter, and configuring watchlists, filter settings, and property files in chapter 4.
8.0.5.0.3	Feb 2018	Added the white list table name in the section Adding, Editing, or Deleting Good Guy Records in Chapter 4, Configuring EDQ, Application Parameters, Message, and Screening. Updated the Application Parameters Configuration Tab to include the four eyes section in the section Configuring Application Level Parameters in Chapter 4, Configuring EDQ, Application Parameters, Message, and Screening. Added the navigation to view the PMF process flow for standard and four-eyes in the section System Configuration and Identity Management Tab in Chapter 2, Getting Started. Added content for the configuring transaction currency for four-eyes in the section Configuring the Transaction Currency in Chapter 4, Configuring EDQ, Application Parameters, Message, and Screening.
8.0.5.0.5	June 2018	Updated section Configuring Operating Model - Multi-Jurisdiction and Multi Business Unit Implementation in Chapter 4, Configuring EDQ, Application Parameters, Message, and Screening.
8.0.5.0.12	Jan 2019	Added the MT 110 message type in Chapter 4, Configuring EDQ, Application Parameters, Message and Screening, and Chapter 5, Configuring Risk Scoring Rules. Updated the EU Reference Data section in Appendix A, Watch Lists.
8.0.5.0.14	Feb 2019	Added a new Watchlist Management Job, Load List data from Stg to Processed table, in the Configuring Jobs section.

Table of Contents

1 About this Guide

This guide provides comprehensive instructions for proper 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. This section focuses on the following topics:

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 Consultants**: 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 EDQ and the SWIFT message and screening parameters in the Oracle Financial Services Transaction Filtering application.
- Configuring Risk Scoring Rules describes how to configure business rules in OFS Inline Processing Engine.

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
`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

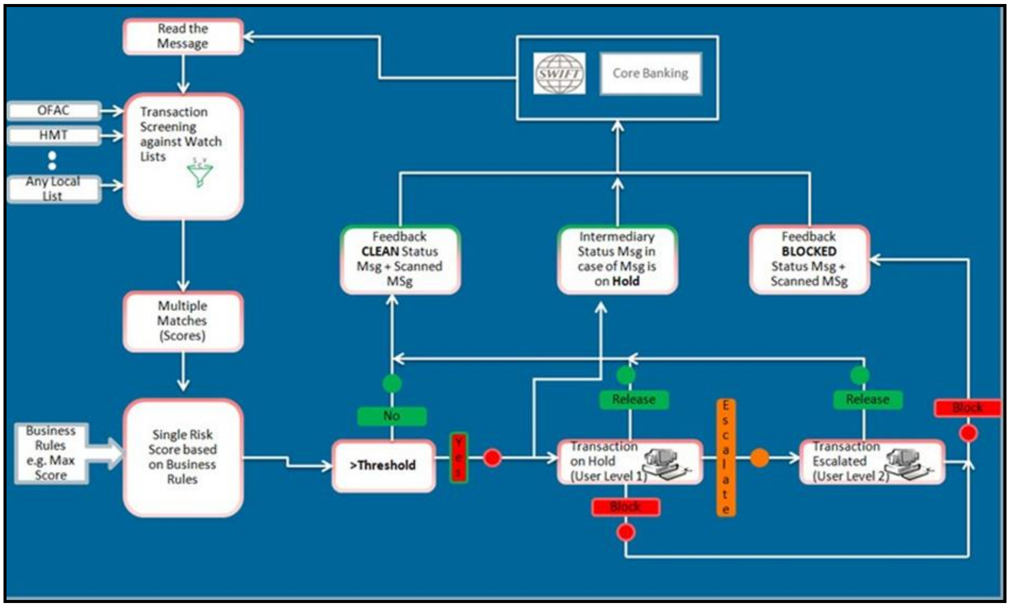
The Oracle Financial Services (OFS) Transaction Filtering application is a real-time filtering system that identifies financial transactions done by blacklisted, sanctioned, and restricted individuals, entities, cities, countries, ships, vessels, and so on. The application can interface with any clearing systems, payment systems, or source systems. The application accepts messages from the source systems in real time and scans them against different watch lists maintained within the system to identify any blacklisted data present within the transaction message, which is in a SWIFT format. The OFS Transaction Filtering application is built using three components: a scoring engine (EDQ), a user interface, and a rule engine (IPE).

Financial institutions use OFS Transaction Filtering for the following tasks:

- Identify transactions done by customers, organizations, and countries which are sanctioned.
- Perform daily checks of customers' names and filter customers' transactions against the OFAC and HMT sanctions lists.
- Generate risk scores for entities with whom business or transactions are prohibited.

2.1 Transaction Filtering Process Flow

Figure 1: Transaction Filtering Process Flow:


Read the Message
SWIFT
Core Banking
OFAC
HMT
Any Local List
Transaction Screening against Watch Lists
Feedback CLEAN Status Msg + Scanned MSg
Intermediary Status Msg in case of Msg is on Hold
Feedback BLOCKED Status Msg + Scanned MSg
Multiple Matches (Scores)
Release
Release
No
Block
Business Rules e.g. Max Score
Single Risk Score based on Business Rules
>Threshold
Yes
Transaction on Hold (User Level 1)
Escalate
Transaction Escalated (User Level 2)
Block

The Transaction Filtering application receives the transaction message from a JMS queue. The message is in a SWIFT format. The transaction message is screened against a watch list through the Enterprise Data Quality (EDQ) platform. The message is sent to the EDQ platform, and EDQ sends back a response. For every match, a match score is generated through the IPE platform. If a match is not found, then the system generates a zero score.

The final score is checked against a threshold limit set within the application. If the score is greater than the threshold limit, then the transaction is treated as a suspicious transaction. If the score is lesser than the threshold limit, then the transaction is treated as a clean transaction.

NOTE

- All field details of the message are stored within the application.
- There may be more than one transaction present within a message. In this case, each transaction is screened against external and internal watch lists.
- Different scores can also be assigned to different watch lists using rules. All scores are based on multiple rules set up in the application and are configurable. In the case of multiple scores, the logic is used to take the maximum score out of all the scores, and the score is treated as a final score for any given transaction.
- For information on IPE, see OFS Inline Processing Engine User Guide.
- If all the transactions within a message are clean, then a feedback message is sent back to the central banking system with a CLEAN status. The message contains the status, message reference ID, and transaction reference ID. If any transaction within a message is found to be suspicious, then the complete message is moved into a HOLD status and is available for user action. For more information, see OFS Transaction Filtering User Guide.

3 Getting Started

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

3.1 Accessing OFSAA Applications

Access to the Oracle Financial Services Transaction Filtering application depends on the Internet or Intranet environment. Oracle Financial Services Transaction Filtering is accessed through Google Chrome. The system administrator provides the intranet address uniform resource locator (URL), User ID, and Password. Log in to the application through the Login page. You will be prompted to change your password on your first login. You can change your password whenever required by logging in. For more information, see the Troubleshooting Your Display section.

To access the Oracle Financial Services Analytical Applications, follow these steps:

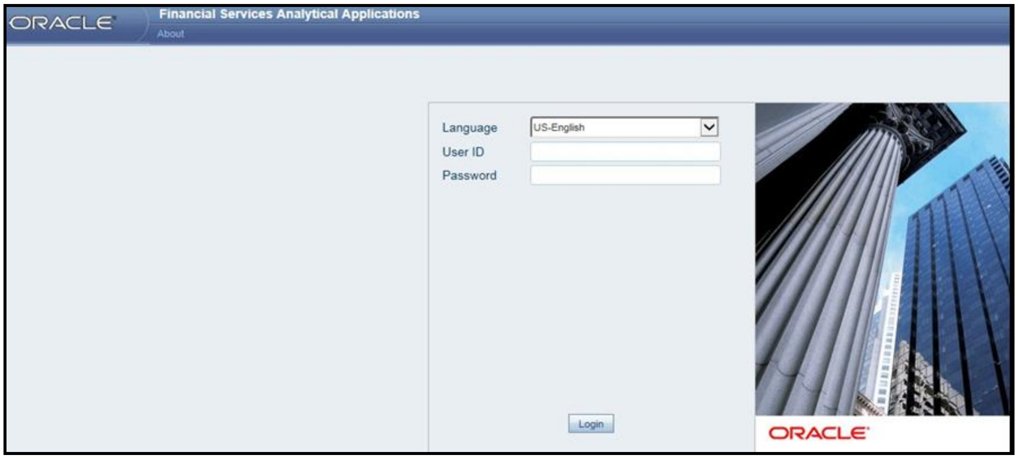
1. Enter the URL into your browser using the following format:

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

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

   The OFSAA Login page is displayed.

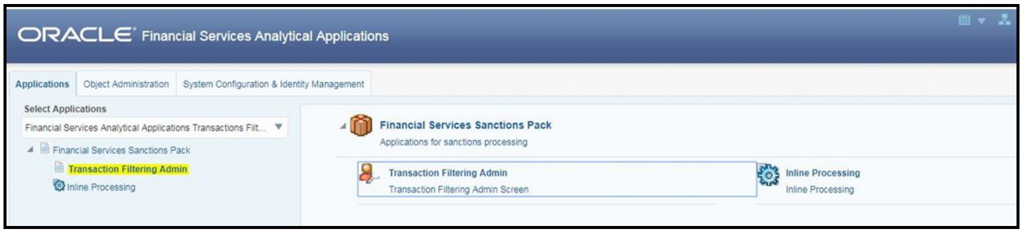
Figure 2: OFSAA Login page



Language: US-English
User ID
Password

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 Oracle Financial Services Analytical Applications page is displayed.

Figure 3: OFSAA Application Page


ORACLE Financial Services Analytical Applications
Applications
Object Administration
System Configuration & Identity Management
Select Applications
Financial Services Analytical Applications Transactions Filt...
Financial Services Sanctions Pack
Transaction Filtering Admin
Inline Processing
Financial Services Sanctions Pack
Applications for sanctions processing
Transaction Filtering Admin
Transaction Filtering Admin Screen
Inline Processing
Inline Processing

3.2 Managing OFSAA Application Page

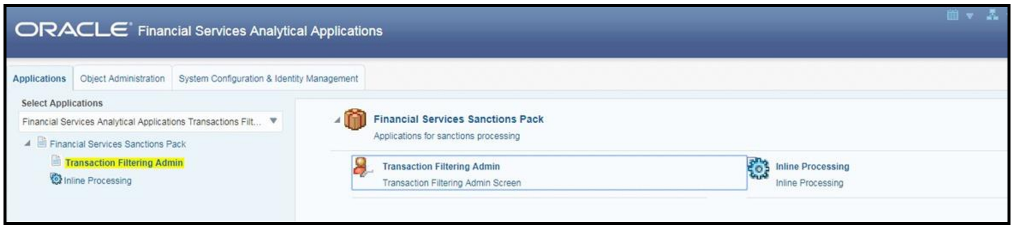
This section describes the options available for system configuration on the OFSAA Application page. The OFSAA Application page has the following tabs:

- Applications Tab
- Object Administration Tab
- System Configuration and Identity Management Tab

3.2.1 Applications Tab

The Applications tab allows the system administrator to configure information related to the Transaction Filtering Admin screens such as the application parameters and the message and screening parameters, and information related to the Inline Processing Engine (IPE).

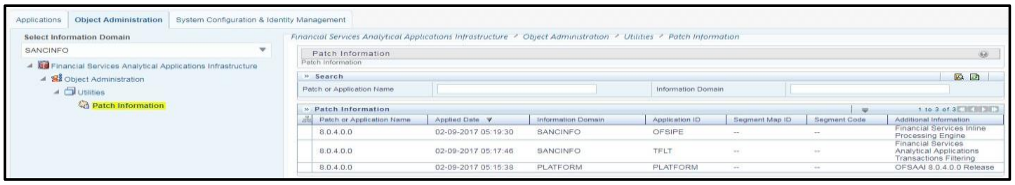
Figure 4: Applications Tab


ORACLE Financial Services Analytical Applications
Applications
Object Administration
System Configuration & Identity Management
Select Applications
Financial Services Analytical Applications Transactions Filt...
Financial Services Sanctions Pack
Transaction Filtering Admin
Inline Processing
Financial Services Sanctions Pack
Applications for sanctions processing
Transaction Filtering Admin
Transaction Filtering Admin Screen
Inline Processing
Inline Processing

3.2.2Object Administration Tab

The Object Administration tab allows the system administrator to search for information related to a patch or infodom.

Figure 5: Object Administration Tab


Applications
Object Administration
System Configuration & Identity Management
Select Information Domain
SANCINFO
Financial Services Analytical Applications Infrastructure
Object Administration
Utilities
Patch Information
Search
1 to 3 of 3

Financial Services Analytical Applications Infrastructure > Object Administration > Utilities > Patch Information

Patch Information
Patch Information

Patch or Application Name:
Information Domain:

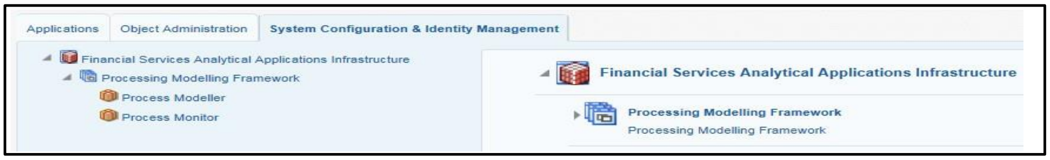
Patch Information

Patch or Application Name	Applied Date	Information Domain	Application ID	Segment Map ID	Segment Code	Additional Information
8.0.4.0.0	02-09-2017 05:19:30	SANCINFO	OFSIPE	--	--	Financial Services Inline Processing Engine
8.0.4.0.0	02-09-2017 05:17:46	SANCINFO	TFLT	--	--	Financial Services Analytical Applications Transactions Filtering
8.0.4.0.0	02-09-2017 05:15:38	PLATFORM	PLATFORM	--	--	OFSAAI 8.0.4.0.0 Release

3.2.3System Configuration and Identity Management Tab

The System Configuration and Identity Management tab allows the System Administrator to provide the security and operational framework required for the Infrastructure. They can configure Server details, Database details, OLAP details, and Information Domains, along with other configuration processes such as segment and metadata mapping, mapping segments to securities, and rules setup. The System Configuration is a one-time activity, which helps the System Administrator make the Infrastructure system operational.

Figure 6: System Configuration and Identity Management Tab


Applications
Object Administration
System Configuration & Identity Management
Financial Services Analytical Applications Infrastructure
Processing Modelling Framework
Process Modeller
Process Monitor
Financial Services Analytical Applications Infrastructure
Processing Modelling Framework
Processing Modelling Framework

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.

3.3.2Enabling Cookies

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

3.3.3Enabling 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.

3.3.4Enabling 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.

3.3.5Setting 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.

3.3.6Enabling 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 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:

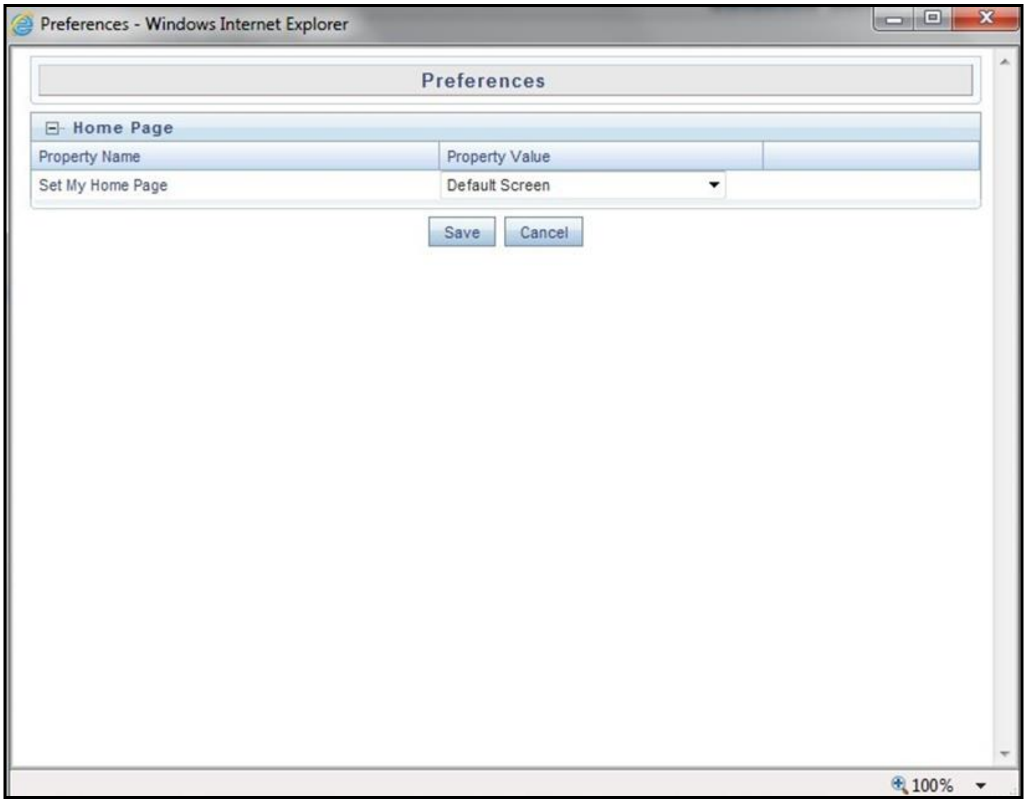
1. Navigate to the **Tools** menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Privacy** tab. In the **Pop-up Blocker** setting, select **Turn on Pop-up Blocker**. The Settings are enabled.
4. Click **Settings** to open the **Pop-up Blocker Settings** 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.

3.3.8 Setting Preferences

The Preferences section enables you to set your OFSAA Home Page. To access this section, follow these steps:

1. Click **Preferences** from the drop-down list in the top right corner, where the username is displayed. The **Preferences** page is displayed.

Figure 7: Preference screen



Property Name	Property Value
Set My Home Page	Default Screen

2. In the **Property Value** drop-down list, select the application which you want to set as the Home Page.

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

3. Click **Save** to save your preference.

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

This section allows you 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: Administration Process Flow

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 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 Oracle Financial Services Analytical Applications Infrastructure User Guide.

4.2.2Mapping a User with a User Group

This section explains how to map Users and User Groups. With this, the user has access to the 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.

MANAGING USER ADMINISTRATION

Table 4: User Group-Role Mapping

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

5 Configuring EDQ, Application and SWIFT Parameters, and SEPA Messages

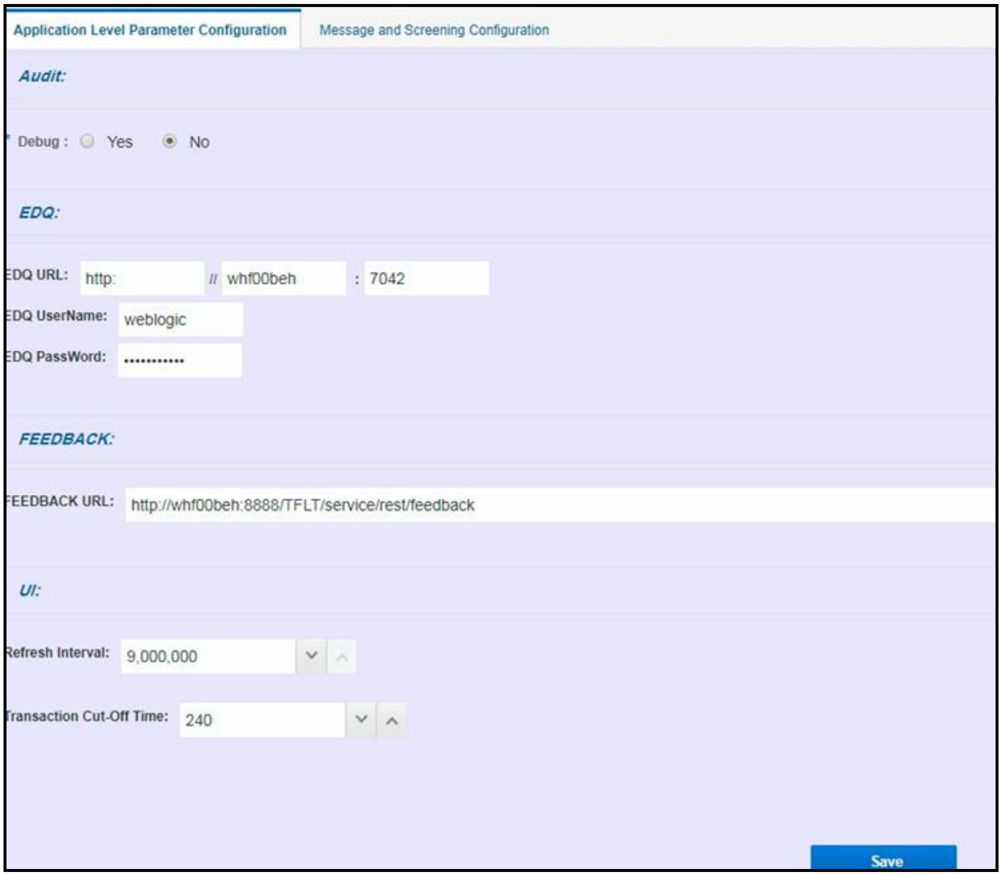
This chapter explains how to import the .dxi files into the Enterprise Data Quality (EDQ) application, run the EDQ jobs, and change the EDQ URL for the Transaction Filtering application. It also explains the steps to configure Application Parameters, SWIFT message parameters, and SEPA message parameters.

5.1 Configuring the Application Level Parameters

To configure the parameters, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** landing page.
2. Click **Transaction Filtering Admin**. The **Application Level Parameter Configuration** is displayed.

Figure 8: Application Level Parameter Configuration Tab


Application Level Parameter Configuration
Message and Screening Configuration
Save

Audit:

* Debug : ○ Yes ● No

EDQ:

EDQ URL: http: // whf00beh : 7042

EDQ UserName: weblogic

EDQ PassWord: ••••••••••••

FEEDBACK:

FEEDBACK URL: http://whf00beh:8888/TFLT/service/rest/feedback

UI:

Refresh Interval: 9,000,000

Transaction Cut-Off Time: 240

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 Appendix B: System Audit Logging Information.

4. 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 user name**: 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.
5. 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.
6. 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.

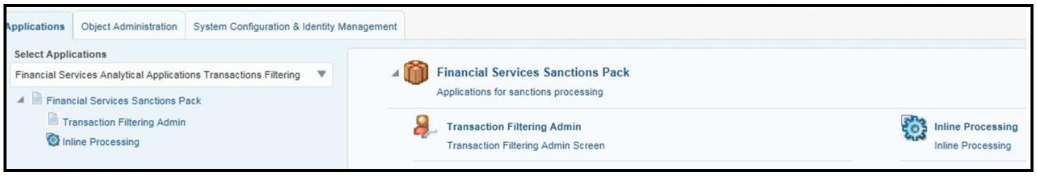
7. Click **Save**. The following confirmation message is displayed**: Records Updated Successfully**.

5.2 Configuring the SWIFT Message Parameters

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

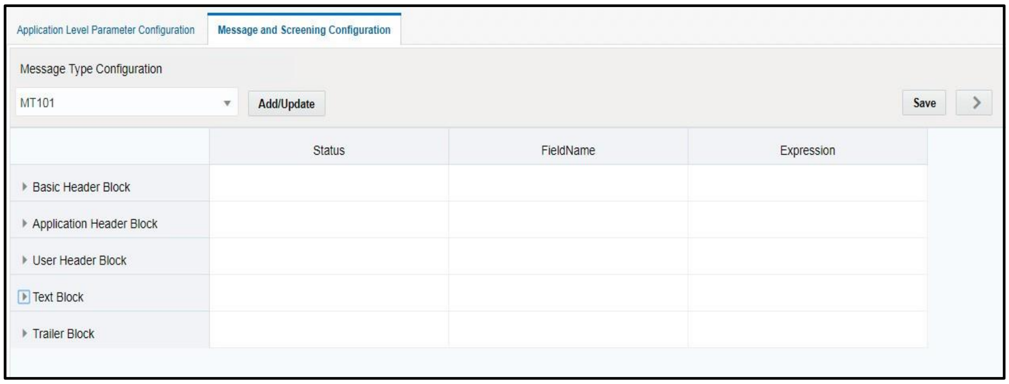
1. Navigate to the **Oracle Financial Services Sanctions application** home page.
2. On the right pane, click **Transaction Filtering Admin**.

Figure 9: Application Level Parameter Configuration Tab


Applications
Object Administration
System Configuration & Identity Management
Select Applications
Financial Services Analytical Applications Transactions Filtering
Financial Services Sanctions Pack
Transaction Filtering Admin
Inline Processing
Financial Services Sanctions Pack
Applications for sanctions processing
Transaction Filtering Admin
Transaction Filtering Admin Screen
Inline Processing
Inline Processing

To view the SWIFT message parameters, select the **Message and Screening Configuration** tab.

Figure 10: Message and Screening Configuration Tab


Application Level Parameter Configuration
Message and Screening Configuration
Add/Update
Save
>

Message Type Configuration: MT101

	Status	FieldName	Expression
Basic Header Block			
Application Header Block			
User Header Block			
Text Block			
Trailer Block			

5.2.1 Message Type Configuration Screen

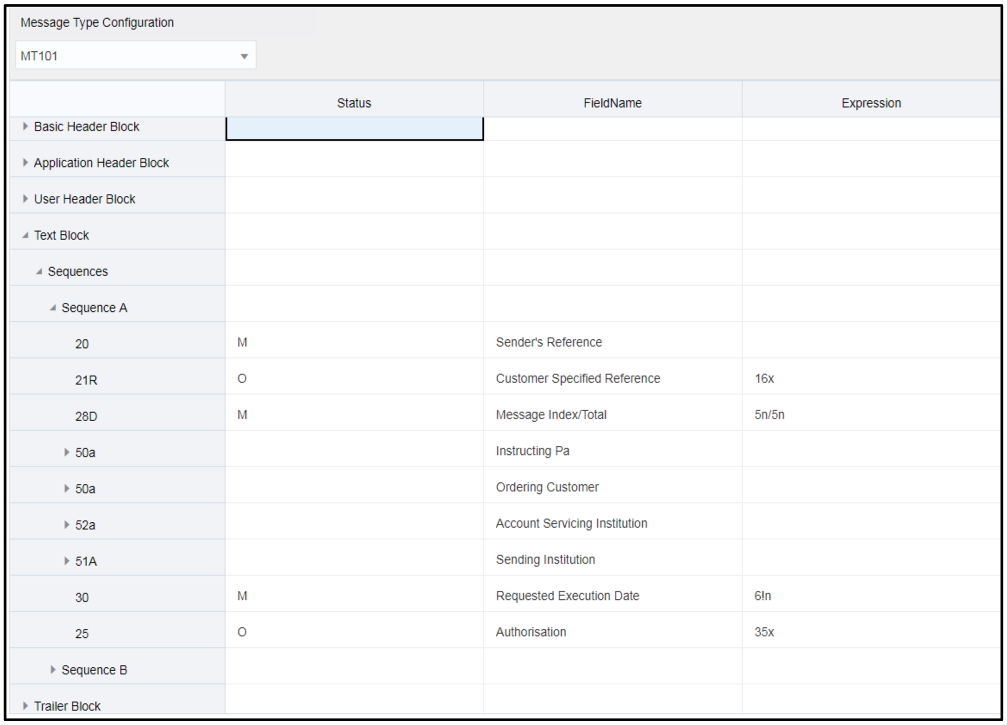
This screen allows you to edit the status, field names, and expressions of the different parameters in the message.

In the Message Type Configuration field, select the SWIFT message format. The following formats are supported:

- MT101
- MT 110
- MT103
- MT202
- MT202 COV

Each message format has four blocks: Basic Header Block, Application Header Block, User Header Block, and Text Block. The fields in the first three blocks remain the same regardless of the message format. The fields in the Text Block may change depending on the message format.

Figure 11: Message Type Configuration Screen



Message Type Configuration

MT101

	Status	FieldName	Expression
Basic Header Block			
Application Header Block			
User Header Block			
Text Block			
Sequences			
Sequence A			
20	M	Sender's Reference	
21R	O	Customer Specified Reference	16x
28D	M	Message Index/Total	5n/5n
50a		Instructing Pa	
50a		Ordering Customer	
52a		Account Servicing Institution	
51A		Sending Institution	
30	M	Requested Execution Date	6!n
25	O	Authorisation	35x
Sequence B			
Trailer Block			

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 particular 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.

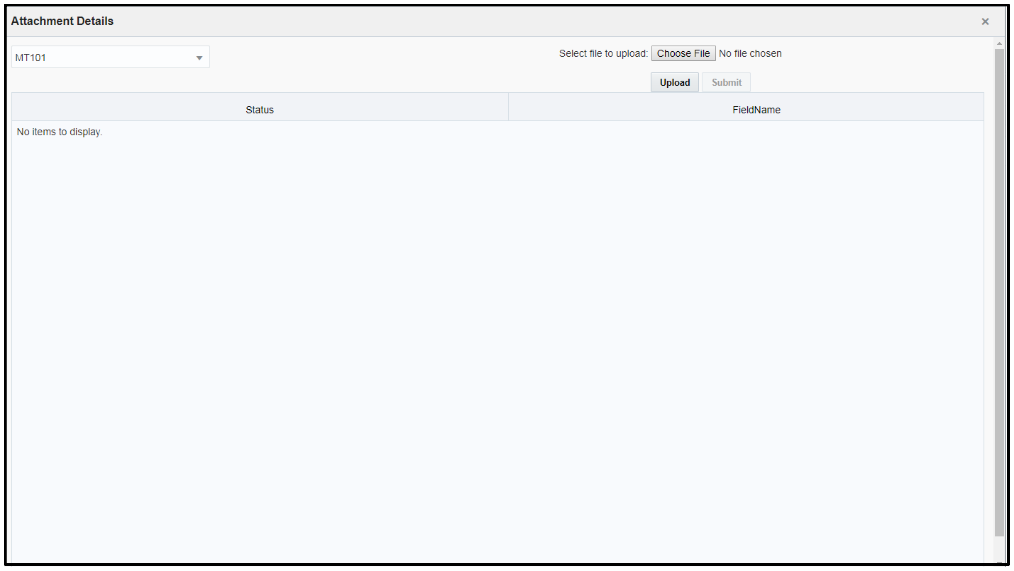
To edit a parameter, click the parameter name. After you make the changes, click **Save**.

5.2.1.1 Adding a New Message Type

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

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 12: Attachment Details Window



Attachment Details

MT101

Select file to upload: Choose File No file chosen

Status	FieldName

No items to display.

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`.

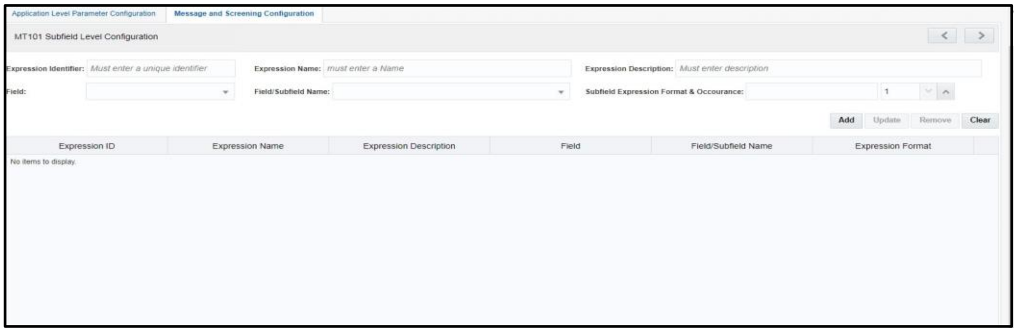
4. Click **Upload**.
5. Click **Submit**. The message is displayed in the following table as *<Message Type_draft>*.

For more information on the JSON format, see Structure of a JSON.

5.2.2 <Message Type> Subfield Level Configuration Screen

This screen allows you to add a subfield to a field in the Message Type Configuration Screen.

Figure 13: <Message Type> Subfield Level Configuration Screen



Application Level Parameter Configuration | Message and Screening Configuration

MT101 Subfield Level Configuration

Expression Identifier: *Must enter a unique identifier*
Expression Name: *must enter a Name*
Expression Description: *Must enter description*
Field:
Field/Subfield Name:
Subfield Expression Format & Occourance: 1

Expression ID	Expression Name	Expression Description	Field	Field/Subfield Name	Expression Format

No items to display.

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

Table 5: Fields in the <Message Type> Subfield Level Configuration Screen

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.
Expression Format	This field is populated when the Field is selected. Select an expression as it as or an element from that expression.
Expression Occurrence	Enter the number of occurrences for the expression within that message. By default, it is always 1.

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.

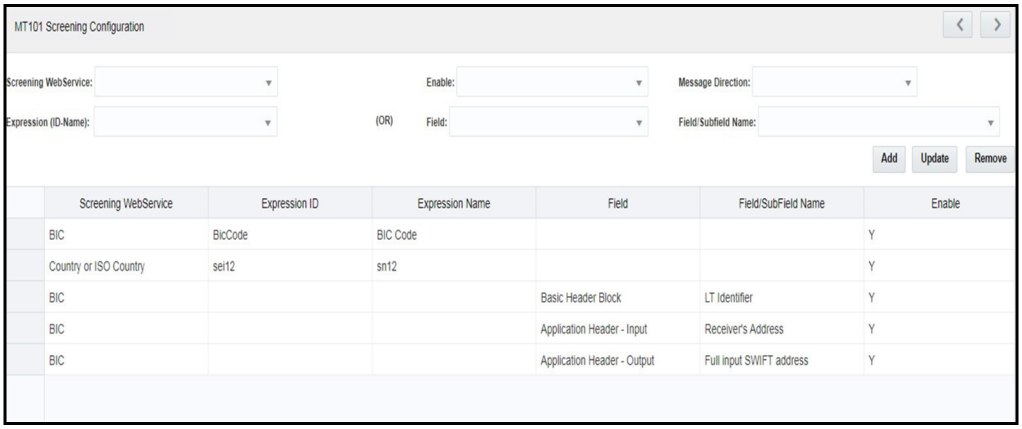
  In this example, if you want to configure the country code for `field 57,` then you can configure `2!a` from Identifier Code expression as a country code by giving unique names in the **Subfield Expression Identifier**, **Subfield Name**, and **Subfield Description** fields.

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

5.2.3 <Message Type> Screening Configuration Screen

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

Figure 14: <Message Type> Screening Configuration Screen



MT101 Screening Configuration

Screening WebService:

Enable:

Message Direction:

Expression (ID-Name):

(OR)

Field:

Field/Subfield Name:

Screening WebService	Expression ID	Expression Name	Field	Field/SubField Name	Enable
BIC	BicCode	BIC Code			Y
Country or ISO Country	sei12	sn12			Y
BIC			Basic Header Block	LT Identifier	Y
BIC			Application Header - Input	Receiver's Address	Y
BIC			Application Header - Output	Full input SWIFT address	Y

1. To add a web service, provide the required values in the fields shown above and click **Add**. Enter values in the following fields:

Table 6: Fields in the <Message Type> Subfield Level Configuration Screen

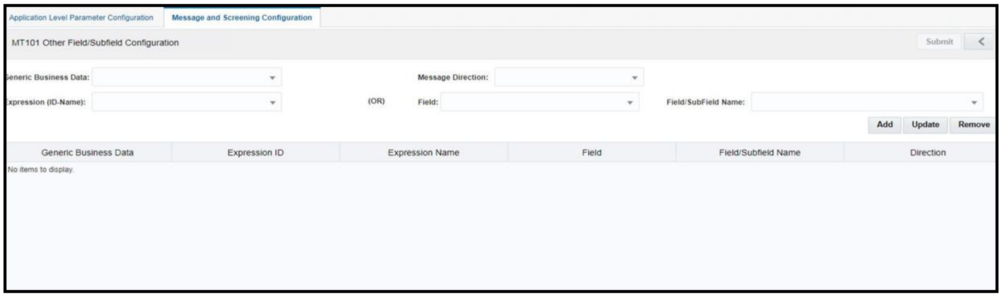
Fields	Field Description
Screening WebService	Select a Screening Webservice from the dropdown list. This field lists all the supported matching web services within the system. This is a mandatory field.
Enable	Select **Yes** to enable the WebService. Select **No** to disable the WebService.
Message Direction	Select **INBOUND(o)** and **OUTBOUND(i)** based on the screening requirement from the drop-down list. If a field has to be screened only for inbound then select INBOUND(o), otherwise select OUTBOUND(i). If that field must be screened for both inbound and outbound then select ANY.
Expression (ID-Name)	Select the Expression that was defined on the previous page. This automatically displays the fields in the next two fields.
Field	If you have not selected from the previous field, then select the Field.
Field/Subfield Name	Select the Subfield Name. This displays the Expression.

2. To update an existing web service, click the name of the web service. The fields are populated with the web service parameters. Once you make the changes, click **Update**.
3. To remove an existing web service, click the name of the web service and click **Remove**.

5.2.4 <Message Type> Other Field/Subfield Configuration Screen

This screen 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 end to end forgiven any message type. You can select each business data to configure the source of data/fields for a given message type based on SWIFT knowledge.

Figure 15: <Message Type> Other Field/Subfield Configuration Screen


Application Level Parameter Configuration
Message and Screening Configuration
MT101 Other Field/Subfield Configuration
Submit
<
Generic Business Data:
Message Direction:
Expression (ID-Name):
(OR)
Field:
Field/SubField Name:
Add
Update
Remove

Generic Business Data	Expression ID	Expression Name	Field	Field/Subfield Name	Direction

No items to display.

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

Table 7: Fields in the <Message Type> Other Field/Subfield Configuration Screen

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.

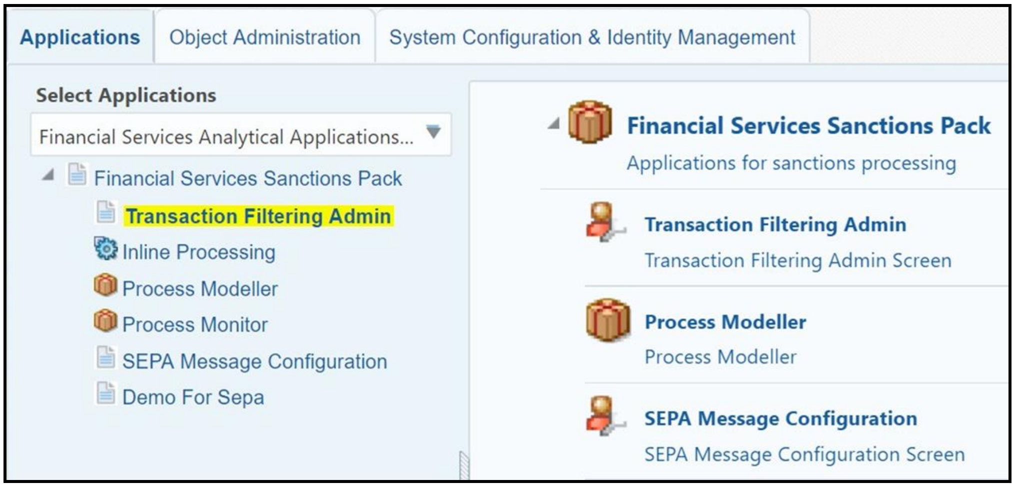
Once you make the changes, click **Update**.

5.3 Configuring the SEPA Message Parameters

To configure the SEPA message parameters, follow these steps:

1. Navigate to the **Oracle Financial Services Sanctions application** home page.
2. On the right pane, click **SEPA Message Configuration**. The **Configuration** screen appears.

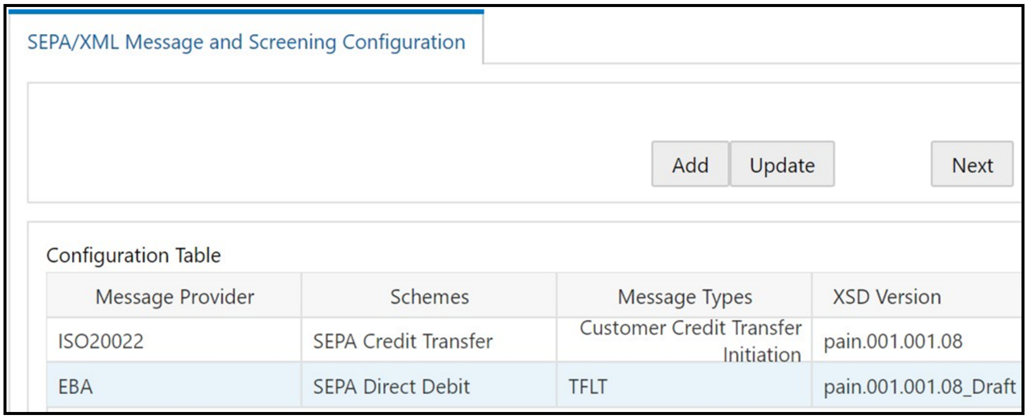
Figure 16: Configuring the SEPA Message Parameters


Applications
Object Administration
System Configuration & Identity Management
Select Applications
Financial Services Analytical Applications...
Financial Services Sanctions Pack
Transaction Filtering Admin
Inline Processing
Process Modeller
Process Monitor
SEPA Message Configuration
Demo For Sepa
Financial Services Sanctions Pack
Applications for sanctions processing
Transaction Filtering Admin
Transaction Filtering Admin Screen
Process Modeller
Process Modeller
SEPA Message Configuration
SEPA Message Configuration Screen

3. To add SEPA parameters, click **Add**.
4. Select the message provider and related scheme and message type for the SEPA parameter.
5. Upload one or more .XSD files.

   Once you click **Upload**, the basic elements related to the file appear. To view all elements, click **Search Elements** and select the parent element/child element combination from the dropdown list, for example, `Pst- lAdr/TwnNm`.
6. Click **Submit**. The SEPA parameter name appears on the Configuration screen with `_Draft` attached to the parameter name.

Figure 17: SEPA Parameter Name on Configuration Screen



Configuration Table

Message Provider	Schemes	Message Types	XSD Version
ISO20022	SEPA Credit Transfer	Customer Credit Transfer Initiation	pain.001.001.08
EBA	SEPA Direct Debit	TFLT	pain.001.001.08_Draft

7. To update the SEPA parameter message details, click the parameter name and then click **Update**.
8. To configure the SEPA parameter screening details, click the parameter name and then click Next. This screen allows you to:
   a. View the `Xpath` of the `.XSD` file.

b. Update the `Xpath` of the `.XSD` file in the Tree section. To do this, expand the section by clicking ▶, selecting the new parent element/child element combination from the dropdown list, and then clicking **Update**.

c. Select the screening webservice applicable to the SEPA parameter. You can also enable all the screening web services by clicking **Enable All**, or you can disable all screening web services by clicking **Disable All**.

d. Select the applicable message direction for the screening webservice (inbound or outbound).

e. Enable or disable the screening webservice

9. To view these details in the **Screening Configuration** section, click **Add**.

10. View the parameter screening details in the Screening Configuration section. Here, you can:

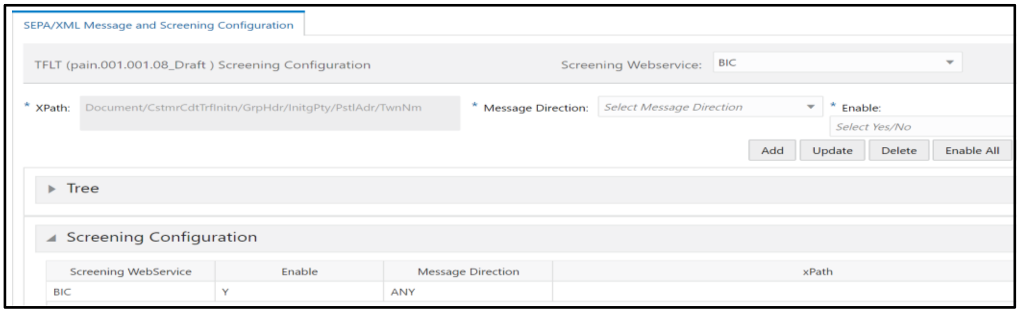
    a. Add a webservice by clicking **Add**.

    b. Update the webservice details by clicking **Update**.

    c. Delete a webservice by clicking **Delete**.

11. To perform these functions, you must first select the screening webservice row and then click the required button.

Figure 18: SEPA Parameter - Screening Configuration



TFLT (pain.001.001.08_Draft) Screening Configuration

Screening Webservice: BIC

* XPath: Document/CstmrCdtTrfInitn/GrpHdr/InitgPty/PstlAdr/TwnNm

* Message Direction: Select Message Direction

* Enable: Select Yes/No

Screening Configuration

Screening WebService	Enable	Message Direction	xPath
BIC	Y	ANY	

12. To configure the field and subfield level details of the SEPA parameter, click Next. This screen allows you to:

    a. View the `Xpath` of the `.XSD` file.

    b. Update the `Xpath` of the `.XSD` file in the Tree section. To do this, expand the section by clicking ▶, selecting the new parent element/child element combination from the dropdown list, and then clicking **Update**.

13. Select the applicable message direction for the screening webservice (inbound or outbound). To view these details in the Field/Subfield Configuration section, click Add.

14. View the field and subfield level details in the Field/Subfield Configuration section. Here, you can:

    a. Add a webservice by clicking **Add**.

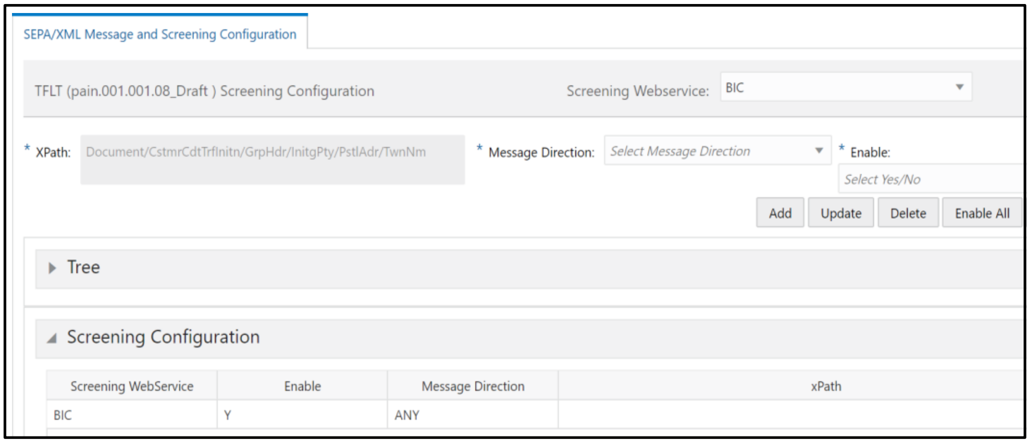
    b. Update the webservice details by clicking **Update**.

    c. Delete a webservice by clicking **Delete**.

15. To perform these functions, you must first select the screening webservice row and then click the required button.

16. Click **Submit**. The SEPA parameter name is updated on the Configuration screen with `_Draft` removed.

Figure 19: SEPA Parameter - Screening Configuration



TFLT (pain.001.001.08_Draft) Screening Configuration

Screening Webservice: BIC

* XPath: Document/CstmrCdtTrfInitn/GrpHdr/InitgPty/PstlAdr/TwnNm

* Message Direction: Select Message Direction

* Enable: Select Yes/No

Screening WebService	Enable	Message Direction	xPath
BIC	Y	ANY	

6 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

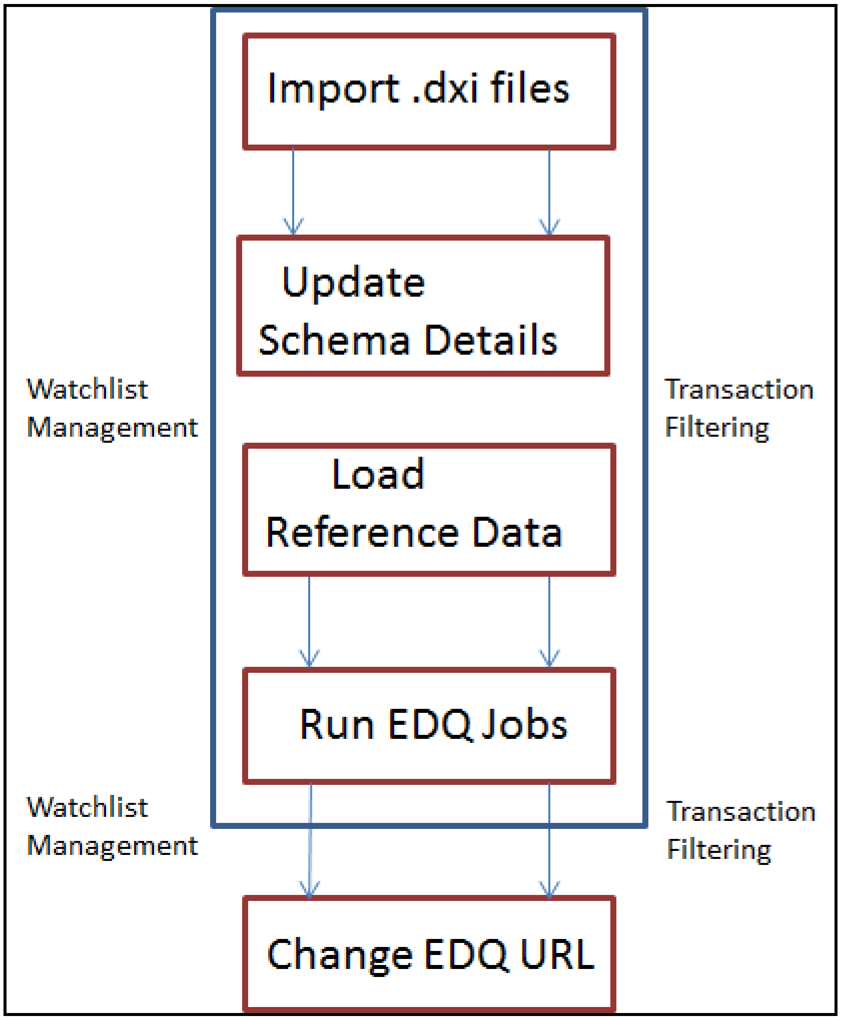
For information on configuring a host in the Transaction Filtering application, see Host Configuration.

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

6.1 EDQ Configuration Process Flow

The following image shows the EDQ configuration process flow:

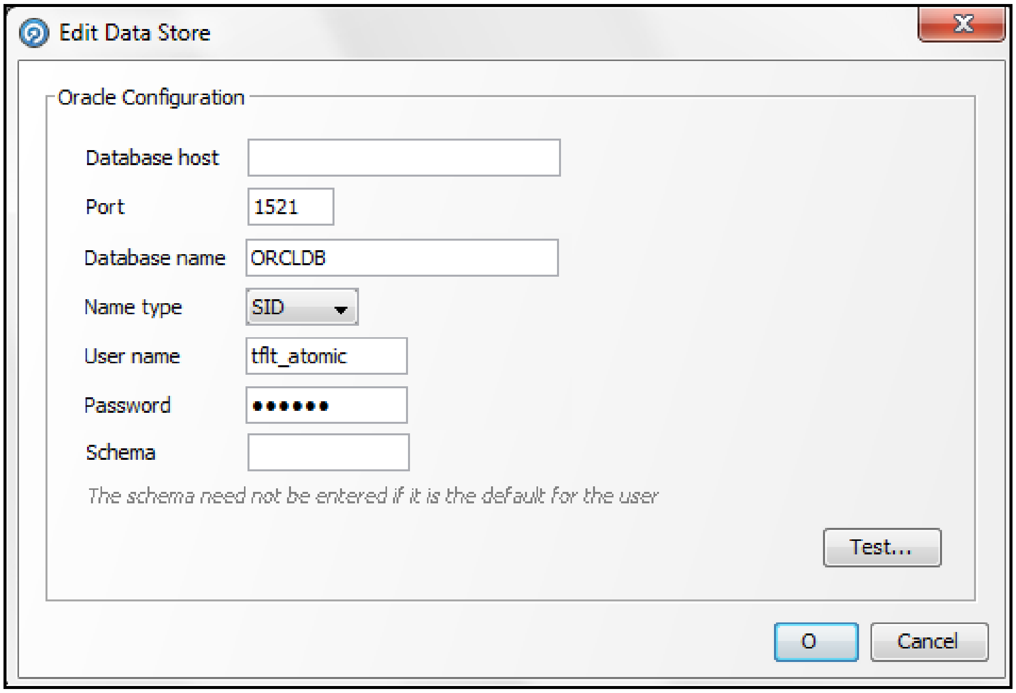
Figure 20: Enterprise Data Quality (EDQ) Configuration Steps



To configure the EDQ, follow these steps:

1. Import the Transaction List management and Transaction screening .dxi files from the `FIC_HOME/Transaction_Processing` path.
2. Enter the organization-specific Atomic schema details as shown:

Figure 21: Edit Data Store Window



Edit Data Store

Oracle Configuration

Database host:

Port: 1521

Database name: ORCLDB

Name type: SID

User name: tflt_atomic

Password: ●●●●●●

Schema:

The schema need not be entered if it is the default for the user

3. Load the Reference data.
4. Run the following jobs under the **Transaction List management** project:
    - Analyze Reference data quality
    - Download Prepare & filter export list data
    - Generate StopPhrases
5. Run the **Transaction Filtering** job under the **Transaction Screening** project.
6. Change the EDQ URL in the Transaction Filtering application.

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

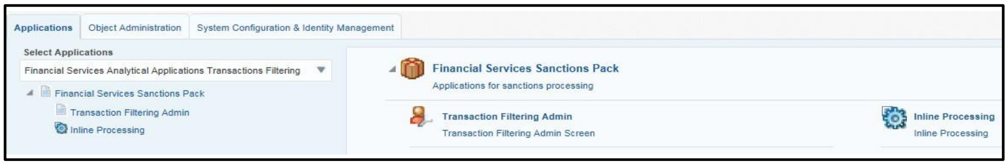
7. Configure the message and screening parameters, if required.

6.2 Changing the EDQ URL

To change the EDQ URL, follow these steps:

1. Navigate to the **Oracle Financial Services Sanctions application** home page.
2. On the right pane, click **Transaction Filtering Admin**.

Figure 22: Changing the EDQ URL


Applications
Object Administration
System Configuration & Identity Management
Select Applications
Financial Services Analytical Applications Transactions Filtering
Financial Services Sanctions Pack
Transaction Filtering Admin
Inline Processing
Financial Services Sanctions Pack
Applications for sanctions processing
Transaction Filtering Admin
Transaction Filtering Admin Screen
Inline Processing
Inline Processing

3. To view the application parameters, select the **Application Parameters Configuration** tab.
4. In the Debug field, 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. For more information on the values in the **Status** column, see Appendix B: System Audit Logging Information.
5. In the **EDQ ReST URL** field, enter the URL.
6. Enter the EDQ UserName and the EDQ PassWord.
7. Click **Save**. The following confirmation message is displayed: Records Updated Successfully.

6.3 General EDQ Configurations

The following sections mention the general EDQ configurations.

6.3.1 Importing the OFS Transaction Filtering Projects

See the *Importing the OFS Customer Screening and OFS Transaction Filtering Projects* section in the Oracle Financial Services Sanctions Installation Guide to import OFS Transaction Filtering projects.

6.3.2Configuring 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 several 'override' configuration settings for externalized options when a Job is run. They offer a convenient way of saving and reusing several 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 UI.

The *watchlist-management.properties* Run Profile controls:

- which watch lists are downloaded, and the configuration of the download process;
- whether filtering is applied to the watch lists; and

- whether Data Quality Analysis is applied to the watch lists. Additionally, the *watchlist-screening.properties* Run Profile controls:
- Real-Time and Batch Screening set up;
- Screening reference ID prefixes and suffixes;
- Watch list routing; and
- configuration of match rules.

The properties controlling match rules are not included in the watchlist-screening.properties Run Profile by default.

6.3.2.1 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 Watchlist
- Dow Jones Anti-Corruption List
- Accuity

Additionally, you can optionally supply reference data from your private watch list using the Private List Interface (PLI) values in the `watchlist-management.properties` Run Profile control which lists are used and how they are downloaded, staged and filtered (or not).

Watch lists can be downloaded automatically (by setting the appropriate values in the Run Profile) or manually (by navigating to the list provider's web site, downloading the list, and saving it to the matching sub-folder in the Landing Area). The staging value must be set to **Y** the first time a watch list is downloaded. Thereafter, leave it set to **Y** to refresh the staged data every time a download is performed, or N to preserve the pre-existing staged data

NOTE

- All downloaded watch lists must be set to filtered or unfiltered.
- The Accuity, Dow Jones, Dow Jones Anti-Corruption, and World-Check lists are all provided as paid services. To use one of these watch lists it is necessary to apply to the individual list providers for an account. Please refer to the relevant provider websites for further information.
- The option to download private watch lists is not supplied, as it is assumed that this data will be available in-house.

For specific configuration information on each of these watch lists, see Appendix A: Watch Lists.

Oracle financial services Customer Screening is pre-configured to work with commercially available and government-provided watch lists. However, you can also screen data against your private watch lists. Sample private watch lists are provided in the `config/landingarea/Private` directory 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.

6.3.2.1.1 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 `watch list-management.properties` run profile:

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

stageddata.ACY_All.visible = Y

stageddata.ACY_Sources.visible = Y
```

6.3.2.1.2 Configuring Match Rules

Match rules and match clusters can be configured and controlled by adding a property to the `watch list-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 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** Ensure that values are capitalized and characters are escaped as applicable.

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.

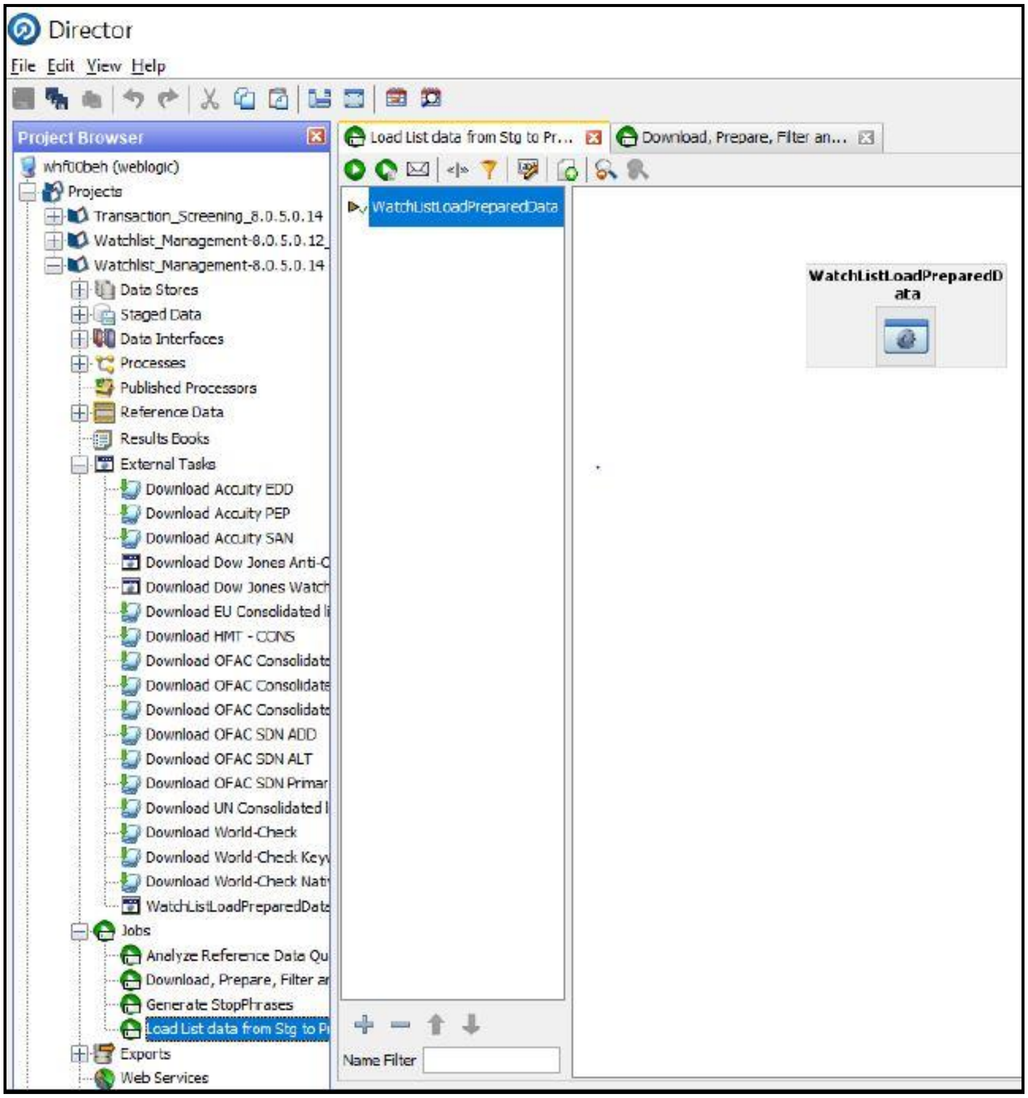
6.3.2.1.3 Configuring Jobs

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 23: EDQ Director Menu



2. Right-click the **WatchListLoadPreparedData** process and click **Enabled**.

6.3.2.2 Filtering Watch List Data

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

6.3.2.2.1 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**.

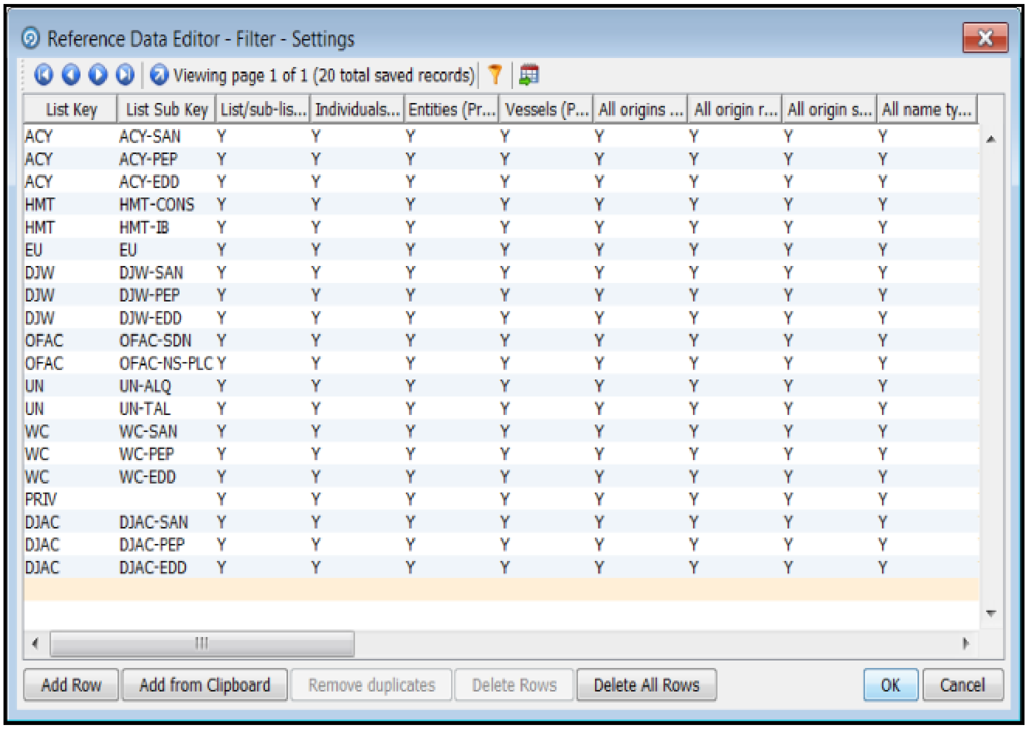
6.3.2.2.2 Configuring Watch List Filtering

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 **Watch List Management** project, even if the **Transaction Filtering** 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 24: Reference Data Editor - Filter - Settings Window



Reference Data Editor - Filter - Settings
Viewing page 1 of 1 (20 total saved records)
Add Row
Add from Clipboard
Remove duplicates
Delete Rows
Delete All Rows
OK
Cancel

List Key	List Sub Key	List/sub-lis...	Individuals...	Entities (Pr...	Vessels (P...	All origins ...	All origin r...	All origin s...	All name ty...
ACY	ACY-SAN	Y	Y	Y	Y	Y	Y	Y	Y
ACY	ACY-PEP	Y	Y	Y	Y	Y	Y	Y	Y
ACY	ACY-EDD	Y	Y	Y	Y	Y	Y	Y	Y
HMT	HMT-CONS	Y	Y	Y	Y	Y	Y	Y	Y
HMT	HMT-IB	Y	Y	Y	Y	Y	Y	Y	Y
EU	EU	Y	Y	Y	Y	Y	Y	Y	Y
DJW	DJW-SAN	Y	Y	Y	Y	Y	Y	Y	Y
DJW	DJW-PEP	Y	Y	Y	Y	Y	Y	Y	Y
DJW	DJW-EDD	Y	Y	Y	Y	Y	Y	Y	Y
OFAC	OFAC-SDN	Y	Y	Y	Y	Y	Y	Y	Y
OFAC	OFAC-NS-PLC	Y	Y	Y	Y	Y	Y	Y	Y
UN	UN-ALQ	Y	Y	Y	Y	Y	Y	Y	Y
UN	UN-TAL	Y	Y	Y	Y	Y	Y	Y	Y
WC	WC-SAN	Y	Y	Y	Y	Y	Y	Y	Y
WC	WC-PEP	Y	Y	Y	Y	Y	Y	Y	Y
WC	WC-EDD	Y	Y	Y	Y	Y	Y	Y	Y
PRIV		Y	Y	Y	Y	Y	Y	Y	Y
DJAC	DJAC-SAN	Y	Y	Y	Y	Y	Y	Y	Y
DJAC	DJAC-PEP	Y	Y	Y	Y	Y	Y	Y	Y
DJAC	DJAC-EDD	Y	Y	Y	Y	Y	Y	Y	Y

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.

6.3.2.2.3 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 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.

6.3.2.2.4 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 **Watch List Management** project.

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

6.3.2.2.5 Filtering World-Check Data

This example describes configuring filtering on the World-Check Sanctions list in the **Watch List Management** project and setting further filters in the **Transaction Filtering** 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.

6.3.2.3 Setting Filtering options in the Run Profiles

In the `watch list-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 `watch list-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
```

6.3.2.3.1 Setting Primary Filters and Linked Profiles in the Watch List Management Project

To set the primary filters, follow these steps:

1. In the `Director` menu, open the `Watch List 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.

6.3.2.3.2 Setting Secondary Filters in the Transaction Filtering Project

To set secondary filters, follow these steps:

1. Open the `Transaction Filtering` 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.

6.3.2.3.3 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 `watch list-screening.properties` Run Profile to **Y**.

6.3.2.4 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`

6.3.2.4.1 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 8: 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

6.3.2.4.2 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 9: 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

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

6.3.2.4.3 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 10: 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

Record ID	Country	ISO Country Code	Country Synonyms	Data Source	Risk Score
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

6.3.2.4.4 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 11: 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

6.3.2.4.5 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 12: 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

6.3.2.4.6 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 13: 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

6.3.2.5 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.

6.4 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

6.4.1 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
```

6.4.2 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
```

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

Alerts are segregated based on the following two dimensions:

- Jurisdiction
- Business Unit/ Line of Business

6.4.3 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.

6.4.4 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.

6.4.4.1 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 14: 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 15: 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.

7 Configuring Risk Scoring Rules

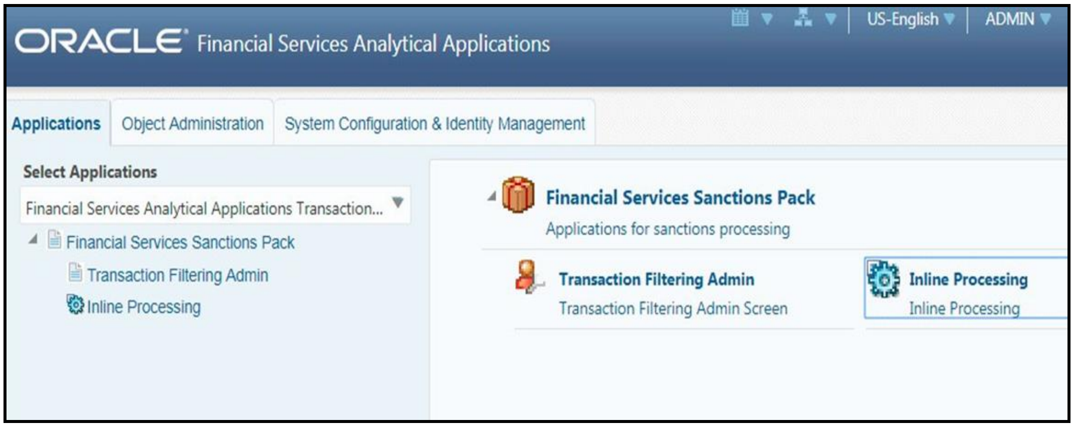
This chapter provides a brief overview of configuring Risk Scoring Rules for Transaction Filtering. These rules are configured in the Inline Processing Engine (IPE). Transaction Filtering has a few ready-to-use business rules. The following steps show the pre-configured business rules and how you can 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** landing page. For more information, see the Inline Processing Menu.

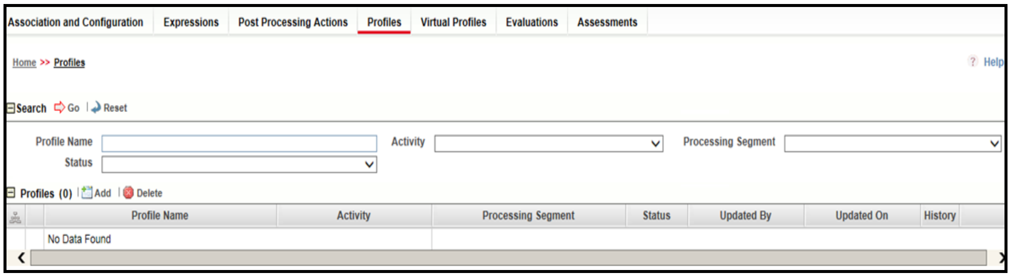
Figure 25: Sanctions Applications Pack Admin Home Page


ORACLE Financial Services Analytical Applications
US-English
ADMIN
Applications
Object Administration
System Configuration & Identity Management
Select Applications
Financial Services Analytical Applications Transaction...
Financial Services Sanctions Pack
Transaction Filtering Admin
Inline Processing
Financial Services Sanctions Pack
Applications for sanctions processing
Transaction Filtering Admin
Transaction Filtering Admin Screen
Inline Processing
Inline Processing

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 26: Profiles Menu



Profile Name	Activity	Processing Segment	Status	Updated By	Updated On	History
No Data Found						

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 Oracle Financial Services 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**.

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

Table 16: 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.

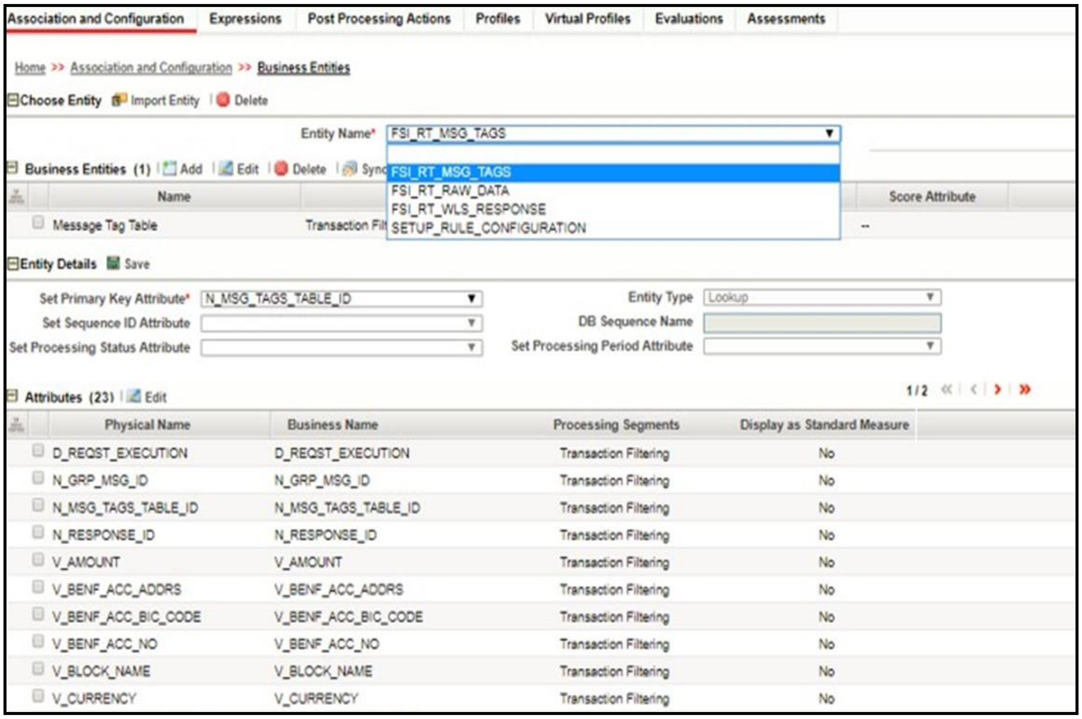
Field	Description
Set Primary Key Attribute	Select the **Primary Key Attribute** from the drop-down list. This shows all the columns of the table. This is a unique attribute of the table which is imported. It is a mandatory field. Composite Primary Keys are not supported.
Set Sequence ID Attribute	Select 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 27: Add a Business Entity



Entity Name* FSI_RT_MSG_TAGS

- FSI_RT_MSG_TAGS
- FSI_RT_RAW_DATA
- FSI_RT_WLS_RESPONSE
- SETUP_RULE_CONFIGURATION

Name		Score Attribute
Message Tag Table	Transaction Fil	--

Set Primary Key Attribute* N_MSG_TAGS_TABLE_ID
Set Sequence ID Attribute
Set Processing Status Attribute
Entity Type Lookup
DB Sequence Name
Set Processing Period Attribute

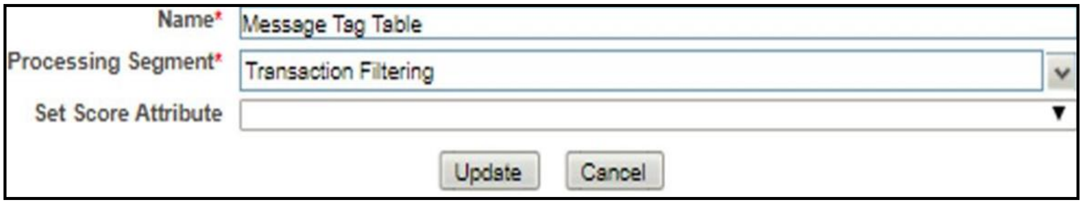
Physical Name	Business Name	Processing Segments	Display as Standard Measure
D_REQST_EXECUTION	D_REQST_EXECUTION	Transaction Filtering	No
N_GRP_MSG_ID	N_GRP_MSG_ID	Transaction Filtering	No
N_MSG_TAGS_TABLE_ID	N_MSG_TAGS_TABLE_ID	Transaction Filtering	No
N_RESPONSE_ID	N_RESPONSE_ID	Transaction Filtering	No
V_AMOUNT	V_AMOUNT	Transaction Filtering	No
V_BENF_ACC_ADDRS	V_BENF_ACC_ADDRS	Transaction Filtering	No
V_BENF_ACC_BIC_CODE	V_BENF_ACC_BIC_CODE	Transaction Filtering	No
V_BENF_ACC_NO	V_BENF_ACC_NO	Transaction Filtering	No
V_BLOCK_NAME	V_BLOCK_NAME	Transaction Filtering	No
V_CURRENCY	V_CURRENCY	Transaction Filtering	No

b. 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>`.

c. Click **Add**.

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

Figure 28: Business Entity attributes



Name* Message Tag Table
Processing Segment* Transaction Filtering
Set Score Attribute

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:

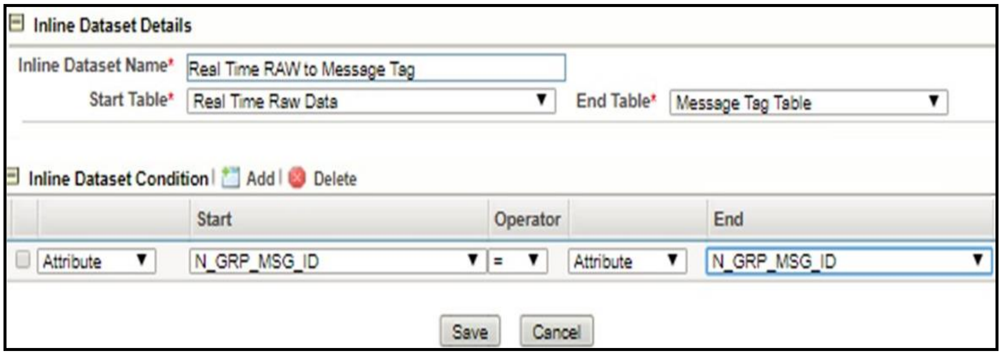
   a. On the **Inline Datasets** page, click **Add**.

   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 29: Inline Datasets Attributes



Inline Dataset Name*: Real Time RAW to Message Tag
Start Table*: Real Time Raw Data
End Table*: Message Tag Table

		Start	Operator		End
□	Attribute	N_GRP_MSG_ID	=	Attribute	N_GRP_MSG_ID

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 Oracle Financial Services 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.

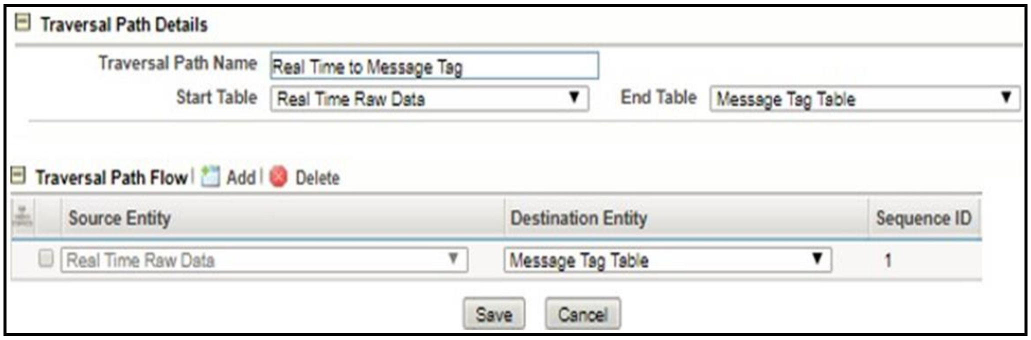
   b. On the **Traversal Paths** page, click **Add**.

   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 30: Traversal Paths Attributes



Traversal Path Name: Real Time to Message Tag
Start Table: Real Time Raw Data
End Table: Message Tag Table

	Source Entity	Destination Entity	Sequence ID
□	Real Time Raw Data	Message Tag Table	1

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 Oracle Financial Services 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

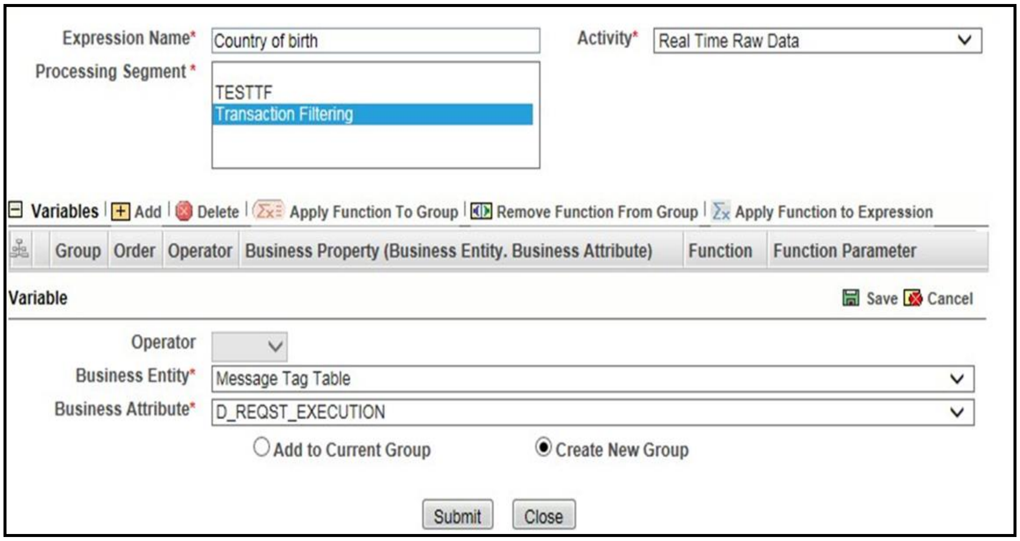
   To add an expression, follow these steps:

   a. Click the **Expressions** menu.

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

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

Figure 31: First Expression Attributes



Expression Name*: Country of birth
Activity*: Real Time Raw Data
Processing Segment*: TESTTF / Transaction Filtering (selected)

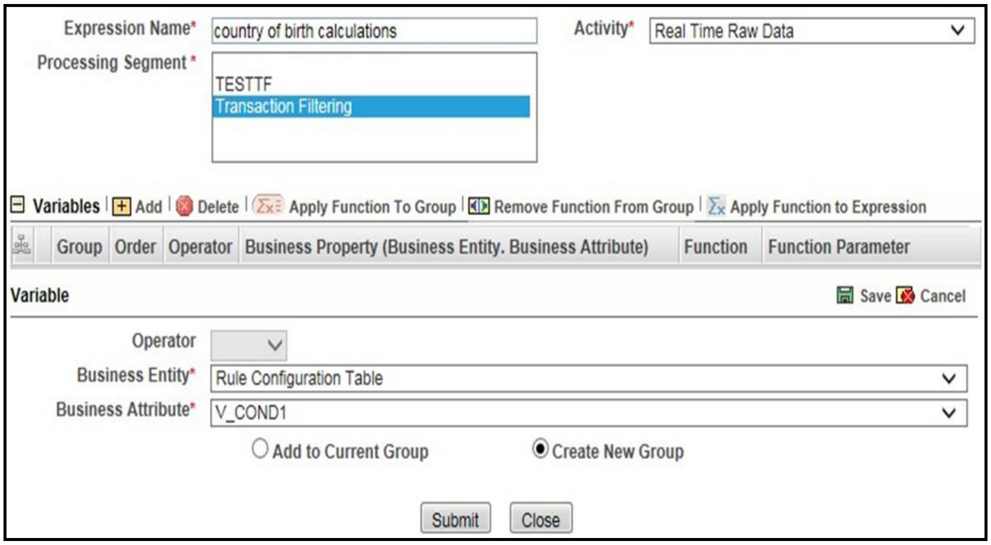
Operator:
Business Entity*: Message Tag Table
Business Attribute*: D_REQST_EXECUTION
○ Add to Current Group ● Create New Group

   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.

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

Figure 32: Second Expression Attributes



Expression Name* country of birth calculations

Activity* Real Time Raw Data

Processing Segment* TESTTF

Transaction Filtering

Group	Order	Operator	Business Property (Business Entity. Business Attribute)	Function	Function Parameter

Variable

Operator

Business Entity* Rule Configuration Table

Business Attribute* V_COND1

○ Add to Current Group ● Create New Group

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

For information on applying a function to the group or expression, see the **Managing Expressions** chapter in the Oracle Financial Services 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 Oracle Financial Services 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 17: 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 filter conditions mentioned in the following table, if the filter values are met as configured then add a risk score of 40.

Table 18: 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 19: Risk-Currency VS Amount Threshold Evaluation Filters

Sl.No	Filter Name	Filter Clause
5.	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) in ('MT101', 'MT103', 'MT202COV', 'MT202')
6.	Jurisdiction	(Real Time Raw Data:V_BIC_CODE) = 'CHASUS33XXX'
7.	Direction	(Message Tag Table:V_DIRECTION) in ('INBOUND','OUTBOUND')
8.	Currency	(Message Tag Table:V_CURRENCY) = 'USD'
9.	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 20: Risk-Currency VS Destination Country Evaluation Filters

Sl.No	Filter Name	Filter Clause
10.	Currency	(Message Tag Table:V_CURRENCY) = (Rule Configuration Table:V_COND1)
11.	Destination Country	(Message Tag Table:V_DESTINATION_CNTRY) = (Rule Configuration Table:V_COND2)
12.	Direction	(Message Tag Table:V_DIRECTION) in ('INBOUND','OUTBOUND')
13.	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) = (Rule Configuration Table:V_TXN_TYPE_CD)
14.	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 21: Risk-High Risk Destination Country Evaluation Filters

Sl.No	Filter Name	Filter Clause
15.	Amount	(Message Tag Table:V_AMOUNT) >= 10000
16.	Currency	(Message Tag Table:V_CURRENCY) = 'EUR'
17.	Destination Country	(Message Tag Table:V_DESTINATION_CNTRY) in ('TH', 'PK')
18.	Direction	(Message Tag Table:V_DIRECTION) = 'OUTBOUND'
19.	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 22: Risk-High Risk Originator Country Evaluation Filters

Sl.No	Filter Name	Filter Clause
20.	Amount	(Message Tag Table:V_AMOUNT) >= 10000
21.	Currency	(Message Tag Table:V_CURRENCY) = 'EUR'

Sl.No	Filter Name	Filter Clause
22.	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) in ('MT101', 'MT103', 'MT202COV', 'MT202')
23.	Direction	(Message Tag Table:V_DIRECTION) = 'INBOUND'
24.	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 23: Risk-Trade Amendments Evaluation Filters

Sl.No	Filter Name	Filter Clause
25.	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) = 'MT707'
26.	Direction	(Message Tag Table:V_DIRECTION) in (('INBOUND','OUTBOUND'))
27.	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 24: Watch List Score Filters

Sl.No	Filter Name	Filter Clause
28.	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
29.	Batch Run ID	(Message Data Attributes:V_BATCH_RUN_ID) = :BATCH_RUN_ID

To add an evaluation, follow these steps:

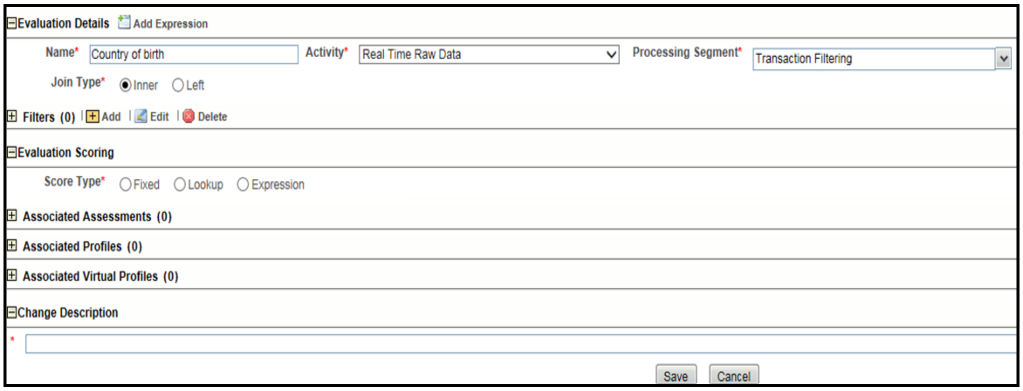
a. Click the **Evaluations** menu.

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

c. Enter a name for the evaluation.

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

Figure 33: Evaluations Attributes



⊟Evaluation Details Add Expression

Name* Country of birth Activity* Real Time Raw Data Processing Segment* Transaction Filtering

Join Type* ● Inner ○ Left

⊞ Filters (0) | Add | Edit | Delete

⊟Evaluation Scoring

Score Type* ○ Fixed ○ Lookup ○ Expression

⊞ Associated Assessments (0)

⊞ Associated Profiles (0)

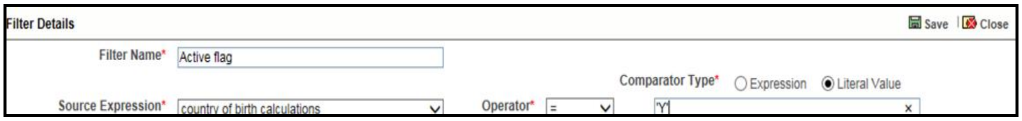
⊞ Associated Virtual Profiles (0)

⊟Change Description

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

f. Select the expression as mentioned in step f.

Figure 34: Evaluations Filters



Filter Details

Filter Name* Active flag

Comparator Type* ○ Expression ● Literal Value

Source Expression* country of birth calculations Operator* = 'Y'

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 considers 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.

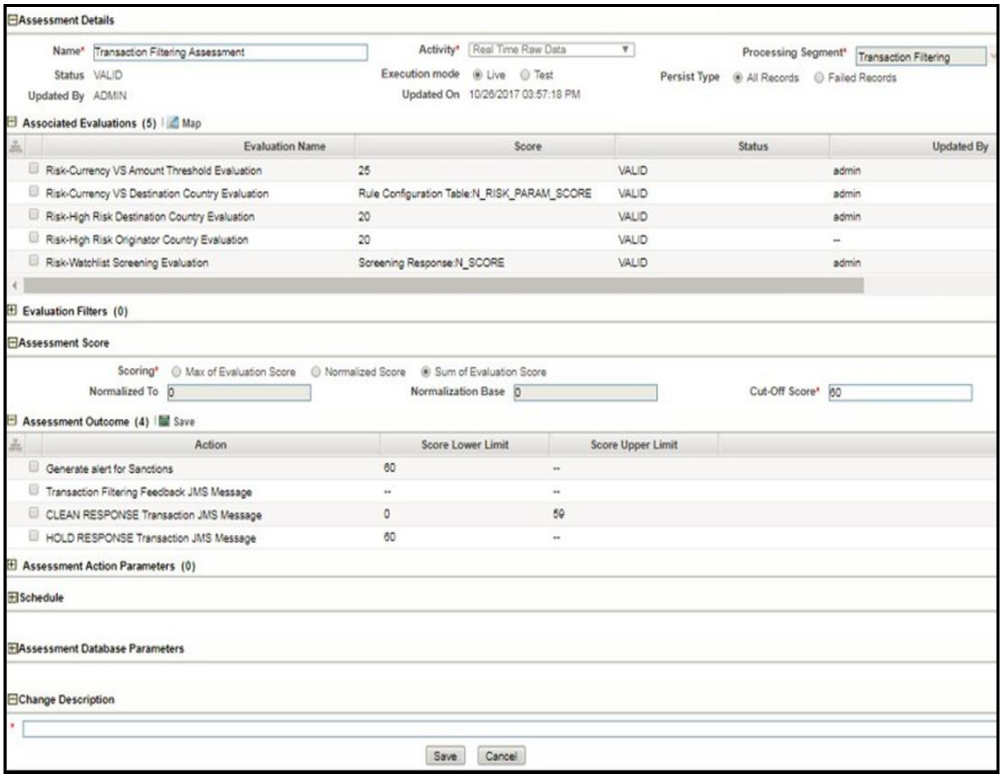
To add an Assessment, follow these steps:

a. Click the **Assessments** menu.

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

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

Figure 35: Sample Assessment



⊟Assessment Details

Name* Transaction Filtering Assessment
Status VALID
Updated By ADMIN
Activity* Real Time Raw Data
Execution mode ● Live ○ Test
Updated On 10/26/2017 03:57:18 PM
Processing Segment* Transaction Filtering
Persist Type ● All Records ○ Failed Records

⊟ Associated Evaluations (5) | Map

Evaluation Name	Score	Status	Updated By
□ Risk-Currency VS Amount Threshold Evaluation	25	VALID	admin
□ Risk-Currency VS Destination Country Evaluation	Rule Configuration Table:N_RISK_PARAM_SCORE	VALID	admin
□ Risk-High Risk Destination Country Evaluation	20	VALID	admin
□ Risk-High Risk Originator Country Evaluation	20	VALID	--
□ Risk-Watchlist Screening Evaluation	Screening Response:N_SCORE	VALID	admin

⊞ Evaluation Filters (0)

⊟Assessment Score

Scoring* ○ Max of Evaluation Score ○ Normalized Score ● Sum of Evaluation Score
Normalized To 0
Normalization Base 0
Cut-Off Score* 60

⊟ Assessment Outcome (4) | Save

Action	Score Lower Limit	Score Upper Limit
□ Generate alert for Sanctions	60	--
□ Transaction Filtering Feedback JMS Message	--	--
□ CLEAN RESPONSE Transaction JMS Message	0	59
□ HOLD RESPONSE Transaction JMS Message	60	--

⊞ Assessment Action Parameters (0)

⊞Schedule

⊞Assessment Database Parameters

⊟Change Description

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 Oracle Financial Services Inline Processing Engine User Guide.

8 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 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.

8.1 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 positional elements.

```
{
   "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. *Child* is 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"
      }
    },
    ..........
  ]
}
```

8.2 Creating JSON for SWIFT Messages with Sequences

To create a JSON, follow these steps:

1. Creating Message Elements
2. Configuring SWIFT Message Blocks

8.2.1 Creating Message Elements

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

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

8.2.2 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 Configuring the Trailer Block.

8.2.2.1 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"
      }
    },

  ]
}
```

8.2.2.2 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"
          }
        },
         ...................
      ]
    }
  ]
}
```

8.2.2.3 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"
      }
      },
    ..................
    ]
  }
```

8.2.2.4 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"
              },
                ...............
            }
          ]
        }
```

```
      ]
    }
  ]
}
```

8.2.2.5 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"
      }
    },
  ..............
  ]
}
```

8.2.3 Example of MT101 with Sequences

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

8.3 Creating JSON for SWIFT Messages without Sequences

To create a JSON, follow these steps:

1. Creating Message Elements
2. Configuring SWIFT Message Blocks

8.3.1 Creating Message Elements

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

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

8.3.2 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.

8.3.2.1 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"
      }
    },
  ..........
  ]
}
```

8.3.3 Example of MT101 without Sequences

To see examples of MT101 with sequences, see 2329509.1.

9 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.

9.1 HM Treasury Watch List

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. For more information, see the HM Treasury website.

Oracle Transaction Filtering uses the list in a semi-colon delimited form. It can be downloaded from the following location:

https://ofsistorage.blob.core.windows.net/publishlive/ConList.csv

9.2 OFAC Watch List

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. For more information, see the Treasury website.

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

9.3 EU Watch List

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. For more information, see the European Commission website.

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.

9.4 UN Watch List

The United Nations (UN) or United Nations Security Council consolidated list is a watch list that includes all individuals and entities who are subject to sanctions measures imposed by the Security Council. For more information, see the UN Security Council website.

Download the consolidated list from https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/consolidated.xml.

9.5 Private Watch List

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.

9.5.1 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 25: 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
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 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
GivenName	String	

Field Name	Expected Data Format	Notes
FamilyName	String	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.
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 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.

Field Name	Expected Data Format	Notes
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**.
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.

Field Name	Expected Data Format	Notes
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'	
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. 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.
customDate1 to customDate5		
customNumber1 to customNumber5		

9.5.2Entity 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 26: 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 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 or 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 screening (that is, an alias is a full entity name). This flag is used during matching.
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.

Field Name	Expected Data Format	Notes
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'	
DataConfidenceScore	Number, between 0 and 100	
DataConfidenceComment	String	
InactiveFlag	String	If populated, this optional field must contain either **Y** or **N**.

Field Name	Expected Data Format	Notes
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. 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.
customDate1 to customDate5	String, representing a date, in the format 'YYYYMMDD'	
customNumber1 to customNumber5	Number	

10 Appendix B: System Audit Logging Information

This appendix contains information on the logs related to the Debug and Info log files.

10.1 Activities for System Audit

The following table contains information related to the system audit activities:

Table 27: 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

10.2 Steps for System Audit Activities

The following table contains information related to the steps for the system audit activities:

Table 28: 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

Step Identifier	Activity Name	Step Name	Step Sequence	Status
2	Raw Message Processing	Raw Message persisted into structure table	2	N
3	Message Parser Processing	Raw Message parsed	1	N
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

Step Identifier	Activity Name	Step Name	Step Sequence	Status
19	Recommend to Block	NA	NA	NA
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

OFSAA Support

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

Send Us Your Comments

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

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

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the My 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 that has all the revised or recently released documents.