Oracle® Financial Services Transaction Filtering

Administration Guide

Release 8.1.2.9.0
G39141-05
July 2025

Oracle Financial Services Transaction Filtering Administration Guide, Release 8.1.2.9.0

G39141-05

Contents

4 Managing User Administration

5 General Configurations

9 Configurations for the US NACHA Batch Process

10 Enterprise Data Quality (EDQ) Configurations

11 Configuring Risk Scoring Rules

12 Simulation

A Watch Lists

B Appendix B: System Audit Logging Information

C Process Modeller Framework (PMF) Configurability

D PMF Configurations for Pool of Analyst

E Delta Watch List Configurations

F Message Categories and Message Types

G Invoking the PMF Workflow from backend

H JMS Cluster Environment Creation

I User Group Customization

J Configurations for the Bearer Token

K Function Codes for User Groups

L Setting the ZEPPELIN_INTERPETER_OUT- PUT_LIMIT in Python Interpreter

M API to Check the Status of EDQ Job

N API to Check the Sanctions Alert Status

O ISO Batch Performance Improvement

Index

Document Control

This table records the number of revisions or changes done to this document as part of a release.

Table Document Control

Version Number	Revision Date	Change Log
8.1.2.9.0	August 2025	Added a new section 8.1.3 External Attributes Screening Configuration for ISO20022 Batch
8.1.2.9.0	April 2025	Added Appendix O: ISO Batch Performance Improvement section.
8.1.2.9.0	February2025	Added Appendix N: API to Check the Sanctions Alert Status section.
8.1.2.8.0	January2025	• Updated Send Requests section. • A note is removed from the Automatic Assignments of Alerts section.
8.1.2.8.0	October 2024	Added Appendix M: API to Check the Status of EDQ Job section.
8.1.2.8.0	August2024	• Removedinformation regarding the Accuity Watchlist. • Automaticrefresh of DJW Sanction List Reference
8.1.2.7.0	February2024	• AddedSwift Message Configurations widget information in the TF Pipeline Widgets table. • Updated Pipeline Canvas figure.
8.1.2.6.0	October 2023	• Added Simulation chapter. • Added Appendix L: Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMIT in PythonInterpreter chapter. • Added the new MX message types in ISO20022 Message Types table.

Table (Cont.) Document Control

Version Number	Revision Date	Change Log
8.1.2.5.0	June2023	• Added Reviewer user role Information. • Added Adding New Message Type in NACHA section. • Added Appendix K: Function Codes for User Groups section. • Updated Configuring the Application Level Parameters section with procedure for enabling and disabling bulk action. • Added Configuring Bulk Action Feature for the Alert List section. • Added retrigger configuration parameters in Automatic Assignments of Alerts section. • Added the new MX message types in ISO20022 Message Types table. • Added Retrigger Functionality section. • Added JMSQueue Creation for SWIFT, Fedwire and ISo20022 Message Types section.
8.1.2.4.0	March2023	• Updated Configuring the Application Level Parameters section with information about Select All option for the Events Table. • Added Wire Stripping Configuration section. • Added Configuring Select All Option for the Events Table section. • Added SWIFT MX Message Types Configuration section. • Added the new MX message types in ISO20022 Message Types table. • Added Appendix J: Configurations for the Bearer Token section.

1
About This Guide

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

1.1 Intended Audience

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

- **Implementation Consultant**: Installs and configures Oracle Financial Services Transaction Filtering at a specific deployment site. The Implementation Consultant also installs and upgrades any additional Oracle Financial Services solution sets and requires access to deployment-specific configuration information (For example, machine names and port numbers).
- **System Administrator**: Configures, maintains, and adjusts the system, and is usually an employee of a specific Oracle customer. The System Administrator maintains user accounts and roles, configures the EDQ, archives data, loads data feeds, and performs post-processing tasks.

1.2 Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support (MOS). For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info Or visit https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs if you are hearing-impaired.

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

- **Configuring the SWIFT Message Parameters** describes how to configure the SWIFT message parameters.
- **Configuring the Fedwire Message Parameters** describes how to configure the Fedwire message parameters.
- **Configurations for the ISO20022 Message Parameters** describe how to configure the ISO20022 message parameters and run the ISO20022 batch.
- **Configurations for the US NACHA Batch Process** describes how to configure the US NACHA batch.
- **Enterprise Data Quality (EDQ) Configurations** describes how to configure the EDQ parameters.
- **Configuring Risk Scoring Rules** describes how to configure business rules in the Inline Processing Engine (IPE).
- **Creating a JSON** describes how to create a JavaScript Object Notation (JSON) for SWIFT messages with sequences and SWIFT messages without sequences.
- **Appendix A: Watch Lists** explains the details of each of the pre-configured watch lists that can be used by Oracle Transaction Filtering.
- **Appendix B: System Audit Logging Information** contains information on the logs related to the Debug and Info log files.
- **Appendix C: Process Modeller Framework (PMF) Configurability** describes how to configure the Process Monitor Facility (PMF) workflow.
- **Appendix D: Time Zone Configuration** describes how to set the time zone for a user.
- **Appendix E: Delta Watch List Configurations** describes how to run and download the delta updates.
- **Appendix F: Message Categories and Message Types** shows the different message types available for the SWIFT, Fedwire, ISO 20022, and US NACHA message types.
- **Appendix G: Invoking the PMF Workflow from backend** shows the different message types available for the SWIFT, Fedwire, ISO 20022, and US NACHA message types.
- **Appendix H: JMS Cluster Environment Creation** shows the different message types available for the SWIFT, Fedwire, ISO 20022, and US NACHA message types.

1.4 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.

1.5 Conventions Used in this Guide

The following table mentions the conventions used in this guide.

Table 1-1 Conventions Used in this Guide

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

2 About Oracle financial Services Transaction Filtering

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

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

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

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

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

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

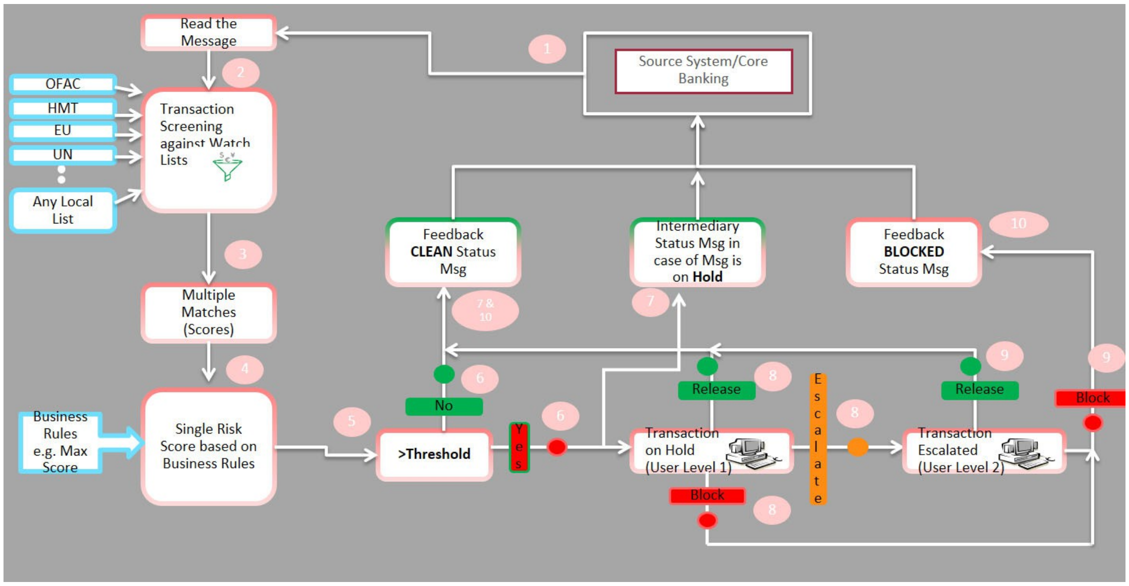
Transaction Filtering against government-regulated watch lists and internal watch lists is a key compliance requirement for financial institutions across the globe. At the turn of the century, Financial Institutions (FIs) were expected to identify customers who were either sanctioned or who lived in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

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

2.1 Transaction Filtering Workflow

The following image describes the Transaction Filtering workflow.

Figure 2-1 Transaction Filtering Workflow


Read the Message
1
Source System/Core Banking
2
OFAC
HMT
EU
UN
Any Local List
Transaction Screening against Watch Lists
3
Multiple Matches (Scores)
4
Business Rules e.g. Max Score
Single Risk Score based on Business Rules
5
>Threshold
No
6
Yes
6
Feedback CLEAN Status Msg
7 & 10
Intermediary Status Msg in case of Msg is on Hold
7
Feedback BLOCKED Status Msg
10
Release
8
Transaction on Hold (User Level 1)
Block
8
Escalate
8
Release
9
Transaction Escalated (User Level 2)
Block
9

The application first receives a message from the payment system and scans it against the watch lists, then provides a risk score for the message. If no suspicious data is found during screening, then the Transaction Filtering application sends a feedback message with the status CLEAN back to the payment system through the message queue. If suspicious data is found during screening, then the message is sent to an Analyst who investigates it using the Transaction Filtering User Interface.

Feedback is sent to the payment system through a message queue, which indicates that the message is on hold. The Analyst reviews the message, which is the first level of review and decides to release, block, or escalate the message. Based on the decision, the system sends a feedback message, either CLEAN or BLOCKED, to the payment system for the reviewed message.

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

The Senior Supervisor can perform Bulk Update (Assign alerts, set alert priority, and change the Due Date Time) and add attachments.

> **Note**
>
> As a Senior Supervisor privilege, the senior supervisor can work on a queue only if there is a backlog.

The Reviewer can view and review the messages and the alerts but cannot perform any other actions.

3
Getting Started

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

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

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

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

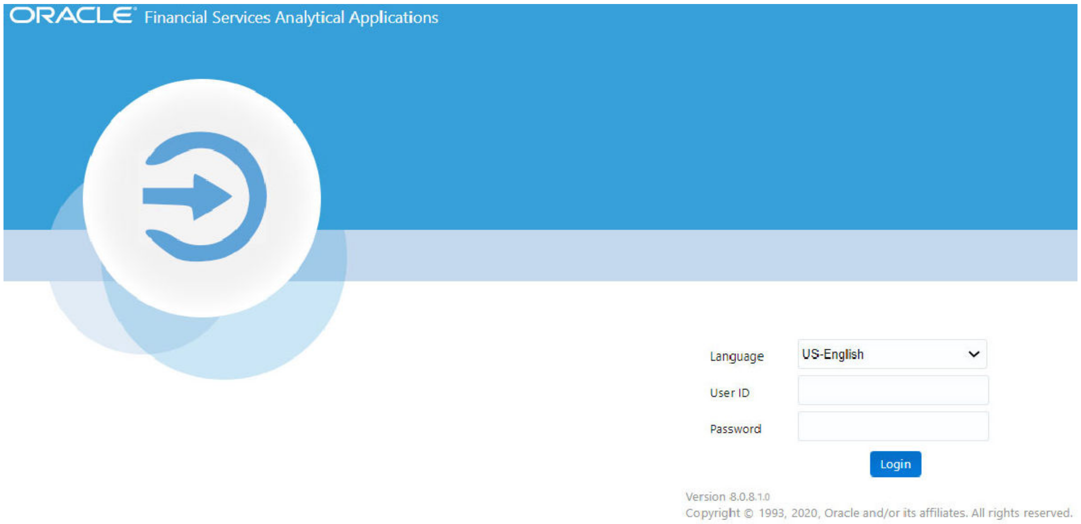
To access the **Oracle Financial Services Analytical Applications** page, follow these steps:

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

   `<scheme/ protocol>://<ip address/ hostname>:<port>/<context-name>/ login.jsp`
   For example: `https://myserver:9080/ofsaaapp/login.jsp`

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

   Figure 3-1 Oracle Financial Services Analytical Applications Login Page

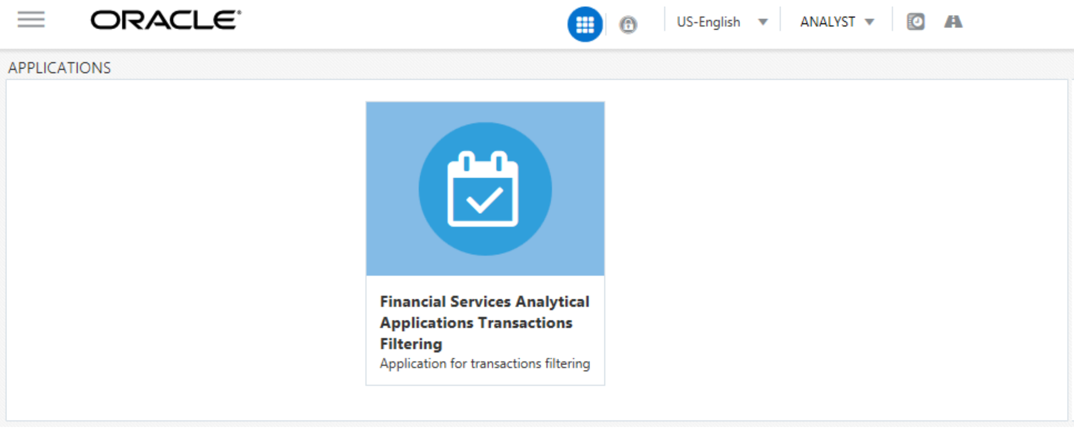
   Language: US-English

   Version 8.0.8.1.0
   Copyright © 1993, 2020, Oracle and/or its affiliates. All rights reserved.

2. Select the language from the **Language** drop-down list. This allows you to use the application in the language of your selection.

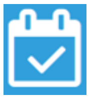
3. Enter your **User ID** and **Password** in the respective fields.
4. Click **Login**. The **Financial Services Analytical Applications Transactions Filtering** landing page is displayed.

Figure 3-2 Financial Services Analytical Applications Transactions Filtering Landing Page


ORACLE
US-English
ANALYST
APPLICATIONS
Financial Services Analytical Applications Transactions Filtering
Application for transactions filtering

5. To view the **Financial Services Analytical Applications Transactions Filtering** landing page, click **Calendar**

Figure 3-3 Calendar icon



.

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

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

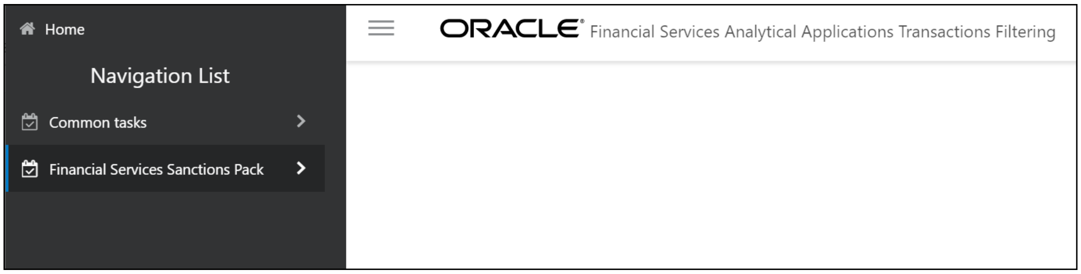
3.2.1 Transaction Filtering Admin Menu

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

To view the menu, follow these steps:

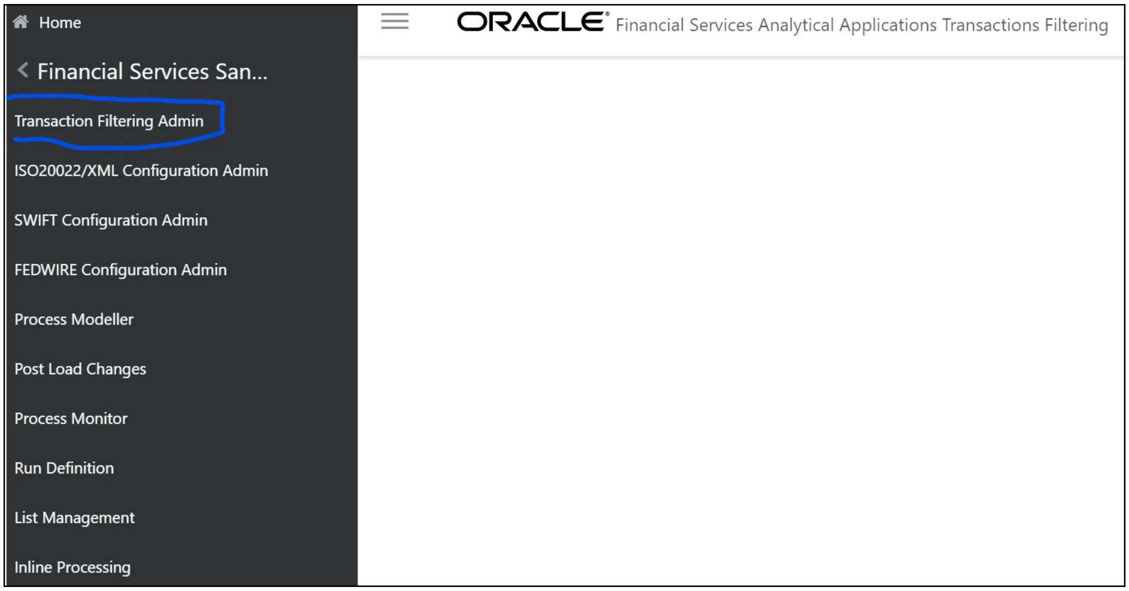
1. From the **Navigation List,** click **Financial Services Sanctions Pack**.

Figure 3-4 Financial Services Sanctions Pack Menu


Home
Navigation List
Common tasks
Financial Services Sanctions Pack
ORACLE Financial Services Analytical Applications Transactions Filtering

2. From the **Navigation List,** click **Transaction Filtering Admin**. The Configuration Screen displays.

Figure 3-5 Transaction Filtering Admin Sub-menu


Home
Financial Services San...
Transaction Filtering Admin
ISO20022/XML Configuration Admin
SWIFT Configuration Admin
FEDWIRE Configuration Admin
Process Modeller
Post Load Changes
Process Monitor
Run Definition
List Management
Inline Processing
ORACLE Financial Services Analytical Applications Transactions Filtering

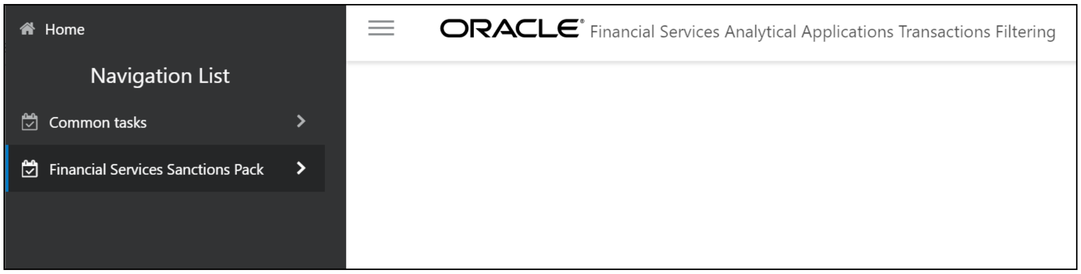
3.2.2 ISO20022 Configuration Admin Menu

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

To view the menu, follow these steps:

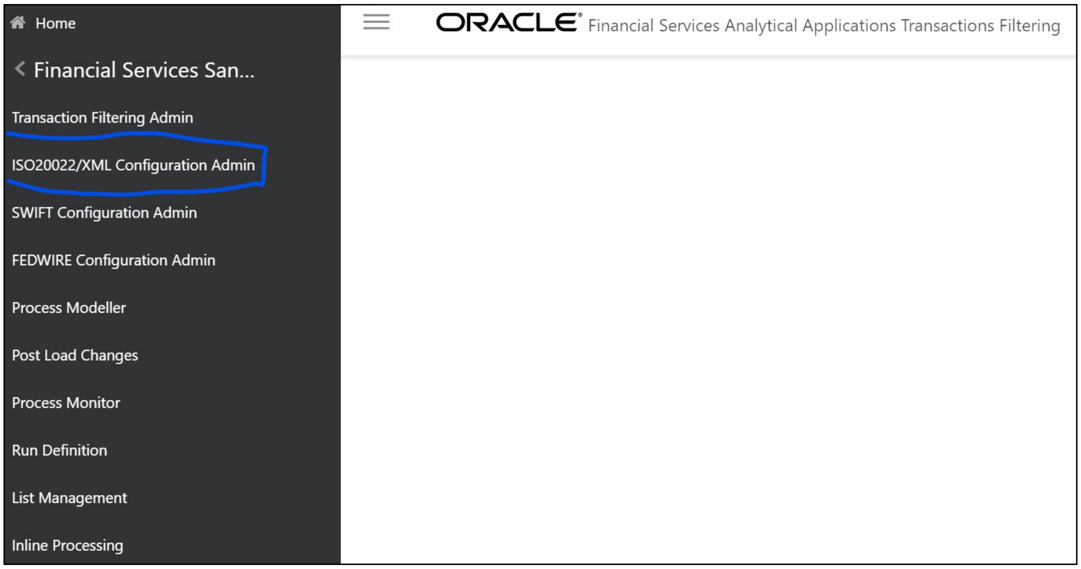
1. From the **Navigation List,** click **Financial Services Sanctions Pack**.

Figure 3-6 Financial Services Sanctions Pack Menu


Home
Navigation List
Common tasks
Financial Services Sanctions Pack
ORACLE Financial Services Analytical Applications Transactions Filtering

2. Click **ISO20022/XML Configuration Admin.** The Configuration Screen displays.

Figure 3-7 ISO20022/XML Configuration Admin Sub-menu


Home
Financial Services San...
Transaction Filtering Admin
ISO20022/XML Configuration Admin
SWIFT Configuration Admin
FEDWIRE Configuration Admin
Process Modeller
Post Load Changes
Process Monitor
Run Definition
List Management
Inline Processing
ORACLE Financial Services Analytical Applications Transactions Filtering

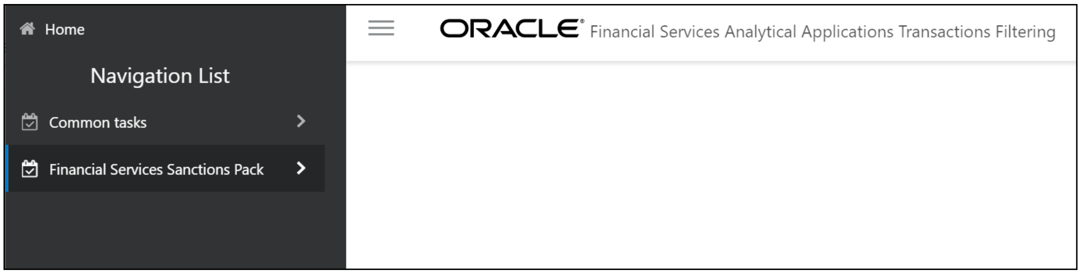
3.2.3 SWIFT Configuration Admin Menu

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

To view the **Configuration Admin** menu, follow these steps:

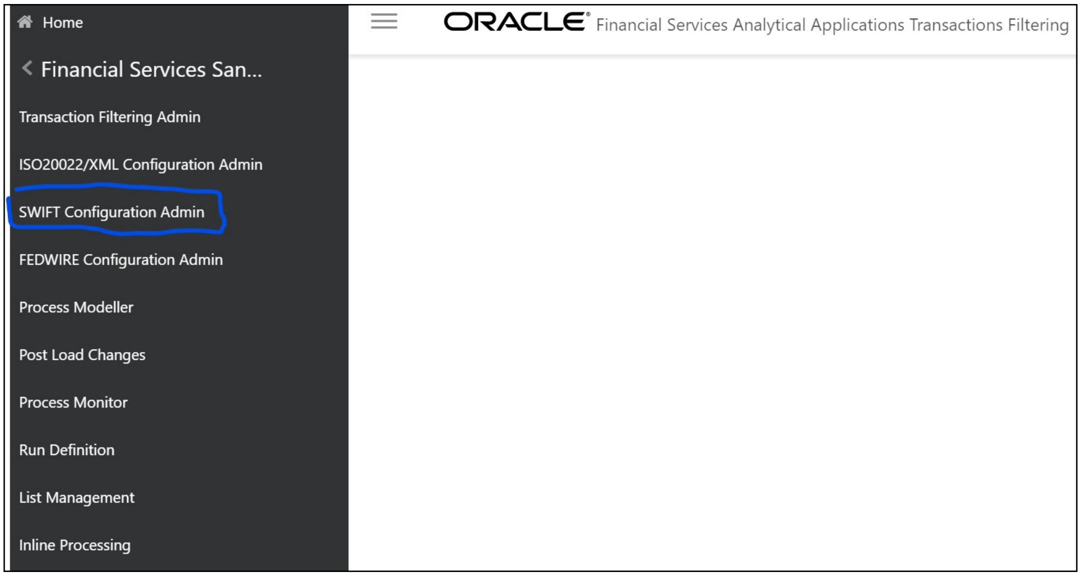
1. From the **Navigation List,** click **Financial Services Sanctions Pack**.

Figure 3-8 Financial Services Sanctions Pack Menu


Home
Navigation List
Common tasks
Financial Services Sanctions Pack
ORACLE Financial Services Analytical Applications Transactions Filtering

2. Click **SWIFT Configuration Admin.** The Configuration Screen displays.

Figure 3-9 SWIFT Configuration Admin Sub-menu


Home
Financial Services San...
Transaction Filtering Admin
ISO20022/XML Configuration Admin
SWIFT Configuration Admin
FEDWIRE Configuration Admin
Process Modeller
Post Load Changes
Process Monitor
Run Definition
List Management
Inline Processing
ORACLE Financial Services Analytical Applications Transactions Filtering

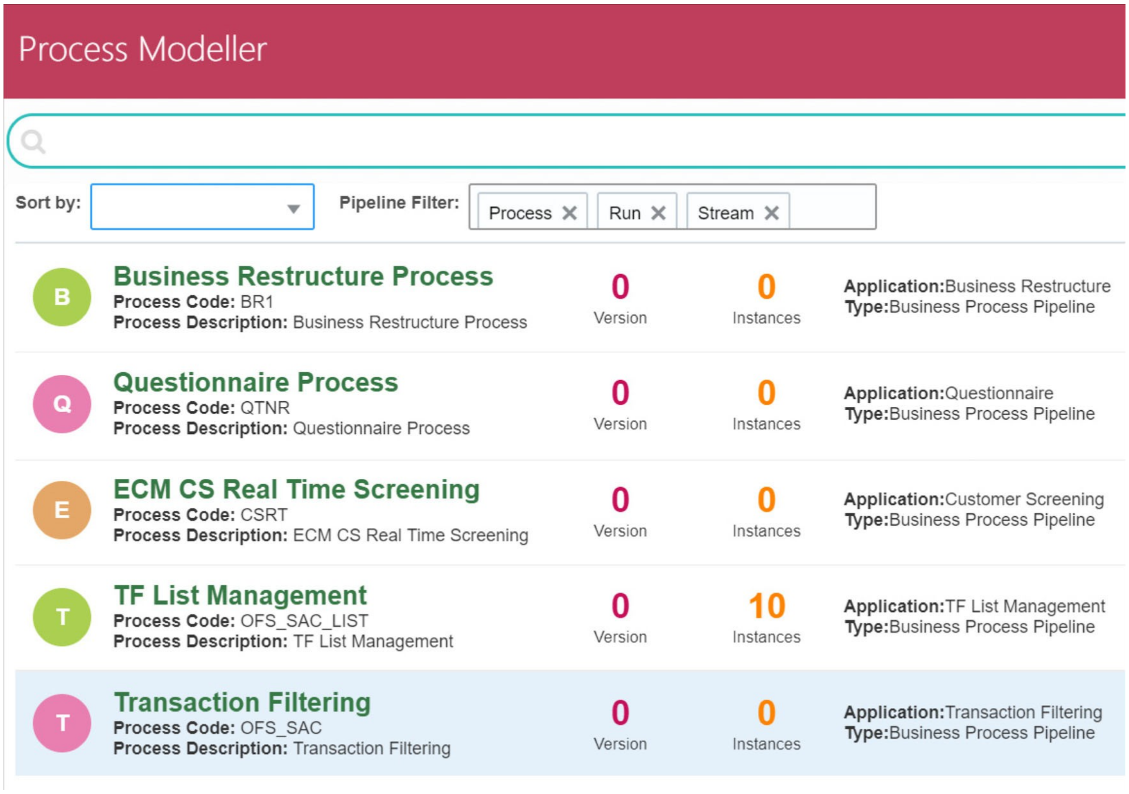
3.2.4 Process Modeller Menu

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

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

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

Figure 3-10   Process Modeller Page



Process Modeller

Sort by:

Pipeline Filter: Process ✕ Run ✕ Stream ✕

B **Business Restructure Process**
Process Code: BR1
Process Description: Business Restructure Process
0 Version
0 Instances
Application: Business Restructure
Type: Business Process Pipeline

Q **Questionnaire Process**
Process Code: QTNR
Process Description: Questionnaire Process
0 Version
0 Instances
Application: Questionnaire
Type: Business Process Pipeline

E **ECM CS Real Time Screening**
Process Code: CSRT
Process Description: ECM CS Real Time Screening
0 Version
0 Instances
Application: Customer Screening
Type: Business Process Pipeline

T **TF List Management**
Process Code: OFS_SAC_LIST
Process Description: TF List Management
0 Version
10 Instances
Application:TF List Management
Type: Business Process Pipeline

T **Transaction Filtering**
Process Code: OFS_SAC
Process Description: Transaction Filtering
0 Version
0 Instances
Application: Transaction Filtering
Type: Business Process Pipeline

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

Figure 3-11   Menu icon

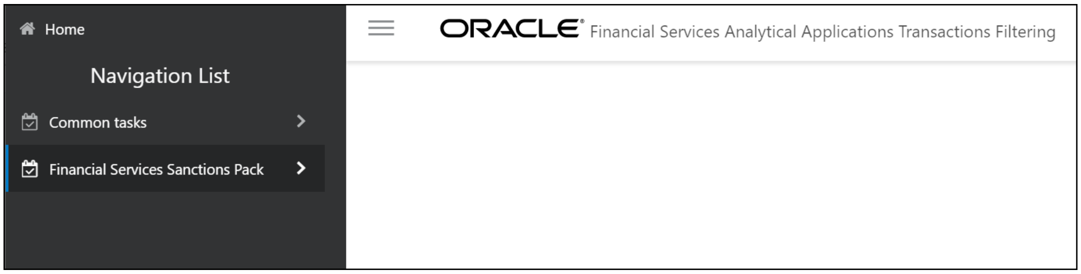
3.2.5 FEDWIRE Configuration Admin Menu

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

To view the **FEDWIRE Configuration Admin** menu, follow these steps:

1. From the **Navigation List,** click **Financial Services Sanctions Pack**.

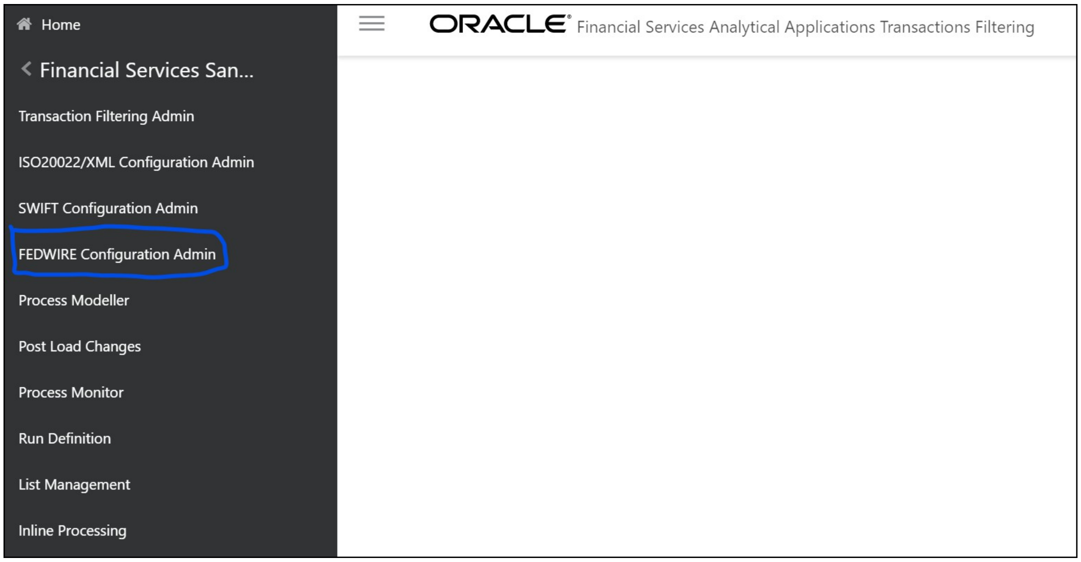
   Figure 3-12   Financial Services Sanctions Pack Menu

   Home
   Navigation List
   Common tasks
   Financial Services Sanctions Pack
   ORACLE Financial Services Analytical Applications Transactions Filtering

2. Click **FEDWIRE Configuration Admin.** The **Configuration Screen** is displayed.

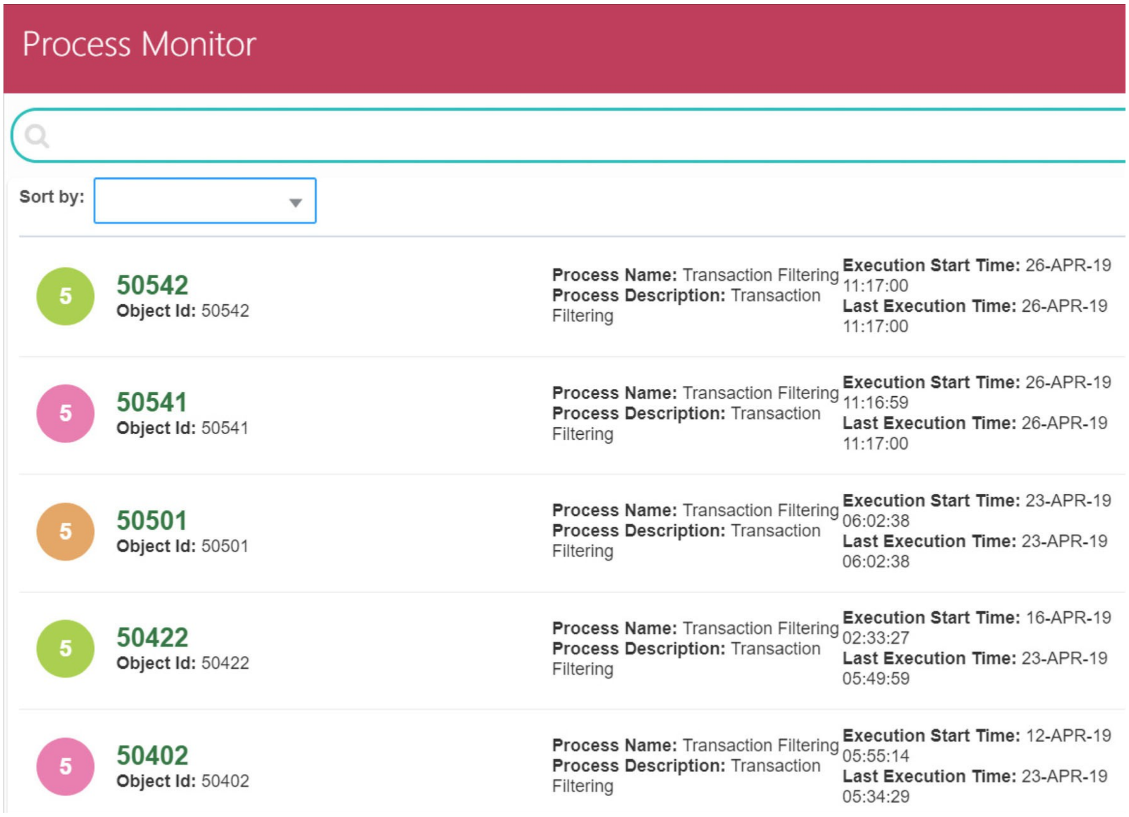
Figure 3-13 FEDWIRE Configuration Admin Sub-menu


Home
Financial Services San...
Transaction Filtering Admin
ISO20022/XML Configuration Admin
SWIFT Configuration Admin
FEDWIRE Configuration Admin
Process Modeller
Post Load Changes
Process Monitor
Run Definition
List Management
Inline Processing
ORACLE Financial Services Analytical Applications Transactions Filtering

3.2.6 Process Monitor Menu

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

Figure 3-14 Process Monitor Menu Page



5 **50542**
Object Id: 50542
Process Name: Transaction Filtering
Process Description: Transaction Filtering
Execution Start Time: 26-APR-19 11:17:00
Last Execution Time: 26-APR-19 11:17:00

5 **50541**
Object Id: 50541
Process Name: Transaction Filtering
Process Description: Transaction Filtering
Execution Start Time: 26-APR-19 11:16:59
Last Execution Time: 26-APR-19 11:17:00

5 **50501**
Object Id: 50501
Process Name: Transaction Filtering
Process Description: Transaction Filtering
Execution Start Time: 23-APR-19 06:02:38
Last Execution Time: 23-APR-19 06:02:38

5 **50422**
Object Id: 50422
Process Name: Transaction Filtering
Process Description: Transaction Filtering
Execution Start Time: 16-APR-19 02:33:27
Last Execution Time: 23-APR-19 05:49:59

5 **50402**
Object Id: 50402
Process Name: Transaction Filtering
Process Description: Transaction Filtering
Execution Start Time: 12-APR-19 05:55:14
Last Execution Time: 23-APR-19 05:34:29

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

Figure 3-15 Menu icon

.

3.2.7 Run Definition Menu

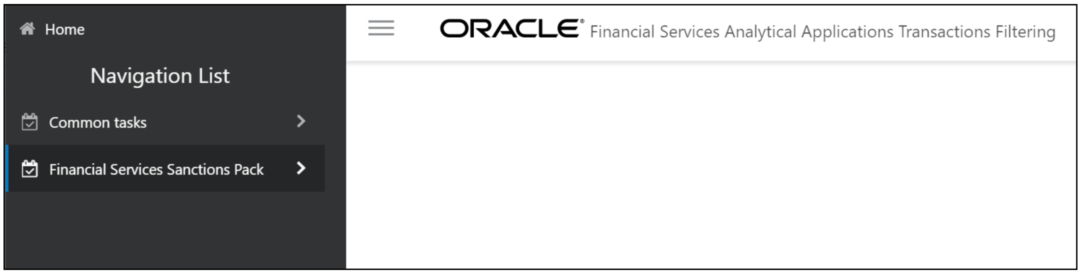
The **Run Definition** menu allows the system administrator to run the batches for the message categories.

To run the batches, follow these steps:

1. Click **Run Definition.** The **Run** page is displayed.

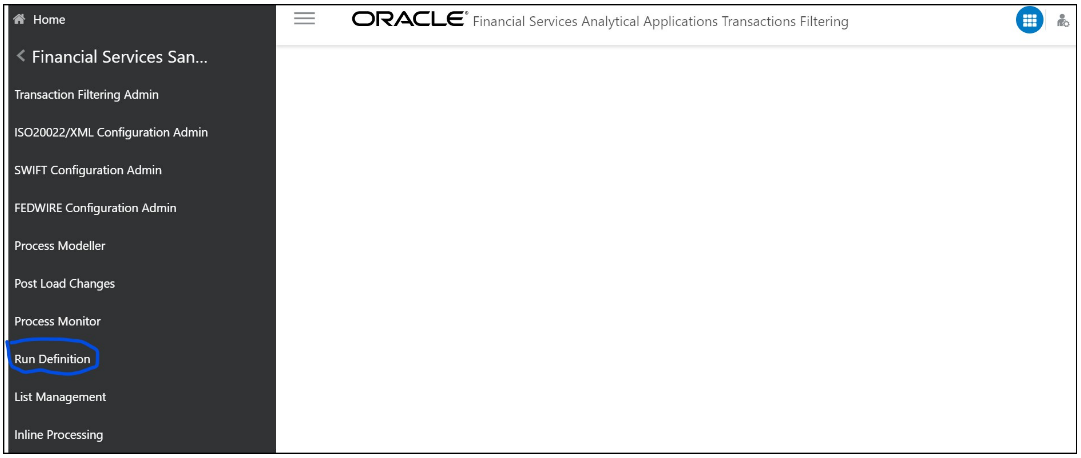
1. From the **Navigation List,** click **Financial Services Sanctions Pack**.

Figure 3-16 Financial Services Sanctions Pack Menu


Home
Navigation List
Common tasks
Financial Services Sanctions Pack
ORACLE Financial Services Analytical Applications Transactions Filtering

2. Click **Run Definition.** The **Run** page is displayed.

Figure 3-17 Transaction Filtering Admin Sub-menu


Home
Financial Services San...
Transaction Filtering Admin
ISO20022/XML Configuration Admin
SWIFT Configuration Admin
FEDWIRE Configuration Admin
Process Modeller
Post Load Changes
Process Monitor
Run Definition
List Management
Inline Processing
ORACLE Financial Services Analytical Applications Transactions Filtering

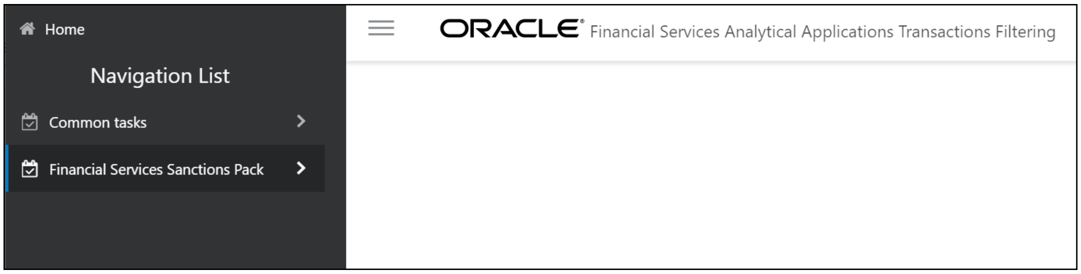
3.2.8 List Management Menu

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

To view the page, follow these steps:

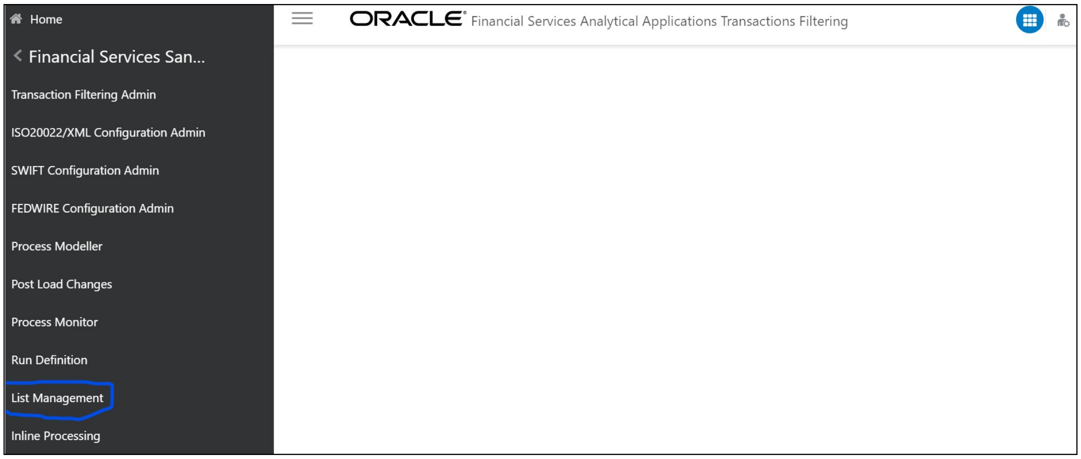
1. From the **Navigation List,** click **Financial Services Sanctions Pack**.

Figure 3-18 Financial Services Sanctions Pack Menu


Home
Navigation List
Common tasks
Financial Services Sanctions Pack
ORACLE Financial Services Analytical Applications Transactions Filtering

2. Click **List Management.** The **Good Guy Summary** page is displayed.

Figure 3-19 List Management Sub-menu


Home
Financial Services San...
Transaction Filtering Admin
ISO20022/XML Configuration Admin
SWIFT Configuration Admin
FEDWIRE Configuration Admin
Process Modeller
Post Load Changes
Process Monitor
Run Definition
List Management
Inline Processing
ORACLE Financial Services Analytical Applications Transactions Filtering

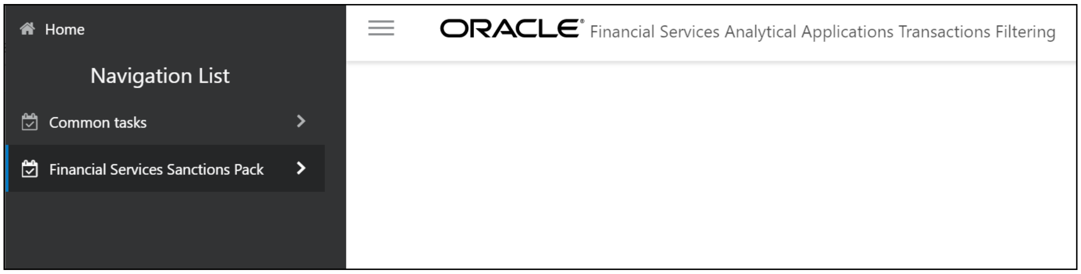
3.2.9 Inline Processing Menu

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

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

1. From the **Navigation List,** click **Financial Services Sanctions Pack**.

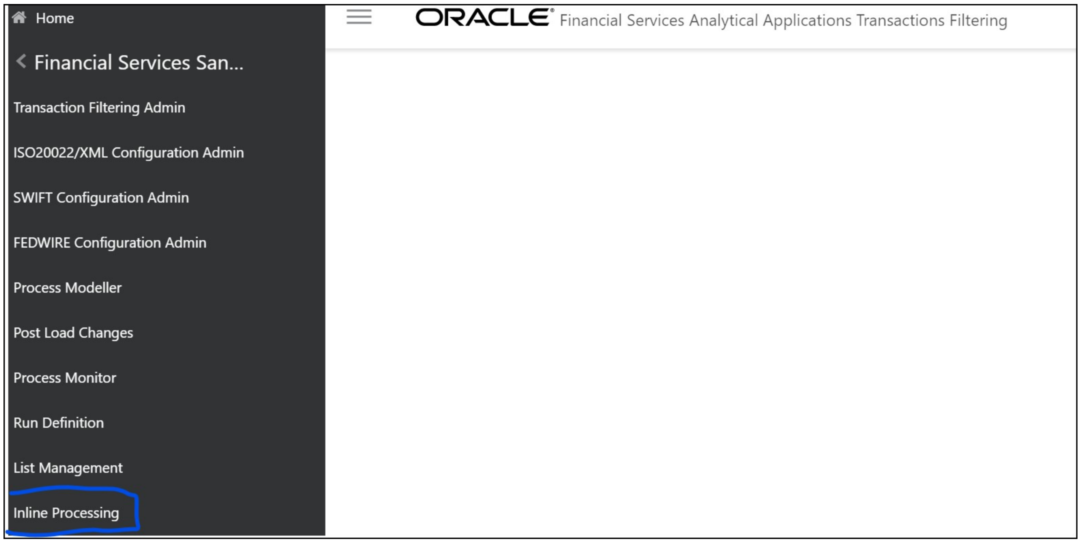
Figure 3-20 Financial Services Sanctions Pack Menu



Home
Navigation List
Common tasks
Financial Services Sanctions Pack
ORACLE Financial Services Analytical Applications Transactions Filtering

2. Click **Inline Processing.** The **Inline Processing** page is displayed.

Figure 3-21 Inline Processing Sub-menu



Home
Financial Services San...
Transaction Filtering Admin
ISO20022/XML Configuration Admin
SWIFT Configuration Admin
FEDWIRE Configuration Admin
Process Modeller
Post Load Changes
Process Monitor
Run Definition
List Management
Inline Processing
ORACLE Financial Services Analytical Applications Transactions Filtering

3.3 Queue Management

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

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

You can view the Queue details in the following formats:

- List View
- Grid View

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

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

3.3.1 List View

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

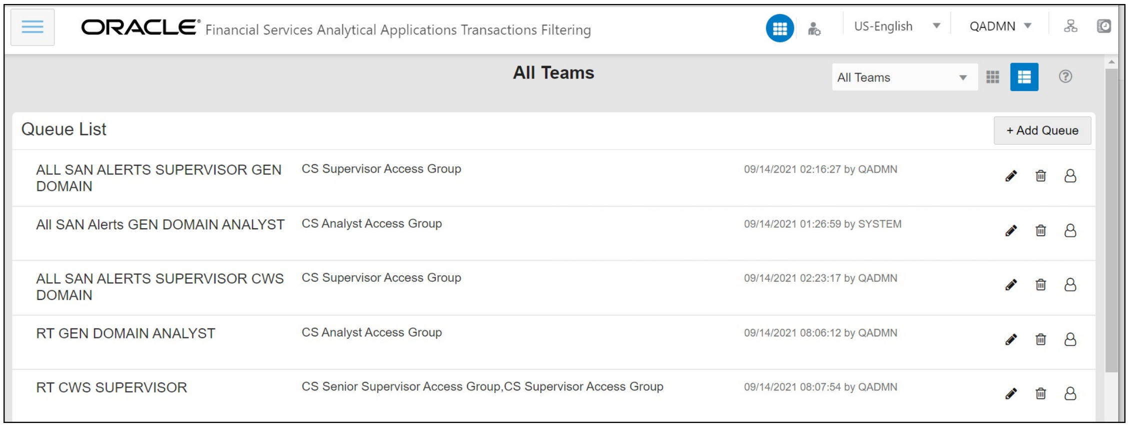
You can select the **hamburger**

Figure 3-22 hamburger

icon to view the **Queue List** for **All Teams** in List View. By default, queue details are displayed in the List View.

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

Figure 3-23 Queue List in List View



ORACLE Financial Services Analytical Applications Transactions Filtering
US-English
QADMN
All Teams
All Teams
Queue List
+ Add Queue

ALL SAN ALERTS SUPERVISOR GEN DOMAIN	CS Supervisor Access Group	09/14/2021 02:16:27 by QADMN
All SAN Alerts GEN DOMAIN ANALYST	CS Analyst Access Group	09/14/2021 01:26:59 by SYSTEM
ALL SAN ALERTS SUPERVISOR CWS DOMAIN	CS Supervisor Access Group	09/14/2021 02:23:17 by QADMN
RT GEN DOMAIN ANALYST	CS Analyst Access Group	09/14/2021 08:06:12 by QADMN
RT CWS SUPERVISOR	CS Senior Supervisor Access Group,CS Supervisor Access Group	09/14/2021 08:07:54 by QADMN

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

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

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

 +Add Queue: Click

Figure 3-24 +Add Queue

button top-right in the Queue List to add a new queue. (only for Queue Admin.)

- - **Delete:** Click the Ellipsis menu and then select Delete and click **Yes** to delete the queue.
  - **Edit:** Click the Ellipsis menu and then select Edit to edit the queue details and click **Finish**.
  - **Open**: Click the Ellipsis menu and then select Open to open the queue to see its details.
  - **Assign**: Click the Ellipsis menu and then select Assign to assign the queue to Groups. (only for Queue Admin)
    - Select the **Groups** to assign the queue.
    - Click **Assign**.

You can change the order of queues are as follows:

- - According to your requirement, you can select the Queue to change the order, drag and drop in the list.
  - Perform the following steps:
    - Select the Queue and right-click. The menu options are displayed as **Cut, Paste Before,** and

Paste After. The only **Cut** is enabled.

- - Select **Cut**.
  - Locate the cursor wherever it needs to be added and right-click. The menu options are **Cut, Paste Before**, and **Paste After**. Only **Paste Before** and **Paste After** are enabled.
  - Select the **Paste Before** or **Paste After** to place the Queue.

> **Note**
>
> If the User Group is selected as the **All Teams** in the **Select Teams** menu, then the Queue Admin cannot sort the priority of the Queues.

3.3.2 Grid View

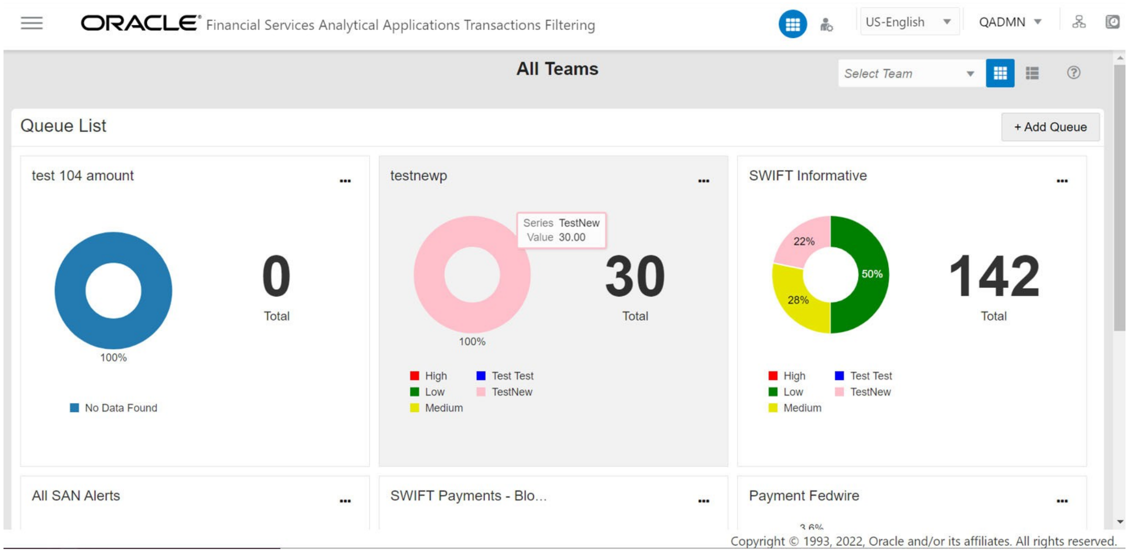
You can select the **thumbview**

Figure 3-25 Grid View icon

icon to view the **Queue List** for **All Teams** in Grid View.

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

Figure 3-26   Queue List in Grid View



ⓘ **Note**

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

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

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

The following are the default priorities in the application:

- High
- Medium
- Low

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

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

To configure the priorities and color code see Configuring New Priority section. Priority configuration for all the alerts to be defined before transaction filtering.

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

▯ **+Add Queue**: Click

Figure 3-27 Add Queue icon

button top-right in the Queue List to add a new queue. (only for Queue Admin.)

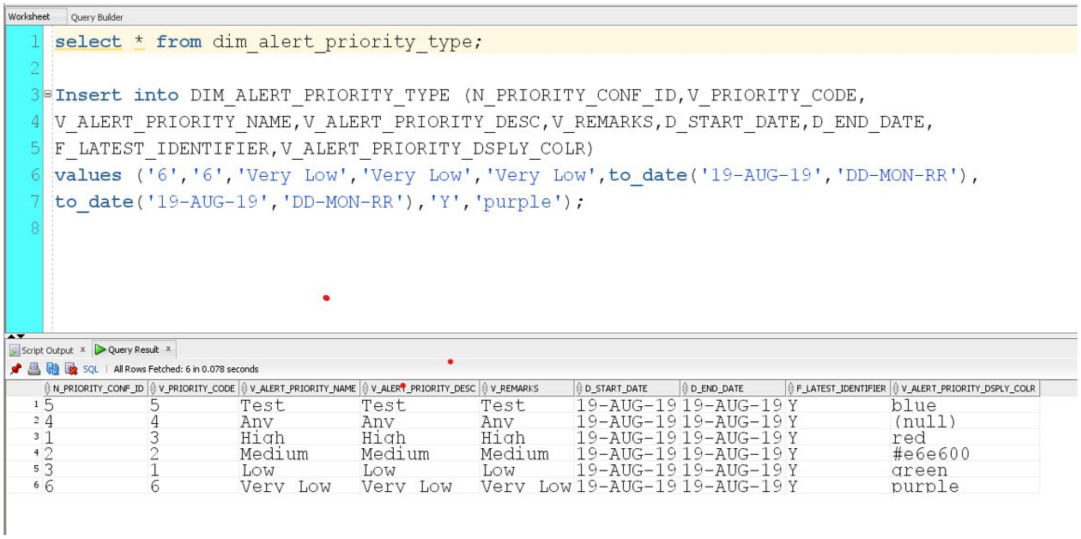
- **Delete:** Click the Ellipsis menu and then select Delete and click **Yes** to delete the queue.
- **Edit:** Click the Ellipsis menu and then select Edit to edit the queue details and click **Finish**.
- **Open**: Click the Ellipsis menu and then select Open to open the queue to see its details.
- **Assign**: Click the Ellipsis menu and then select Assign to assign the queue to Groups. (only for Queue Admin)
  - Select the **Groups** to assign the queue.
  - Click **Assign**.

3.3.3 Configuring New Priority

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

1. Access the Atomic Schema and access the DIM_ALERT_PRIORITY_TYPE table.
2. Insert the parameter to the following columns:
   - N_PRIORITY_CONF_ID
   - V_PRIORITY_CODE
   - V_ALERT_PRIORITY_NAME
   - V_ALERT_PRIORITY_DESC
   - V_REMARKS
   - D_START_DATE
   - D_END_DATE
   - F_LATEST_IDENTIFIER
   - V_ALERT_PRIORITY_DSPLY_COLR

Figure 3-28   DIM_ALERT_PRIORITY_TYPE Table



```
select * from dim_alert_priority_type;

Insert into DIM_ALERT_PRIORITY_TYPE (N_PRIORITY_CONF_ID,V_PRIORITY_CODE,
V_ALERT_PRIORITY_NAME,V_ALERT_PRIORITY_DESC,V_REMARKS,D_START_DATE,D_END_DATE,
F_LATEST_IDENTIFIER,V_ALERT_PRIORITY_DSPLY_COLR)
values ('6','6','Very Low','Very Low','Very Low',to_date('19-AUG-19','DD-MON-RR'),
to_date('19-AUG-19','DD-MON-RR'),'Y','purple');
```

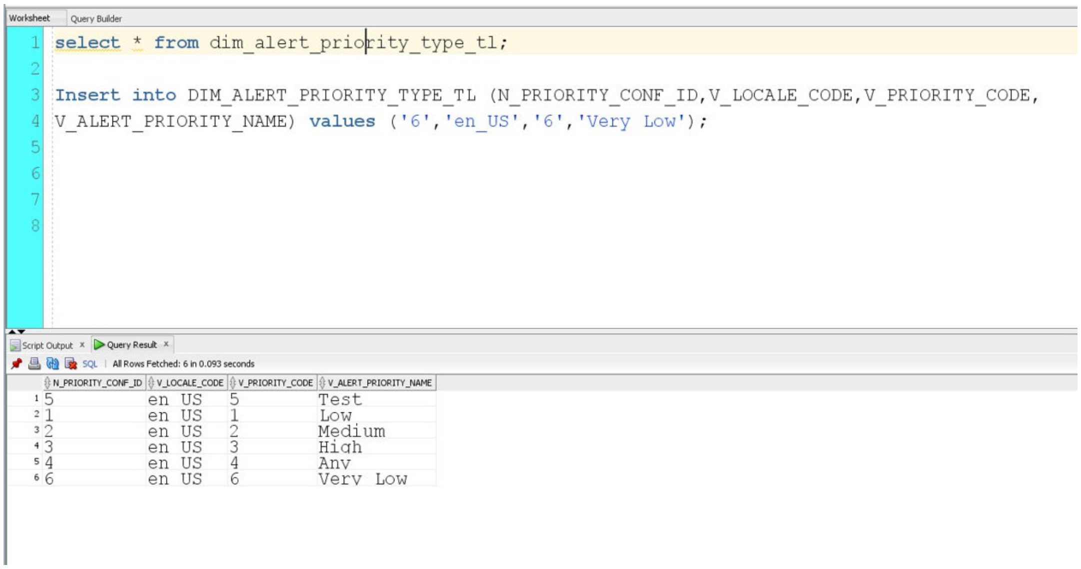
All Rows Fetched: 6 in 0.078 seconds

	N_PRIORITY_CONF_ID	V_PRIORITY_CODE	V_ALERT_PRIORITY_NAME	V_ALERT_PRIORITY_DESC	V_REMARKS	D_START_DATE	D_END_DATE	F_LATEST_IDENTIFIER	V_ALERT_PRIORITY_DSPLY_COLR
1	5	5	Test	Test	Test	19-AUG-19	19-AUG-19	Y	blue
2	4	4	Any	Any	Any	19-AUG-19	19-AUG-19	Y	(null)
3	1	3	High	High	High	19-AUG-19	19-AUG-19	Y	red
4	2	2	Medium	Medium	Medium	19-AUG-19	19-AUG-19	Y	#e6e600
5	3	1	Low	Low	Low	19-AUG-19	19-AUG-19	Y	green
6	6	6	Very Low	Very Low	Very Low	19-AUG-19	19-AUG-19	Y	purple

3. Access the DIM_ALERT_PRIORITY_TYPE_TL table.
4. Insert the parameter to the following columns:
   - N_PRIORITY_CONF_ID
   - V_LOCALE_CODE
   - V_PRIORITY_CODE
   - V_ALERT_PRIORITY_NAME

> ⓘ **Note**
>
> The DIM_ALERT_PRIORITY_TYPE table and DIM_ALERT_PRIORITY_TYPE_TL table must have same parameter value entry

Figure 3-29   DIM_ALERT_PRIORITY_TYPE_TL Table



```
select * from dim_alert_priority_type_tl;

Insert into DIM_ALERT_PRIORITY_TYPE_TL (N_PRIORITY_CONF_ID,V_LOCALE_CODE,V_PRIORITY_CODE,
V_ALERT_PRIORITY_NAME) values ('6','en_US','6','Very Low');
```

All Rows Fetched: 6 in 0.093 seconds

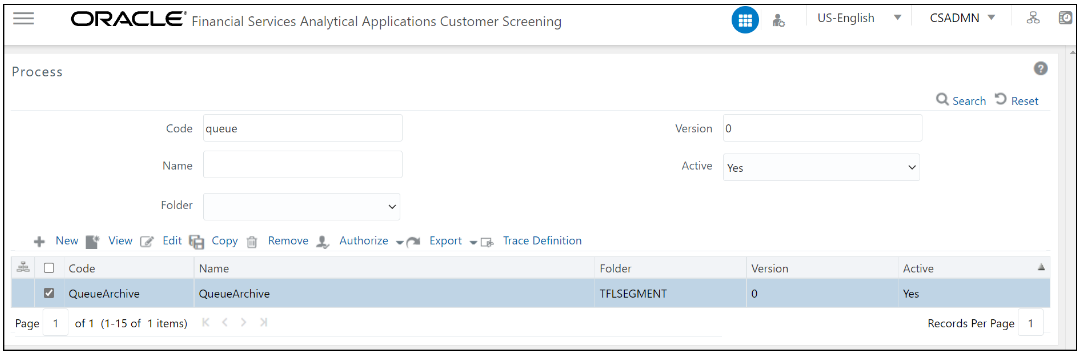
	N_PRIORITY_CONF_ID	V_LOCALE_CODE	V_PRIORITY_CODE	V_ALERT_PRIORITY_NAME
1	5	en_US	5	Test
2	1	en_US	1	Low
3	2	en_US	2	Medium
4	3	en_US	3	High
5	4	en_US	4	Any
6	6	en_US	6	Very Low

3.3.4 Archiving a Queue

To archive the inactive queues, follow these steps:

1. Log on to the Customer Screening application.
2. Click **Common Tasks**, then click **Rule Run Framework**, and then click **Process**. The **Process** page appears.
3. Search for Queue in the **Code** field and select Queue Archive.

Figure 3-30 Process Page



ORACLE Financial Services Analytical Applications Customer Screening — US-English — CSADMN

Process

Search Reset

Code	queue	Version	0
Name		Active	Yes
Folder			

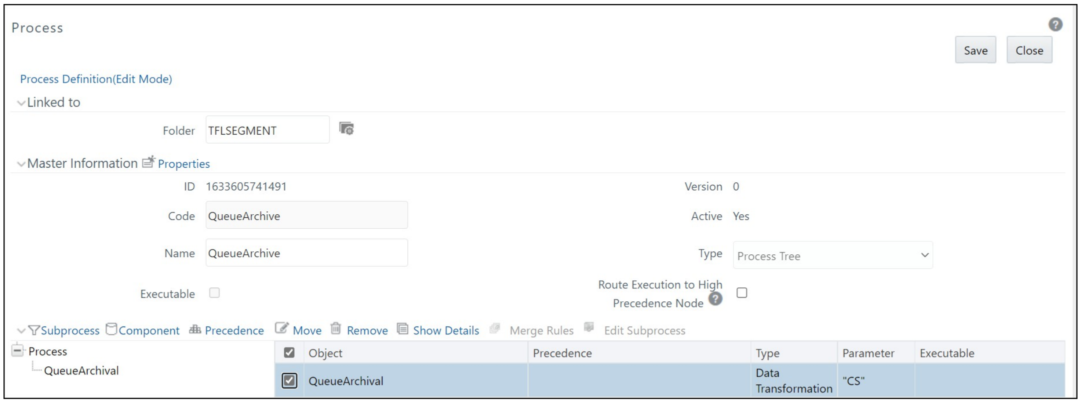
New View Edit Copy Remove Authorize Export Trace Definition

☐	Code	Name	Folder	Version	Active
☑	QueueArchive	QueueArchive	TFLSEGMENT	0	Yes

Page 1 of 1 (1-15 of 1 items) Records Per Page 1

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

Figure 3-31 Process Definition (Edit Mode)



Process

Save Close

Process Definition(Edit Mode)

Linked to

Folder TFLSEGMENT

Master Information Properties

ID	1633605741491	Version	0
Code	QueueArchive	Active	Yes
Name	QueueArchive	Type	Process Tree
Executable	☐	Route Execution to High Precedence Node	☐

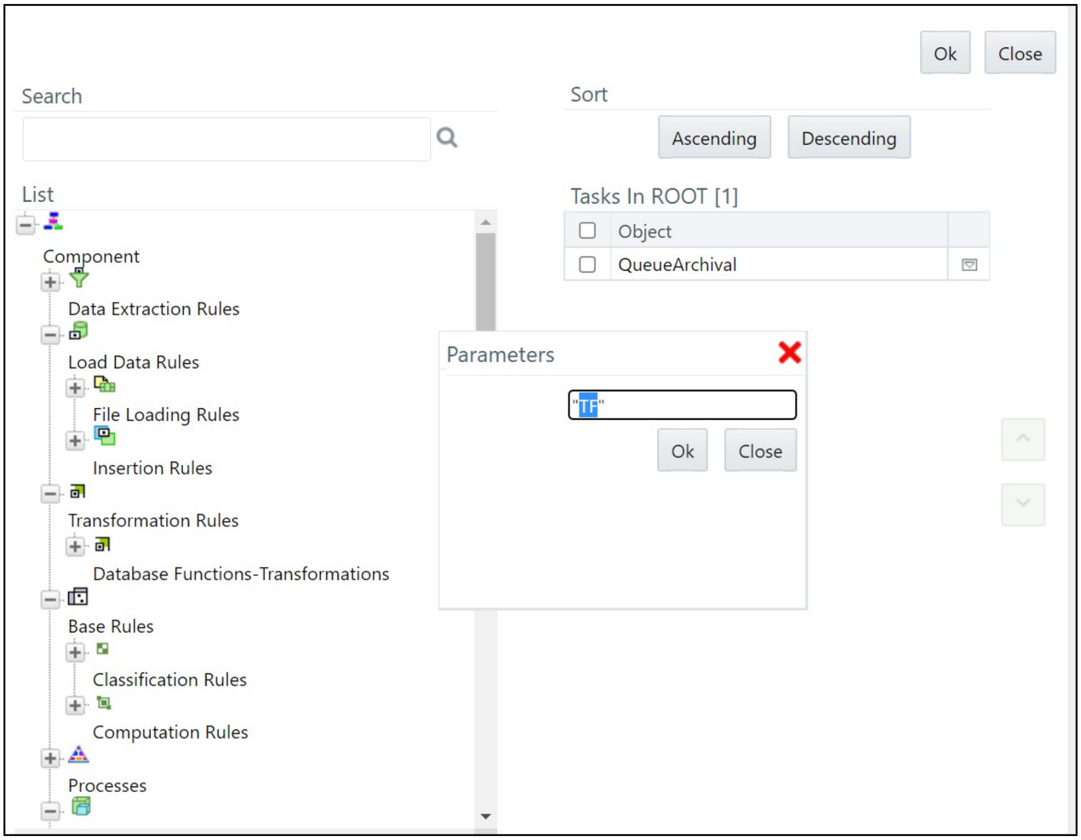
Subprocess Component Precedence Move Remove Show Details Merge Rules Edit Subprocess

Process
QueueArchival

☑	Object	Precedence	Type	Parameter	Executable
☑	QueueArchival		Data Transformation	"CS"	

5. Select the QueueArchival object and then select **Component**.
6. In the **Parameters** window, select the QueuArchival task and then click **drop-down list** . By default the parameter value will be selected as “TF”.

Figure 3-32   Component Selector Window



Tasks In ROOT [1]

□	Object
□	QueueArchival

Parameters: "TF"

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

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

3.4 Troubleshooting Your Display

If you experience problems logging into Oracle Financial Services 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.

3.4.1 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.

3.4.2 Enabling Cookies

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

3.4.3 Enabling Temporary Internet Files

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

To 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.

3.4.4 Enabling File Downloads

This section describes how to enable file downloads. To enable file downloads, follow these steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Security** tab and then click **Local Intranet**.
4. Click **Custom Level**. The **Security Settings** dialog box is displayed.
5. Under the **Downloads** section, ensure that **Enable** is selected for all options.
6. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

3.4.5 Setting Printing Options

This section explains how to enable printing background colors and images. To enable this option, follow these steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Advanced** tab. In the **Settings** list.
4. Under the **Printing** setting, click **Print background colors and images**.
5. Click **OK** to exit the **Internet Options** dialog box.

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

3.4.6 Enabling the Pop-Up Blocker

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

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

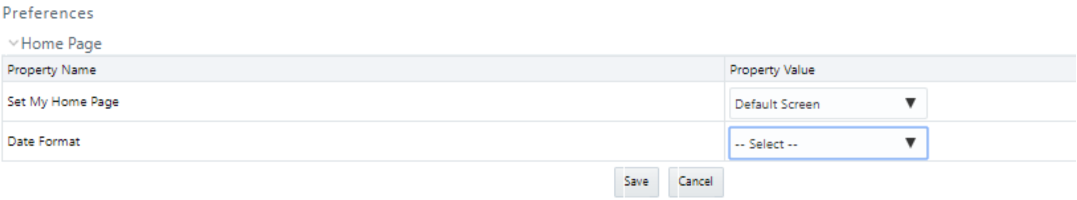
1. Navigate to the **Tools** menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Privacy** tab. In the **Pop-up Blocker** setting, select **Turn on Pop-up Blocker**. The Set- tings are enabled.
4. Click **Settings** to open the **Pop-up Blocker Settings**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

3.4.7 Setting Preferences

Use the Preferences section to enable you to set your OFSAA home page. To access this section, follow these steps:

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

Figure 3-33 Preferences Page



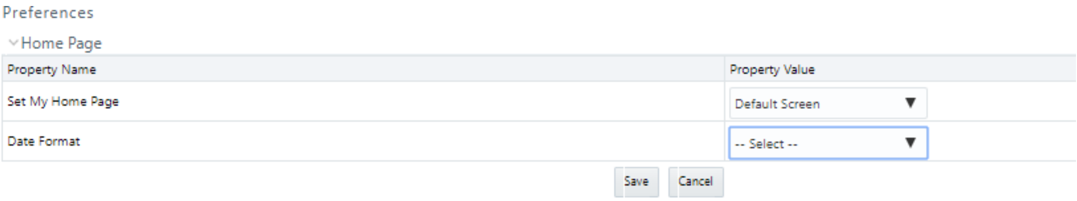
Preferences

Home Page

Property Name	Property Value
Set My Home Page	Default Screen ▼
Date Format	-- Select -- ▼

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

Figure 3-34 Preferences Page



Preferences

Home Page

Property Name	Property Value
Set My Home Page	Default Screen ▼
Date Format	-- Select -- ▼

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

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

4. In the **Date Format** drop-down list, select the date format that you want to see. The options available are dd/MM/yyyy or M/dd/yyyy.

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

4

Managing User Administration

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

4.1 About User Administration

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

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

4.2 Managing User Administration

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

Table 4-1 User Administration

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

4.2.1 Creating and Authorizing a User

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

4.2.2 Mapping Users with User Groups

This section explains how to map Users with User Groups. The user has access to privileges as per the role. The sysadm user maps a user to a user group in the Transaction Filtering application.

Table 4-2 User Group-Role Mapping

Role	Group Name	User Group Code
Administrator	Transaction Filtering Administrator Group	TFLTADMINISTATORGRP
Reviewer	Transaction Filtering Reviewer Group	TFLTREVIEWERGRP
Analyst	Transaction Filtering Analyst Group	TFLTANALYSTGRP

Table 4-2 (Cont.) User Group-Role Mapping

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

Table 4-3 User Group-Role Mapping

Role	Group Name	User Group Code
Senior Supervisor	Transaction Filtering Senior Supervisor Group	TFSNRRSUPERVISORGRP
Audit	Transaction Filtering Audit Group	TFAUDITGRP

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

5 General Configurations

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

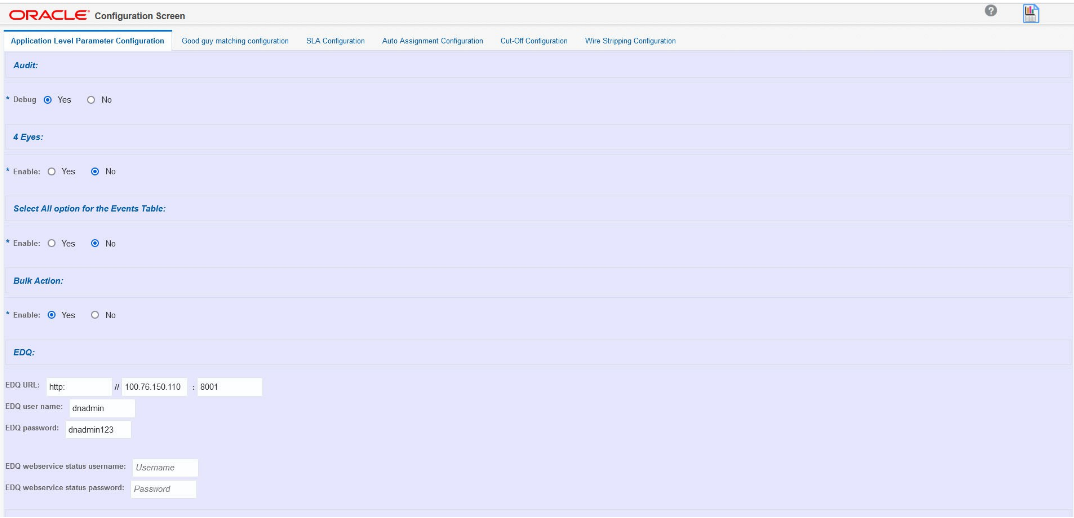
5.1 Configuring the Application Level Parameters

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

To configure the parameters, follow these steps:

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

Figure 5-1 Application Level Parameter Configuration Tab


ORACLE Configuration Screen
Application Level Parameter Configuration
Good guy matching configuration
SLA Configuration
Auto Assignment Configuration
Cut-Off Configuration
Wire Stripping Configuration

Audit:

* Debug ● Yes ○ No

4 Eyes:

* Enable: ○ Yes ● No

Select All option for the Events Table:

* Enable: ○ Yes ● No

Bulk Action:

* Enable: ● Yes ○ No

EDQ:

EDQ URL: http: // 100.76.150.110 : 8001

EDQ user name: dnadmin

EDQ password: dnadmin123

EDQ webservice status username: Username

EDQ webservice status password: Password

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 **Sta- tus** column. If you select **No**, then only those steps for which the value is **Y** in the **Status** column are logged in the system.

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

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

> **Note**
>
> If the 4 Eyes workflow is enabled, then the new alert data should be posted to the UI to view the new options which are Message Statuses, Blocked Recommended and Released Recommended.

5. In the **Select All option for the Events Table** section select **Yes** to enable **Select All** option and select **No** to disable **Select All** option in Alert list details Event tab. For more information on alert details and event table, see Oracle Financial Services Transaction Filtering User Guide.
6. In the **Bulk Action** section select **Yes** to enable Bulk Action option and select **No** to disable the Bulk Action option in the Alert list page.
7. 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 Num- ber
   - **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.
   - **EDQ webservice status username**
   - **EDQ webservice status password**
8. In the **ECM L2 Analysis** section, select **Yes** to enable and then provide the following values:
   - **ECM L2 Case Creation URL** in the following format:
     <http>: <Hostname of the server in which ECM is installed>: <Port Num- ber>/<Context>
   - **ECM Case Creation user name**: Enter the ECM username.
   - **ECM Case Creation password**: Enter the ECM password.
9. 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.
10. Custom feedback configuration can be done in the tables for HOLD, CLEAN and AUTORELEASE status.

    We introduced the new table and created the new Post processing actions similar as from IPE screen from admin UI to the table. (FCC_TF_PP_ACTIONS).

The table contains the post processing action code, code attributes, Query and text message. These configurations are editable like how we can in admin UI screen.

After installing this patch the post processing actions from the new table will be considered for message posting.

Once the message is processed, whether the Feedback is sent or not will be recorded in the table. (FCC_TF_RAW_FEEDBACK).

This table contains group message id, feedback sent or not along with post processing action code.

This table is useful in re-triggering the messages to send the feedback successfully for those feedback which are not sent.

11. Table contains the post processing action code, code attributes , Query and text message.
12. 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.

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

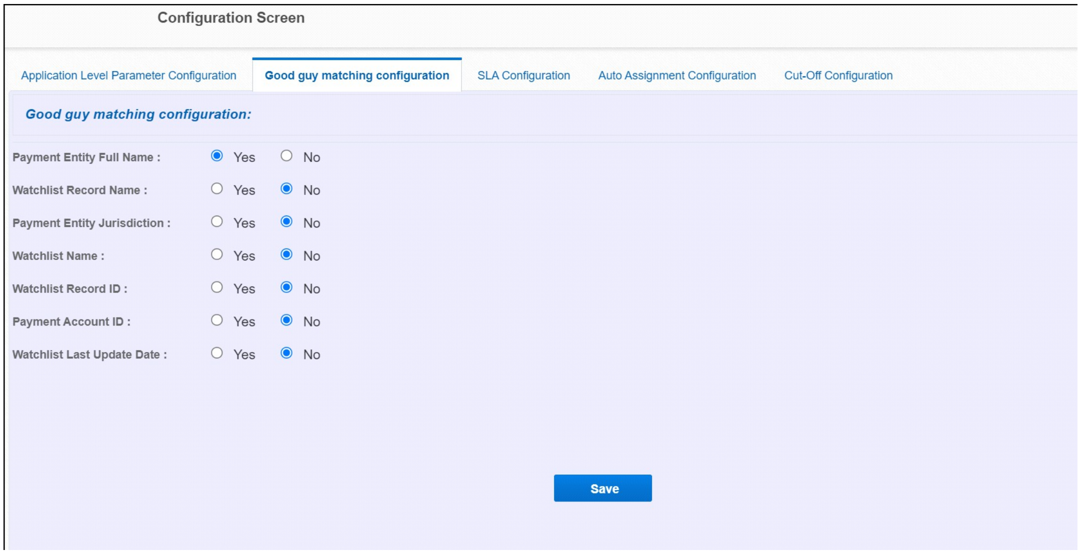
5.2 Configuring the Good Guy Matching Parameters

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

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

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** landing page.
2. Click **Transaction Filtering Admin** and then click the **Good Guy Matching Configuration** tab.

Figure 5-2   Good Guy Matching Configuration Tab


Configuration Screen
Application Level Parameter Configuration
Good guy matching configuration
SLA Configuration
Auto Assignment Configuration
Cut-Off Configuration
Save

Good guy matching configuration:

Payment Entity Full Name :	● Yes	○ No
Watchlist Record Name :	○ Yes	● No
Payment Entity Jurisdiction :	○ Yes	● No
Watchlist Name :	○ Yes	● No
Watchlist Record ID :	○ Yes	● No
Payment Account ID :	○ Yes	● No
Watchlist Last Update Date :	○ Yes	● No

- **Payment Entity Full Name:** The payment entity full name must be matched, so it is mandatory to set the value in the **Payment Entity Full Name** to **Yes**. If you do not set it to **Yes**, an error message, “**The Payment Entity Full Name should be set as Yes mandatorily**.” is displayed.

5.3 Configuring the SLA Parameters

Banks or FIs want to settle payments within a specified time. To achieve this, related alerts should be closed well within this specified time. The cut-off time is the defined duration by when the alert has to be closed. This is the time from when the Analyst starts working on the alert till the time the alert is closed. The SLA is defined as the time from when the alert is created or reopened to when the Payment is made. The Cut-off time will be well within the SLA. You must define the cut-off time and SLA.

Use the **SLA Configuration** window to define an SLA for a combination of message category, message type, currency, jurisdiction, business domain, message direction, transaction amount range, and message priority.

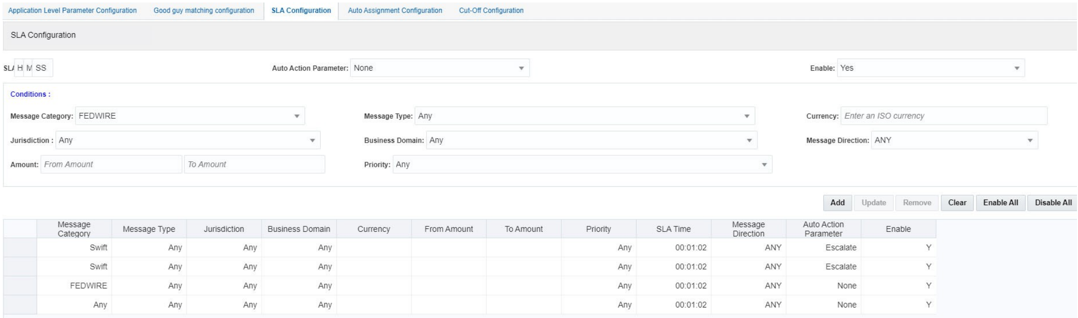
> **Note**
>
> The SLA time must be defined in HH:MM:SS format.

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

To set the SLA time, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** landing page.
2. Click **Transaction Filtering Admin** and then click the **SLA Configuration** tab.

Figure 5-3 SLA Configuration Tab


Application Level Parameter Configuration
Good guy matching configuration
SLA Configuration
Auto Assignment Configuration
Cut-Off Configuration
Add
Update
Remove
Clear
Enable All
Disable All

SLA Configuration

SLA H M SS

Auto Action Parameter: None

Enable: Yes

Conditions :

Message Category: FEDWIRE

Message Type: Any

Currency: Enter an ISO currency

Jurisdiction : Any

Business Domain: Any

Message Direction: ANY

Amount: From Amount To Amount

Priority: Any

	Message Category	Message Type	Jurisdiction	Business Domain	Currency	From Amount	To Amount	Priority	SLA Time	Message Direction	Auto Action Parameter	Enable
	Swift	Any	Any	Any				Any	00:01:02	ANY	Escalate	Y
	Swift	Any	Any	Any				Any	00:01:02	ANY	Escalate	Y
	FEDWIRE	Any	Any	Any				Any	00:01:02	ANY	None	Y
	Any	Any	Any	Any				Any	00:01:02	ANY	None	Y

3. Enter the SLA time in HH:MM:SS format.
4. Select an automatic action for an alert that is overdue. You can do one of the following:
   - Recommend to block the transaction
   - Block the transaction
   - Recommend to release the transaction
   - Release the transaction
   - Escalate the transaction
5. Select **Yes** to enable a specific combination, else select **No**.
6. To create a combination, use the following conditions. This is an optional step.
   - **Message Category**: Select the message category used for the transaction. You can also select **Any** to indicate that regardless of the message category, the SLA time is enabled for the combination. If you select **Any**, you cannot select a message type.
   - **Message Types**: Select a message type for the message category. You can also select **All** to indicate that the SLA time is enabled for all message types.
   - **Currency**: Enter the ISO currency code of the currency used for the transaction.
   - **Jurisdiction**: Select the jurisdiction/geography if the defined SLA time must apply to only this jurisdiction. You can also select **All** to select all jurisdictions/geographies.
   - **Business Domain**: Select the business domain if the defined SLA time must apply to only this business domain. You can also select **All** to select all business domains.
   - **Message Direction**: Select INBOUND for transactions that are coming into your account and select OUTBOUND for transactions that are going out of your account. You can also select **Any** to select any message direction.
   - **Amount**: Select the amount range used in the transaction.
   - **Priority**: Set a specific alert priority or select **Any** to indicate that the alert can have any priority.

Table 5-1 General Actions

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

Table 5-1 (Cont.) General Actions

To...	Do this...
Remove a configuration	Select the configuration you want to remove and click **Remove**. The selected configuration is removed from the table.
Clear the values of some of the fields in a configuration	Click **Clear**. You can only clear the values of the Cut-Off Time, Currency, and Amount fields.
Enable all configurations	Click **Enable All**.
Disable all configurations	Click **Disable All**.

5.4 Automatic Assignments of Alerts

The Transaction Filtering application provides two options for assigning alerts:

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

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

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

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

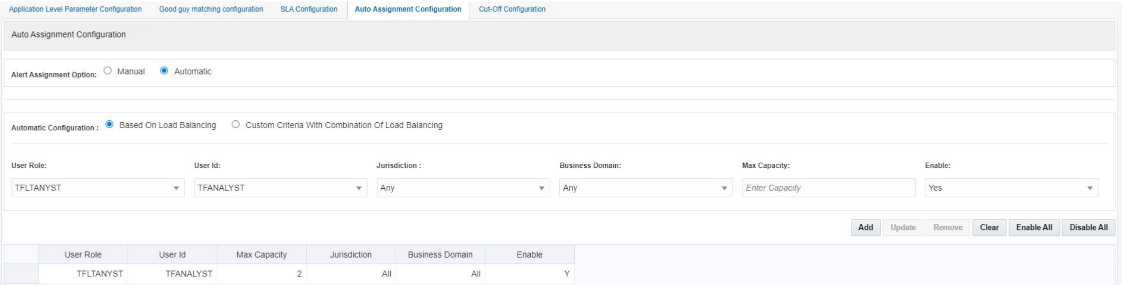
To configure an alert to be assigned manually or automatically, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** landing page.
2. Click **Transaction Filtering Admin** and then click the **Auto Assignment Configuration** tab.
3. Select **Automatic** to auto-assign the alert to the selected role. Select **Manual** to manually assign an alert to the selected user.

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

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

Figure 5-4 Auto Assignment Configuration Tab with Based on Load Balancing Selection


Application Level Parameter Configuration
Good guy matching configuration
SLA Configuration
Auto Assignment Configuration
Cut-Off Configuration
Add
Update
Remove
Clear
Enable All
Disable All

Auto Assignment Configuration

Alert Assignment Option: ○ Manual ● Automatic

Automatic Configuration : ● Based On Load Balancing ○ Custom Criteria With Combination Of Load Balancing

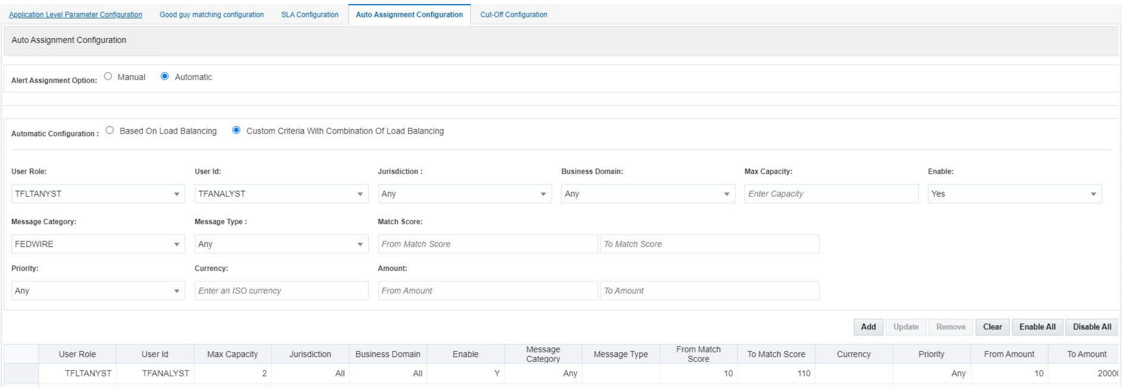
User Role: TFLTANYST
User Id: TFANALYST
Jurisdiction : Any
Business Domain: Any
Max Capacity: Enter Capacity
Enable: Yes

User Role	User Id	Max Capacity	Jurisdiction	Business Domain	Enable
TFLTANYST	TFANALYST	2	All	All	Y

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

Figure 33: Auto Assignment Configuration Tab Custom Criteria with Combination of Load Balancing

Figure 5-5 Auto Assignment Configuration Tab Custom Criteria with Combination of Load Balancing


Application Level Parameter Configuration
Good guy matching configuration
SLA Configuration
Auto Assignment Configuration
Cut-Off Configuration
Add
Update
Remove
Clear
Enable All
Disable All

Auto Assignment Configuration

Alert Assignment Option: ○ Manual ● Automatic

Automatic Configuration : ○ Based On Load Balancing ● Custom Criteria With Combination Of Load Balancing

User Role: TFLTANYST
User Id: TFANALYST
Jurisdiction : Any
Business Domain: Any
Max Capacity: Enter Capacity
Enable: Yes
Message Category: FEDWIRE
Message Type : Any
Match Score: From Match Score To Match Score
Priority: Any
Currency: Enter an ISO currency
Amount: From Amount To Amount

User Role	User Id	Max Capacity	Jurisdiction	Business Domain	Enable	Message Category	Message Type	From Match Score	To Match Score	Currency	Priority	From Amount	To Amount
TFLTANYST	TFANALYST	2	All	All	Y	Any		10	110		Any	10	2000

The following conditions must be defined:

- **User Role**: Select the role to whom you want to automatically assign alerts. When you select the role, all users who belong to that role are displayed in the *User ID* field. You can assign an alert to any user except the Admin user.
- **User ID**: Select the user to whom you want to automatically assign alerts.
- **Jurisdiction**: Select the jurisdiction applicable to the combination, or select **All** to indicate that for all jurisdictions, the alert auto-assignment is enabled for the combination.
- **Business Domain**: Select the business domain applicable to the combination or select **All**.
- **Max Capacity**: Select the maximum number of alerts that can be investigated by the selected user.
- **Enable Flag**: Select **Yes** to enable the combination.

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

- **Message Category**: Select the message category used for the combination or select **Any** to indicate that regardless of the message category, the alert auto-assignment is enabled for the combination.
- **Message Types**: Select a message type for the message category or select **None.**
- **Match Score**: Select the match score range. If the match score is between this range, then the alert is assigned to the selected user based on the configuration.
- **Priority**: Set the message priority or select **Any**.
- **Currency**: Enter the ISO currency code of the currency used during the transaction.
- **Amount**: Select the amount range used in the transaction.

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

Table 6:

Table 5-2 General Actions

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

5.5 Configuring the Cut-Off Parameters for Alerts

Banks or FIs want to settle payments within a specified time. To achieve this, related alerts should be closed well within this specified time. The cut-off time is the defined duration by when the alert has to

be closed. This is the time from when the Analyst starts working on the alert till the time the alert is closed. The SLA is defined as the time from when the alert is created or reopened to when the Payment is made. The Cut-off time will be well within the SLA. You must define the cut-off time and SLA.

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

> ⓘ **Note**
>
> The cut-off time must be defined in HH:MM:SS format and will be based on your locale.

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

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

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

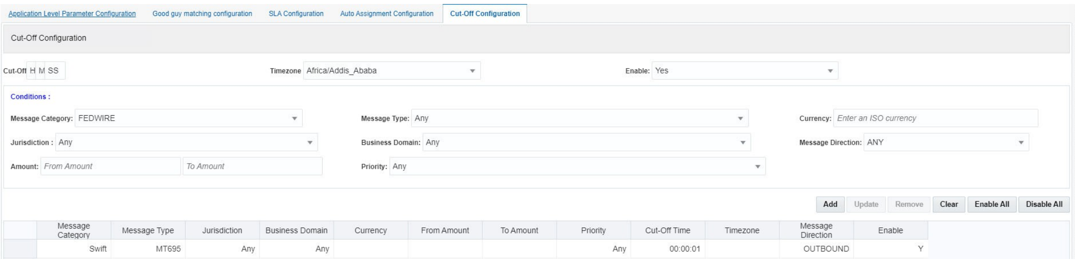
When the cut-off time is set for an alert, the alert displays the time in *green* in the Investigation User Interface until the cut-off time is passed. After the cut-off time is passed, that is, the alert becomes overdue and is not investigated within the defined cut-off time, then the alert displays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

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

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

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** landing page.
2. Click **Transaction Filtering Admin** and then click the **Cut-Off Configuration** tab.

Figure 5-6 Cut-Off Configuration Tab



Cut-Off: H M SS
Timezone: Africa/Addis_Ababa
Enable: Yes

Message Category: FEDWIRE
Message Type: Any
Currency: Enter an ISO currency
Jurisdiction : Any
Business Domain: Any
Message Direction: ANY
Amount: From Amount To Amount
Priority: Any

	Message Category	Message Type	Jurisdiction	Business Domain	Currency	From Amount	To Amount	Priority	Cut-Off Time	Timezone	Message Direction	Enable
	Swift	MT695	Any	Any				Any	00:00:01		OUTBOUND	Y

3. Enter the cut-off time in HH:MM:SS format. This is the time period by when the alert must be closed by the investigator.
4. Enter the locale. The cut-off time is displayed based on your selection.
5. Select **Yes** to enable a specific combination, else select **No**.
6. To create a combination, use the following conditions. This is an optional step.
   - **Message Category**: Select the message category used for the transaction. You can also select **Any** to indicate that regardless of the message category, the cut-off time is enabled for the combination. If you select **Any**, you cannot select a message type.

- **Message Types**: Select a message type for the message category. You can also select **All** to indicate that the cut-off time is enabled for all message types.
- **Jurisdiction**: Select the jurisdiction/geography if the defined cut-off time must apply to only this jurisdiction. You can also select **All** to select all jurisdictions/geographies.
- **Business Domain**: Select the business domain if the defined cut-off time must apply to only this business domain. You can also select **All** to select all business domains.
- **Currency**: Enter the ISO currency code of the currency used for the transaction.
- **Amount**: Select the amount range used in the transaction.
- **Priority**: Set a specific alert priority or select **Any** to indicate that the alert can have any priority.
- **Message Direction**: Select INBOUND for transactions that are coming into your account and select OUTBOUND for transactions that are going out of your account. You can also select **Any** to select any message direction.

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

Table 5-3 General Actions

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

5.6 Wire Stripping Configuration

Wire Stripping is a deliberate and illegal practice of removing, tampering, or altering the payment information from wire transfers, so that the identity of potentially sanctioned countries, entities, or individuals is hidden. Wire Stripping practice involves the following methods:

- A financial institution deleting information from the wire transfer message
- Inserting false information in the wire transfer message
- Requesting that the transferring institution delete or falsify an incoming transfer message

For example,

If the sanctioned country A needs to purchase goods from the country B, the transaction originates with the business in sanctioned country A sending funds to an intermediary bank in Country C. Banks from Country C then transfers funds to Country B.

When the bank from Country C transfers the money to the bank in Country B, the details are stripped, i.e., the wire details are removed during the fund transfer to the bank in Country B to avoid OFAC filter detection. The bank from Country B then forwards the currency to the Country B-based goods supplier, and the materials are supplied at the intermediary location (Country C). The intermediary bank (Country C) may remove evidence of any nexus with the sanctioned country (Country A) from within the Society for Worldwide Interbank Financial

Telecommunications (SWIFT) messages, inserting false details or returning it to the customer to resubmit.

The Financial Institutions (FIs) may conceal or remove true originators from the transactions to avoid the sanctions-monitoring programs put in place by those institutions. The FI may weed out, tamper, or even alter the payment details of the transfer. In some instances, some FIs even go a step further and advise originating banks in the sanctioned countries on how to format their transfers to allow the transactions to avoid detection entirely.

As a result of the wire stripping activities, the institutions are subjected to substantial regulatory fines and reputation damage.

To detect potential wire-stripping activity, a FI needs to focus on comparing previously submitted and rejected payments. In many cases, payments are linked to other payments, and discrepancies between these payment pairs may indicate that wire stripping has occurred. A possible detection method for this situation is to compare certain key fields of these payment pairs. This method will require FIs to maintain and leverage historical profiles of payment messages that were blocked or rejected.

TF will generate a suspected wire stripping alert using methodology built into the product and harnessing the power of EDQ.

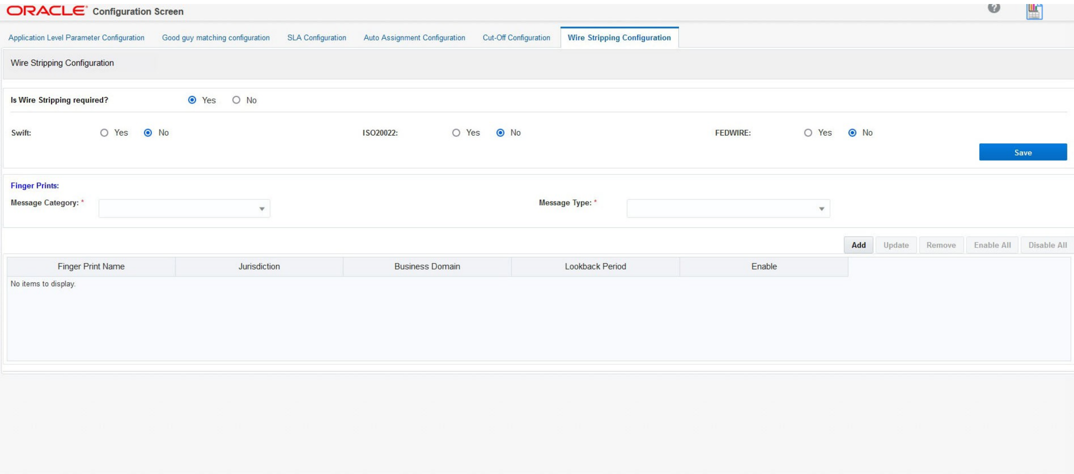
When a message is blocked or rejected by the sanctions team, the transaction is stored in the database of blocked transactions (the property of the transaction is configurable) with a unique identifier code or Fingerprint assigned. Using the Fingerprint, identical wire transfers are identified with variable attributes and a look back period.

The fingerprint is calculated on items such as currency, amount, ordering customer, beneficiary bank or other beneficiary information. Fingerprint contains a combination of multiple fields to compare. You can create multiple rules in Transaction Filtering Admin which will create multiple fingerprints.

To configure the Fingerprint attributes for the Wire Stripping, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** landing page.
2. Click **Transaction Filtering Admin**. The Configuration screen is displayed.
3. Click **Wire Stripping Configuration** tab.

Figure 5-7 Wire Stripping Configuration Tab



ORACLE Configuration Screen
Application Level Parameter Configuration
Good guy matching configuration
SLA Configuration
Auto Assignment Configuration
Cut-Off Configuration
Wire Stripping Configuration
Save
Add
Update
Remove
Enable All
Disable All

Wire Stripping Configuration

Is Wire Stripping required? ● Yes ○ No

Swift: ○ Yes ● No   ISO20022: ○ Yes ● No   FEDWIRE: ○ Yes ● No

Finger Prints:

Message Category: *   Message Type: *

Finger Print Name	Jurisdiction	Business Domain	Lookback Period	Enable
No items to display.				

4. In the **Wire Stripping configuration** section, select **Yes** if wire stripping is required or select **No**
   if wire stripping is not required. By default **No** is selected.

   If you select **Yes**, message category section and Fingerprint sections are enabled.

5. Select **Yes** adjacent to Message Category (Swift, ISO20022 and FEDWIRE) and click **Save** to add the message category to the fingerprint list. You can add multiple message category to the fin- gerprint.

6. In the Fingerprint section, to display the fingerprint list table select the message category from the **Message Category** drop-down list and message type from the **Message Type** drop-down list.
   The Fingerprint list table displays the results for the combination of message category and mes- sage type that you selected.

   To add new fingerprint to the Fingerprint list table click **Add**. The Add Fingerprint Screen is dis- played.

   For information on available message types, see Appendix F: Message Categories and Message Types.

   To add new fingerprint to the Fingerprint list table using the Add Fingerprint Screen, follow the subsequent steps:

   a. Enter the parameter value for the following fields:

      > **Note**
      >
      > The following fields are mandatory.

      - **Fingerprint Details**
        - **Fingerprint Name:** You can enter the desired fingerprint name.
        - **Enable**: Select Yes or No to enable or disable the fingerprint. By default, the value is Y.
        - **Jurisdiction**: Select a jurisdiction name from the drop-down list.
        - **Business Domain**: Select a Business Domain name from the drop-down list.
        - **Look back Period (days)**: Enter the time period in days. The lookback period (days) is the time limit the WS alert generator uses to consider the previous alerts for comparison.
      - **Attribute Details**
        - **Business Data**: Select the Business Data parameter from the drop-down list.
        - **Condition Type**: Select the matching condition type as Exact, Contains, or Percentage Range.

   a. Select the field combinations and click **Add** to add the new fingerprint to the Fingerprint Attribute Table.
      You can add multiple Fingerprint attribute by repeating the above steps with different com- bination.

   b. To edit a fingerprint attribute in the table follow the below steps:

      i. Select the attribute from the Fingerprint Attribute table.

      ii. Edit the Fingerprint details and Attribute details in the Add Fingerprint screen.

iii. Click **Update**.

c. To Remove the fingerprint attribute from the table, select the attribute row and click **Remove**. Click **OK** to confirm.

d. Click **Cancel** to reset the Fingerprint attribute table.

e. Click **Save** to add the Fingerprint with selected Fingerprint attributes for the message type selected in Step 6 in **Fingerprints** section. You can add multiple Fingerprint for the message type with different attribute combinations.

7. The following buttons are enabled when a fingerprint is added/available in the Fingerprint list table:.

- **Update**: To update the selected Fingerprint.
- **Remove:** To delete the selected Fingerprint.
- **Enable All:** To enable all the Fingerprints in the table.
- **Disable All:** To Disable all the Fingerprints in the table.

The selected attribute combinations of Fingerprint for the massage type will be considered to compare the posted message with the previously blocked alerts within the look-back period.

If the current posted message matches with previously compared alerts, a risk score will be generated using the assessment in the IPE. For Wire Stripping Fingerprint Evaluation, a risk score of 100 is preconfigured to create an alert for all matched messages.

For more information on configuring the Wire Stripping Fingerprint risk score, see Configuring Risk Scoring Rules. For more information on alert list, see Oracle Financial Services Transaction Filtering User Guide.

5.6.1 Configuring Business Data Attribute

You can configure the business data for the fingerprint for SWIFT, Fedwire, and ISO20022 message categories. To configure the business data attribute follow the subsequent steps:

- To configure the business data attribute for SWIFT or Fedwire message category, follow the below steps:
  1. Access the Atomic Schema and access the DIM_SANCTIONS_FIELD_DESC table.
  2. Insert the parameters in the columns. For more information See Data Model Reference Guide.
  3. To enable a particular business data attribute in the Fingerprint, add **Y** for the selected busi- ness data in the F_ENABLE_FOR_FINGER_PRINT column.

To configure the business data attribute for ISO20022 message category, follow the below steps:

1. Access the Atomic Schema and access the DIM_TF_XML_MSG_TAG_FLD table.
2. Insert the parameters in the columns. For more information See Data Model Reference Guide .
3. To enable the business data attribute in the Fingerprint, add **Y** for the business data in the

F_ENABLE_FOR_FINGER_PRINT column.

1. After configuring and executing the above step, you must add required conditions for the busi- ness data. To add conditions business data follow the below steps:

a. Access the Atomic Schema and access the FCC_TF_WS_BUS_FLD_COND_MAP table.

b. Enter the input value for the following columns:

   - N_BUSINESS_FLD_ID: For the business field ID, refer N_MSG_TAG_FLD_ID column from DIM_TF_XML_MSG_TAG_FLD table for ISO20022 and N_SANCTION_DESC_CODE column from DIM_SANCTIONS_FIELD_DESC table for SWIFT/Fedwire.
   - N_MSG_CATEG_CODE: For the message category type, refer N_MSG_CATEG_CODE col- umn from DIM_MESSAGE_CATEGORY table.
   - N_CONDITION_ID: For the conditions required for the new business data, refer N_CON- DITION_ID column from FCC_TF_WS_FINGER_PRINT_COND table.

5.6.2 Configuring Wire Stripping Validation for WS Alert Details Screen

You can enable or disable Wire Stripping Validation for WS Alert in Alert Details Screen. To configure the Wire Stripping Validation, follow the subsequent steps:

1. Access the Atomic Schema and access the SETUP_RT_PARAMS table.
2. To disable the Wire Stripping Validation, set the V_ATTRIBUTE_VALUE2 to **N** for V_PARAM_NAME= 'WIRESTRIPPING_FINGERPRINT_CONF' parameter.

To enable the Wire Stripping Validation, set the V_ATTRIBUTE_VALUE2 to **Y** for V_PARAM_NAME= 'WIRESTRIPPING_FINGERPRINT_CONF' parameter.

5.7 Setting the Priority for Messages

You can set the priority for a specific message category as **High**, **Medium**, and **Low** based on certain criteria such as the message jurisdiction, message type, and amount. The seeded message categories are **High**, **Medium**, and **Low**. To add other priority types, add the required priority type in the DIM_ALERT_PRIORITY_TYPE table.

> **Note**
>
> The ready-to-use application extracts some of the key fields of the message into the FSI_RT_MSG_TAG table.

If you want to use any field to define the priority, write an SQL query in the V_ATTRIBUTE_VALUE1

column of the SETUP_RT_PARAMS table. At the end of the query, add the following *where* clause:

where `t.n_grp_msg_id = [GRP_MSG_ID] and rownum = 1`

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

1. Run the following query to view the `SETUP_RT_PARAMS` table:
   select * from `SETUP_RT_PARAMS;`
2. Search for the `MESSAGE_PRIORITY` value in the `V_PARAM_NAME` column.
3. In the `V_ATTRIBUTE_VALUE1` column, write the query or function to define the priority. You can write functions or queries based on your criteria.

5.8 Running the Purge Utility

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

> **Note**
>
> The archival period can be configured by users who have the required permissions under each legal entity policy or local data protection requirements. The archival period also applicable for the AdminGuide_Transaction Filtering_8.0. 7.0.0 and AdminGuide_Transcation Filtering_8.1.1.0.0. For more information, see Sanctions Application Pack.

To run the purge utility, follow these steps:

1. Go to the purgeTF.sh file in the <installed area>/ficdb/bin/ directory and replace the ##Infodom## placeholder with the name of your Infodom.
2. Run the purge utility from the `<installed area>/ficdb/bin/` directory using the following command:
   ./purgeTF.sh <from date in mm/dd/yyyy> <to date in mm/dd/yyyy> S/H S stands for soft delete and H stands for hard delete.

   For example, ./purgeTF.sh 11/11/2019 11/12/2019 S
3. Verify the purge logs in the following directory:
   <installed area>/ficdb/log/TFpurge/ path

5.9 Adding, Editing or Deleting Good Guy Records

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

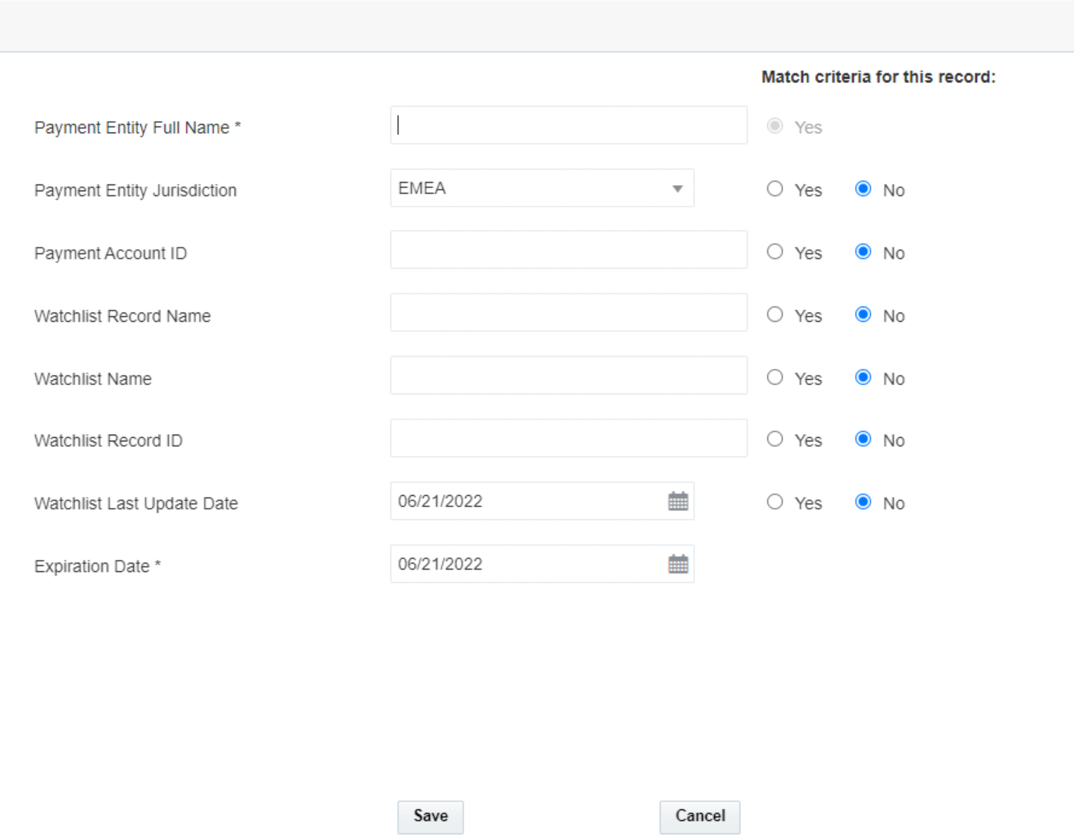
5.9.1 Adding a Good Guy Record

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

To add a record, follow these steps:

1. Click **List Management** on the **Financial Services Analytical Applications Transactions Filtering** landing page.
2. In the **Good Guy Summary** section, click **Add** ✚. A pop-up window is displayed.

Figure 5-8   Good Guy Summary Pop-up Window



Match criteria for this record:

Payment Entity Full Name *		● Yes
Payment Entity Jurisdiction	EMEA	○ Yes ● No
Payment Account ID		○ Yes ● No
Watchlist Record Name		○ Yes ● No
Watchlist Name		○ Yes ● No
Watchlist Record ID		○ Yes ● No
Watchlist Last Update Date	06/21/2022	○ Yes ● No
Expiration Date *	06/21/2022	

3. Enter the required details.
4. Click **Save**.

5.9.2 Editing a Good Guy Record

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

To edit the good guy record, follow these steps:

1. In the **Good Guy Summary** section, click **Actions**.
2. From the drop-down list, click **Edit**.
3. Make the necessary changes to the record.
4. Enter your reasons for editing the record.
5. Click **Save**.

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

5.9.3 Deleting a Good Guy Record

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

To delete the good guy record, follow these steps:

1. In the **Good Guy Summary** section, click **Actions**.
2. From the drop-down list, click **Delete**.
3. Enter your reasons for deleting the record.
4. Click **Save**.

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

- – **V_ORIGIN**: This column contains the watch list name.
  - **V_WHITE_ENTITY_NAME**: This column contains the watch list record name.
  - **V_WHITE_NAME**: This column contains the input message name.
  - **V_IDENTIFIER_CODE**: This column contains the ID of the party name present in the

V_WHITE_NAME column and comes from the input message.

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

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

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

5.9.4 Good Guy Attributes

The system will generate a hash code to capture the current state of attributes on the WL side based on EDQ configuration.

When a name event/match is taking place, and the **Last Updated Date** with fingerprinting option is selected as **Yes**.

If there is no change to the **Last Updated Date** field, then this is considered positive for good guy (match will be considered good guy if all other conditions are met).

If there is a change to the **Last Updated Date** field, then the hashcode will be compared. If they are identical, then this is considered positive for a good guy (match will be considered good guy if all other conditions are met).

The following fields are used for hashcode calculation:

1. WL - entities - prepared data:
   - dnListKey (e.g. "DJW")
   - dnListSubKey (e.g. "DJW-SAN" or "DJW-EDD")
   - dnListRecordType (e.g. "SAN" or "EDD")
   - dnListRecordId (e.g. "1044689")
   - dnOriginalEntityName
   - dnEntityName
   - dnPrimaryName
   - dnOriginalScriptName
   - dnAddress
   - dnCity

   - dnState
   - dnAddressCountryCode
   - dnAddressCountry
   - dnAllCountries
   - dnAllCountryCodes (e.g. "RU")
2. WL - individuals - prepared data
   - dnListKey (e.g. "DJW")
   - dnListSubKey (e.g. "DJW-SAN" or "DJW-EDD")
   - dnListRecordType (e.g. "SAN" or "EDD")
   - dnListRecordId (e.g. "1044689")
   - dnOriginalFullName
   - dnOriginalGivenNames
   - dnOriginalFamilyName
   - dnFullName
   - dnGivenNames
   - dnFamilyName
   - dnPrimaryName
   - dnOriginalScriptName
   - dnAddress
   - dnCity
   - dnState
   - dnAddressCountryCode
   - dnAddressCountry
   - dnAllCountries
   - dnAllCountryCodes (e.g. "RU")

- The fields used for hash code calculation should be configurable by consulting as global configuration (1 set of fields).
- This configuration cannot be changed per list type.
- This is expected to be a 1-time activity that will happen during implementation.

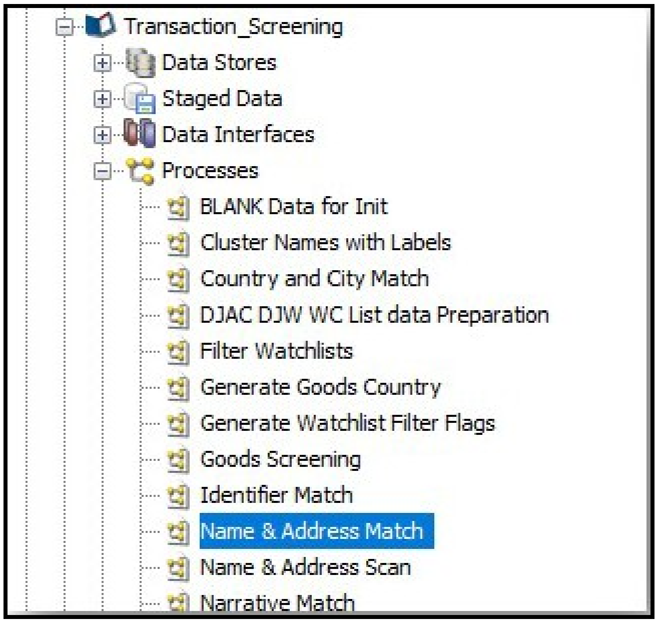
This functionality is expected to work for all types of lists - 3rd party lists and internal lists. This means an analyst should be able to mark a good guy based on an internal list match.

5.9.4.1 Managing the Good Guy Attributes

To change the Good Guy Attributes, follow these steps:

1. From the EDQ URL, open the Director and the Transaction_Screening Project.

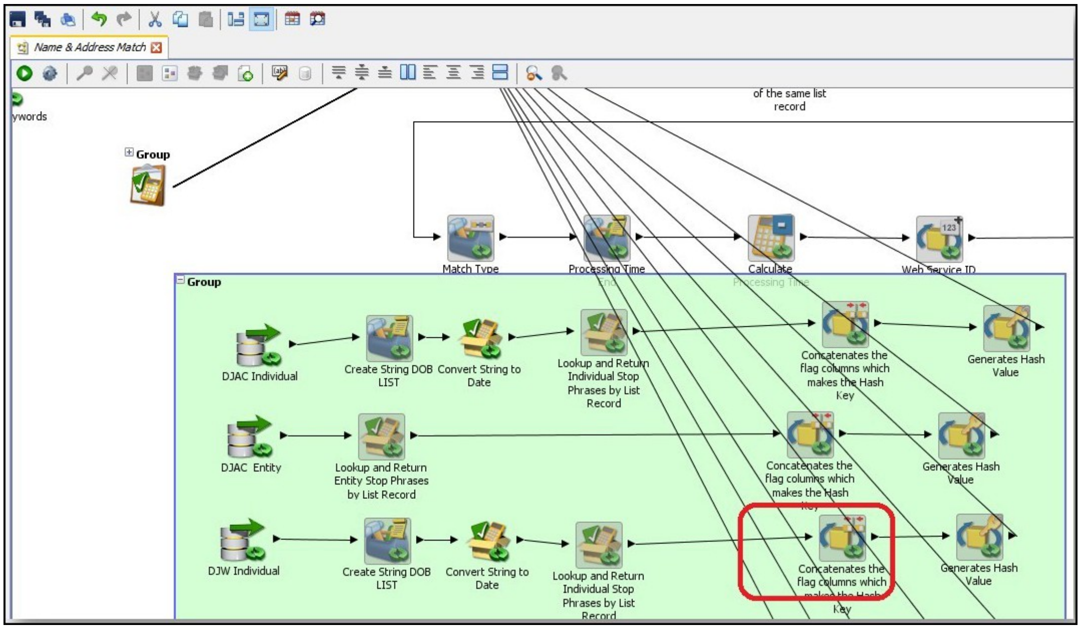
Figure 5-9 Transaction Screening Project



- Transaction_Screening
  - Data Stores
  - Staged Data
  - Data Interfaces
  - Processes
    - BLANK Data for Init
    - Cluster Names with Labels
    - Country and City Match
    - DJAC DJW WC List data Preparation
    - Filter Watchlists
    - Generate Goods Country
    - Generate Watchlist Filter Flags
    - Goods Screening
    - Identifier Match
    - Name & Address Match
    - Name & Address Scan
    - Narrative Match

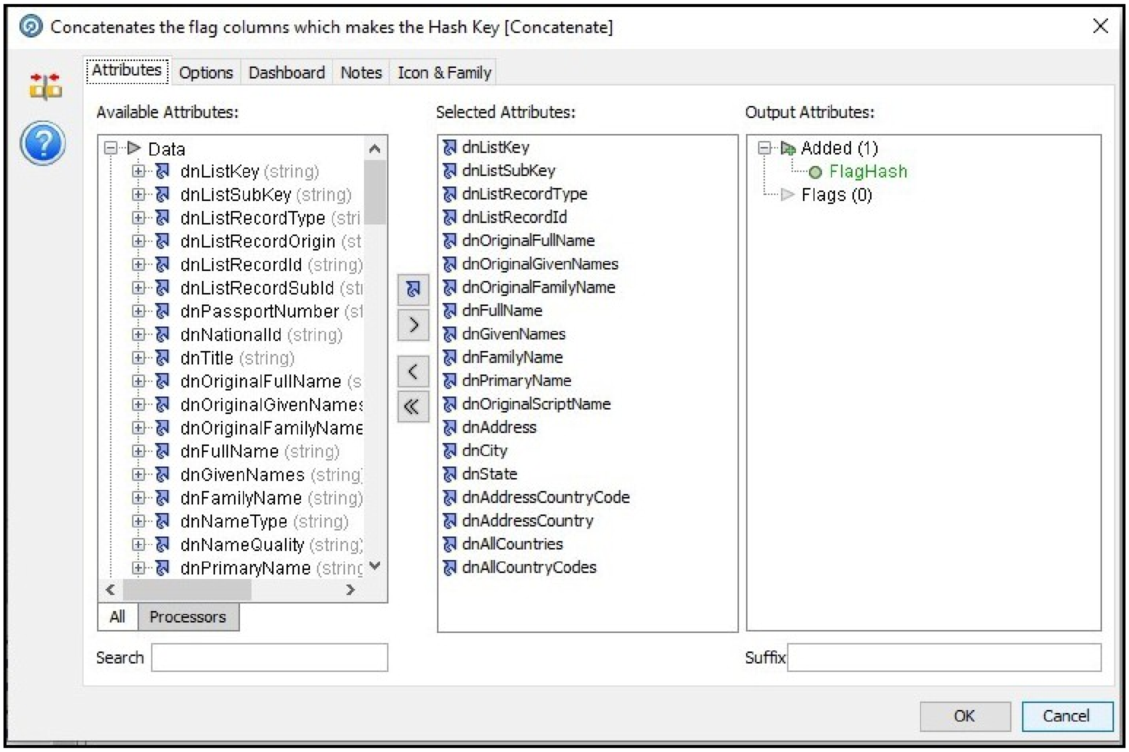
2. From Processes, open the **Name & Address Match**.

Figure 5-10 Name and Address Match


Name & Address Match
ywords
of the same list record
Group
Match Type
Processing Time
Calculate
Web Service ID
Group
DJAC Individual
Create String DOB LIST
Convert String to Date
Lookup and Return Individual Stop Phrases by List Record
Concatenates the flag columns which makes the Hash Key
Generates Hash Value
DJAC Entity
Lookup and Return Entity Stop Phrases by List Record
Concatenates the flag columns which makes the Hash Key
Generates Hash Value
DJW Individual
Create String DOB LIST
Convert String to Date
Lookup and Return Individual Stop Phrases by List Record
Concatenates the flag columns which makes the Hash Key
Generates Hash Value

3. Expand the group and double click "**Concatenates the flag columns which makes the Hash Key**".
4. You can map and unmap required set of attributes to make the hash key.

Figure 5-11 Attributes for Concatenates the flag columns which makes the Hash Key



Available Attributes:

```
Data
  dnListKey (string)
  dnListSubKey (string)
  dnListRecordType (stri
  dnListRecordOrigin (st
  dnListRecordId (string)
  dnListRecordSubId (st
  dnPassportNumber (st
  dnNationalId (string)
  dnTitle (string)
  dnOriginalFullName (s
  dnOriginalGivenNames
  dnOriginalFamilyName
  dnFullName (string)
  dnGivenNames (string)
  dnFamilyName (string)
  dnNameType (string)
  dnNameQuality (string)
  dnPrimaryName (string
```

Selected Attributes:

```
dnListKey
dnListSubKey
dnListRecordType
dnListRecordId
dnOriginalFullName
dnOriginalGivenNames
dnOriginalFamilyName
dnFullName
dnGivenNames
dnFamilyName
dnPrimaryName
dnOriginalScriptName
dnAddress
dnCity
dnState
dnAddressCountryCode
dnAddressCountry
dnAllCountries
dnAllCountryCodes
```

Output Attributes:

```
Added (1)
  FlagHash
Flags (0)
```

5.10 Generating Email for Different Statuses

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

- Notification Email
- Task Email

5.10.1 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
```

A notification email is generated for nearing cut-off/nearing SLA to supervisor and the template is as

follows. Two different emails are sent for cut-off and SLA.

Subject: **Notification-<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
Notification ID : <id>
Message Category: <Message Category> Transaction Type : <Message Type>
Message Reference: <Message Reference> Batch Reference: <Batch Reference>
Transaction Reference: <Transaction Reference>
Status : <HOLD/ASSIGNED/ESCALATED/BLOCK RECOMMENDED/RELEASE RECOMMENDED >
User Comments: <User comments>
Received On : <2017-07-25 12:03:19.0>
Please access the below link to logon to Transaction Filtering System
<Application URL>
 Regards,
Admin
```

5.10.2 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
```

A task email is generated for nearing cut-off/nearing SLA to supervisor and the template is as follows.

Two different emails are sent for cut-off and SLA.

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

```
Hi TFSUPERVISOR/TFANALYST,
This is to inform you that a Notification has been generated for you in your
inbox for
Task ID : <id>
Message Category: <Message Category> Transaction Type : <Message Type>
Message Reference: <Message Reference> Batch Reference: <Batch Reference>
```

```
Transaction Reference: <Transaction Reference>
Status : <Overdue Cut-off/ Overdue SLA> Note: not sure exact status name so
use exact status which are used for cut-off overdue and SLA overdue.
User Comments: <User comments> applicable to escalated only Received On :
2017-07-25 12:03:19.0
Please access the below link to logon to Transaction Filtering System.
<Application URL>
Regards,
Admin
```

5.11 Configuring Alerts in Multiple Jurisdictions and Business Domains

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

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.

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

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

> **Note**
>
> All business domains in the system reside in the FCC_SWIFT_BUS_DMN_MAP table.

5.11.1 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 5-4 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)

   Table 8:

   Table 5-5 Columns used to provide additional information for Jurisdictions

Column	Data Type and Length
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 9:

   Table 5-6 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)

Table 5-6 (Cont.) Columns used to provide additional information for Business Domains

Column	Data Type and Length
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 and map with the additional columns STATUS_CD, ALERT_TYPE_CD.

   Note

   - Refer N_SANCTION_STATUS_CODE column from DIM_SANCTIONS_STATUS table for list of Status codes.
   - Refer N_ALERT_TYPE_CODE column from DIM_SANC_TF_ALERT_- TYPE table for list of alert types.

   If multiple jurisdictions are 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.

   If multiple business domains exist 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 avail- able in the fsi_rt_al_msg_tag table. If the customer wants to use any field as a jurisdiction or business domain from this table, then an SQL query must be written in the Setup_Rt_Param table to extract the respective column.

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

5.11.2 Configurations to Automatically Assign Transactions

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

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

Example:
http://whf00bls:8930/SAN807SEPA/SanctionsService

5.11.3 Configurations to Automatically Release Transactions

To configure a transaction for the *Auto Release* status, run the following query:

select * from fsi_rt_auto_release;

By default, the configuration is empty, which means that no transactions can be auto released. You can set the following values in the fsi_rt_auto_release table:

- Message category in the V_MSG_CATEGORY column. For example, a message category of 1 is mapped to the SWIFT message type by default. To see all default values, run the following query:

select * from dim_message_category;

- Message type in the N_SWIFT_MSG_ID column. For example, a message type of 1 is mapped to the MT101 message type by default. To see all default values, run the following query:

select * from dim_sanctions_swift;

- Jurisdiction in the V_JURISDICTION column.
- Business Domain in the V_BUSINESS_DOMAIN column.
- To see the default values for jurisdiction and business domain, run the following query:

select v_attribute_value1 from setup_rt_params where V_PARAM_NAME in ('MESSAGE_JURISDICTION','MESSAGE_BUSINESS_DOMAIN')

- To enable the configuration, set the **F_ENABLED** column to **Y**.

5.12 Version Control

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

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

5.12.1 Version Control for SWIFT Messages and IPE

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

1. Export the new file using the and save it in your local drive.
2. Import the file into the Transaction Filtering application.

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

5.12.2 Version Control for ISO20022

The steps involved for ISO20022 are explained here:

1. Export the new file and save it in your local drive.
2. Import the file into the Transaction Filtering application.
3. You can now compare this file with another file. Ensure that you place these files in separate folders.

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

5.12.3 Version Control for EDQ

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

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

   menu.
2. Click **View** and select **Configuration Analysis** in the **EDQ Director** menu.
3. In the pop-up which appears, select the versions that you want to compare.
4. Click **Configuration**.
5. In the pop-up which appears, select the differences only and click **OK**.
6. In the same window, select **Start Comparison**. This gives all changes between the two files. For more information, see Oracle Enterprise Data Quality Documentation.

5.13 Running the Migration Utility for SWIFT, Fedwire and ISO20022

Use this migration utility to import and export the SWIFT and Fedwire message configurations. For information on configuring the SWIFT message parameters, see Configuring the SWIFT Message Parameters. For information on configuring the Fedwire message parameters, see Configuring the Fedwire Message Parameters.

The message types provided in this utility are available in the TF_Swift_Migration_Utility/output/MSG_TYPES directory.

To export the configurations, follow these steps:

1. Navigate to the TF_Swift_Migration_Utility/config or TF_Swift_Migration_Util- ity/TF_Swift_Migration_Utlity/config directory. For more information on configuring the migration utility see the readme.txt fie within the folder.
2. Open the Dynamic.properties file and update the placeholders as shown:

Table 5-7 Configurations required in the Dynamic.properties file when running the export file

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

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

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

WARNING

Do not change the folder name to MSG_TYPES. This will overwrite

the ready-to-use message types provided with the utility.

To import the configurations, follow these steps:

1. Navigate to the FIC_HOME/Transaction_Processing/TF_Swift_Migration_Utlity/ config directory.
2. Open the SWIFT_MSG_TYPES.txt file and add the message types that you want to import to the Exported folder mentioned in the export configuration steps.
3. Open the Dynamic.properties file and update the placeholders as shown: **Table 11:**

Table 5-8 Configurations required in the Dynamic.properties file when running the import file

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

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

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

WARNING

Do not change the folder name to MSG_TYPES. This will overwrite

the ready-to-use message types provided with the utility.

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

5.13.1 Restoring a Previous Message Configuration

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

Follow these steps to restore the configuration:

1. Export the message configuration from the environment.

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

2. To restore the previous version, Import the saved configuration.

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

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

5.14 Running the Migration Utility for ISO20022

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

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

1. Navigate to the $FIC_HOME/Transaction_Processing/TF_Config_Migration_Util- ity/config directory.
2. Open the Dynamic.properties file and update the placeholders as shown:

Table 5-9 Configurations required in the Dynamic.properties file when running the export file

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

Table 5-9 (Cont.) Configurations required in the Dynamic.properties file when running the export file

Placeholder	Update with...
##N_XSD_CONF_ID##	Your ISO20022 ID. This is available in the n_xsd_conf_id column in the fcc_tf_xml_xsd_conf table. If you are providing multiple IDs, add the IDs separated by commas. For example, 1,2,3,4.

3. Navigate to the TF_Config_Migration_Utility/bin directory and run the required com- mand.

./export.sh SEPA

To import the configuration, follow these steps:

1. Navigate to the TF_Config_Migration_Utility/config directory.
2. Open the Dynamic.properties file and update the placeholders as shown:

Table 5-10 Configurations required in the Dynamic.properties file when running the import file

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

3. Navigate to the TF_Config_Migration_Utility/bin directory and run the required com- mand.

./ import.sh SEPA.

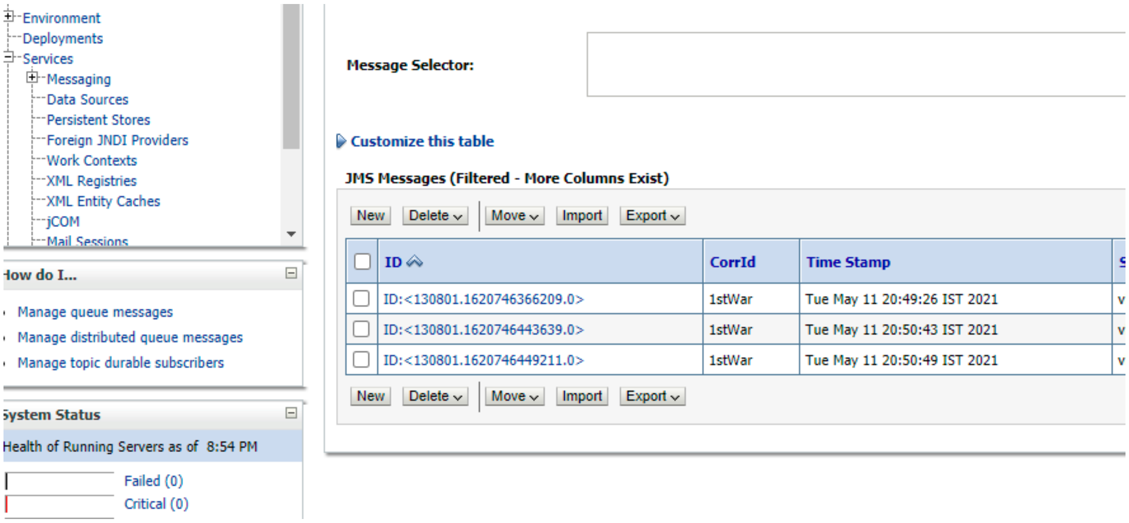
5.15 Configuring JMS Correlation ID

JMS message has two properties (column) called Correlation ID and Message Identifier. To set the Correlation ID, use the following sample code:

See *Code for Adaptor for SWIFT* section in the **Technical Integration Guide**. SourceEntity srcEntity = new SourceEntity(busName); // already there srcEntity.setCorrelationID("12345"); // corrid to be set (Optional)

Both initial and final feedback are set with same correlation ID while sending response to output queue.

Figure 5-12 JMS Message Output Queue



JMS Messages (Filtered - More Columns Exist)

☐	ID	CorrId	Time Stamp	S
☐	ID:<130801.1620746366209.0>	1stWar	Tue May 11 20:49:26 IST 2021	v
☐	ID:<130801.1620746443639.0>	1stWar	Tue May 11 20:50:43 IST 2021	v
☐	ID:<130801.1620746449211.0>	1stWar	Tue May 11 20:50:49 IST 2021	v

5.16 Configuring Parallel Processing

To enable parallel calling of EDQ web services, the following are the new configuration parameters introduced:

Setup_rt_params table:

- ENABLE_PARALLEL_WS_CALL - This Parameter is to indicate if a calling of EDQ Webservices from parser should be parallel or sequential. If the value is set to Y, it will be parallel. If the value is set to N, it will be sequential.
- ENABLE_PARALLEL_WS_TAGS_CALL - This Parameter is to indicate if a calling of EDQ Web- services tags from the parser should be parallel or sequential. If the value is set to Y, it will be parallel. If the value is set to N, it will be sequential. By default OOB, both the parameters will be set to N.

static.properties file:

The following are the new parameters introduced in the static.properties file under

<DeployedContext>/TFLT.ear/TFLT.war/conf:

- – tf.edq.webservices.maxthread.count=6 - This Parameter is used to indicate EDQ Webservices thread count. This creates a thread pool with 6 threads executing the tasks.
  – tf.edq.webservices.tags.maxthread.count=5 - This Parameter is used to indicate EDQ Webservices tags thread count. This creates a thread pool with 5 threads executing the tasks. By default OOB thread count for both parameters is set to 6 and 5, respectively.

5.17 Configuring Additional Columns on the Alert List page

This configuration allows you to add additional column(s) on the Alert Search and List page and view additional information. It also provides the ability to execute the customized query to fetch the data in the columns against each Alert ID and shows the new columns in the

Columns drop-down list while saving the view. To add a column on the Search and List page and filters, follow these steps :

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

   See FCC_SANC_LIST_PAGE_CONFIG.xlsx file for sample entries for Case ID and BIC Code Key

   > **Note**
   >
   > Add an entry only for the `DEFAULT` view.
   >
   > "`TABLE_NAME`" column must have ' `FSI_RT_ALERTS`' value
   >
   > "`COLUMN_NAME`" column must have alias column name value in the parent table like `caseId`, `bicCodeKey` and so on.

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

   See fcc_san_list_config.xlsx file with sample entries for `Case ID` and `BIC Code` Key.

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

   See fcc_san_list_config_tl.xlsx file for sample entries for Case ID and BIC Code Key.

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

4. Update "`v_query`" column in table "`FCC_SANC_LIST_PAGE_QUERY_CONF`" where "`V_QUERY_IDENTIFIER`" column value is ‘`TF_ALERTLIST_GRID`', with the new column details in select query to get the data for new column.

5. Update "`v_query`" column in table "`FCC_SANC_LIST_PAGE_QUERY_CONF`" where "`V_QUERY_IDENTIFIER`" column value is ‘`TF_ALERTLIST_GRID_FROM_QUEUE`', with the new column details in select query to get the data for new column.

6. Update "`v_query`" column in table "`FCC_SANC_LIST_PAGE_QUERY_CONF`" where "`V_QUERY_IDENTIFIER`" column value is ‘`TF_CLOSED_ALERT_GRID`', with the new column details in select query to get the data for new column

7. This is an optional step. Do not follow the below steps if you are trying to configure the column from the existing listed tables in the query do not follow the below steps. If not, follow the below step,

   - update "`v_query`" column in this table "`FCC_SANC_LIST_PAGE_QUERY_CONF`" where "`V_QUERY_IDENTIFIER` " column value is ‘ `TF_ALERTS_COUNT_IN_QUEUE`’ with the new column details in select query to get the updated count value.
   - update "`v_query`" column in this table "`FCC_SANC_LIST_PAGE_QUERY_CONF`" where "`V_QUERY_IDENTIFIER` " column value is ‘ `TF_ALERTS_ZIPPER_COUNT`’ with the new column details in select query to get the updated count value.

5.18 Configuring the Parameters for Highlighting the Matched Data

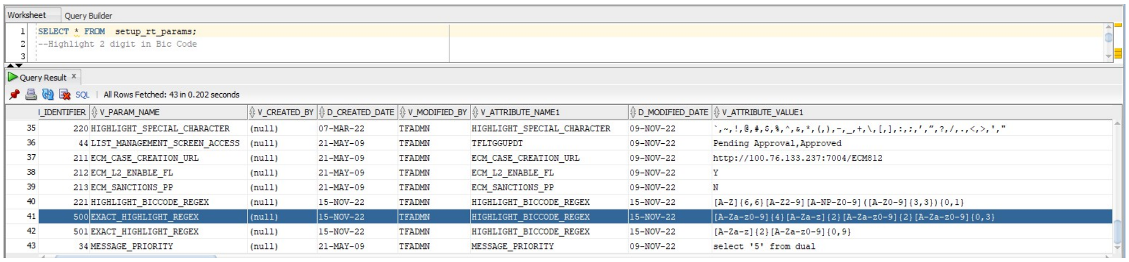
You can configure parameters to highlight the matched data inside tag value when the event parameters match with the alert in the Alert Details page. For more information on Alert Details, see Oracle Financial Services Transaction Filtering User Guide.

To configure the parameters to highlight the matched data inside tag value, follow the below steps:

1. Access the Atomic Schema and access the SETUP_RT_PARAMS table.
2. Insert the attribute value for the required parameters in the table. For example, to consider the matched data for BIC, follow the below steps:
   a. Access the Atomic Schema and access the SETUP_RT_PARAMS table.
   b. Insert the regular expression for EXACT_HIGHLIGHT_REGEX in the table.

For example, the regular expression value[A-Za-z0-9]{4}[A-Za-z]{2}[A-Za-z0- 9]{2}[A-Za-z0-9]{0,3} satisfies BIC codes to highlight the matched data.

Figure 5-13 SETUP_RT_PARAMS



```
SELECT * FROM  setup_rt_params;
--Highlight 2 digit in Bic Code
```

All Rows Fetched: 43 in 0.202 seconds

	I_IDENTIFIER	V_PARAM_NAME	V_CREATED_BY	D_CREATED_DATE	V_MODIFIED_BY	V_ATTRIBUTE_NAME1	D_MODIFIED_DATE	V_ATTRIBUTE_VALUE1
35	220	HIGHLIGHT_SPECIAL_CHARACTER	(null)	07-MAR-22	TFADMN	HIGHLIGHT_SPECIAL_CHARACTER	09-NOV-22	`,~,!,@,#,$,%,^,&,*,(,),-,_,+,\,[,],:,;,',",?,/,.,<,>,',""
36	44	LIST_MANAGEMENT_SCREEN_ACCESS	(null)	21-MAY-09	TFADMN	TFLTGGUPDT	09-NOV-22	Pending Approval,Approved
37	211	ECM_CASE_CREATION_URL	(null)	21-MAY-09	TFADMN	ECM_CASE_CREATION_URL	09-NOV-22	http://100.76.133.237:7004/ECM812
38	212	ECM_L2_ENABLE_FL	(null)	21-MAY-09	TFADMN	ECM_L2_ENABLE_FL	09-NOV-22	Y
39	213	ECM_SANCTIONS_PP	(null)	21-MAY-09	TFADMN	ECM_SANCTIONS_PP	09-NOV-22	N
40	221	HIGHLIGHT_BICCODE_REGEX	(null)	15-NOV-22	TFADMN	HIGHLIGHT_BICCODE_REGEX	15-NOV-22	[A-Z]{6,6}[A-Z2-9][A-NP-Z0-9]([A-Z0-9]{3,3}){0,1}
41	500	EXACT_HIGHLIGHT_REGEX	(null)	15-NOV-22	TFADMN	HIGHLIGHT_BICCODE_REGEX	15-NOV-22	[A-Za-z0-9]{4}[A-Za-z]{2}[A-Za-z0-9]{2}[A-Za-z0-9]{0,3}
42	501	EXACT_HIGHLIGHT_REGEX	(null)	15-NOV-22	TFADMN	HIGHLIGHT_BICCODE_REGEX	15-NOV-22	[A-Za-z]{2}[A-Za-z0-9]{0,9}
43	34	MESSAGE_PRIORITY	(null)	21-MAY-09	TFADMN	MESSAGE_PRIORITY	09-NOV-22	select '5' from dual

```
MERGE INTO SETUP_RT_PARAMS T USING (
SELECT '500' N_PARAM_IDENTIFIER, 'EXACT_HIGHLIGHT_REGEX' V_PARAM_NAME, ''
V_CREATED_BY, to_date('15-11-2022' , 'dd-mm-yyyy') D_CREATED_DATE, 'TFADMN'
V_MODIFIED_BY, 'HIGHLIGHT_BICCODE_REGEX' V_ATTRIBUTE_NAME1, to_date('15-11-
2022' , 'dd-mm-yyyy') D_MODIFIED_DATE, '[A-Z]{6,6}[A-Z2-9][A-NP-Z0-9]([A-Z0-
9]{3,3}){0,1}' V_ATTRIBUTE_VALUE1, '' V_ATTRIBUTE_NAME2, ''
V_ATTRIBUTE_VALUE2, '' V_ATTRIBUTE_NAME3, '' V_ATTRIBUTE_VALUE3, ''
V_ATTRIBUTE_NAME4, '' V_ATTRIBUTE_VALUE4, 'List of BIC codes to be used to
highlight 2 digit county code within the matches.' V_ATTRIBUTE1_DESCRIPTION,
'' V_ATTRIBUTE2_DESCRIPTION, '' V_ATTRIBUTE3_DESCRIPTION, ''
V_ATTRIBUTE4_DESCRIPTION, '' V_PARAM_DESC, '' V_ATTRIBUTE_NAME5, ''
V_ATTRIBUTE5_DESCRIPTION, '' V_ATTRIBUTE_VALUE5 FROM DUAL) S
ON ( T.N_PARAM_IDENTIFIER = S.N_PARAM_IDENTIFIER )
WHEN MATCHED THEN UPDATE SET T.V_PARAM_NAME = S.V_PARAM_NAME, T.V_CREATED_BY
= S.V_CREATED_BY, T.D_CREATED_DATE = S.D_CREATED_DATE, T.V_MODIFIED_BY =
S.V_MODIFIED_BY, T.V_ATTRIBUTE_NAME1 = S.V_ATTRIBUTE_NAME1, T.D_MODIFIED_DATE
= S.D_MODIFIED_DATE, T.V_ATTRIBUTE_VALUE1 = S.V_ATTRIBUTE_VALUE1,
T.V_ATTRIBUTE_NAME2 = S.V_ATTRIBUTE_NAME2, T.V_ATTRIBUTE_VALUE2 =
S.V_ATTRIBUTE_VALUE2, T.V_ATTRIBUTE_NAME3 = S.V_ATTRIBUTE_NAME3,
T.V_ATTRIBUTE_VALUE3 = S.V_ATTRIBUTE_VALUE3, T.V_ATTRIBUTE_NAME4 =
S.V_ATTRIBUTE_NAME4, T.V_ATTRIBUTE_VALUE4 = S.V_ATTRIBUTE_VALUE4,
T.V_ATTRIBUTE1_DESCRIPTION = S.V_ATTRIBUTE1_DESCRIPTION,
T.V_ATTRIBUTE2_DESCRIPTION = S.V_ATTRIBUTE2_DESCRIPTION,
T.V_ATTRIBUTE3_DESCRIPTION = S.V_ATTRIBUTE3_DESCRIPTION,
T.V_ATTRIBUTE4_DESCRIPTION = S.V_ATTRIBUTE4_DESCRIPTION, T.V_PARAM_DESC =
S.V_PARAM_DESC, T.V_ATTRIBUTE_NAME5 = S.V_ATTRIBUTE_NAME5,
T.V_ATTRIBUTE5_DESCRIPTION = S.V_ATTRIBUTE5_DESCRIPTION, T.V_ATTRIBUTE_VALUE5
= S.V_ATTRIBUTE_VALUE5
WHEN NOT MATCHED THEN INSERT
 (N_PARAM_IDENTIFIER,V_PARAM_NAME,V_CREATED_BY,D_CREATED_DATE,V_MODIFIED_BY,V
 _ATTRIBUTE_NAME1,D_MODIFIED_DATE,V_ATTRIBUTE_VALUE1,V_ATTRIBUTE_NAME2,V_ATTR
IBUTE_VALUE2,V_ATTRIBUTE_NAME3,V_ATTRIBUTE_VALUE3,V_ATTRIBUTE_NAME4,V_ATTRIB
UTE_VALUE4,V_ATTRIBUTE1_DESCRIPTION,V_ATTRIBUTE2_DESCRIPTION,V_ATTRIBUTE3_DE
SCRIPTION,V_ATTRIBUTE4_DESCRIPTION,V_PARAM_DESC,V_ATTRIBUTE_NAME5,V_ATTRIBUT
E5_DESCRIPTION,V_ATTRIBUTE_VALUE5)
VALUES
 (S.N_PARAM_IDENTIFIER,S.V_PARAM_NAME,S.V_CREATED_BY,S.D_CREATED_DATE,S.V_MOD
IFIED_BY,S.V_ATTRIBUTE_NAME1,S.D_MODIFIED_DATE,S.V_ATTRIBUTE_VALUE1,S.V_ATTR
IBUTE_NAME2,S.V_ATTRIBUTE_VALUE2,S.V_ATTRIBUTE_NAME3,S.V_ATTRIBUTE_VALUE3,S.
V_ATTRIBUTE_NAME4,S.V_ATTRIBUTE_VALUE4,S.V_ATTRIBUTE1_DESCRIPTION,S.V_ATTRIB
UTE2_DESCRIPTION,S.V_ATTRIBUTE3_DESCRIPTION,S.V_ATTRIBUTE4_DESCRIPTION,S.V_P
ARAM_DESC,S.V_ATTRIBUTE_NAME5,S.V_ATTRIBUTE5_DESCRIPTION,S.V_ATTRIBUTE_VALUE
5)
```

/

5.19 Configuring Select All Option for the Events Table

This configuration allows you to enable and disable **Select All** option feature for the events table in alerts details page. For more information on alert details and event table, see Oracle Financial Services Transaction Filtering User Guide.

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

1. Access the Atomic Schema and access the SETUP_RT_PARAMS table.
2. For the TF_SELECT_ALL_EVENTS_FLAG parameter enter the V_ATTRIBUTE_VALUE1 value as **Y** to enable the **Select All** check box in the event table for the match summary. Enter N to disable the **Select All** check box.

5.20 Configuring Bulk Action Feature for the Alert List

This configuration allows you to enable and disable **Bulk Action** feature in the alerts list page. For more information on alert list page, see Oracle Financial Services Transaction Filtering User Guide.

To configure bulk action feature in the alert list page, follow the below steps:

1. Access the Atomic Schema and access the SETUP_RT_PARAMS table.
2. For the ENABLE_BULK_ACTION_FLAG parameter enter the V_ATTRIBUTE_VALUE1 value as **Y** to enable the **Bulk Action** feature in the alert list page. Enter N to disable the **Bulk Action** fea- ture.

5.21 Retrigger Functionality

While posting the SWIFT/Fedwire/ISO20022 messages, if any of the EDQ web service pointing to the application is down, messages will be retriggered once all the required web services are up.

The Retrigger configuration parameters are:

- RETRIGGER_INTERVAL_MINS parameter in the setup_rt_params table under atomic schema. By default, V_ATTRIBUTE_VALUE1 value is set to 30 min which are customizable and can be changed (increased/decreased) as per user requirement.
- RETRIGGER_MAX_RETRIES parameter in the setup_rt_params table under atomic schema. By default, V_ATTRIBUTE_VALUE1 value is set to 5, which is customizable and can be changed (increased/decreased) as per user requirement. Once the max value is reached per message, the retrigger loop will be terminated, and the V_RETRY_STATUS_CD parameter is updated to T for the particular message in FSI_RT_RAW_DATA table.

5.21.1 Configuring Data Source in WebLogic Application Server

If the ENABLE_PARALLEL_WS_CALL and ENABLE_PARALLEL_WS_TAGS_CALL parameter values are **Y** in the SETUP_RT_PARAMS table, it is recommended to perform the following configuration in Weblogic Application Server to avoid retrigger failure.

1. Open WebLogic Application Server. For more information, see Oracle Financial ServicesSanctions Pack Installation and Configuration Guide.
2. From the LHS menu (Domain Structure), click Services **Data Sources**. The Summary of JDBC Data Sources window is displayed.
3. Select **SANCINFO** from the **Data Sources** table. The Settings for SANCINFO window is displayed.
4. Select the **Connection Pool** tab.
5. Click **Advanced.** The Advanced informations are displayed.
6. Click and select the **Test Connections On Reserve** Check box and enter the value as **SQL IS VALID** in Test Table Name.
7. Click **Save**.

5.22 Multiple wars deployment configuration

We introduced a new parameter named `node.id` in `static.properties` file.

It has to be changed based on the EAR file.

For example, if you have multiple EARs like TFLT, TFLT1, TFLT2, make sure node.id value should be same and unique as the EAR name.

It helps in finding which messages are processed through which EAR and the same helps in re- triggering them properly.

6 Configuring the SWIFT Message Parameters

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

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** landing page.
2. Click **SWIFT Configuration Admin**. The **Message and Screening Configurations** tab is dis- played.

> **Note**
>
> The following screens are the same for the Fedwire and SWIFT message parameters.

This tab has the following windows:

- – Message and Screening Configurations Window
  - – <Message Type> Subfield Level Configuration Window
  - – <Message Type> Screening Configuration Window
  - – <Message Type> Other Field/Subfield Configuration Window

6.1 Message and Screening Configurations Window

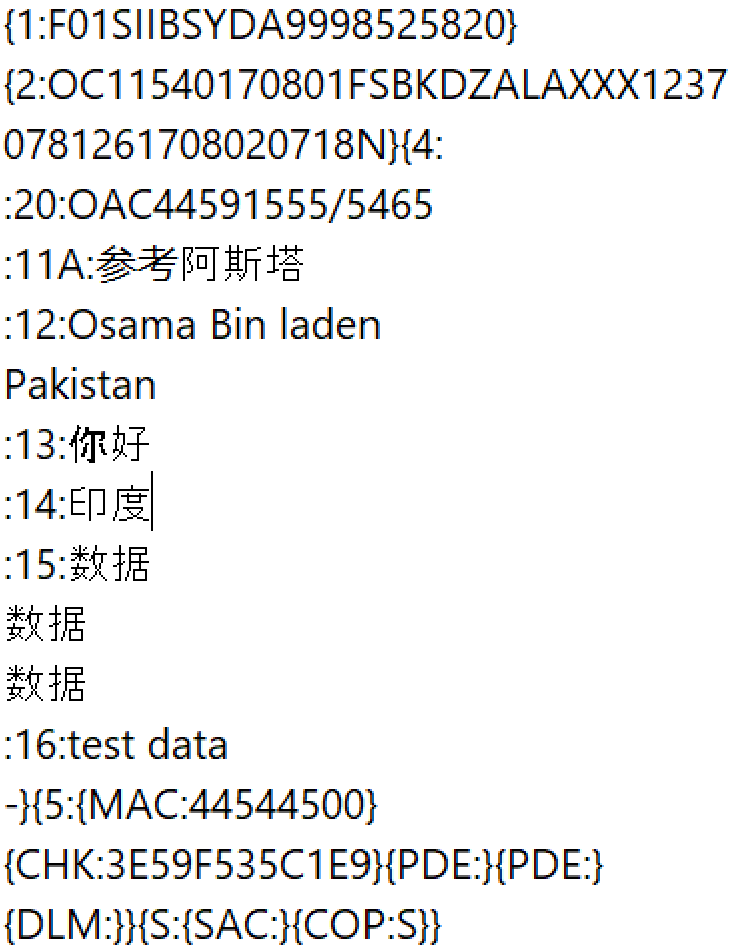
This window allows you to edit the status, field names, and expressions of the different JSON parameters in the message.

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

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

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

Figure 6-1   Sample format for MTC11/MTC22/MTC33/MTC44 SWIFT message type



```
{1:F01SIIBSYDA9998525820}
{2:OC11540170801FSBKDZALAXXX1237
0781261708020718N}{4:
:20:OAC44591555/5465
:11A:参考阿斯塔
:12:Osama Bin laden
Pakistan
:13:你好
:14:印度
:15:数据
数据
数据
:16:test data
-}{5:{MAC:44544500}
{CHK:3E59F535C1E9}{PDE:}{PDE:}
{DLM:}}{S:{SAC:}{COP:S}}
```

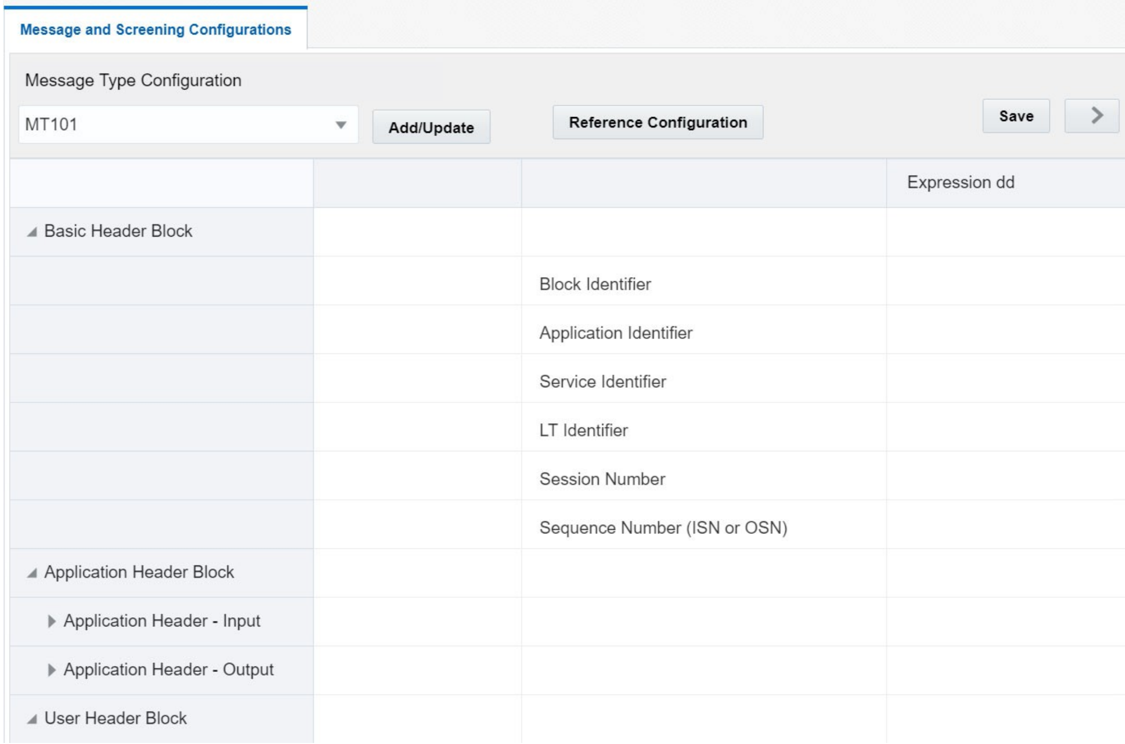
In this example, C11 can be either 11 or 11A and not 111. So, the tag can either start with two numbers or two numbers and one alphabet. The value in the 11A tag represents 100k in the JSON expression, and the value in the 15 tag represents 100*100k in the JSON expression.

A sample JSON is shown:

```
{
"attr": {
"id": "t4:2:2",
"field": "12",
"status": "M",
"fieldName": "Entity Type", "expression": "100k", "regex": "",
"editable": "Y"
}
},
{
"attr": {
"id": "t4:2:3",
"field": "13",
"status": "M",
"fieldName": "Entity Relationship",
"expression": "100*100k", "regex": "",
"editable": "Y"
}
},
```

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

Figure 6-2 Message and Screening Configurations Window for SWIFT



Message Type Configuration

MT101

			Expression dd
◢ Basic Header Block			
		Block Identifier	
		Application Identifier	
		Service Identifier	
		LT Identifier	
		Session Number	
		Sequence Number (ISN or OSN)	
◢ Application Header Block			
▶ Application Header - Input			
▶ Application Header - Output			
◢ User Header 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 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.

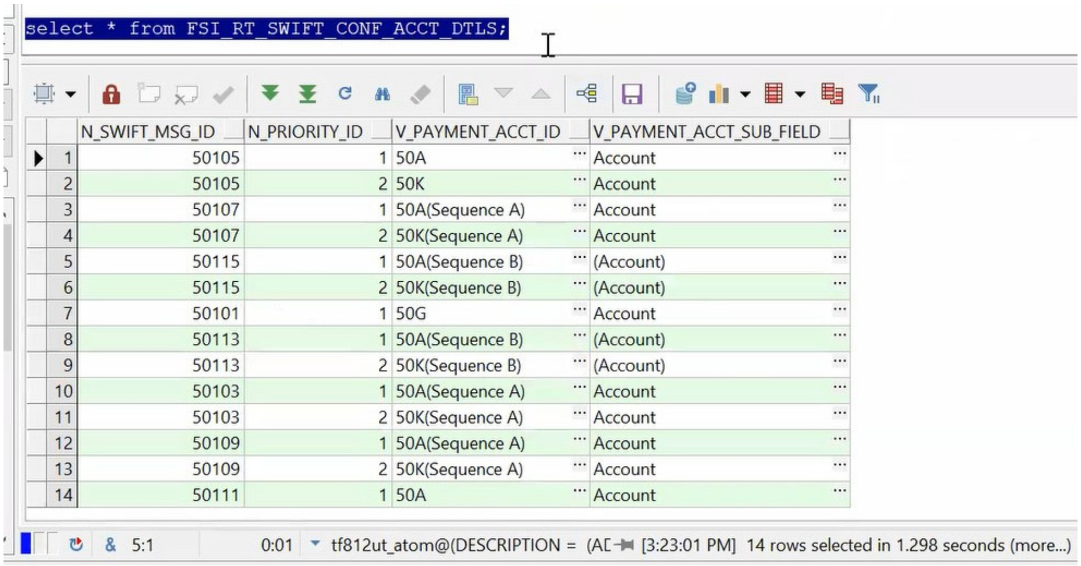
To edit a parameter, click the parameter name. After you make the changes, click **Save**.

6.1.1 Adding or Updating 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 6-3 Attachment Details Window



```
select * from FSI_RT_SWIFT_CONF_ACCT_DTLS;
```

	N_SWIFT_MSG_ID	N_PRIORITY_ID	V_PAYMENT_ACCT_ID	V_PAYMENT_ACCT_SUB_FIELD
1	50105	1	50A	Account
2	50105	2	50K	Account
3	50107	1	50A(Sequence A)	Account
4	50107	2	50K(Sequence A)	Account
5	50115	1	50A(Sequence B)	(Account)
6	50115	2	50K(Sequence B)	(Account)
7	50101	1	50G	Account
8	50113	1	50A(Sequence B)	(Account)
9	50113	2	50K(Sequence B)	(Account)
10	50103	1	50A(Sequence A)	Account
11	50103	2	50K(Sequence A)	Account
12	50109	1	50A(Sequence A)	Account
13	50109	2	50K(Sequence A)	Account
14	50111	1	50A	Account

```
5:1    0:01    tf812ut_atom@(DESCRIPTION = (AD    [3:23:01 PM]  14 rows selected in 1.298 seconds (more...)
```

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.

6.1.2 Repeating Sequences

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

6.1.3 Configuring the References

To view and change the message reference or transaction reference, click **Reference Configuration**. Reference Configuration tab has the following fields:

- Message Identifier
- Transaction Reference
- Payment Account ID
  - Field
  - Field/Subfield Name

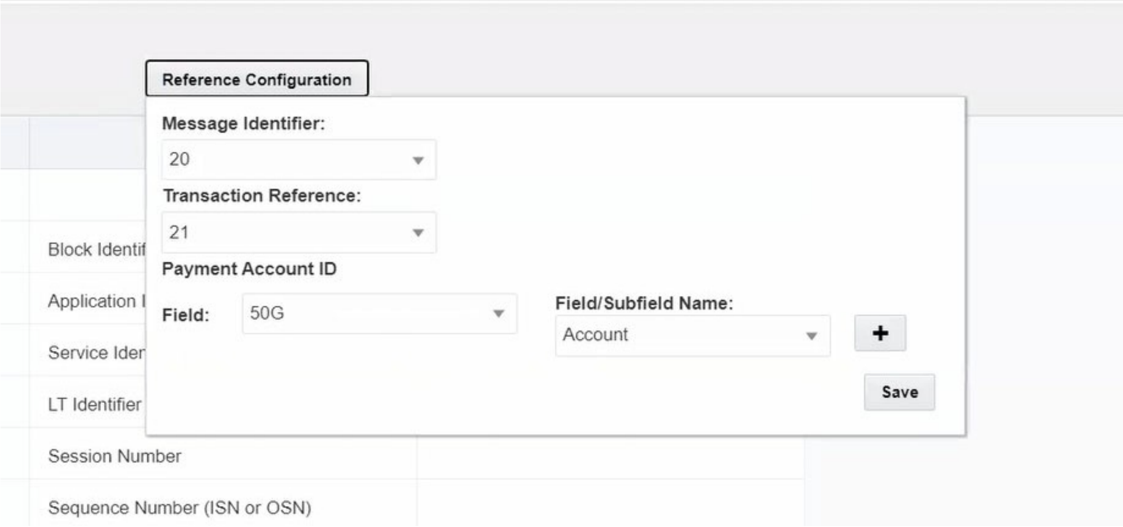
Any message which contains message references or transaction references, or both, must be configured.

For the **Message Reference** field, a unique identifier must be configured at the message level for all message categories.

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

For the **Payment Account ID** field, a unique identifier can be configured for each message type. You can enter multiple field values for **Payment Account ID** by clicking the plus icon.

Figure 6-4   Reference Configuration Window



Reference Configuration

Message Identifier: 20

Transaction Reference: 21

Payment Account ID

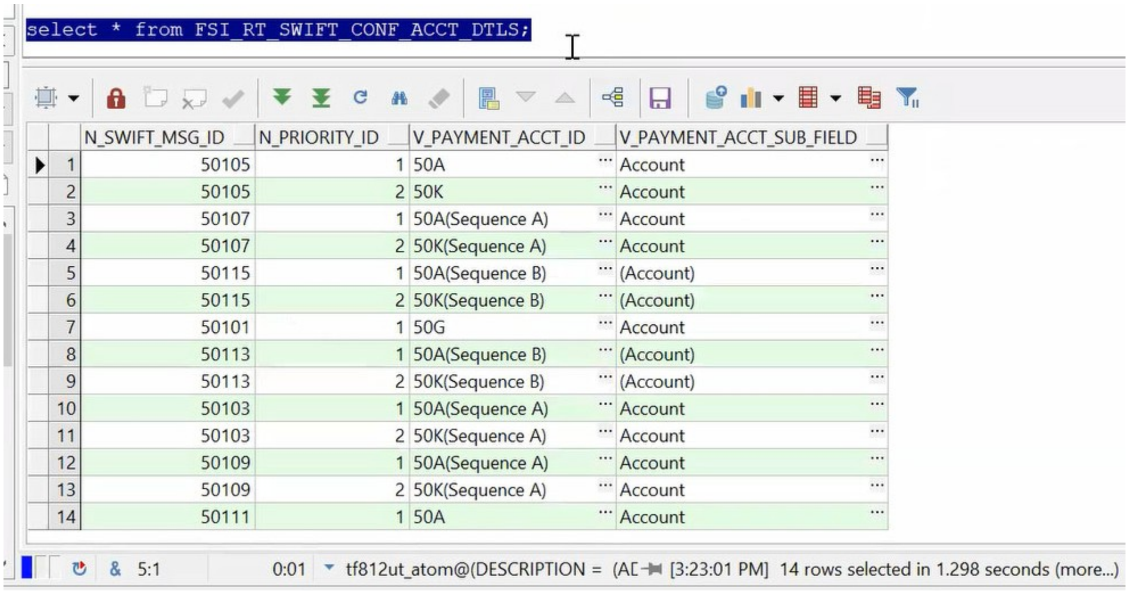
Field: 50G

Field/Subfield Name: Account

Newly added entries for the Payment account ID are stored in the FSI_RT_SWIFT_CONF_ACCT_DTLS

table.

Figure 6-5 FSI_RT_SWIFT_CONF_ACCT_DTLS Table



```
select * from FSI_RT_SWIFT_CONF_ACCT_DTLS;
```

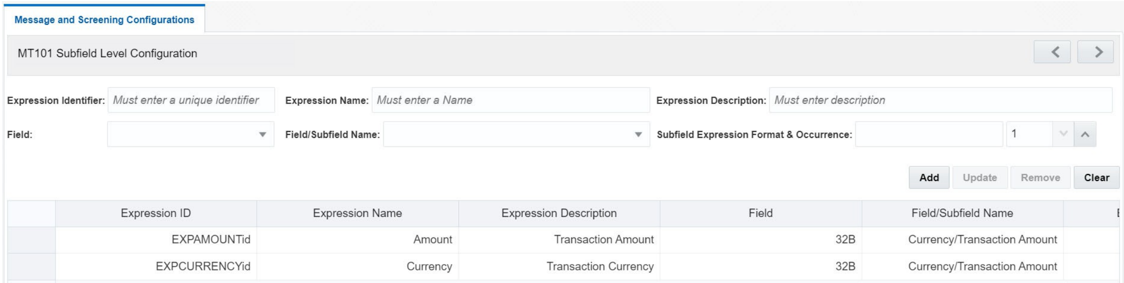
	N_SWIFT_MSG_ID	N_PRIORITY_ID	V_PAYMENT_ACCT_ID	V_PAYMENT_ACCT_SUB_FIELD
1	50105	1	50A	Account
2	50105	2	50K	Account
3	50107	1	50A(Sequence A)	Account
4	50107	2	50K(Sequence A)	Account
5	50115	1	50A(Sequence B)	(Account)
6	50115	2	50K(Sequence B)	(Account)
7	50101	1	50G	Account
8	50113	1	50A(Sequence B)	(Account)
9	50113	2	50K(Sequence B)	(Account)
10	50103	1	50A(Sequence A)	Account
11	50103	2	50K(Sequence A)	Account
12	50109	1	50A(Sequence A)	Account
13	50109	2	50K(Sequence A)	Account
14	50111	1	50A	Account

```
5:1    0:01    tf812ut_atom@(DESCRIPTION = (AD    [3:23:01 PM]  14 rows selected in 1.298 seconds (more...)
```

6.2 <Message Type> Subfield Level Configuration Window

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

Figure 6-6 <Message Type> Subfield Level Configuration Window



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 & Occurrence: 1

	Expression ID	Expression Name	Expression Description	Field	Field/Subfield Name
	EXPAMOUNTid	Amount	Transaction Amount	32B	Currency/Transaction Amount
	EXPCURRENCYid	Currency	Transaction Currency	32B	Currency/Transaction Amount

1. To add a subfield, provide the required values in the fields shown in the window and click **Add**

   Figure 6-7 Add

   Enter values in the following fields:

Table 6-1   Fields in the <Message Type> Subfield Level Configuration Window

Fields	Field Description
Expression Identifier	Enter a unique identifier. It must begin with an alpha character and must not contain any spaces. This is a mandatory field.
Expression Name	Enter a name for the expression. The name must be in capital letters. This is a mandatory field.
Expression Description	Enter a description for the Expression. This is a mandatory field.
Field	This field displays a complete list of fields in the drop-down for the given message type. Select the field from this drop-down field to configure the expression.
Field/Subfield Name	This field displays the respective field name or subfield options for the field that was previously selected. Select the subfield from the drop- down list.

Table 6-2   Fields in the <Message Type> Subfield Level Configuration Window

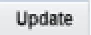
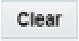
Fields	Field Description
Subfield Expression Format & Occurrence	This field is populated when the Field is selected. Select an expression as it as or an element from that expression. You can also enter the number of occurrences for the expression within that message. By default, it is always 1.
Add button	To add a subfield, provide the required values in the fields shown above and click **Add** **Figure 6-8 Add**
Update button	To update an existing subfield, click the name of the subfield. After you make the changes, click **Update** **Figure 6-9 Update**  .

Table 6-2 (Cont.) Fields in the <Message Type> Subfield Level Configuration Window

Fields	Field Description
Remove button	To remove an existing subfield, click the name of the subfield and click **Remove** **Figure 6-10 Remove** .
Clear button	To clear the data in these fields, click **Clear** **Figure 6-11 Clear**  .

2. To update an existing subfield, click the name of the subfield. After you make the changes, click **Update.**
3. To remove an existing subfield, click the name of the subfield and click **Remove**.
4. To clear the data in these fields, click **Clear**.

You can configure the subfield in two ways:

- By configuring the **subfield level data within the option** expression: Do this if you want to configure specific data within the expression.
  For example, if field 57 has four options A, B, C, and D in MT103 message but you want to configure BIC (Identifier Code) from option A:

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

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

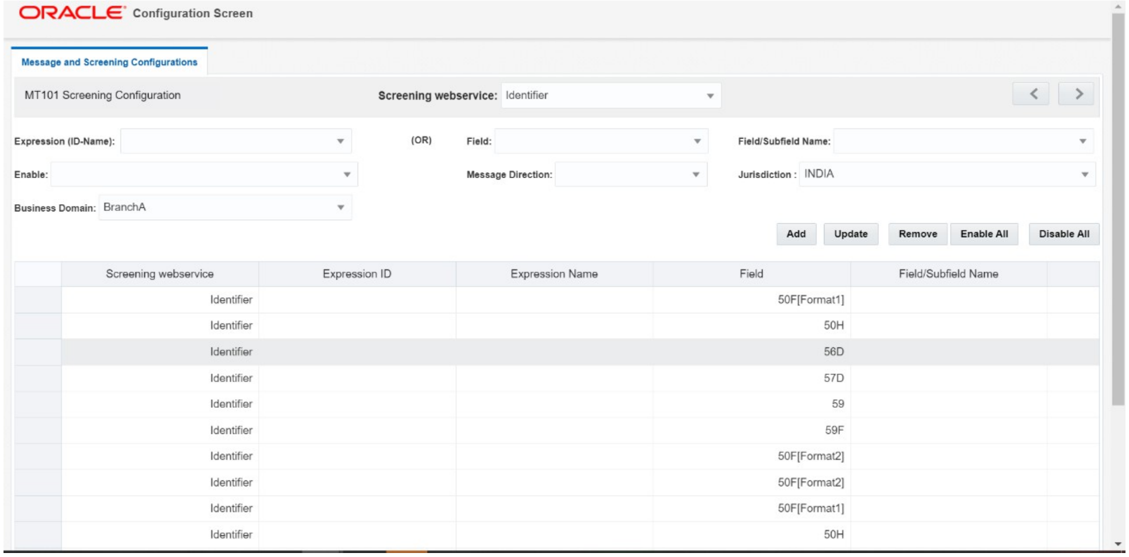
- In this example, if you want to configure the country code for field 57, then you can configure 2!a from Identifier Code expression as a country code by giving unique names in the **Sub- field Expression Identifier**, **Subfield Name**, and **Subfield Description** fields.
  By configuring the element level data within the subfield expression: Do this if you want to further configure any data out of the subfield.

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

6.3 <Message Type> Screening Configuration Window

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

Figure 6-12 <Message Type> Screening Configuration Window



Configuration Screen

MT101 Screening Configuration

Screening webservice: Identifier

Expression (ID-Name): (OR) Field: Field/Subfield Name:

Enable: Message Direction: Jurisdiction : INDIA

Business Domain: BranchA

Screening webservice	Expression ID	Expression Name	Field	Field/Subfield Name
Identifier			50F[Format1]	
Identifier			50H	
Identifier			56D	
Identifier			57D	
Identifier			59	
Identifier			59F	
Identifier			50F[Format2]	
Identifier			50F[Format2]	
Identifier			50F[Format1]	
Identifier			50H	

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

Table 6-3 Fields in the <Message Type> Screening Configuration Window

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

Table 6-3 (Cont.) Fields in the <Message Type> Screening Configuration Window

Fields	Field Description
Message Direction	Select **INBOUND(o)** and **OUTBOUND(i)** based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select **inbound**, else select **outbound**. If that field must be screened for both inbound and outbound, then select **ANY**.

Table 6-4 Fields in the <Message Type> Screening Configuration Window

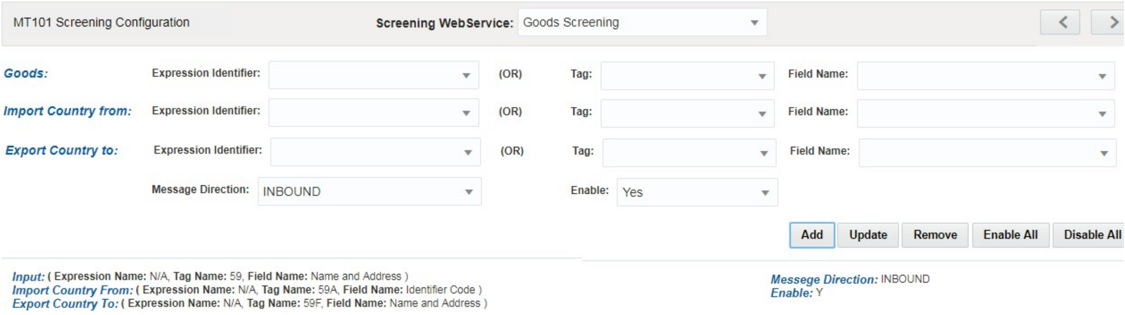
Fields	Field Description
Jurisdiction	Select **All** to apply the Webservice for all jurisdictions or select the specific jurisdiction to apply the webservice for a specific jurisdiction. Use the kdd_jrsdcn table to configure the jurisdiction values. It has the following columns: • JRSDCN_CD: Values must be unique. • JRSDCN_NM: Actual jurisdiction name. • JRSDCN_DSPLY_NM: Jurisdiction name displayed in the Message and Configurations screen. • JRSDCN_DESC_TX: Optional field to adbusinesd descriptions for the jurisdictions.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** **Figure 6-13 Add** .
Update button	To update a web service, select the web service that you want to update and click **Update** **Figure 6-14 Update** .

Table 6-4 (Cont.) Fields in the <Message Type> Screening Configuration Window

Fields	Field Description
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** **Figure 6-15 Remove** .
Enable All button	To enable all web services, click **Enable All** **Figure 6-16 Enable All** .
Disable All button	To disable all web services, click **Disable All** **Figure 6-17 Disable All** .

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

Figure 6-18 Fields for Goods Web Services



MT101 Screening Configuration

Screening WebService: Goods Screening

Goods:	Expression Identifier:		(OR)	Tag:		Field Name:
Import Country from:	Expression Identifier:		(OR)	Tag:		Field Name:
Export Country to:	Expression Identifier:		(OR)	Tag:		Field Name:
	Message Direction:	INBOUND		Enable:	Yes	

Input: (**Expression Name:** N/A, **Tag Name:** 59, **Field Name:** Name and Address)
Import Country From: (**Expression Name:** N/A, **Tag Name:** 59A, **Field Name:** Identifier Code)
Export Country To: (**Expression Name:** N/A, **Tag Name:** 59F, **Field Name:** Name and Address)

Messege Direction: INBOUND
Enable: Y

Table 6-5   Fields in the Goods Web Service Window

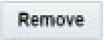
Fields	Field Description
Expression Identifier	Select the Expression for the good.
Tag	Select the tag related to the good. Based on the tag selected, the field name is populated.
Field Name	The field name is populated based on the tag selected.
Message Direction	Select **INBOUND(o)** and **OUTBOUND(i)** based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select **inbound**, else select **outbound**. If that field must be screened for both inbound and outbound, then select **ANY**.
Enable	Select **Yes** to enable the message in a direction. Select **No** to disable the message in a direction.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** **Figure 6-19 Add** .
Update button	To update a web service, select the web service that you want to update and click **Update** **Figure 6-20 Update** .
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** **Figure 6-21 Remove**  .

Table 6-5 (Cont.) Fields in the Goods Web Service Window

Fields	Field Description
Enable All button	To enable all web services, click **Enable All** **Figure 6-22 Enable All** .
Disable All button	To disable all web services, click **Disable All** **Figure 6-23 Disable All** .

6.3.1 Enabling or Disabling a Web Service

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

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

Table 6-6 Web Services in Transaction Filtering

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

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

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

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

6.3.2 Updating and Removing a Web Service

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

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

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

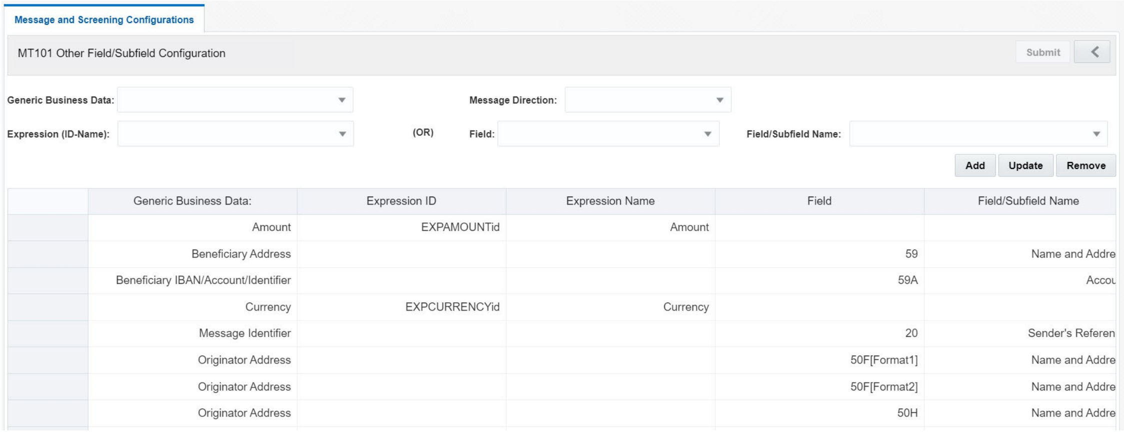
Data for the Trade goods and Trade port web services are taken from a reference table. To populate data for these web services, do this:

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

6.4 <Message Type> Other Field/Subfield Configuration Window

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

Figure 6-24 <Message Type> Other Field/Subfield Configuration Window



MT101 Other Field/Subfield Configuration

Generic Business Data:
Message Direction:
Expression (ID-Name): (OR) Field:
Field/Subfield Name:

	Generic Business Data:	Expression ID	Expression Name	Field	Field/Subfield Name
	Amount	EXPAMOUNTid	Amount		
	Beneficiary Address			59	Name and Addre
	Beneficiary IBAN/Account/Identifier			59A	Accou
	Currency	EXPCURRENCYid	Currency		
	Message Identifier			20	Sender's Referen
	Originator Address			50F[Format1]	Name and Addre
	Originator Address			50F[Format2]	Name and Addre
	Originator Address			50H	Name and Addre

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

Table 6-7   Fields in the <Message Type> Other Field/Subfield Configuration Window

Fields	Field Description
Generic Business Data	This field displays the Business Name of the record that is selected. It is mandatory to configure this field. If the message contains one or more of the B, C, D, or E sequences, you must configure the field with the first tag of the sequence according to the SWIFT standard.
Message Direction	Select **INBOUND(o)** and **OUTBOUND(i)** based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select **inbound**, else select **outbound**. If that field must be screened for both inbound and outbound, then select **ANY**.
Expression (ID-Name)	Select an expression identifier. When you select an expression identifier, the values are populated in the **Field** and **Field/Subfield Name** fields.
Field	Select the field name.
Field/Subfield Name	Select the Subfield Name. This displays the Expression.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** **Figure 6-25 Add** .
Update button	To update a web service, select the web service that you want to update and click **Update** **Figure 6-26 Update** .

Table 6-8   Fields in the <Message Type> Other Field/Subfield Configuration Window

Fields	Field Description
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** **Figure 6-27 Remove** Remove .

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

7

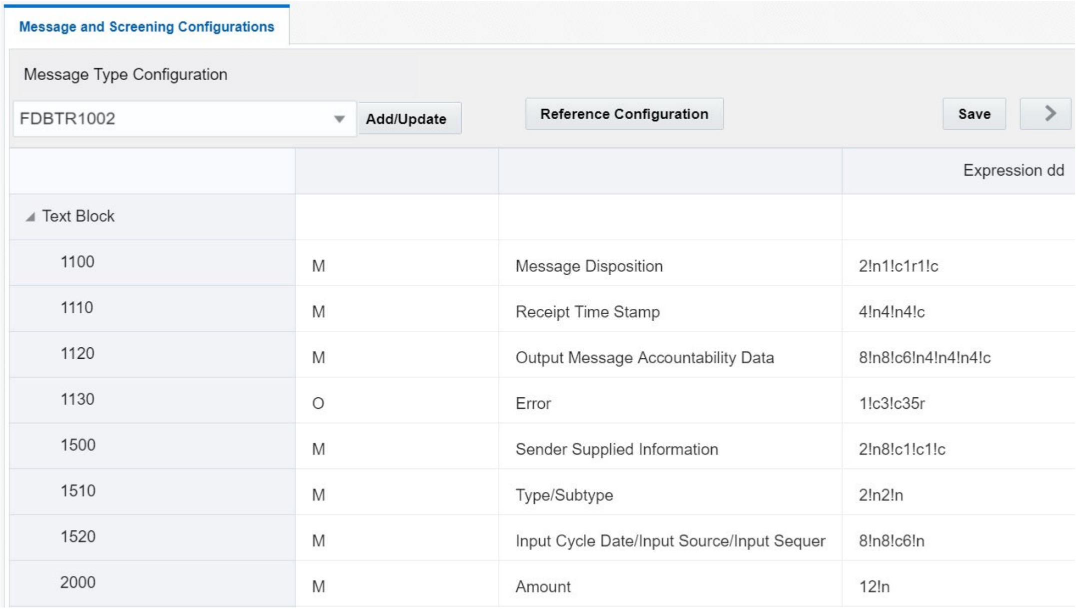
Configuring the Fedwire Message Parameters

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

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** landing page.
2. Click **FEDWIRE Configuration Admin**. The **Message and Screening Configurations** tab is dis- played.

> ⓘ **Note**
>
> The following screens are the same for the Fedwire and SWIFT message parameters.

Figure 7-1   Message and Screening Configurations tab for Fedwire



Message and Screening Configurations
Message Type Configuration
FDBTR1002
Add/Update
Reference Configuration
Save

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

> ⓘ **Note**
>
> The text block tag 8200 (Unstructured Addenda Structure) is added as an optional tag to FDBTR and FDCTP message types for the release 8.1.2.2.

This tab has the following windows:

- Message Type Configuration Window
- <Message Type> Subfield Level Configuration Window

- <Message Type> Screening Configuration Window
- <Message Type> Other Field/Subfield Configuration Window

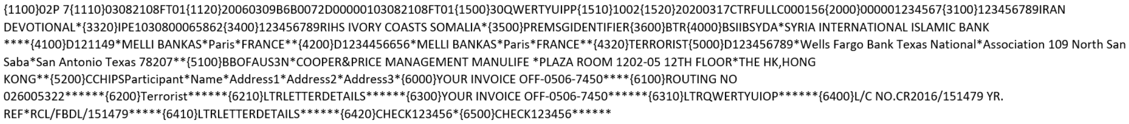
7.1 Message Type Configuration Window

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

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

The following image shows a sample Fedwire message:

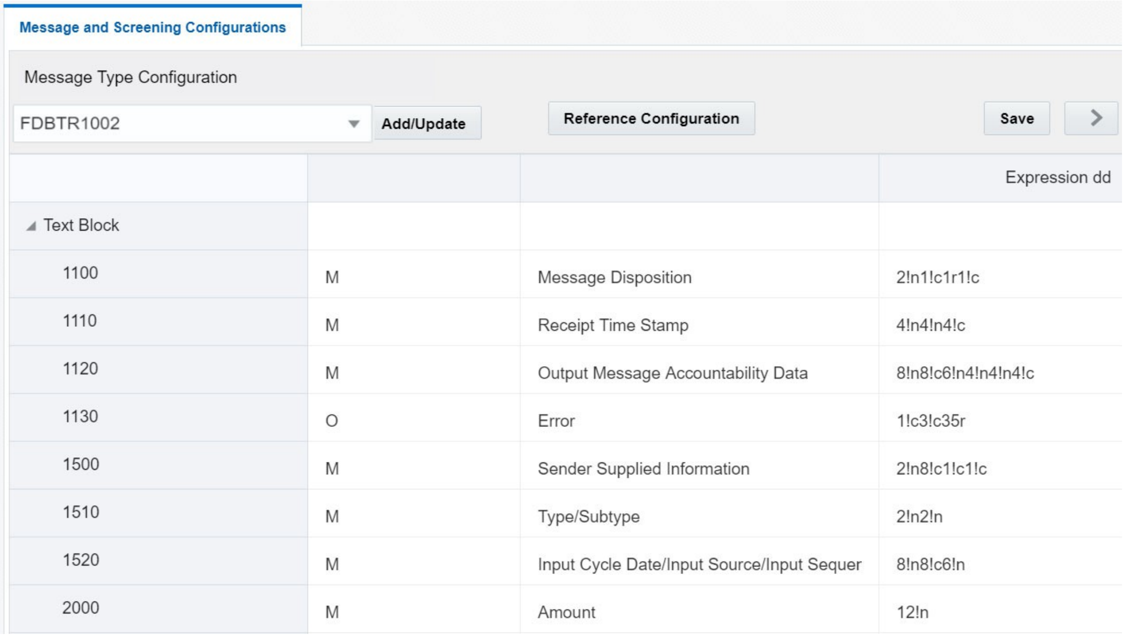
Figure 7-2   Sample Fedwire Message



```
{1100}02P 7{1110}03082108FT01{1120}20060309B6B0072D000001003082108FT01{1500}30QWERTYUIPP{1510}1002{1520}20200317CTRFULLC000156{2000}000001234567{3100}123456789IRAN
DEVOTIONAL*{3320}IPE1030800065862{3400}123456789RIHS IVORY COASTS SOMALIA*{3500}PREMSGIDENTIFIER{3600}BTR{4000}BSIIBSYDA*SYRIA INTERNATIONAL ISLAMIC BANK
****{4100}D121149*MELLI BANKAS*Paris*FRANCE**{4200}D1234456656*MELLI BANKAS*Paris*FRANCE**{4320}TERRORIST{5000}D123456789*Wells Fargo Bank Texas National*Association 109 North San
Saba*San Antonio Texas 78207**{5100}BBOFAUS3N*COOPER&PRICE MANAGEMENT MANULIFE *PLAZA ROOM 1202-05 12TH FLOOR*THE HK,HONG
KONG**{5200}CCHIPSParticipant*Name*Address1*Address2*Address3*{6000}YOUR INVOICE OFF-0506-7450****{6100}ROUTING NO
026005322******{6200}Terrorist******{6210}LTRLETTERDETAILS******{6300}YOUR INVOICE OFF-0506-7450******{6310}LTRQWERTYUIOP******{6400}L/C NO.CR2016/151479 YR.
REF*RCL/FBDL/151479*****{6410}LTRLETTERDETAILS******{6420}CHECK123456*{6500}CHECK123456******
```

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

Figure 7-3   Message and Screening Configurations tab for Fedwire



Message Type Configuration
FDBTR1002

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

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

- **Status**: This column mentions whether the field is Mandatory (**M**) or Optional (**O**).
- **FieldName**: This column describes the name of the given field as per Fedwire standards.

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

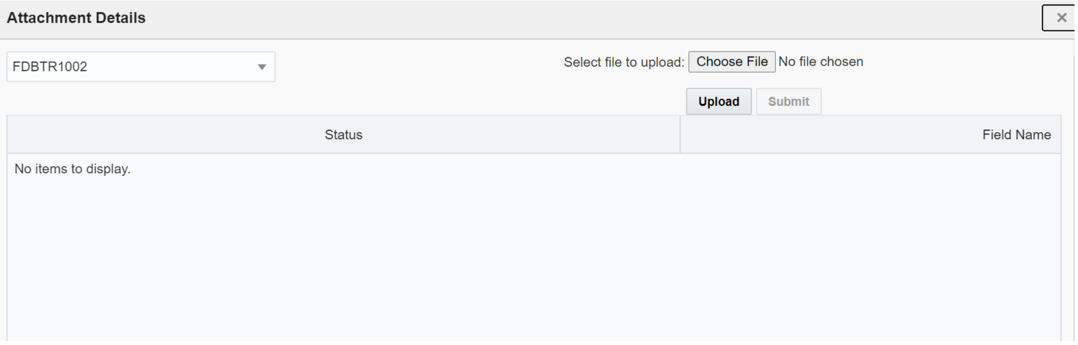
To edit a parameter, click the parameter name. After you make the changes, click **Save**.

7.1.1 Adding or Updating a New Message Type

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

1. Click **Add/Update**. The **Attachment Details** window is displayed.
2. Select the type of message that you want to add or update from the drop-down list.

Figure 7-4 Attachment Details Window



FDBTR1002

No items to display.

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

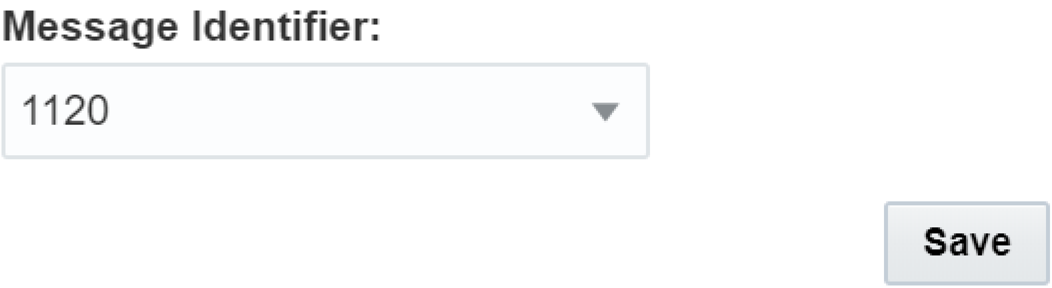
> **Note**
>
> This file must be of the format .json or .txt.

4. Click **Upload**.
5. Click **Submit**. The message is displayed in the following table as <Message Type_draft>. For information on the JSON structure, see Structure of a JSON.

7.1.2 Configuring Message and Transaction References

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

Figure 7-5 Reference Configuration Window



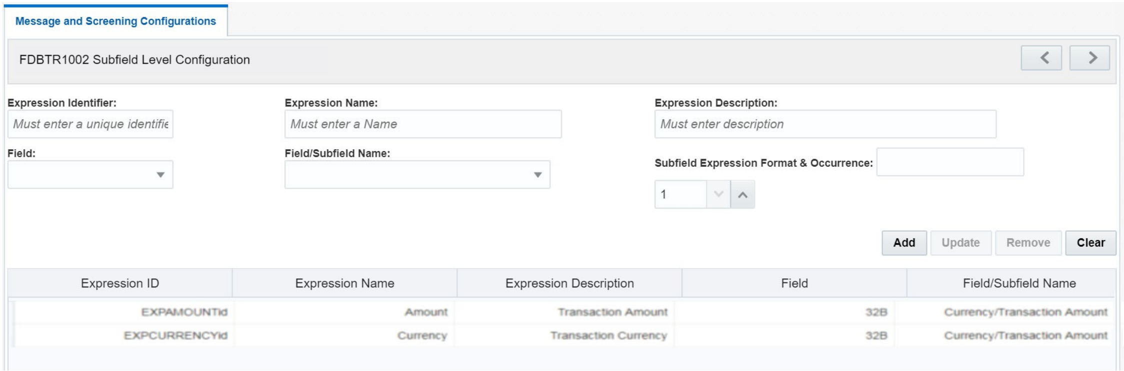
Message Identifier: 1120

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

7.2 <Message Type> Subfield Level Configuration Window

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

Figure 7-6 <Message Type> Subfield Level Configuration Window



Message and Screening Configurations

FDBTR1002 Subfield Level Configuration

Expression Identifier: Must enter a unique identifie

Expression Name: Must enter a Name

Expression Description: Must enter description

Field:

Field/Subfield Name:

Subfield Expression Format & Occurrence: 1

Expression ID	Expression Name	Expression Description	Field	Field/Subfield Name
EXPAMOUNTId	Amount	Transaction Amount	32B	Currency/Transaction Amount
EXPCURRENCYId	Currency	Transaction Currency	32B	Currency/Transaction Amount

1. To add a subfield, provide the required values in the fields shown in the window and click **Add**

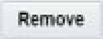
Figure 7-7 Add

. Enter values in the following fields:
Table 19:

Table 7-1 Fields in the <Message Type> Subfield Level Configuration Window

Fields	Field Description
Expression Identifier	Enter a unique identifier. It must begin with an alpha character and must not contain any spaces. This is a mandatory field.
Expression Name	Enter a name for the expression. The name must be in capital letters. This is a mandatory field.
Expression Description	Enter a description for the Expression. This is a mandatory field.
Field	This field displays a complete list of fields in the drop-down for the given message type. Select the field from this drop-down field to configure the expression.
Field/Subfield Name	This field displays the respective field name or subfield options for the field that was previously selected. Select the subfield from the drop- down list.

Table 7-1 (Cont.) Fields in the <Message Type> Subfield Level Configuration Window

Fields	Field Description
Subfield Expression Format & Occurrence	This field is populated when the Field is selected. Select an expression as it as or an element from that expression. You can also enter the number of occurrences for the expression within that message. By default, it is always 1.
Add button	To add a subfield, provide the required values in the fields shown above and click **Add** **Figure 7-8 Add** .
Update button	To update an existing subfield, click the name of the subfield. After you make the changes, click **Update** **Figure 7-9 Update** .
Remove button	To remove an existing subfield, click the name of the subfield and click **Remove** **Figure 7-10 Remove**  .
Clear button	To clear the data in these fields, click **Clear** . **Figure 7-11 Clear**

You can configure the subfield in two ways:

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

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

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

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

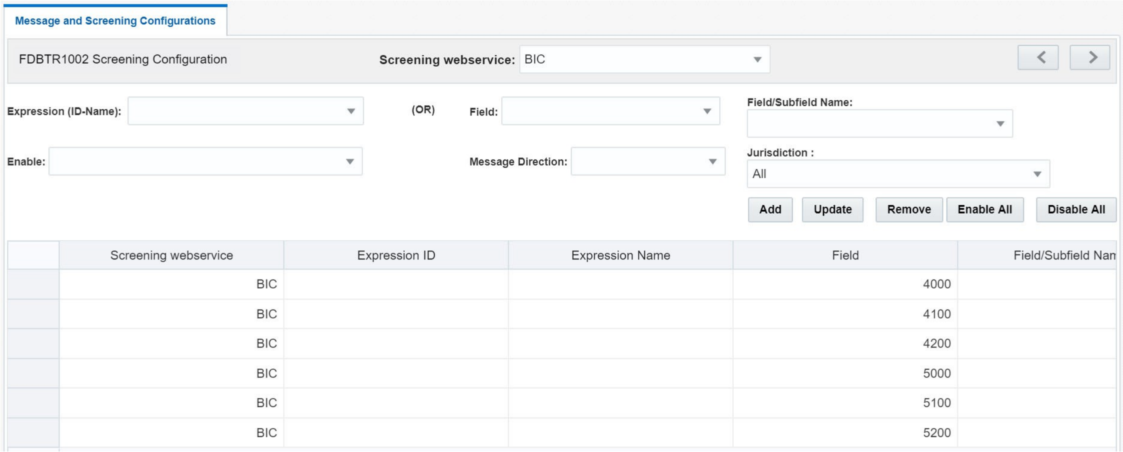
- By configuring the element level data within the subfield expression: Do this if you want to further configure any data out of the subfield.
- a. In this example, if you want to configure the country code for field 57, then you can config- ure 2!a from Identifier Code expression as a country code by giving unique names in the **Sub- field Expression Identifier**, **Subfield Name**, and **Subfield Description** fields.

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

7.3 <Message Type> Screening Configuration Window

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

Figure 7-12 Screening Configuration Window



Screening webservice: BIC

Jurisdiction : All

	Screening webservice	Expression ID	Expression Name	Field	Field/Subfield Nan
	BIC			4000	
	BIC			4100	
	BIC			4200	
	BIC			5000	
	BIC			5100	
	BIC			5200	

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

Table 7-2   Fields in the <Message Type> Screening Configuration Window

Fields	Field Description
Screening WebService	Select a screening web service from the drop-down list. This field lists all the supported matching web services in the **Transaction Filtering** application. The following web services are available: • BIC • Country and City • Goods Screening • Name and Address • Narrative or Free Text Information • Port Screening The fields for all web services except Goods Screening are as shown here. For information on the fields for Goods Screening, see .
Expression (ID-Name)	Select an expression identifier. When you select an expression identifier, the values are populated in the **Field** and **Field/Subfield Name** fields.
Field	Select the field name.
Field/Subfield Name	Select the subfield name. This displays the expression.
Enable	Select **Yes** to enable the web service. Select **No** to disable the web service.
Message Direction	Select INBOUND(o) and OUTBOUND(i) based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select **inbound**, else select **outbound**. If that field must be screened for both inbound and outbound, then select **ANY**.
Jurisdiction	Select **All** to apply the Webservice for all jurisdictions or select the specific jurisdiction to apply the webservice for a specific jurisdiction. Use the kdd_jrsdcn table to configure the jurisdiction values. It has the following columns: • JRSDCN_CD: Values must be unique. • JRSDCN_NM: Actual jurisdiction name. • JRSDCN_DSPLY_NM: Jurisdiction name displayed in the Message and Configurations screen. • JRSDCN_DESC_TX: Optional field to add descriptions for the jurisdictions.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** **Figure 7-13 Add** .

Table 7-2 (Cont.) Fields in the <Message Type> Screening Configuration Window

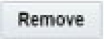
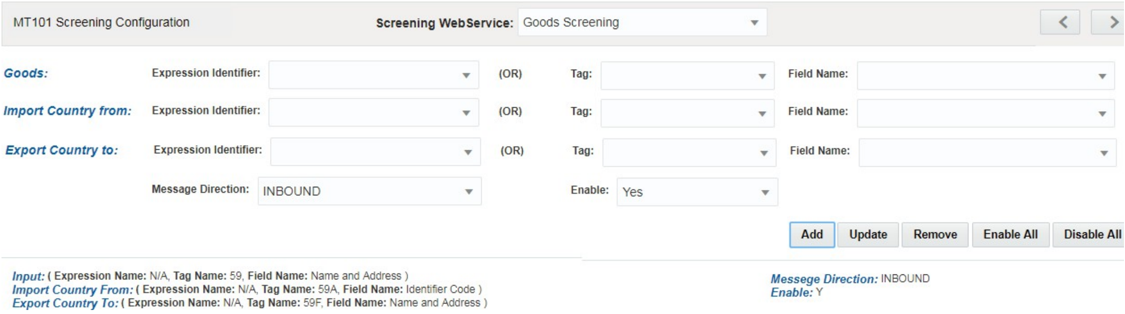
Fields	Field Description
Update button	To update a web service, select the web service that you want to update and click **Update** **Figure 7-14 Update** .
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** **Figure 7-15 Remove**  .

Table 7-3 Fields in the <Message Type> Screening Configuration Window

Fields	Field Description
Enable All button	To enable all web services, click **Enable All** **Figure 7-16 Enable All** .
Disable All button	To disable all web services, click **Disable All** **Figure 7-17 Disable All** .

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

Figure 7-18 Fields for Goods Web Services



MT101 Screening Configuration

Screening WebService: Goods Screening

Goods: Expression Identifier: (OR) Tag: Field Name:

Import Country from: Expression Identifier: (OR) Tag: Field Name:

Export Country to: Expression Identifier: (OR) Tag: Field Name:

Message Direction: INBOUND

Enable: Yes

Input: (**Expression Name:** N/A, **Tag Name:** 59, **Field Name:** Name and Address)
Import Country From: (**Expression Name:** N/A, **Tag Name:** 59A, **Field Name:** Identifier Code)
Export Country To: (**Expression Name:** N/A, **Tag Name:** 59F, **Field Name:** Name and Address)

Messege Direction: INBOUND
Enable: Y

Table 7-4 Fields in the Goods Web Service Window

Fields	Field Description
Expression Identifier	Select the Expression for the good.
Tag	Select the tag related to the good. Based on the tag selected, the field name is populated.
Field Name	The field name is populated based on the tag selected.
Message Direction	Select INBOUND(o) and OUTBOUND(i) based on the screening require- ment from the drop-down list. If a field must be screened only for incom- ing messages, select **inbound**, else select **outbound**. If that field must be screened for both inbound and outbound, then select **ANY**.
Enable	Select **Yes** to enable the message in a direction. Select **No** to disable the message in a direction.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** **Figure 7-19 Add** .
Update button	To update a web service, select the web service that you want to update and click **Update** **Figure 7-20 Update** .

Table 7-4 (Cont.) Fields in the Goods Web Service Window

Fields	Field Description
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** **Figure 7-21 Remove** .
Enable All button	To enable all web services, click **Enable All** **Figure 7-22 Enable All** .
Disable All button	To disable all web services, click **Disable All** **Figure 7-23 Disable All** .

7.3.1 Enabling or Disabling a Web Service

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

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

Table 22:

Table 7-5 Web Services used in Transaction Filtering

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

Table 7-5 (Cont.) Web Services used in Transaction Filtering

Web Service	Web Service ID
Port Screening	Port Screening
Goods Screening	Goods Screening

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

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

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

7.3.2 Updating and Removing a Web Service

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

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

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

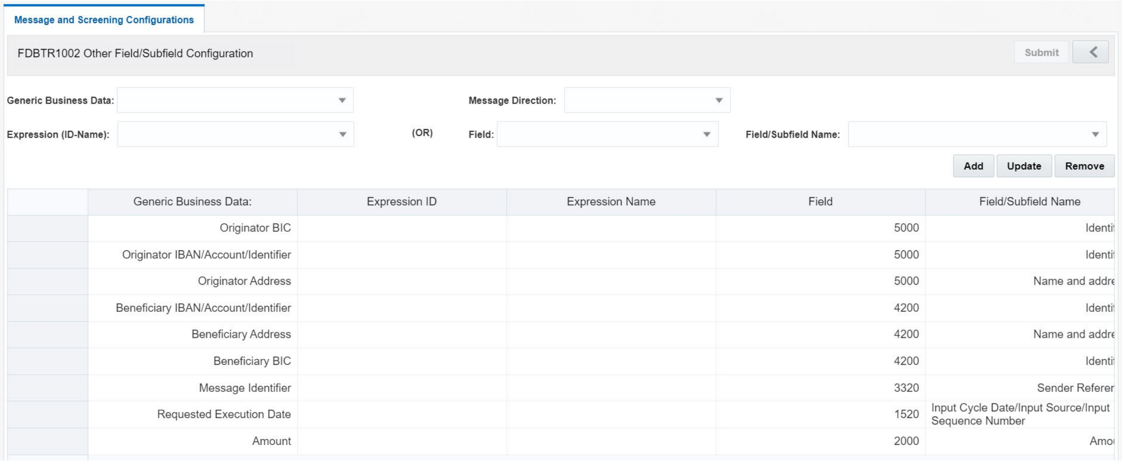
Data for the Trade goods and Trade port web services are taken from a reference table. To populate data for these web services, do this:

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

7.4 <Message Type> Other Field/Subfield Configuration Window

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

Figure 7-24   Other Field/Subfield Configuration Window



	Generic Business Data:	Expression ID	Expression Name	Field	Field/Subfield Name
	Originator BIC			5000	Identi
	Originator IBAN/Account/Identifier			5000	Identi
	Originator Address			5000	Name and addre
	Beneficiary IBAN/Account/Identifier			4200	Identi
	Beneficiary Address			4200	Name and addre
	Beneficiary BIC			4200	Identi
	Message Identifier			3320	Sender Referer
	Requested Execution Date			1520	Input Cycle Date/Input Source/Input Sequence Number
	Amount			2000	Amo

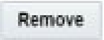
To update the parameter, click the parameter name. The fields are populated with the field parameters. The following fields are displayed in this window:

Table 23:

Table 7-6   Fields in the <Message Type> Other Field/Subfield Configuration Window

Fields	Field Description
Generic Business Data	This field displays the business name of the record that is selected. It is mandatory to configure this field. If the message contains one or more of the B, C, D, or E sequences, you must configure the field with the first tag of the sequence according to the Fedwire standard.
Message Direction	Select INBOUND(o) and OUTBOUND(i) based on the screening requirement from the drop-down list. If a field must be screened only for incoming messages, select inbound, else select outbound. If that field must be screened for both inbound and outbound, then select ANY.
Expression (ID-Name)	Select an expression identifier. When you select an expression identifier, the values are populated in the Field and Field/Subfield Name fields.
Field	Select the field name.
Field/Subfield Name	Select the Subfield Name. This displays the Expression.
Add button	To add a web service, provide the required values in the fields shown above and click **Add** **Figure 7-25 Add** Add .

Table 7-6 (Cont.) Fields in the <Message Type> Other Field/Subfield Configuration Window

Fields	Field Description
Update button	To update a web service, select the web service that you want to update and click **Update** **Figure 7-26 Update** .
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** **Figure 7-27 Remove**  .

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

8 Configurations for ISO20022 Message Parameters

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

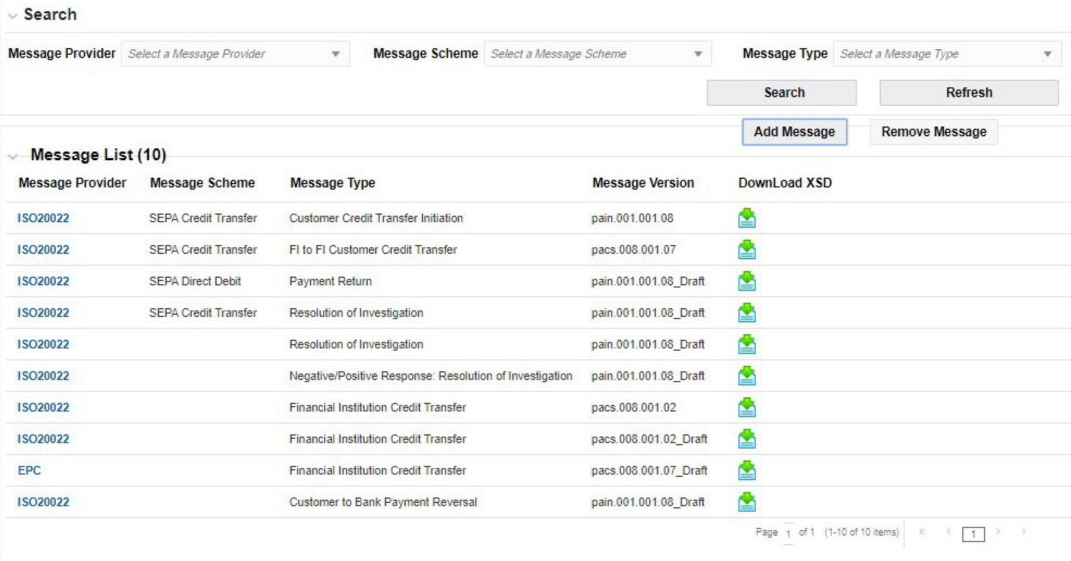
> **Note**
>
> The XPath of an element is the logical structure or hierarchy of the element within the XSD file.

8.1 Configuring the ISO20022 Message Parameters

To configure the ISO20022 message parameters, follow these steps:

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

   Figure 8-1 Configuration Window - ISO20022

   Message List (10)

Message Provider	Message Scheme	Message Type	Message Version	DownLoad XSD
ISO20022	SEPA Credit Transfer	Customer Credit Transfer Initiation	pain.001.001.08	⬇
ISO20022	SEPA Credit Transfer	FI to FI Customer Credit Transfer	pacs.008.001.07	⬇
ISO20022	SEPA Direct Debit	Payment Return	pain.001.001.08_Draft	⬇
ISO20022	SEPA Credit Transfer	Resolution of Investigation	pain.001.001.08_Draft	⬇
ISO20022		Resolution of Investigation	pain.001.001.08_Draft	⬇
ISO20022		Negative/Positive Response: Resolution of Investigation	pain.001.001.08_Draft	⬇
ISO20022		Financial Institution Credit Transfer	pacs.008.001.02	⬇
ISO20022		Financial Institution Credit Transfer	pacs.008.001.02_Draft	⬇
EPC		Financial Institution Credit Transfer	pacs.008.001.07_Draft	⬇
ISO20022		Customer to Bank Payment Reversal	pain.001.001.08_Draft	⬇

   Page 1 of 1 (1-10 of 10 items) 1

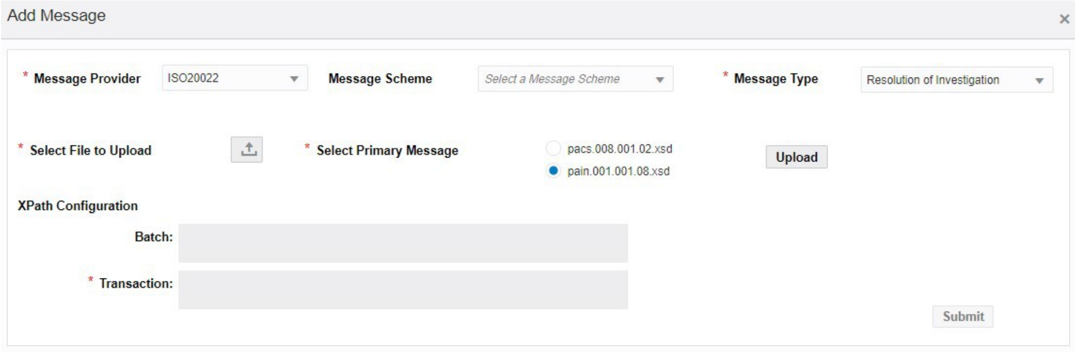
   The Message List displays the XSD files associated with each message provider /scheme/ mes- sage type combination. Click the link in the **Message Provider** column to view the transaction XPaths for the message for every screening type. You can download the XSD for a message by

Figure 8-2 Download Icon

clicking **Download** in the **Download XSD** column. The XSD is downloaded as a zip folder; unzip the folder to view the XSD files.

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

Figure 8-3 Add Message Dialog Box



Add Message ×

* Message Provider: ISO20022

Message Scheme: Select a Message Scheme

* Message Type: Resolution of Investigation

* Select File to Upload

* Select Primary Message: ○ pacs.008.001.02.xsd ● pain.001.001.08.xsd

Upload

XPath Configuration

Batch:

* Transaction:

Submit

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

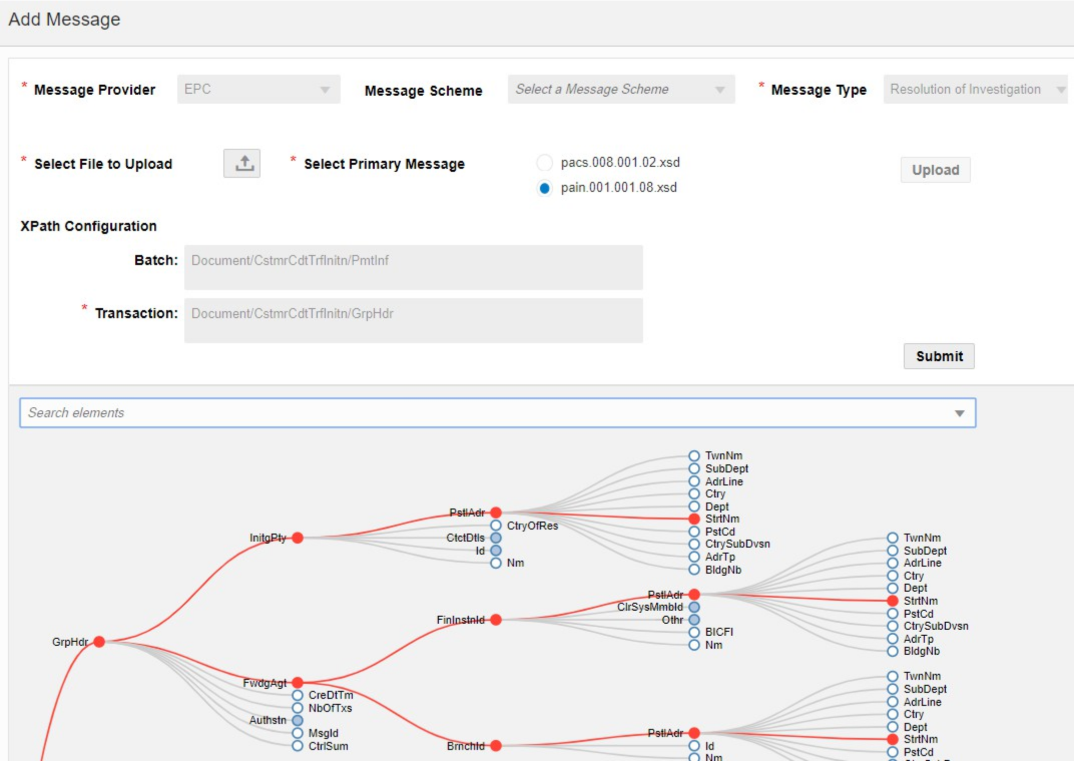
> **Note**
>
> The message provider, message scheme, and message type values are mapped in the fcc_tf_xml_pro_sch_msg_map table.

4. To upload the parent XSD file and one or more child XSD files, click **Upload**

Figure 8-4 Upload Icon

and select the XSD file from your local drive. After you select the file and click **Open**, the XSD file name appears next to the Upload button. Select the radio button next to the primary file name and click **Upload**. A confirmation message appears, "**File uploaded successfully**." The basic elements related to the uploaded file appear in a tree view.

Figure 8-5 Add Message Dialog Box



Add Message

* Message Provider: EPC

Message Scheme: Select a Message Scheme

* Message Type: Resolution of Investigation

* Select File to Upload

* Select Primary Message: ○ pacs.008.001.02.xsd ● pain.001.001.08.xsd

Upload

XPath Configuration

Batch: Document/CstmrCdtTrfInitn/PmtInf

* Transaction: Document/CstmrCdtTrfInitn/GrpHdr

Submit

Search elements

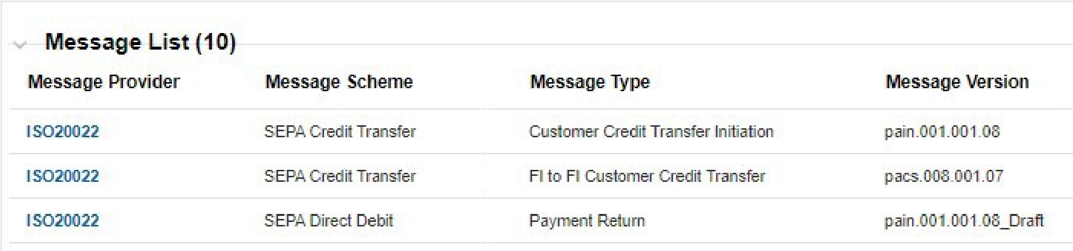
If you want to see the XPath of an element, select the element from the drop-down field. In the example window, the XPath for the StrNm element is highlighted in red.

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

> ⓘ **Note**
>
> To view the child elements for a parent element, mouse over the parent element and click the parent element in the Tree view. If **Zero**
>
> **Figure 8-6 Zero Icon**
>
>
>
> is displayed beside the element name, it means that there are no more child elements you can drill down to.

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

Figure 8-7 Message List Window

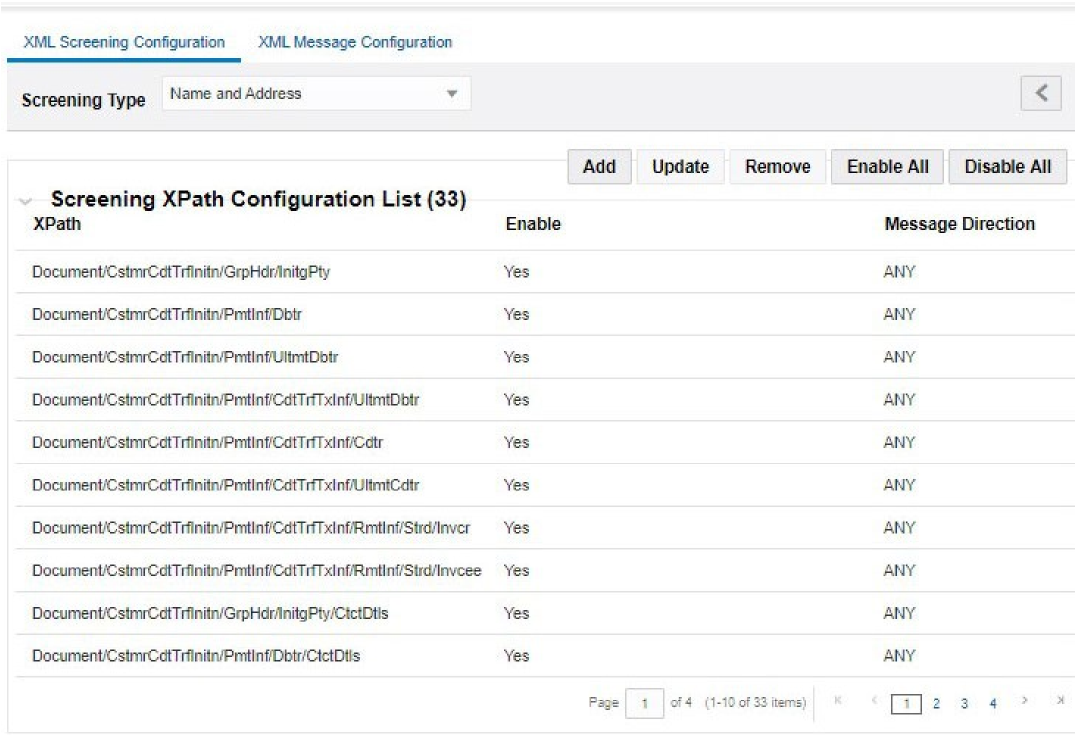


Message List (10)

Message Provider	Message Scheme	Message Type	Message Version
ISO20022	SEPA Credit Transfer	Customer Credit Transfer Initiation	pain.001.001.08
ISO20022	SEPA Credit Transfer	FI to FI Customer Credit Transfer	pacs.008.001.07
ISO20022	SEPA Direct Debit	Payment Return	pain.001.001.08_Draft

6. Navigate to **ISO20022/XML Configuration Admin** in the Admin UI. To complete the configura- tion, click the message provider link. The **XML Screening Configuration** tab is displayed.

Figure 8-8 XML Screening Configuration



Screening Type: Name and Address

Screening XPath Configuration List (33)

XPath	Enable	Message Direction
Document/CstmrCdtTrfInitn/GrpHdr/InitgPty	Yes	ANY
Document/CstmrCdtTrfInitn/PmtInf/Dbtr	Yes	ANY
Document/CstmrCdtTrfInitn/PmtInf/UltmtDbtr	Yes	ANY
Document/CstmrCdtTrfInitn/PmtInf/CdtTrfTxInf/UltmtDbtr	Yes	ANY
Document/CstmrCdtTrfInitn/PmtInf/CdtTrfTxInf/Cdtr	Yes	ANY
Document/CstmrCdtTrfInitn/PmtInf/CdtTrfTxInf/UltmtCdtr	Yes	ANY
Document/CstmrCdtTrfInitn/PmtInf/CdtTrfTxInf/RmtInf/Strd/Invcr	Yes	ANY
Document/CstmrCdtTrfInitn/PmtInf/CdtTrfTxInf/RmtInf/Strd/Invcee	Yes	ANY
Document/CstmrCdtTrfInitn/GrpHdr/InitgPty/CtctDtls	Yes	ANY
Document/CstmrCdtTrfInitn/PmtInf/Dbtr/CtctDtls	Yes	ANY

Page 1 of 4 (1-10 of 33 items) 1 2 3 4

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

Table 24:

Table 8-1 Other Actions

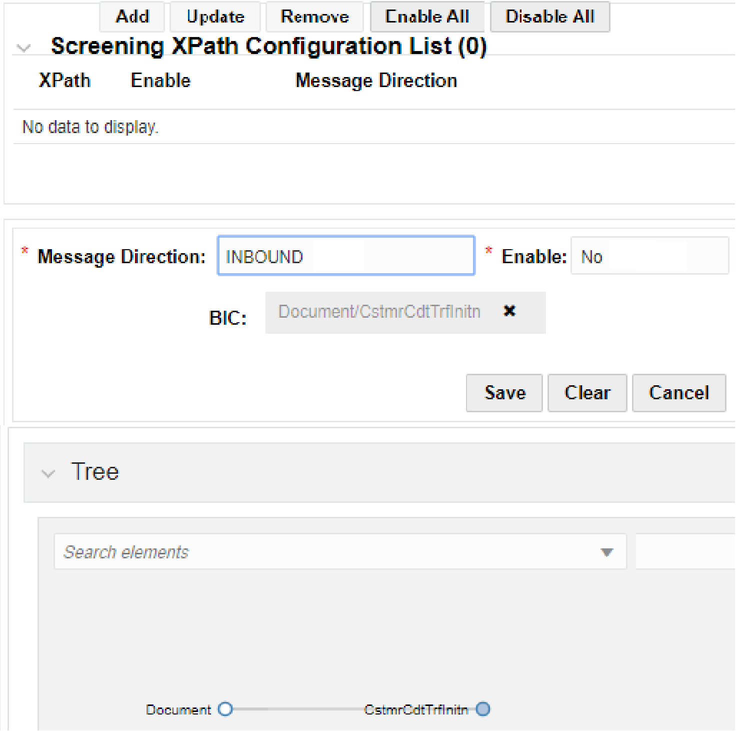
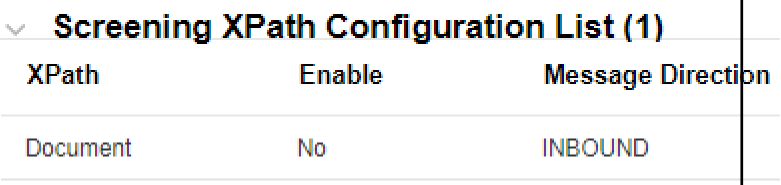
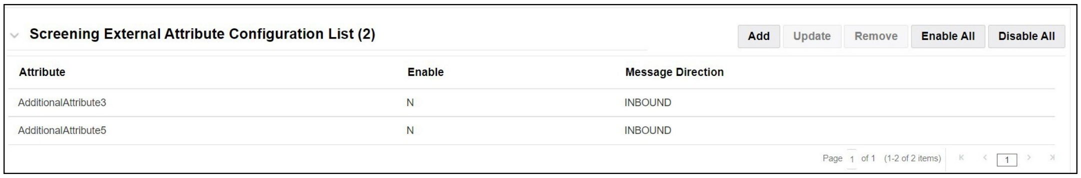
To...	Do this...
Add a web service configuration	Click **Add**. The following fields appear: **Figure 8-9 Add a web service configuration**  Add Update Remove Enable All Disable All Save Clear Cancel Tree Search elements Document CstmrCdtTrfInitn Screening XPath Configuration List (0) XPath Enable Message Direction No data to display. * Message Direction: INBOUND * Enable: No BIC: Document/CstmrCdtTrfInitn Select the message direction and enable or disable the web service and click **Save**. Clicking **Clear** clears any values selected. If you click **Cancel**, the fields disappear. In the Tree view, right-click any element node and click the element to view the element's XPath. The fields appear in the **Screening XPath Configuration List** section. **Figure 8-10 Add a web service configuration - tree view**  Screening XPath Configuration List (1) XPath | Enable | Message Direction Document | No | INBOUND
Update a web service configuration	Select the configuration you want to update and click **Update**. The fields shown in the previous row appear. Make the required changes and click **Save**. The updated values are displayed in the **Screening XPath Con- figuration List** section.

Table 8-1 (Cont.) Other Actions

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

7. Navigate to **ISO20022/XML Configuration Admin** in the Admin UI and click the message pro- vider link. To add the screening configuration of External Attribute, select the Attributes under the **Screening External Attribute Configuration** list. The **Screening External Attribute Con- figuration** list is displayed.

Figure 8-11 External Attribute List Window



Screening External Attribute Configuration List (2)

Attribute	Enable	Message Direction
AdditionalAttribute3	N	INBOUND
AdditionalAttribute5	N	INBOUND

Page 1 of 1 (1-2 of 2 items)

In this tab, you can view the details of the attribute name, enable status, and message direction details. You can also perform the following actions:

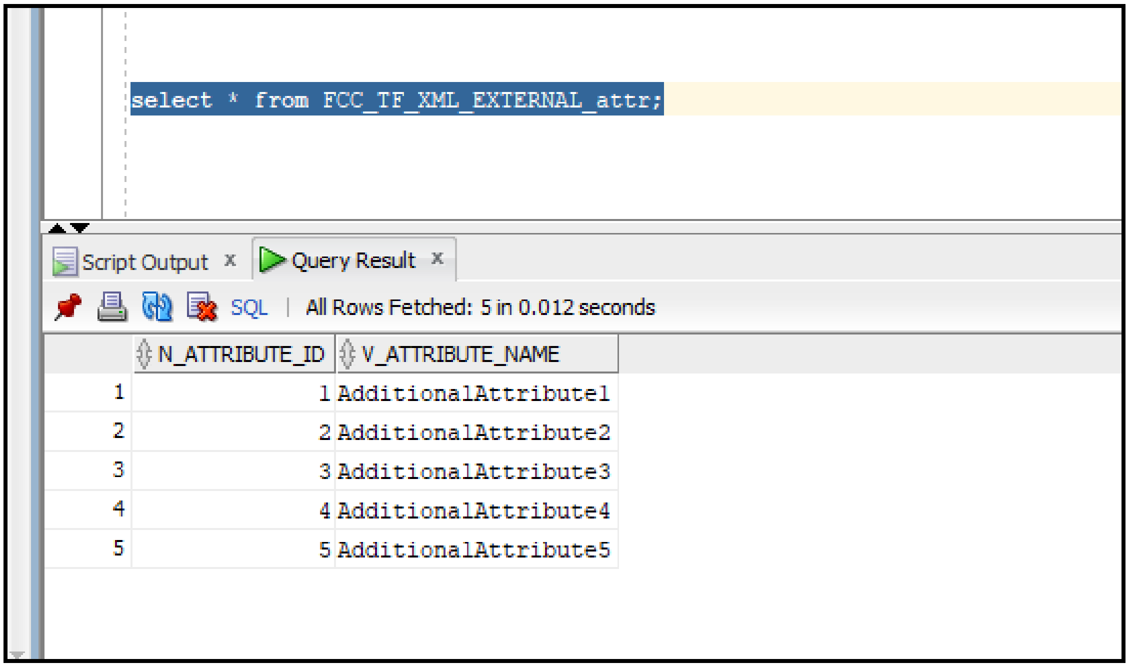
> **Note**
>
> The **Add** button will only appear when the user configures the FCC_TF_XML_EXTERNAL_ATTR and FCC_TF_XML_EXTERNAL_ATTR_MLS tables. Refer the following examples.

Example: 1

To configure FCC_TF_XML_EXTERNAL_ATTR table, run the following query similar way in your atomic schema:

```
REM INSERTING into FCC_TF_XML_EXTERNAL_attr SET DEFINE OFF;
Insert into FCC_TF_XML_EXTERNAL_attr (N_ID,V_ATTRIBUTE_NAME) values
(1,'AdditionalAttribute1');
Insert into FCC_TF_XML_EXTERNAL_attr (N_ID,V_ATTRIBUTE_NAME) values
(2,'AdditionalAttribute2');
Insert into FCC_TF_XML_EXTERNAL_attr (N_ID,V_ATTRIBUTE_NAME) values
(3,'AdditionalAttribute3');
Insert into FCC_TF_XML_EXTERNAL_attr (N_ID,V_ATTRIBUTE_NAME) values
(4,'AdditionalAttribute4');
Insert into FCC_TF_XML_EXTERNAL_attr (N_ID,V_ATTRIBUTE_NAME) values
(5,'AdditionalAttribute5');
```

Figure 8-12 Example 1



```
select * from FCC_TF_XML_EXTERNAL_attr;
```

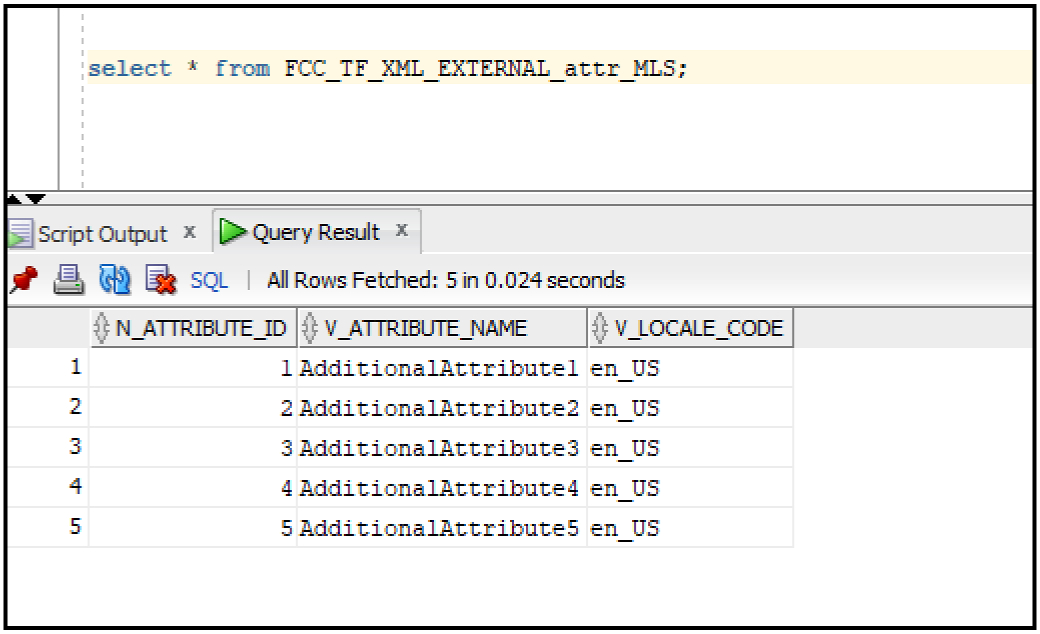
	N_ATTRIBUTE_ID	V_ATTRIBUTE_NAME
1	1	AdditionalAttribute1
2	2	AdditionalAttribute2
3	3	AdditionalAttribute3
4	4	AdditionalAttribute4
5	5	AdditionalAttribute5

Example: 2

To configure FCC_TF_XML_EXTERNAL_ATTR_MLS table, run the following query similar way in your atomic schema:

```
REM INSERTING into FCC_TF_XML_EXTERNAL_attr_MLS SET DEFINE OFF;
Insert into FCC_TF_XML_EXTERNAL_attr_MLS
(N_ID,V_ATTRIBUTE_NAME,V_LOCALE_CODE) values
(1,'AdditionalAttribute1','en_US');
Insert into FCC_TF_XML_EXTERNAL_attr_MLS
(N_ID,V_ATTRIBUTE_NAME,V_LOCALE_CODE) values
(2,'AdditionalAttribute2','en_US');
Insert into FCC_TF_XML_EXTERNAL_attr_MLS
(N_ID,V_ATTRIBUTE_NAME,V_LOCALE_CODE) values
(3,'AdditionalAttribute3','en_US');
Insert into FCC_TF_XML_EXTERNAL_attr_MLS
(N_ID,V_ATTRIBUTE_NAME,V_LOCALE_CODE) values
(4,'AdditionalAttribute4','en_US');
Insert into FCC_TF_XML_EXTERNAL_attr_MLS
(N_ID,V_ATTRIBUTE_NAME,V_LOCALE_CODE) values
(5,'AdditionalAttribute5','en_US');
```

Figure 8-13   Example 2



```
select * from FCC_TF_XML_EXTERNAL_attr_MLS;
```

All Rows Fetched: 5 in 0.024 seconds

	N_ATTRIBUTE_ID	V_ATTRIBUTE_NAME	V_LOCALE_CODE
1	1	AdditionalAttribute1	en_US
2	2	AdditionalAttribute2	en_US
3	3	AdditionalAttribute3	en_US
4	4	AdditionalAttribute4	en_US
5	5	AdditionalAttribute5	en_US

Table 25:

Table 8-2   Other Actions

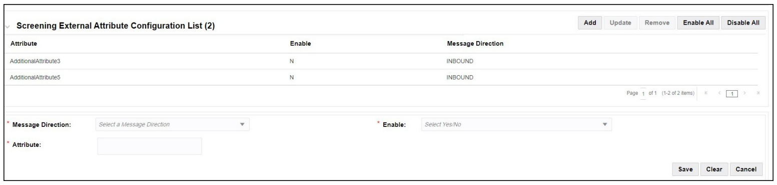
To...	Do this...
Add an external attribute configuration	Click **Add**. The following fields appear: **Figure 8-14 Add an External Attribute configuration**  Screening External Attribute Configuration List (2) Add · Update · Remove · Enable All · Disable All Attribute · Enable · Message Direction AdditionalAttribute3 · N · INBOUND AdditionalAttribute5 · N · INBOUND Page 1 of 1 (1-2 of 2 items) * Message Direction: Select a Message Direction * Enable: Select Yes/No * Attribute: Save · Clear · Cancel Select the message direction and enable or disable the web service and click **Save**. Clicking **Clear** clears any values selected. If you click **Cancel**, the fields disappear.
Update a web service configuration	Select the configuration you want to update and click **Update**. The fields shown in the previous row appear. Make the required changes and click **Save**. The updated values are displayed in the **Screening External Attribute Configuration List** section.
Remove a web service configuration	Select the configuration you want to remove and click **Remove**. The selected configuration is removed from the **Screening External Attribute Configuration List** section.
Enable all web service configurations	Click **Enable All**.

Table 8-2 (Cont.) Other Actions

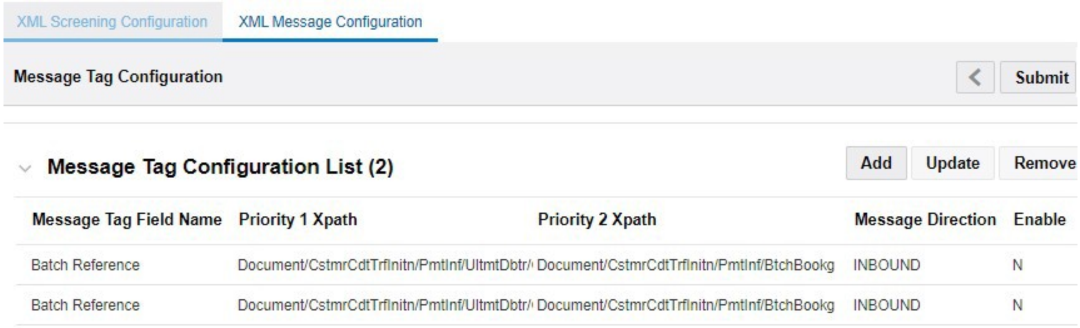
Disable all web service configurations	Click **Disable All**.

1. After configuring the External Attributes, give the following attribute names (Same attribute names which are populated in the above tables) in message posting jsp.
   Example: SanctionsPost.jsp

   ```
   String AdditionalAttribute1 = request.getParameter("AdditionalAttribute1");
    String AdditionalAttribute2 =
   request.getParameter("AdditionalAttribute2");
    String AdditionalAttribute3 =
   request.getParameter("AdditionalAttribute3");
   String AdditionalAttribute4 =
   request.getParameter("AdditionalAttribute4");
   String AdditionalAttribute5 = request.getParameter("AdditionalAttribute5");
   ```

2. To view the message tag configurations for a field, click the **XML Message Configuration** tab.

Figure 8-15 XML Message Configuration Tab


XML Screening Configuration
XML Message Configuration
Message Tag Configuration
Submit
Add
Update
Remove

Message Tag Configuration List (2)

Message Tag Field Name	Priority 1 Xpath	Priority 2 Xpath	Message Direction	Enable
Batch Reference	Document/CstmrCdtTrfInitn/PmtInf/UltmtDbtr/	Document/CstmrCdtTrfInitn/PmtInf/BtchBookg	INBOUND	N
Batch Reference	Document/CstmrCdtTrfInitn/PmtInf/UltmtDbtr/	Document/CstmrCdtTrfInitn/PmtInf/BtchBookg	INBOUND	N

You can also perform the following actions:

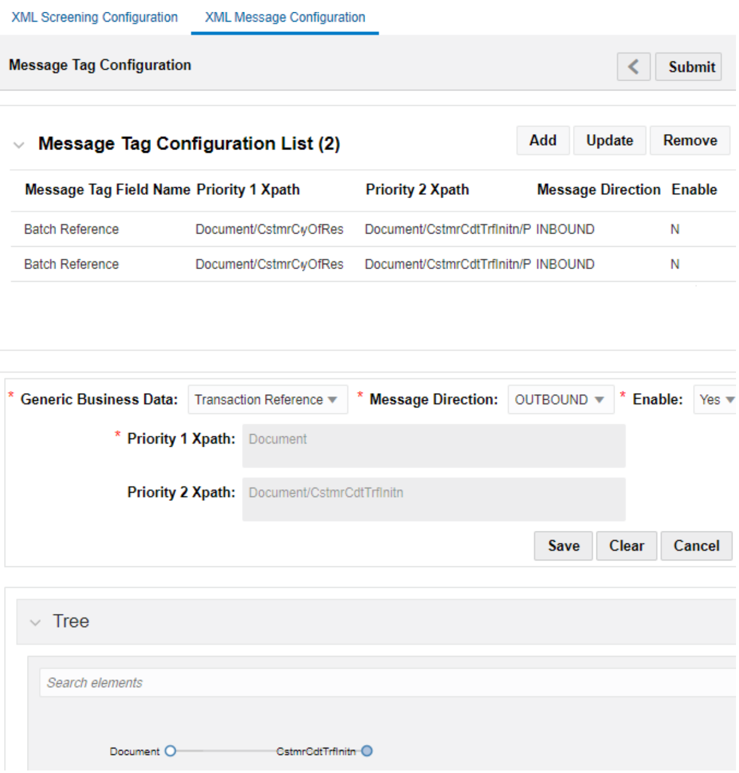
Table 8-3 Other Actions

To...	Do this...

Table 8-3 (Cont.) Other Actions

<table>
<tr>
<td>Add a message configuration</td>
<td>
Click <b>Add</b>. The following fields appear:

<b>Figure 8-16 Add a message configuration</b>



Message Tag Configuration List (2)

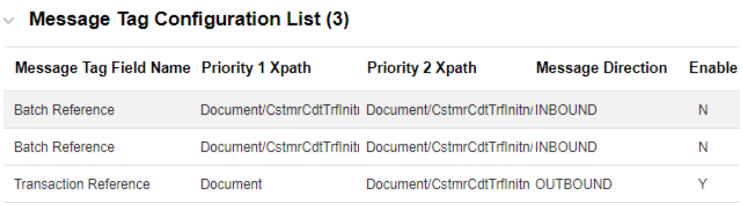
<table>
<tr><th>Message Tag Field Name</th><th>Priority 1 Xpath</th><th>Priority 2 Xpath</th><th>Message Direction</th><th>Enable</th></tr>
<tr><td>Batch Reference</td><td>Document/CstmrCyOfRes</td><td>Document/CstmrCdtTrfInitn/P</td><td>INBOUND</td><td>N</td></tr>
<tr><td>Batch Reference</td><td>Document/CstmrCyOfRes</td><td>Document/CstmrCdtTrfInitn/P</td><td>INBOUND</td><td>N</td></tr>
</table>

* Generic Business Data: Transaction Reference
* Message Direction: OUTBOUND
* Enable: Yes
* Priority 1 Xpath: Document
Priority 2 Xpath: Document/CstmrCdtTrfInitn

Select the business data value, message direction, enable or disable the value, choose the <b>Priority 1 XPath</b> and <b>Priority 2 XPath,</b> and click <b>Save</b>. Clicking <b>Clear</b> clears any values selected. If you click <b>Cancel</b>, the fields disappear.

In the Tree view, right-click any element node and click the element to view it's XPath. The fields appear in the <b>Message Tag Configuration List</b> section.

<b>Figure 8-17 Add a message configuration - tree view</b>



Message Tag Configuration List (3)

<table>
<tr><th>Message Tag Field Name</th><th>Priority 1 Xpath</th><th>Priority 2 Xpath</th><th>Message Direction</th><th>Enable</th></tr>
<tr><td>Batch Reference</td><td>Document/CstmrCdtTrfInit</td><td>Document/CstmrCdtTrfInitn/</td><td>INBOUND</td><td>N</td></tr>
<tr><td>Batch Reference</td><td>Document/CstmrCdtTrfInit</td><td>Document/CstmrCdtTrfInitn/</td><td>INBOUND</td><td>N</td></tr>
<tr><td>Transaction Reference</td><td>Document</td><td>Document/CstmrCdtTrfInitn</td><td>OUTBOUND</td><td>Y</td></tr>
</table>
</td>
</tr>
<tr>
<td>Update a message configuration</td>
<td>Select the configuration you want to update and click <b>Update</b>. The fields shown in the previous row appear. Make the required changes and click <b>Save</b>. The updated values are displayed in the <b>Message Tag Configu- ration List</b> section.</td>
</tr>
</table>

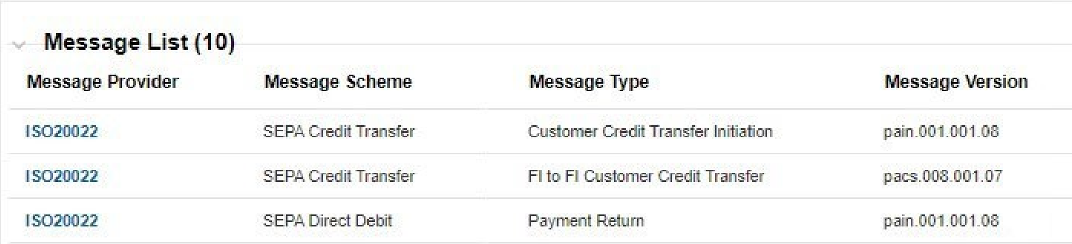
Table 8-3 (Cont.) Other Actions

Remove a message configuration	Select the configuration you want to remove and click **Remove**. The selected configuration is removed from the **Message Tag Configuration List** section.

> **Note**
>
> The ready-to-use business data values are available in the DIM_TF_XML_MSG_TAG_FLD column. You can add a new value in this column.

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

Figure 8-18 Message List Window



Message List (10)

Message Provider	Message Scheme	Message Type	Message Version
ISO20022	SEPA Credit Transfer	Customer Credit Transfer Initiation	pain.001.001.08
ISO20022	SEPA Credit Transfer	FI to FI Customer Credit Transfer	pacs.008.001.07
ISO20022	SEPA Direct Debit	Payment Return	pain.001.001.08

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

8.1.1 SWIFT MX Message Types Configuration

The SWIFT MX is a XML message definition used on the SWIFT network. Majority of the MX messages are ISO 20022 messages. TF will not support mix of different message types in single file. One MX message will have one type of message.

For more information on configuration of XML message parameter, see Configuring the ISO20022 Message Parameters. For SWIFT MX message types see ISO20022 Message Types table.

8.1.2 Running the ISO20022 Batch

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

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

   For example, `/scratch/fccmappchef/SANC807/ftpshare/SANCINFO/STAGE/SEPA/inputXML/20200214`.

   `20200214` is the MIS Date folder.

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

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

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

```
##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUT- BOUND/INPUT
```

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

For example,

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

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

- The `VAL_ERROR`, `PRCSNG_ERROR`, `PROCESSED`, and `FEEDBACK` folders are created as part of the batch processing.
- If any message XML fails during validation, then it is moved to the `VAL_ERROR` folder. The directory structures for `OUTBOUND` and `INBOUND` are as follows:

```
##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUT- BOUND/
VAL_ERROR
```

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

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

  ```
  ##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUT- BOUND/
  PRCSNG_ERROR
  ```

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

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

  ```
  ##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUT- BOUND/
  VAL_ERROR
  ```

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

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

  ```
  ##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUT- BOUND/
  FEEDBACK
  ```

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

- The logs of the batch are available in the following path: `##FIC_DB_HOME##/log/TF_XML`

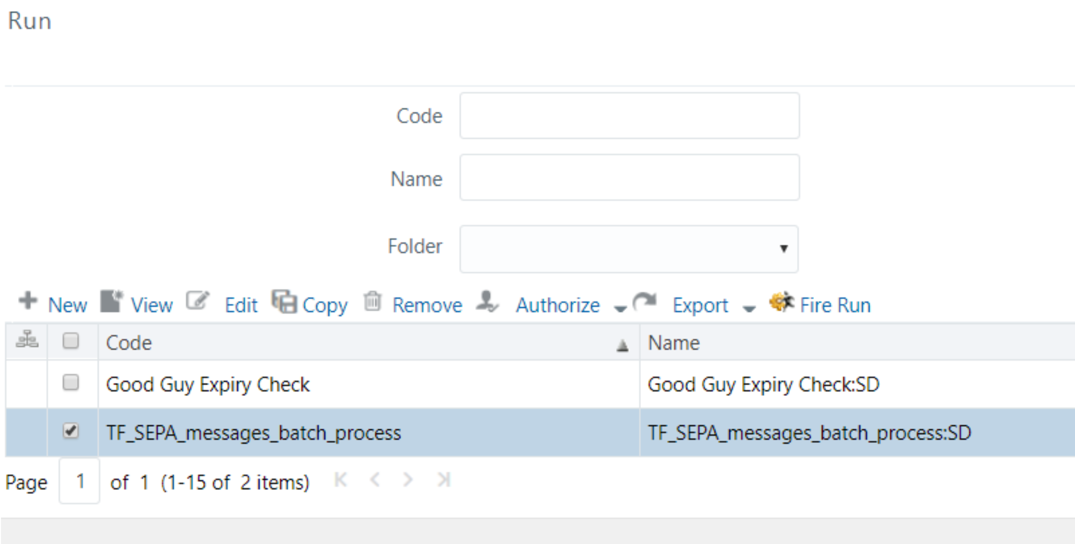
  For example, `/scratch/fccmappchef/SANC807/SANC807/ficdb/log/TF_XML`

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

To run the batch, follow these steps:

1. Navigate to the **Run** page. For more information, see the Run Definition Menu.

Figure 8-19 Run Page

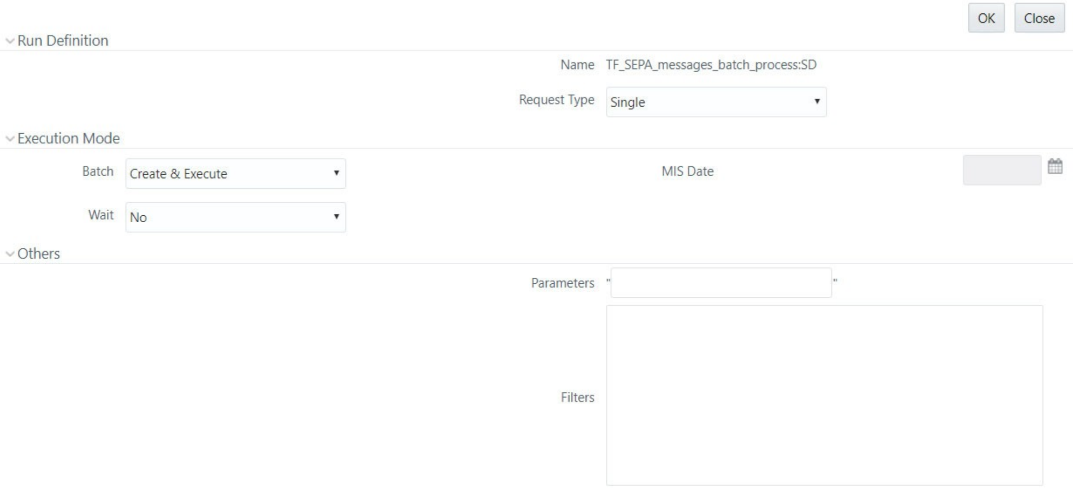


☐	Code	Name
☐	Good Guy Expiry Check	Good Guy Expiry Check:SD
☑	TF_SEPA_messages_batch_process	TF_SEPA_messages_batch_process:SD

Page 1 of 1 (1-15 of 2 items)

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

Figure 8-20   Fire Run Page



Name	TF_SEPA_messages_batch_process:SD
Request Type	Single
Batch	Create & Execute
Wait	No
MIS Date	
Parameters	" "
Filters	

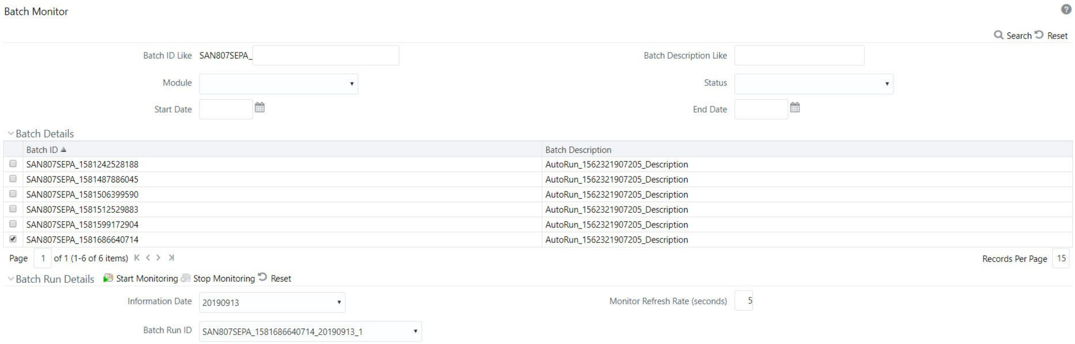
3. Select **Single** as the **Request Type**.
4. Select **Create & Execute** in the **Batch** field. The **MIS Date** field is displayed.
5. Select the date on which you want to execute the run. This date must be the same as the folder you create before you run the ISO20022 batch. In the example shown, since the **MIS Date** folder name is 20190913, the date you must select is 09/13/2019.
6. Click **OK**.

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

To access the **Batch Monitor** page, click **Operations** , and then click **Batch Monitor**. The **Batch Monitor** page has details of all batches. The batch you have executed is the last in the **Batch Details** list. To run the batch, follow these steps:

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

Figure 8-21   Batch Monitor Page



Batch ID Like	SAN807SEPA_
Batch Description Like	
Module	
Status	
Start Date	
End Date	

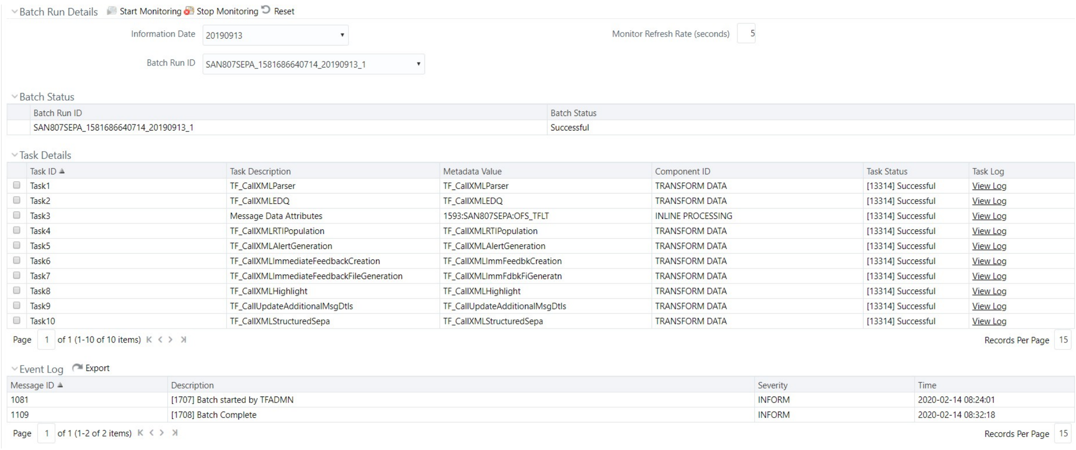
	Batch ID ▲	Batch Description
□	SAN807SEPA_1581242528188	AutoRun_1562321907205_Description
□	SAN807SEPA_1581487886045	AutoRun_1562321907205_Description
□	SAN807SEPA_1581506399590	AutoRun_1562321907205_Description
□	SAN807SEPA_1581512529883	AutoRun_1562321907205_Description
□	SAN807SEPA_1581599172904	AutoRun_1562321907205_Description
☑	SAN807SEPA_1581686640714	AutoRun_1562321907205_Description

Page 1 of 1 (1-6 of 6 items)   Records Per Page 15

Information Date	20190913
Monitor Refresh Rate (seconds)	5
Batch Run ID	SAN807SEPA_1581686640714_20190913_1

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

Figure 8-22   Tasks in the Batch Monitor Page



Batch Run Details   Start Monitoring   Stop Monitoring   Reset

Information Date: 20190913

Monitor Refresh Rate (seconds): 5

Batch Run ID: SAN807SEPA_1581686640714_20190913_1

Batch Status

Batch Run ID	Batch Status
SAN807SEPA_1581686640714_20190913_1	Successful

Task Details

	Task ID ▲	Task Description	Metadata Value	Component ID	Task Status	Task Log
□	Task1	TF_CallXMLParser	TF_CallXMLParser	TRANSFORM DATA	[13314] Successful	View Log
□	Task2	TF_CallXMLEDQ	TF_CallXMLEDQ	TRANSFORM DATA	[13314] Successful	View Log
□	Task3	Message Data Attributes	1593:SAN807SEPA:OFS_TFLT	INLINE PROCESSING	[13314] Successful	View Log
□	Task4	TF_CallXMLRTIPopulation	TF_CallXMLRTIPopulation	TRANSFORM DATA	[13314] Successful	View Log
□	Task5	TF_CallXMLAlertGeneration	TF_CallXMLAlertGeneration	TRANSFORM DATA	[13314] Successful	View Log
□	Task6	TF_CallXMLImmediateFeedbackCreation	TF_CallXMLImmFeedbkCreation	TRANSFORM DATA	[13314] Successful	View Log
□	Task7	TF_CallXMLImmediateFeedbackFileGeneration	TF_CallXMLImmFdbkFiGeneratn	TRANSFORM DATA	[13314] Successful	View Log
□	Task8	TF_CallXMLHighlight	TF_CallXMLHighlight	TRANSFORM DATA	[13314] Successful	View Log
□	Task9	TF_CallUpdateAdditionalMsgDtls	TF_CallUpdateAdditionalMsgDtls	TRANSFORM DATA	[13314] Successful	View Log
□	Task10	TF_CallXMLStructuredSepa	TF_CallXMLStructuredSepa	TRANSFORM DATA	[13314] Successful	View Log

Page 1 of 1 (1-10 of 10 items)   Records Per Page 15

Event Log   Export

Message ID ▲	Description	Severity	Time
1081	[1707] Batch started by TFADMN	INFORM	2020-02-14 08:24:01
1109	[1708] Batch Complete	INFORM	2020-02-14 08:32:18

Page 1 of 1 (1-2 of 2 items)   Records Per Page 15

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

The task details are as follows:

Table 8-4   Task Details

Task ID	Task Name	Task Description
Task1	TF_CallXMLParser	Parses the XML data into the pre-processing tables.
Task2	TF_CallXMLEDQ	Calls EDQ data to check if there are any matches.
Task3	Message Data Attributes	NA
Task4	TF_CallXMLRTIPopulation	Moves data from the ISO20022 configuration tables to the SWIFT configuration tables to generate OBI reports.
Task5	TF_CallXMLAlertGeneration	Creates alerts and loads data into the alert tables.
Task6	TF_CallXMLImmediateFeedbackCreation	Populates the feedback table.
Task7	TF_CallXMLImmediateFeedbackFileGeneration	Generates the feedback in an XML format in the INBOUND/feedback directory for the date on which the run is triggered.
Task8	TF_CallXMLHighlight	Populates the highlighted column in the fsi_rt_al_raw_data table.
Task9	TF_CallUpdateAdditionalMsgDtls	Populates the post-processing alert table with the additional details provided for the alert.
Task10	TF_CallXMLStructuredSepa	Populates the data in the Structured Message tab in the Investigation User Interface.

8.1.3 External Attributes Screening Configuration for ISO20022 Batch

For the external attributes screening configuration for the ISO20022 Batch follow the subsequent steps:

1. Add the attribute names (case-sensitive) to `FCC_TF_XML_EXTERNAL_ATTR`, `FCC_TF_XML_EXTERNAL_ATTR_MLS` table in the Atomic Schema.
2. Login to OFSAA Transactions Filtering application as TFADMN.
3. Navigate to ISO20022/XML Configuration Admin screen.
4. Open any ISO20022 Message Provider and configure the external attributes for each screening type separately. For reference, see Step 6 in section 8.1 and Table 25.

Expected JSON Format and keywords by Transaction Filtering Application:

- The filename of external attributes should be in the format `filename_external_attributes.json`, where The filename stands for the corresponding ISO20022 batch xml filename. OFS TRANSACTION FILTERING ADMINISTRATION GUIDE | 101 CONFIGURATIONS FOR THE ISO20022 MESSAGE PARAMETERS CONFIGURING THE ISO20022 MESSAGE PARAMETERS.
  For Example, If the batch xml filename is pacs.003.001.02.xml, then the external attributes filename should be pacs.003.001.02_external_attributes.json.
- External Attributes JSON file must be placed in the same folder (INPUT folder) where the batch XML file is located.
- The subsequent JSON format must be followed to screen the external attributes.
  1. JSON format for Batches of Transactions XML:

```
{
"batch_external_attributes": [{
"batch_id": [batch id given in PmtInfId tag],
"external_attributes": {
"jurisdiction":"All",
"business_domain":"GEN",
"priority":"Medium",
[…configured external attributes with attribute value as key-value pair…]
}
}, {
"batch_id": [batch id given in PmtInfId tag],
"external_attributes": {
"jurisdiction":"EMEA",
"business_domain":"All",
"priority":"Medium",
[…configured external attributes with attribute value as key-value pair…]
}
}, …..,.
]
}
```

2. JSON format for single Transaction XML:
`{ "batch_external_attributes": [{ "batch_id": "", "external_attributes": { "jurisdiction":"EMEA", "business_domain":"GEN", "priority":"High", OFS TRANSACTION FILTERING ADMINISTRATION GUIDE | 102 CONFIGURATIONS FOR THE ISO20022 MESSAGE PARAMETERS CONFIGURING THE ISO20022 MESSAGE PARAMETERS […configured external attributes with attribute value as key-value pair…] } }] }`

   (OR)

```
{
"batch_external_attributes": [{
"external_attributes": {
"jurisdiction":"EMEA",
"business_domain":"GEN",
"priority":"High",
[…configured external attributes with attribute value as key-value pair…]
}
}]
}
```

> **Note**
>
> - If payment contains single transaction, `batch_id` label is not mandatory. If a payment contains multiple batches of transactions, `batch_id` label is mandatory.
> - The jurisdiction, business_domain and priority labels are optional. If you provide these labels in JSON, application will take these values. Otherwise, the application will take the value from `SETUP_RT_PARAMS` table.
> - The Message Direction will be taken based on the folder structure (either OUTBOUND or INBOUND) under which you place the files.
> - The batch_external_attributes, batch_id, external_attributes, jurisdiction, business_domain, and priority labels should not be changed.
> - The value of jurisdiction must be a value of `JRSDCN_NM` column from `KDD_JRSDCN` table.
> - The value of business_domain must be a value of `TF_BUS_DMN_NM` column from `DIM_KDD_BUS_DMN` table.
> - The value of priority must be a value of `V_ALERT_PRIORITY_NAME` column from `DIM_ALERT_PRIORITY_TYPE` table.

8.2 Audit Queries

Table 8-5 Audit Queries for ISO20022

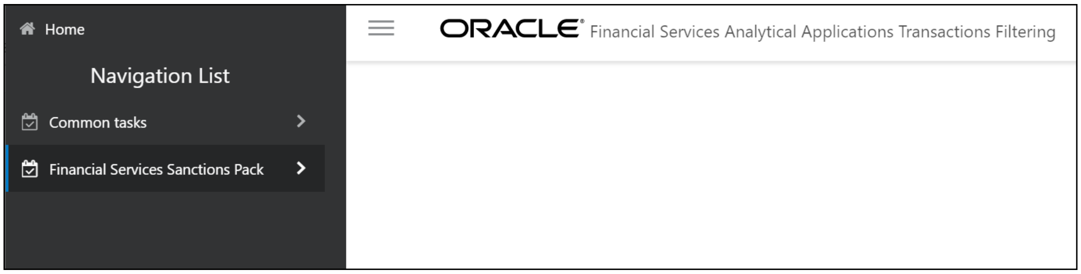
Table Name	Query	Description
FCC_TF_XML_XSD_CONF	Select * from FCC_TF_XML_XSD_CONF_HIST	Run this query to see the history of all the actions that have been performed.
FCC_TF_XML_MSG_TAG_FLD_X- PATH	Select * from FCC_TF_XML_MSG_TAG_FLD_XPATH _HIST	Run this query to see the history of all the actions performed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

9 Configurations for the US NACHA Batch Process

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

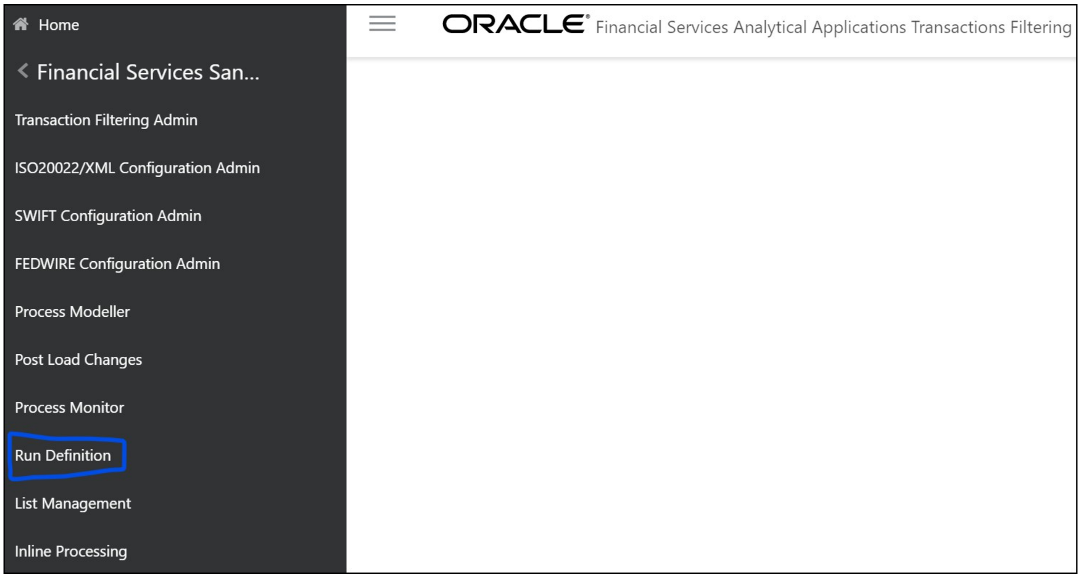
1. On the **Financial Services Analytical Applications Transactions Filtering** landing page, click **Financial Services Sanctions Pack.**

Figure 9-1 Financial Services Sanctions Pack Menu


Home
Navigation List
Common tasks
Financial Services Sanctions Pack
ORACLE Financial Services Analytical Applications Transactions Filtering

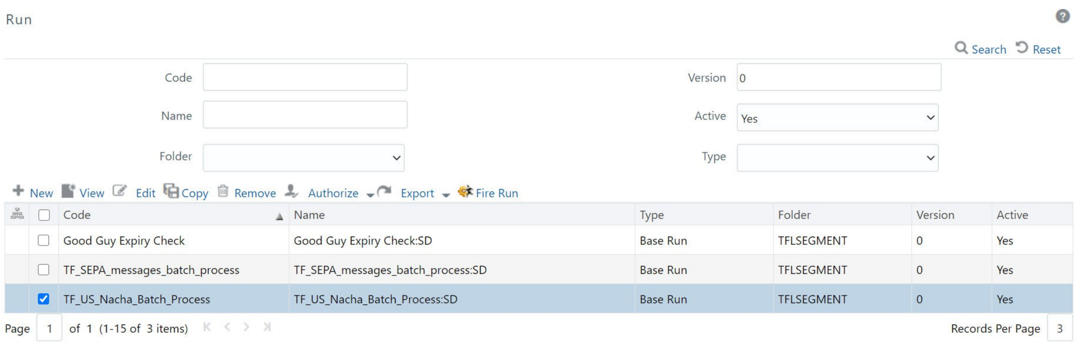
2. Click **Run Definition.** The **Run page** is displayed.

Figure 9-2 Run Definition Link


Home
Financial Services San...
Transaction Filtering Admin
ISO20022/XML Configuration Admin
SWIFT Configuration Admin
FEDWIRE Configuration Admin
Process Modeller
Post Load Changes
Process Monitor
Run Definition
List Management
Inline Processing
ORACLE Financial Services Analytical Applications Transactions Filtering

3. In the **Run** page, select the **TF_US_NACHA_Batch_Process** batch.

Figure 9-3 Run Page



Run

Search Reset

Code:
Version: 0
Name:
Active: Yes
Folder:
Type:

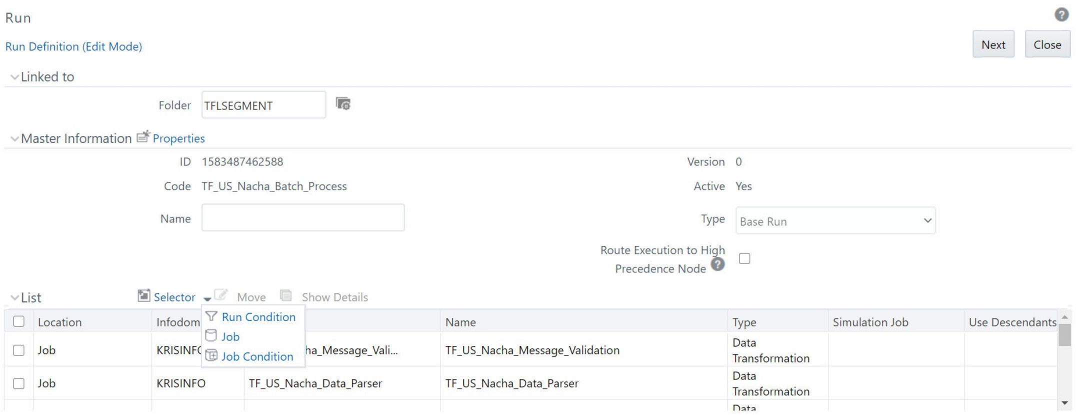
	Code	Name	Type	Folder	Version	Active
□	Good Guy Expiry Check	Good Guy Expiry Check:SD	Base Run	TFLSEGMENT	0	Yes
□	TF_SEPA_messages_batch_process	TF_SEPA_messages_batch_process:SD	Base Run	TFLSEGMENT	0	Yes
☑	TF_US_Nacha_Batch_Process	TF_US_Nacha_Batch_Process:SD	Base Run	TFLSEGMENT	0	Yes

Page 1 of 1 (1-15 of 3 items)

Records Per Page 3

4. Click **Edit** . The **Run** page is displayed in Edit mode.

Figure 9-4 Run Definition (Edit Mode)



Run

Run Definition (Edit Mode)

Linked to

Folder: TFLSEGMENT

Master Information Properties

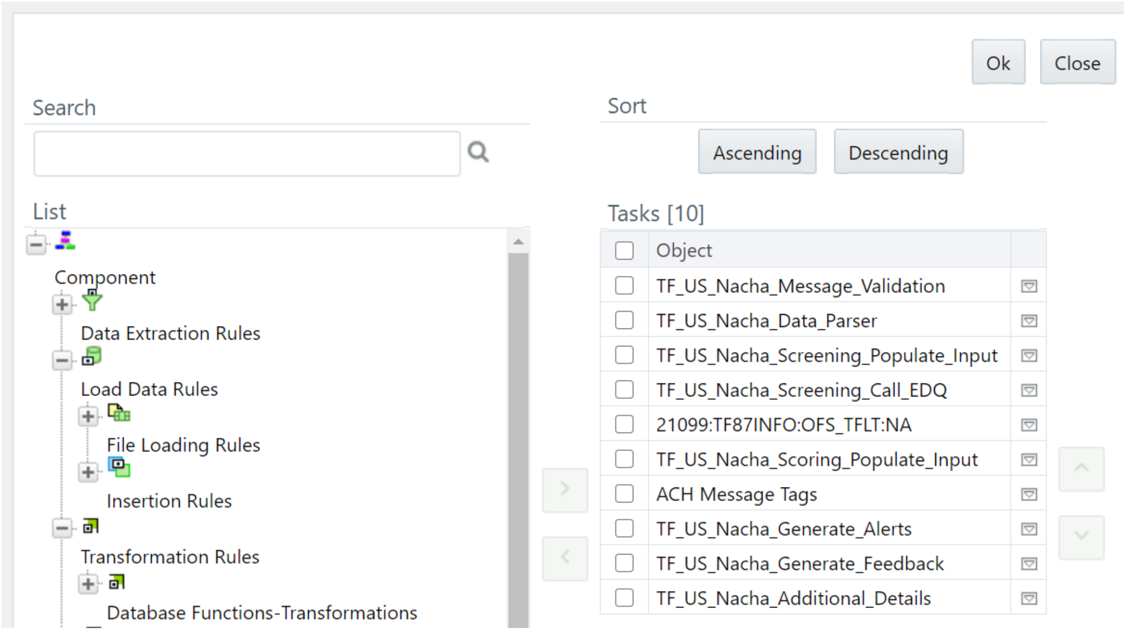
ID: 1583487462588
Version: 0
Code: TF_US_Nacha_Batch_Process
Active: Yes
Name:
Type: Base Run
Route Execution to High Precedence Node: □

List

□	Location	Infodom		Name	Type	Simulation Job	Use Descendants
□	Job	KRISINFO	ha_Message_Vali...	TF_US_Nacha_Message_Validation	Data Transformation		
□	Job	KRISINFO	TF_US_Nacha_Data_Parser	TF_US_Nacha_Data_Parser	Data Transformation		
					Data		

5. Click **Selector** Selector and then click **Job** Job from the drop-down list. The **Component Selec- tor** window is displayed.

Figure 9-5 Component Selector Window



Search

Sort

List

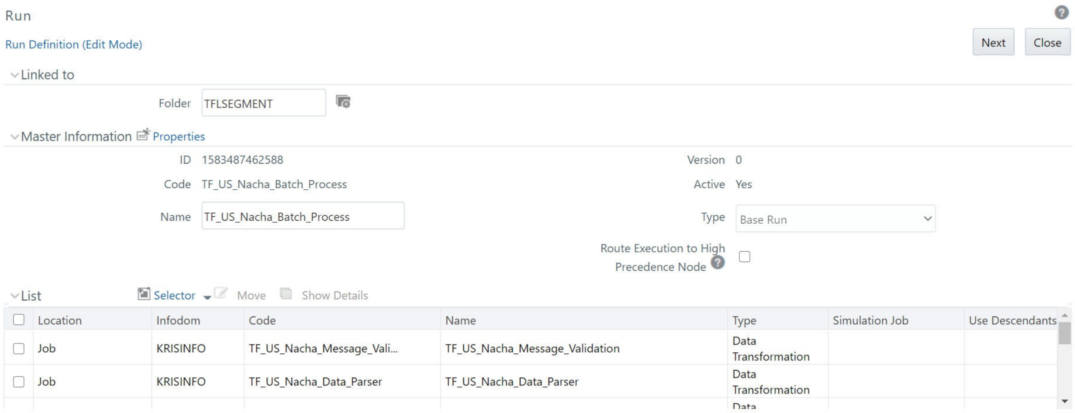
- Component
  - Data Extraction Rules
  - Load Data Rules
    - File Loading Rules
    - Insertion Rules
  - Transformation Rules
    - Database Functions-Transformations

Tasks [10]

□	Object
□	TF_US_Nacha_Message_Validation
□	TF_US_Nacha_Data_Parser
□	TF_US_Nacha_Screening_Populate_Input
□	TF_US_Nacha_Screening_Call_EDQ
□	21099:TF87INFO:OFS_TFLT:NA
□	TF_US_Nacha_Scoring_Populate_Input
□	ACH Message Tags
□	TF_US_Nacha_Generate_Alerts
□	TF_US_Nacha_Generate_Feedback
□	TF_US_Nacha_Additional_Details

1. Deselect the 21099:TF87INFO:OFS_TFLT:NA task.
2. Click **Ok**. The **Run** page with the **Run Definition** is displayed in Edit mode.
3. Provide a **Name** for the batch.

Figure 9-6 Run Definition (Edit Mode) – Batch Name



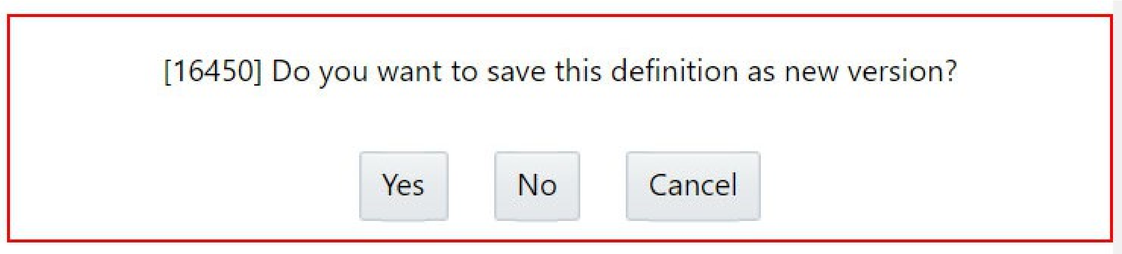
Folder: TFLSEGMENT

ID: 1583487462588
Version: 0
Code: TF_US_Nacha_Batch_Process
Active: Yes
Name: TF_US_Nacha_Batch_Process
Type: Base Run
Route Execution to High Precedence Node: □

□	Location	Infodom	Code	Name	Type	Simulation Job	Use Descendants
□	Job	KRISINFO	TF_US_Nacha_Message_Vali...	TF_US_Nacha_Message_Validation	Data Transformation		
□	Job	KRISINFO	TF_US_Nacha_Data_Parser	TF_US_Nacha_Data_Parser	Data Transformation		
					Data		

4. Click **Next**.
5. Click **Save**.
6. Click **No** in the **Run Rule Framework** dialog box.

Figure 9-7 Run Rule Framework Dialog Box



[16450] Do you want to save this definition as new version?

9.1 Adding New Message Type in NACHA

To add new NACHA message type in the Data Base (DB) perform the subsequent steps:

1. Goto ConvAchData.ctl file in the #FTPSHARE_PATH#/#INFODOM#/STAGE/US_NACHA/conf directory.
2. The ConvAchData.ctl file has the entries for all NACHA Message types. To add an entry for the new message type, open ConvAchData.ctl file and follow the below example format to provide the entry.

   Entry for message type **CCD**:

```
INTO TABLE FCC_ACH_IP
WHEN (V_BTH_HDR_STANDARD_ENTRY_CODE='CCD') (
V_NACHA_MSG_ID "SEQ_TF_NACHA.NEXTVAL",
V_HDR_RECORD_TYPE_CODE POSITION(1:1) CHAR TERMINATED BY WHITESPACE,
N_HDR_PRIORITY_CODE POSITION(2:3) INTEGER EXTERNAL TERMINATED BY
WHITESPACE,
V_HDR_IMMEDIATE_DESTINATION POSITION(4:13) CHAR TERMINATED BY WHITESPACE,
V_HDR_IMMEDIATE_ORIGIN POSITION(14:23) CHAR TERMINATED BY WHITESPACE,
V_HDR_TXN_DATE POSITION(24:29) CHAR TERMINATED BY WHITESPACE,
V_HDR_TXN_TIME POSITION(30:33) CHAR TERMINATED BY WHITESPACE,
V_HDR_FILE_ID_MODIFIER POSITION(34:34) CHAR TERMINATED BY WHITESPACE,
V_HDR_RECORD_SIZE POSITION(35:37) CHAR TERMINATED BY WHITESPACE,
V_HDR_BLOCKING_FACTOR POSITION(38:39) CHAR TERMINATED BY WHITESPACE,
V_HDR_FORMATCODE POSITION(40:40) CHAR TERMINATED BY WHITESPACE,
V_HDR_IMMEDIATE_DEST_NAME POSITION(41:63) CHAR TERMINATED BY WHITESPACE,
V_HDR_IMMEDIATE_ORIGIN_NAME POSITION(64:86) CHAR TERMINATED BY WHITESPACE,
V_HDR_REFERENCE_CODE POSITION(87:94) CHAR TERMINATED BY WHITESPACE,
V_BTH_HDR_RECORD_TYPE_CODE POSITION(95:95) CHAR TERMINATED BY WHITESPACE,
N_BTH_HDR_SERVICE_CODE POSITION(96:98) INTEGER EXTERNAL TERMINATED BY
WHITESPACE,
V_BTH_HDR_COMPANY_NAME POSITION(99:114) CHAR TERMINATED BY WHITESPACE,
V_BTH_HDR_COMPANY_DISC_DATE POSITION(115:134) CHAR TERMINATED BY
WHITESPACE,
V_BTH_HDR_COMPANY_ID POSITION(135:144) CHAR TERMINATED BY WHITESPACE,
V_BTH_HDR_STANDARD_ENTRY_CODE POSITION(145:147) CHAR TERMINATED BY
WHITESPACE,
V_BTH_HDR_COMPANY_ENTERY_DESC POSITION(148:157) CHAR TERMINATED BY
WHITESPACE,
V_BTH_HDR_COMPANY_DESC_DATE POSITION(158:163) CHAR TERMINATED BY
WHITESPACE,
V_BTH_HDR_EFFECTIVE_ENTRY_DATE POSITION(164:169) CHAR TERMINATED BY
WHITESPACE,
V_BTH_HDR_SETTLEMENT_DATE POSITION(170:172) CHAR TERMINATED BY WHITESPACE,
V_BTH_HDR_ORG_STATUS_COD POSITION(173:173) CHAR TERMINATED BY WHITESPACE,
V_BTH_HDR_ORG_DFI_ID POSITION(174:181) CHAR TERMINATED BY WHITESPACE,
N_BTH_HDR_BATCH_NUMBER_RAW POSITION(182:188) INTEGER EXTERNAL TERMINATED
BY WHITESPACE,
V_ENTRY_RECORD_TYPE_CODE POSITION(189:189) CHAR TERMINATED BY WHITESPACE,
N_ENTRY_TRXN_CODE POSITION(190:191) INTEGER EXTERNAL TERMINATED BY
WHITESPACE,
V_ENTRY_RECEVING_DFI_ID POSITION(192:199) CHAR TERMINATED BY WHITESPACE,
V_ENTRY_CHECK_DIGIT POSITION(200:200) CHAR TERMINATED BY WHITESPACE,
V_ENTRY_DFI_ACC_NUM POSITION(201:217) CHAR TERMINATED BY WHITESPACE,
V_ENTRY_AMOUNT POSITION(218:227)CHAR TERMINATED BY WHITESPACE,
V_ENTRY_INDIVIDUAL_ID_NUM POSITION(228:242) CHAR TERMINATED BY WHITESPACE,
V_ENTRY_RCV_COMPANY_NAME POSITION(243:264) CHAR TERMINATED BY WHITESPACE,
V_ENTRY_DISCRETIONARY_DATE POSITION(265:266) CHAR TERMINATED BY WHITESPACE,
V_ENTRY_ADD_RECORD_INDICATOR POSITION(267:267) CHAR TERMINATED BY
WHITESPACE,
N_ENTRY_TRACE_NUMBER POSITION(268:282) CHAR TERMINATED BY WHITESPACE,
N_TRACE_NUMBER POSITION(276:282) INTEGER EXTERNAL TERMINATED BY WHITESPACE,
V_ADDENDA_TYPE_CODE POSITION(284:285) CHAR TERMINATED BY WHITESPACE,
V_ADDENDA_RECORD POSITION(283:376) CHAR TERMINATED BY WHITESPACE,
V_BTH_CTL_RECORD_TYPE POSITION(377:377) CHAR TERMINATED BY WHITESPACE,
V_BTH_CTL_SERVICE_CODE POSITION(378:380) INTEGER EXTERNAL TERMINATED BY
WHITESPACE,
N_BTH_CTL_ENTRY_ADDENDA_COUNT POSITION(381:386) INTEGER EXTERNAL
TERMINATED BY WHITESPACE,
N_BTH_CTL_ENTRY_HASH POSITION(387:396) INTEGER EXTERNAL TERMINATED BY
WHITESPACE,
V_BTH_CTL_DEBIT_AMOUNT POSITION(397:408) CHAR TERMINATED BY WHITESPACE,
V_BTH_CTL_CREDIT_AMOUNT POSITION(409:420) CHAR TERMINATED BY WHITESPACE,
V_BTH_CTL_COMPANY_ID POSITION(421:430) CHAR TERMINATED BY WHITESPACE,
V_BTH_CTL_MSG_AUTH_CODE POSITION(431:449) CHAR TERMINATED BY WHITESPACE,
V_BTH_CTL_RESERVED POSITION(450:455) CHAR TERMINATED BY WHITESPACE,
V_BTH_CTL_ORG_DFI_ID POSITION(456:463) CHAR TERMINATED BY WHITESPACE,
V_BTH_CTL_BATCH_NUM POSITION(464:470) CHAR TERMINATED BY WHITESPACE,
V_CTL_RECORD_TYPE POSITION(471:471) CHAR TERMINATED BY WHITESPACE,
N_CTL_BATCH_COUNT POSITION(472:477) INTEGER EXTERNAL TERMINATED BY
WHITESPACE,
N_CTL_BLOCK_COUNT POSITION(478:483) INTEGER EXTERNAL TERMINATED BY
WHITESPACE,
N_CTL_ENTRY_COUNT POSITION(484:491) INTEGER EXTERNAL TERMINATED BY
WHITESPACE,
N_CTL_ENTRY_HASH POSITION(492:501) INTEGER EXTERNAL TERMINATED BY
WHITESPACE,
V_CTL_TOTAL_DEBIT_AMOUNT POSITION(502:513) CHAR TERMINATED BY WHITESPACE,
V_CTL_TOTAL_CREDIT_AMOUNT POSITION(514:525) CHAR TERMINATED BY WHITESPACE,
V_CTL_RESERVED POSITION(526:564) CHAR TERMINATED BY WHITESPACE,
N_FILE_ID POSITION(565:571) INTEGER EXTERNAL TERMINATED BY WHITESPACE,
N_BTH_HDR_BATCH_NUMBER "trim(:N_FILE_ID
)||''||trim(:N_BTH_HDR_BATCH_NUMBER_RAW)",
N_TXN_ID "trim(:N_FILE_ID
 )||''||trim(:N_BTH_HDR_BATCH_NUMBER_RAW)||''||
trim(:N_ENTRY_TRACE_NUMBER)",
V_PATH POSITION(572:641) CHAR TERMINATED BY WHITESPACE,
V_filename POSITION(642:900) CHAR TERMINATED BY WHITESPACE
)
```

> ⓘ **Note**
>
> The V_HDR_RECORD_TYPE_CODE column name in FCC_ACH_IP table has the value of POSITION (1:1). This position is given per message specification. Similarly, entries will be added for other parameters per the Message standards.

3. Save and run the `ConvAchData.ctl` file to load the newly added message data in to the DB.

The Enterprise Data Quality (EDQ) configurations for each message must be configured in the `FCC_ACH_EDQ_CONF` table and Inline Processing Engine (IPE) configurations for each message must be configured in `FCC_ACH_IPE_CONF` table. For more information on `FCC_ACH_EDQ_- CONF` table and `FCC_ACH_IPE_CONF` table, see Oracle Financial Services Data Model Reference Guide

10 Enterprise Data Quality (EDQ) Configurations

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

EDQ has the following key features:

- Integrated data profiling, auditing, and cleansing and matching
- Browser-based client access
- Ability to handle all types of data (for example, customer, product, asset, financial, and operational)
- Connection to any Java Database Connectivity (JDBC) compliant data sources and targets
- Multi-user project support (Role-based access, issue tracking, process annotation, and version control)
- Representational State Transfer Architecture (REST) support for designing processes that may be exposed to external applications as a service
- Designed to process large data volumes
- A single repository to hold data along with gathered statistics and project tracking information, with shared access
- Intuitive graphical user interface designed to help you solve real-world information quality issues quickly
- Easy, data-led creation and extension of validation and transformation rules
- Fully extensible architecture allowing the insertion of any required custom processing For more information on EDQ, see Oracle Enterprise Data Quality Documentation.

10.1 Performance Improvement Measures for EDQ

> **Note**
>
> The following are some recommendations to help improve performance when you are dealing with bulk transactions. Perform these steps ONLY after you have completed all configurations for EDQ.

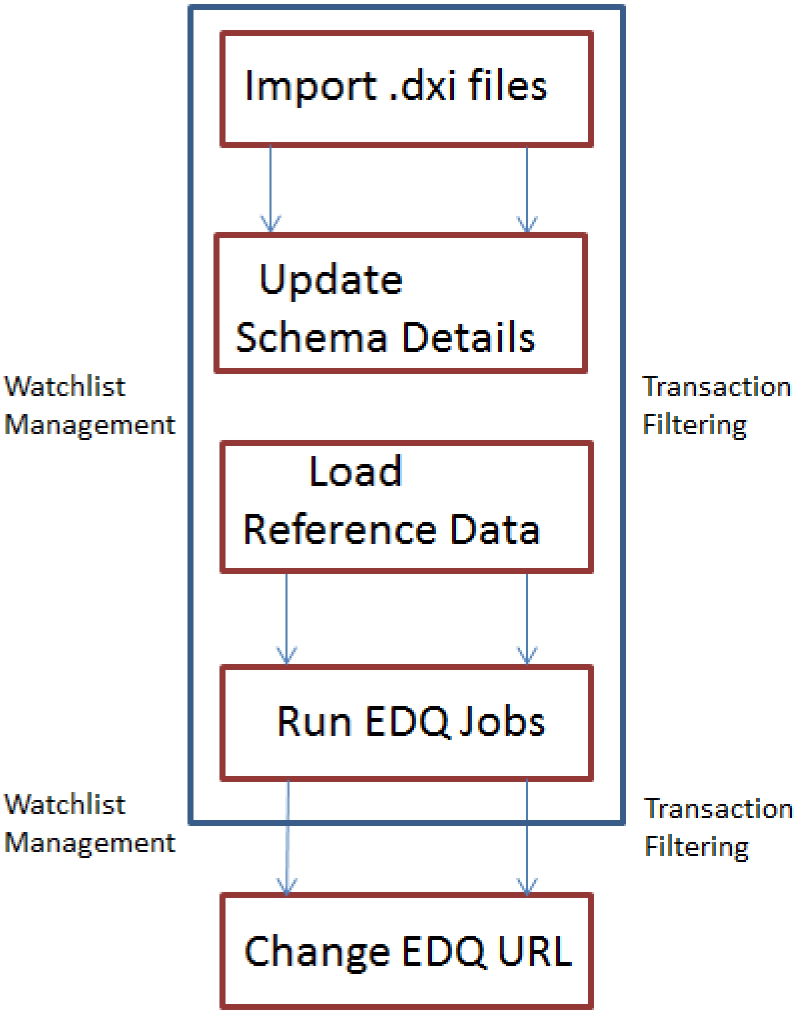
- Web Services are CPU-intensive, that is, they are frequently executed, and receive intermittent sets of simultaneous requests. Simultaneously running all batch requests slows down the real- time processing response time. To avoid this, set the following properties in the `director.properties` file in the `<domain_name>/edq/oedq.local.home/` directory:

  - Run the data preparation job for web services, for example, `Watch-list Management`, when real-time processing stops.
  - Set the `runtime.threads` value to a number which is lesser than the total cpu-cores so that both the cpu-cores can run in parallel. This ensures that the batch does not occupy all cores and allows real-time processing to run. The default value is 0, that is, the batch threads equal the number of cpu-cores on the system.
  - Set the `runtime.intervalthreads` value to display the number of cpu-cores. This allows for simultaneous processing, efficient resource utilization, and faster turnaround time. The default value is 1, that is, requests are processed sequentially on a single core which leads to underutilization.
  - Set the `workunitexecutor.outputThreads` value to a number which is greater than the number of cpu-cores and number of connection to write results and staged data to the database to tune IO heavy real-time process. This is particularly useful when the database machine is more powerful than the EDQ server.
  - Set the `resource.cache.maxrows` value to increase the number of rows for the reference data in memory. This yields a faster response time. By default, the maximum number of rows you can load is 100000.
- Optimize the data cluster definition and size of each cluster for real-time processing.
- Optimize attributes which are critical to performance such as watch list types, reference data size, and data store size.
- Optimize data for the `EDQ_RES` and `EDQ_STAGING` tablespace to improve performance. The minimum size for `EDQ_RES` must be 200-300 GB.
- Optimize the OEDQ job performance by minimizing result writing and disabling the sort and filtering feature.
- Adjust the response time by tuning the java options in the EDQ domain. To do this, follow these steps:
  - Open the `setStartupEnv.sh` file in the `<domain name given for EDQ>/bin` directory.
  - Update the `-server -d64 -Xms16G -Xmx16G -XX:+UseG1GC -XX:+UseAdaptiveSizePolicy -XX:MaxGCPauseMillis=500 -Doracle.jdbc.javaNetNio=false -XX:InitiatingHeapOccupancyPercent=80 -XX:ReservedCodeCacheSize=128m` `attribute in the # Startup parameters for STARTUP_GROUP EDQ-MGD-SVRS` section based on your requirments.
- Set the OEDQ parser processor to **Parse Mode** instead of to **Parse And Profile**.
- Update the user credentials for *dnadmin* from the default realm to the authentication realm.
- Enable the EDQ domain to operate in production mode.
- Disable the following clusters in Name and Address service to improve performance:
- Individual Family Name
- Individual Given Name
- Entity Name Meta
- Entity Start End Name Tokens
- Individual Initials

10.2 EDQ Configuration Process Flow

The following image shows the EDQ configuration process flow:

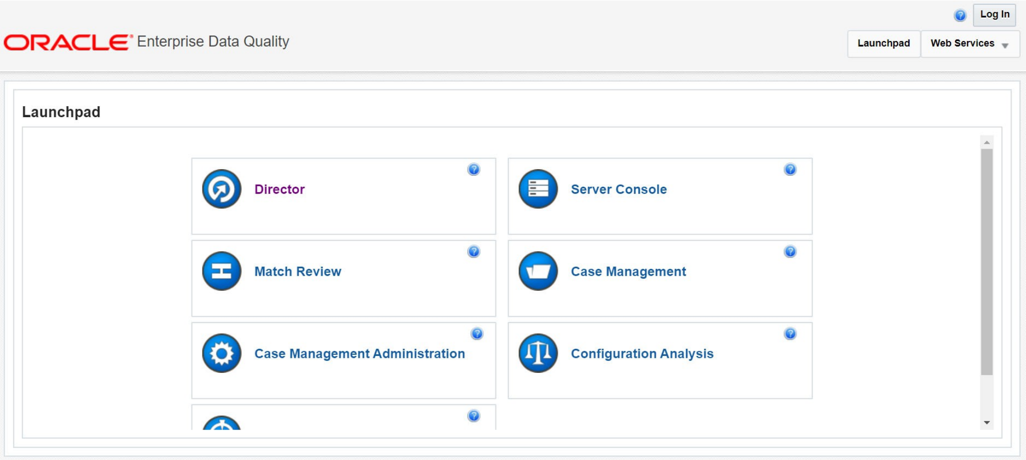
Figure 10-1 Enterprise Data Quality (EDQ) Configuration Steps



To configure EDQ, follow these steps:

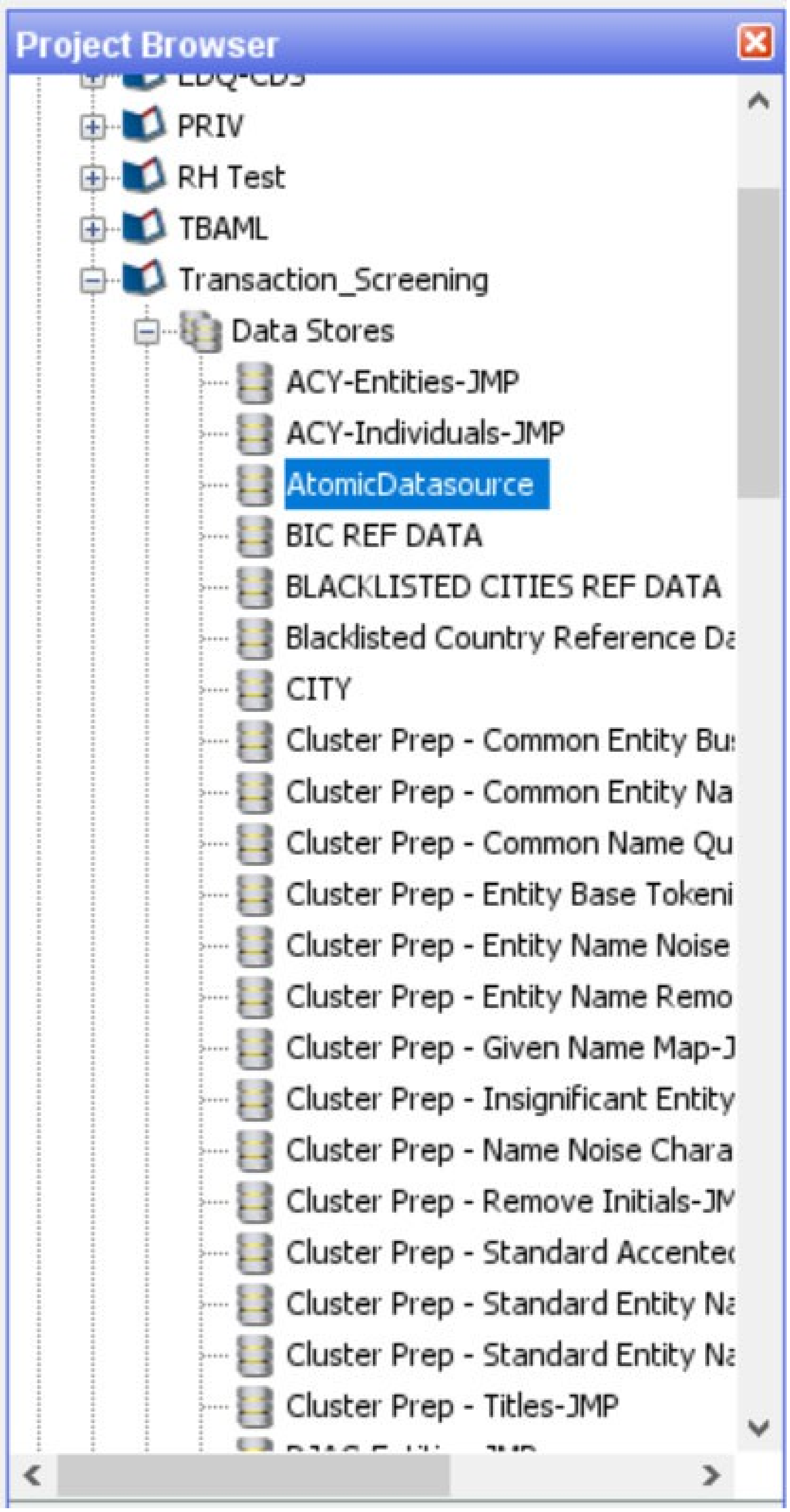
1. Import the `Watchlist Management.dxi` file from the `FIC_HOME/SanctionsCommon` path.
2. Import the `Transaction_Screening.dxi` file from the `FIC_HOME/Transaction_Processing` path (This is for SWIFT messages only).
3. Import the `Transaction_Screening_SEPA.dxi` file from the `FIC_HOME/Transaction_Processing` path (This is for ISO20022 messages only).
4. For these projects, enter the applicable organization-specific Atomic schema details in the **Edit Data Store** window. To access the **Edit Data Store** window, follow these steps:
   a. Go to the EDQ URL and open the **Director** menu. The **Director** landing page appears.

Figure 10-2   Director Menu in EDQ



b. In the **Director** landing page, expand the **Transaction_Screening** project in the **Project Browser** pane.

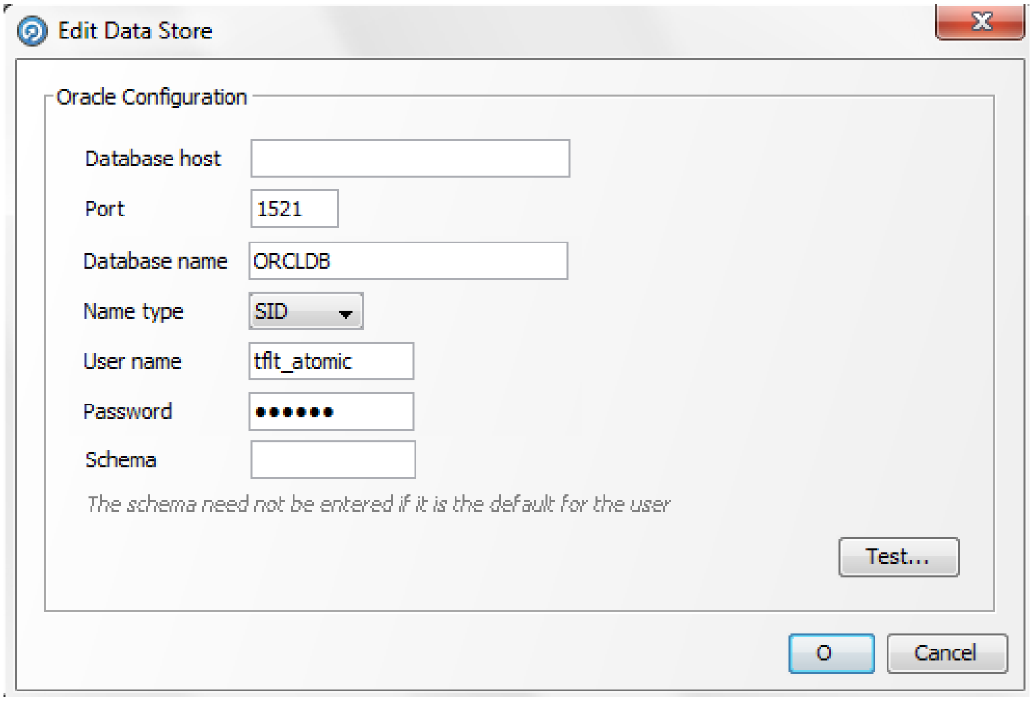
Figure 10-3 Project Browser Pane



Project Browser
EDQ-CDS
PRIV
RH Test
TBAML
Transaction_Screening
Data Stores
ACY-Entities-JMP
ACY-Individuals-JMP
AtomicDatasource
BIC REF DATA
BLACKLISTED CITIES REF DATA
Blacklisted Country Reference Da
CITY
Cluster Prep - Common Entity Bu
Cluster Prep - Common Entity Na
Cluster Prep - Common Name Qu
Cluster Prep - Entity Base Tokeni
Cluster Prep - Entity Name Noise
Cluster Prep - Entity Name Remo
Cluster Prep - Given Name Map-J
Cluster Prep - Insignificant Entity
Cluster Prep - Name Noise Chara
Cluster Prep - Remove Initials-JM
Cluster Prep - Standard Accentec
Cluster Prep - Standard Entity Na
Cluster Prep - Standard Entity Na
Cluster Prep - Titles-JMP

c. Expand the **Data Stores** node and open **AtomicDatasource**. The **Edit Data Store** window appears.

Figure 10-4 Edit Data Store Window

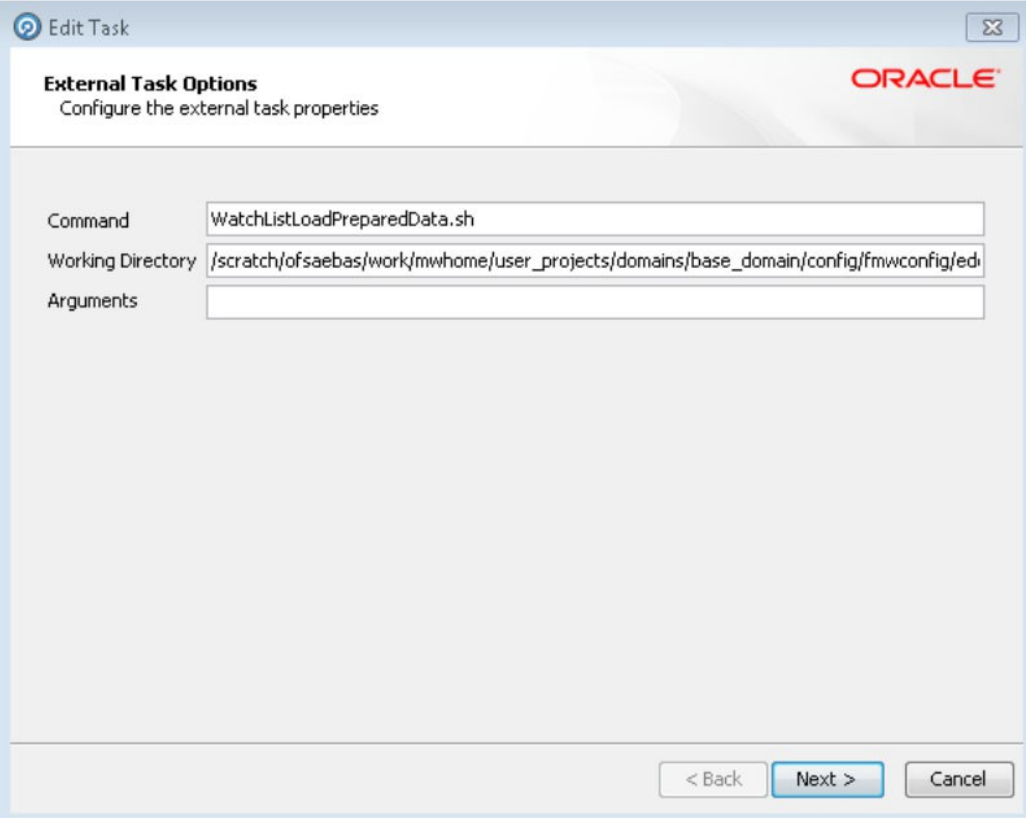


Database host:
Port: 1521
Database name: ORCLDB
Name type: SID
User name: tflt_atomic
Password: ●●●●●●
Schema:

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

5. Load the Reference data. For more information on Reference data, see Viewing Reference Data for Web Services.
6. Update the command area path in the following locations:
   - `Watchlist Management > External Tasks > WatchListLoadPreparedData`
   - `Transaction_Screening > External Tasks > WatchListLoadData`
   - `Transaction_Screening > External Tasks > SanctionedListRefLoadData`

Figure 10-5 Edit Task Window



External Task Options
Configure the external task properties

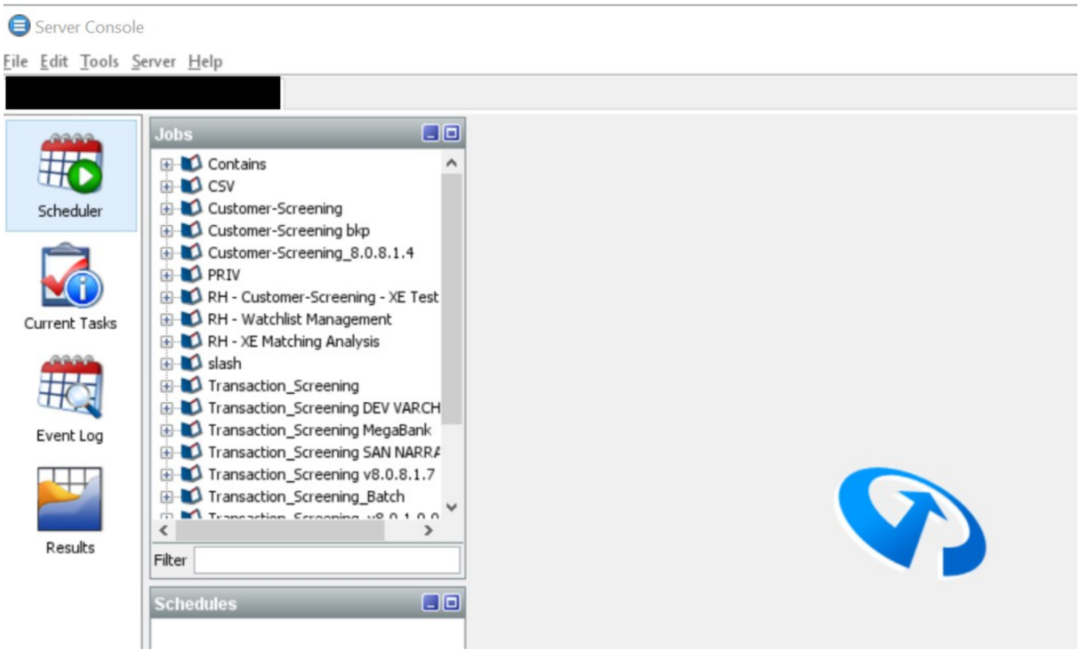
Command: WatchListLoadPreparedData.sh

Working Directory: /scratch/ofsaebas/work/mwhome/user_projects/domains/base_domain/config/fmwconfig/edı

Arguments:

7. Go to the EDQ URL and open the **Server Console** menu. The **Server Console** landing page appears.

Figure 10-6 Server Console Menu in EDQ


Server Console
File Edit Tools Server Help
Scheduler
Current Tasks
Event Log
Results
Jobs
Contains
CSV
Customer-Screening
Customer-Screening bkp
Customer-Screening_8.0.8.1.4
PRIV
RH - Customer-Screening - XE Test
RH - Watchlist Management
RH - XE Matching Analysis
slash
Transaction_Screening
Transaction_Screening DEV VARCH
Transaction_Screening MegaBank
Transaction_Screening SAN NARRA
Transaction_Screening v8.0.8.1.7
Transaction_Screening_Batch
Filter
Schedules

[redacted]

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

- Analyze Reference Data Quality
- Download, Prepare, Filter and Export All Lists
- Generate StopPhrases

9. Run the **MAIN** job under the **Transaction_Screening** project.
10. Change the EDQ URL in the Transaction Filtering application. To change the EDQ URL, see Con- figuring the Application Level Parameters.

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

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

10.2.1 Importing the Transaction Screening Project

For information on importing the Transaction Screening project, see the *Importing the OFS Customer Screening and OFS Transaction Filtering Projects* section in the Oracle Financial Services Sanctions Installation Guide.

10.2.2 Configuring Watch List Management and Transaction Filtering

The Oracle Financial Services Transaction Filtering distribution contains two run Profiles for configuring Watch List Management and screening: `watchlist-management.properties` and `watchlist-screening.properties`. These profiles are available in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory when you log into the WinSCP server.

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

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

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

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

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

10.2.2.1 Preparing Watch List Data

Oracle Financial Services Transaction Filtering is pre-configured to handle reference data from the following sources:

- HM Treasury
- OFAC
- EU consolidated list
- UN consolidated list
- World-Check
- Dow Jones watch list
- Dow Jones Anti-Corruption List
- Accuity Reference Data
- For information on the watch lists, see Appendix A: Watch Lists.

10.2.2.2 Setting Up Private Watch List

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 data, 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

> **Note**
>
> watchlist- management.properties

Run Profile, follow these steps:

1. Move your private watch list data to the staging area by setting

   > **Note**
   >
   > phase.PRIV\ -\ Stage\ reference\ lists.enabled

   to **Y**.
2. Set

   > **Note**
   >
   > 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.

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

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

- Watch list snapshots
- Intermediate filtered watch list staged data
- Centralized reference data staged data and snapshots

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

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

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

```
stageddata.ACY_All.visible = Y
```

```
stageddata.ACY_Sources.visible = Y
```

Configuring Match Rules

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

Note

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

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

```
phase.*.process.*.[I0100]\ Exact\ name\ only.san_ule_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.*.[I0100]\ Exact\ name\ only.san_rule_en- abled =
false
```

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

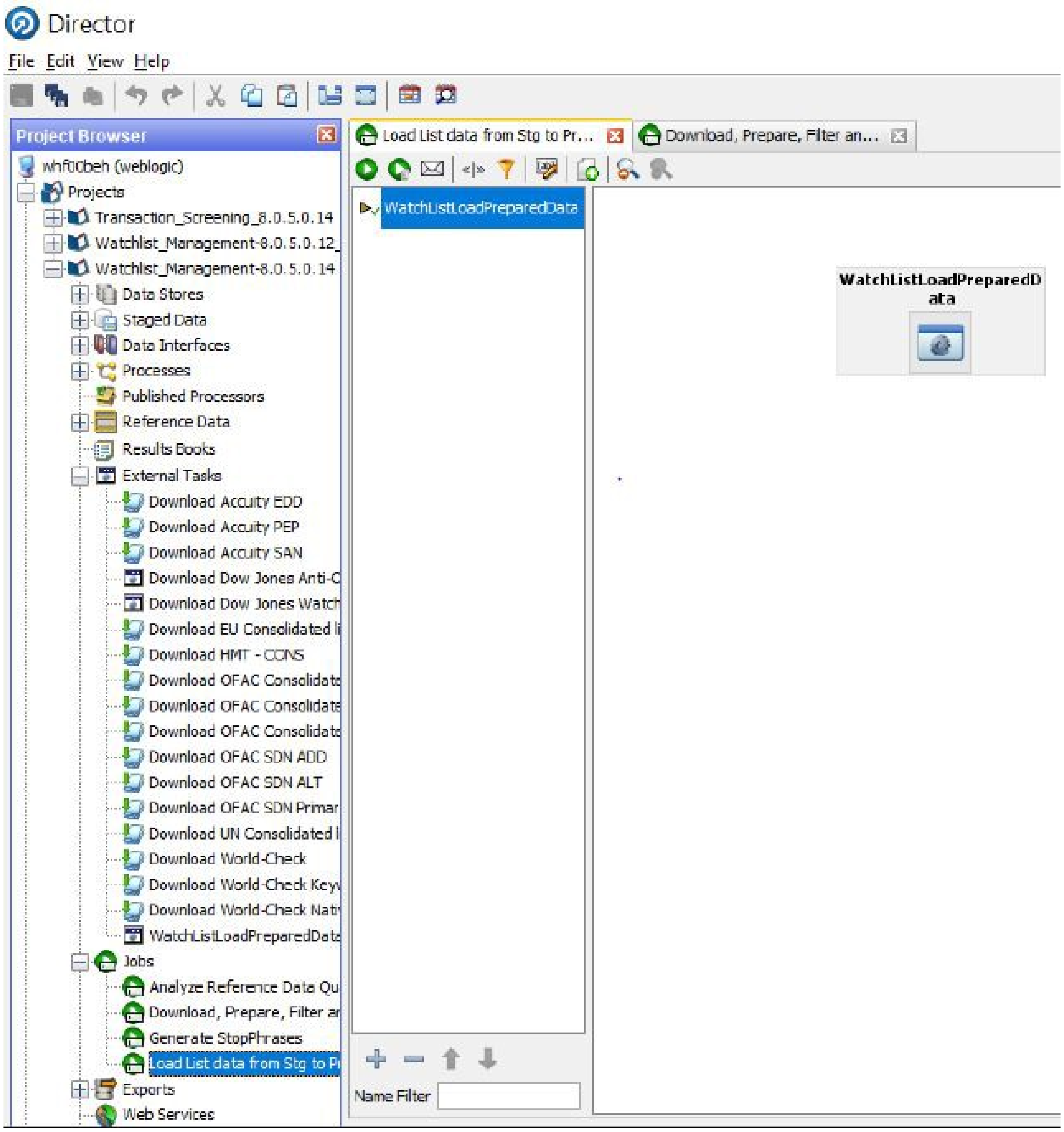
Configuring Jobs

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 10-7 EDQ Director Menu


Director
File Edit View Help
Project Browser
whf00beh (weblogic)
Projects
Transaction_Screening_8.0.5.0.14
Watchlist_Management-8.0.5.0.12
Watchlist_Management-8.0.5.0.14
Data Stores
Staged Data
Data Interfaces
Processes
Published Processors
Reference Data
Results Books
External Tasks
Download Accuity EDD
Download Accuity PEP
Download Accuity SAN
Download Dow Jones Anti-C
Download Dow Jones Watch
Download EU Consolidated li
Download HMT - CONS
Download OFAC Consolidate
Download OFAC Consolidate
Download OFAC Consolidate
Download OFAC SDN ADD
Download OFAC SDN ALT
Download OFAC SDN Primar
Download UN Consolidated l
Download World-Check
Download World-Check Keyw
Download World-Check Nati
WatchListLoadPreparedData
Jobs
Analyze Reference Data Qu
Download, Prepare, Filter ar
Generate StopPhrases
Load List data from Stg to Pr
Exports
Web Services
Load List data from Stg to Pr...
Download, Prepare, Filter an...
WatchListLoadPreparedData
WatchListLoadPreparedData
Name Filter

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

10.2.2.3 Filtering Watch List Data

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

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**.

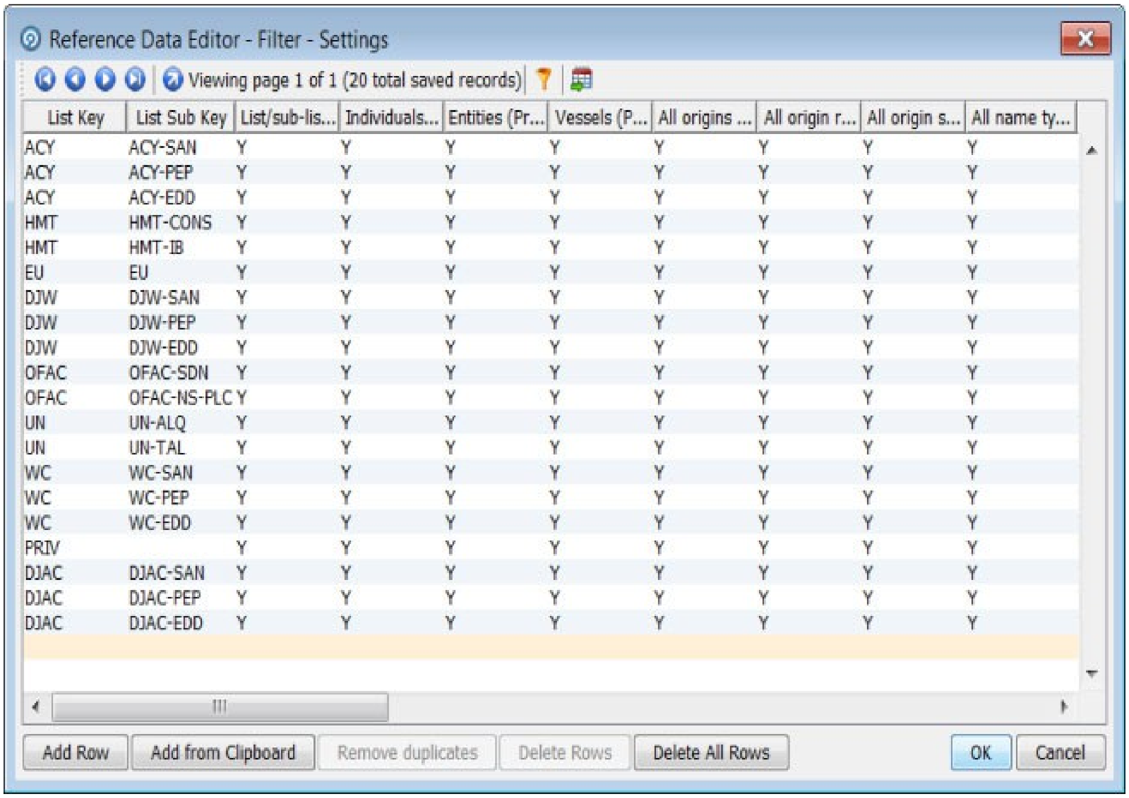
Configuring Watch List Filtering

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

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

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

Figure 10-8 Reference Data Editor - Filter - Settings Window



Viewing page 1 of 1 (20 total saved records)

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.

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.

Setting Multiple Values for Primary and Secondary Filters

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

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

To filter using one or more of these options, set the relevant value in the Filter - Settings reference data to **N**, and then make further changes to the corresponding reference data.

> **Note**
>
> When you set the Filter - Settings reference data to **N**, only the records that match the values set in the corresponding reference data are included. For example, if you set the value of All name qualities to **N** in Filter - Settings, then you can determine which name qualities must be included for each watch list in the Filter - Primary Name Qualities reference data. For instance, if you include a row for high-quality names in the EU watch list, but you do not include rows for medium-quality and low-quality names for this watch list, then only records with high-quality names are included in the watch list.

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

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

Filtering World-Check Data

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

- Enable filtering in the Run Profiles
- Configure the Primary filters in the Watch List Management project to return only active records for sanctioned individuals (not entities) originating from the EU list
- Enable the filtering of Linked Profiles in the Watch List Management project
- Configure the Secondary filters in the Transaction Filtering project to further filter out all Linked Profiles of deceased individuals.

Setting Filtering options in the Run Profiles

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

```
phase.WC\ -\ Prepare\ without\ filtering.enabled = N
phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = Y
phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = Y
In the watchlist-screening.properties Run Profile, set the World-Check
filtering phases as follows:
phase.WC\ -\ Load\ without\ filtering.enabled = N
phase.WC\ -\ Load\ with\ filtering\ (Part\ 1).enabled = Y
phase.WC\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y
```

Setting Primary Filters and Linked Profiles in the Watchlist Management Project

To set the primary filters, follow these steps:

1. In the `Director` menu, open the `Watchlist Management` project and expand the `Reference Data` node.
2. Locate the `Filter - Settings` reference data and double-click to open it.
3. Ensure the List/sub-list value in the WC-SAN row is set to **Y**.
4. Set the `Entities` value in the WC-SAN row to **N**.
5. Set the `Inactive` value in the WC-SAN row to **N**.
6. Set the `All Origins` value in the WC-SAN row to **N**.
7. Ensure all other values in the `WC-SAN` row are set to **Y**.
8. Click **OK** to close the reference data and save changes.
9. Locate the `Filter - Origins` reference data and double-click to open it.
10. Add a new row with the following values:
    a. List Key - WC
    b. List Sub Key - WC-SAN
    c. Origin - EU
11. Change the `Linked Profiles` value in the `WC-SAN` row to **Y**.
12. Click **OK** to close the `Filter Settings` reference data and save changes.

Setting Secondary Filters in the Transaction_Screening Project

To set secondary filters, follow these steps:

1. Open the `Transaction_Screening` project, and expand the reference data link.
2. Locate the `Filter - Settings` reference data file, and double-click to open it.
3. Set the `Deceased` value in the `WC-SAN` row to **N**.
4. Click **OK** to close the reference data and save changes.

Screening All Data Using Sanctions Rules

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

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

10.2.2.4 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`

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 10-1 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

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

Table 10-2 Sample Data for Sanctioned Cities

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

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

Table 10-3 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

Table 10-4 Sample Data for Sanctioned Countries

Record ID	Country	ISO Country Code	Country Synonyms	Data Source	Risk Score
2	DEMOCRA TIC 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 Reg- ulations)	85
4	ZIMBABWE	ZW	NA	ITAR (International Traffic in Arms Reg- ulations)	90
5	CENTRAL AFRICAN REPUBLIC	CF	NA	EAR (Export Administration Regula- tions)	85
6	BELARUS	BY	NA	EAR (Export Administration Regula- tions)	80

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

Table 10-5 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

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

Table 10-6 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

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

Table 10-7 Sample Data for Prohibited Ports

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

10.2.2.5 Extending Prohibition Screening

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

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

11

Configuring Risk Scoring Rules

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

Before you configure the rules, you must update the sequence ID for IPE. To do this, execute the following script in the *Config* schema as a post-installation step:

```
Begin p_set_sequence_value('TASKS','5000000','Y'); end;
```

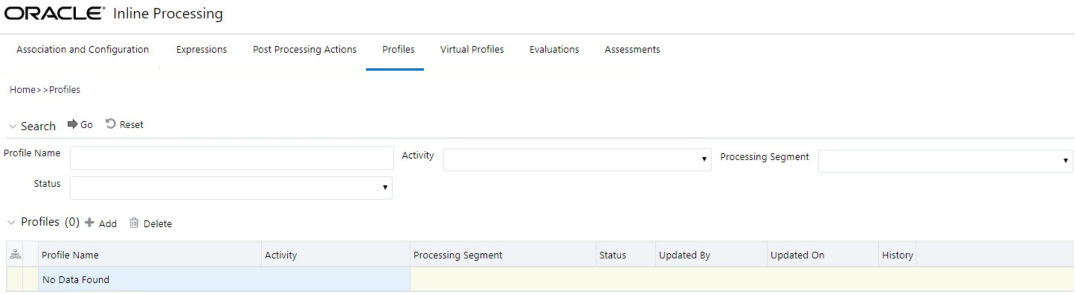
For information on the post-installation activities, see the Oracle Financial Services Behavior Detection Installation Guide .

> **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.
2. Click **Inline Processing**. The **Inline Processing** page is displayed.
   The following window shows the **Profiles** menu. Profiles are an aggregation of information. Pro- files 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 11-1 Profiles Menu

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

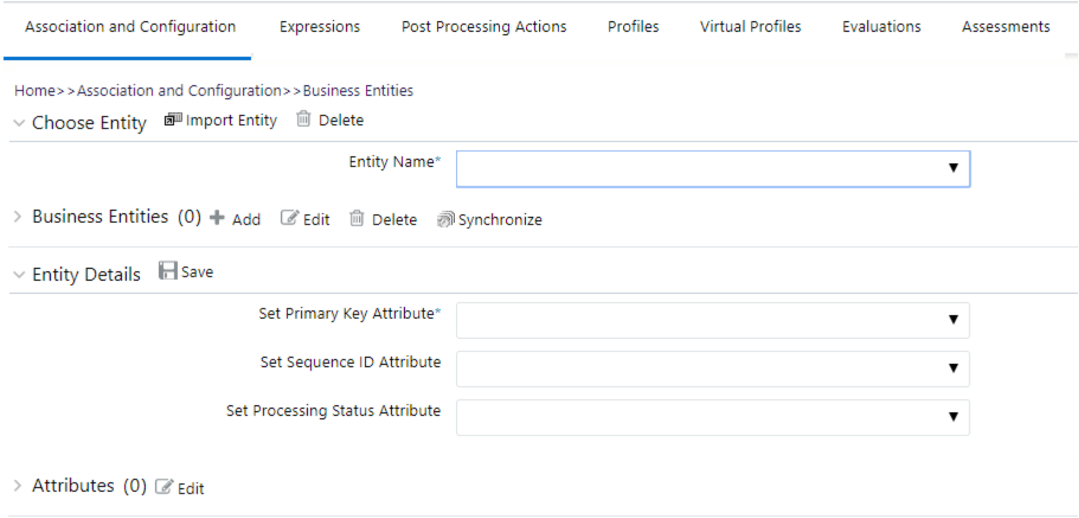
3. Import data model tables into IPE using the **Business Entities** sub-menu. A Business Entity is a virtual layer that can be added to an existing table. You can add a new business entity and search for existing business entities to modify or remove a business entity For more information on Business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

To import a table, follow these steps:

- Click the **Association and Configuration** menu**,** then click the **Business Entities** sub-menu.
- Select the Business Entity you want to import.
- Click **Import Entity**

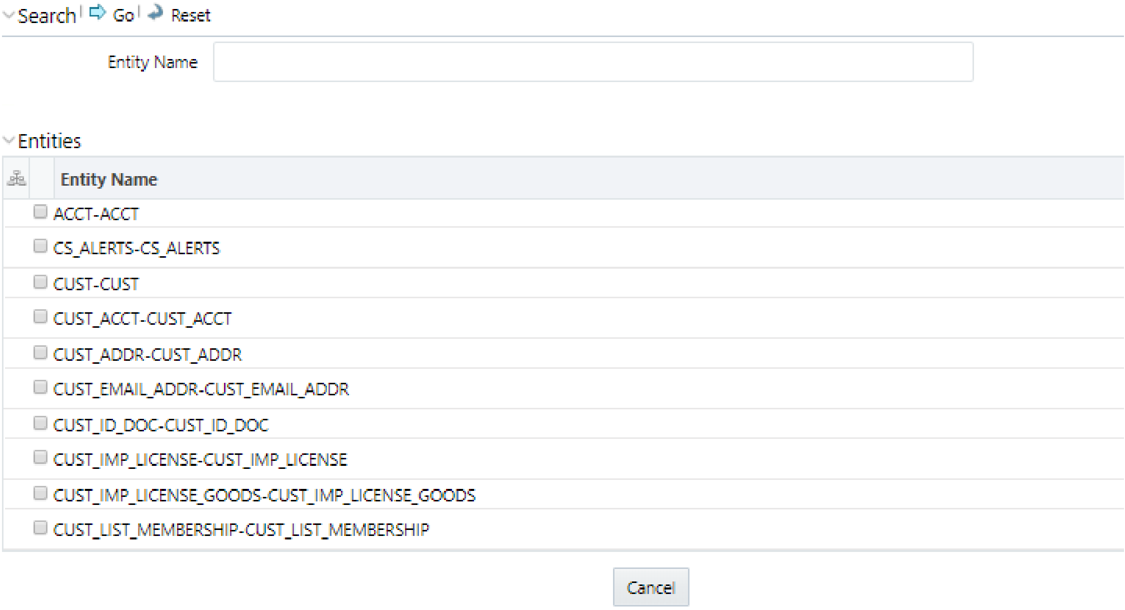
Figure 11-2 Import Entity icon.

Figure 11-3 Import Table Action



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

Figure 11-4   Entities List



- □ ACCT-ACCT
- □ CS_ALERTS-CS_ALERTS
- □ CUST-CUST
- □ CUST_ACCT-CUST_ACCT
- □ CUST_ADDR-CUST_ADDR
- □ CUST_EMAIL_ADDR-CUST_EMAIL_ADDR
- □ CUST_ID_DOC-CUST_ID_DOC
- □ CUST_IMP_LICENSE-CUST_IMP_LICENSE
- □ CUST_IMP_LICENSE_GOODS-CUST_IMP_LICENSE_GOODS
- □ CUST_LIST_MEMBERSHIP-CUST_LIST_MEMBERSHIP

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

Table 11-1   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.

Table 11-2   Business Entity Fields

Field	Description
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.

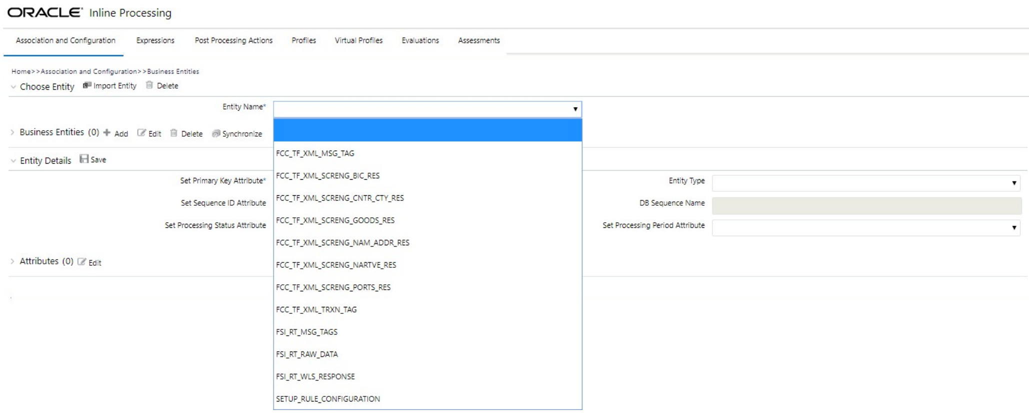
Table 11-2 (Cont.) Business Entity Fields

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.

- Click **Save**.

1. Add a business entity. To do this, follow these steps:
    - In the **Business Entities** sub-menu, select an entity from the **Entity Name** drop-down.

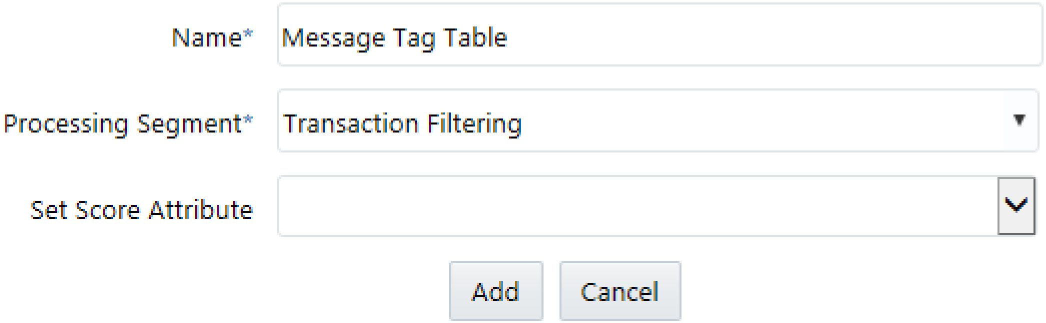
Figure 11-5 Entities List



    - Click **Add**.

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

Figure 11-6   Business Entity attributes



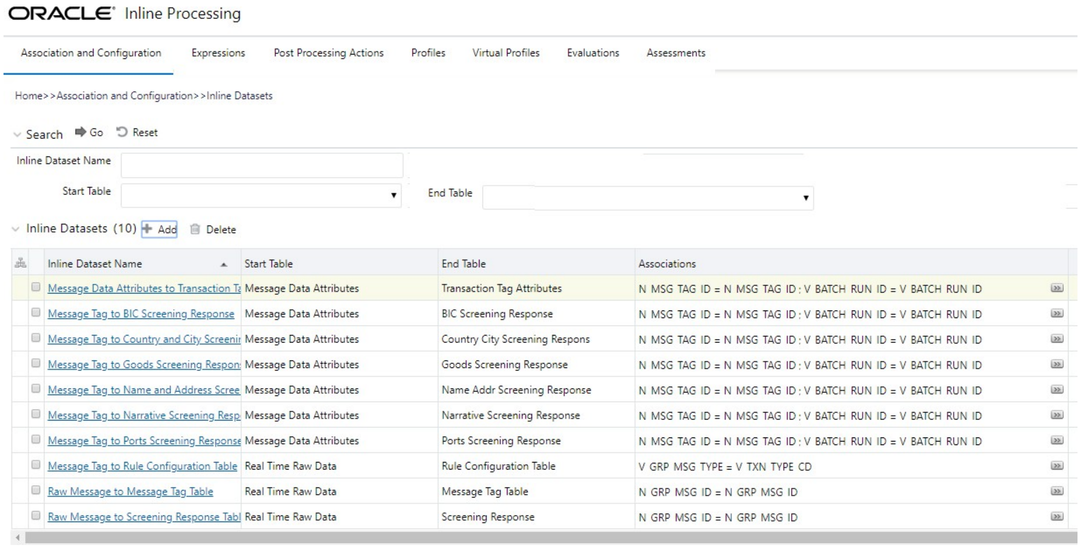
Name*	Message Tag Table
Processing Segment*	Transaction Filtering ▼
Set Score Attribute	

3. Click **Add**. The new parameter is added to the list of Business Entities on the **Business Entities** page.
4. 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 Data- set, you must define at least one join.

To add a join, follow these steps:

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

Figure 11-7   Inline Datasets page



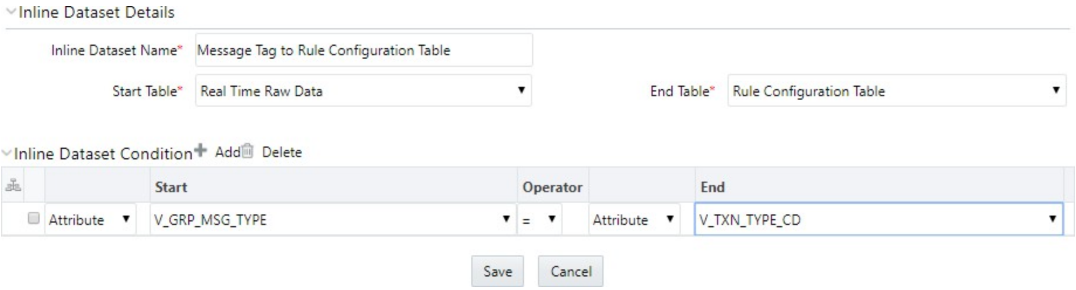
Home>>Association and Configuration>>Inline Datasets

Inline Dataset Name			
Start Table	▼	End Table	▼

	Inline Dataset Name	Start Table	End Table	Associations
□	Message Data Attributes to Transaction Ta	Message Data Attributes	Transaction Tag Attributes	N MSG TAG ID = N MSG TAG ID : V BATCH RUN ID = V BATCH RUN ID
□	Message Tag to BIC Screening Response	Message Data Attributes	BIC Screening Response	N MSG TAG ID = N MSG TAG ID : V BATCH RUN ID = V BATCH RUN ID
□	Message Tag to Country and City Screenin	Message Data Attributes	Country City Screening Respons	N MSG TAG ID = N MSG TAG ID : V BATCH RUN ID = V BATCH RUN ID
□	Message Tag to Goods Screening Respon	Message Data Attributes	Goods Screening Response	N MSG TAG ID = N MSG TAG ID : V BATCH RUN ID = V BATCH RUN ID
□	Message Tag to Name and Address Scree	Message Data Attributes	Name Addr Screening Response	N MSG TAG ID = N MSG TAG ID : V BATCH RUN ID = V BATCH RUN ID
□	Message Tag to Narrative Screening Resp	Message Data Attributes	Narrative Screening Response	N MSG TAG ID = N MSG TAG ID : V BATCH RUN ID = V BATCH RUN ID
□	Message Tag to Ports Screening Response	Message Data Attributes	Ports Screening Response	N MSG TAG ID = N MSG TAG ID : V BATCH RUN ID = V BATCH RUN ID
□	Message Tag to Rule Configuration Table	Real Time Raw Data	Rule Configuration Table	V GRP MSG TYPE = V TXN TYPE CD
□	Raw Message to Message Tag Table	Real Time Raw Data	Message Tag Table	N GRP MSG ID = N GRP MSG ID
□	Raw Message to Screening Response Tabl	Real Time Raw Data	Screening Response	N GRP MSG ID = N GRP MSG ID

- Enter a name for the inline dataset.
- In the **Start Table** field, select the start table of the join.
- In the **End Table** field, select the end table of the join.

Figure 11-8 Inline Datasets Attributes



Inline Dataset Details

Inline Dataset Name*: Message Tag to Rule Configuration Table

Start Table*: Real Time Raw Data ▾

End Table*: Rule Configuration Table ▾

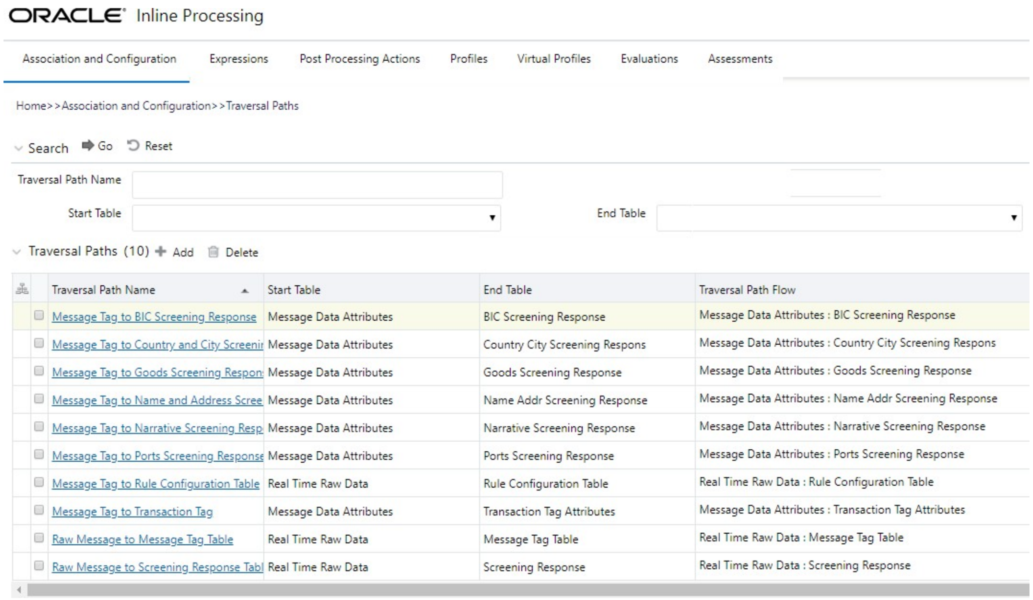
Inline Dataset Condition + Add 🗑 Delete

		Start	Operator		End
□	Attribute ▾	V_GRP_MSG_TYPE ▾	= ▾	Attribute ▾	V_TXN_TYPE_CD ▾

- Click **Add**.
- 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.

1. 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:
   - Click the **Traversal Paths** sub-menu in the **Association and Configuration** menu.
   - On the **Traversal Paths** page, click **Add**.

   Figure 11-9 Traversal Paths Page

   Traversal Path Name:

   Start Table: ▾

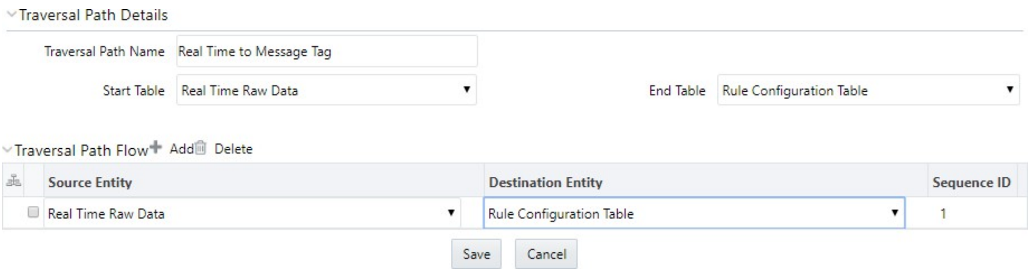
   End Table: ▾

   Traversal Paths (10) + Add 🗑 Delete

	Traversal Path Name ▲	Start Table	End Table	Traversal Path Flow
□	Message Tag to BIC Screening Response	Message Data Attributes	BIC Screening Response	Message Data Attributes : BIC Screening Response
□	Message Tag to Country and City Screenir	Message Data Attributes	Country City Screening Respons	Message Data Attributes : Country City Screening Respons
□	Message Tag to Goods Screening Respon	Message Data Attributes	Goods Screening Response	Message Data Attributes : Goods Screening Response
□	Message Tag to Name and Address Scree	Message Data Attributes	Name Addr Screening Response	Message Data Attributes : Name Addr Screening Response
□	Message Tag to Narrative Screening Resp	Message Data Attributes	Narrative Screening Response	Message Data Attributes : Narrative Screening Response
□	Message Tag to Ports Screening Response	Message Data Attributes	Ports Screening Response	Message Data Attributes : Ports Screening Response
□	Message Tag to Rule Configuration Table	Real Time Raw Data	Rule Configuration Table	Real Time Raw Data : Rule Configuration Table
□	Message Tag to Transaction Tag	Message Data Attributes	Transaction Tag Attributes	Message Data Attributes : Transaction Tag Attributes
□	Raw Message to Message Tag Table	Real Time Raw Data	Message Tag Table	Real Time Raw Data : Message Tag Table
□	Raw Message to Screening Response Tabl	Real Time Raw Data	Screening Response	Real Time Raw Data : Screening Response

   - Enter a name for the traversal path.
   - In the **Start Table** field, select the same start table that you selected in step c.<XREF>
   - In the **End Table** field, select the same end table that you selected in step d.<XREF>

Figure 11-10   Traversal Paths Attributes



Traversal Path Details

Traversal Path Name: Real Time to Message Tag

Start Table: Real Time Raw Data

End Table: Rule Configuration Table

Traversal Path Flow

Source Entity	Destination Entity	Sequence ID
Real Time Raw Data	Rule Configuration Table	1

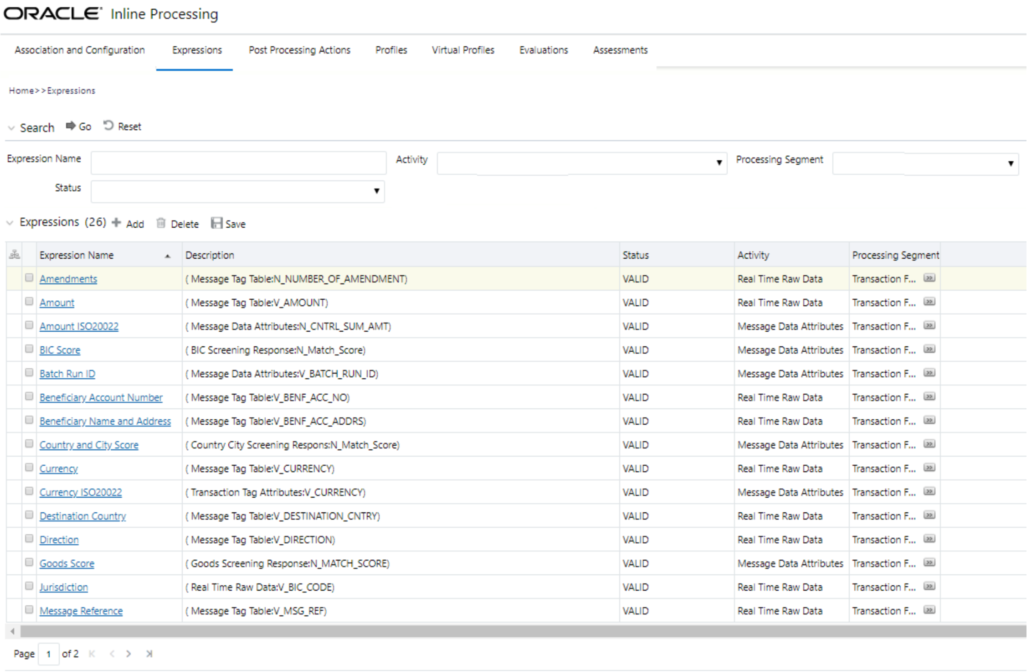
- Click **Add**.
- Select the values for the traversal path flow as shown in the figure.
- Click **Save**. The new path is added to the list of traversal paths on the **Traversal Paths** page. For more information on traversal paths, see the **Managing Traversal Paths** section in the Oracle Financial Services Inline Processing Engine User Guide.

2. 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:

- Click the **Expressions** menu.
- On the **Expressions** page, click **Add**.

Figure 11-11   Expressions Page



Home>>Expressions

Expression Name:

Activity:

Processing Segment:

Status:

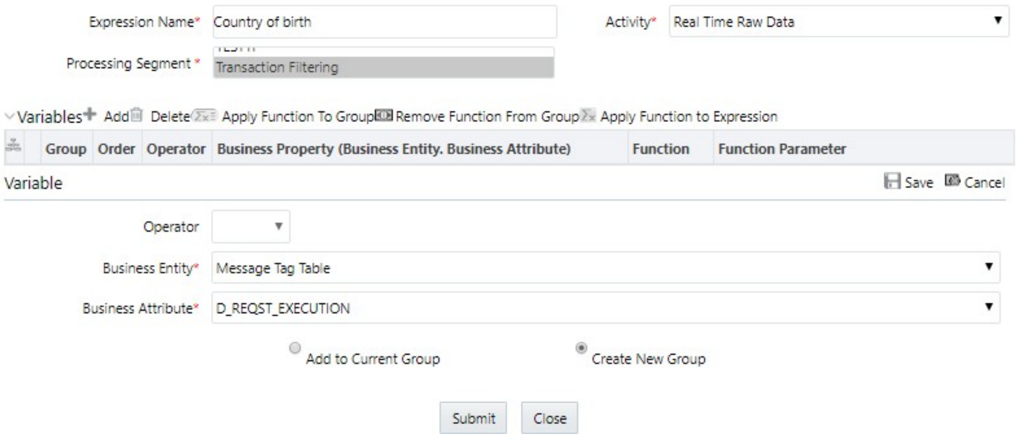
Expressions (26)

Expression Name	Description	Status	Activity	Processing Segment
Amendments	(Message Tag Table:N_NUMBER_OF_AMENDMENT)	VALID	Real Time Raw Data	Transaction F...
Amount	(Message Tag Table:V_AMOUNT)	VALID	Real Time Raw Data	Transaction F...
Amount ISO20022	(Message Data Attributes:N_CNTRL_SUM_AMT)	VALID	Message Data Attributes	Transaction F...
BIC Score	(BIC Screening Response:N_Match_Score)	VALID	Message Data Attributes	Transaction F...
Batch Run ID	(Message Data Attributes:V_BATCH_RUN_ID)	VALID	Message Data Attributes	Transaction F...
Beneficiary Account Number	(Message Tag Table:V_BENF_ACC_NO)	VALID	Real Time Raw Data	Transaction F...
Beneficiary Name and Address	(Message Tag Table:V_BENF_ACC_ADDRS)	VALID	Real Time Raw Data	Transaction F...
Country and City Score	(Country City Screening Respons:N_Match_Score)	VALID	Message Data Attributes	Transaction F...
Currency	(Message Tag Table:V_CURRENCY)	VALID	Real Time Raw Data	Transaction F...
Currency ISO20022	(Transaction Tag Attributes:V_CURRENCY)	VALID	Message Data Attributes	Transaction F...
Destination Country	(Message Tag Table:V_DESTINATION_CNTRY)	VALID	Real Time Raw Data	Transaction F...
Direction	(Message Tag Table:V_DIRECTION)	VALID	Real Time Raw Data	Transaction F...
Goods Score	(Goods Screening Response:N_MATCH_SCORE)	VALID	Message Data Attributes	Transaction F...
Jurisdiction	(Real Time Raw Data:V_BIC_CODE)	VALID	Real Time Raw Data	Transaction F...
Message Reference	(Message Tag Table:V_MSG_REF)	VALID	Real Time Raw Data	Transaction F...

Page 1 of 2

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

Figure 11-12 First Expression Attributes



Expression Name*: Country of birth

Activity*: Real Time Raw Data

Processing Segment*: Transaction Filtering

Variables + Add Delete Apply Function To Group Remove Function From Group Apply Function to Expression

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

Variable — Save Cancel

Operator:

Business Entity*: Message Tag Table

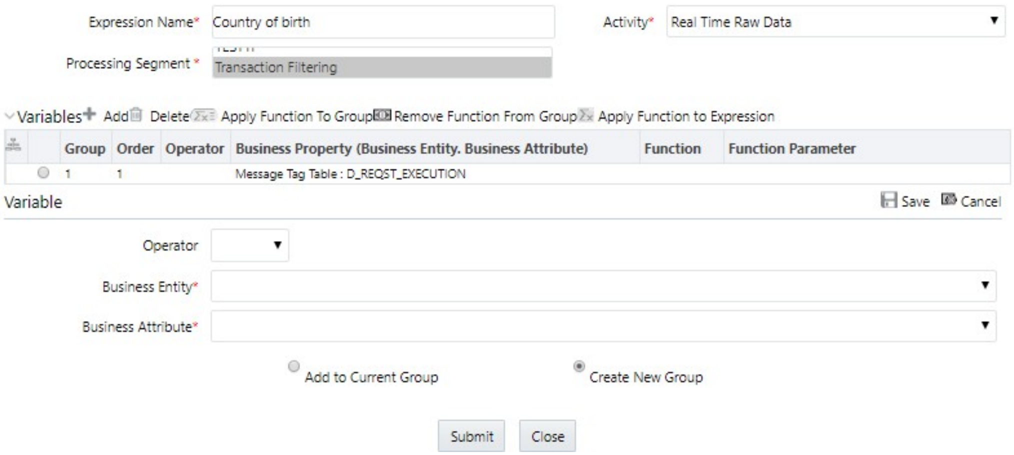
Business Attribute*: D_REQST_EXECUTION

○ Add to Current Group ● Create New Group

Submit Close

- Select the business entity and the business attribute where the value of the new parameter resides.
- Click the **Save icon**. The variable is displayed on the window.

Figure 11-13 First Expression Displayed



Expression Name*: Country of birth

Activity*: Real Time Raw Data

Processing Segment*: Transaction Filtering

Variables + Add Delete Apply Function To Group Remove Function From Group Apply Function to Expression

	Group	Order	Operator	Business Property (Business Entity. Business Attribute)	Function	Function Parameter
○	1	1		Message Tag Table : D_REQST_EXECUTION		

Variable — Save Cancel

Operator:

Business Entity*:

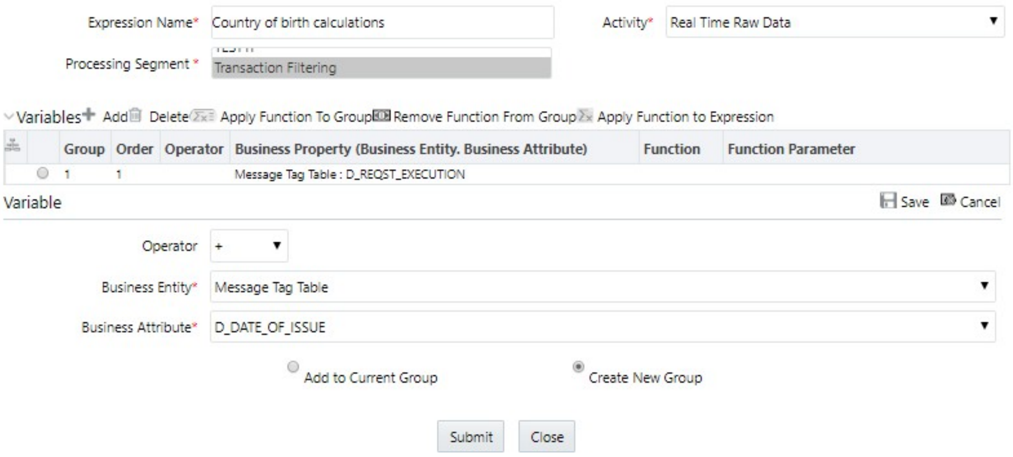
Business Attribute*:

○ Add to Current Group ● Create New Group

Submit Close

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

Figure 11-14 Second Expression Attributes



Expression Name* Country of birth calculations

Activity* Real Time Raw Data

Processing Segment * Transaction Filtering

	Group	Order	Operator	Business Property (Business Entity. Business Attribute)	Function	Function Parameter
○	1	1		Message Tag Table : D_REQST_EXECUTION		

Variable

Operator +

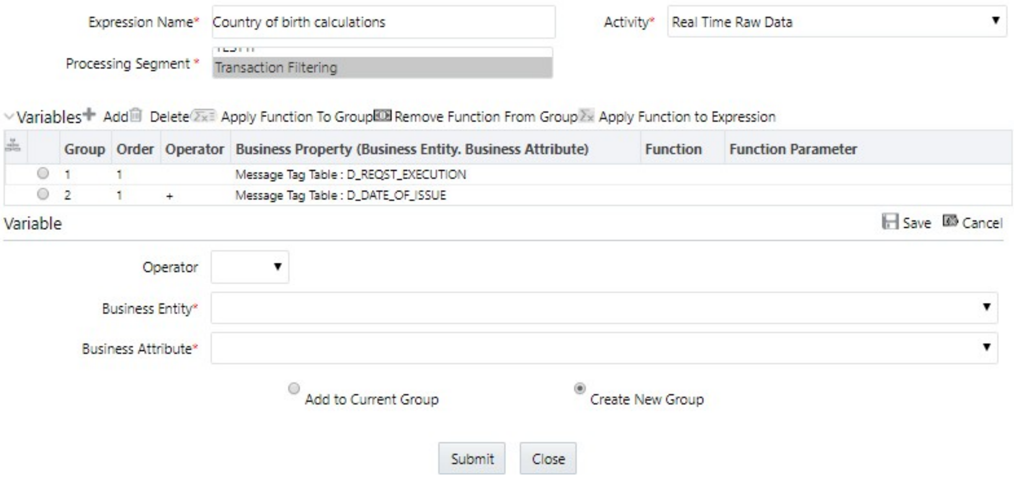
Business Entity* Message Tag Table

Business Attribute* D_DATE_OF_ISSUE

○ Add to Current Group ● Create New Group

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

Figure 11-15 Second Expression Displayed



Expression Name* Country of birth calculations

Activity* Real Time Raw Data

Processing Segment * Transaction Filtering

	Group	Order	Operator	Business Property (Business Entity. Business Attribute)	Function	Function Parameter
○	1	1		Message Tag Table : D_REQST_EXECUTION		
○	2	1	+	Message Tag Table : D_DATE_OF_ISSUE		

Variable

Operator

Business Entity*

Business Attribute*

○ Add to Current Group ● Create New Group

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.

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

3. 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.

   ISO20022 Risk-Currency VS Amount Threshold Evaluation
   For all filter 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 11-3 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'

Risk- High Risk Party Evaluation

Table 11-4 Risk- High-Risk Party Evaluation Filters

Sl.No	Filter Name	Filter Clause
1	Beneficiary Account Number	(Message Tag Table:V_BENF_ACC_NO) = (Rule Configu- ration 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'))

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 11-5 Risk-Currency VS Amount Threshold Evaluation Filters

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

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 11-6 Risk-Currency VS Destination Country Evaluation Filters

Sl.No	Filter Name	Filter Clause
1	Currency	(Message Tag Table:V_CURRENCY) = (Rule Configuration Table:V_COND1)
2	Destination Country	(Message Tag Table:V_DESTINATION_CNTRY) = (Rule Configu- ration Table:V_COND2)

Table 11-7 Risk-Currency VS Destination Country Evaluation Filters

Sl.No	Filter Name	Filter Clause
1	Direction	(Message Tag Table:V_DIRECTION) in ('INBOUND','OUTBOUND')
2	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) = (Rule Configuration Table:V_TXN_TYPE_CD)
3	Rule Name	(Rule Configuration Table:V_RISK_RULE_CODE) = 'TF_CCY_C- TRY_RSK'

Risk-High Risk Destination Country Evaluation

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

> **Note**
>
> This score is configurable.

Table 11-8 Risk-High Risk Destination Country Evaluation Filters

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

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 11-9 Risk-High Risk Originator Country Evaluation Filters

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

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 11-10 Risk-Trade Amendments Evaluation Filters

Sl.No	Filter Name	Filter Clause
1	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) = 'MT707'
2	Direction	(Message Tag Table:V_DIRECTION) in (('INBOUND','OUTBOUND'))
3	Number of Amendments	(Message Tag Table:N_NUMBER_OF_AMENDMENT)>= 5

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.

Watch List Score

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

> **Note**
>
> - This evaluation applies to the ISO message category.
> - This score is configurable.

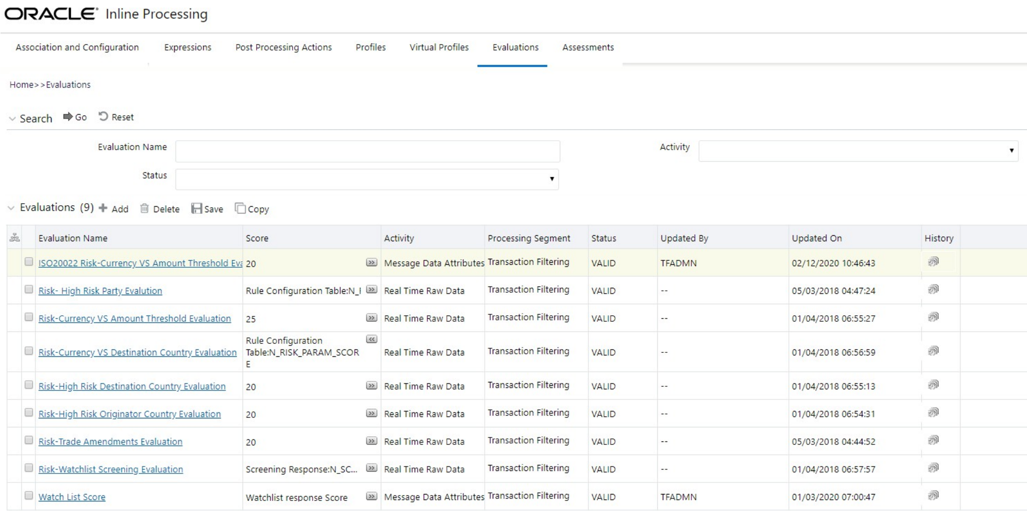
Table 11-11 Watch List Score Filters

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

To add an evaluation, follow these steps:

- Click the **Evaluations** menu.
- On the **Evaluations** page, click **Add**.

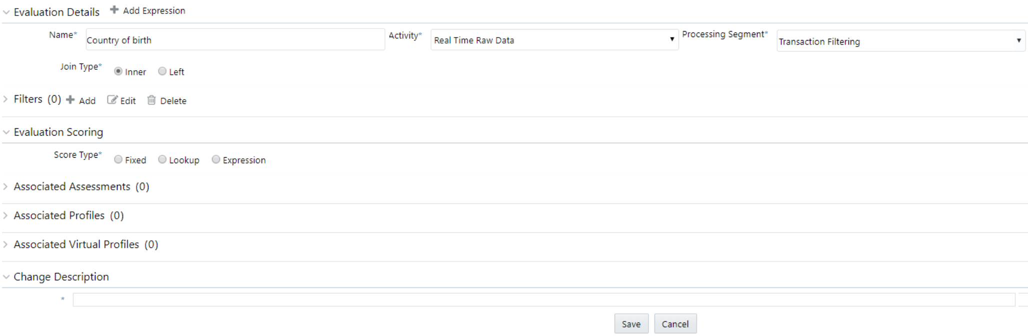
Figure 11-16 Evaluations Page



Evaluation Name	Score	Activity	Processing Segment	Status	Updated By	Updated On	History
ISO20022 Risk-Currency VS Amount Threshold Eva	20	Message Data Attributes	Transaction Filtering	VALID	TFADMN	02/12/2020 10:46:43	
Risk- High Risk Party Evalution	Rule Configuration Table:N_I	Real Time Raw Data	Transaction Filtering	VALID	--	05/03/2018 04:47:24	
Risk-Currency VS Amount Threshold Evaluation	25	Real Time Raw Data	Transaction Filtering	VALID	--	01/04/2018 06:55:27	
Risk-Currency VS Destination Country Evaluation	Rule Configuration Table:N_RISK_PARAM_SCORE	Real Time Raw Data	Transaction Filtering	VALID	--	01/04/2018 06:56:59	
Risk-High Risk Destination Country Evaluation	20	Real Time Raw Data	Transaction Filtering	VALID	--	01/04/2018 06:55:13	
Risk-High Risk Originator Country Evaluation	20	Real Time Raw Data	Transaction Filtering	VALID	--	01/04/2018 06:54:31	
Risk-Trade Amendments Evaluation	20	Real Time Raw Data	Transaction Filtering	VALID	--	05/03/2018 04:44:52	
Risk-Watchlist Screening Evaluation	Screening Response:N_SC...	Real Time Raw Data	Transaction Filtering	VALID	--	01/04/2018 06:57:57	
Watch List Score	Watchlist response Score	Message Data Attributes	Transaction Filtering	VALID	TFADMN	01/03/2020 07:00:47	

- Enter a name for the evaluation.
- Select an activity for the evaluation and the **Transaction Filtering** processing segment.

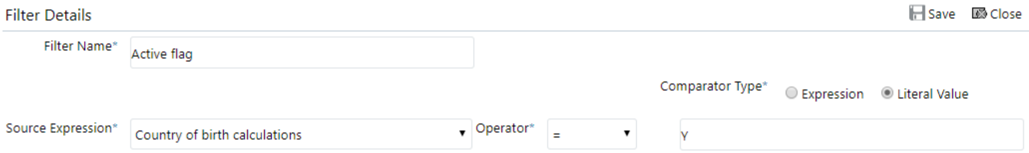
Figure 11-17 Evaluations Attributes



Name*: Country of birth
Activity*: Real Time Raw Data
Processing Segment*: Transaction Filtering
Join Type*: ● Inner ○ Left
Score Type*: ○ Fixed ○ Lookup ○ Expression

- To add a filter for the evaluation, click **Add**.
- Select the expression as mentioned in step f.

Figure 11-18 Evaluations Filters



Filter Details

Filter Name*: Active flag

Comparator Type*: ○ Expression ● Literal Value

Source Expression*: Country of birth calculations

Operator*: =

Y

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

4. 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.

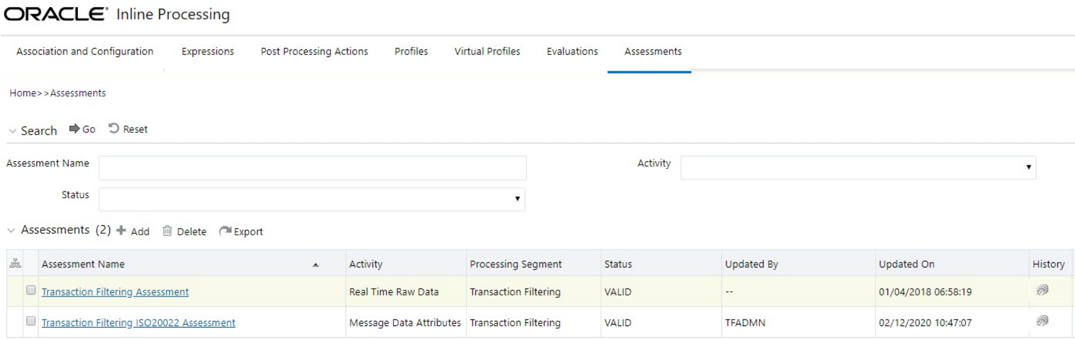
The risk score is calculated at the assessment level is as follows:

- 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:

- Click the **Assessments** menu.

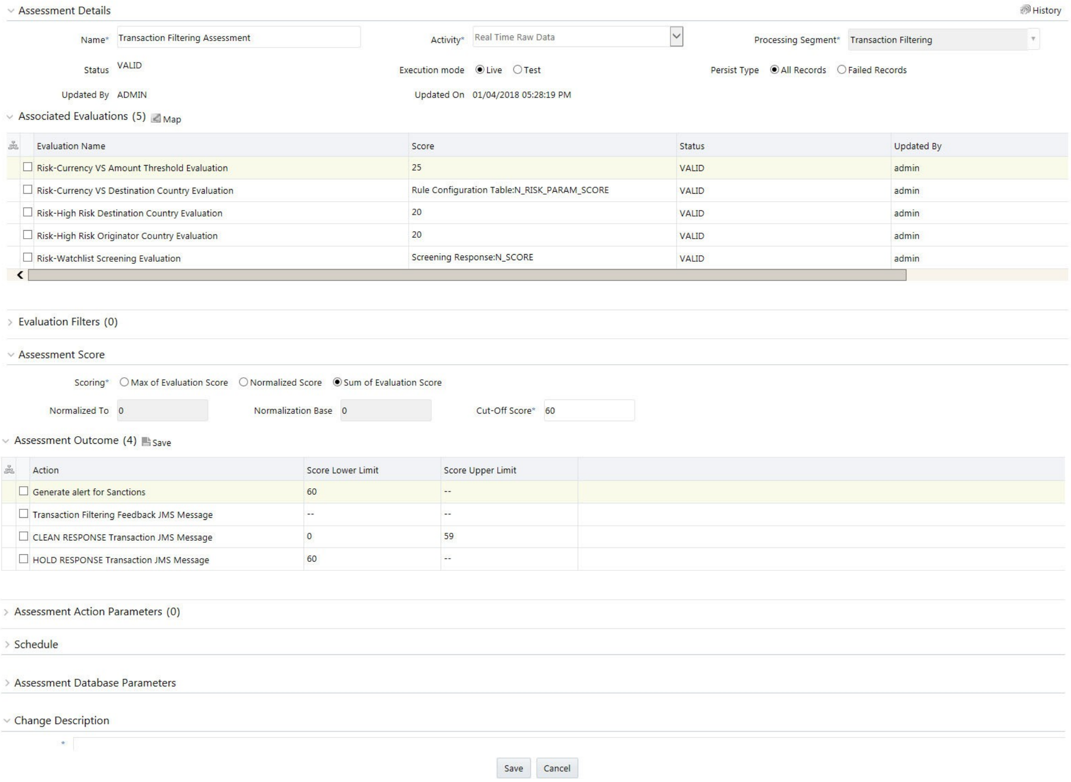
Figure 11-19 Assessments Page



	Assessment Name	Activity	Processing Segment	Status	Updated By	Updated On	History
□	Transaction Filtering Assessment	Real Time Raw Data	Transaction Filtering	VALID	--	01/04/2018 06:58:19	
□	Transaction Filtering ISO20022 Assessment	Message Data Attributes	Transaction Filtering	VALID	TFADMN	02/12/2020 10:47:07	

- On the **Assessments** page, click **Add**. The following image shows the evaluations for the **Transaction Filtering** Assessment:

Figure 11-20 Assessments Attributes



Assessment Details

Name* Transaction Filtering Assessment

Activity* Real Time Raw Data

Processing Segment* Transaction Filtering

Status VALID

Execution mode ● Live ○ Test

Persist Type ● All Records ○ Failed Records

Updated By ADMIN

Updated On 01/04/2018 05:28:19 PM

Associated Evaluations (5)

	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	admin
□	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)

	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

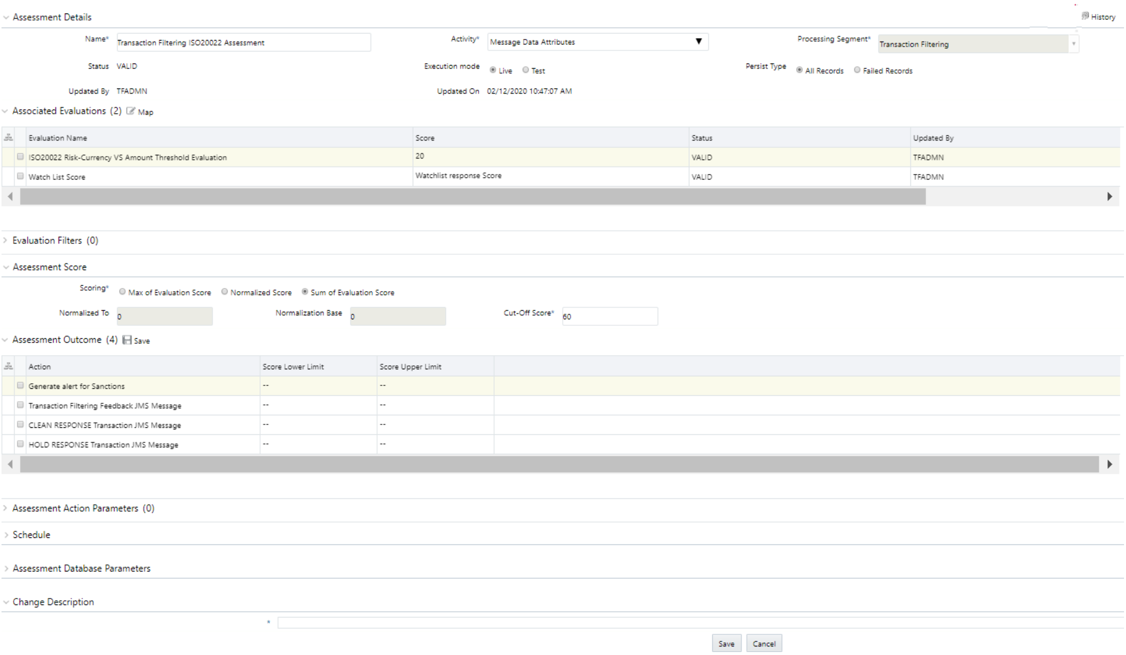
Assessment Database Parameters

Change Description

*

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

Figure 11-21 Sample Assessment



Assessment Details

Name* Transaction Filtering ISO20022 Assessment

Activity* Message Data Attributes

Processing Segment* Transaction Filtering

Status VALID

Execution mode ● Live ○ Test

Persist Type ● All Records ○ Failed Records

Updated By TFADMN

Updated On 02/12/2020 10:47:07 AM

Associated Evaluations (2)

	Evaluation Name	Score	Status	Updated By
□	ISO20022 Risk-Currency VS Amount Threshold Evaluation	20	VALID	TFADMN
□	Watch List Score	Watchlist response Score	VALID	TFADMN

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)

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

Assessment Action Parameters (0)

Schedule

Assessment Database Parameters

Change Description

*

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

12
Simulation

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

To view the changes in the simulation data for a deeper analysis, you can use the data extraction feature. You can run multiple simulations and compare the results using data extraction.

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

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

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

12.1 TF Process Flow

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

Figure 12-1 Simulation Process Flow

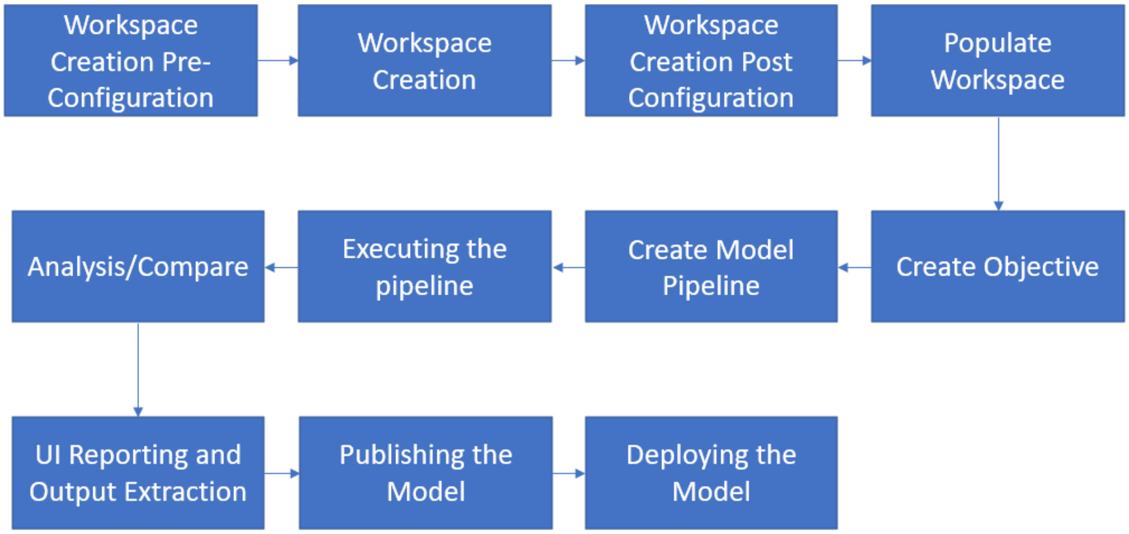
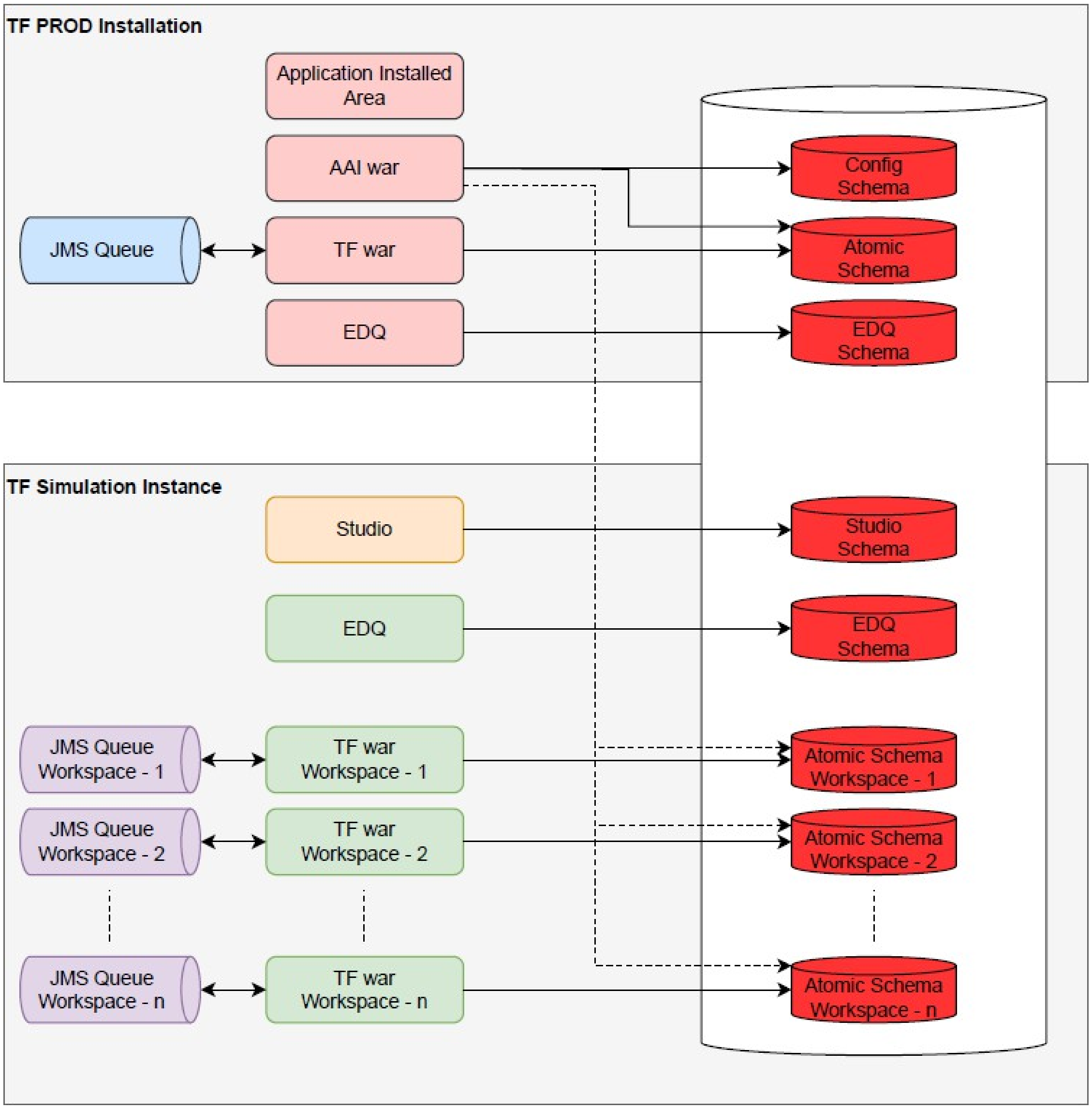


Figure 12-2 TF Data Flow



12.2 Integrating With Compliance Studio

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

Topics:

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

- Workspace Creation
- Workspace Creation Post-Configuration

12.2.1 Workspace Creation Pre-Requisite

Following are the pre-requisites for workspace creation:

1. Create User tablespace in simulation database by executing below script as sysdba user:
   ```
   CREATE TABLESPACE AIF_USER_TS DATAFILE '<DATAFILE PATH>/
   aif_user_data_tablespace.dbf' SIZE 1G REUSE AUTOEXTEND ON NEXT 500M MAXSIZE
   UNLIMITED;
   ```
   DATAFILE PATH example: `/scratch/oraofss/app/oradata`
2. Perform the Zippelin Interpreter Configuration in Compliance Studio UI. See Appendix L: Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMIT in Python Interpreter.
3. Create Instance Token for Production and Simulation in Sanctions Application. See Appendix J: Configurations for the Bearer Token.

12.2.2 Workspace Creation Pre-Configuration

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

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

12.2.2.1 Create Database Schema for the new workspace

Follow the subsequent steps to configuring new Database schema:

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

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

```
sys.dba_tables to <NEW SCHEMA>; grant select on sys.Dba_tab_columns to
<NEW SCHEMA>; grant create RULE to <NEW SCHEMA>;
 grant create any trigger to <NEW SCHEMA>; grant drop any trigger to <NEW
SCHEMA>;
 grant select on SYS.DBA_RECYCLEBIN to <NEW SCHEMA>;
 grant execute on <SIM CONFIG SCHEMA>.checkenvfordataredaction to
 <NEW SCHEMA>;
 --Sandbox specially
 grant connect, resource, dba to <NEW SCHEMA>;
```

2. Run the Below script once the user is created:

```
CREATE OR REPLACE SYNONYM <NEW SCHEMA>.checkenvfordataredaction FOR <SIM
CONFIG SCHEMA>.checkenvfordataredaction;
CREATE OR REPLACE SYNONYM <NEW SCHEMA>.cssms_role_mast FOR <SIM CONFIG
SCHEMA>.cssms_role_mast;
CREATE OR REPLACE SYNONYM <NEW SCHEMA>.cssms_group_role_map FOR <SIM
CONFIG SCHEMA>.cssms_group_role_map;
CREATE OR REPLACE SYNONYM <NEW SCHEMA>.cssms_usr_group_map_view FOR <SIM
CONFIG SCHEMA>.cssms_usr_group_map_view;
CREATE OR REPLACE SYNONYM <NEW SCHEMA>.cssms_group_role_map FOR <SIM
CONFIG SCHEMA>.cssms_group_role_map;
CREATE OR REPLACE SYNONYM <NEW SCHEMA>.cssms_usr_profile FOR <SIM CONFIG
SCHEMA>.cssms_usr_profile;
CREATE OR REPLACE SYNONYM <NEW SCHEMA>.cssms_usr_group_map FOR <SIM CONFIG
SCHEMA>.cssms_usr_group_map;
CREATE OR REPLACE SYNONYM <NEW SCHEMA>.Cssms_Role_Function_Map FOR <SIM
CONFIG SCHEMA>.Cssms_Role_Function_Map;
```

12.2.2.2 Add the schema to wallet in the Compliance Studio Setup

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

1. Add the database schema credentials in the wallet using the following command:
   `mkstore -wrl <WALLET LOCATION> -createCredential <NEW SCHEMA>_alias <NEW SCHEMA>`
2. After you run the command, a prompt is displayed. Enter the password `<NEW SCHEMA PASSWORD>` associated with the database user account in the prompt. You are the prompted to re-enter the password and the wallet password that you entered during wallet creation.
3. Update the `tnsnames.ora` file to include the following entry.
   `<NEW SCHEMA>_alias = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL= TCP) (HOST = <<IP ADDRESS>)(PORT = <<PORT NUMBER>>)) ) (CONNECT_DATA = (SERVICE_NAME = <<SERVICE NAME>) ) )`
4. Repeat the above steps for Production Database Schema if not added.

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

12.2.2.3 Add the infodom in Weblogic Console

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

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

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

12.2.2.4 Configure the infodom in tnsnames.ora in Simulation Sanctions Setup

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

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

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

12.2.2.5 Display the OFSAA Environment Menu in Compliance Studio UI

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

1. Click the **User** Icon right top corner.
2. Click **Identity Management.** The Identity Management window is displayed.
   For more information on Identity Management, see OFS Admin Console User Guide.
3. Click **Groups**. The Groups window is displayed.
4. Select **Workspace Administrator** from the list to display the Group Details page.
5. Select **Mapped Roles** tab. The Mapped Roles window is displayed.
6. Click **New Mapping**. The Unmapped Roles window is displayed.
7. Click **Authorization View.**

8. Search for OFSAA Environment Menu Access, and select **OFSAA Environment Menu Access**.
9. Click Authorize to display **OFSAA Environment** in the UI.

12.2.2.6 Registering the OFSAA Environment Details

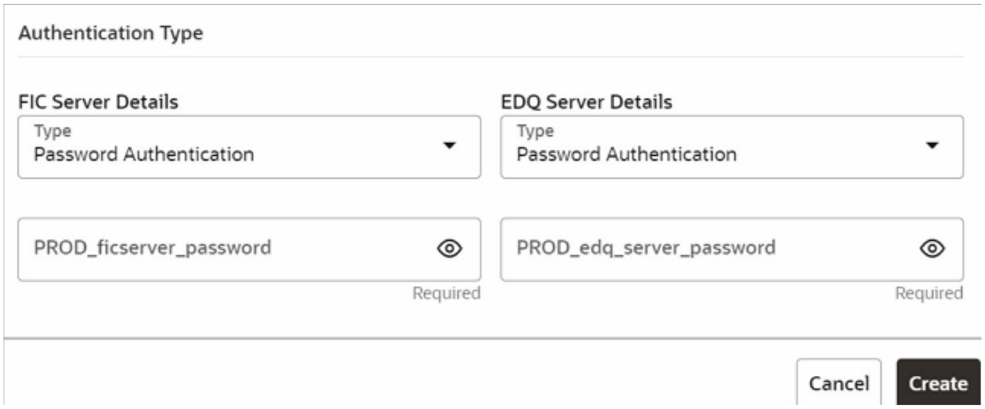
To Register the OFSAA Environment details, follow the subsequent steps:

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

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

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

Figure 12-3 Password Authentication



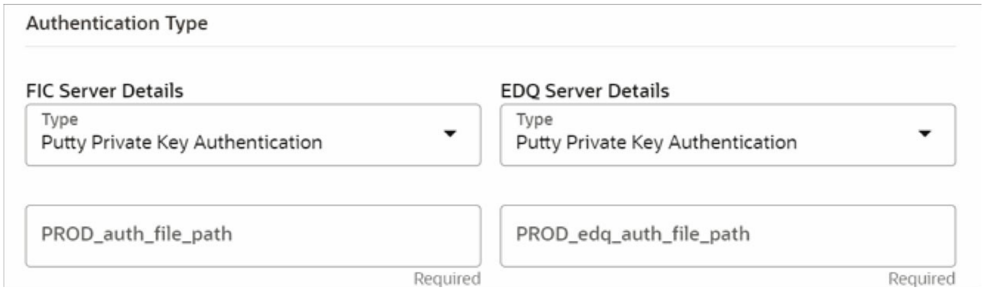
Authentication Type

FIC Server Details
Type: Password Authentication
PROD_ficserver_password
Required

EDQ Server Details
Type: Password Authentication
PROD_edq_server_password
Required

     b. Putty Private Key Authentication

Figure 12-4 Putty Private Key Authentication



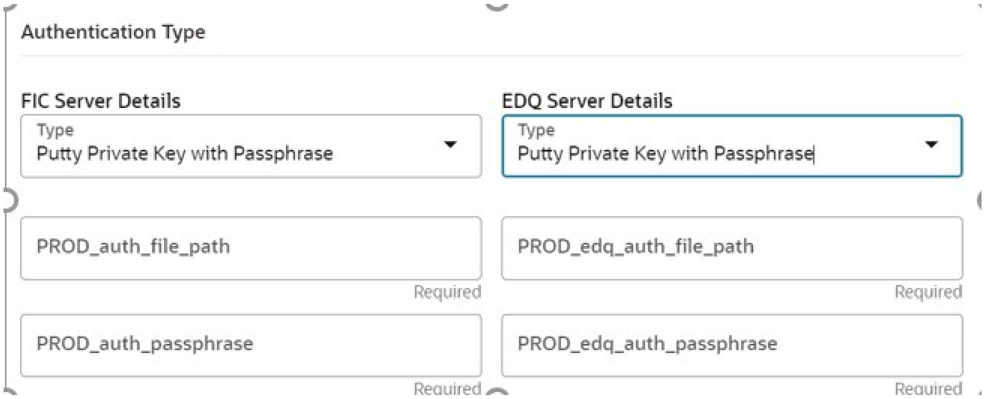
Authentication Type

FIC Server Details
Type: Putty Private Key Authentication
PROD_auth_file_path (Required)

EDQ Server Details
Type: Putty Private Key Authentication
PROD_edq_auth_file_path (Required)

c. Putty Private Key with Passphrase Authentication

Figure 12-5 Putty Private Key with Passphrase Authentication



Authentication Type

FIC Server Details
Type: Putty Private Key with Passphrase
PROD_auth_file_path (Required)
PROD_auth_passphrase (Required)

EDQ Server Details
Type: Putty Private Key with Passphrase
PROD_edq_auth_file_path (Required)
PROD_edq_auth_passphrase (Required)

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

5. Click **Create**.

The following table provides information about Key and Values for OFSAA Environment Registration.

Table 12-1 OFSAA Production Environment Key and Values

Key	Description
PROD_baseUrl	Sanctions application base URL. (Example: http://host name>:<port>/<context- name>)
PROD_app_id	Application ID (Example: OFS_TFLT)
PROD_infodom	infodom ID (Example: SANC812INFO)
PROD_ficserver_hostname	Server IP address where ftpshare is located
PROD_ficserver_username	ficserver user name
PROD_ficserver_password	ficserver password
PROD_ftpshare_path	ftpshare path (Example: /scratch/sanc812/sanc/ftpshare)

Table 12-1 (Cont.) OFSAA Production Environment Key and Values

Key	Description
PROD_edq_server_hostname	EDQ server host name
PROD_edq_server_username	EDQ server user name
PROD_edq_server_password	EDQ server password
PROD_edq_runprofiles_path	EDQ run profiles path (Example: /scratch/ ofsaaapp/EDQ/Middleware/Oracle_Home/ user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/runprofiles/)
PROD_edq_autorun_directory	EDQ Autorun directory (Example: /scratch/ ofsaaapp/EDQ/Middleware/Oracle_Home/ user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/autorun/)
PROD_edq_exportproject_directory	EDQ export project directory (Example: /scratch/ ofsaaapp/test/TFSIM/Export/)
PROD_edq_jshell_jar_directory	EDQ jshell and jar directory (Example: /scratch/ ofsaaapp/EDQ/Middleware/Oracle_Home/edq/ oracle.edq/)
PROD_edq_management_port	EDQ management port ID
PROD_edq_director_username	EDQ director user name
PROD_edq_director_password	EDQ director password
PROD_edq_landingarea_path	EDQ landing area path (Example: /scratch/ ofsaaapp/EDQ/Middleware/Oracle_Home/ user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/landingarea/)
PROD_edq_project_name	EDQ project name (Example: Transaction _Filter- ing)
PROD_instanceName	Instance name (Example: SIMULATION)
PROD_instanceAccessToken	Instance access token ID
PROD_edq_baseUrl	EDQ base URL (Example: http://host name>:<port>)
PROD_auth_file_path	FIC Server Private Key File Path (Refer section 12.2.2.8)
PROD_local_auth_file_path	Production Web Server Private Key File Path (Refer section 12.2.2.8)
PROD_edq_auth_file_path	EDQ Server Private Key File Path (Refer section 12.2.2.8)
PROD_auth_passphrase	Password for FIC Server Private Key File
PROD_edq_auth_passphrase	Password for EDQ Server Private Key File
SIM_base Url	Sanction application Base URL (Example: http:// host name>:<port>/<context-name>)
SIM_ficserver_hostname	Server ip address where ftpshare is located
SIM_ficserver_username	ficserver user name
SIM_ficserver_password	ficserver password
SIM_ftpshare_path	ftpshare path (Example: /scratch/tf812dev/ san_812/ ftpshare)
SIM_edq_server_hostname	EDQ server host name
SIM_edq_server_username	EDQ server user name
SIM_edq_server_password	EDQ server password

Table 12-1 (Cont.) OFSAA Production Environment Key and Values

Key	Description
SIM_edq_autorun_directory	EDQ autorun directory (Example: /scratch/ ofsaaapp/EDQ/Middleware/Oracle_Home/ user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/autorun/)
SIM_edq_importproject_directory	EDQ import project directory (Example: /scratch/ ofsaaapp/test/TFSIM/Import/)
SIM_edq_jshell_jar_directory	EDQ jshell and jar directory (Example: /scratch/ ofsaaapp/EDQ/Middleware/Oracle_Home/edq/ oracle.edq/)
SIM_edq_management_port	EDQ management port
SIM_edq_director_username	EDQ director username
SIM_edq_director_password	EDQ director_password
SIM_edq_landingarea_path	EDQ landingarea_path (Example: /scratch/ ofsaaapp/ Oracle/Middleware/Oracle_Home/ user_projects/ domains/base_domain/config/ fmwconfig/edq/ oedq.local.home/landingarea/)
SIM_instanceAccessToken	Instance access token ID
SIM_instanceName	Instance Name
SIM_sys_admin_user	System admin user ID
SIM_sys_auth_user	System authentication user ID
SIM_edq_baseUrl	EDQ base URL (Example: http://host name>:<port>)
SIM_edq_runprofiles_path	EDQ run profiles path (Example: /scratch/ ofsaaapp/EDQ/Middleware/Oracle_Home/ user_projects/domains/base_domain/config/ fmwconfig/edq/oedq.local.home/runprofiles/)
SIM_t3_url	T3 URL (Example: t3://host name>:<port>)
SIM_app_server	Type of web server (WEBLOGIC/WEBSPHERE)
SIM_web_server_username	Web server user name
SIM_web_server_password	Web server password
SIM_auth_file_path	FIC Server Private Key File Path (Refer section 12.2.2.8)
SIM_edq_auth_file_path	EDQ Server Private Key File Path (Refer section 12.2.2.8)
SIM_auth_passphrase	Password for FIC Server Private Key File
SIM_edq_auth_passphrase	Password for EDQ Server Private Key File

12.2.2.7 Procedure to Create PPK File

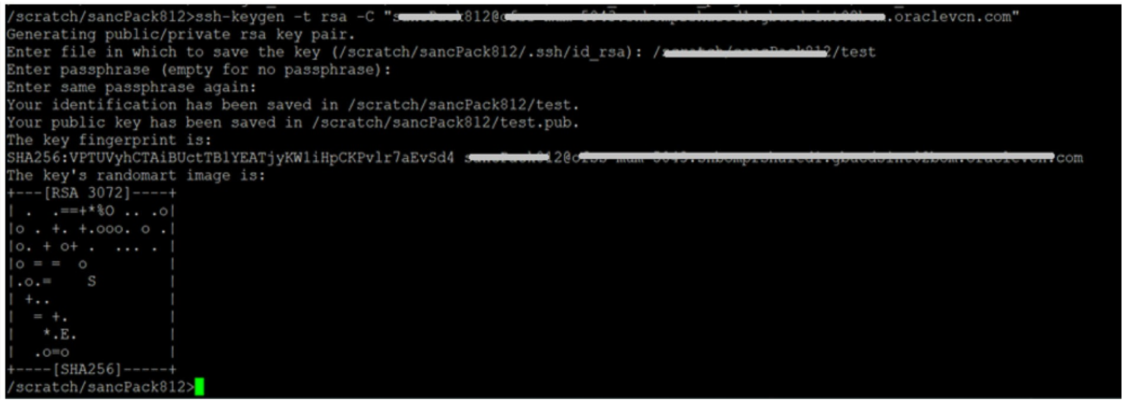
Open the putty session and run the below command:

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

Replace username & hostname with respective server details.

For reference, see below screenshot:

Figure 12-6 Procedure to Create PPK File



```
/scratch/sancPack812>ssh-keygen -t rsa -C "s[redacted]812@[redacted].oraclevcn.com"
Generating public/private rsa key pair.
Enter file in which to save the key (/scratch/sancPack812/.ssh/id_rsa): /[redacted]/test
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /scratch/sancPack812/test.
Your public key has been saved in /scratch/sancPack812/test.pub.
The key fingerprint is:
SHA256:VPTUVyhCTAiBUctTB1YEATjyKW1iHpCKPvlr7aEvSd4 [redacted]2@[redacted]com
The key's randomart image is:
+---[RSA 3072]----+
| .  .==+*%O .. .o|
|o . +. +.ooo. o .|
|o. + o+ .  ... . |
|o = =  o         |
|.o.=    S        |
| +..             |
|  = +.           |
|   *.E.          |
|  .o=o           |
+----[SHA256]-----+
/scratch/sancPack812>
```

12.2.2.8 Different ways of PPK File Registration

1. Once the PPK file is generated it will create both private Key and public Key.
2. Create a file with name **authorized_keys**. Permission should be 644.
3. Place the public key inside authorized keys file present in ssh folder. Now verify once connecting to winscp using the Private Key file.
   In OFSAA Registration we can either give in any one of the following ways:

   Method 1:

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

   Method 2:

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

> **Note**
>
> Ensure that PPK Files are generated in Production FIC, Web servers, Simulation FIC, Web servers, EDQ servers and Public Keys of all the above servers are shared across in **authorized_keys** in all servers.

12.2.2.9 Configuring the Data Source

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

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

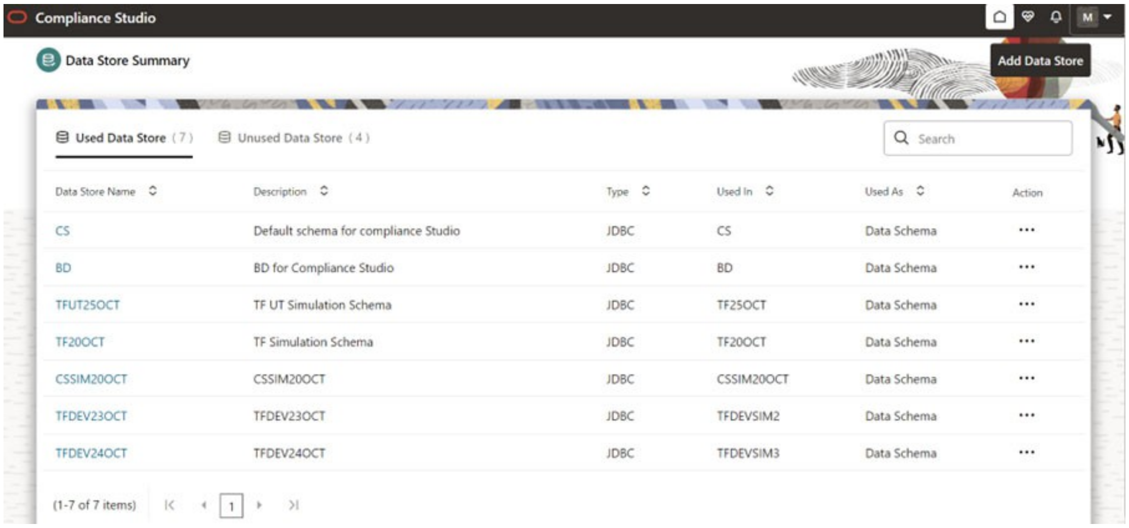
After Pre-configuration procedures you must add new data source in the compliance studio application.

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

Follow the subsequent steps to add the new data source:

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

Figure 12-7 Data Source Summary Page



Data Store Name	Description	Type	Used In	Used As	Action
CS	Default schema for compliance Studio	JDBC	CS	Data Schema	•••
BD	BD for Compliance Studio	JDBC	BD	Data Schema	•••
TFUT25OCT	TF UT Simulation Schema	JDBC	TF25OCT	Data Schema	•••
TF20OCT	TF Simulation Schema	JDBC	TF20OCT	Data Schema	•••
CSSIM20OCT	CSSIM20OCT	JDBC	CSSIM20OCT	Data Schema	•••
TFDEV23OCT	TFDEV23OCT	JDBC	TFDEVSIM2	Data Schema	•••
TFDEV24OCT	TFDEV24OCT	JDBC	TFDEVSIM3	Data Schema	•••

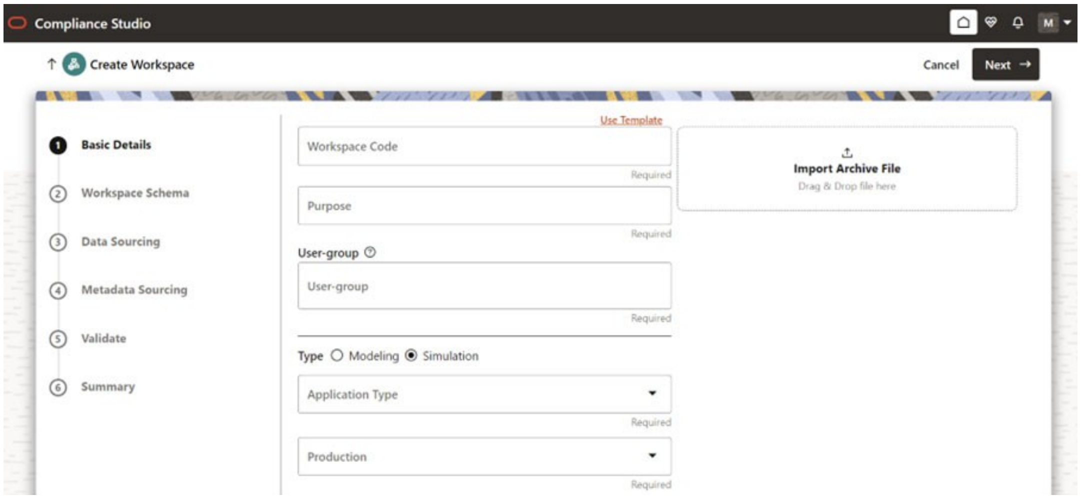
(1-7 of 7 items) 1

12.2.3 Workspace Creation

The Workspace creation requires entry of the source of dataset, validation, and deployment. To create a Workspace, follow the subsequent steps:

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

Figure 12-8 Create Workspace



Workspace Code
Required

Purpose
Required

User-group
User-group
Required

Type ○ Modeling ● Simulation

Application Type
Required

Production
Required

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

Use the pre-configured template to load the data base and metadata objects to the workspace. To use the pre-configured template, follow the subsequent steps:

1. Click **Use template**. Use template pop up window is displayed.
2. Select TFWorkspaceTemplate.zip from the library drop-down. The Update schema mapping is displayed.
3. Select the following target schema field details:
   - New Data Schema: Enter/select the newly created schema ID.
   - New Data Source Name: Enter/select the production data source name.
4. Click **Update** to load the pre-configured template. Click **Cancel** to close the window.

The following steps show the various phases from workspace creation to deployment:

1. Configuring Basic Details
2. Configuring Workspace Schema
3. Configuring Data Sourcing
4. Configuring Metadata Sourcing
5. Validating Workspace
6. Displaying Summary

12.2.3.1 Configuring Basic Details

To configure the basic details follow the subsequent steps:

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

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

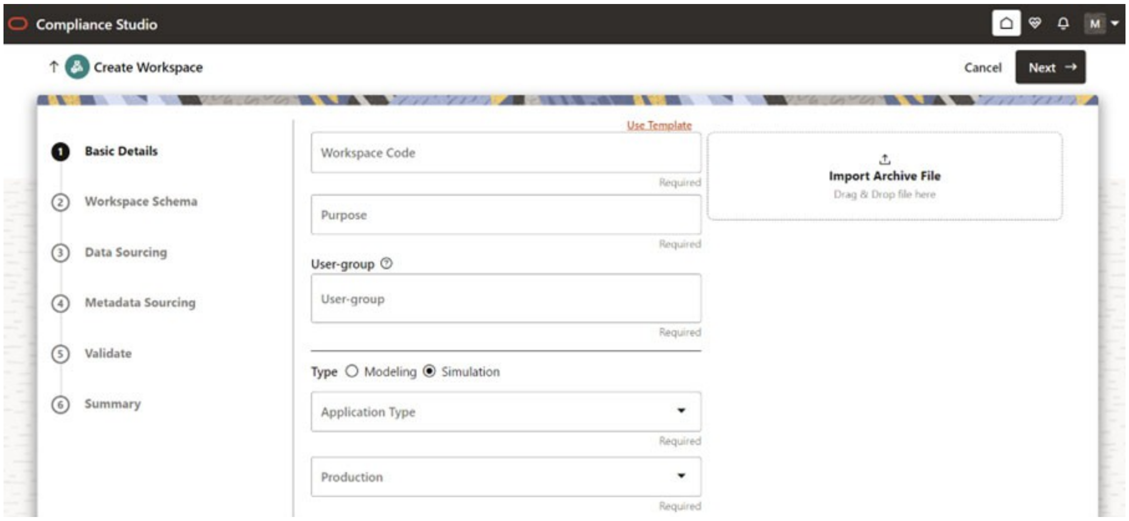
Table 12-2 Basic Details Fields Details

Fields	Description
Workspace Code	Enter the code of the workspace. This field is lim- ited to 20 characters.
Purpose	Enter the purpose of the creation of the Workspace.
User group	Click on this field to display a list of User-group values. Select the required value. • Modeling Approver • Modeling Reviewer • Modeling User
Type	Select the type of Workspace as Modeling or Simulation.
SubType	If you have selected Modeling, select the subtype of Workspace as Sandbox Workspace or Production Workspace.

Table 12-2 (Cont.) Basic Details Fields Details

Fields	Description
Application Type	Select Transaction Filtering
Production	The TF Production drop down value will be popu- lated as a result of registering the OFSAA Environ- ment Details.
Simulation	The TF Simulation drop down value will be popu- lated as a result of registering the OFSAA Environ- ment Details.
Simulation Infodom	Enter Infodom name (<<Simulation Infodom>>).
Simulation User Group Code	Enter the User Group Code. This field is lim-ited to 20 characters.
Simulation User ID	Enter the User ID. This field is lim-ited to 20 char- acters.
Simulation User Password	Enter the User Password.
Simulation DB Server	Enter the DB IP address.
Simulation DB Schema name	Enter simulation Schema name (<NEW SCHEMA>).
Simulation DB Password	Enter the password (<NEW SCHEMA PASS- WORD>).
Simulation Jdbc Connection String	Enter the connection Sting (Example: jdbc:ora-cle:thin:@100.76.133.237:1521/fccmdb).
Simulation Message Posting Queue Name	Enter the simulation message posting queue name (Example: sourceEntityQueue)
Simulation TF Domain	Enter the TF domain name (Example: SF)

Figure 12-9 Basic Details Window



Type ○ Modeling ● Simulation

12.2.3.2 Configuring Workspace Schema

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

12.2.3.3 Configuring Data Sourcing

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

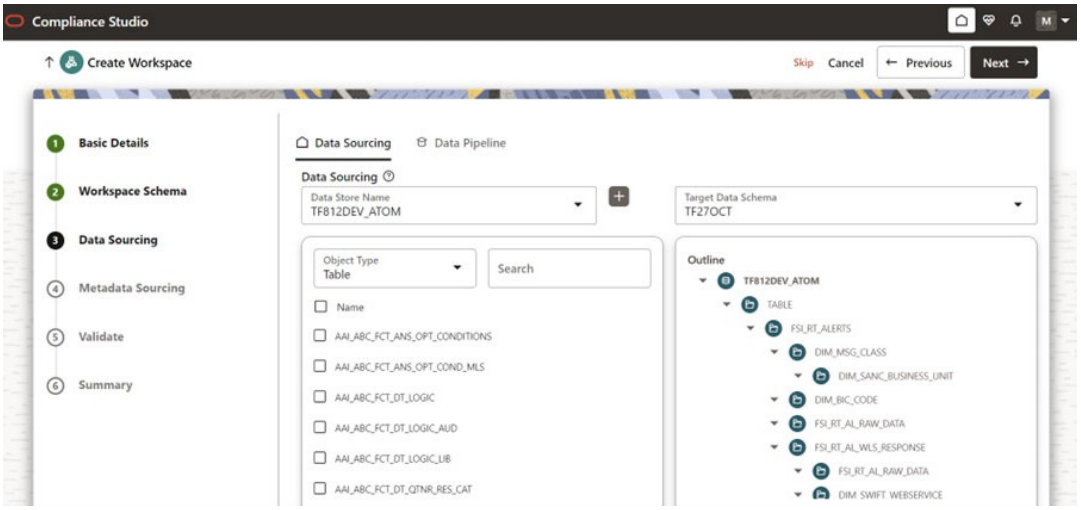
In case any of the selected tables are not present in the target schema, those tables are included in the failed objects count in the workspace provisioning summary.

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

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

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

Figure 12-10 Data Sourcing



Data Store Name
TF812DEV_ATOM

Target Data Schema
TF27OCT

Object Type
Table

☐ Name
☐ AAI_ABC_FCT_ANS_OPT_CONDITIONS
☐ AAI_ABC_FCT_ANS_OPT_COND_MLS
☐ AAI_ABC_FCT_DT_LOGIC
☐ AAI_ABC_FCT_DT_LOGIC_AUD
☐ AAI_ABC_FCT_DT_LOGIC_LIB
☐ AAI_ABC_FCT_DT_QTNR_RES_CAT

12.2.3.4 Configuring Metadata Sourcing

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

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

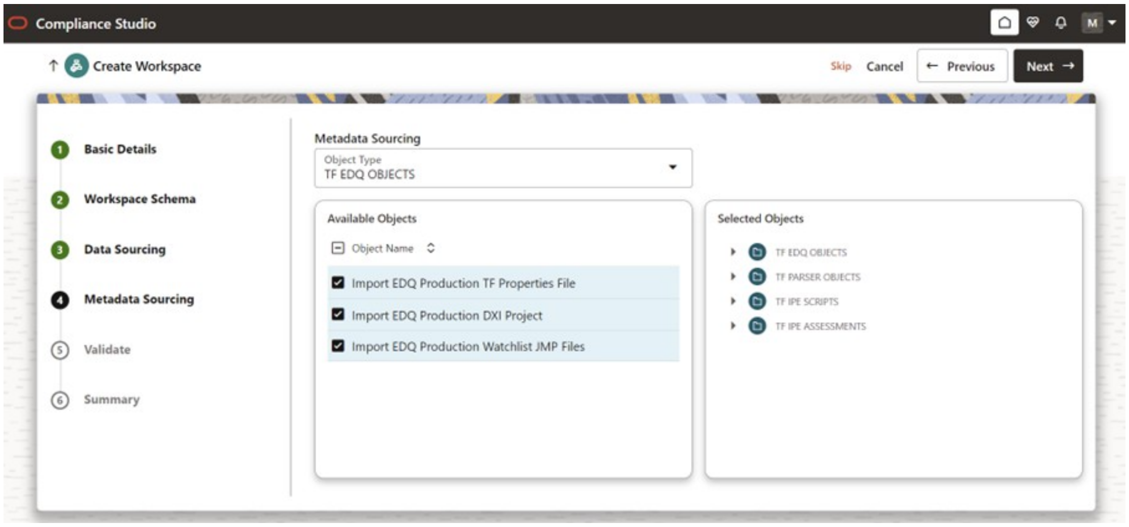
As a part of using the template, all the TF specific metadata sourcing objects are available by default. If you are not using the template, follow the Metadata Sourcing Object Type and Names table and select the metadata objects manually.

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

Table 12-3 Metadata Sourcing Object Type and Names

Object Type	Object Name
TF IPE ASSESSMENTS	Transaction Filtering Assessment
	ACH Transaction Filtering
	Auto Release Transaction Filtering
TF EDQ OBJECTS	IMPORT EDQ PRODUCTION DXI PROJECT
	IMPORT EDQ PRODUCTION WATCHLIST JMP FILES
	IMPORT EDQ PRODUCTION TF PROPERTIES FILE
TF IPE SCRIPTS	TF IPE Post Processing Actions
TF PARSER OBJECTS	Import SWIFT Parser

Figure 12-11 Metadata Sourcing



Metadata Sourcing

Object Type: TF EDQ OBJECTS

Available Objects

□ Object Name

☑ Import EDQ Production TF Properties File

☑ Import EDQ Production DXI Project

☑ Import EDQ Production Watchlist JMP Files

Selected Objects

- TF EDQ OBJECTS
- TF PARSER OBJECTS
- TF IPE SCRIPTS
- TF IPE ASSESSMENTS

12.2.3.5 Validating Workspace

The **Validate** pane displays a preview of the configuration values entered in the previous panes. Click

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

12.2.3.6 Displaying Summary

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

12.2.4 Workspace Creation Post-Configuration

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

1. Configuration in Sanctions Application
2. Update Files in TFLT WAR Associated with the Workspace

3. Importing Workspace Metadata for ML4AML for the created Workspace
4. Populate the Work Space
5. WebLogic console configuration

12.2.4.1 Configuration in Sanctions Application

Follow the subsequent steps to configure the Sanctions application:

1. Login to the Simulation Environment Sanctions Application as SYSADMN user.
2. Click Identity Management.
3. Click **User Group Role Map** from User Administrator.
4. Select the same **User Group Code** value created/entered during the workspace creation and click **Map**.
5. Grant the IPE Write role access to the workspace and click **Ok**.
6. Logout from the application.
7. Login to the Simulation Environment Sanctions Application as SYSAUTH user.
8. Click **Identity Management**. The Identity Management page is displayed.
9. Click **User Group Authorization**.
10. Select IPE Write from mapped roles and click **Authorize**.
11. Click **Ok** and logout from the application.
12. Login to the Simulation Environment Sanctions Application using the following credentials
    - User ID: Simulation User ID (Credential created while creating sandbox workspace)
    - Password: Simulation User Password (Credential created while creating sandbox workspace)
13. From the home page click **TF** tile.
14. Click **Common Frameworks** from the LHS.
15. Select **Inline Processing**. The Oracle Inline Processing window is displayed.
16. Click Post Processing Action tab.
17. Select **CLEAN RESPONSE Transaction JMS Message** from Post Processing Actions list.
18. Click **JNDI Provider URL** from Action Parameters list. The Action Parameters window is displayed.
19. Update the Action Parameter Value with Simulation Environment’s t3 URL value.
20. Click J**NDI Connection User Name** and **JNDI Connection Password** and provide the Simulation Environment's web server username and password.
21. Close the window.

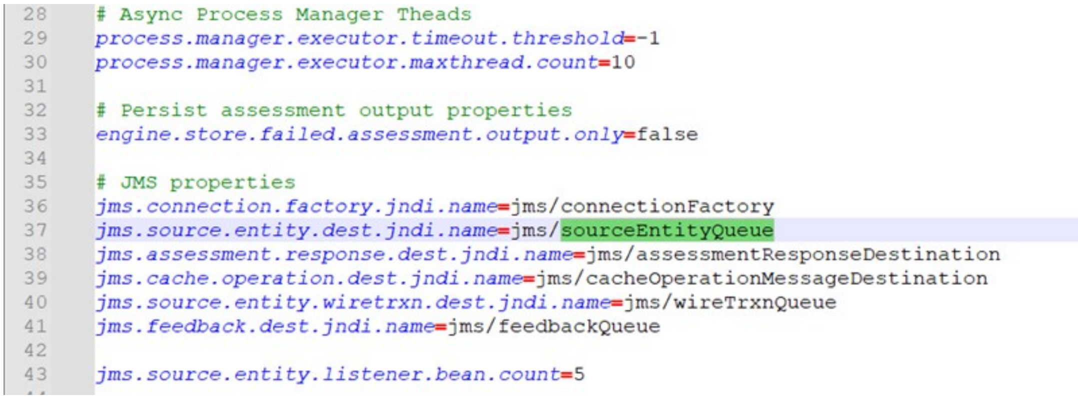
12.2.4.2 Update Files in TFLT WAR Associated with the Workspace

To update files in TFLT WAR, which is associated with the workspace follow the subsequent steps:

1. In the Simulation Environment, go to the following path:
   `TFLT.ear/TFLT.war/conf`

2. Open the `static.properties` file and make sure that the jms Queue name (jms.source.entity.dest.jndi.name) is same as the value (Simulation Message Posting Queue Name) given while creating sandbox workspace.

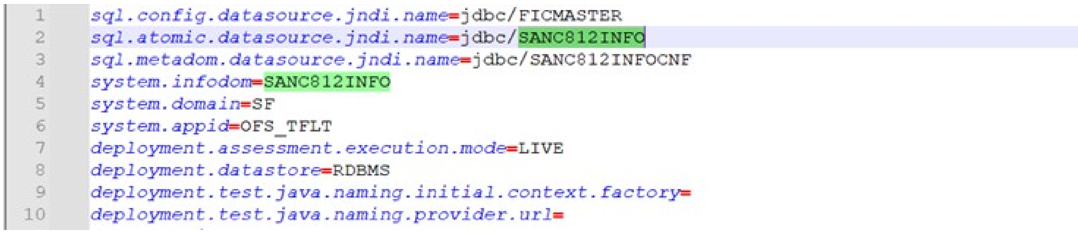
Figure 12-12 static.properties file



```
# Async Process Manager Theads
process.manager.executor.timeout.threshold=-1
process.manager.executor.maxthread.count=10

# Persist assessment output properties
engine.store.failed.assessment.output.only=false

# JMS properties
jms.connection.factory.jndi.name=jms/connectionFactory
jms.source.entity.dest.jndi.name=jms/sourceEntityQueue
jms.assessment.response.dest.jndi.name=jms/assessmentResponseDestination
jms.cache.operation.dest.jndi.name=jms/cacheOperationMessageDestination
jms.source.entity.wiretrxn.dest.jndi.name=jms/wireTrxnQueue
jms.feedback.dest.jndi.name=jms/feedbackQueue

jms.source.entity.listener.bean.count=5
```

3. Open the `install.properties` file and update the `sql.atomic.datasource.jndi.name` and `system.infodom` with Sandbox workspace's infodom (<<`Simulation Infodom`>>).

Figure 12-13 install.properties file

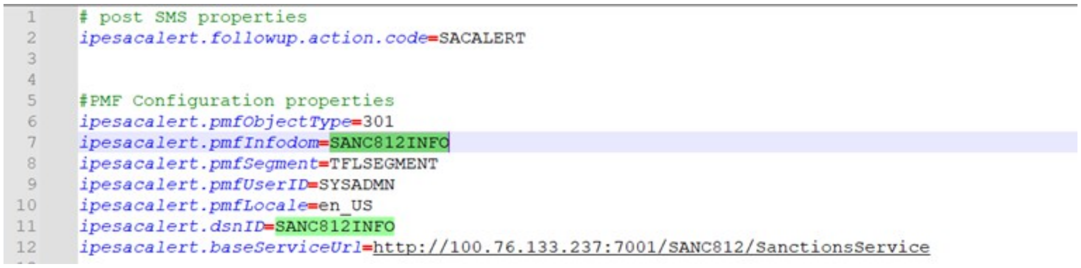


```
sql.config.datasource.jndi.name=jdbc/FICMASTER
sql.atomic.datasource.jndi.name=jdbc/SANC812INFO
sql.metadom.datasource.jndi.name=jdbc/SANC812INFOCNF
system.infodom=SANC812INFO
system.domain=SF
system.appid=OFS_TFLT
deployment.assessment.execution.mode=LIVE
deployment.datastore=RDBMS
deployment.test.java.naming.initial.context.factory=
deployment.test.java.naming.provider.url=
```

4. Go to `ext` folder.

5. Open `spring-postSacalert.properties` file and update the `ipesacalert.pmfInfodom` and `ipesacalert.dsnID` with Sandbox workspace's infodom.

Figure 12-14 spring-postSacalert.properties file



```
# post SMS properties
ipesacalert.followup.action.code=SACALERT


#PMF Configuration properties
ipesacalert.pmfObjectType=301
ipesacalert.pmfInfodom=SANC812INFO
ipesacalert.pmfSegment=TFLSEGMENT
ipesacalert.pmfUserID=SYSADMN
ipesacalert.pmfLocale=en_US
ipesacalert.dsnID=SANC812INFO
ipesacalert.baseServiceUrl=http://100.76.133.237:7001/SANC812/SanctionsService
```

12.2.4.3 Importing Workspace Metadata for ML4AML for the created Workspace

1. Login to Compliance Studio installed UNIX Machine.

2. Navigate to the following path:
   `/deployed/ml4aml/bin`

3. Execute the following UNIX command once, against the schema used in the current Sandbox workspace: `./importWorkspaceSQL.sh -w <NEW_SCHEMA>_alias`

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

12.2.4.4 Populate the Work Space

Populate Workspace for the respected sandbox workspace. See Populating the Workspace for work space population.

12.2.4.5 WebLogic console configuration

To configure the Simulation Sanction Weblogic console, follow the subsequent steps:

1. Login to the Simulation Sanction Weblogic Server.
2. Go to Deployments.
3. Update the Sanctions application war and corresponding TFLT war that are configured in Update Files in TFLT WAR Associated with the Workspace section.

12.3 Managing a Workspace

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

- Launching a Workspace
- Viewing the Workspace
- Editing the Workspace
- Deleting the Workspace
- Downloading the Workspace

12.4 Populating the Workspace

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

To populate the Workspace, follow these steps:

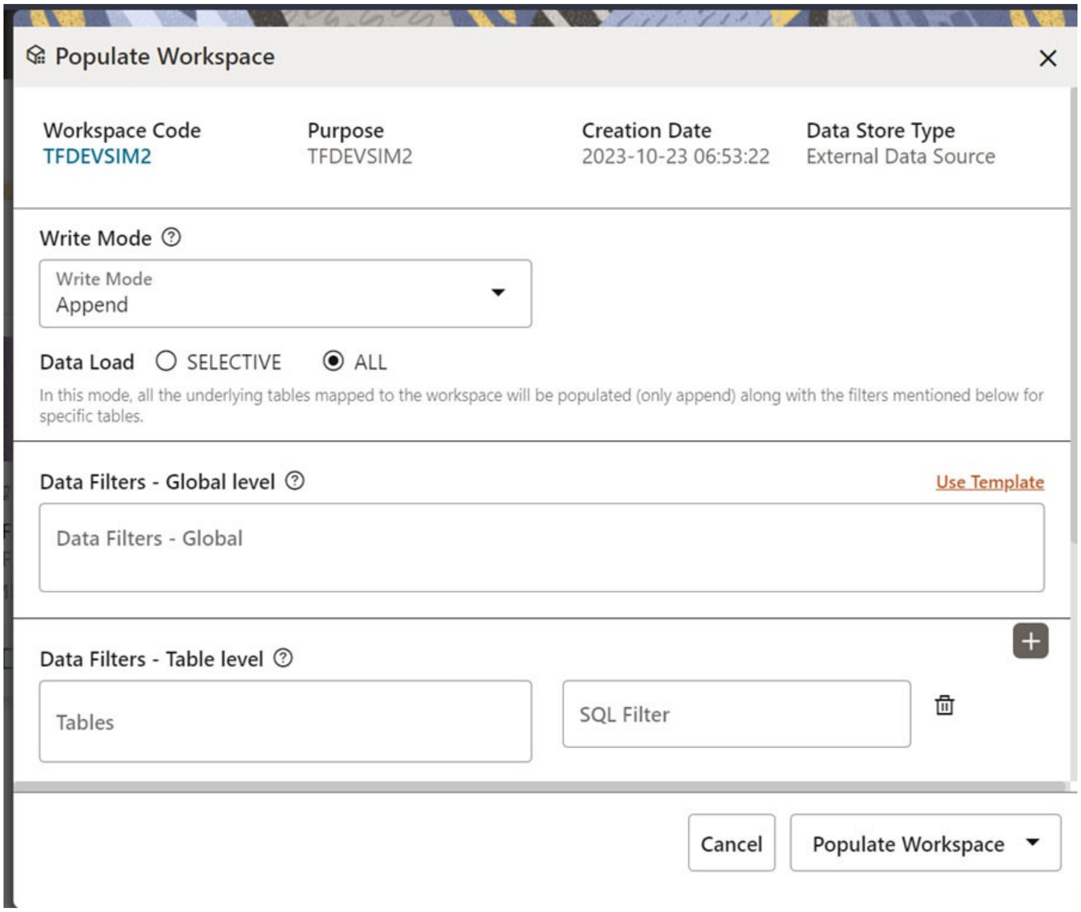
1. ••• Navigate to the **Workspace Summary** page. The page displays Workspace records in a table.
2. Click **Action** next to corresponding Workspace and select **Populate Workspace** to populate the Workspace with data from source data schema to target data schema in the **Populate Workspace** window.

3. You ca use the pre-configured template to auto populate the field values and filters. click **Use Template** and select `TFGroupMessageTypeFilterTemplate.zip` file from the library list to auto populate the values.

   > **Note**
   >
   > You must replace the SQL Filter (`$V_GRP_MSG_TYPE$`) value with the message type.

4. You can enter the field values manually. For reference, see the Populate Workspace table.

Figure 12-15 Populate Workspace Window



Populate Workspace

Workspace Code: TFDEVSIM2
Purpose: TFDEVSIM2
Creation Date: 2023-10-23 06:53:22
Data Store Type: External Data Source

Write Mode: Append

Data Load ○ SELECTIVE ● ALL

In this mode, all the underlying tables mapped to the workspace will be populated (only append) along with the filters mentioned below for specific tables.

Data Filters - Global level

Data Filters - Table level

The following table provides descriptions for the fields in the **Populate Workspace** window.

Table 12-4 Populate Workspace

Field	Description
Workspace Code	The code of the Workspace.
Purpose	The description for the Workspace.
Creation Date	The date on which the Workspace was created.

Table 12-4 (Cont.) Populate Workspace

Field	Description
Data Source Type	The source of data. The value can be the OFSAA Data Schema or an external data source.
Data Filter - Global	Enter the data filter that needs to be applied on all the tables selected for data sourcing. For example: If MISDATE is equal to Today, then it is applied to all tables (wherever it is available) for selected Data Sources during population. If this field is not found (MISDATE) in the tables, it is not updated.
Data Filter - Table level	Provide the data filters individually on the tables here. **NOTE:** You can provide multiple table names for the same SQL filter. For example, there are two tables called Student and Employee in the target data source, and below filters are applied: • MISDATE as Today for Student and Employee tables • ID as 1 for Student table Then, Student table will be populated with MISDATE and ID filters and Employee table will be populated with only MISDATE filter. Global Filters will not be applicable for those tables on which filters have been applied individually. If the same table name is provided in more than one rows here, then filter condition is generated as a conjunction of all the provided filters.
Fetch Size	Enter the Fetch size of JDBC properties for data upload
Batch Commit Size	Enter the Batch Commit size of JDBC properties for data upload
Write Mode	Populate the workspace in **append** mode.
Rejection Threshold	Following two options are available: • Custom Rejection Threshold Enter the maximum of number of inserts that may fail for any of the selected tables. You can provide the maximum number of inserts that can fail while loading data to a given table from all the sources. In case of threshold breach, all the inserts into the particular target schema will be rolled back. However, it will con- tinue with populating the next target schema. • Unlimited Here, all the errors will be ignored during the data population.
Data Load	Available options are SELECTIVE and ALL. Use ALL for first time data population

5. Click **Populate Workspace** to start the process.

Here, you can create the batch using Create Batch, or create and execute using Create and Execute Batch option. On selecting either of these options, a workspace population task gets added to the batch.

> **Note**
>
> You may require approval from an approver to populate the workspace.

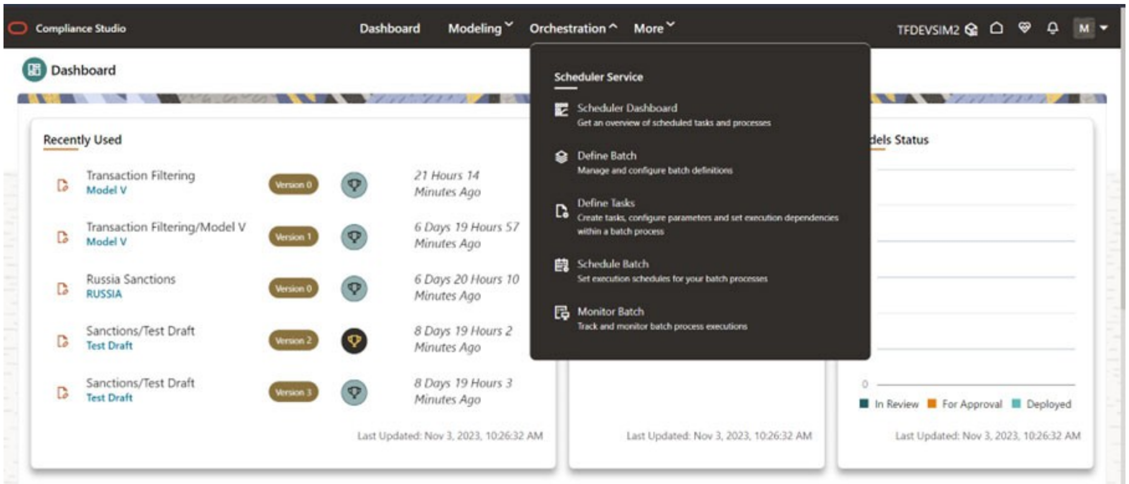
- When you select Create and Execute Batch option, it allows you to create batch and triggers the batch as well.

- When you select 'Create Batch' option, it allows you to prepare the batch and then execute or schedule the batch at a later time through Scheduler Service window.

The Workspace population task execution can be tracked in the 'Monitor Batch' window. For more information on Scheduler Service and Workspace population task execution, see Oracle Financial Services Compliance Studio User Guide .

> **Note**
>
> - You can only run the workspace population for once.
> - Any table that is deselected from the data sourcing definition will **NOT** be dropped.

Figure 12-16   Accessing Scheduler Service from Dashboard


Compliance Studio
Dashboard
Modeling
Orchestration
More
TFDEVSIM2
M
Dashboard
Scheduler Service
Scheduler Dashboard
Get an overview of scheduled tasks and processes
Define Batch
Manage and configure batch definitions
Define Tasks
Create tasks, configure parameters and set execution dependencies within a batch process
Schedule Batch
Set execution schedules for your batch processes
Monitor Batch
Track and monitor batch process executions
dels Status
0
In Review
For Approval
Deployed

Recently Used

Transaction Filtering Model V	Version 0	21 Hours 14 Minutes Ago
Transaction Filtering/Model V Model V	Version 1	6 Days 19 Hours 57 Minutes Ago
Russia Sanctions RUSSIA	Version 0	6 Days 20 Hours 10 Minutes Ago
Sanctions/Test Draft Test Draft	Version 2	8 Days 19 Hours 2 Minutes Ago
Sanctions/Test Draft Test Draft	Version 3	8 Days 19 Hours 3 Minutes Ago

Last Updated: Nov 3, 2023, 10:26:32 AM

Last Updated: Nov 3, 2023, 10:26:32 AM

Last Updated: Nov 3, 2023, 10:26:32 AM

12.5 Managing Model Pipelines

Model Pipeline allows you to create and publish models based on the workspaces created from datasets in the database. The published models are then deployed in production to be consumed by users. For the subsequent information on model pipelines, see Managing Model Pipelines section in Oracle Financial Services Compliance Studio User Guide.

- Prerequisites
- Access the Workspace Dashboard Window
- Accessing the Model Pipelines
- Reviewing, Approving Model
- Import a Workspace Model Data into a New Model
- Import/Export Models
- Using View Models
- Editing Models
- Deleting Objectives and Draft Models
- Creating Seeded Models

12.5.1 Creating a Model

Model creation and deployment undergoes a workflow of Model Governance where the users in the system have privileges that restrict the activities, they can do in the model creation and deployment workflow.

12.5.1.1 Creating Objective (Folders)

Create folders called Objectives within which you can create Models. To create an Objective, follow these steps:

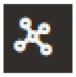
1. Click Launch Workspace

   Figure 12-17 Launch Icon

   next to corresponding Workspace to Launch Workspace and display the **Dashboard** window with application configuration and model creation menu.

2. In the Mega menu, click **Modeling** and select **Pipelines**

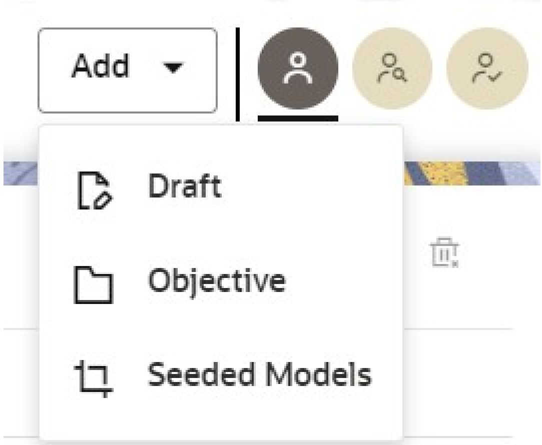
   Figure 12-18 Pipeline

   from the drop down to display the
   Model Pipeline window.

3. Click **Add** and select **Objective** from the list to display the **Objective Details** dialog box.

   Figure 12-19 Select Objective from Add

4. Enter details in Objective **Name** and **Description** fields in the Add **Objective** dialog box.
5. Click **Save**.

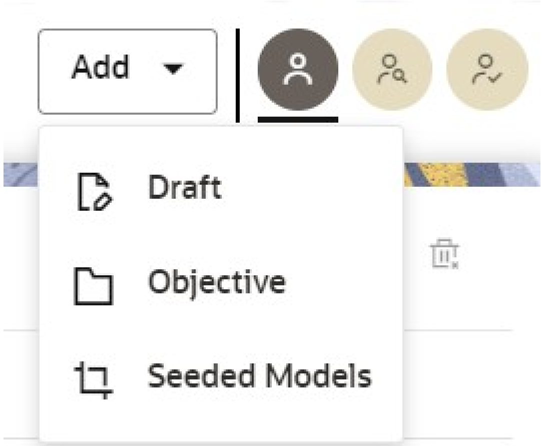
12.5.1.2 Creating Draft Models Using Seeded Model

Create Models that are classified as draft models. These models will be reviewed before being sent for Scoring.

To create a draft Model, follow these steps:

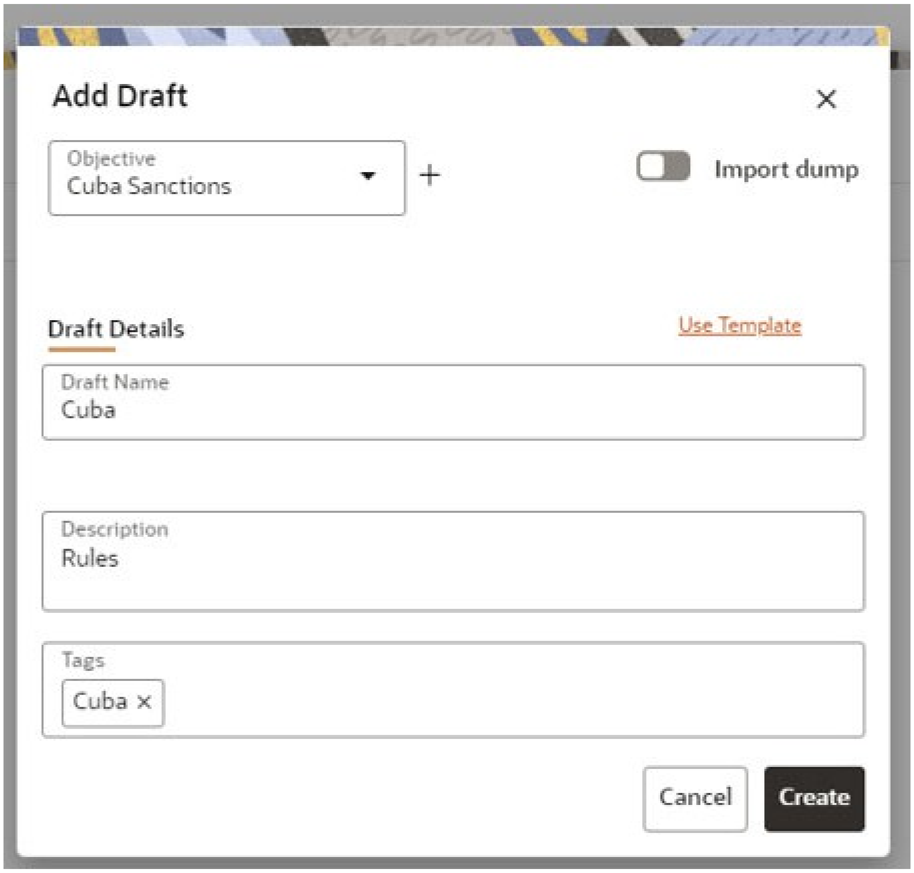
1. Click Launch Workspace next to corresponding Workspace to Launch Workspace and display the **Dashboard** window with application configuration and model creation menu.
2. Open the Objective.
3. Click **Add** and select **Draft** from the list to display the **Add Draft** dialog box.

Figure 12-20 Draft



4. **Create New Model** is the default setting in the **Model Details** dialog box. To create a new model, follow these steps:
   a. Click **Use Template**.
   b. Select the TF Simulation zip file (TFSIMULATION_1697204758446.zip) from the templates.
   c. Enter details for Draft **Name** and **Description**

Figure 12-21 Model Details - Create New Model



Add Draft

Objective: Cuba Sanctions

Import dump

Draft Details

Use Template

Draft Name: Cuba

Description: Rules

Tags: Cuba

.

d. Enter a tag in the **Tags** field.

e. Click **Create**. a model pipeline will be created from the template.

To clone the objects for Real time EDQ, Swift Message Configurations, and Swift Message Parse Widgets, follow the subsequent steps:

a. Navigate to the **Design Pipeline** page.

b. From the pipeline canvas double click on the widget to open the widget details screen on the right side.

c. In the widget screen under the Custom Parameters tab, click **Copy** to open the **Clone Objects** Window.

d. Select the source model ID from the **Clone Objects** Window and select the version from which you want to clone the widget.

> **Note**
>
> For the first model, select model ID as **PROD**.

e. Click **Copy**. The TF Widget clone process begins. Once the cloning is completed, the current model ID and version will automatically be populated in the widget screen.

f. Click **Save** to save the widget.

12.5.1.3 Cloning a Model

You can pick any published model and clone the contents to a new draft in the same objective or clone the content to the current parent draft. The cloned draft can be edited and used further. Audit Trail window also captures the clone information.

To clone the model details, follow these steps:

1. Open a Published Model in Pipeline Designer.
2. Select **Clone to new Draft** to Re-image parent draft with current.

12.6 Model Pipeline

Modeling refers to the process of designing a prototype based on a structured data model for statistical analysis and for simulating actual events and functions. A user with access to the Workspace can create or modify models in a workspace. Model versions are preserved in the Workspace, along with execution and output histories. Once a model has been validated in the Workspace and considered fit for use, modelers can request to push the Model into the production environment.

The following sections are available on the Model Pipeline window:

- Pipeline
- Dashboard
- Notebook
- Simulations
- Execution History
- Compare

12.6.1 Pipeline

A pipeline is an embedded data processing engine that runs inside the application to filter, transform, and migrate data on-the-fly. Pipelines are a set of data processing elements called widgets connected in series, where the output of one widget is the input to the next element. Use the Pipeline canvas to create the model and execute the pipeline using widgets.

To create a model using pipeline designer, follow the subsequent steps:

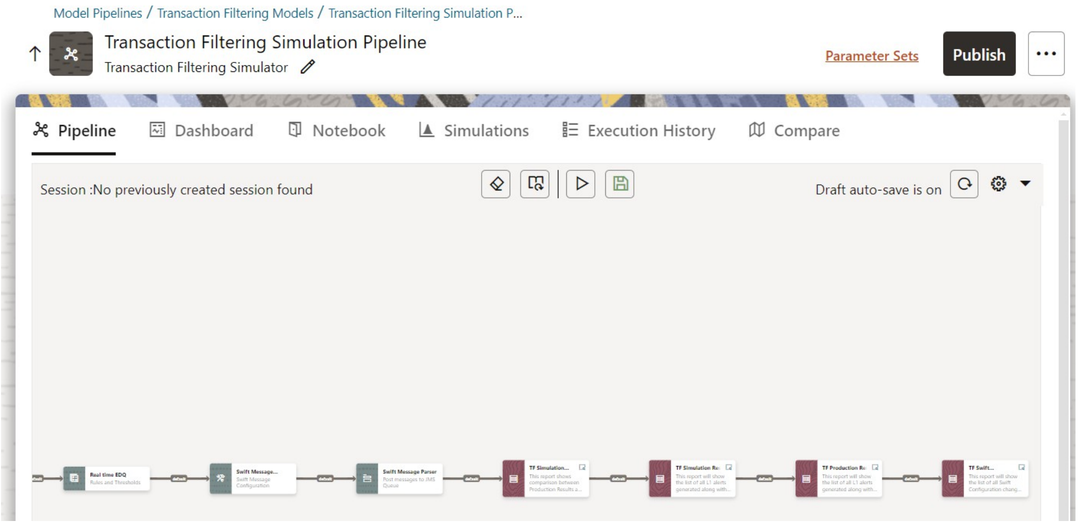
1. ⊕ Navigate to the **Pipeline Designer** page. Pipeline Canvas is displayed.
2. Click on the Connector to display the widgets.
3. Select Transaction Filtering from the list.
4. Select a widget and add the widget to the pipeline canvas. For information on widgets, see the TF Pipeline Widgets table.
5. From the pipeline canvas double click on the widget to open the widget details screen on the right side.
6. In the widget screen under the Custom Parameters tab, click **Copy** to open the **Clone Objects**
   Window.

7. Select the source model ID from the **Clone Objects** Window and select the version from which you want to clone the widget.

> ⓘ **Note**
>
> For the first model, select model ID as **PROD**.

8. Click **Copy**. The TF Widget clone process begins. Once the cloning is completed, the current model ID and version will automatically be populated in the widget screen.
9. Click **Save** to save the widget.
10. Click **Add** the next widget and repeat from step 2 to step 8.

Figure 12-22 Pipeline Canvas


Model Pipelines / Transaction Filtering Models / Transaction Filtering Simulation P...
Transaction Filtering Simulation Pipeline
Transaction Filtering Simulator
Parameter Sets
Publish
Pipeline
Dashboard
Notebook
Simulations
Execution History
Compare
Session :No previously created session found
Draft auto-save is on
default
Real time EDQ
Rules and Thresholds
Swift Message...
Swift Message Configuration
Swift Message Parser
Post messages to JMS Queue
TF Simulation...
This report shows comparison between Production Results a...
TF Simulation Re
This report will show the list of all L1 alerts generated along with...
TF Production Re
This report will show the list of all L1 alerts generated along with...
TF Swift...
This report will show the list of all Swift Configuration chang...

The TF Pipeline Widgets table gives information about TF pipeline widgets.

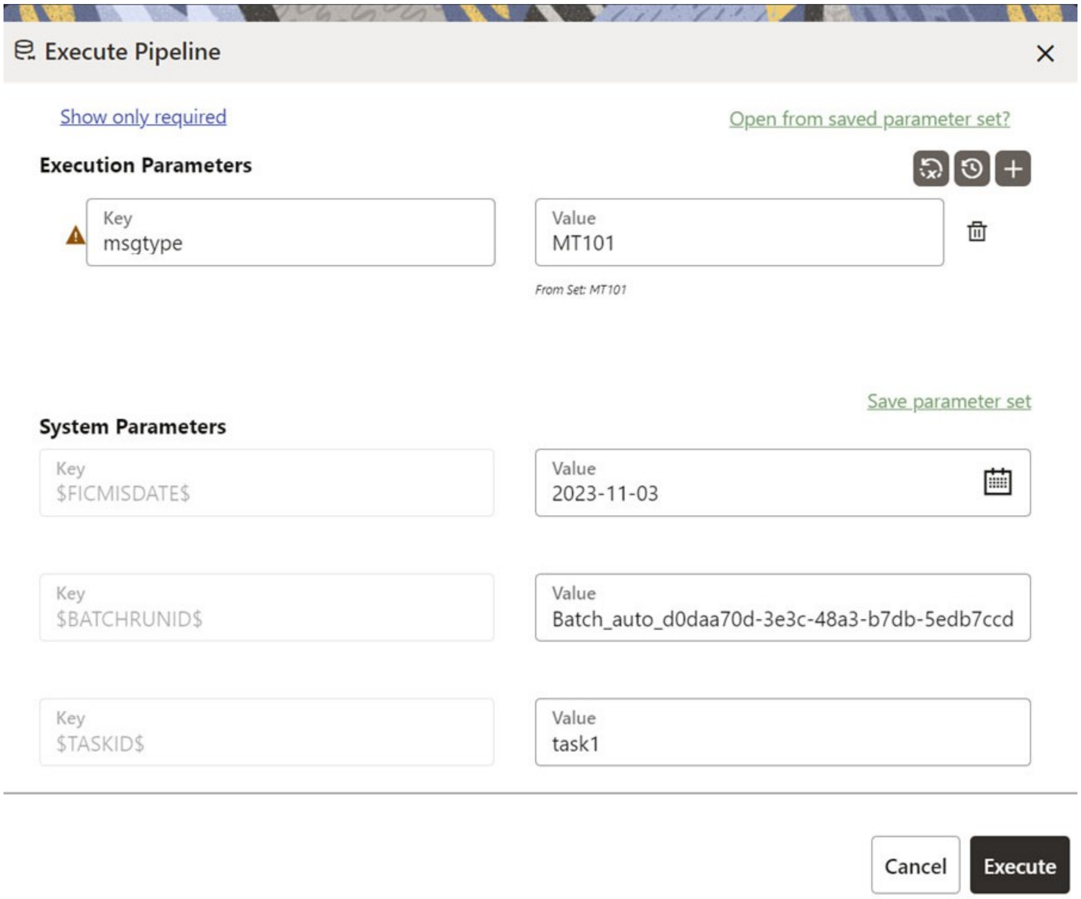
Table 12-5 TF Pipeline Widgets

Widget	Description
Real time EDQ	Opens EDQ homepage where users can log in to EDQ director and tune the EDQ rules of the project with respective model_id with version 0.
Swift Message Configurations	Add/Edit/Remove Swift Configurations
Swift Message Parser	Posts the selected messages (transactions) to the JMS queue
TF Simulation Report	Displays the Summary of alerts and event hits for the current simulation run.
TF Simulation Data	Displays the events generated for the current simulation run.
TF Production Data	Displays the production events for which the simulation was carried out.
TF Swift Configurations Audit	This report will show the list of all Swift Configuration changes with respect to Source Model Swift Configurations.

To execute the pipeline follow the subsequent steps:

1. Click execute icon ▷. Execute Pipeline window is displayed.

Figure 12-23 Execute Pipeline Window



Execute Pipeline

Show only required

Open from saved parameter set?

Execution Parameters

Key: msgtype
Value: MT101
From Set: MT101

Save parameter set

System Parameters

Key: $FICMISDATE$
Value: 2023-11-03

Key: $BATCHRUNID$
Value: Batch_auto_d0daa70d-3e3c-48a3-b7db-5edb7ccd

Key: $TASKID$
Value: task1

2. Click **Open from saved Parameter set?** to import the template.
3. If your not importing the template enter the execution Key and Value manually. Execution parameters are the filters to apply to production data for the simulation run. You configure these filters in FCC_TF_SIMULATION_FILTERS table. For more information on FCC_TF_SIMULATION_FILTERS, see OFS Sanctions Data Model Reference Guide.

> **Note**
>
> Select the flow, which you want to execute Scoring, Training, and Experimentation. It displays all the keys defined for all the paragraphs in the notebook with a placeholder for providing the values.

4. You can add new parameters using **Add**

Figure 12-24 Add

.

> **Note**
>
> If the parameter is not defined in the notebook, it will not be used for the execution. In case of multi select, if there are common parameters among the chosen scenarios, it will take the value based on the order of selection. that is first chosen scenario parameter will be taken.

5. But if open from saved scenarios again (not on single go), then already added will get replaced by the newly added (same as what existed)
6. Execution is performed based on selected link types. It filters out all the not required/ unused parameters. And, all the unused parameters for the current execution are displayed with a

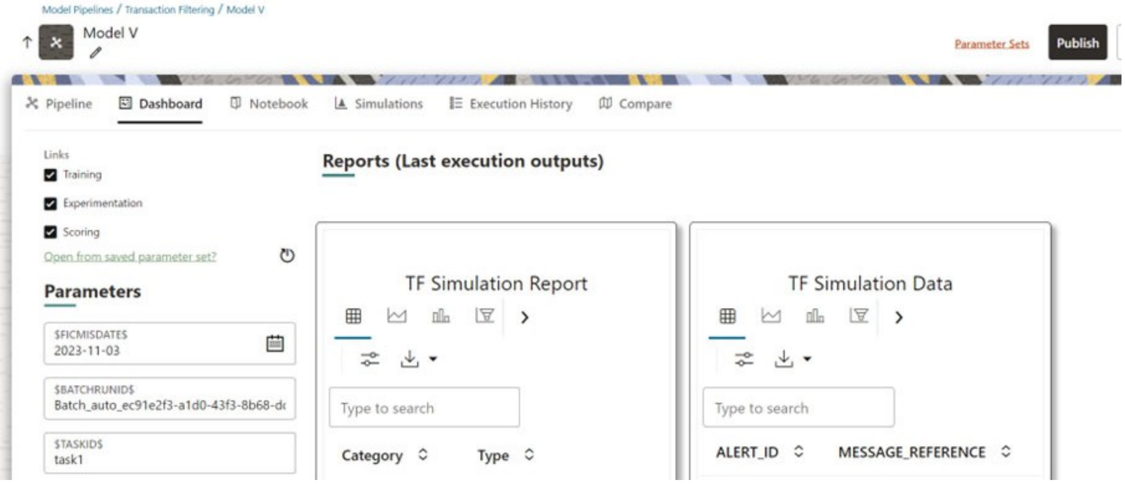
   warning ⚠ . To view the only required parameters, click **Show only required** link.
7. Click Reset ⟳ to reset the entered data.
8. Click Delete 🗑 to delete the entered Key and Value. For example, refer to below Figure.
9. ✓ Click **Execute** to initiate the execution. The widgets in pipelines are executed sequentially and

you can see icon on each widget for a successful execution. For individual widget execution details click the widget and click **View Details**.

12.6.2 Dashboard

The Dashboard of the Pipeline Designer allows you to execute shows the execution output of the Model.

Figure 12-25 Dashboard Tab



Model Pipelines / Transaction Filtering / Model V

Model V

Links

☑ Training

☑ Experimentation

☑ Scoring

Open from saved parameter set?

Parameters

$FICMISDATE$: 2023-11-03

$BATCHRUNID$: Batch_auto_ec91e2f3-a1d0-43f3-8b68-dc

$TASKID$: task1

Reports (Last execution outputs)

TF Simulation Report

Type to search

Category | Type

TF Simulation Data

Type to search

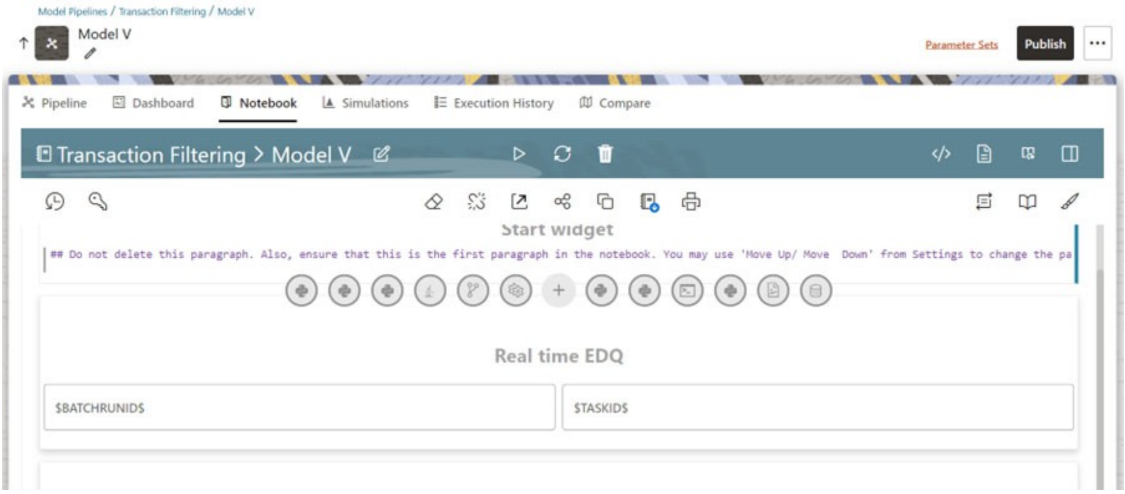
ALERT_ID | MESSAGE_REFERENCE

12.6.3 Notebook

Navigate to Notebook tab to view the paragraphs. You can run, invalidate session, edit, add, and export the notebook in the Notebook tab.

> **Note**
>
> By default the code is not displayed in the UI. To display code in the UI, click the visibility icon and select code.

Figure 12-26 Notebook Tab

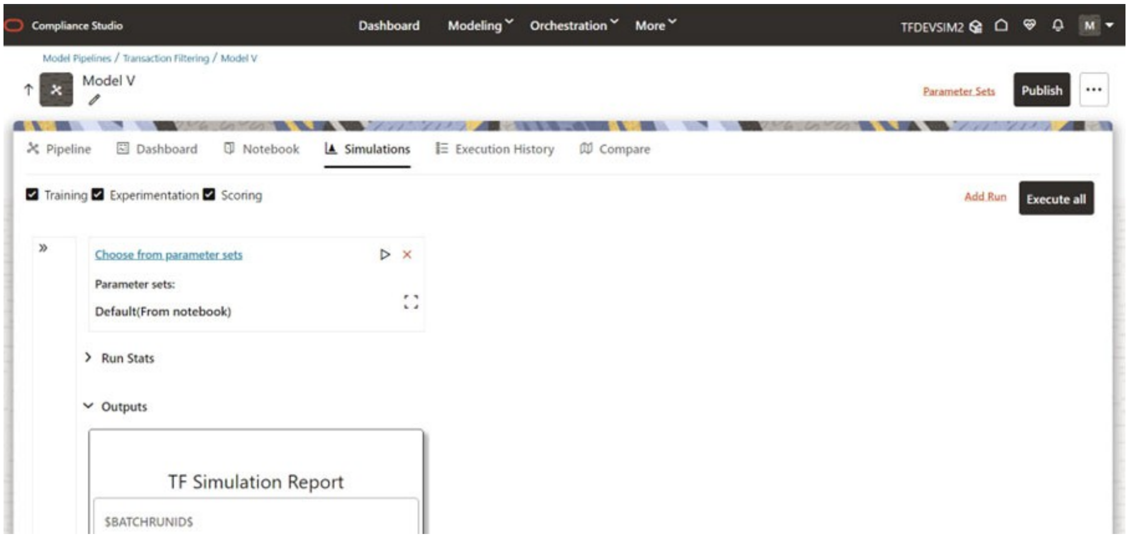


```
## Do not delete this paragraph. Also, ensure that this is the first paragraph in the notebook. You may use 'Move Up/ Move  Down' from Settings to change the pa
```

12.6.4 Simulations

The simulation flow allows for iterative execution along that path with input drivers (variables) that are passed through a parameter set. You can either create a new parameter set or use the existing parameter set and execute it from this tab.

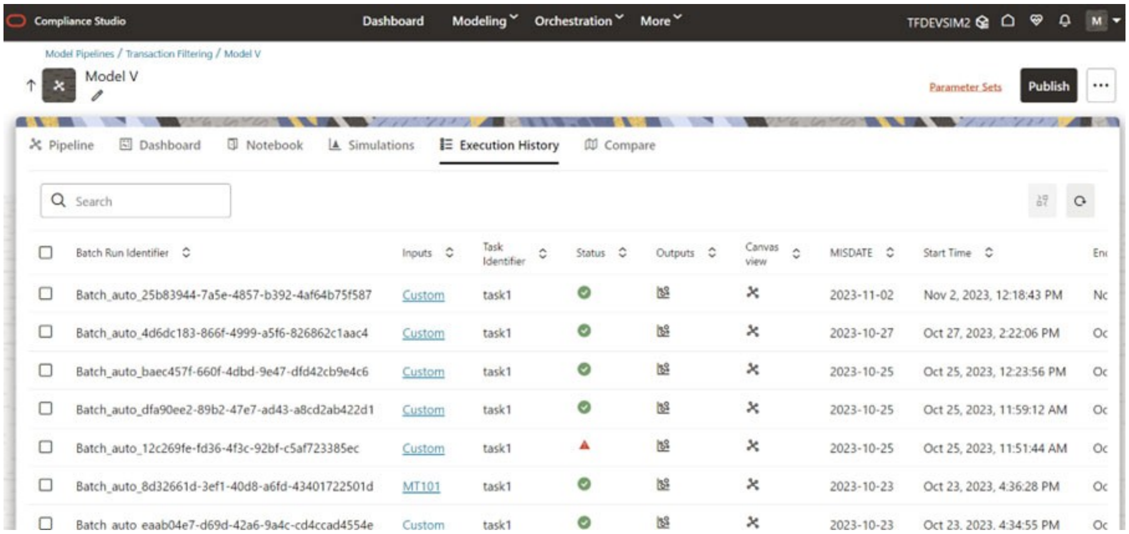
Figure 12-27 Simulation Tab



12.6.5 Execution History

This section of Pipeline Designer shows the history of the executions of the current pipeline. You can view the list of executions, check the report for the corresponding simulation run, and extract the report. You can compare multiple executions by selecting multiple executions and click on Compare icon.

Figure 12-28 Execution History



☐	Batch Run Identifier	Inputs	Task Identifier	Status	Outputs	Canvas view	MISDATE	Start Time	En
☐	Batch_auto_25b83944-7a5e-4857-b392-4af64b75f587	Custom	task1	✓	▦	✕	2023-11-02	Nov 2, 2023, 12:18:43 PM	Nc
☐	Batch_auto_4d6dc183-866f-4999-a5f6-826862c1aac4	Custom	task1	✓	▦	✕	2023-10-27	Oct 27, 2023, 2:22:06 PM	Oc
☐	Batch_auto_baec457f-660f-4dbd-9e47-dfd42cb9e4c6	Custom	task1	✓	▦	✕	2023-10-25	Oct 25, 2023, 12:23:56 PM	Oc
☐	Batch_auto_dfa90ee2-89b2-47e7-ad43-a8cd2ab422d1	Custom	task1	✓	▦	✕	2023-10-25	Oct 25, 2023, 11:59:12 AM	Oc
☐	Batch_auto_12c269fe-fd36-4f3c-92bf-c5af723385ec	Custom	task1	▲	▦	✕	2023-10-25	Oct 25, 2023, 11:51:44 AM	Oc
☐	Batch_auto_8d32661d-3ef1-40d8-a6fd-43401722501d	MT101	task1	✓	▦	✕	2023-10-23	Oct 23, 2023, 4:36:28 PM	Oc
☐	Batch_auto_eaab04e7-d69d-42a6-9a4c-cd4ccad4554e	Custom	task1	✓	▦	✕	2023-10-23	Oct 23, 2023, 4:34:55 PM	Oc

To download the report follow the subsequent steps:

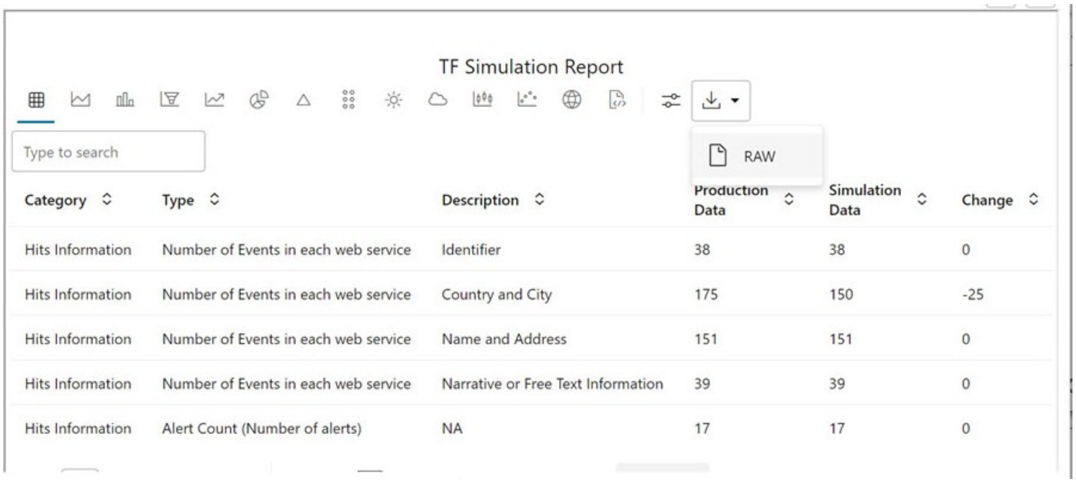
1. click the output icon ▦ for the respective batch. Output Details Page is displayed. Following Output report tiles are displayed
   - Start Widget

- TF Specific widget
- Report Widget

2. From the Report Widget tile click the download icon to download the report in the text file format.

> **Note**
>
> You must open the report text file in excel or drag and drop in excel to view the output.

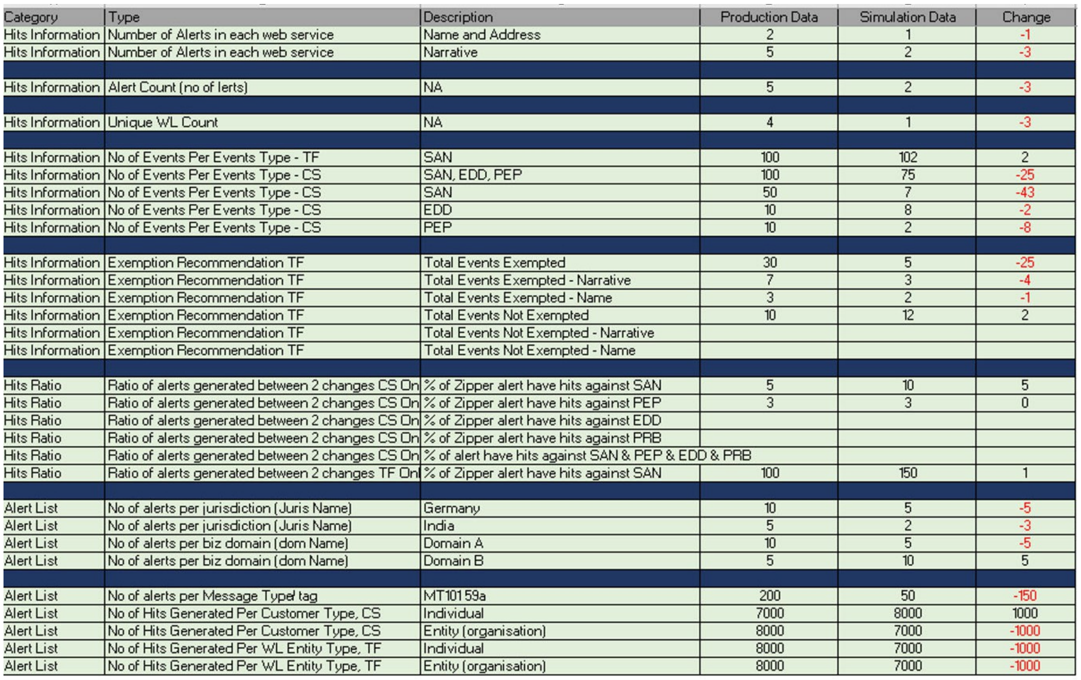
Figure 12-29 Report Extraction Tile



TF Simulation Report

Category	Type	Description	Production Data	Simulation Data	Change
Hits Information	Number of Events in each web service	Identifier	38	38	0
Hits Information	Number of Events in each web service	Country and City	175	150	-25
Hits Information	Number of Events in each web service	Name and Address	151	151	0
Hits Information	Number of Events in each web service	Narrative or Free Text Information	39	39	0
Hits Information	Alert Count (Number of alerts)	NA	17	17	0

Figure 12-30 Extracted Output Sample



Category	Type	Description	Production Data	Simulation Data	Change
Hits Information	Number of Alerts in each web service	Name and Address	2	1	-1
Hits Information	Number of Alerts in each web service	Narrative	5	2	-3
Hits Information	Alert Count (no of lerts)	NA	5	2	-3
Hits Information	Unique WL Count	NA	4	1	-3
Hits Information	No of Events Per Events Type - TF	SAN	100	102	2
Hits Information	No of Events Per Events Type - CS	SAN, EDD, PEP	100	75	-25
Hits Information	No of Events Per Events Type - CS	SAN	50	7	-43
Hits Information	No of Events Per Events Type - CS	EDD	10	8	-2
Hits Information	No of Events Per Events Type - CS	PEP	10	2	-8
Hits Information	Exemption Recommendation TF	Total Events Exempted	30	5	-25
Hits Information	Exemption Recommendation TF	Total Events Exempted - Narrative	7	3	-4
Hits Information	Exemption Recommendation TF	Total Events Exempted - Name	3	2	-1
Hits Information	Exemption Recommendation TF	Total Events Not Exempted	10	12	2
Hits Information	Exemption Recommendation TF	Total Events Not Exempted - Narrative			
Hits Information	Exemption Recommendation TF	Total Events Not Exempted - Name			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against SAN	5	10	5
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against PEP	3	3	0
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against EDD			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against PRB			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of alert have hits against SAN & PEP & EDD & PRB			
Hits Ratio	Ratio of alerts generated between 2 changes TF On	% of Zipper alert have hits against SAN	100	150	1
Alert List	No of alerts per jurisdiction (Juris Name)	Germany	10	5	-5
Alert List	No of alerts per jurisdiction (Juris Name)	India	5	2	-3
Alert List	No of alerts per biz domain (dom Name)	Domain A	10	5	-5
Alert List	No of alerts per biz domain (dom Name)	Domain B	5	10	5
Alert List	No of alerts per Message Type/ tag	MT101 59a	200	50	-150
Alert List	No of Hits Generated Per Customer Type, CS	Individual	7000	8000	1000
Alert List	No of Hits Generated Per Customer Type, CS	Entity (organisation)	8000	7000	-1000
Alert List	No of Hits Generated Per WL Entity Type, TF	Individual	8000	7000	-1000
Alert List	No of Hits Generated Per WL Entity Type, TF	Entity (organisation)	8000	7000	-1000

12.6.6 Compare

The Compare option allows you to compare the executions with champion model. To compare, follow these steps:

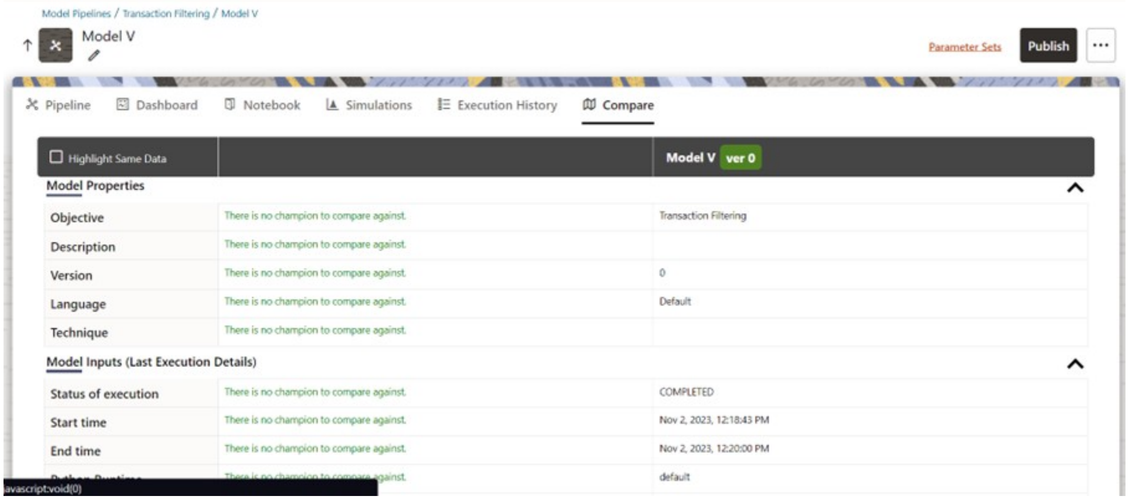
1. Navigate to Execution Summary window.
2. Select the executions using the corresponding check-boxes.
3. Click Compare .

The Execution Comparison window is displayed.

The Window shows the following comparison details:

- Model Properties
- Model Input (Last Execution Details)
- Audit Log
- Model Script
- Model Output (Last Execution Outputs)

Figure 12-31 Compare Tab



□ Highlight Same Data		Model V ver 0
Model Properties		
Objective	There is no champion to compare against.	Transaction Filtering
Description	There is no champion to compare against.	
Version	There is no champion to compare against.	0
Language	There is no champion to compare against.	Default
Technique	There is no champion to compare against.	
Model Inputs (Last Execution Details)		
Status of execution	There is no champion to compare against.	COMPLETED
Start time	There is no champion to compare against.	Nov 2, 2023, 12:18:43 PM
End time	There is no champion to compare against.	Nov 2, 2023, 12:20:00 PM
Python Runtime	There is no champion to compare against.	default

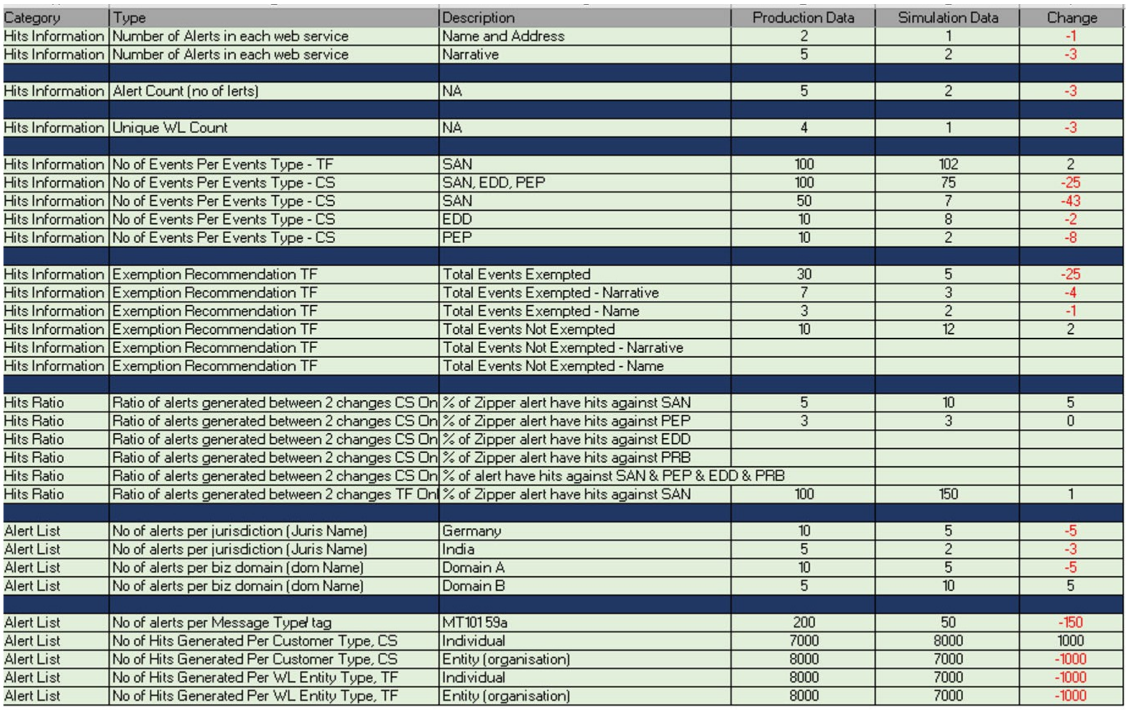
12.7 Report Extraction

You can view the output of the executions from all the tabs of the model pipeline. Execution History tab allows you to download the execution output to the local system. For more information, see Execution History.

Note

- You must open the report text file in excel or drag and drop in excel to view the output.
- If the execution output is truncated, update the Zeppelin interpreter output limit. For more information, see Appendix L: Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMIT in Python Interpreter.

Figure 12-32 Extracted Output Sample



Category	Type	Description	Production Data	Simulation Data	Change
Hits Information	Number of Alerts in each web service	Name and Address	2	1	-1
Hits Information	Number of Alerts in each web service	Narrative	5	2	-3
Hits Information	Alert Count (no of lerts)	NA	5	2	-3
Hits Information	Unique WL Count	NA	4	1	-3
Hits Information	No of Events Per Events Type - TF	SAN	100	102	2
Hits Information	No of Events Per Events Type - CS	SAN, EDD, PEP	100	75	-25
Hits Information	No of Events Per Events Type - CS	SAN	50	7	-43
Hits Information	No of Events Per Events Type - CS	EDD	10	8	-2
Hits Information	No of Events Per Events Type - CS	PEP	10	2	-8
Hits Information	Exemption Recommendation TF	Total Events Exempted	30	5	-25
Hits Information	Exemption Recommendation TF	Total Events Exempted - Narrative	7	3	-4
Hits Information	Exemption Recommendation TF	Total Events Exempted - Name	3	2	-1
Hits Information	Exemption Recommendation TF	Total Events Not Exempted	10	12	2
Hits Information	Exemption Recommendation TF	Total Events Not Exempted - Narrative			
Hits Information	Exemption Recommendation TF	Total Events Not Exempted - Name			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against SAN	5	10	5
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against PEP	3	3	0
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against EDD			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of Zipper alert have hits against PRB			
Hits Ratio	Ratio of alerts generated between 2 changes CS On	% of alert have hits against SAN & PEP & EDD & PRB			
Hits Ratio	Ratio of alerts generated between 2 changes TF Onl	% of Zipper alert have hits against SAN	100	150	1
Alert List	No of alerts per jurisdiction (Juris Name)	Germany	10	5	-5
Alert List	No of alerts per jurisdiction (Juris Name)	India	5	2	-3
Alert List	No of alerts per biz domain (dom Name)	Domain A	10	5	-5
Alert List	No of alerts per biz domain (dom Name)	Domain B	5	10	5
Alert List	No of alerts per Message Type/ tag	MT101 59a	200	50	-150
Alert List	No of Hits Generated Per Customer Type, CS	Individual	7000	8000	1000
Alert List	No of Hits Generated Per Customer Type, CS	Entity (organisation)	8000	7000	-1000
Alert List	No of Hits Generated Per WL Entity Type, TF	Individual	8000	7000	-1000
Alert List	No of Hits Generated Per WL Entity Type, TF	Entity (organisation)	8000	7000	-1000

12.8 Publishing a Pipeline

If your satisfied with the results of the execution you can publish the pipeline. Publish the pipeline will backup the current model pipeline with non editable mode. To publish the pipeline, follow these steps:

1. Click Launch Workspace next to corresponding Workspace to Launch Workspace and display the **Dashboard** window with application configuration and model creation menu.
2. In the Mega menu, click **Modeling** and select **Pipelines** from the drop down to display the
   Model Pipeline window.
3. Select the Objective from the list. The publish canvas is displayed.

4. Click **Publish**. Publish Pipeline pop-up is displayed.
5. Enter the field details. See the following table.

Table 12-6 Publish Pipeline

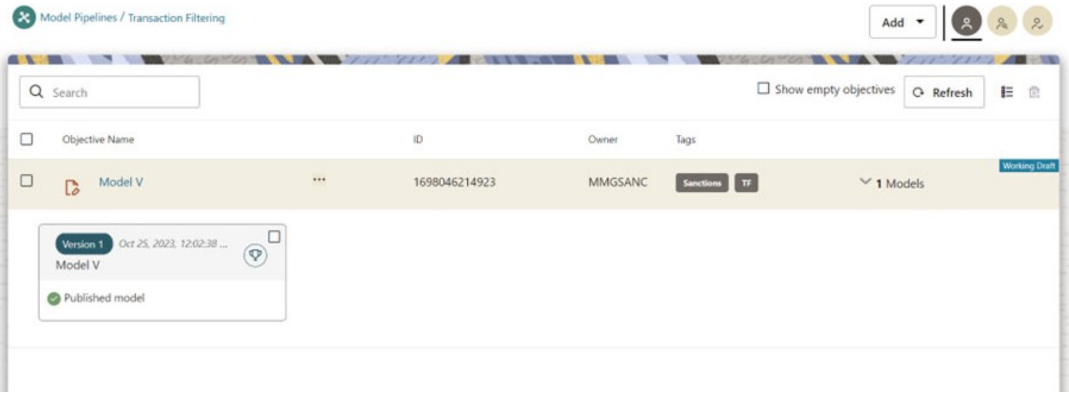
Field or Icon	Description
Model Name	The field displays the name of the Model. Modify the name if required.
Model Description	The field displays the description for the Model. Enter or modify the description if required.
Technique	Enter the registered technique to use.
Run Version	Select a rub version.
Variable Mapping	The table displays the OFSAA variables and datasets used in the creation of the Training Model.
Script	The table displays the Paragraphs created in the Training Model. Select the Paragraphs that you want to use to create the Scoring Model. Track Output - Select this to track the output of the paragraph.

6. Select the required configuration and click **Publish** to publish the pipeline or click **Cancel** to go back to previous page.

To view the published model follow the subsequent steps:

1. Navigate to **Model Pipeline** page
2. Click **Models** in-line with the Object Name. published models are displayed.

Figure 12-33 Published Model



Model Pipelines / Transaction Filtering

Add ▾

Search

□ Show empty objectives

Refresh

□	Objective Name	ID	Owner	Tags	
□	Model V ···	1698046214923	MMGSANC	Sanctions TF	1 Models

The published models are then deployed in production to be consumed by users. The iterations of comparison between various models lead to the elimination of undesired models and the filter of a few robust ones that can be considered for deployment in production. Modelers then use their better judgment to consolidate their choice and fix on one model - the champion model. The champion model is also called the scoring model or the actual model in this document.

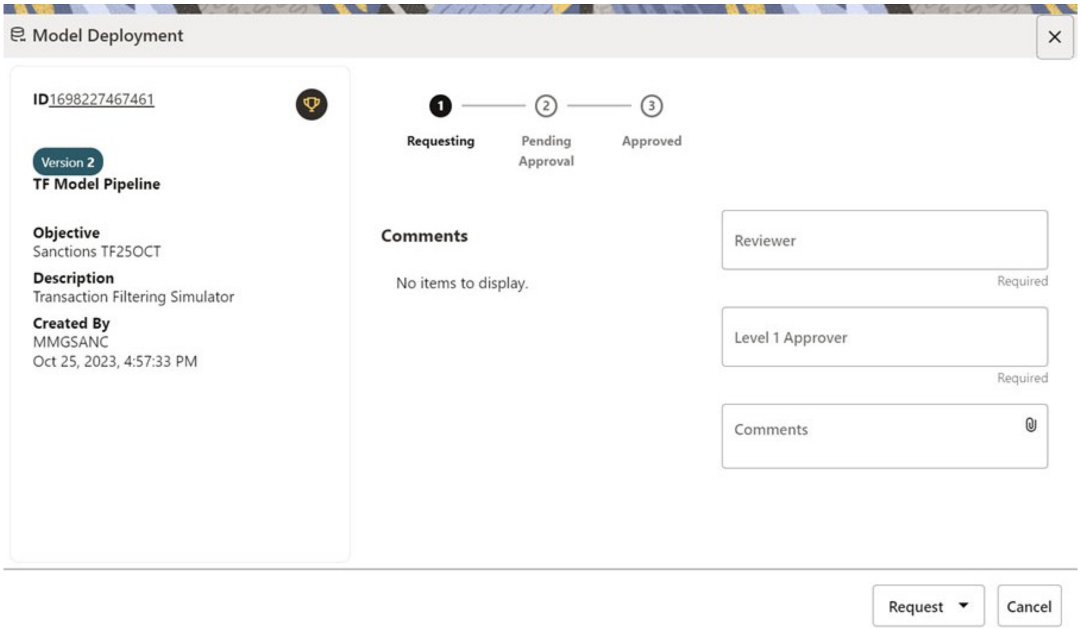
12.9 Deploying the Model

You can promote the published model to production by deploying the Model. For the subsequent information, see Oracle Financial Services Compliance Studio User Guide.

- Understanding Model Governance
- Request Model Acceptance
- Review Models and Move to Approve or Reject
- Approve Models and Promote to Production
- Deploying Models in Production and Make it a Global Champion
- Executing Models using Scheduler Service To deploy the model follow the subsequent steps:

1. Click Launch Workspace next to corresponding Workspace to Launch Workspace and display the **Dashboard** window with application configuration and model creation menu.
2. In the Mega menu, click **Modeling** and select **Pipelines** from the drop down to display the
   Model Pipeline window.
3. Select the Objective name from the list and select the published Model.
4. Click to view the Model Deployment screen.

Figure 12-34 Model Deployment Window



Model Deployment

ID1698227467461

Version 2
TF Model Pipeline

Objective
Sanctions TF25OCT

Description
Transaction Filtering Simulator

Created By
MMGSANC
Oct 25, 2023, 4:57:33 PM

Comments

No items to display.

Reviewer
Required

Level 1 Approver
Required

Comments

5. Select the value for the following fields:
   - Reviewer
   - Level 1 Approver
   - Comments
6. Click **Request** and select **Model Acceptance** action.

7. Click **Cancel** to cancel the model Deployment.

> **Note**
>
> For each workspace there can be only one champion model.

12.10 Audit Trail

For information on using audit trail, see Oracle Financial Services Compliance Studio User Guide.

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.

A.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

A.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

A.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.

A.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 .

A.5 World-Check Watch List

World-Check provides a subscription-based service, offering a consolidated list of PEPs (Politically Exposed Persons) and entities and individuals appearing on the HM Treasury, OFAC, and other world lists. Three levels of subscription are provided: Standard, Premium, and Premium+. Some features of the World-Check lists are only available to users with a higher subscription level. For more information, see the World-Check website.

To download the World-Check Premium+ feed, set values in the WC Setup section of the `watch list- management. properties` run profile as follows:

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

```
phase.WC\ -\ Download\ native\ aliases.enabled = Y phase.WC\ -\ Stage\ reference\
lists.enabled = Y phase.*.snapshot.*.use_native_aliases = 1
```

To download the Standard or Premium feeds, set values in the WC Setup section of the `watchlist-management.properties` run profile as follows:

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

```
phase.WC\ -\ Download\ native\ aliases.enabled = N phase.WC\ -\ Stage\ reference\
lists.enabled = Y phase.*.snapshot.*.use_native_aliases = 0
```

See the World-Check website for more details: https://risk.thomsonreuters.com/en/products/third-party-risk/world-check-know-your-customer.html

> **Note**
>
> If your instance of Oracle Transaction Filtering uses the WebLogic application server, and you are screening against the World-Check watch list, then, to download the World-Check reference data successfully, you must add the following to the 'Server Start' arguments of your EDQ managed server: - DUseSunHttpHandler=true. This is only required if you are using the WebLogic application server and screening against the World-Check watch list.

A.6 Dow Jones Watch List

Dow Jones provides a subscription-based service offering a consolidated list of PEPs (Politically Exposed Persons) and entities and individuals appearing on the various sanctions lists. For more information, see the Dow Jones website.

The Dow Jones watch list automated download task uses one of two script files that are provided with Oracle Transaction Filtering to provide further configuration of the download process. These script files are:

- download-djw.sh (for use on Unix platforms)
- download-djw.bat (for use on Windows platforms)

The script files are invoked by the automated task and will download the data files and copy them to the appropriate sub-folder of the OEDQ landing area.

> **Note**
>
> In Watchlist Management Project under Reference Data, the “DJW List Provider Static”, contains the entire Dow Jones List Providers. It contains the score and the flag irrespective whether it belongs to Sanctions List or not. User has the privilege to change the flag and score based on their preference.

A.7 Dow Jones Anti-Corruption Watch List

Dow Jones provides a subscription-based service containing data to help you assess, investigate, and monitor third-party risk about anti-corruption compliance regulation. For more information, see the Dow Jones website.

The Dow Jones Anti-Corruption List automated download task uses one of two script files that are provided with Oracle Transaction Filtering to provide further configuration of the download process. These script files are:

- download-djac.sh (for use on Unix platforms)
- download-djac.bat (for use on Windows platforms)

The script files are invoked by the automated task and will download the data files and copy them to the appropriate sub-folder of the OEDQ landing area.

A.8 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.

B

Appendix B: System Audit Logging Information

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

B.1 Activities for System Audit

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

Table B-1 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

B.2 Steps for System Audit Activities

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

Table B-2 Steps for System Audit Activities

Step Identifier	Activity Name	Step Name	Step Sequence	Status
1	Raw Message Processing	Record the receipt of the raw message	1	Y
2	Raw Message Processing	Raw Message persisted into structure table	2	N
3	Message Parser Processing	Raw Message parsed	1	N
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

Table B-2 (Cont.) Steps for System Audit Activities

Step Identifier	Activity Name	Step Name	Step Sequence	Status
8	watch list Processing	Scoring performed	4	Y
9	watch list Processing	Response Received	5	Y
10	watch list Processing	Response persisted	6	N
11	Alert Manager Processing	Transaction Hold	1	N
12	Alert Manager Processing	Alert Persisted	2	N
13	Hold	Hold Transaction Workflow Invoked	1	Y
14	Hold	Hold Transaction Workflow completed	2	Y
15	Assigned	Assigned Transaction Workflow Invoked	1	Y
16	Assigned	Assigned Transaction Workflow completed	2	Y
17	Escalate	Escalated Transaction Workflow Invoked	1	Y
18	Escalate	Escalated Transaction Workflow completed	2	Y
19	Recommend to Block	NA	NA	NA
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

C

Process Modeller Framework (PMF) Configurability

This appendix contains information on the steps required to configure the ready-to-use Process Modeller Framework (PMF) workflow. On the **Process Modeller** page, click the transaction that you want to configure and follow the steps in the following sequence. For information on how to access the **Process Modeller** page, see the Process Modeller Menu.

C.1 Configuring the Human Task in the PMF Page

To configure all human tasks on the **PMF** page, follow these steps:

1. Navigate to the **Process Flow** subtab in the **Process Modeller** tab. The **PMF** page is displayed.
2. Drag and drop **Human Task** on to the PMF page. For information on all components avail- able, see the **Components for Designing Your Process Flow** chapter in the Oracle Financial Services Analytical Applications Infrastructure Process Modelling Framework (PMF) Orchestration Guide .
3. Double-click **Human Task** .
4. In the Activity dialog, provide the following information:
   - A unique activity name in the **Activity Name** field. After you provide a name, it appears after the icon on the **PMF** page.
   - The activity description in the **Activity Description** field.
   - The current status of the transaction in the **Status** field.
   - The next status of the transaction in the **Outcomes** field.
5. Click **Transitions** and then click **Add**.
   - In the **Add New Transition** dialog, provide the following information:
   - A unique transition name in the **Transition Name** field.
   - The destination status of the transaction in the **Connected To** field.
   - The execution or decision rule for a status in the **Decision Rule** field. Here you need to map the specific rule to the current status or create the rule according to the business require- ment.
   - The order of the transaction in the **Order** field.

You can also configure the fields in the **Action and Notifications** subtabs. For more information, see the **Action Tab for Creating Tasks/Notification** section in Oracle Financial Services Analytical Applications Infrastructure Process Modelling Framework (PMF) Orchestration Guide .

C.1.1 Mapping the Transaction Statuses and Transaction Outcomes

After you provide the new transaction status and outcome in step 4, you need to map the values in the required tables to update the value on the **PMF** page.

To update the status on the **PMF** page, populate the following status in the Config schema:

1. Run `select * from AAI_WF_STATUS_B t where t.v_app_package_id = 'OFS_SAC'` and `select * from AAI_WF_STATUS_TL where t.v_app_package_id = 'OFS_SAC'` queries.
2. In the `AAI_WF_STATUS_B` table, populate a unique entry in the `v_status_id` column for each new status and map the same entry in the `AAI_WF_STATUS_TL` table for a column. For example, populate the entry `OFS_SAC` in the `v_app_package_id` column.
3. When you map the new status, it appears on the PMF page.
   - Ensure that data is provided in all required columns in the `AAI_WF_STATUS_TL` table.
   - When doing the mapping in any other configuration tables, ensure that you provide the same status that is mentioned in the `v_status_name` column in the `AAI_WF_STATUS_TL` table.

To update the outcome on the PMF page, populate the following status in the Config schema:

1. Run the `select * from AAI_WF_OUTCOME_B t` and where t.v_app_package_id = 'OFS_SAC' queries.
2. In the `AAI_WF_OUTCOME_B` table, populate a unique outcome ID in the v_outcome_id column for each new status and map the same entry in the `AAI_WF_OUTCOME_TL` table.
   - Ensure that data is provided in all required columns in the `AAI_WF_OUTCOME_TL` table.
   - When doing the mapping in any other configuration tables, ensure that you provide the same status that is mentioned in the `AAI_WF_OUTCOME_TL` table.
   - After you complete the above steps, refresh the application and web servers.

C.1.2 Adding Data Fields for the PMF Status

To add a new data field for each new status, for example, TF_BLOCKED_NEW, click the **Data Fields** subtab in the **Process Modeller** page and click **Add**. For information on the fields, see the **Data Fields** section in the Oracle Financial Services Analytical Applications Infrastructure Process Modelling Framework (PMF) Orchestration Guide .

> **Note**
>
> If the data field name contains more than one word, give an underscore (_) between each word. The name will not be valid if you provide a space between each word.

You can also edit an existing data field, follow these steps:

1. Select the radio button of the data field that you want to edit.
2. Click **Edit**.

C.1.3 Adding Application Rules for the PMF Status

To add a new application rule for each new status, for example, RB_TO_Block_New, click the **Application Rule** subtab in the **Process Modeller** page and click **Add**. For information on the fields, see the **Application Rules** section in the Oracle Financial Services Analytical Applications Infrastructure Process Modelling Framework (PMF) Orchestration Guide.

C.1.3.1 Mapping Rule Types to Application Rules

If you select a new rule type for the application rule, you must then map it to the rule. To map a rule, run the `select * from aai_aom_app_comp_attr_mapping` query.

If a static rule is present with n_static_grp_id = 501, then run the `select * from AAI_AOM_STATIC` query.

C.1.3.2 Mapping User Groups to Application Rules

If you have also mapped a new user group to the rule, then you need to map the entry in the `DOMAIN_JUR_GRP_MAP` table. After you map the user group to the rule, run the `select * from DOMAIN_JUR_GRP_MAP` query to update the `DOMAIN_JUR_GRP_MAP` table.

The steps required to create a new user group are available in Creating New User Groups. For more information, see the **User Administrator** section in the Oracle Financial Services Analytical Applications Infrastructure User Guide.

C.1.4 Configurations Required for the Audit Tables

Before you update the tables, you must first provide a unique value in the `n_activity_id` column in the `SETUP_RT_AUD_ACTIVITY` table and then provide the same value in the `n_activity_id` column in the `SETUP_RT_AUD_STEPS` table.

After this is done, run the `select * from SETUP_RT_AUD_ACTIVITY` query to update the `SETUP_RT_AUD_ACTIVITY` table and run the `select * from SETUP_RT_AUD_STEPS` query to update the `SETUP_RT_AUD_STEPS` table.

After the tables are updated, provide two entries, 1 and 2, in the n_step_sequence column in the `SETUP_RT_AUD_STEPS` table.

> **Note**
>
> The value provided in the `v_status_name` column in the `AAI_WF_STA- TUS_TL` table must be a combination of one of the following values:
>
> - The value provided in `v_sanction_status_name` in `dim_sanc- tions_status` table and the name of the transaction workflow invoked for entry 1.
> - The value provided in `v_sanction_status_name` in `dim_sanc- tions_status` table and the name of the transaction workflow completed for entry 2.

C.1.5 Configurations Required for the setup_rt_params Table

To configure the table in the ATOMIC schema, follow these steps:

1. Provide the function code in the `v_attribute_value1` column where `v_attribute_name1 = 'TF_ FUNCTION_CODES'`.
2. Provide the status codes according to the `v_attribute_name1` value in the `v_attribute_value1` column where `v_attribute_name1 = 'TF_FUNCTION_AND_STATUS_CODES'`.
3. Provide all status codes in the `v_attribute_value1` column against each function code in the `v_attribute_name1` column. This displays the dynamic status filter.
4. Provide the code for each status to be displayed to the user for that function code in the `v_at- tribute_value1` column.
5. Provide the code for each status to be displayed to the user in the *Transaction Summary* window in the `v_attribute_value2` column.
6. Provide the code for each action that must be displayed to the user for that transaction in the `v_attribute_value3` column.
7. To create an order for the transactions, follow these steps:
   - Provide `TF USERWORKFLOWCLAUSE` in the `v_param_name` column.
   - Provide `TF_ORDERBY_PRECEDENCE` in the `v_attribute_name1` column.
   - Provide `TF_ORDERBY_FUNCCODE` in the `v_attribute_name2` column.
   - Provide the function code for which you want to do the order in the `v_attribute_value2` column. For example, use `TFLTANYSE` for the analyst user.
   - Provide `TF_ORDERBY_CLAUSES` in the `v_attribute_name3` column.
   - Provide the *order by query* in the `v_attribute_value3` column. For a sample value, see the value for the `TFLTANYSE` function code.
8. Update the fields in the feedback response JSON for blocked and released payments in the `v_attribute_value1` column in the `FEEDBACK_RESPNSE_CONFIGURATION` row and restart the WebLogic server.
9. Update the `v_attribute_value1` column as **Y** where `v_param_name = ' ECM_SANCTIONS_PP'`,if ECM pack is installed in the same server where Sanctions also installed.

C.1.6 TIME_ZONE Configurations Required for the dim_- sanctions_status Table

To configure the table in the ATOMIC schema, follow these steps:

1. Create a unique value for the new PMF status in the `n_sanction_status_code` column. This value must be the same in the `AAI_WF_STATUS_B` and `AAI_WF_STATUS_TL` columns. For more information, see Configurations Required for the Audit Tables.
2. Provide the activity name as mentioned in step 4 of the Configuring the Human Task in the PMF Page section in the `v_remarks` column.
3. Provide a unique data field value in the `v_applicable_params` column where `n_sanction_staus_key = 101` (ApplicationParams) and `n_sanction_staus_key = 202 (PMFParams)`.
4. To update the image path for the alert status, update the `v_sanction_status_img_path` value.
5. To update the image path for the list of actions, update the `v_sanction_dropdown_img_path` value.

6. To configure the action status:
   - Provide the value `StatusActon` if a status action must be fired.
   - Provide the value `PendingTrxnsCount` if the count of pending transactions is required for a particular action.
   - Provide the value `PendingTrxnsSuspiciousCountAndStatusActon` if the count of pending transactions and count of pending suspicious transactions are both required.
7. In the `v_data_field` column, give the same data field created in the PMF page data field section.
8. Update the `v_owner_update` column in the `fsi_rt_alerts` table if the owner must be updated.
9. Provide the audit message in the `v_audit_msg` column. This value must be the same as the value provided in the `v_sanction_status_name` column. For more information, see Configurations Required for the Audit Tables .

> **Note**
>
> For a new status, the `v_applicable_params` column must be left blank.

C.1.7 Creating New User Groups

To add a new user group, follow these steps:

1. Create a function.
2. Create a role.
3. Map the function to the role.
4. Create a user.
5. Map the user to a user group and a role.
6. Map the user to a user group and a domain.
7. Map the user to a user group.

C.1.8 Other Configurations

The user group is now created. After it is created, follow these steps:

1. Map the group in the `domain_jur_grp_map` table.
2. Login to the Config schema.
3. Run the `select * from cssms_folder_function_map` query.
4. Add the new function to the `Transaction Filter` folder (TransactionFiltering `TFLTADMIN`).
5. Run the `select t.v_access_code,t.v_menu_id from aai_menu_b t where t.v_menu_id in('OFS_TFLTSCRN','OFS_TFLT')` query.
6. Add the new function in the `v_access_code` column.
7. To map the new function, add an entry in the `v_access_code` column in the `aai_menu_b` table by running a query with the entry mentioned in the following format: `select * from aai_menu_b t where t.v_menu_id like '%OFS_TFLT%';` query.

8. To map the function to a folder, run a query with the function mentioned in the following format: `select * from cssms_folder_function_map p where p.v_function_code like '%TF%';` query.

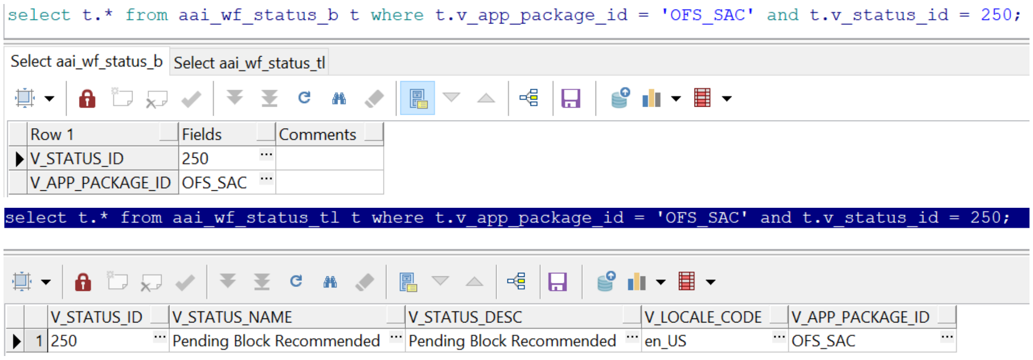
D

PMF Configurations for Pool of Analyst

To configure the PMF Pool of Analyst configuration to set the new statuses, follow these steps:

1. Perform the following queries and introduce new status in the following tables.
   - Select * `from AAI_WF_STATUS_B t where t.v_app_package_id = 'OFS_SAC';`
   - Select * `from AAI_WF_STATUS_TL t where t.v_app_package_id = 'OFS_SAC';`
   - Create unique `v_status_id` in `AAI_WF_STATUS_B` table and map the same in the `AAI_WF_STATUS_TL` table and fill all the other columns data. This data will show in the PMF screen while mapping new status.

Figure D-1 Example 1



```
select t.* from aai_wf_status_b t where t.v_app_package_id = 'OFS_SAC' and t.v_status_id = 250;
```

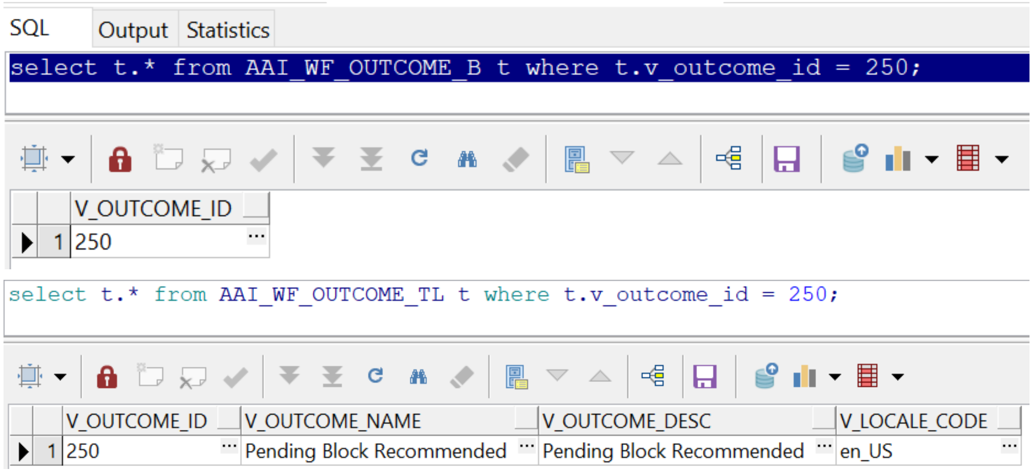
Row 1	Fields	Comments
V_STATUS_ID	250	
V_APP_PACKAGE_ID	OFS_SAC	

```
select t.* from aai_wf_status_tl t where t.v_app_package_id = 'OFS_SAC' and t.v_status_id = 250;
```

	V_STATUS_ID	V_STATUS_NAME	V_STATUS_DESC	V_LOCALE_CODE	V_APP_PACKAGE_ID
1	250	Pending Block Recommended	Pending Block Recommended	en_US	OFS_SAC

2. Perform the following query and introduce new Outcome in both the following tables.
   - Select * `from AAI_WF_OUTCOME_B ;`
   - Select * `from AAI_WF_OUTCOME_TL;`
   - Create unique outcome ID in `AAI_WF_OUTCOME_B` table and map the same in `AAI_WF_OUT- COME_TL` table and provide other columns data.

Figure D-2 Example 2



```
select t.* from AAI_WF_OUTCOME_B t where t.v_outcome_id = 250;
```

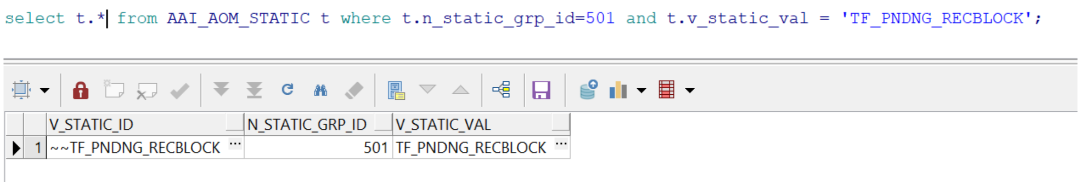
	V_OUTCOME_ID
1	250

```
select t.* from AAI_WF_OUTCOME_TL t where t.v_outcome_id = 250;
```

	V_OUTCOME_ID	V_OUTCOME_NAME	V_OUTCOME_DESC	V_LOCALE_CODE
1	250	Pending Block Recommended	Pending Block Recommended	en_US

3. Perform the following query and add a new entry for the new status to come up in the `TF_AC- TION` drop-down list while adding new Application rule. Select `* from AAI_AOM_STATIC t` where `t.n_static_grp_id=501;`

Figure D-3 Example 3



```
select t.* from AAI_AOM_STATIC t where t.n_static_grp_id=501 and t.v_static_val = 'TF_PNDNG_RECBLOCK';
```

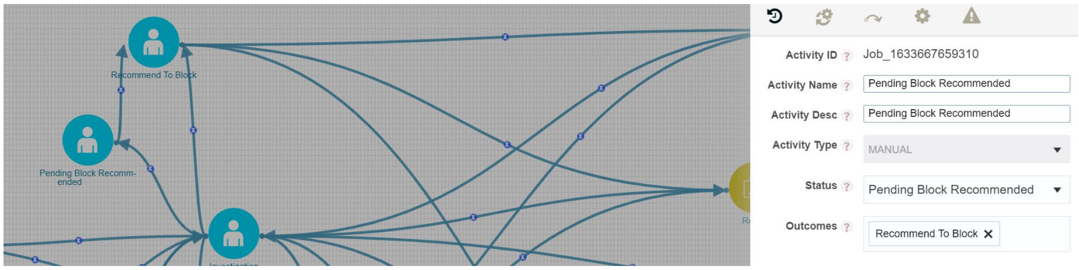
	V_STATIC_ID	N_STATIC_GRP_ID	V_STATIC_VAL
1	~~TF_PNDNG_RECBLOCK	501	TF_PNDNG_RECBLOCK

4. Create Human task in PMF screen that you want to introduce in-between existing status or you want to introduce new status or create separate status.
   Activity

   Activity Name* Activity Description
   Status* - New Status Name.

   Outcomes - Where has to go (Destination Status).
   Example: If we have to introduce a new status between Investigation and Recommend to Block as Pending Recommend to Block, first add the new activity as shown in the following Figures (Pending Block Recommended).

Figure D-4 Activity Statuses



Activity ID	Job_1633667659310
Activity Name	Pending Block Recommended
Activity Desc	Pending Block Recommended
Activity Type	MANUAL
Status	Pending Block Recommended
Outcomes	Recommend To Block ✕

Transitions

Add ->

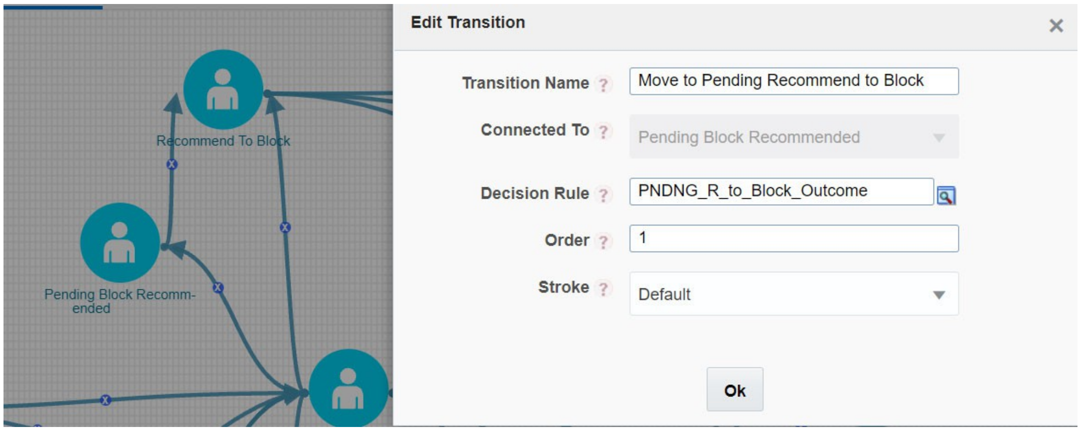
Transition Name - Unique Name for the particular Transition. Connected To – Destination status.

Decision Rule - Map to decision rule for particular status. Order - 1

Stroke – Default.

Example: First Transition between **Investigation** and **Pending Block Recommended** the next one between **Pending Block Recommended** and **Recommend to Block.**

Figure D-5 Edit Transaction – Pending Block Recommended



Edit Transition

Transition Name: Move to Pending Recommend to Block

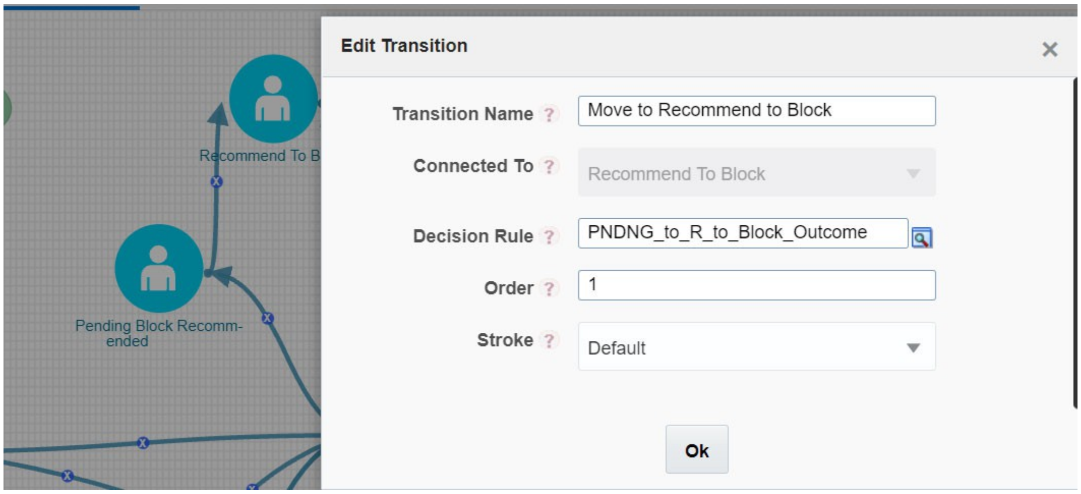
Connected To: Pending Block Recommended

Decision Rule: PNDNG_R_to_Block_Outcome

Order: 1

Stroke: Default

Figure D-6 Edit Transaction – Recommend To Block



Edit Transition

Transition Name: Move to Recommend to Block

Connected To: Recommend To Block

Decision Rule: PNDNG_to_R_to_Block_Outcome

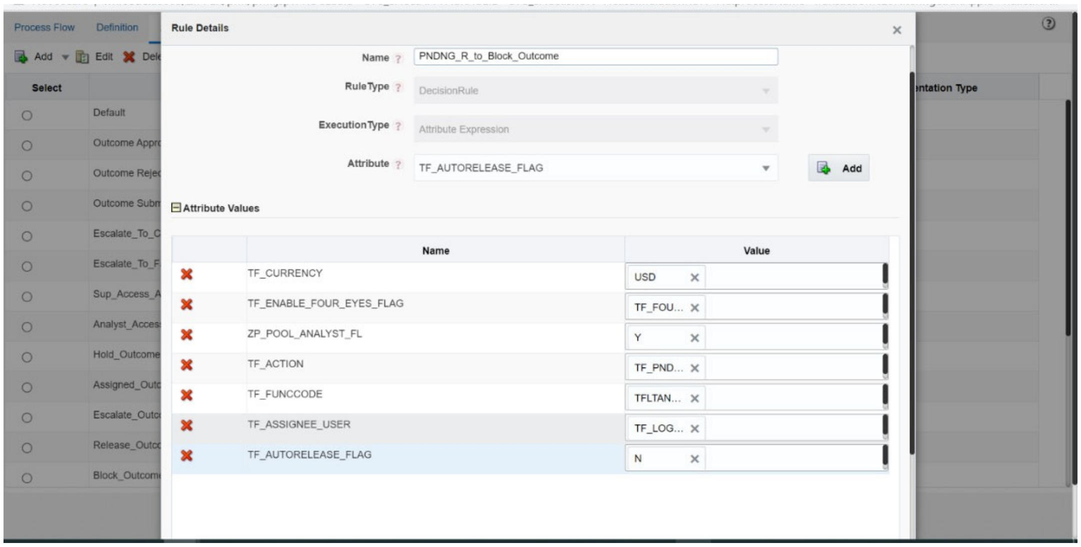
Order: 1

Stroke: Default

In Transition Decision Rule Map the specified rule for the current status. Or create as per business requirement.

Example: For the decision rules, add the following 2 decision rules.

Figure D-7 Rule Details – Decision Rule 1



Name: PNDNG_R_to_Block_Outcome

RuleType: DecisionRule

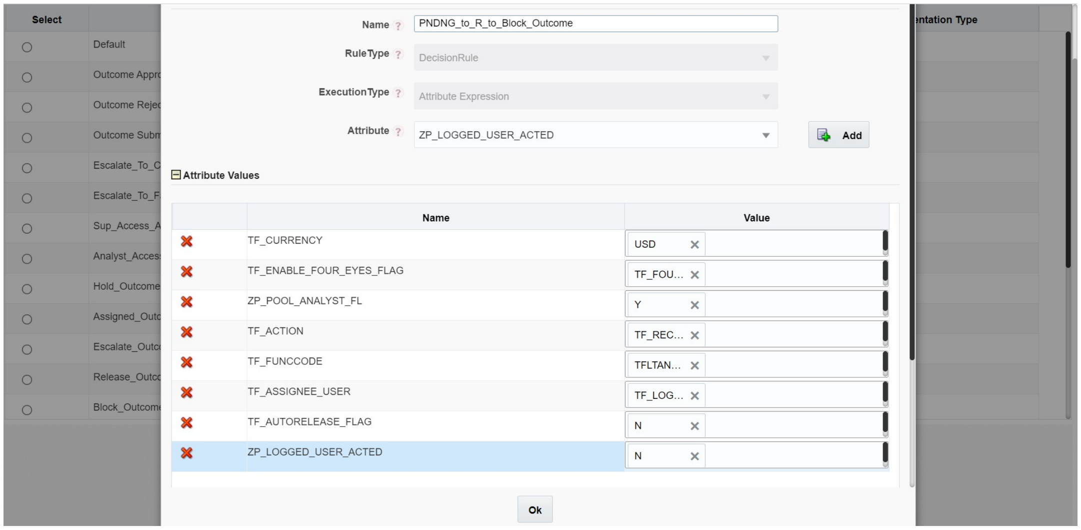
ExecutionType: Attribute Expression

Attribute: TF_AUTORELEASE_FLAG

Attribute Values

	Name	Value
✖	TF_CURRENCY	USD
✖	TF_ENABLE_FOUR_EYES_FLAG	TF_FOU...
✖	ZP_POOL_ANALYST_FL	Y
✖	TF_ACTION	TF_PND...
✖	TF_FUNCCODE	TFLTAN...
✖	TF_ASSIGNEE_USER	TF_LOG...
✖	TF_AUTORELEASE_FLAG	N

Figure D-8 Rule Details – Decision Rule 2



Name: PNDNG_to_R_to_Block_Outcome

RuleType: DecisionRule

ExecutionType: Attribute Expression

Attribute: ZP_LOGGED_USER_ACTED

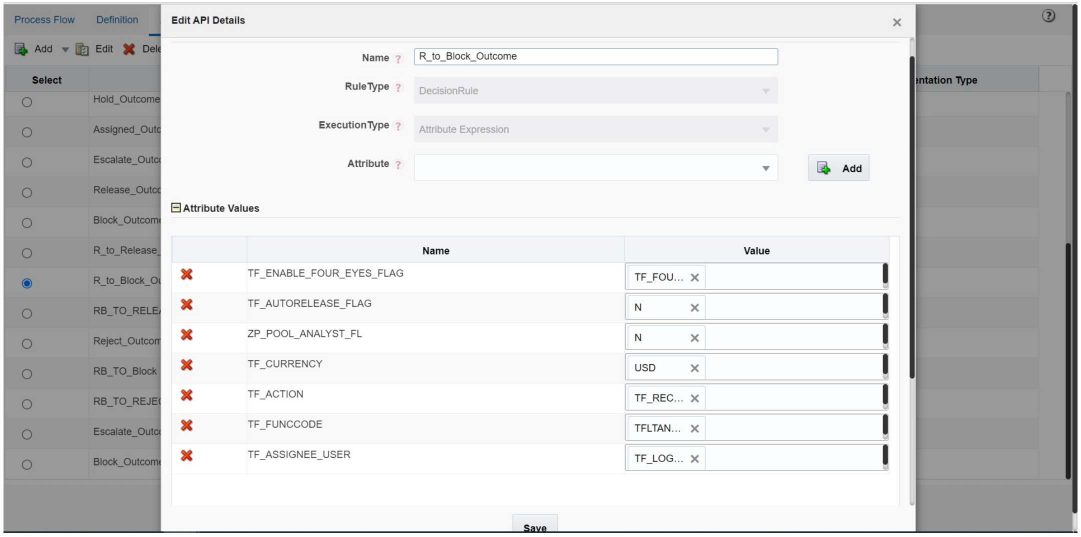
Attribute Values

	Name	Value
✖	TF_CURRENCY	USD
✖	TF_ENABLE_FOUR_EYES_FLAG	TF_FOU...
✖	ZP_POOL_ANALYST_FL	Y
✖	TF_ACTION	TF_REC...
✖	TF_FUNCCODE	TFLTAN...
✖	TF_ASSIGNEE_USER	TF_LOG...
✖	TF_AUTORELEASE_FLAG	N
✖	ZP_LOGGED_USER_ACTED	N

Edit the existing decision rule, by adding the ZP_POOL_ANALYST_FL.

> **Note**
>
> The attribute ZP_LOGGED_USER_ACTED value is Y then the user has acted first on the POA status.

Figure D-9 Edit API Details



Name: R_to_Block_Outcome

RuleType: DecisionRule

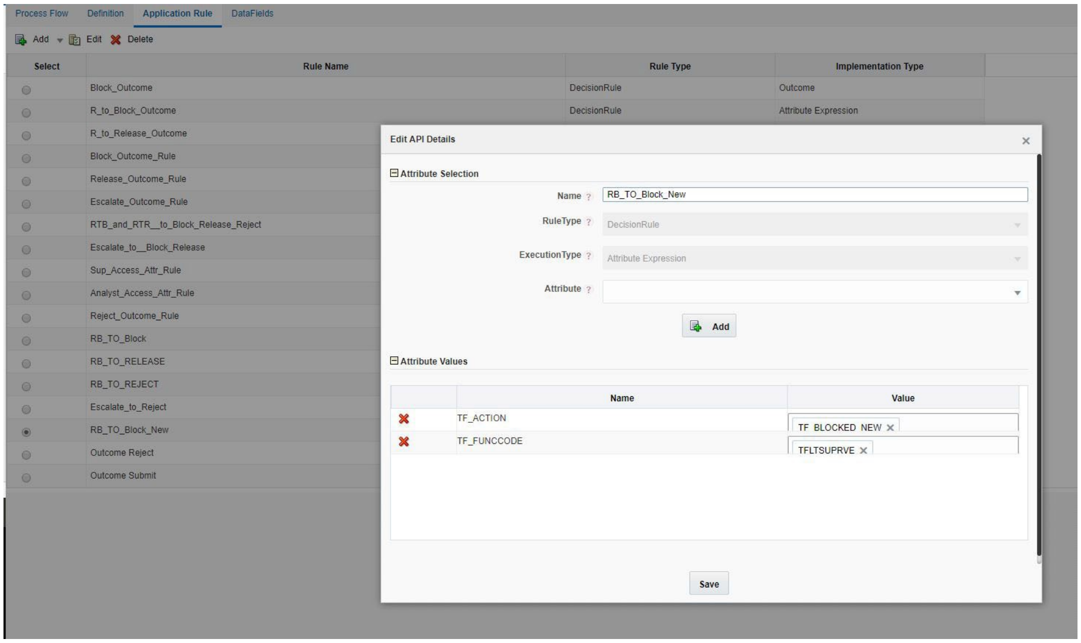
ExecutionType: Attribute Expression

Attribute:

Attribute Values

	Name	Value
✖	TF_ENABLE_FOUR_EYES_FLAG	TF_FOU...
✖	TF_AUTORELEASE_FLAG	N
✖	ZP_POOL_ANALYST_FL	N
✖	TF_CURRENCY	USD
✖	TF_ACTION	TF_REC...
✖	TF_FUNCCODE	TFLTAN...
✖	TF_ASSIGNEE_USER	TF_LOG...

Figure D-10 Edit API Details – Adding Attribute Values



Select	Rule Name	Rule Type	Implementation Type
○	Block_Outcome	DecisionRule	Outcome
○	R_to_Block_Outcome	DecisionRule	Attribute Expression
○	R_to_Release_Outcome		
○	Block_Outcome_Rule		
○	Release_Outcome_Rule		
○	Escalate_Outcome_Rule		
○	RTB_and_RTR__to_Block_Release_Reject		
○	Escalate_to__Block_Release		
○	Sup_Access_Attr_Rule		
○	Analyst_Access_Attr_Rule		
○	Reject_Outcome_Rule		
○	RB_TO_Block		
○	RB_TO_RELEASE		
○	RB_TO_REJECT		
○	Escalate_to_Reject		
●	RB_TO_Block_New		
○	Outcome Reject		
○	Outcome Submit		

Attribute Selection

Name: RB_TO_Block_New

RuleType: DecisionRule

ExecutionType: Attribute Expression

Attribute:

Attribute Values

	Name	Value
✖	TF_ACTION	TF BLOCKED NEW
✖	TF_FUNCCODE	TFLTSUPRVE

5. Access for the new status (example: Pending Review (96)) should be given to **TFLTANYSE** in order to take/update action on events.

6. Follow these steps:

   a. select `* from setup_rt_params` where `V_PARAM_NAME = 'TF_FUNCTION_AND_STATUS_CODES' and V_ATTRIBUTE_NAME1 = 'TFLTANYSE';`

   b. Append `V_ATTRIBUTE_VALUE3` with the newly added Pending review Status.

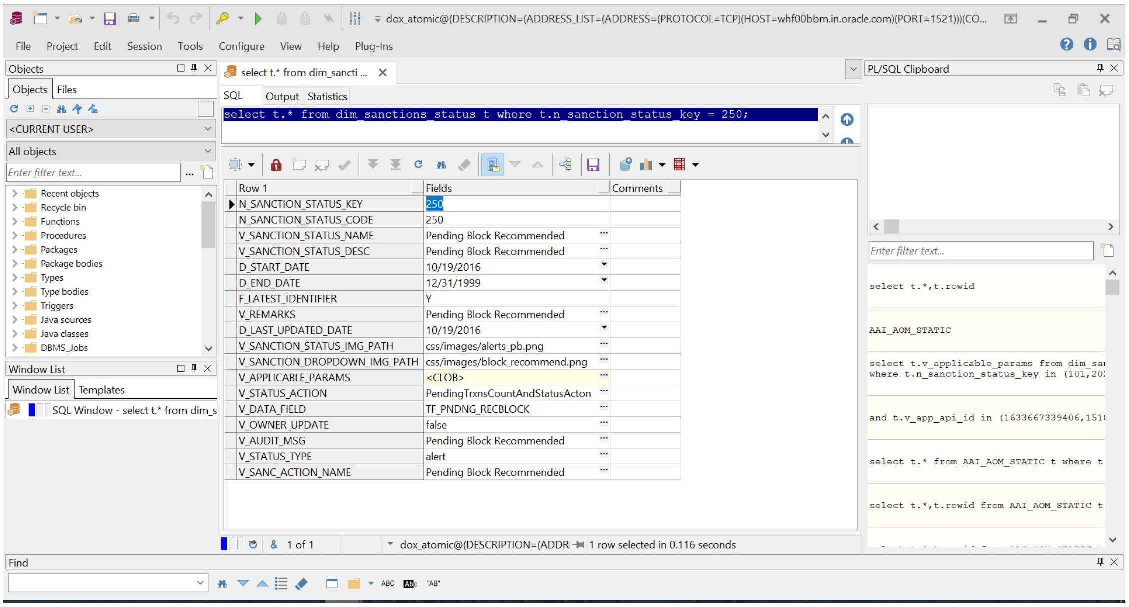
   c. Example: 2,96

> **Note**
>
> - To get the V_ATTRIBUTE_VALUE3 ; refer the dim_sanctions_sta- tus table.
> - This is the Customized example for Pending Review (96) to be added manu- ally.

D.1 Mapping the dim_sanctions_status Table

Create a new entry for newly created status and provide the unique `n_sanction_status_code`. The new n_sanction_status_code must be the same as `AAI_WF_STATUS_B` and `AAI_WF_STATUS_TL` that you have created while configuring PMF screen.

Figure D-11 dim_Sanctions_status Table



```
select t.* from dim_sanctions_status t where t.n_sanction_status_key = 250;
```

Row 1	Fields	Comments
N_SANCTION_STATUS_KEY	250	
N_SANCTION_STATUS_CODE	250	
V_SANCTION_STATUS_NAME	Pending Block Recommended	
V_SANCTION_STATUS_DESC	Pending Block Recommended	
D_START_DATE	10/19/2016	
D_END_DATE	12/31/1999	
F_LATEST_IDENTIFIER	Y	
V_REMARKS	Pending Block Recommended	
D_LAST_UPDATED_DATE	10/19/2016	
V_SANCTION_STATUS_IMG_PATH	css/images/alerts_pb.png	
V_SANCTION_DROPDOWN_IMG_PATH	css/images/block_recommend.png	
V_APPLICABLE_PARAMS	<CLOB>	
V_STATUS_ACTION	PendingTrxnsCountAndStatusActon	
V_DATA_FIELD	TF_PNDNG_RECBLOCK	
V_OWNER_UPDATE	false	
V_AUDIT_MSG	Pending Block Recommended	
V_STATUS_TYPE	alert	
V_SANC_ACTION_NAME	Pending Block Recommended	

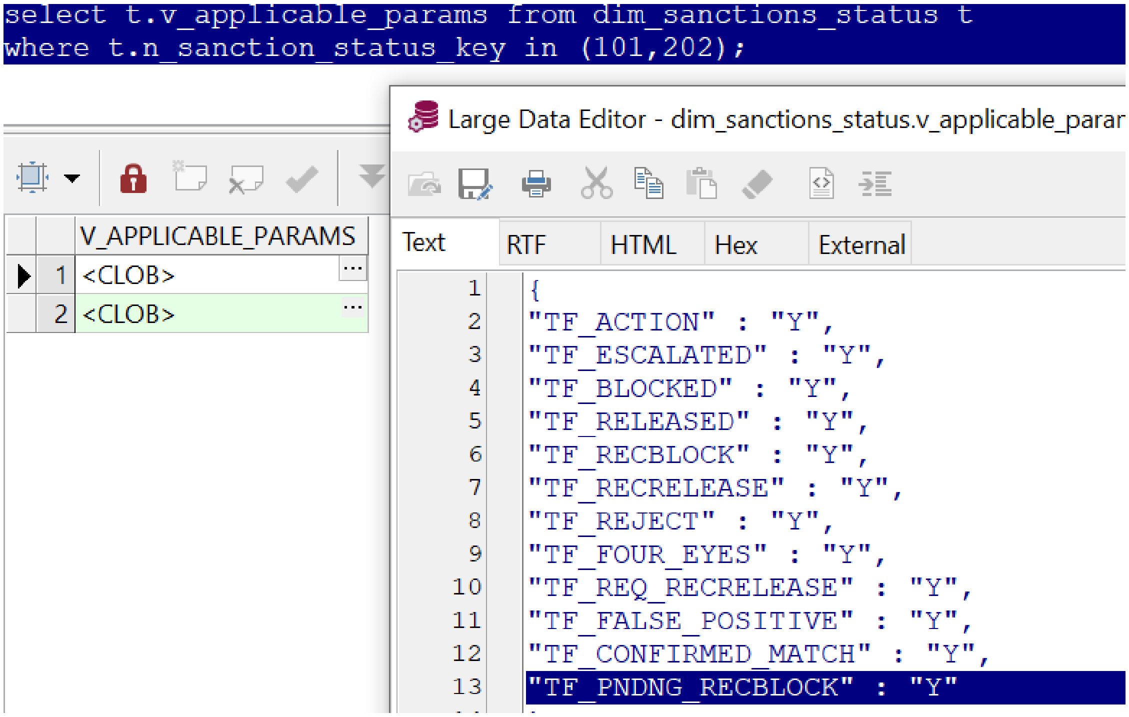
```
1 of 1    dox_atomic@(DESCRIPTION=(ADDR    1 row selected in 0.116 seconds
```

```
select t.*,t.rowid
AAI_AOM_STATIC
select t.v_applicable_params from dim_sa
where t.n_sanction_status_key in (101,20
and t.v_app_api_id in (1633667339406,151
select t.* from AAI_AOM_STATIC t where t
select t.*,t.rowid from AAI_AOM_STATIC t
```

D.2 Adding Data Fields to the JSON Object

To add a new data field to the JSON object in the following clob columns, follow these steps: Select `t.v_applicable_params from dim_sanctions_status t` where `t.n_sanction_status_key in (101,202);`

Figure D-12   Applicable Params



```
select t.v_applicable_params from dim_sanctions_status t
where t.n_sanction_status_key in (101,202);
```

	V_APPLICABLE_PARAMS
1	<CLOB>
2	<CLOB>

```
{
"TF_ACTION" : "Y",
"TF_ESCALATED" : "Y",
"TF_BLOCKED" : "Y",
"TF_RELEASED" : "Y",
"TF_RECBLOCK" : "Y",
"TF_RECRELEASE" : "Y",
"TF_REJECT" : "Y",
"TF_FOUR_EYES" : "Y",
"TF_REQ_RECRELEASE" : "Y",
"TF_FALSE_POSITIVE" : "Y",
"TF_CONFIRMED_MATCH" : "Y",
"TF_PNDNG_RECBLOCK" : "Y"
```

Also provide all the following fields:

- `v_sanction_status_img_path` - Image path for status of the alert image.
- `v_sanction_dropdown_img_path` - Image path for action clicked list of action image.
- `v_applicable_params` – keep it blank for new status column.
- `v_status_action` - If only particular action has to be fired, then provide `statusActon`, if `PendingTrxnsCount` is required for the particular action, then provide `PendingTrxnsCount`, and if `PendingTrxnsCount` and `PendingSuspiciousCount` both is required, then provide `PendingTrxnsSuspiciousCountAndStatusActon`.
- `v_data_field` - Provide the same data field as added in AAI_AOM_STATIC table.
- `v_owner_update - fsi_rt_alerts table v_owner` column has to be updated or not.
- `v_remarks` column name should be the same as that you have given name in pmf screen **Activity Name.**
- Always provide `v_owner_update` true only when status is as like end mode (Ex: Blocked, Released) else provide as false.
- `v_audit_msg` - Provide the Audit Message (Audit message should be same as `v_sanction_staus_name` value).

D.3 List of Attributes Passed to Workflow

The following table provides the list of Attributes passed to workflow:

Table D-1 SWIFT Message Types

Attributes	Description
TF_ACTION	Action to be performed.
WF_DSNID	Infodom value.
WF_MESSAGE_TYPE	Message Type.
WF_MESSAGE_REFERENCE	Message Reference.
WF_USER_COMMENT	System hardcoded comment.
WF_APPLICATION_URL	Application url hardcoded logic.
TF_LOGIN_USER	Logged in user.
TF_FUNCCODE	Logged in user function code.
TF_ASSIGNEE_USER	Logged in user.
TF_ENABLE_FOUR_EYES_-FLAG	Y/N value based on the configuration.
TF_CURRENCY	Currency of the message.
WF_OUTCOME_ID	Outcome Id for the action.
TF_AUTORELEASE_FLAG	Y/N based on the configuration for the message.
TF_AMOUNT	Amount of the message.
TF_WATCHLIST_TYPE	Watchlist type of the event with maximum score of the message.
TF_WATCHLIST_SUB_TYPE	Watchlist sub type of the event with maximum score of the message.
TF_MESSAGE_TYPE	Message Type of the message.
TF_MSG_CATEGORY	Message Category of the message.
TF_MSG_PRIORITY	Message Priority of the message.
TF_JURISDICTION	Jurisdiction of the message.
TF_BUSINESS_DOMAIN	Business Domain of the message.
TF_ALERT_TYPE	Alert Type of the message (1 or 2).
ZP_POOL_ANALYST_FL	Y/N based on the configuration in setup_rt_params.
ZP_LOGGED_USER_ACTED	if the logged in user is the same person who performed the previous action then ZP_LOGGED_USER_ACTED = Y else its N.
TF_GRP_MSG_ID	Group Message Id of the message.

D.4 Attribute to Configure the Auto Refresh in Queue Management

The following table provides the list of Attribute to configure the Auto Refresh in Queue Management:

Table 56:

Table D-2 Q_AUTO_REFRESH_TIME Attribute

Attributes	Description
Q_AUTO_REFRESH_TIME	Provide the time in mille second for the attribute in CS_APPLN_PARAMS table. By default it’s 25000 i.e 25 seconds but the value is editable.

E
Delta Watch List Configurations

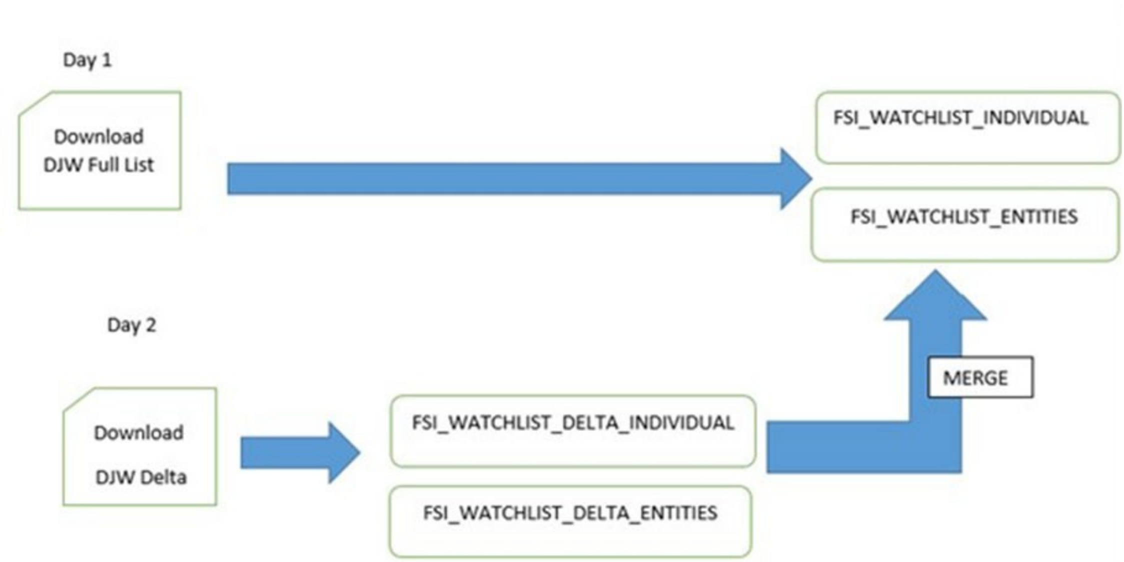
> **Note**
>
> These configurations are performed when you do not want to download the full watch list, and only want to download the delta watch list. This helps to reduce the download time and is not part of the screening process.

Oracle recommends that you always use the full watch list during the screening process. Due to the clustering strategy which is implemented in the screening process, you do not need to download the delta watch list. There are certain cases in which you are required to download the delta watch list files, for example, if the full watch list files are not yet available for download or if you want to save time.

Customers who download the delta watch list files must first download the full watch list files and then download the delta watch list files. The delta watch list is then merged into the full watch list before screening.

The following image shows the information flow for the delta watch list:

Figure E-1 Flow for Delta Watch List



When you download the full watch list, data is stored in the `FSI_WATCHLIST_INDIVIDUAL` and `FSI_WATCHLIST_ENTITIES` tables. When you download the delta watch list, data is first stored in the `FSI_WATCHLIST_DELTA_INDIVIDUAL` and `FSI_WATCHLIST_DELTA_ENTITIES` tables. Then, based

on the value in the ACTION Flag tag in the delta watch list, it merges with the full watch list. The ACTION flag key is a non-editable value, and can be one of the following values:

- **new**: If the value is `new`, it means that these records are new and are added to the full watch list when the delta files are merged with the full watch list.
- **chg**: If the value is `chg`, it means that these records are modified and are added to the full watch list when the delta files are merged with the full watch list.
- **del**: If the value is `del`, it means that these records are no longer active and are removed from the full watch list when the delta files are merged with the full watch list.

> **Note**
>
> You must always run the full watch list files before you run the delta watch list files. The full watch list files must be downloaded if, for example, the download of the delta watch list files has failed for multiple days. You can also run the full watch list once every week to ensure that the complete data has been processed.

The following watchlist management jobs are used for the full list and the delta list:

- Analyze Reference Data Quality
- Download, Prepare, Filter, and Export All Lists
- Generate StopPhrases
- The following watchlist management job is used for the full list:
  - Load List data from Stg to Processed table
- The following Transaction Filtering job is used for the full list and the delta list:
  - Main

Before you run the delta watchlist files, ensure that you run the full watchlist files. You can run the delta watch list files if, for example, the delta downloads have failed for multiple days or the filter criteria are changed. You can also run the delta watch list once every week to ensure that the complete data has been processed.

E.1 Configurations for the Full and Delta Watch Lists

The following configurations must be done for both full and delta watch list updates in the `watchlist-management.properties` run profile. The run profile is available in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory when you log in to the WinSCP server.

- Set `phase.Initialise\ staged\ data.enabled = N` to disable the .jmp file updates.
- Set `phase.Initialise\ staged\ data\ DB.enabled = Y` to initialize the database.
- Set `phase.Initilize\ Prepared\ List\ Data.enabled = N` to disable the .jmp file updates.
- Set `phase.Initilize\ Prepared\ List\ Data\ DB.enabled = Y` to prepare the database.

E.1.1 Running the Full Watch list

To run the full watch list, follow these steps:

1. Set the following properties in the `watchlist-management.properties` file:
   - `phase.DJW\ -\ Download.enabled = Y.`

   - `phase.DJW\ -\ Download\ Delta.enabled = N.`
   - `phase.DJW\ -\ Stage\ reference\ lists.enabled = Y.`
   - `phase.DJW\ -\ Sanction_List_Reference.enabled = Y`
   - `phase.DJW\ -\ Keywords_Preparation.enabled = Y`
   - `phase.*.export.*.ind_table_name = FSI_WATCHLIST_INDIVIDUAL.`
   - `phase.*.export.*.entities_table_name = FSI_WATCHLIST_ENTITIES.`
   - `phase.Import1_Full_DB.enabled = Y`
   - `phase.Import2_Full_DB.enabled = Y`
   - `phase.Import3_Full_DB.enabled = Y`

2. Set the following properties in the `transaction-screening.properties` file:
   - `phase.DJW\ -\ Load\ without\ filtering.enabled = N`
   - `phase.DJW\ -\ Load\ without\ filtering\ DB.enabled = Y`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 1).enabled = N`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y`
3. Set the following properties in the `transaction-screening-batch.properties` file:
   - `phase.DJW\ -\ Load\ without\ filtering.enabled = N`
   - `phase.DJW\ -\ Load\ without\ filtering\ DB.enabled = Y`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 1).enabled = N`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y`
   - `phase.DJW\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y`

E.1.2 Running the Delta Watch List

To run the delta watch list, set the following properties in the `watchlist-management.properties` file:

- `phase.DJW\ -\ Download.enabled = N.`
- `phase.DJW\ -\ Download\ Delta.enabled = Y.`
- `phase.DJW\ -\ Stage\ reference\ lists.enabled = Y.`
- `phase.DJW\ -\ Sanction_List_Reference.enabled = Y`
- `phase.DJW\ -\ Keywords_Preparation.enabled = Y`
- `Set phase.*.export.*.ind_table_name = FSI_WATCHLIST_DELTA_INDIVIDUAL.`
- `Set phase.*.export.*.entities_table_name = FSI_WATCHLIST_DELTA_ENTI- TIES.`
- `phase.Import1_Full_DB.enabled = N`
- `phase.Import2_Full_DB.enabled = N`
- `phase.Import3_Full_DB.enabled = N`
- `phase.Import1_Delta_DB.enabled = Y`
- `phase.Import2_Delta_DB.enabled = Y`

- `phase.Import3_Delta_DB.enabled = Y`

E.1.3 Merging the Delta Watch List to the Full Watch List

To merge the delta watch list with the full watch list, set the following properties in the `watchlist- management.properties` file:

- `phase.Delta\ Merge.enabled = Y.`
- `phase.Linked\ Profiles.enabled = Y.`

E.2 Delta Watch List Configurations for the World-Check Watch List

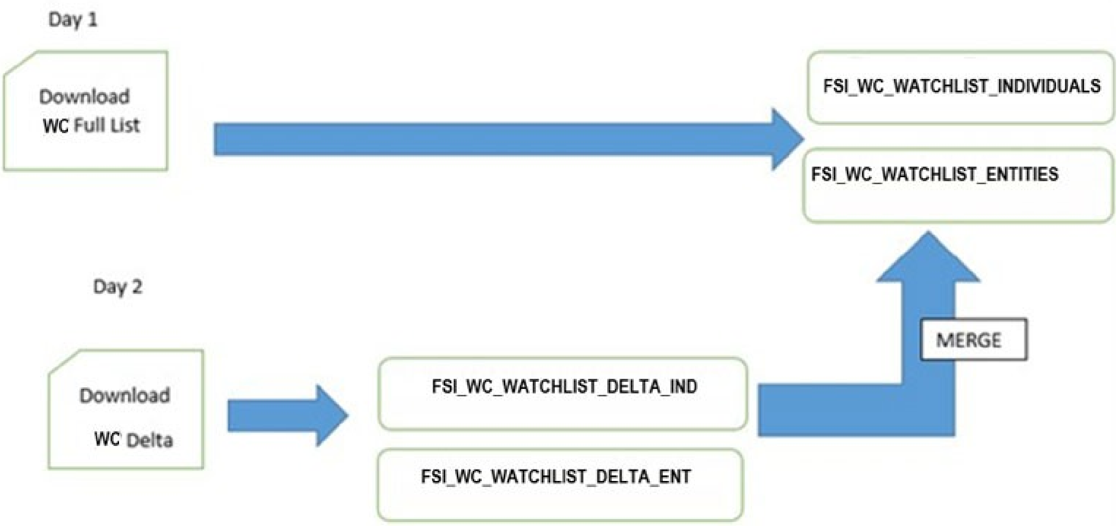
> **Note**
>
> These configurations are performed when you do not want to download the full watch list, and only want to download the delta watch list. This helps to reduce the download time and is not part of the screening process.

Transaction Filtering recommends that you always use the full watch list during the screening process. Due to the clustering strategy, which is implemented in the screening process, you must not download the delta watch list. There are certain cases in which you must download the delta watch list files, for example, if the full watch list files are not yet available for download or if you want to save time.

Customers who download the delta watch list files must first download the full watch list files and then download the delta watch list files. The delta watch list is then merged into the full watch list before screening.

The following image shows the information flow for the delta watch list:

Figure E-2 Flow for Delta Watch List


Day 1
Download WC Full List
FSI_WC_WATCHLIST_INDIVIDUALS
FSI_WC_WATCHLIST_ENTITIES
Day 2
Download WC Delta
FSI_WC_WATCHLIST_DELTA_IND
FSI_WC_WATCHLIST_DELTA_ENT
MERGE

When you download the full watch list, data is stored in the FSI_WC_WATCHLIST_INDIVIDUALS and FSI_WC_WATCHLIST_ENTITIES tables. When you download the delta watch list, data is first stored in the FSI_WC_WATCHLIST_DELTA_IND and FSI_WC_WATCHLIST_DELTA_ENT tables. Then the data is merged into the main table. For more information, see Merging the Delta Watch List to the Full Watch List.

> **Note**
>
> You must always run the full watch list files before you run the delta watch list files. The full watch list files must be downloaded if, for example, the download of the delta watch list files has failed for multiple days. You can also run the full watch list once every week to ensure that the complete data has been processed.

E.2.1 Configurations for the Full and Delta Watch Lists

The following configurations must be done for both full and delta watch list updates in the `watchlist-management.properties` run profile. The run profile is available in the `<domain_name>/edq/oedq.local.home/runprofiles/` directory when you log in to the WinSCP server.

- Set `phase.Initialise\ staged\ data.enabled = N` to disable the `.jmp` file updates.
- Set `phase.Initialise\ staged\ data\ DB.enabled = Y` to initialize the database.
- Set `phase.Initilize\ Prepared\ List\ Data.enabled = N` to disable the `.jmp` file updates.
- Set `phase.Initilize\ Prepared\ List\ Data\ DB.enabled = Y` to prepare the database.
- Set `phase.All\ List\ Entity\ and\ Individual\ reference\ data.enabled = N`.
- Set `phase.All\ List\ Entity\ and\ Individual\ reference\ data\ DB.enabled= Y`.
- Set `phase.DQ-Watchlist\ BIC\ Extraction\ JSON\ Preparation.enabled = N`.
- Set `phase.DQ-Watchlist\ BIC\ Extraction\ JSON\ Preparation\ DB.enabled = Y`.

E.2.2 Running the Full Watch List

To run the full watch list, follow these steps:

1. Set the following properties in the `watchlist-management - TF.properties` file:
   - `phase.WC\ -\ Download.enabled = Y.`
   - `phase.WC\ -\ Download\ Delta.enabled = N.`
   - `phase.WC\ -\ Stage\ reference\ lists.enabled = Y.`
   - `phase.*.export.*.wc_ind_table_name=FSI_WC_WATCHLIST_INDIVIDUAL`
   - `phase.*.export.*.wc_entities_table_name=FSI_WC_WATCHLIST_ENTITIES`
   - `phase.Import1_Full_DB.enabled = Y`
   - `phase.Import2_Full_DB.enabled = Y`
   - `phase.Import3_Full_DB.enabled = Y`

   To run the full watch list without filtering, set the following properties:

- `phase.WC\ -\ Prepare\ without\ filtering.enabled = N`
- `phase.WC\ -\ Prepare\ without\ filtering\ Full\ DB.enabled = Y`

To run the full watch list with filtering, set the following properties:

- `phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = N`
- `phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = N`
- `phase.WC\ -\ Prepare\ with\ filtering\ Full\ DB.enabled = Y`

To run the full watch list without filtering, set the following proper- ties:

- `phase.WC\ -\ Load\ without\ filtering.enabled = N`
- `phase.WC\ -\ Load\ without\ filtering\ DB.enabled = Y`

To run the full watch list with filtering, set the following properties:

- `phase.WC\ -\ Load\ with\ filtering\ (Part\ 1).enabled = N`
- `phase.WC\ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y`
- `phase.WC\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y`

2. Set the following properties in the `transaction-screening.properties` file:
   - `phase.WC\ -\ Load\ without\ filtering.enabled = N`
   - `phase.WC\ -\ Load\ without\ filtering\ DB.enabled = Y`
   - `phase.WC\ -\ Load\ with\ filtering\ (Part\ 1).enabled = N`
   - `phase.WC\ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y`
   - `phase.WC\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y`
3. Set the following properties in the `transaction-screening-batch.properties` file:
   - `phase.WC\ -\ Load\ without\ filtering.enabled = N`
   - `phase.WC \ -\ Load\ without\ filtering\ DB.enabled = Y`
   - `phase.WC \ -\ Load\ with\ filtering\ (Part\ 1).enabled = N`
   - `phase.WC \ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y`
   - `phase.WC \ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y`

E.2.3 Running the Delta Watch List

To run the delta watch list, follow these steps:

1. Set the following properties in the `watchlist-management - TF.properties` file:
   - `phase.WC\ -\ Download.enabled = N.`
   - `phase.WC\ -\ Download\ Delta.enabled = Y.`
   - `phase.WC\ -\ Stage\ reference\ lists.enabled = Y.`
   - `phase.*.export.*.wc_ind_table_name=FSI_WC_WATCHLIST_DELTA_IND`
   - `phase.*.export.*.wc_entities_table_name=FSI_WC_WATCHLIST_DELTA_ENT`
   - `phase.Import1_Full_DB.enabled = N`
   - `phase.Import2_Full_DB.enabled = N`
   - `phase.Import3_Full_DB.enabled = N`

  - `phase.Import1_Delta_DB.enabled = Y`
  - `phase.Import2_Delta_DB.enabled = Y`
  - `phase.Import3_Delta_DB.enabled = Y`
2. To run the delta watch list without filtering, set the following properties:
  - `phase.WC\ -\ Prepare\ without\ filtering.enabled = N`
  - `set phase.WC\ -\ Prepare\ without\ filtering\ Delta\ DB.enabled = Y`

To run the delta watch list with filtering, set the following properties:

- `phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = N`
- `phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = N`
- `phase.WC\ -\ Prepare\ with\ filtering\ Delta\ DB.enabled = Y`

E.2.4 Merging the Delta Watch List to the Full Watch List

To merge the delta watch list with the full watch list, set the following properties in the `watchlist- management.properties` file:

- `phase.WC\Delta\ Merge.enabled = Y.`
- `phase.WC\Linked\ Profiles.enabled = Y.`

F

Message Categories and Message Types

A user of the Transaction Filtering application can use the following message categories:

- SWIFT Message Types
- ISO20022 Message Types
- Fedwire Message Types
- US NACHA Message Types

Each message category has different message types defined. The following tables list the message categories and associated message types.

F.1 SWIFT Message Types

For the SWIFT message category, the message types numbered 1 to 8 are the ready-to-use message types that you can use after you log in. The other message types must be imported manually using the SWIFT migration utility. For information on the steps, see Running the Migration Utility for SWIFT, Fedwire and ISO20022 .

Table 57: SWIFT Message Types

Table F-1 SWIFT Message Types

S.No	Message Type	S.No	Message Type	S.No	Message Type	S.No	Message Type
1	MT101	**2**	MT102	**3**	MT103	**4**	MT103STP
5	MT104	**6**	MT105	**7**	MT107	**8**	MT110
9	MT111	**10**	MT112	**11**	MT190	**12**	MT191
13	MT192	**14**	MT195	**15**	MT196	**16**	MT198
17	MT199	**18**	MT200	**19**	MT201	**20**	MT202
21	MT202COV	**22**	MT203	**23**	MT204	**24**	MT205
25	MT205COV	**26**	MT210	**27**	MT290	**28**	MT291
29	MT292	**30**	MT295	**31**	MT296	**32**	MT298
33	MT299	**34**	MT300	**35**	MT304	**36**	MT305
37	MT306	**38**	MT320	**39**	MT321	**40**	MT350
41	MT362	**42**	MT395	**43**	MT396	**44**	MT399
45	MT400	**46**	MT410	**47**	MT412	**48**	MT416
49	MT420	**50**	MT430	**51**	MT455	**52**	MT456
53	MT490	**54**	MT491	**55**	MT492	**56**	MT495
57	MT496	**58**	MT498	**59**	MT499	**60**	MT515
61	MT516	**62**	MT526	**63**	MT536	**64**	MT537
65	MT540	**66**	MT541	**67**	MT542	**68**	MT543
69	MT544	**70**	MT545	**71**	MT546	**72**	MT547
73	MT548	**74**	MT564	**75**	MT566	**76**	MT568
77	MT581	**78**	MT590	**79**	MT591	**80**	MT592

Table F-1 (Cont.) SWIFT Message Types

S.No	Message Type	S.No	Message Type	S.No	Message Type	S.No	Message Type
81	MT595	82	MT596	83	MT599	84	MT604
85	MT605	86	MT606	87	MT607	88	MT608
89	MT671	90	MT695	91	MT696	92	MT699
93	MT700	94	MT701	95	MT705	96	MT707
97	MT708	98	MT710	99	MT711	100	MT720
101	MT721	102	MT730	103	MT732	104	MT734
105	MT740	106	MT742	107	MT747	108	MT750
109	MT752	110	MT754	111	MT756	112	MT759
113	MT760	114	MT765	115	MT767	116	MT768
117	MT769	118	MT790	119	MT791	120	MT792
121	MT795	122	MT796	123	MT798	124	MT799
125	MT801	126	MT802	127	MT824	128	MT890
129	MT895	130	MT896	131	MT899	132	MT900
133	MT910	134	MT940	135	MT942	136	MT950
137	MT985	138	MT986	139	MT995	140	MT996
141	MT998	142	MT999	143	MT761	144	MT775
145	MT569	146	MT558	147	MT330	148	MT567

F.2 ISO20022 Message Types

For the ISO20022 message category, the following message types are the ready-to-use message types that you can use after you log in.

Table F-2 ISO20022 Message Types

S.No	Message Type	S. No	Message Type	S. No	Message Type	S. No	Message Type
1	Pain.001.001.08	2	Pacs.008.001.07	3	Pacs.003.001.02	4	Pacs.008.001.02
5	Pacs.008.001.08	6	Pacs.010.001.03	7	Pain.001.001.09	8	Pacs.009.001.08
9	Pacs.004.001.09	10	Camt.050.001.05	11	camt.026.001.09	12	camt.027.001.09
13	camt.028.001.11	14	camt.029.001.11	15	camt.031.001.06	16	camt.032.001.04
17	camt.033.001.06	18	camt.038.001.04	19	camt.052.001.08	20	camt.052.001.10
21	camt.053.001.08	22	camt.053.001.10	23	camt.054.001.08	24	camt.054.001.09
25	camt.054.001.10	26	camt.056.001.10	27	camt.060.001.05	28	camt.060.001.06
29	camt.087.001.08	30	pacs.002.001.12	31	pacs.003.001.10	32	pacs.004.001.12
33	pacs.008.001.11	34	pacs.009.001.10	35	pacs.010.001.05	36	pacs.028.001.05
37	pacs.002.001.13	38	pacs.007.001.12	39	camt.034.001.06	40	camt.030.001.05

F.3 Fedwire Message Types

For the Fedwire message category, the following message types are the ready-to-use message types that you can use after you log in.

Table 59: Fedwire Message Types

Table F-3 Fedwire Message Types

S.No	Message Type	S. No	Message Type	S. No	Message Type	S. No	Message Type
1	FDCTR1000	**2**	FDBTR1002	**3**	FDCTR1002	**4**	FDCTR1008
5	FDCTR1600	**6**	FDCTR1602	**7**	FDBTR1600	**8**	FDBTR1000
9	FDBTR1008	**10**	FDBTR1602	**11**	FDCTP1000	**12**	FDCTP1002
13	FDCTP1008	**14**	FDCTP1600	**15**	FDCTP1602	**16**	FDCKS1600
17	FDCKS1602	**18**	FDDEP1600	**19**	FDDEP1602	**20**	FDFFR1600
21	FDFFR1602	**22**	FDFFS1600	**23**	FDFFS1602	**24**	FDDRC1031
25	FDDRW1032	**26**	FDSVC1090	**27**	FDDRB1631	**28**	FDDRW1632
29	FDSVC1690	**30**	FDSVC1590	**31**	FDBTR1500	**32**	FDDRC1531
33	FDDRW1532	-	-	-	-	-	-

F.4 US NACHA Message Types

For the US NACHA message category, the following message types are the ready-to-use message types that you can use after you log in.

Table F-4 US NACHA Message Types

S. No	Message Type	S.No	Message Type	S. No	Message Type	S. No	Message Type
1	IAT	**2**	CTX	**3**	BOC	**4**	RCK
5	POP	**6**	WEB	**7**	CCD	**8**	TEL
9	PPD	**10**	ARC	**11**	CIE	-	-

G

Invoking the PMF Workflow from backend

This appendix describes invoking the Process Modeller Framework (PMF) workflow from the backend for the alert.

Table G-1 PMF Workflow Invoking Parameters

Parameter Name	Parameter Description
Object ID	This represents the unique object ID. For Sanctions, the object ID can be alert ID or Good Guy Whitelist ID.
Object Type	This represents the object type for the object ID. For Sanctions, the object type will be **301** for alert and **302** for Good Guy Whitelist.
Infodom	This represents the name of the infodom in which Sanctions are installed.
Segment	This represents the name of the segment. For Sanctions, it will be**TFLSEGMENT**.
User ID	This represents the User ID that is triggering the workflow. Pass the value as **SYSTEM**.
Locale	This represents the locale. Pass the value as **en_US**.
Application Params	This represents the list of workflow data fields with their respective value.
Security Params	This represents the list of workflow security data fields with their respective value.

To trigger the workflow for Sanctions Alerts, follow the below code snippet.

```
DECLARE
lv_infodom varchar2(4000); lv_segment varchar2(4000);
TYPE alert_record_ids IS TABLE OF fsi_rt_alerts.n_grp_msg_id%TYPE;
l_alert_record_ids alert_record_ids;
appParams array_varchar := array_varchar();
secMap array_varchar := array_varchar(); BEGIN
appParams.extend();
appParams(1) := 'TF_ACTION=MANUAL_CLOSE';
appParams.extend(); appParams(2) := 'Role=SYSTEM'; select t.v_attribute_value1
into lv_infodom
from setup_rt_params t
where t.v_param_name = 'TFLT_INFODOM'; select t.v_attribute_value1
into lv_segment
from setup_rt_params t
where t.v_param_name = 'TFLT_SEGMENT'; select t.n_grp_msg_id bulk collect
into l_alert_record_ids from fsi_rt_alerts t
where t.n_status_cd in (1,2);
FOR recId IN 1 .. l_alert_record_ids.COUNT loop
startWorkflowForExpireRecord(l_alert_record_ids(recId),
'301',
lv_infodom, lv_segment, 'SYSTEM',
'en_US', appParams, secMap);
```

```
end loop;
EXCEPTION
WHEN OTHERS THEN
dbms_output.put_line(SQLCODE || SQLERRM); ROLLBACK;
END;
```

H

JMS Cluster Environment Creation

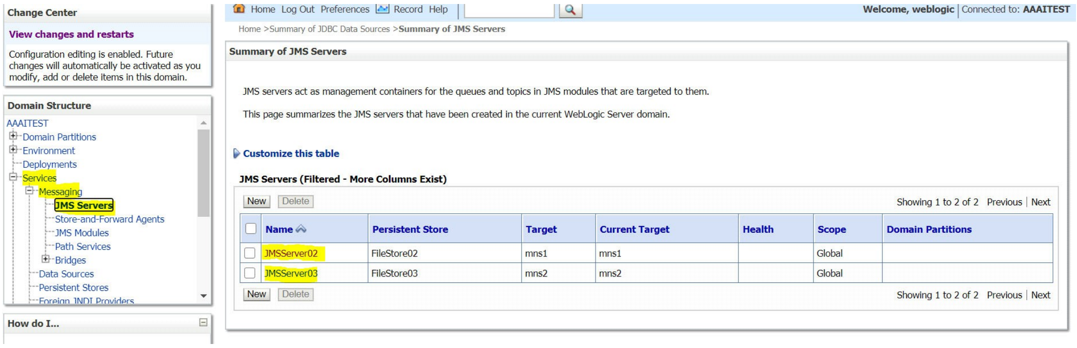
JMS servers act as management containers for the queues and topics in JMS modules that are targeted to them. JMS cluster servers in a domain work together to provide a more scalable and reliable application platform than a single server. A cluster appears to its clients as a single server, but it is a group of servers acting as one.

H.1 JMS Server Creation

To create the JMS server and file store, follow these steps:

1. Log in to **Weblogic Console**.
2. From the **Domain Structure** select **Services**, click **JMS Servers** from **Messaging** drop-down, and click **New** in the **JMS Servers** table.

Figure H-1 Weblogic Console Page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Summary of JMS Servers

JMS servers act as management containers for the queues and topics in JMS modules that are targeted to them.

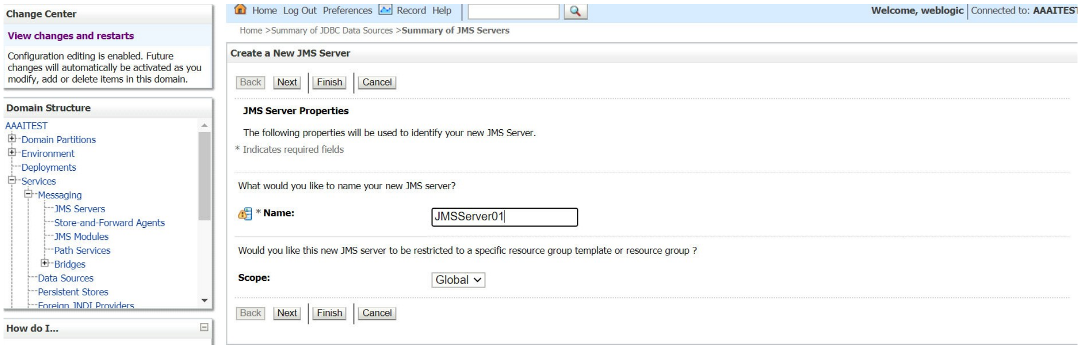
This page summarizes the JMS servers that have been created in the current WebLogic Server domain.

JMS Servers (Filtered - More Columns Exist)

□	Name	Persistent Store	Target	Current Target	Health	Scope	Domain Partitions
□	JMSServer02	FileStore02	mns1	mns1		Global	
□	JMSServer03	FileStore03	mns2	mns2		Global	

3. In the **JMS Server Properties** page**,** enter the JMS server name in the **Name** field and click **Next.**

Figure H-2 JMS Server Properties Page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New JMS Server

JMS Server Properties

The following properties will be used to identify your new JMS Server.

* Indicates required fields

What would you like to name your new JMS server?

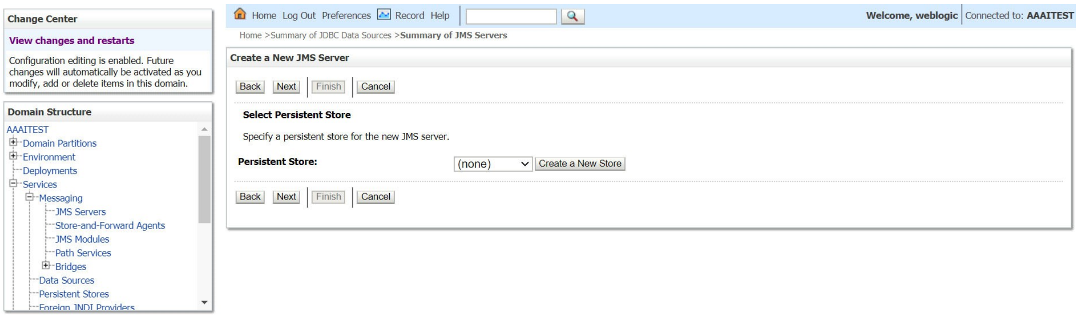
* Name: JMSServer01

Would you like this new JMS server to be restricted to a specific resource group template or resource group ?

Scope: Global

4. In the **Select Persistent Store** page**,** select **Create a New Store** from **Persistent Store** Field to specify a persistent store for the new JMS server.

Figure H-3 Select Persistent Store page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

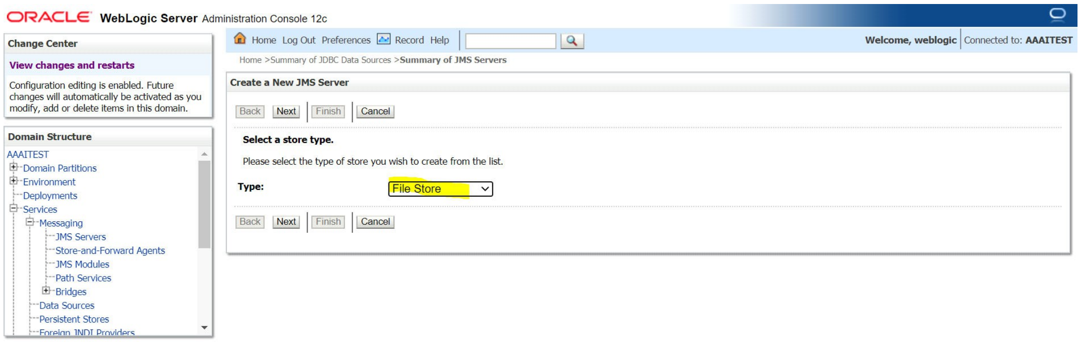
Select Persistent Store

Specify a persistent store for the new JMS server.

Persistent Store: (none)

5. In the **Select a store type** page**,** select **File Store** from **Type** Field and click **Next.**

Figure H-4 Select a store type page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

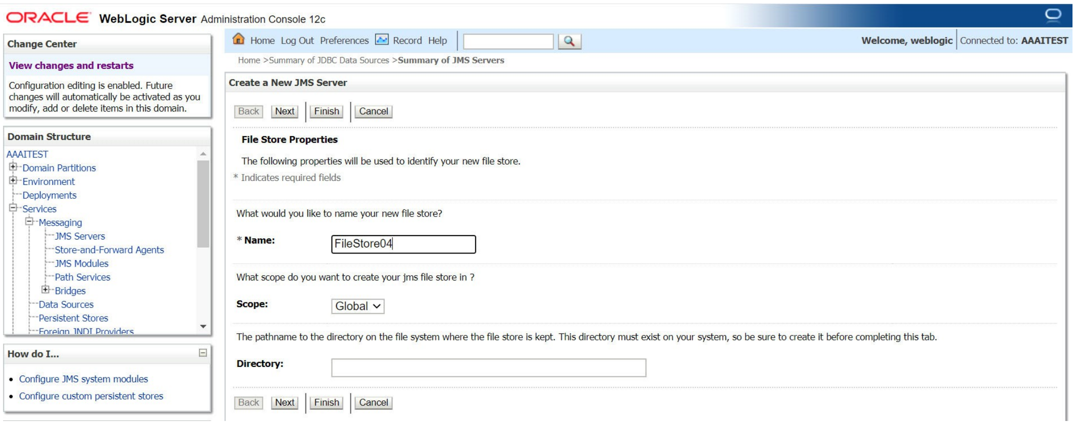
Select a store type.

Please select the type of store you wish to create from the list.

Type: File Store

6. In the **File Store Properties** page, enter the new file store name in the **Name** field and click Next.

Figure H-5 File Store Properties page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

File Store Properties

The following properties will be used to identify your new file store.

* Indicates required fields

What would you like to name your new file store?

* Name: FileStore04

What scope do you want to create your jms file store in ?

Scope: Global

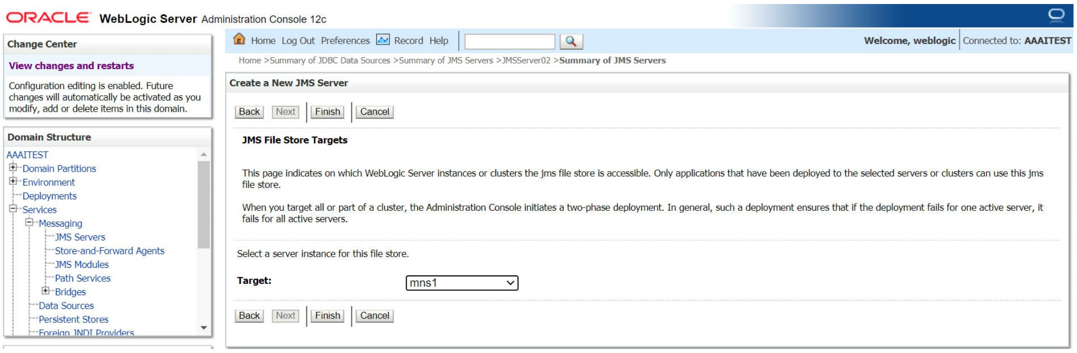
The pathname to the directory on the file system where the file store is kept. This directory must exist on your system, so be sure to create it before completing this tab.

Directory:

7. In the **JMS File Store Targets** page, select a target as one of the named server from **Target** Field drop down and Click **Finish.**

> **Note**
>
> - Only applications deployed to the selected servers or clusters can use the JMS file store.
> - When you target all or part of the cluster, the Administration Console initiates a two-phase deployment. Two-phase deployment ensures that if the deployment fails for one active server, it fails for all active servers.

Figure H-6 JMS File Store Targets page


ORACLE WebLogic Server Administration Console 12c
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITEST
Home >Summary of JDBC Data Sources >Summary of JMS Servers >JMSServer02 >Summary of JMS Servers
Change Center
View changes and restarts
Domain Structure
AAAITEST
Domain Partitions
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
Back Next Finish Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New JMS Server

JMS File Store Targets

This page indicates on which WebLogic Server instances or clusters the jms file store is accessible. Only applications that have been deployed to the selected servers or clusters can use this jms file store.

When you target all or part of a cluster, the Administration Console initiates a two-phase deployment. In general, such a deployment ensures that if the deployment fails for one active server, it fails for all active servers.

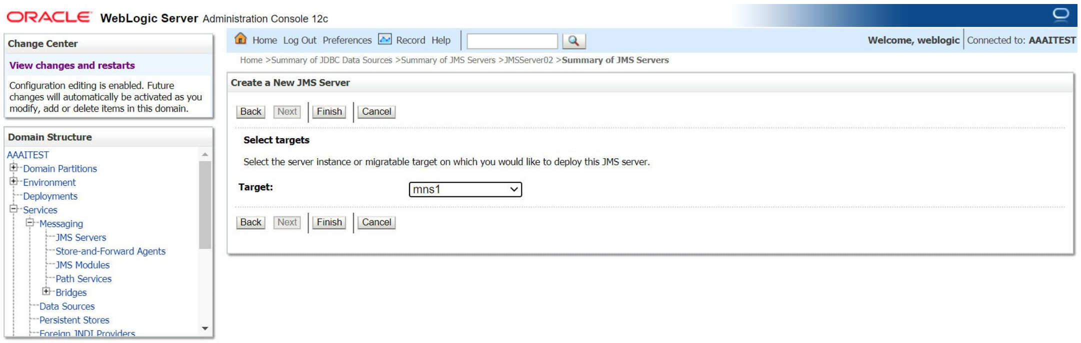
Select a server instance for this file store.

Target: mns1

> **Note**
>
> You will receive a message on successful activation and file store creation.

8. Select the same target name from the **JMS File Store Targets** page in the **Target** field drop down in the **Select targets** page and click **Finish** to create the JMS server and its respective file store.

Figure H-7 Select targets page


ORACLE WebLogic Server Administration Console 12c
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITEST
Home >Summary of JDBC Data Sources >Summary of JMS Servers >JMSServer02 >Summary of JMS Servers
Change Center
View changes and restarts
Domain Structure
AAAITEST
Domain Partitions
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
Back Next Finish Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New JMS Server

Select targets

Select the server instance or migratable target on which you would like to deploy this JMS server.

Target: mns1

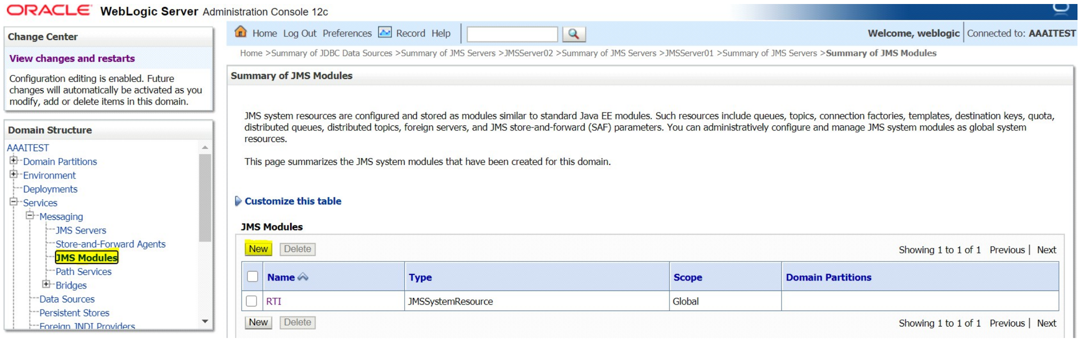
H.2 JMS Module Creation

JMS system resources are configured and stored as modules similar to standard Java EE modules. Such resources include queues, topics, connection factories, templates, destination keys, quota, distributed queues, distributed topics, and JMS store-and-forward (SAF) parameters. You can administratively configure and manage JMS system modules as global system resources.

To Create the JMS Module, follow these steps:

1. Log in to **Weblogic Console**.
2. From the **Domain Structure** Select **Services**, click **JMS Modules** from **Messaging** drop-down, and Click **New** in the **JMS Modules** table.

Figure H-8 Weblogic Console Page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Home >Summary of JDBC Data Sources >Summary of JMS Servers >JMSServer02 >Summary of JMS Servers >JMSServer01 >Summary of JMS Servers >**Summary of JMS Modules**

Summary of JMS Modules

JMS system resources are configured and stored as modules similar to standard Java EE modules. Such resources include queues, topics, connection factories, templates, destination keys, quota, distributed queues, distributed topics, foreign servers, and JMS store-and-forward (SAF) parameters. You can administratively configure and manage JMS system modules as global system resources.

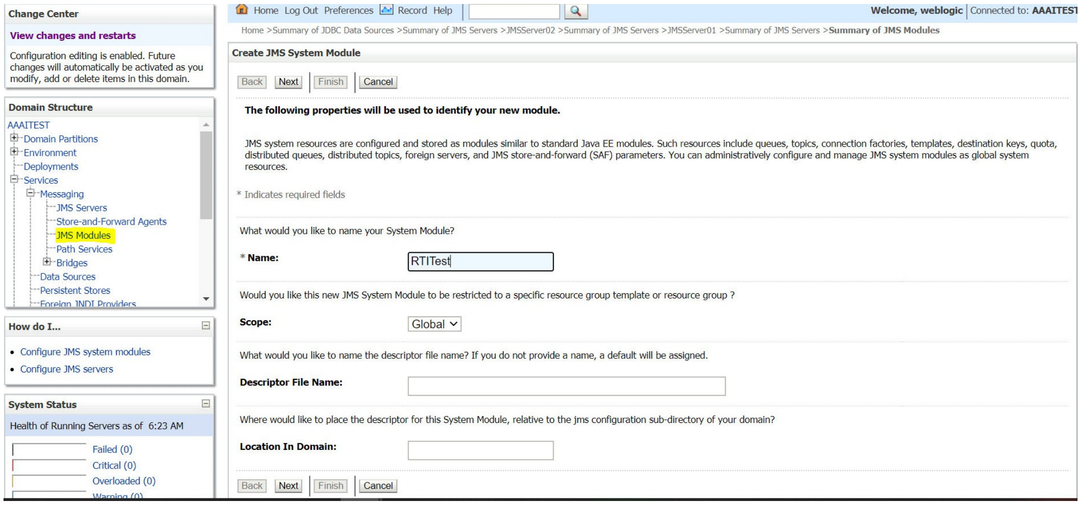
This page summarizes the JMS system modules that have been created for this domain.

JMS Modules

□	Name	Type	Scope	Domain Partitions
□	RTI	JMSSystemResource	Global	

3. In the **Create JMS System Module** page**,** enter the JMS Module name as RTI in the **Name** field and click **Next.**

Figure H-9 Create JMS System Module Page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Health of Running Servers as of 6:23 AM

Home >Summary of JDBC Data Sources >Summary of JMS Servers >JMSServer02 >Summary of JMS Servers >JMSServer01 >Summary of JMS Servers >**Summary of JMS Modules**

Create JMS System Module

The following properties will be used to identify your new module.

JMS system resources are configured and stored as modules similar to standard Java EE modules. Such resources include queues, topics, connection factories, templates, destination keys, quota, distributed queues, distributed topics, foreign servers, and JMS store-and-forward (SAF) parameters. You can administratively configure and manage JMS system modules as global system resources.

* Indicates required fields

What would you like to name your System Module?

* **Name:** RTITest

Would you like this new JMS System Module to be restricted to a specific resource group template or resource group ?

Scope: Global

What would you like to name the descriptor file name? If you do not provide a name, a default will be assigned.

Descriptor File Name:

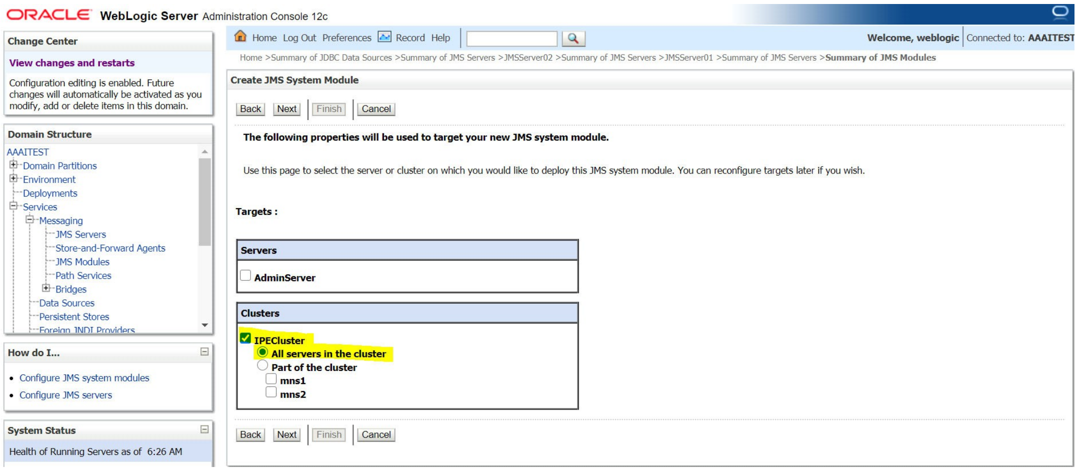
Where would like to place the descriptor for this System Module, relative to the jms configuration sub-directory of your domain?

Location In Domain:

4. Select Servers or Clusters on which you deploy the JMS system module from the **Targets** Field. The cluster name that was created in step 6.1.8 will be listed under **IPECluster**.

> **Note**
>
> You can configure the targets later if required.

Figure H-10   Create JMS System Module



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Health of Running Servers as of 6:26 AM

Create JMS System Module

The following properties will be used to target your new JMS system module.

Use this page to select the server or cluster on which you would like to deploy this JMS system module. You can reconfigure targets later if you wish.

Targets :

Servers

□ AdminServer

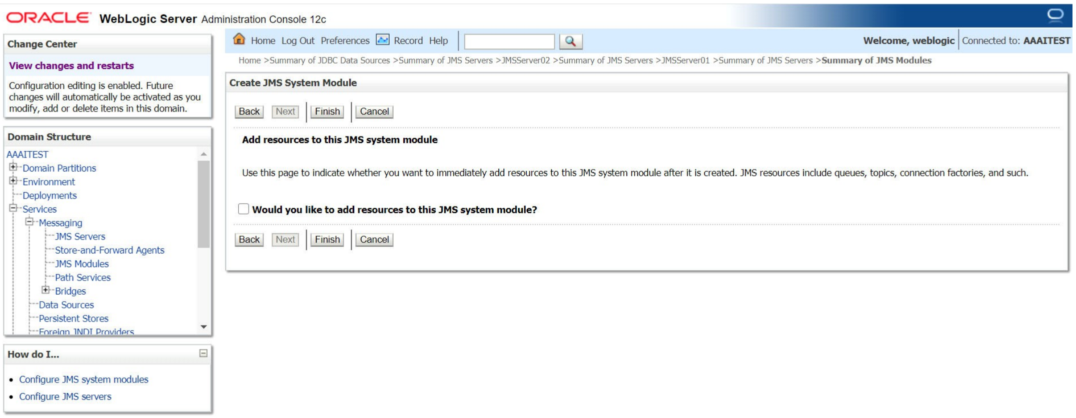
Clusters

☑ IPECluster
- ● All servers in the cluster
- ○ Part of the cluster
  - □ mns1
  - □ mns2

5. To add resources to the JMS system module and to create JMS modules check the box in the **Create JMS System Module page** and click **Finish.**

> **Note**
>
> You will receive message on successful creation of the JWS module.

Figure H-11   Create JMS System Module



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create JMS System Module

Add resources to this JMS system module

Use this page to indicate whether you want to immediately add resources to this JMS system module after it is created. JMS resources include queues, topics, connection factories, and such.

□ Would you like to add resources to this JMS system module?

H.3 Sub-Deployment Creation

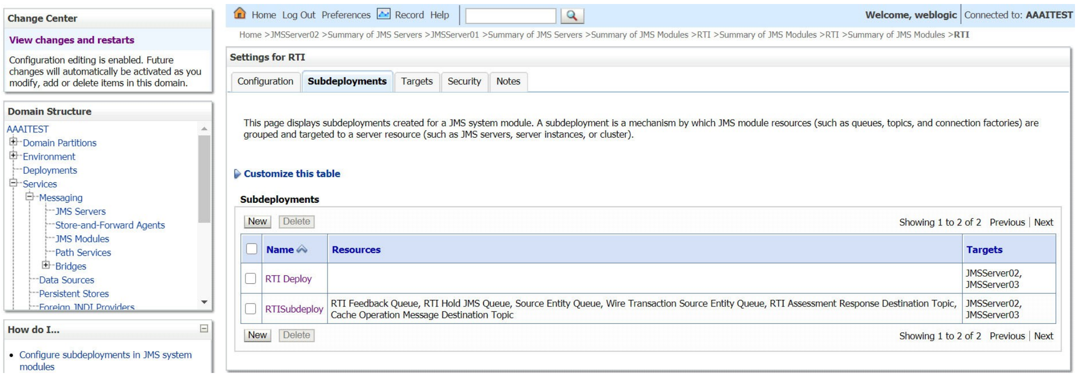
A sub-deployment is a mechanism by which JMS module resources such as queues, topics, and connection factories are grouped and targeted to a server resource such as JMS servers, server instances or cluster.

To create the Sub-Deployment follow these steps:

1. Log in to **Weblogic Console**.
2. From the **Domain Structure** Select **Services** and click **JMS Modules** from **Messaging** drop- down. The **Summary of JMS Module** page is displayed.
3. Select **RTI** from **JMS Modules** table. The **Settings for RTI** page is displayed.

4. Select **subdeployments** from the tabs.
5. Enter the sub-deployment name as **RTI Deploy** in **subdeployment** table and click **Next**.

Figure H-12   Settings for RTI



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Home >JMSServer02 >Summary of JMS Servers >JMSServer01 >Summary of JMS Servers >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >**RTI**

Settings for RTI

This page displays subdeployments created for a JMS system module. A subdeployment is a mechanism by which JMS module resources (such as queues, topics, and connection factories) are grouped and targeted to a server resource (such as JMS servers, server instances, or cluster).

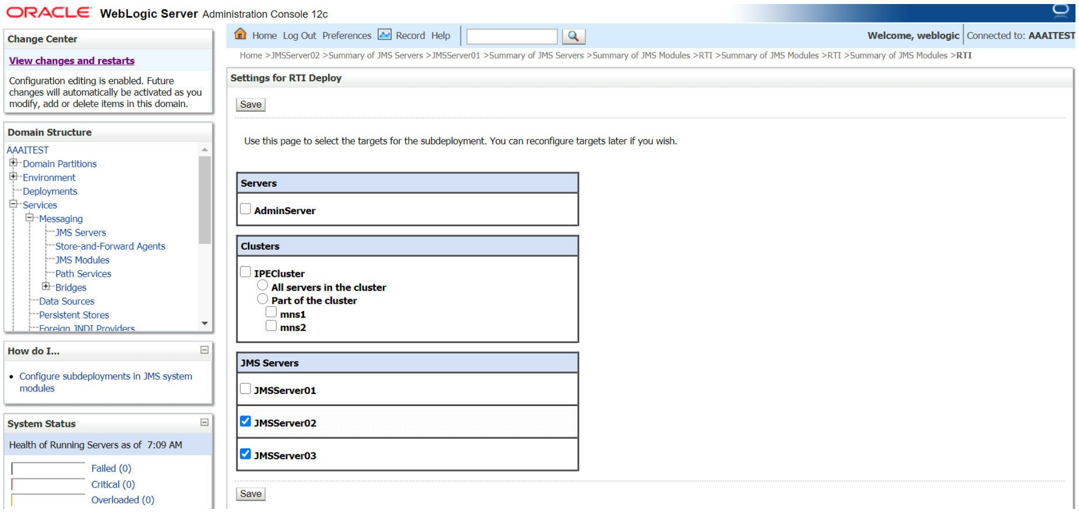
Subdeployments

□	Name	Resources	Targets
□	RTI Deploy		JMSServer02, JMSServer03
□	RTISubdeploy	RTI Feedback Queue, RTI Hold JMS Queue, Source Entity Queue, Wire Transaction Source Entity Queue, RTI Assessment Response Destination Topic, Cache Operation Message Destination Topic	JMSServer02, JMSServer03

6. Select the JMS servers created previously from the **JMS Servers** list from the **Settings for RTI Deploy** page and click **Save.** The **RTI** sub-deployment is created**.**

> **Note**
>
> You can configure the targets later if required.

Figure H-13   Settings for RTI Deploy Page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Health of Running Servers as of 7:09 AM

Home >JMSServer02 >Summary of JMS Servers >JMSServer01 >Summary of JMS Servers >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >**RTI**

Settings for RTI Deploy

Use this page to select the targets for the subdeployment. You can reconfigure targets later if you wish.

Servers

□ AdminServer

Clusters

□ IPECluster
- ○ All servers in the cluster
- ○ Part of the cluster
  - □ mns1
  - □ mns2

JMS Servers

□ JMSServer01

☑ JMSServer02

☑ JMSServer03

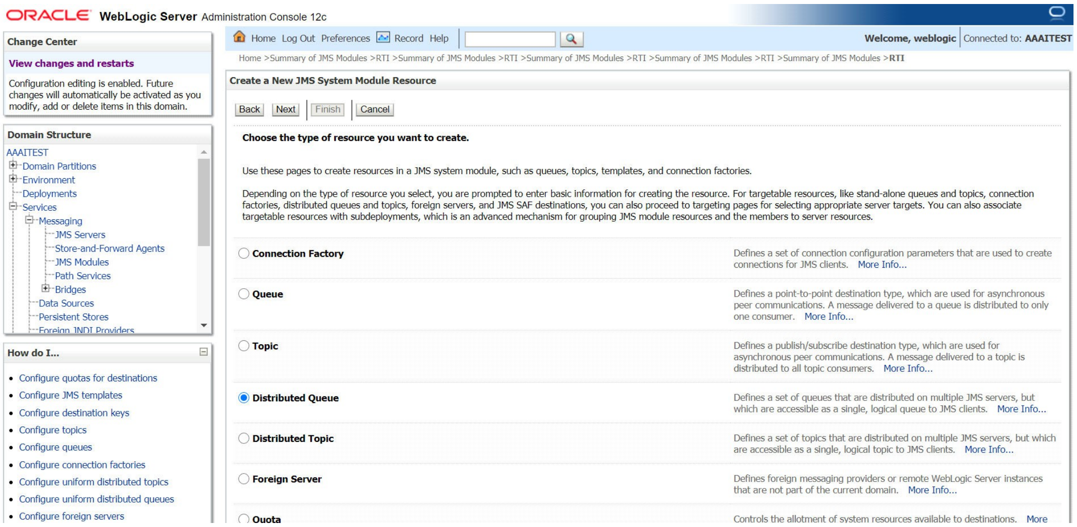
H.4 Distributed Queues Creation

Depending on the type of resources selected you are prompted to enter the basic information for creating the resources. For target resources like stand-alone queues and topics, connection factories, distributed queues and topics, foreign servers, and JMS SAF destinations you can proceed to target pages for selecting appropriate server targets. You can associate target resources with sub- deployments, which is an advanced mechanism for grouping JMS module resources and the members to server resources. To create the Distribute Queues, follow these steps:

> ⓘ **Note**
>
> Queues must be created as per the IPE Configuration guide with the same naming convention. See JMS Queue Creation for SWIFT, Fedwire and ISO20022 Message Types for information about JMS Queue creation for SWIFT, Fedwire and ISo20022 Message types.

1. Log in to **Weblogic Console**.
2. From the **Domain Structure** Select **Services** and click **JMS Modules** from **Messaging** drop- down. The **Summary of JMS Module** page is displayed.
3. Select **RTI** from **JMS Modules** table. The **Settings for RTI** page is displayed.
4. Click **New** and select **Distribute Queue** from **Create a New a JMS System Module Resource** page.

Figure H-14 Create a New JMS System Module Resource page


ORACLE WebLogic Server Administration Console 12c
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: AAAITEST
Home >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI
Change Center
View changes and restarts
Domain Structure
AAAITEST
Domain Partitions
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
How do I...
Configure quotas for destinations
Configure JMS templates
Configure destination keys
Configure topics
Configure queues
Configure connection factories
Configure uniform distributed topics
Configure uniform distributed queues
Configure foreign servers
Back
Next
Finish
Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New JMS System Module Resource

Choose the type of resource you want to create.

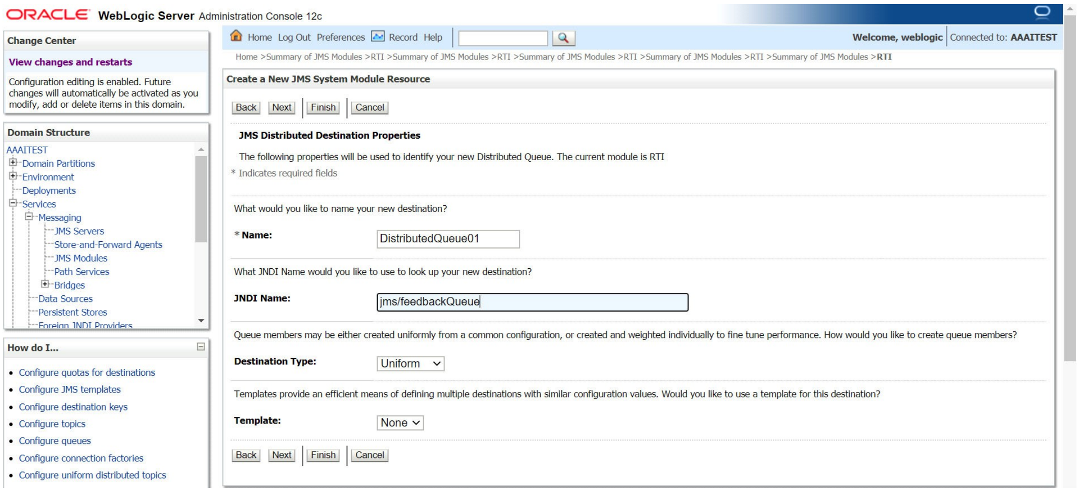
Use these pages to create resources in a JMS system module, such as queues, topics, templates, and connection factories.

Depending on the type of resource you select, you are prompted to enter basic information for creating the resource. For targetable resources, like stand-alone queues and topics, connection factories, distributed queues and topics, foreign servers, and JMS SAF destinations, you can also proceed to targeting pages for selecting appropriate server targets. You can also associate targetable resources with subdeployments, which is an advanced mechanism for grouping JMS module resources and the members to server resources.

○ Connection Factory	Defines a set of connection configuration parameters that are used to create connections for JMS clients. More Info...
○ Queue	Defines a point-to-point destination type, which are used for asynchronous peer communications. A message delivered to a queue is distributed to only one consumer. More Info...
○ Topic	Defines a publish/subscribe destination type, which are used for asynchronous peer communications. A message delivered to a topic is distributed to all topic consumers. More Info...
● Distributed Queue	Defines a set of queues that are distributed on multiple JMS servers, but which are accessible as a single, logical queue to JMS clients. More Info...
○ Distributed Topic	Defines a set of topics that are distributed on multiple JMS servers, but which are accessible as a single, logical topic to JMS clients. More Info...
○ Foreign Server	Defines foreign messaging providers or remote WebLogic Server instances that are not part of the current domain. More Info...
○ Quota	Controls the allotment of system resources available to destinations. More

5. Enter the name and JDNI name in **Name** and **JNDI Name** Fields respectively as per the IPE Configuration guide and click **Next**.

Figure H-15 JMS Distributed Destination Properties page


ORACLE WebLogic Server Administration Console 12c
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: AAAITEST
Home >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI
Change Center
View changes and restarts
Domain Structure
AAAITEST
Domain Partitions
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
How do I...
Configure quotas for destinations
Configure JMS templates
Configure destination keys
Configure topics
Configure queues
Configure connection factories
Configure uniform distributed topics
Back
Next
Finish
Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New JMS System Module Resource

JMS Distributed Destination Properties

The following properties will be used to identify your new Distributed Queue. The current module is RTI

* Indicates required fields

What would you like to name your new destination?

* Name: DistributedQueue01

What JNDI Name would you like to use to look up your new destination?

JNDI Name: jms/feedbackQueue

Queue members may be either created uniformly from a common configuration, or created and weighted individually to fine tune performance. How would you like to create queue members?

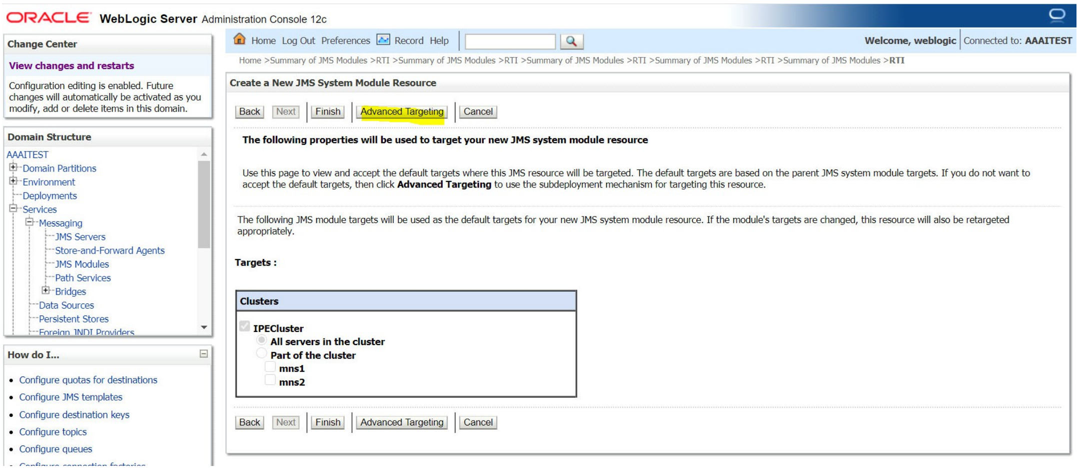
Destination Type: Uniform

Templates provide an efficient means of defining multiple destinations with similar configuration values. Would you like to use a template for this destination?

Template: None

6. Select **Advanced Targeting**.

Figure H-16 Create a New JMS System Module Resource page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New JMS System Module Resource

The following properties will be used to target your new JMS system module resource

Use this page to view and accept the default targets where this JMS resource will be targeted. The default targets are based on the parent JMS system module targets. If you do not want to accept the default targets, then click **Advanced Targeting** to use the subdeployment mechanism for targeting this resource.

The following JMS module targets will be used as the default targets for your new JMS system module resource. If the module's targets are changed, this resource will also be retargeted appropriately.

Targets :

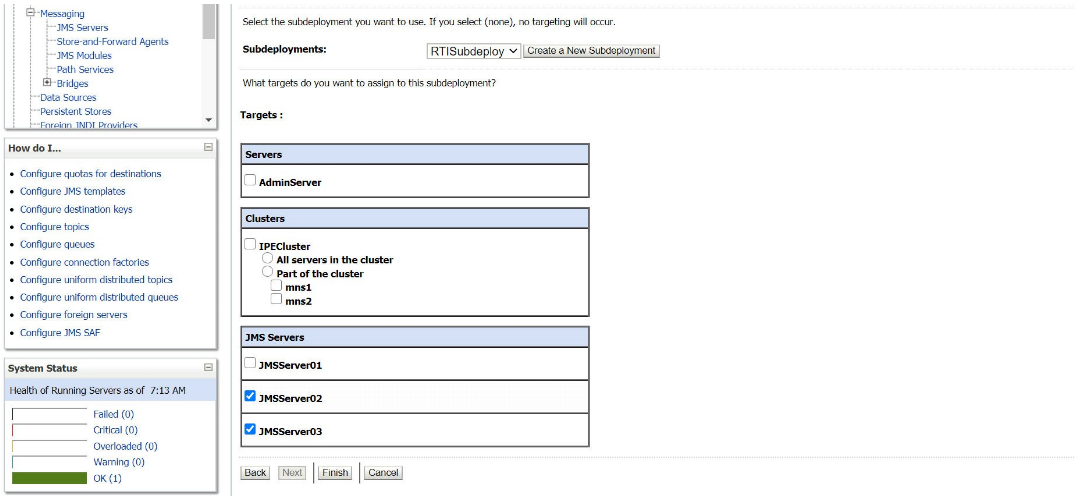
Clusters

☑ **IPECluster**
● **All servers in the cluster**
○ **Part of the cluster**
□ **mns1**
□ **mns2**

7. Select **RTISubdeploy** from the **subdeployment** field drop down list and select the JMS servers created. Click **Finish**. The distributed queue is successfully created.

> **Note**
>
> You will receive message on successful creation of the JWS distributed queue.

Figure H-17 Create a New JMS System Module Resource page



Health of Running Servers as of 7:13 AM

Select the subdeployment you want to use. If you select (none), no targeting will occur.

Subdeployments: RTISubdeploy

What targets do you want to assign to this subdeployment?

Targets :

Servers

□ **AdminServer**

Clusters

□ **IPECluster**
○ **All servers in the cluster**
○ **Part of the cluster**
□ **mns1**
□ **mns2**

JMS Servers

□ **JMSServer01**

☑ **JMSServer02**

☑ **JMSServer03**

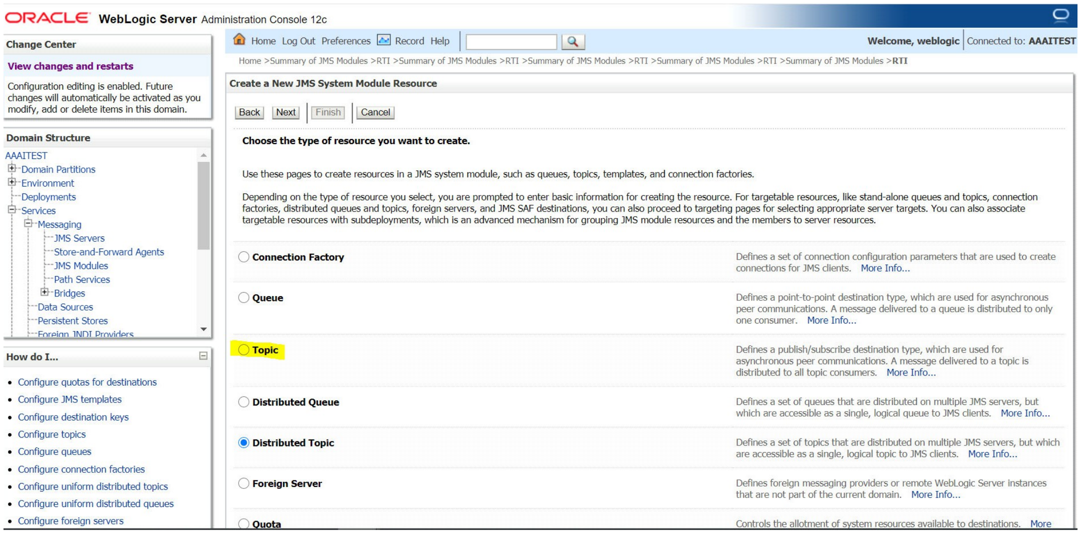
H.5 Distributed Topic Creation

To create the Distribute Topic, follow these steps:

> **Note**
>
> Topics must be created as per the IPE Configuration guide with the same naming convention.

1. Log in to **Weblogic Console**.
2. From **Domain Structure** Select **Services** and click **JMS Modules** from **Messaging** drop-down. The **Summary of JMS Module** page is displayed.
3. Select **RTI** from **JMS Modules** table. The **Settings for RTI** page is displayed.
4. Click **New** and select **Distribute Topic** from **Create a New a JMS System Module Resource** page.

Figure H-18 Create a New JMS System Module Resource page


ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.
Domain Structure
AAAITEST
Domain Partitions
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
How do I...
Configure quotas for destinations
Configure JMS templates
Configure destination keys
Configure topics
Configure queues
Configure connection factories
Configure uniform distributed topics
Configure uniform distributed queues
Configure foreign servers
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITEST
Home >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI
Back Next Finish Cancel

Create a New JMS System Module Resource

Choose the type of resource you want to create.

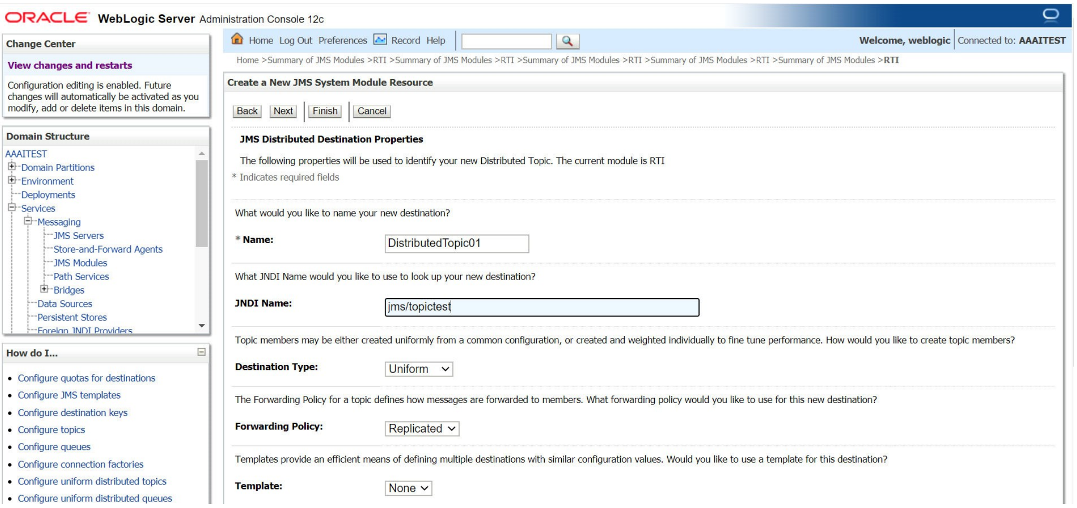
Use these pages to create resources in a JMS system module, such as queues, topics, templates, and connection factories.

Depending on the type of resource you select, you are prompted to enter basic information for creating the resource. For targetable resources, like stand-alone queues and topics, connection factories, distributed queues and topics, foreign servers, and JMS SAF destinations, you can also proceed to targeting pages for selecting appropriate server targets. You can also associate targetable resources with subdeployments, which is an advanced mechanism for grouping JMS module resources and the members to server resources.

○ **Connection Factory**	Defines a set of connection configuration parameters that are used to create connections for JMS clients. More Info...
○ **Queue**	Defines a point-to-point destination type, which are used for asynchronous peer communications. A message delivered to a queue is distributed to only one consumer. More Info...
○ **Topic**	Defines a publish/subscribe destination type, which are used for asynchronous peer communications. A message delivered to a topic is distributed to all topic consumers. More Info...
○ **Distributed Queue**	Defines a set of queues that are distributed on multiple JMS servers, but which are accessible as a single, logical queue to JMS clients. More Info...
● **Distributed Topic**	Defines a set of topics that are distributed on multiple JMS servers, but which are accessible as a single, logical topic to JMS clients. More Info...
○ **Foreign Server**	Defines foreign messaging providers or remote WebLogic Server instances that are not part of the current domain. More Info...
○ **Quota**	Controls the allotment of system resources available to destinations. More

5. Enter the name and JDNI name in **Name** and **JNDI Name** Fields respectively as per the IPE Configuration guide and click **Next**.

Figure H-19 JMS Distributed Destination Properties page


ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.
Domain Structure
AAAITEST
Domain Partitions
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
How do I...
Configure quotas for destinations
Configure JMS templates
Configure destination keys
Configure topics
Configure queues
Configure connection factories
Configure uniform distributed topics
Configure uniform distributed queues
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITEST
Home >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI
Back Next Finish Cancel

Create a New JMS System Module Resource

JMS Distributed Destination Properties

The following properties will be used to identify your new Distributed Topic. The current module is RTI

* Indicates required fields

What would you like to name your new destination?

*** Name:** DistributedTopic01

What JNDI Name would you like to use to look up your new destination?

JNDI Name: jms/topictest

Topic members may be either created uniformly from a common configuration, or created and weighted individually to fine tune performance. How would you like to create topic members?

Destination Type: Uniform

The Forwarding Policy for a topic defines how messages are forwarded to members. What forwarding policy would you like to use for this new destination?

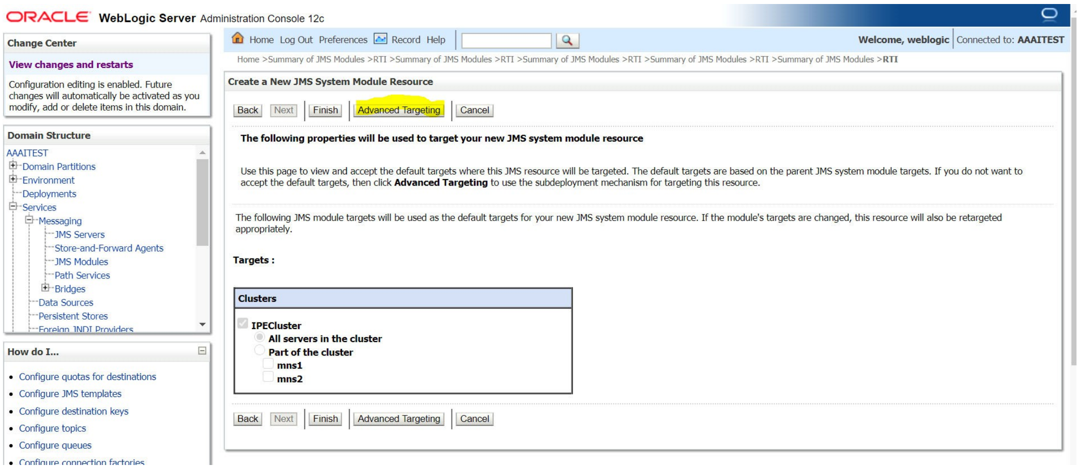
Forwarding Policy: Replicated

Templates provide an efficient means of defining multiple destinations with similar configuration values. Would you like to use a template for this destination?

Template: None

6. Select **Advanced Targeting**.

Figure H-20 Create a New JMS System Module Resource page


ORACLE WebLogic Server Administration Console 12c
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITEST
Home >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI
Change Center
View changes and restarts
Domain Structure
AAAITEST
Domain Partitions
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
How do I...
Configure quotas for destinations
Configure JMS templates
Configure destination keys
Configure topics
Configure queues
Configure connection factories
Back
Next
Finish
Advanced Targeting
Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New JMS System Module Resource

The following properties will be used to target your new JMS system module resource

Use this page to view and accept the default targets where this JMS resource will be targeted. The default targets are based on the parent JMS system module targets. If you do not want to accept the default targets, then click **Advanced Targeting** to use the subdeployment mechanism for targeting this resource.

The following JMS module targets will be used as the default targets for your new JMS system module resource. If the module's targets are changed, this resource will also be retargeted appropriately.

Targets :

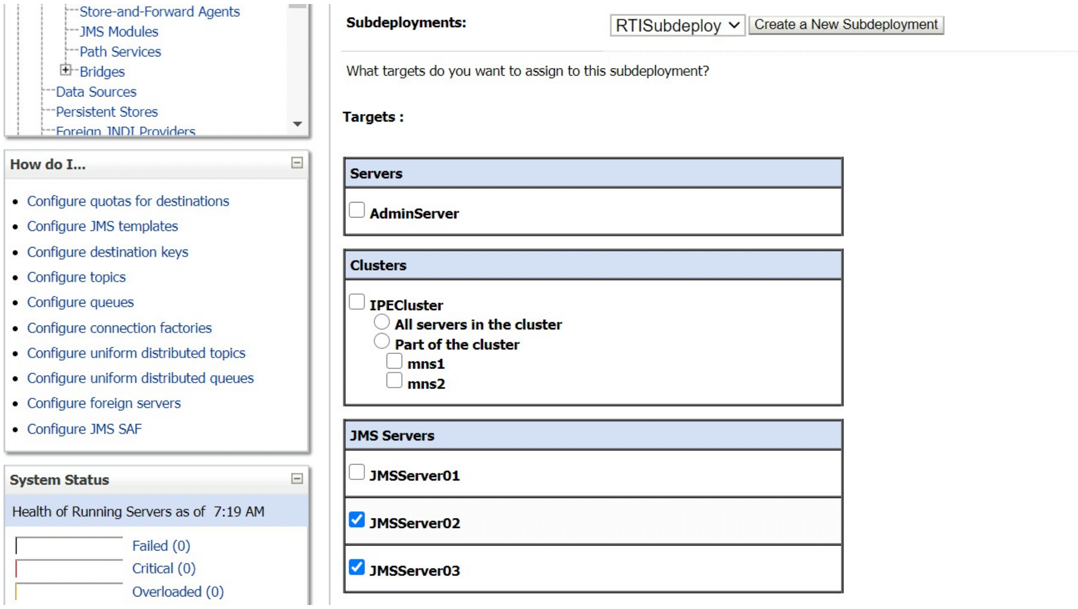
Clusters

☑ **IPECluster**
● **All servers in the cluster**
○ **Part of the cluster**
□ **mns1**
□ **mns2**

7. Select **RTISubdeploy** from the **subdeployment** field drop down list and select the JMS servers created. Click **Finish**. The distributed topic is successfully created.

> **Note**
>
> You will receive message on successful creation of the JWS distributed topic.

Figure H-21 Create a New JMS System Module Resource page



Health of Running Servers as of 7:19 AM

Subdeployments: RTISubdeploy

What targets do you want to assign to this subdeployment?

Targets :

Servers

□ **AdminServer**

Clusters

□ **IPECluster**
○ **All servers in the cluster**
○ **Part of the cluster**
□ **mns1**
□ **mns2**

JMS Servers

□ **JMSServer01**
☑ **JMSServer02**
☑ **JMSServer03**

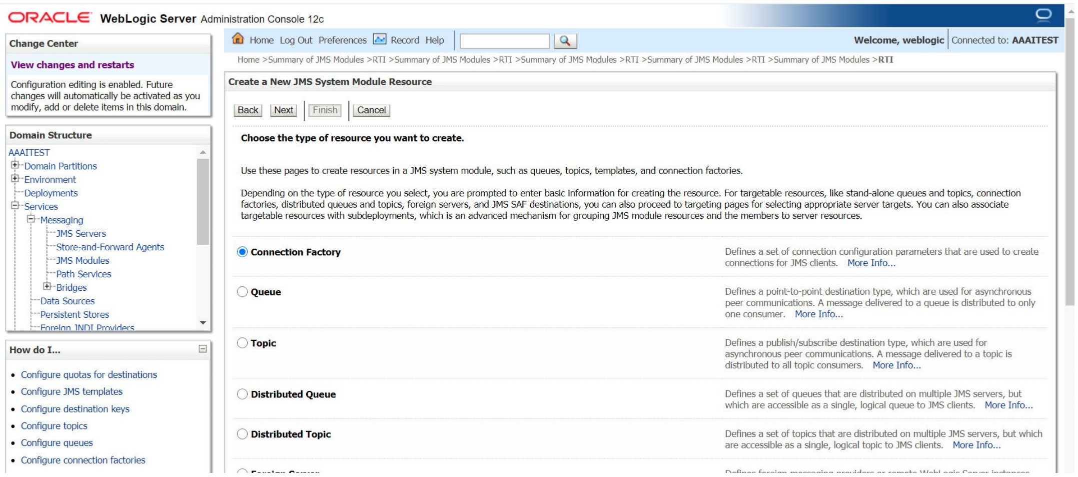
H.6 Connection Factory Creation

To create the Connection Factory, follow these steps:

> **Note**
>
> Connections must be created as per theIPE Configuration guide with the same naming convention.

1. Log in to **Weblogic Console**.
2. From **Domain Structure** Select **Services** and click **JMS Modules** from **Messaging** drop-down. The **Summary of JMS Module** page is displayed.
3. Select **RTI** from **JMS Modules** table. The **Settings for RTI** page is displayed.
4. Click **New** and select **Connection Factory** from **Create a New a JMS System Module Resource** page.

Figure H-22 Create a New JMS System Module Resource page


WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITEST
Home >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI
Domain Structure
AAAITEST
Domain Partitions
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
How do I...
Configure quotas for destinations
Configure JMS templates
Configure destination keys
Configure topics
Configure queues
Configure connection factories
Back
Next
Finish
Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New JMS System Module Resource

Choose the type of resource you want to create.

Use these pages to create resources in a JMS system module, such as queues, topics, templates, and connection factories.

Depending on the type of resource you select, you are prompted to enter basic information for creating the resource. For targetable resources, like stand-alone queues and topics, connection factories, distributed queues and topics, foreign servers, and JMS SAF destinations, you can also proceed to targeting pages for selecting appropriate server targets. You can also associate targetable resources with subdeployments, which is an advanced mechanism for grouping JMS module resources and the members to server resources.

● **Connection Factory** — Defines a set of connection configuration parameters that are used to create connections for JMS clients. More Info...

○ **Queue** — Defines a point-to-point destination type, which are used for asynchronous peer communications. A message delivered to a queue is distributed to only one consumer. More Info...

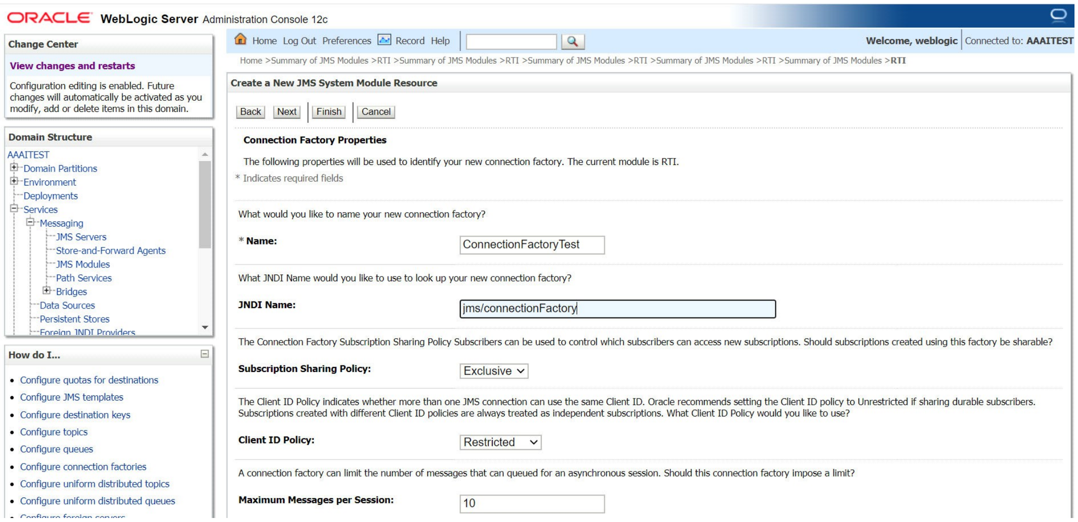
○ **Topic** — Defines a publish/subscribe destination type, which are used for asynchronous peer communications. A message delivered to a topic is distributed to all topic consumers. More Info...

○ **Distributed Queue** — Defines a set of queues that are distributed on multiple JMS servers, but which are accessible as a single, logical queue to JMS clients. More Info...

○ **Distributed Topic** — Defines a set of topics that are distributed on multiple JMS servers, but which are accessible as a single, logical topic to JMS clients. More Info...

5. Enter the name and JDNI name in **Name** and **JNDI Name** Fields respectively as per the IPE Configuration guide and click **Next**.

Figure H-23 Connection Factory Properties page


WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITEST
Home >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI >Summary of JMS Modules >RTI
Domain Structure
AAAITEST
Domain Partitions
Environment
Deployments
Services
Messaging
JMS Servers
Store-and-Forward Agents
JMS Modules
Path Services
Bridges
Data Sources
Persistent Stores
Foreign JNDI Providers
How do I...
Configure quotas for destinations
Configure JMS templates
Configure destination keys
Configure topics
Configure queues
Configure connection factories
Configure uniform distributed topics
Configure uniform distributed queues
Back
Next
Finish
Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New JMS System Module Resource

Connection Factory Properties

The following properties will be used to identify your new connection factory. The current module is RTI.

* Indicates required fields

What would you like to name your new connection factory?

* **Name:** ConnectionFactoryTest

What JNDI Name would you like to use to look up your new connection factory?

JNDI Name: jms/connectionFactory

The Connection Factory Subscription Sharing Policy Subscribers can be used to control which subscribers can access new subscriptions. Should subscriptions created using this factory be sharable?

Subscription Sharing Policy: Exclusive

The Client ID Policy indicates whether more than one JMS connection can use the same Client ID. Oracle recommends setting the Client ID policy to Unrestricted if sharing durable subscribers. Subscriptions created with different Client ID policies are always treated as independent subscriptions. What Client ID Policy would you like to use?

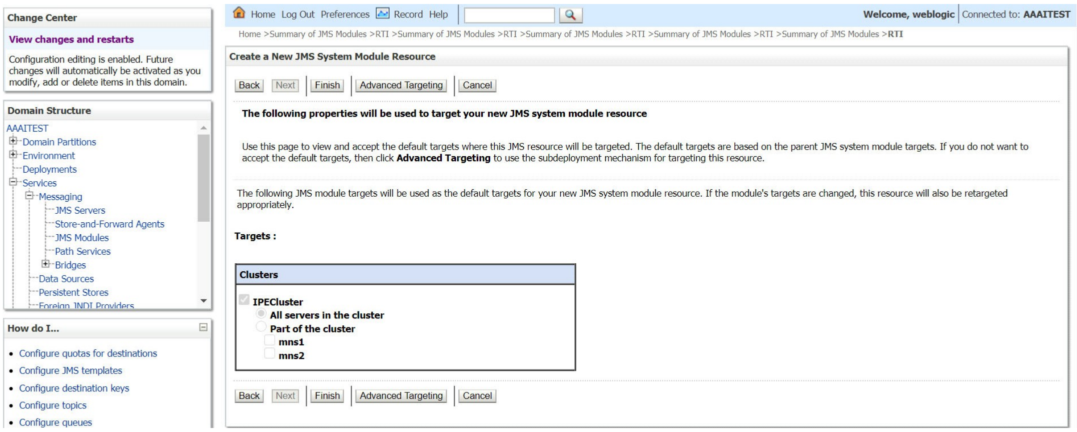
Client ID Policy: Restricted

A connection factory can limit the number of messages that can queued for an asynchronous session. Should this connection factory impose a limit?

Maximum Messages per Session: 10

6. Select **Advanced Targeting**.

Figure H-24 Create a New JMS System Module Resource page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Create a New JMS System Module Resource

The following properties will be used to target your new JMS system module resource

Use this page to view and accept the default targets where this JMS resource will be targeted. The default targets are based on the parent JMS system module targets. If you do not want to accept the default targets, then click **Advanced Targeting** to use the subdeployment mechanism for targeting this resource.

The following JMS module targets will be used as the default targets for your new JMS system module resource. If the module's targets are changed, this resource will also be retargeted appropriately.

Targets :

☑ IPECluster
● All servers in the cluster
○ Part of the cluster
□ mns1
□ mns2

7. Select the JMS Servers created and Click **Finish**. The Connection Factory is successfully created.

> **Note**
>
> You will receive message on successful creation of the JWS Connection Factory.

H.7 JMS Queue Creation for SWIFT, Fedwire and ISO20022 Message Types

The JMS Queues for Fedwire and ISO20022 are created similar to JMS Queue for SWIFT. For more information about JMS Queue creation, see the IPE Configuration guide .

The following table provides the information about the JMS queues for SWIFT, Fedwire and ISO2022 message types.

Table H-1 WebLogic JMS Queues - Field Value

Message Type	Queue Name	Fields	-	-
-	-	**Name**	**JNDI name**	**Subdeployment**
SWIFT	RTI Source Entity Queue	Enter the name as RTI Source Entity Queue	Enter the JNDI name as jms/ sourceEntityQueue	Select the Subdeployment as RTISubDeploy
FedWire	RTI Source Fed Entity Queue	Enter the name as RTI Source Entity Queue	Enter the JNDI name as jms/ sourceFedEntity-Queue	Select the Subdeployment as RTISubDeploy
ISO20022	RTI Source Sepa Entity Queue	Enter the name as RTI Source Entity Queue	Enter the JNDI name as jms/ sourceSepaEntity-Queue	Select the Subdeployment as RTISubDeploy

I

User Group Customization

When a new user group for Transaction Filtering is created from Oracle Financial Services Analytical Applications (OFSAA) user Interface (UI), you must insert an entry in the CSSMS_GROUP_MAST_PACK table manually with the product id OFS_TF.

J

Configurations for the Bearer Token

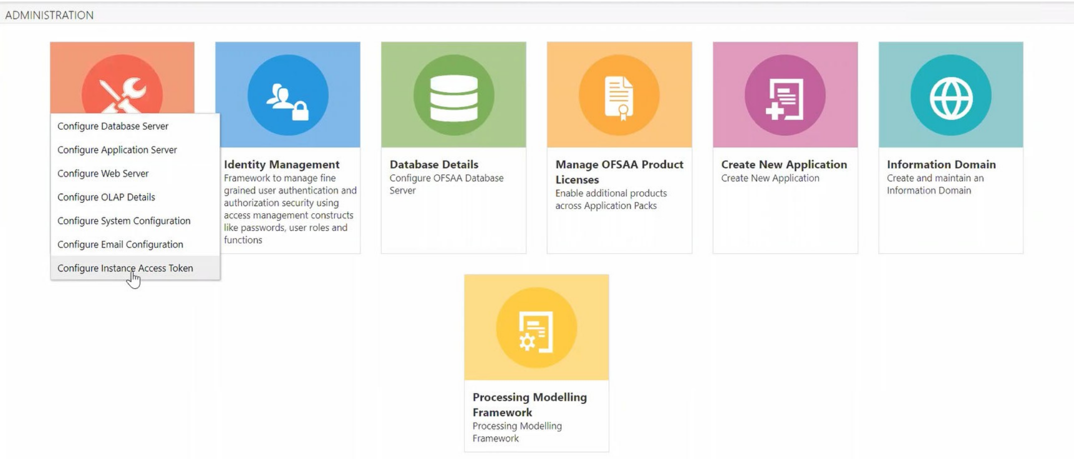
- The following section takes you through the process of generating a token and using it to get the individual or entity JSON, depending on the API request. A token is used to authorize the request.
- You can begin by generating a password for the user who sends the request. After the password is generated, generate a token to authorize this request. The default time for token expiration is 3600 seconds (1 hour) and can be changed. To change the validity, see Change Token Validity.

J.1 Generate User Password

To generate a password for the user, follow these steps:

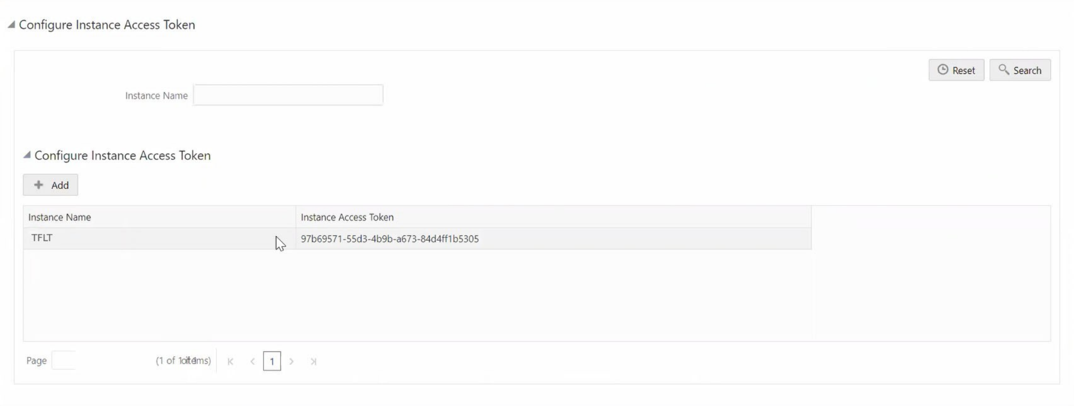
1. Log in as a system administrator.
2. Click **System Configuration** in the **Administration** page and select **Configure Instance Access Token**. The **Configure Instance Access Token** window is displayed.

Figure J-1 Administration Page


ADMINISTRATION
Configure Database Server
Configure Application Server
Configure Web Server
Configure OLAP Details
Configure System Configuration
Configure Email Configuration
Configure Instance Access Token
Identity Management
Framework to manage fine grained user authentication and authorization security using access management constructs like passwords, user roles and functions
Database Details
Configure OFSAA Database Server
Manage OFSAA Product Licenses
Enable additional products across Application Packs
Create New Application
Create New Application
Information Domain
Create and maintain an Information Domain
Processing Modelling Framework
Processing Modelling Framework

3. In the **Configure Instance Access Token** section, click **Add.** A new window is displayed.

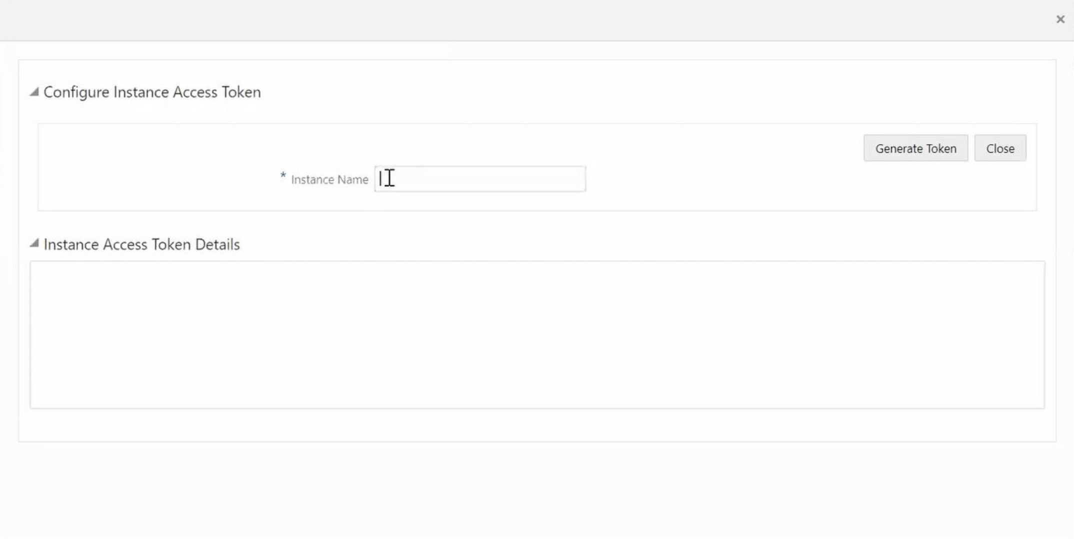
Figure J-2 Configure Setup Access Token


Configure Instance Access Token
Reset
Search
Instance Name
Configure Instance Access Token
Add
Page
(1 of 1items)
1

Instance Name	Instance Access Token
TFLT	97b69571-55d3-4b9b-a673-84d4ff1b5305

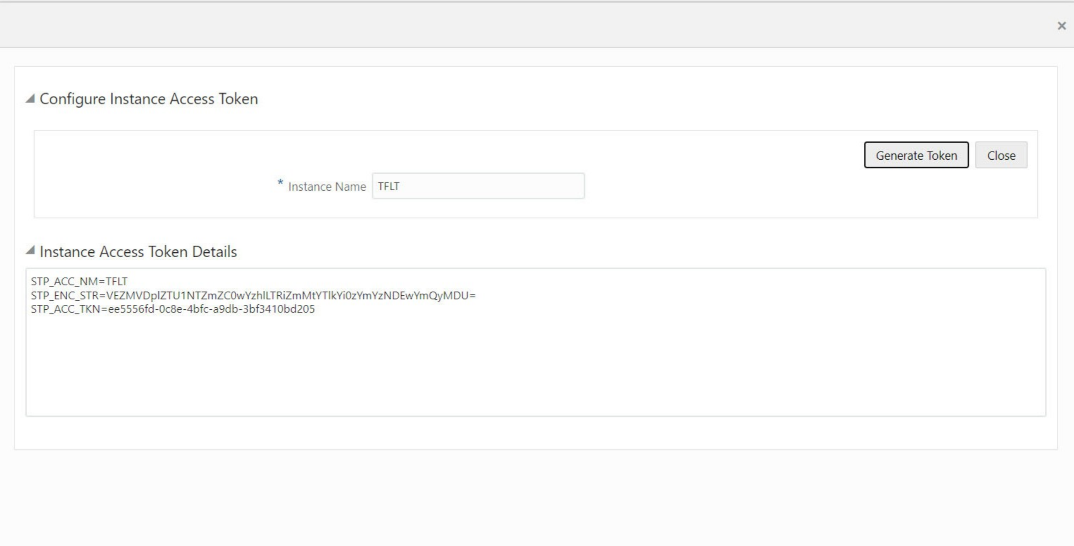
4. Enter the username in the **Instance Name** field and click **Generate Token.** The token is displayed in the **Instance Access Token Details** section.

Figure J-3 Generate Token Button


×
Configure Instance Access Token
Generate Token
Close
* Instance Name
Instance Access Token Details

5. Copy and save the text generated in the **Instance Access Token Details** section.

Figure J-4 Setup Access Token Details


×
Configure Instance Access Token
Generate Token
Close
Instance Access Token Details

* Instance Name: TFLT

```
STP_ACC_NM=TFLT
STP_ENC_STR=VEZMVDplZTU1NTZmZC0wYzhlLTRiZmMtYTlkYi0zYmYzNDEwYmQyMDU=
STP_ACC_TKN=ee5556fd-0c8e-4bfc-a9db-3bf3410bd205
```

The **STP_ACC_NM** field displays the username. The **STP_ACC_TKN** field displays the password.

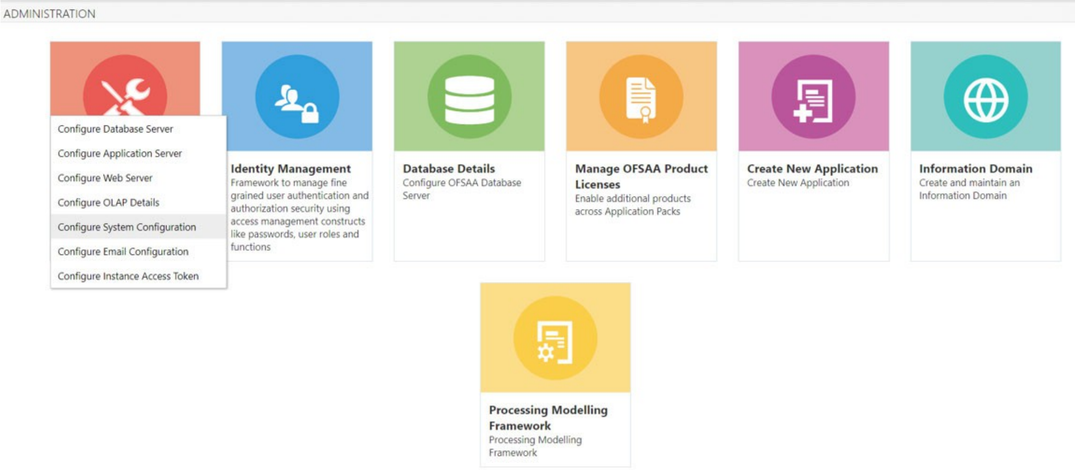
6. Click **Close** and log out as the system administrator.

J.2 Change Token Validity

To generate a password for the user, follow these steps:

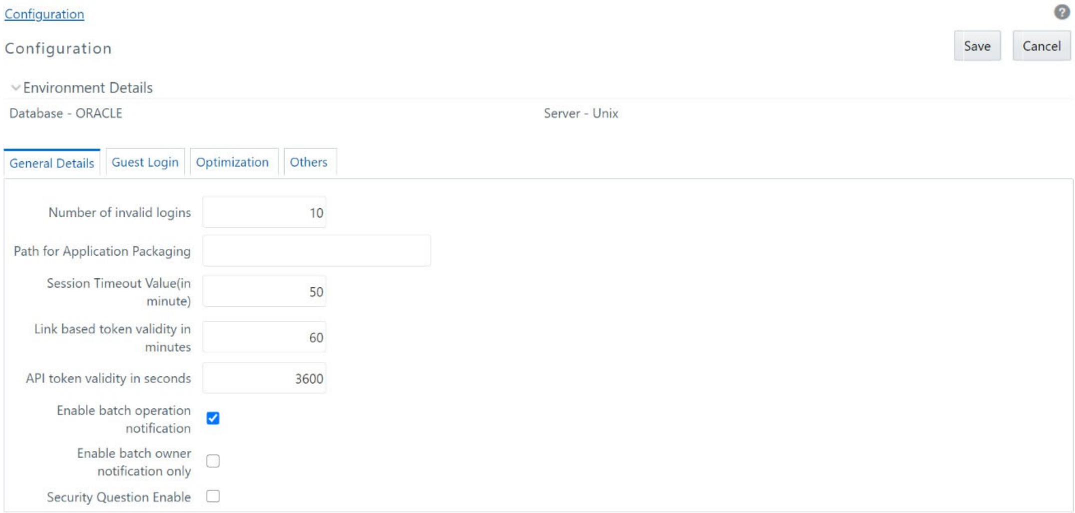
1. Log in as a system administrator.
2. Click **System Configuration** in the **Administration** page and select **Configure System Configuration**. The **Configuration** window is displayed.

Figure J-5 Administration Page


ADMINISTRATION
Configure Database Server
Configure Application Server
Configure Web Server
Configure OLAP Details
Configure System Configuration
Configure Email Configuration
Configure Instance Access Token
Identity Management
Framework to manage fine grained user authentication and authorization security using access management constructs like passwords, user roles and functions
Database Details
Configure OFSAA Database Server
Manage OFSAA Product Licenses
Enable additional products across Application Packs
Create New Application
Create New Application
Information Domain
Create and maintain an Information Domain
Processing Modelling Framework
Processing Modelling Framework

3. In the **Configuration window, c**hange the token validity time in the **API token validity** in **seconds** field.

Figure J-6 Configuration window with the API token validity in seconds field shown



Configuration

Configuration

Environment Details

Database - ORACLE

Server - Unix

General Details | Guest Login | Optimization | Others

Number of invalid logins: 10

Path for Application Packaging:

Session Timeout Value(in minute): 50

Link based token validity in minutes: 60

API token validity in seconds: 3600

Enable batch operation notification: ☑

Enable batch owner notification only: □

Security Question Enable: □

4. Click **Save**.

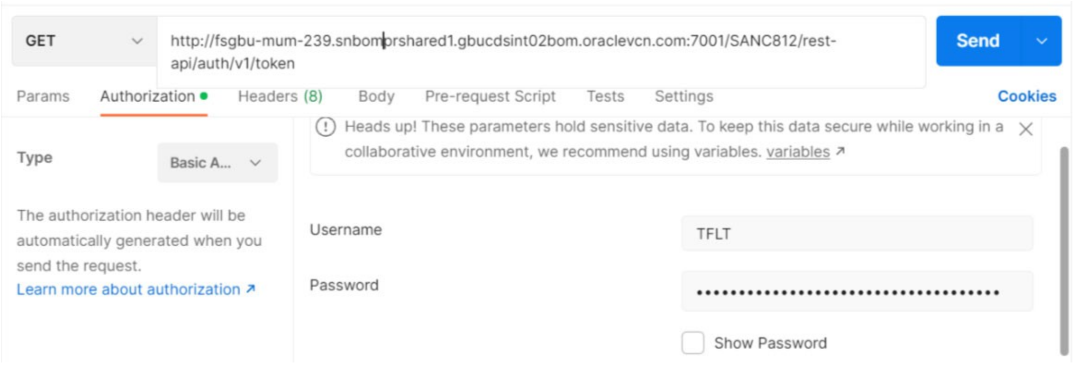
J.3 Generate Token

After the password is generated, you can generate the token. To generate the token, open your API client and follow these steps:

> **Note**
>
> - You may use the desktop version of the Postman client to perform these steps. Postman is an open-source, collaborative platform for API development. For more information, see Postman Docs.
> - You can also use any other API client, such as cURL. For more information, see REST APIs for Oracle Database.

1. Open the Postman client and click **Create a request**.
2. Select the request type as **GET** and enter the request URL in the following format: `##APP_URL##/rest-api/auth/v1/token`

Figure J-7 Request



GET http://fsgbu-mum-239.snbomprshared1.gbucdsintO2bom.oraclevcn.com:7001/SANC812/rest-api/auth/v1/token

Type: Basic A...

The authorization header will be automatically generated when you send the request.

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables.

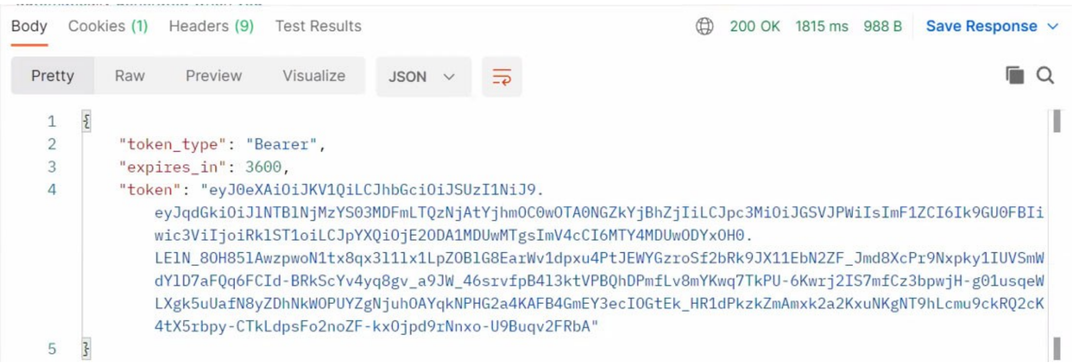
Username: TFLT

Password: ••••••••••••••••••••••••••••••••••••

□ Show Password

3. Select the **Authorization** menu and then select the **TYPE** as **Basic Auth**.
4. Enter the username and password.
   The username is the value generated for the **STP_ACC_NM** attribute and the password is the value generated for the **STP_ACC_TKN** attribute.
5. Click **Send**. The token is displayed in the **Response** field.

Figure J-8 Response



```
{
    "token_type": "Bearer",
    "expires_in": 3600,
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
        eyJqdGkiOiJlNTBlNjMzYS03MDFmLTQzNjAtYjhmOC0wOTA0NGZkYjBhZjIiLCJpc3MiOiJGSVJPWiIsImF1ZCI6Ik9GU0FBIi
        wic3ViIjoiRklST1oiLCJpYXQiOjE2ODA1MDUwMTgsImV4cCI6MTY4MDUwODYxOH0.
        LElN_8OH85lAwzpwoN1tx8qx3l1lx1LpZOBlG8EarWv1dpxu4PtJEWYGzroSf2bRk9JX11EbN2ZF_Jmd8XcPr9Nxpky1IUVSmW
        dYlD7aFQq6FCId-BRkScYv4yq8gv_a9JW_46srvfpB4l3ktVPBQhDPmfLv8mYKwq7TkPU-6Kwrj2IS7mfCz3bpwjH-g01usqeW
        LXgk5uUafN8yZDhNkWOPUYZgNjuhOAYqkNPHG2a4KAFB4GmEY3ecIOGtEk_HR1dPkzkZmAmxk2a2KxuNKgNT9hLcmu9ckRQ2cK
        4tX5rbpy-CTkLdpsFo2noZF-kxOjpd9rNnxo-U9Buqv2FRbA"
}
```

J.4 Send Requests

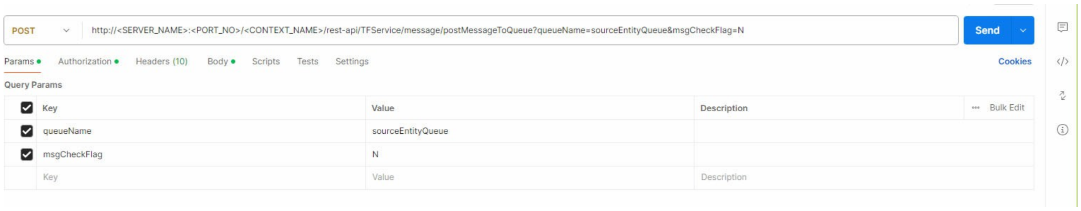
1. Do the following configuration before sending the request using the **POST** request feature.
   a. Go to the path `##DOMIAN_HOME##/applications/##context.ear##/##context.war##/conf`
   b. Open the `RestAPIConf.properties` file.
   c. Add the `hostname` and `port` values inside the `RestAPIConf.properties` file For Example: `hostname=fsgbu-mum-239.snbomprshared1.gbucdsint02bom.oraclevcn.com port=7001`
2. Requests are sent using the **POST** request feature. Use the token generated to authorize the request and pass the JSON in the correct format.

> **Note**
>
> - You may use the desktop version of the Postman client to perform these steps. Postman is an open-source, collaborative platform for API development. For more information, see Postman Docs.
> - You can also use any other API client, such as cURL. For more information, see REST APIs for Oracle Database.

1. In the Postman client, select the request type as **POST** and enter the request URL in the following format:
   - For SWIFT: `##APP_URL##/rest-api/TFService/message/postMessage- ToQueue?queueName=sourceEntityQueue&msgCheckFlag=N`
   - For ISO20022: `##APP_URL##/rest-api/TFService/message/postMessage- ToQueue?queueName=sourceSepaEntityQueue&businessName=RT SEPA Message Attributes&domain=SR&msgCheckFlag=N&externalData=Message Direction:OUTBOUND`

- For Fedwire: `##APP_URL##/rest-api/TFService/message/postMessage- ToQueue?queueName=sourceFedEntityQueue&msgCheckFlag=N`

Figure J-9 Request

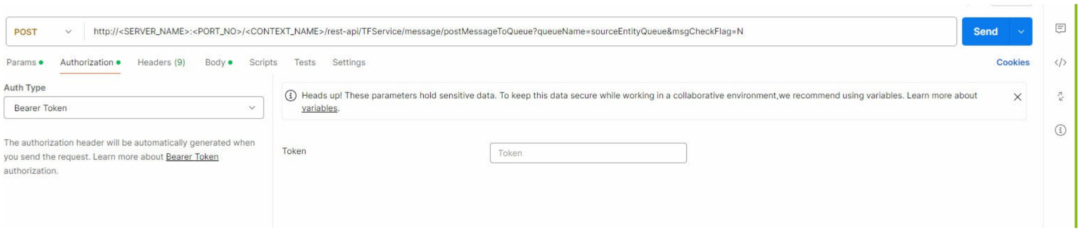


POST http://<SERVER_NAME>:<PORT_NO>/<CONTEXT_NAME>/rest-api/TFService/message/postMessageToQueue?queueName=sourceEntityQueue&msgCheckFlag=N

☑	Key	Value	Description
☑	queueName	sourceEntityQueue	
☑	msgCheckFlag	N	
	Key	Value	Description

2. In the **Authorization** menu, select the **TYPE** as **Bearer Token**.

Figure J-10 Authorization



POST http://<SERVER_NAME>:<PORT_NO>/<CONTEXT_NAME>/rest-api/TFService/message/postMessageToQueue?queueName=sourceEntityQueue&msgCheckFlag=N

Auth Type: Bearer Token

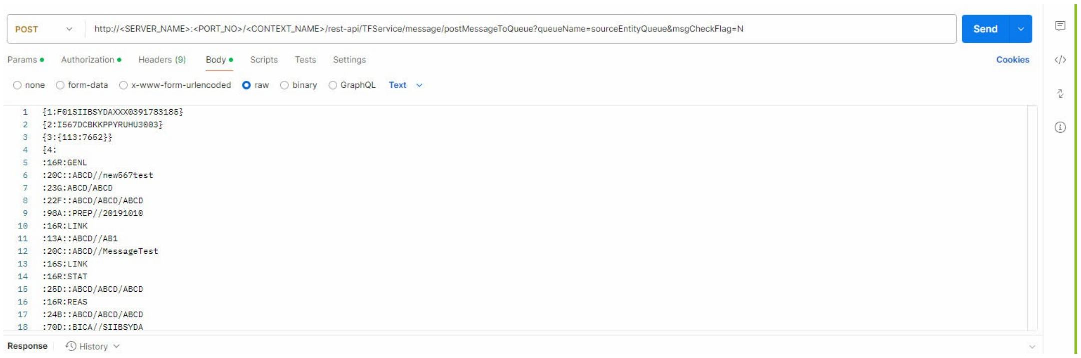
The authorization header will be automatically generated when you send the request. Learn more about Bearer Token authorization.

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment,we recommend using variables. Learn more about variables.

Token: Token

3. Paste the token generated in the **Token** field.
4. Select **Body** tab and select **raw**.
5. Insert the message in the text field.
6. Click **Send**.

Figure J-11 Body Tab



POST http://<SERVER_NAME>:<PORT_NO>/<CONTEXT_NAME>/rest-api/TFService/message/postMessageToQueue?queueName=sourceEntityQueue&msgCheckFlag=N

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL Text

```
{1:F01SIIBSYDAXXX0391783185}
{2:I567DCBKKPPYRUHU3003}
{3:{113:7652}}
{4:
:16R:GENL
:20C::ABCD//new567test
:23G:ABCD/ABCD
:22F::ABCD/ABCD/ABCD
:98A::PREP//20191010
:16R:LINK
:13A::ABCD//AB1
:20C::ABCD//MessageTest
:16S:LINK
:16R:STAT
:25D::ABCD/ABCD/ABCD
:16R:REAS
:24B::ABCD/ABCD/ABCD
:70D::BICA//SIIBSYDA
```

K

Function Codes for User Groups

All actions or functions in the Transaction Filtering (TF) application is configured with a function code. You can define the functionalities for the particular user group by assigning the required functional code to the user group. If a function code is mapped to the user group, the functionality corresponding to the functional code is enabled in the UI.

Table K-1   Function Codes for User Groups

Function Codes	Function Name and Description	TFLTANYST	TFLTSUPV	TFSNRSUPER	TFREADONLY
TFQALLALRT	**TF Queue All Alerts Access:** Access to View All Alerts on the List Page through Queue	-	-		
TFACSALLQ	**TF All Queue Open Access:** Access to open any queue in the Queue dashboard	-	-		
TFQGETNEXT	**TF Get Next Queue Access:** Access to get the next queue alerts on the details page	-	-		
TFQGNXTALL	**TF Get Next Access to View All Alerts:** Access to view all alerts from get next in the queue	-	-		
TFALRTASGN	**TF Alert Assignment Access:** Access to assign alerts when the user opens an alert from the List Page				-
TFALATCHM T	**TF Alert List Attachment Access:** Access to select and save attachments for an alert in the List Page				-
TFBLKACNT	**Transaction Filtering Bulk Update Access:** This function gives access to Bulk Update in List Page.	-	-		-
TFADATCHM T	**TF Alert Details Attachment Access:** Access to select and save attachments for an alert on the Details Page				-
TFEVNTDECN	**TF Event Decision Access:** Access to take event-level action in alert Details Page				-

Table K-1 (Cont.) Function Codes for User Groups

Function Codes	Function Name and Description	TFLTANYST	TFLTSUPV	TFSNRSUPER	TFREADONLY
TFEVNTCMTS	**TF Event Level Comments Access:** Access to add or update event-level comments in the alert Details Page				-
TFALRTDECN	**TF Alert Decision Access:** Access to take alert level action for an alert on the Details Page				-
TFLTLMACTN	**TF List Management Actions Access:** Access to List Management Action Buttons	-			-
TFLISTMGMT	**TFLISTMGMT:** Access to TF List Management under the Navigation menu	-			
TFBLKTKACN	Bulk Action Function Code			-	-
TFWSINVADT	**TF Wire Stripping Investigation Audit Access:** Access to insert audit for ws investigation against compared alert into current alert audit history				-

ⓘ **Note**

If you configure any of the following function codes to a user group, you must also configure the TFALRTASGN function code to the user group as a mandatory function code:

- TFADATCHMT
- TFEVNTDECN
- TFEVNTCMTS
- TFWSINVADT

L

Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMIT in Python Interpreter

An interpreter is a program that directly executes instructions written in a programming or scripting language without requiring them previously to be compiled into a machine language program.

Interpreters are plug-ins that enable users to use a specific language to process data in the backend. In Compliance Studio, Interpreters are used in Notebooks to execute code in different languages. Each The interpreter has a set of adjusted and applied properties across all notebooks. For more information on Interpreter Configuration and Connectivity, see OFS Compliance Studio Administration and Configuration Guide.

Using the **zeppelin.interpreter.output.limit** field you can enter the output message limit. Any message that exceeds the limit is truncated.

L.1 Configuring through the UI

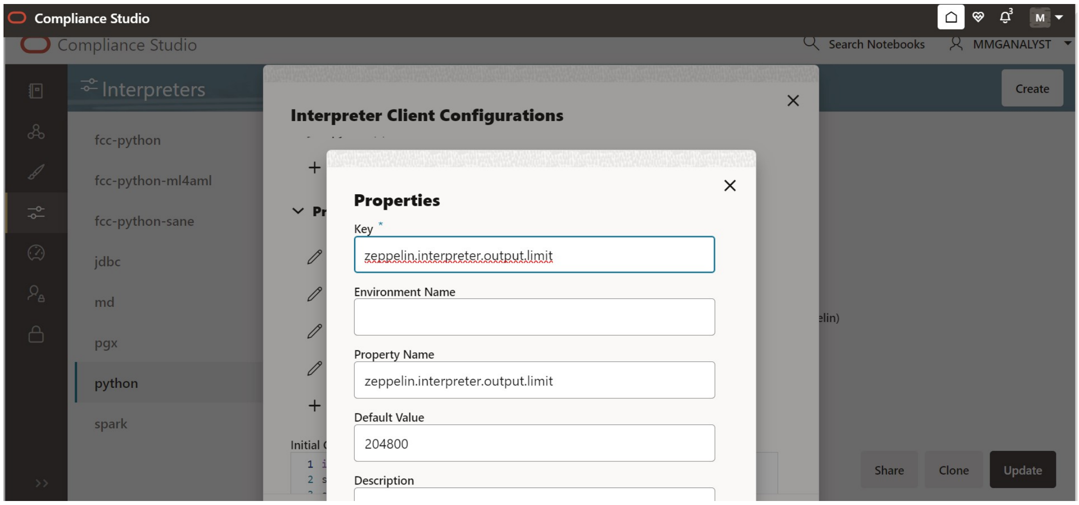
Follow the subsequent steps to configure the **zeppelin.interpreter.output.limit** through the UI:

Using the Wizard Screen:

1. Click the **User** Icon right top corner.
2. Go to **Data Studio Options**.
3. Click **Interpreters**. The Interpreters page is displayed.
4. select the python interpreter for which you want to configure the **zeppelin.interpreter.output.limit.**
5. Select python from the LHS options.
6. Click on the Wizard Icon.
7. From the RHS side click on **oracle.datastudio.python.DsPythonInterpreter** under Interpreter Client Configurations. The Interpreter Client Configuration popup is displayed.
8. Under Properties, click on +Properties. The Properties popup is displayed.
9. Fill the options as shown in the following spring-postSacalert.properties file figure . Set the default value to 870400 (for 1000 records approx.).

> **Note**
>
> - Configuration using the Wizard screen is preferable to other ways of configuration.
> - If the data is more than 1000 records, update the **zeppelin.python.maxResult** in properties to the desired value and **zeppelin.interpreter.output.limit** as 870.4 x maxResult.
> - If you cannot see the **Create** and **Cancel** buttons, click on the header label of the Properties window.
> - The default value for zeppelin.interpreter.output.limit i is 102400 (in bytes)
> - Increasing the default value from 102400 bytes to an immense value will slow down the rendering of outputs of python paragraphs.

Figure L-1 spring-postSacalert.properties file



Properties

Key *: zeppelin.interpreter.output.limit

Environment Name:

Property Name: zeppelin.interpreter.output.limit

Default Value: 204800

Description

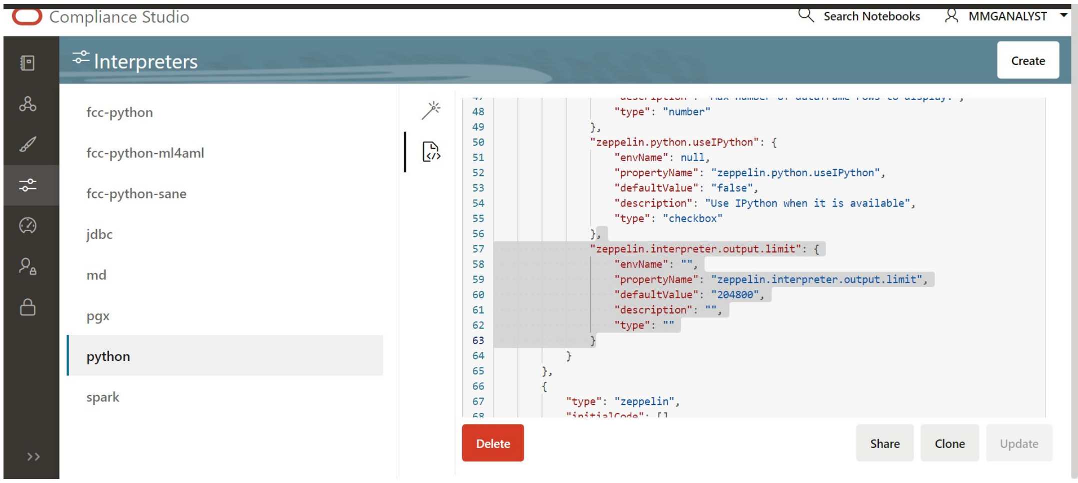
10. Click **Create**. The Interpreter Client Configuration popup is displayed and **zeppelin.interpreter.output.limit** is displayed under **Properties**.
11. Click **Confirm.** The Interpreter Client Configuration window is displayed.
12. Click **Update**.
13. Restart the Compliance Studio application to reflect the changes.

Configuration through JSON Screen:

1. Click the **User** Icon right top corner.
2. Go to **Data Studio Options**.
3. Click **Interpreters**. The Interpreters page is displayed.
4. select the python interpreter for which you want to configure the **zeppelin.interpreter.output.limit.**
5. Select python from the LHS options.
6. Click on the Icon. The JSON configuration screen is displayed.

7. Scroll down and locate interpreterClientConfigs with className **oracle.datastudio.python.DsPythonInterpreter**. you can find the properties section with zeppelin configurations.
8. Add the **zeppelin.interpreter.output.limit**. See the following figure .

Figure L-2   JSON Screen



```
                "type": "number"
            },
            "zeppelin.python.useIPython": {
                "envName": null,
                "propertyName": "zeppelin.python.useIPython",
                "defaultValue": "false",
                "description": "Use IPython when it is available",
                "type": "checkbox"
            },
            "zeppelin.interpreter.output.limit": {
                "envName": "",
                "propertyName": "zeppelin.interpreter.output.limit",
                "defaultValue": "204800",
                "description": "",
                "type": ""
            }
        }
    },
    {
        "type": "zeppelin",
        "initialCode": []
```

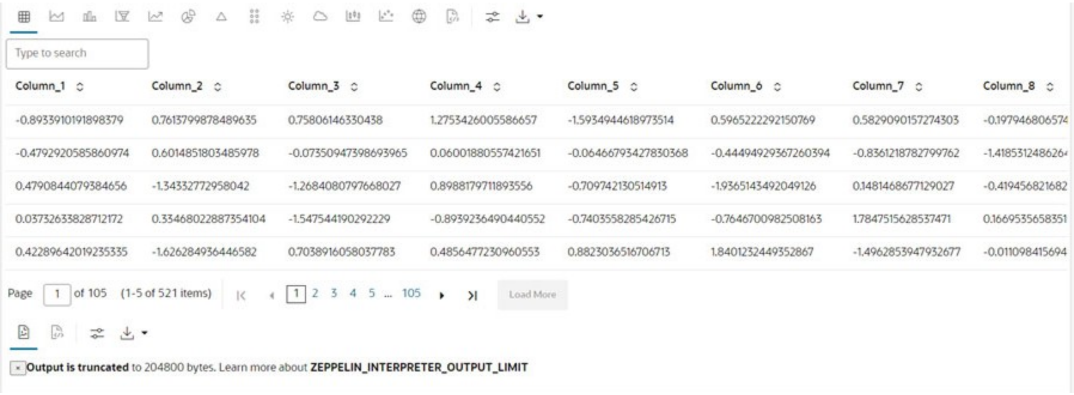
9. The update button will be enabled in the bottom right corner after the JSON modification. Click **Update.**
10. Restart the Compliance Studio application to reflect the changes.

L.2 Configuring through the Filesystem

Follow the subsequent steps to configure the **zeppelin.interpreter.output.limit** through the filesystem:

1. Go to the python interpreter option as pointed out in section Configuring through the UI. You can see the python interpreter listed there if you have run the MMG services before. Delete it, if you run the MMG Application for the first time on a fresh schema, then you don’t need to do this step.
2. After deleting the python interpreter or if the start has not been done, go to the filesystem inside mmg-home/mmg-studio/server/builtin/interpreters, and open python.json in a text editor.
3. Scroll down under **interpreterClientConfigs** with className **,racle.datastudio.python.DsPythonInterpreter,** you will find the following properties section with Zeppelin configurations. After the last entry in properties, add the zeppelin.interpreter.output.limit using the JSON screen.
4. Save the python.json with the desired default value.
5. Restart the Compliance Studio application to reflect the changes.

Figure L-3 Output in table view



Column_1	Column_2	Column_3	Column_4	Column_5	Column_6	Column_7	Column_8
-0.8933910191898379	0.7613799878489635	0.75806146330438	1.2753426005586657	-1.5934944618973514	0.5965222292150769	0.5829090157274303	-0.197946806574
-0.4792920585860974	0.6014851803485978	-0.07350947398693965	0.06001880557421651	-0.06466793427830368	-0.44494929367260394	-0.8361218782799762	-1.418531248626
0.4790844079384656	-1.34332772958042	-1.2684080797668027	0.8988179711893556	-0.709742130514913	-1.9365143492049126	0.1481468677129027	-0.419456821682
0.03732633828712172	0.33468022887354104	-1.547544190292229	-0.8939236490440552	-0.7403558285426715	-0.7646700982508163	1.7847515628537471	0.1669535658351
0.42289642019235335	-1.626284936446582	0.7038916058037783	0.4856477230960553	0.8823036516706713	1.8401232449352867	-1.4962853947932677	-0.011098415694

☒ **Output is truncated** to 204800 bytes. Learn more about **ZEPPELIN_INTERPRETER_OUTPUT_LIMIT**

You can see the ZEPPELIN_INTERPRETER_OUTPUT_LIMIT value as a warning if the table content is more than the set default value for zeppelin.interpreter.output.limit, and accordingly, you can modify the default value for the same.

M

API to Check the Status of EDQ Job

You can check the status of the EDQ job by sending a real-time request in GET method. To execute the request, follow the subsequent steps:

1. Open Postman or a relevant tool.
2. Go to the Header tab.
3. Send a request using the GET method. The request must be in the following format:
   `http://<App_Host>:<App_Port>/TFLT/service/checkEDQ?edqUrl=http://<Edq_Host>:<Edq_Port>`

Enter the following optional parameters in the Query Params table:

Table 2: Query Params for Individual Screening

Table M-1   Query Params for Individual Screening

Key	Value
extraServiceName	< WEBSERVICE URL>
timeoutSeconds	<Place Holder Value>

> **Note**
>
> The Key and Value fields are case sensitive.

You will get the following sample response for a successful execution:

```
{"payload":[{"serviceUrl":"http://100.76.129.18:8001/edq/restws/
Transaction_Screening:Name_x20 x26 x20_Address_x20_Screening","serviceName ":
"Name & Address Realtime Screening","responseCode":200,"status":"SUCCESS"},
{"serviceUrl":"http:// 100.76.129.18:8001/edq/restws/ Transaction_Screening:
Identifier_x20_Screening","serviceName":"Identifier Screening","responseCode":
200,"status":"SUCCESS"},{"serviceUrl":"http:// 100.76.129.18:8001/edq/restws/
Transaction_Screening:
Country_x20 x26 x20_City_x20_scanning_x20_Web_x20_Se rvice","serviceName":
"Country And City Scanning","responseCode":200,"status":"SUCCESS"},
{"serviceUrl":
"http:// 100.76.129.18:8001/edq/restws/ Transaction_Screening:
Narrative_x20_Web_x20_Service","serviceName":"Narrativ e
Screening","responseCode":
200,"status":"SUCCESS"},{"serviceUrl":"http:// 100.76.129.18:8001/edq/restws/
Transaction_Screening:
Port_x20_Screening","serviceName":"Port
Screening","responseCode":200,"status":"SUCCESS"},
{"serviceUrl":"http:// 100.76.129.18:8001/edq/restws/
Transaction_Screening:Goods_x20_Screening",
"serviceName":"Goods
Screening","responseCode":200,"status":"SUCCESS"}],"message":
"EDQ and Enabled webservices are up.","status":"SUCCESS"}
```

N

API to Check the Sanctions Alert Status

You can check the status of Sanctions alerts by sending a real-time request in GET method. To execute the request, follow the subsequent steps:

1. Open **Postman** or a relevant tool.
2. Go to the **Header** tab.
3. Send a request using the **GET** method. The request must be in the following format: `http://<App_Host>:<App_Port>/<context name>/SanctionsService/ alertsZipper/ getAlertSummary?alertId=<alertId>`

You will get the following **sample response** for a successful execution:

```
{
"response": {
"autoreleaseflag": "N",
"msgclasskey": "-1",
"createddate": "11-Feb-25 12.43.01 AM",
"overdueslanotifsts": "",
"grpmsgtype": "pacs.003.001.02",
"slamindate": "",
"autoactionstatuscd": "",
"modifieddate": "17-Feb-25 11.59.08 AM",
"lastmodifiedby": "SYSTEM",
"statuscd": "2",
"lockedtimedate": "21-Feb-25 12.40.51 AM",
"score": "99",
"createdby": "SYSTEM",
"entityName": "TF",
"biccode": "",
"applicablestatus": "",
"dataOrigin": "TF_L1",
"assigneeuser": "TFANALYST",
"msgclasscode": "",
"cutoffendmindate": "",
"msgtype": "2",
"responseid": "511983",
"direction": "OUTBOUND",
"displaycutofftimezone": ": ",
"owner": "",
"grpmsgid": "99025",
"comments": "Alert is Created, Transaction is on Hold",
"entityCode": "512009",
"entityType": "TF_ESC_ALERT",
"focusFlag": "N",
"jurisdictioncode": "All",
"priority": "1",
"businessdomian": "All",
"biccodekey": "-1",
"alertreceiveddate": "2025-02-11T12:43:00Z",
"alerttype": "1",
"overduenotifsts": "",
"lockedby": "TFANALYST",
"entityTypeCode": "TF_ESC_ALERT",
"riskscore": "99",
"fiswsalert": "N",
"alertid": "512009"
},
"message": "Alert summary retrieved for this Id=512009",
"status": "SUCCESS"
}
```

O

ISO Batch Performance Improvement

You can improve the ISO batch performance using the following options:

- Multiparser
- MultiEDQ
- MultiFeedback.

O.1 Multiparser

Follow the subsequent steps to improve the ISO batch performance using the multiparser option:

1. Create a **ficdb**, **fichome** and **inputXML** folder in target server(s).
2. Copy the entire **ficdb** folder and files under **ficdb** from Master server (OFSAA ficserver) to target server's **ficdb** folder.
3. Create a **conf** folder under fichome in target server.
4. Copy the entire files under `$FIC_HOME/conf` from Master server to target server's **fichome/conf** folder.
5. Add the absolute path of ficdb with label FIC_DB_HOME to .profile in target server.
   For example: `export FIC_DB_HOME=<FIC_DB_HOME_PATH> is a commad that you need to enter in .profile.`
6. Add the absolute path of fichome with label `FIC_HOME` to `.profile` in target server.
   For example: `export FIC_HOME=<FIC_HOME_PATH>` is a command that you need to enter in .profile.
7. Add the parser server details to `FCC_TF_ISOBATCH_PARSER_SERVERS` table which will be used for multiParser using the subsequent utility:
   In Master server, Navigate to `$FIC_DB_HOME/bin` and execute `./ISOBatchParserServerInsert.sh <infodom_name>` to add target server(s) when prompted.

   For example:./ISOBatchParserServerInsert.sh SANC812INFO is the command that you need to execute.

   > **Note**
   >
   > Task1 (`TF_CallXMLParser`) of ISO20022 Batch has two operational modes:
   >
   > - normal (N)
   > - multiparser (M)
   >
   > By default, parser will execute in normal mode(N).

8. Change the operational mode only in Master server's `CallXMLParser.sh` under **ficdb/bin** folder.

> **Note**
>
> Target Servers operational mode should always be N.

9. Once the batch message files are placed in the Master server's XML PATH, Navigate to `$FIC_DB_HOME/bin` path and execute `./ISOBatchInputFilesDistributor.sh <infodom_name> <mis_date_xml_path`. It will distribute the message files to target server.
   For example: `./ISOBatchInputFilesDistributor.sh SANC812INFO /scratch/tf812dev/san_812/ftpshare/SANC812INFO/STAGE/SEPA/inputXML/20240205`

O.2 MultiEDQ

Follow the subsequent steps to improve the Iso batch performance using the MultiEDQ option:

1. Navigate to `$FIC_HOME/utility/AppPckMastSynch/bin` and open the **./AppPckMastSynch.sh** file.
2. Change the $Pack name to **OFS_SANC_PACK** and save and execute the file.
3. Add the EDQ server details to the `FCC_TF_ISOBATCH_EDQ_SERVERS` table, which will be used for multiEDQ using the below utility.
4. In the Master server, Navigate to `$FIC_DB_HOME/bin and execute ./ISOBatchEDQServerInsert.sh <infodom_name>` to add target EDQ server(s) when prompted.
   For example: `./ISOBatchEDQServerInsert.sh SANC812INFO` is the command that you need to execute.

> **Note**
>
> All the servers in the FCC_TF_ISOBATCH_EDQ_SERVERS table will be used for MultiEDQ.

5. In the TFADMIN screen, navigate to the **Financial Services Sanctions Pack** and go to **Post Load Changes**.
6. Edit the `TF_CallXMLEDQ` task, add a New Input Parameter as `SERVERID`, and Click **Finish**.
7. Create new tasks that are copies of `TF_CallXMLEDQ`. The number of new tasks should be **n-1** for **n** servers, which are added in the `FCC_TF_ISOBATCH_EDQ_SERVERS` table.
8. Navigate to **Financial Services Sanctions** and go to **Rule Run Framework**.
9. Go to **Process**.
10. Select `TF_CallXMLEDQProcess` and Click **Edit**.
11. Click **Component**.
12. Move the newly added tasks from the left (Transformation Rules) to the Right Side in the new Window.
13. Now, there are **n** tasks. For each task, right click and add parameters.
14. In Parameters, enter a Server ID (example: "Server1") from the `V_SERVER_ID` column of the `FCC_TF_ISOBATCH_EDQ_SERVERS` table.
15. Add Server ID as a parameter for each task. Click on **OK**.

> **Note**
>
> Server ID should be enclosed in double-quotes.

All the tasks will be shown with parameters in the Process definition window.

16. Click **Save** and click **No** to save as a new version.

O.3 MultiFeedback

Follow the subsequent steps to improve the Iso batch performance using the MultiFeedback option:

> **Note**
>
> Task6 (TF_CallXMLImmediateFeedbackCreation) of ISO20022 Batch has two operational modes:
>
> - normal (N)
> - multiparser (M)
>
> By default, the feedback generation will execute in normal mode(N).

1. Change the operational mode only in the master server's `CallImmediateXMLFeedbackCreation.sh` under **ficdb/bin** folder.
2. Target Server's operational mode should always be **N**

O.4 Message Data Attributes (IPE) for Custom Batches

> **Note**
>
> To view/edit the Build Hierarchies in TF Admin screen you must map the following user role to the **TFLTADMINISTATORGRP** user group in the System Administrator Screen and authorize the same:
>
> - BMM Hierarchy Access
> - BMM Hierarchy Authorize
> - BMM Hierarchy Read Only
> - BMM Hierarchy Write

If you have a customized TF SEPA Batch, do the subsequent steps:

> **Note**
>
> The following optimization will be automatically updated if it is OOB SEPA Batch (ID:1562321907205). You can refer to the ID under master information of TF_SEPA_messages_batch_process.

1. In the Run definition screen, select `TF_SEPA_messages_batch_process` batch and click Edit.
2. In the Run definition Window, click the **Selector** Drop down and Click **Job Condition**. **The Filter selector** window is displayed.
3. Select **SEPA Batch Hierarchy** from the Left menu and click **Select**. It will move the filter to the right side.
4. Click **OK**. The above Job Condition (Hierarchy) is added to the Tasks List.
5. Click **Next**.
6. Under Detail Information, double-click on the **SEPA Batch Hierarchy** icon on the Job Condition Column. The **Member Selection** window is displayed.
7. Click the current batch and click **Select**. It will be added to the Selected Members List below.
8. Click **ROOT** in Selected Members (if available) and click on Deselect Button on top to remove it from Selected Members List. Finally the current batch should be present in the Selected Members List.
9. Click **OK**.
10. Under Jobs List, select the **Check box** of the current batch for Message Data Attributes (Task3).
11. Click **Save**
12. Click **Yes**.

> **Note**
>
> If you are installing patch 8.0.8.2.19 you must perform the *Message Data Attributes (IPE) for Custom Batches* chapter.

Glossary

Index