Oracle Financial Services

Transaction Filtering

Administration Guide

Release 8.1.2.4.0

March 2023

F22529-01

OFS Transaction Filtering Admin Guide

Document Control

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

Table 1: Document Control

Version Number	Revision Date	Change Log
2.0	April 2023	• Added Appendix J: Configurations for the Bearer Token section. • Added Adding New Message Type in NACHA section. • Added JMS Queue Creation for SWIFT, Fedwire and ISO20022 Message Types section.
1.0	March 2023	• 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.

Contents

1 About This Guide ... 7

1.1 Intended Audience ... 7

1.2 Access to Oracle Support ... 7

1.3 How This Guide is Organized ... 7

1.4 Where to Find More Information ... 8

1.5 Conventions Used in this Guide ... 8

2 About Oracle financial Services Transaction Filtering ... 10

2.1 Transaction Filtering Workflow ... 10

3 Getting Started ... 12

3.1 Accessing the Oracle Financial Services Analytical Applications (OFSAA) Page ... 12

3.2 Managing the Oracle Financial Services Analytical Applications (OFSAA) Page ... 13

3.2.1 Transaction Filtering Admin Menu ... 13

3.2.2 ISO20022 Configuration Admin Menu ... 14

3.2.3 SWIFT Configuration Admin Menu ... 15

3.2.4 Process Modeller Menu ... 16

3.2.5 FEDWIRE Configuration Admin Menu ... 18

3.2.6 Process Monitor Menu ... 19

3.2.7 Run Definition Menu ... 20

3.2.8 List Management Menu ... 21

3.2.9 Inline Processing Menu ... 22

3.3 Queue Management ... 23

3.3.1 List View ... 23

3.3.2 Grid View ... 25

3.3.3 Configuring New Priority ... 26

3.3.4 Archiving a Queue ... 28

3.4 Troubleshooting Your Display ... 29

3.4.1 Enabling JavaScript ... 29

3.4.2 Enabling Cookies ... 30

3.4.3 Enabling Temporary Internet Files ... 30

3.4.4 Enabling File Downloads ... 30

3.4.5 Setting Printing Options 30

3.4.6 Enabling the Pop-Up Blocker 31

3.4.7 Setting Preferences 31

4 Managing User Administration 32

4.1 About User Administration 32

4.2 Managing User Administration 32

4.2.1 Creating and Authorizing a User 32

4.2.2 Mapping Users with User Groups 32

5 General Configurations 34

5.1 Configuring the Application Level Parameters 34

5.2 Configuring the Good Guy Matching Parameters 35

5.3 Configuring the SLA Parameters 36

5.4 Automatic Assignments of Alerts 38

5.5 Configuring the Cut-Off Parameters for Alerts 40

5.6 Wire Stripping Configuration 42

5.6.1 Configuring Business Data Attribute 45

5.6.2 Configuring Wire Stripping Validation for WS Alert Details Screen 46

5.7 Setting the Priority for Messages 46

5.8 Running the Purge Utility 47

5.9 Adding, Editing or Deleting Good Guy Records 47

5.9.1 Adding a Good Guy Record 47

5.9.2 Editing a Good Guy Record 48

5.9.3 Deleting a Good Guy Record 48

5.9.4 Good Guy Attributes 49

5.9.5 Managing the Good Guy Attributes 50

5.10 Generating Email for Different Statuses 52

5.10.1 Notification Email 52

5.10.2 Task Email 53

5.11 Configuring Alerts in Multiple Jurisdictions and Business Domains 54

5.11.1 Configuring Jurisdictions and Business Domains 55

5.11.2 Configurations to Automatically Assign Transactions 57

5.11.3 Configurations to Automatically Release Transactions 57

5.12 Version Control 58

5.12.1 Version Control for SWIFT Messages and IPE 58

5.12.2 Version Control for ISO20022 58

5.12.3 Version Control for EDQ 58

5.13 Running the Migration Utility for SWIFT, Fedwire and ISO20022 59

5.13.1 Restoring a Previous Message Configuration 60

5.14 Running the Migration Utility for ISO20022 60

5.15 Configuring JMS Correlation ID 62

5.16 Configuring Parallel Processing 62

5.17 Configuring Additional Columns on the Alert List page 63

5.18 Configuring the Parameters for Highlighting the Matched Data 64

5.19 Configuring Select All Option for the Events Table 65

5.20 Retrigger Functionality 65

6 Configuring the SWIFT Message Parameters 66

6.1 Message and Screening Configurations Window 66

6.1.1 Adding or Updating a New Message Type 68

6.1.2 Repeating Sequences 69

6.1.3 Configuring the References 69

6.2 <Message Type> Subfield Level Configuration Window 71

6.3 <Message Type> Screening Configuration Window 72

6.3.1 Enabling or Disabling a Web Service 75

6.3.2 Updating and Removing a Web Service 76

6.3.3 Populating Data for the Trade Goods and Trade Port Web Services 76

6.4 <Message Type> Other Field/Subfield Configuration Window 77

7 Configuring the Fedwire Message Parameters 79

7.1 Message Type Configuration Window 79

7.1.1 Adding or Updating a New Message Type 80

7.1.2 Configuring Message and Transaction References 81

7.2 <Message Type> Subfield Level Configuration Window 81

7.3 <Message Type> Screening Configuration Window 83

7.3.1 Enabling or Disabling a Web Service ... 86

7.3.2 Updating and Removing a Web Service ... 87

7.3.3 Populating Data for the Trade Goods and Trade Port Web Services ... 87

7.4 <Message Type> Other Field/Subfield Configuration Window ... 87

8 Configurations for ISO20022 Message Parameters ... 89

8.1 Configuring the ISO20022 Message Parameters ... 89

8.1.1 SWIFT MX Message Types Configuration ... 99

8.1.2 Running the ISO20022 Batch ... 99

8.2 Audit Queries ... 104

9 Configurations for the US NACHA Batch Process ... 105

9.1 Adding New Message Type in NACHA ... 108

10 Enterprise Data Quality (EDQ) Configurations ... 112

10.1 Performance Improvement Measures for EDQ ... 112

10.2 EDQ Configuration Process Flow ... 113

10.2.1 Importing the Transaction Screening Project ... 119

10.2.2 Configuring Watch List Management and Transaction Filtering ... 119

11 Configuring Risk Scoring Rules ... 132

12 Appendix A: Watch Lists ... 148

12.1 HM Treasury Watch List ... 148

12.2 OFAC Watch List ... 148

12.3 EU Watch List ... 148

12.4 UN Watch List ... 149

12.5 World-Check Watch List ... 149

12.6 Dow Jones Watch List ... 150

12.7 Dow Jones Anti-Corruption Watch List ... 150

12.8 Accuity Watch List ... 150

12.8.1 Using the Accuity Group File ... 151

12.8.2 New Alerts Resulting from Use of the Group File ... 151

12.9 Private Watch List ... 152

12.9.1 Individual Private Watch List Input Attributes ... 152

12.9.2 Entity Private Watch List Input (PLI) Attributes ... 156

13 Appendix B: System Audit Logging Information 161

13.1 Activities for System Audit 161

13.2 Steps for System Audit Activities 161

14 Appendix C: Process Modeller Framework (PMF) Configurability 163

14.1 Configuring the Human Task in the PMF Page 163

14.1.1 Mapping the Transaction Statuses and Transaction Outcomes 163

14.2 Adding Data Fields for the PMF Status 164

14.3 Adding Application Rules for the PMF Status 164

14.3.1 Mapping Rule Types to Application Rules 164

14.3.2 Mapping User Groups to Application Rules 165

14.4 Configurations Required for the Audit Tables 165

14.5 Configurations Required for the setup_rt_params Table 165

14.6 TIME_ZONE Configurations Required for the dim_sanctions_status Table 166

14.7 Creating New User Groups 167

14.8 Other Configurations 167

15 Appendix D: PMF Configurations for Pool of Analyst 168

15.1 Mapping the dim_sanctions_status Table: 173

15.2 Adding Data Fields to the JSON Object 173

15.3 List of Attributes Passed to Workflow 175

15.4 Attribute to Configure the Auto Refresh in Queue Management 176

16 Appendix E: Delta Watch List Configurations 177

16.1 Configurations for the Full and Delta Watch Lists 178

16.1.1 Running the Full Watch list 178

16.1.2 Running the Delta Watch List 179

16.1.3 Merging the Delta Watch List to the Full Watch List 179

16.2 Delta Watch List Configurations for the World-Check Watch List 180

16.2.1 Configurations for the Full and Delta Watch Lists 180

16.2.2 Running the Full Watch List 181

16.2.3 Running the Delta Watch List 182

16.2.4 Merging the Delta Watch List to the Full Watch List 183

17 Appendix F: Message Categories and Message Types 184

17.1 SWIFT Message Types 184
17.2 ISO20022 Message Types 185
17.3 Fedwire Message Types........ 186
17.4 US NACHA Message Types........ 186
18 Appendix G: Invoking the PMF Workflow from backend........ 187
19 Appendix H: JMS Cluster Environment Creation........ 189
19.1 JMS Server Creation 189
19.2 JMS Module Creation 192
19.3 Sub-Deployment Creation........ 194
19.4 Distributed Queues Creation 195
19.5 Distributed Topic Creation 198
19.6 Connection Factory Creation 200
19.7 JMS Queue Creation for SWIFT, Fedwire and ISO20022 Message Types 202
20 Appendix I: User Group Customization........ 1
21 Appendix J: Configurations for the Bearer Token........ 2
21.1 Generate User Password........ 2
21.2 Change Token Validity 4
21.3 Generate Token 5
21.4 Send Requests 6
22 OFSAA Support Contact Details 8
23 Send Us Your Comments........ 9

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 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=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 2: Conventions Used

Table 2lists the conventions used in this guide.

Table 2: 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.

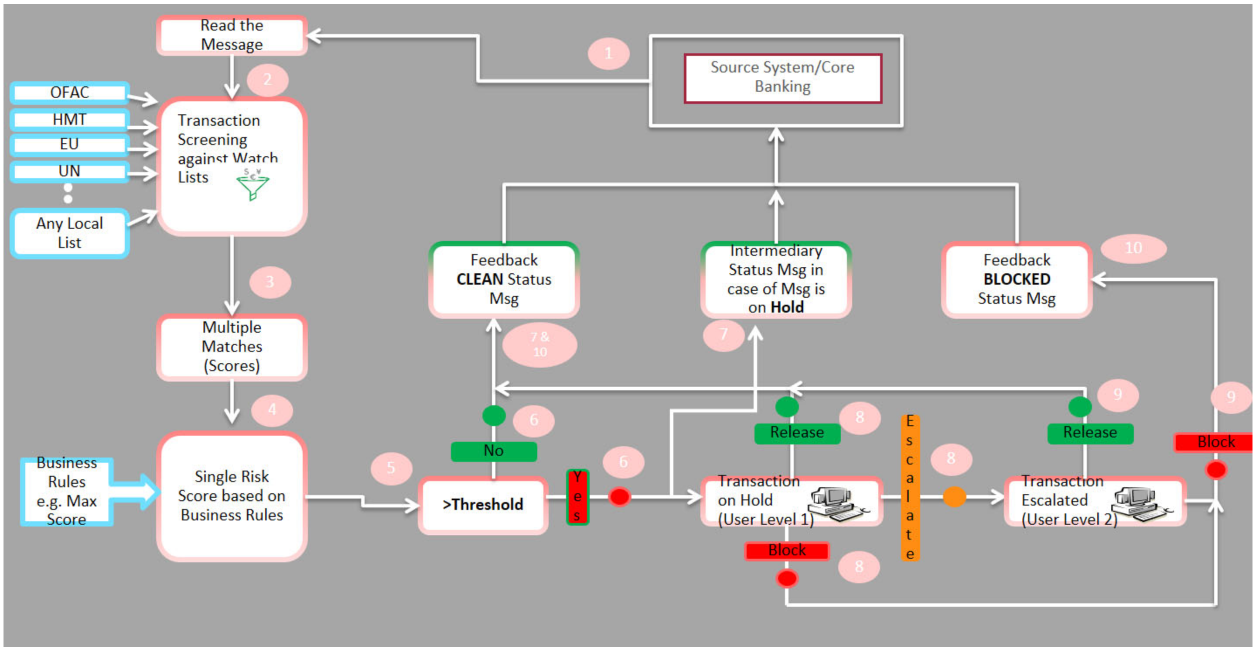
Transaction Filtering against government-regulated watch lists and internal watch lists is a key compliance requirement for financial institutions across the globe. At the turn of the century, Financial Institutions (FIs) were expected to identify customers who were either sanctioned or who lived in 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 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.

3 Getting Started

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

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

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

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

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

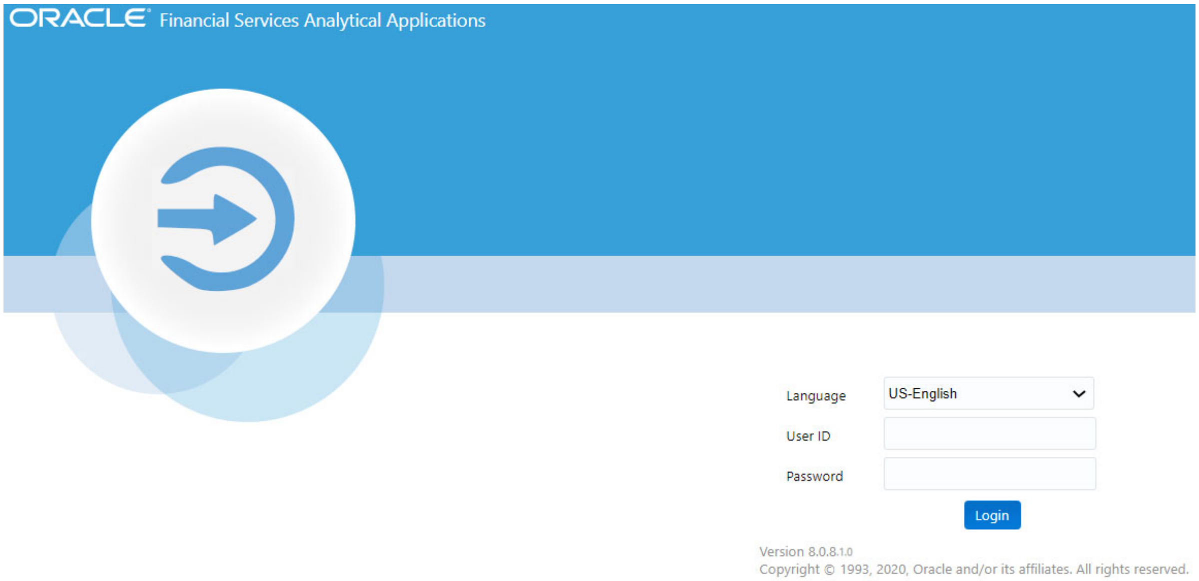
1. Enter the URL into your browser using the following format:

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

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

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

Figure 2: Oracle Financial Services Analytical Applications Login Page



Language: US-English

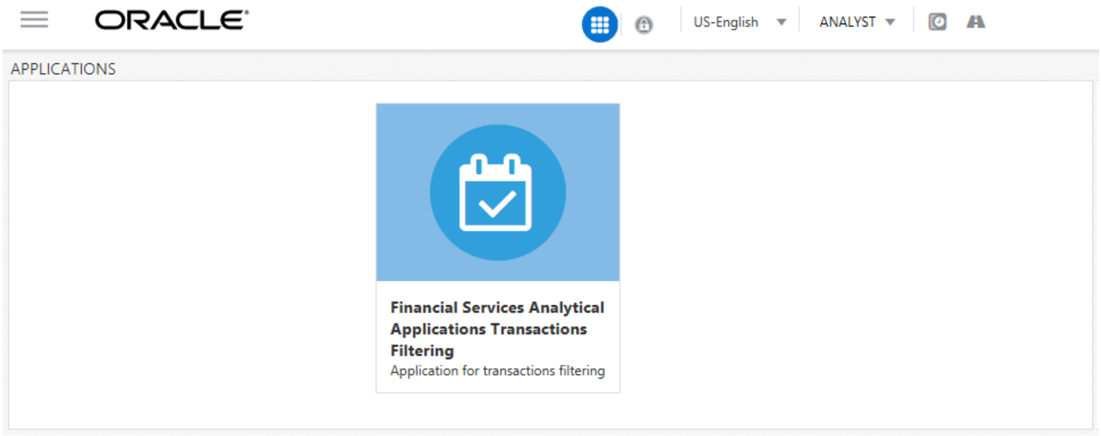
User ID

Password

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: 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** ☑.

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.

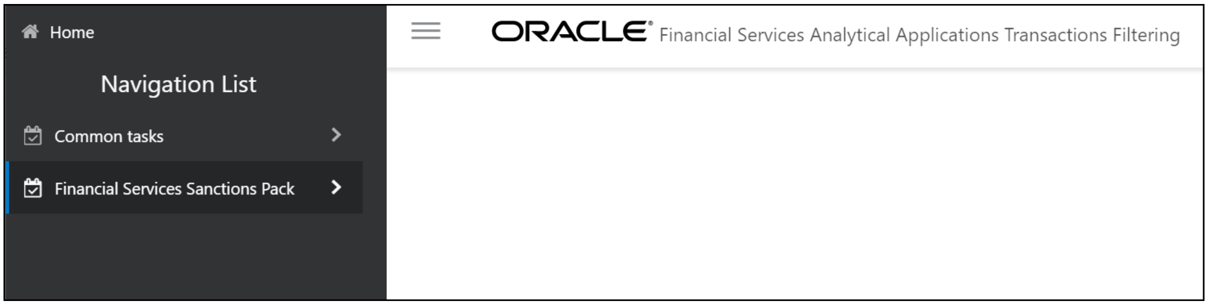
3.2.1 Transaction Filtering Admin Menu

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:

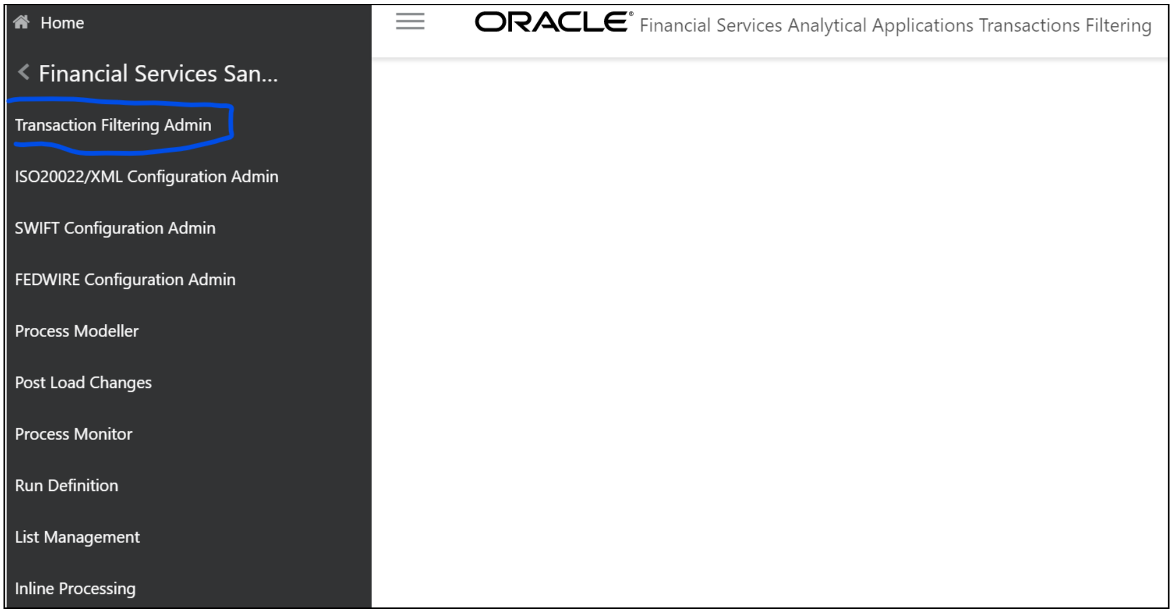
1. From the **Navigation List,** click **Financial Services Sanctions Pack**.

Figure 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, c**lick **Transaction Filtering Admin**. The Configuration Screen displays.

Figure 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

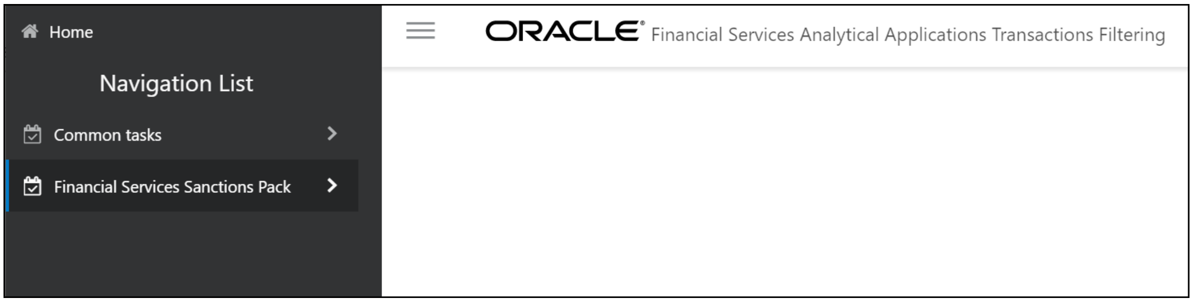
3.2.2 ISO20022 Configuration Admin Menu

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:

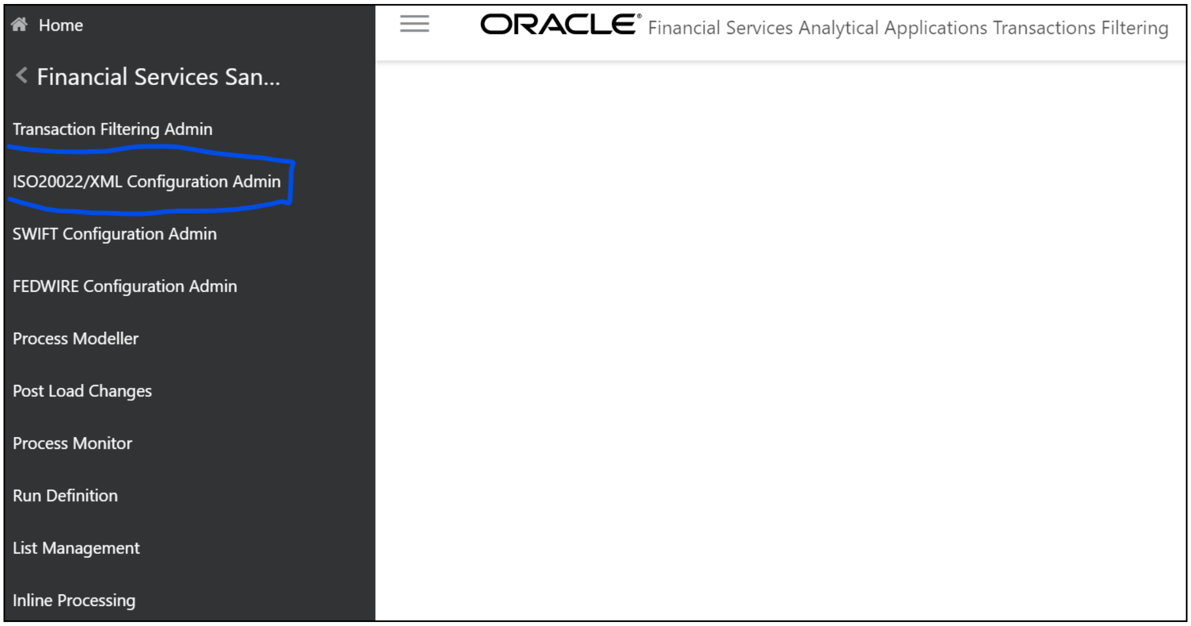
1. Click **Financial Services Sanctions Pack.**

Figure 6: Financial Services Sanctions Pack Menu


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

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

Figure 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

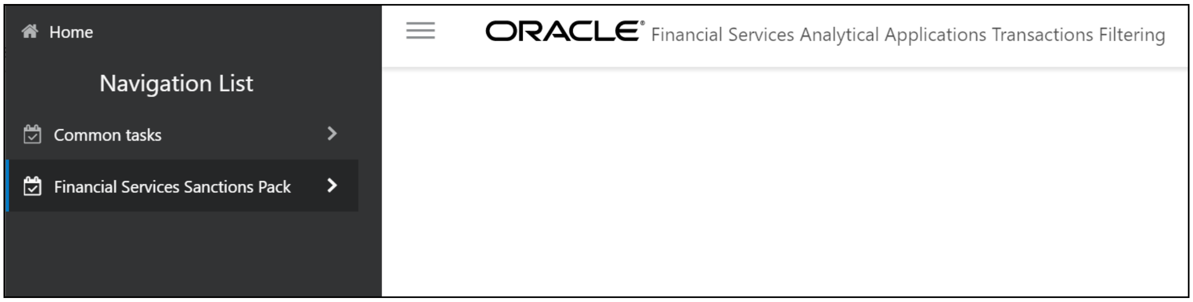
3.2.3 SWIFT Configuration Admin Menu

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:

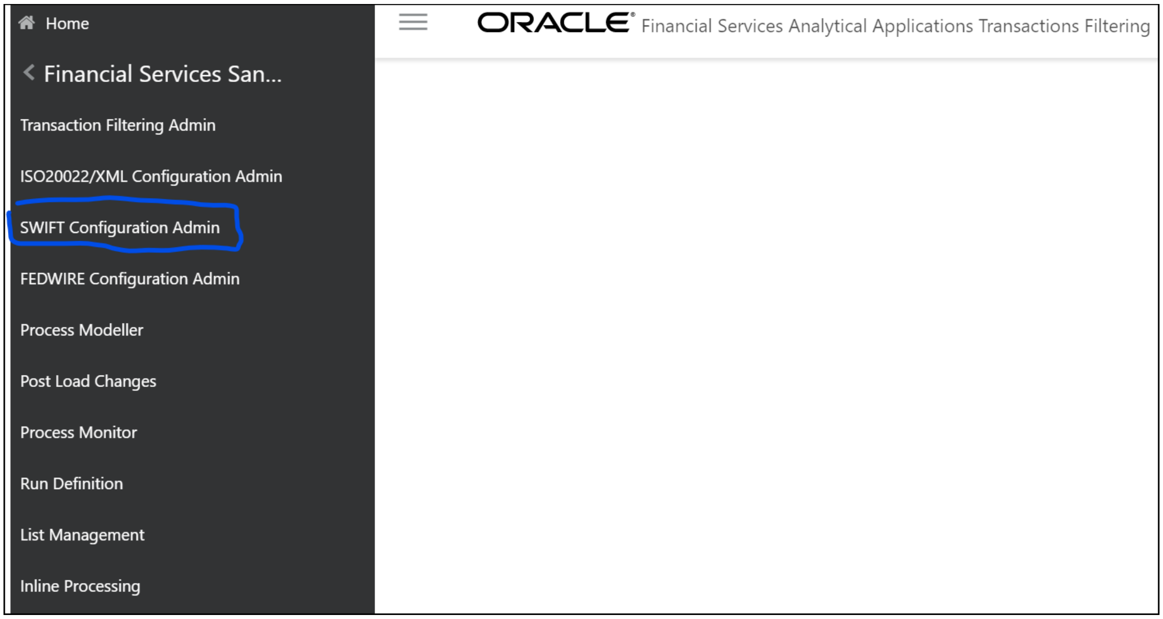
1. Click **Financial Services Sanctions Pack**.

Figure 8: Financial Services Sanctions Pack Menu


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

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

Figure 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

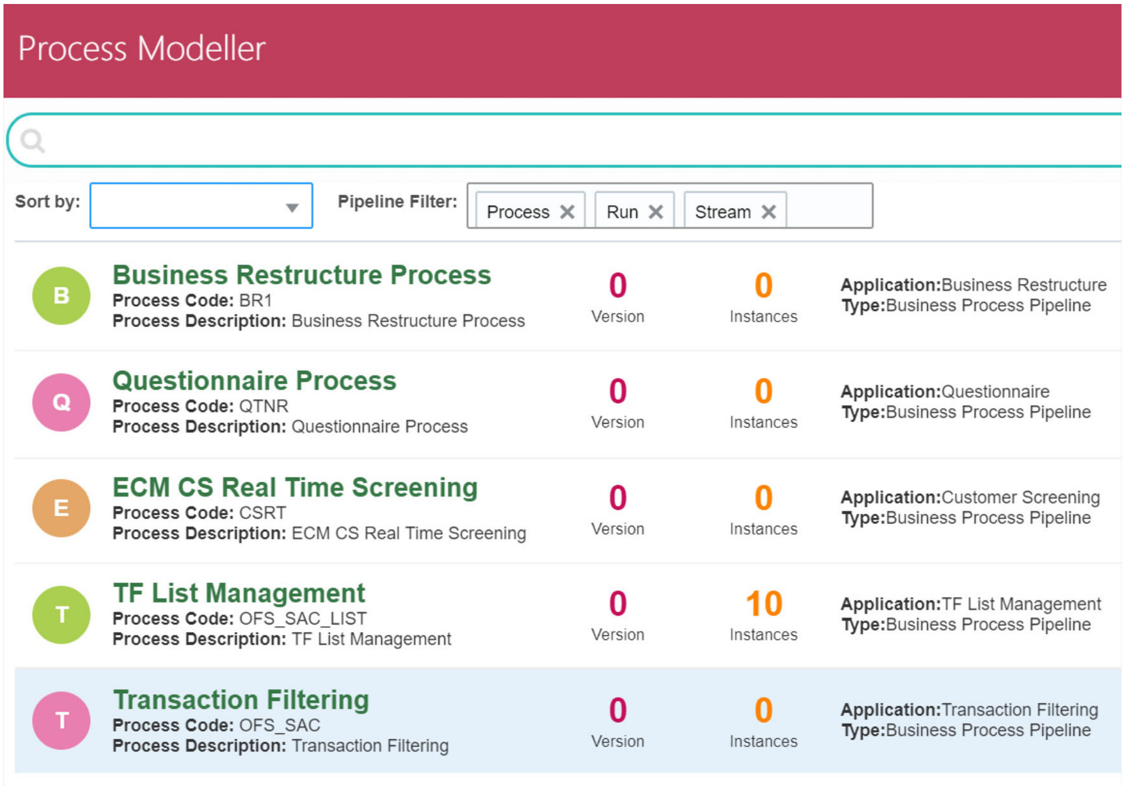
3.2.4 Process Modeller Menu

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 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

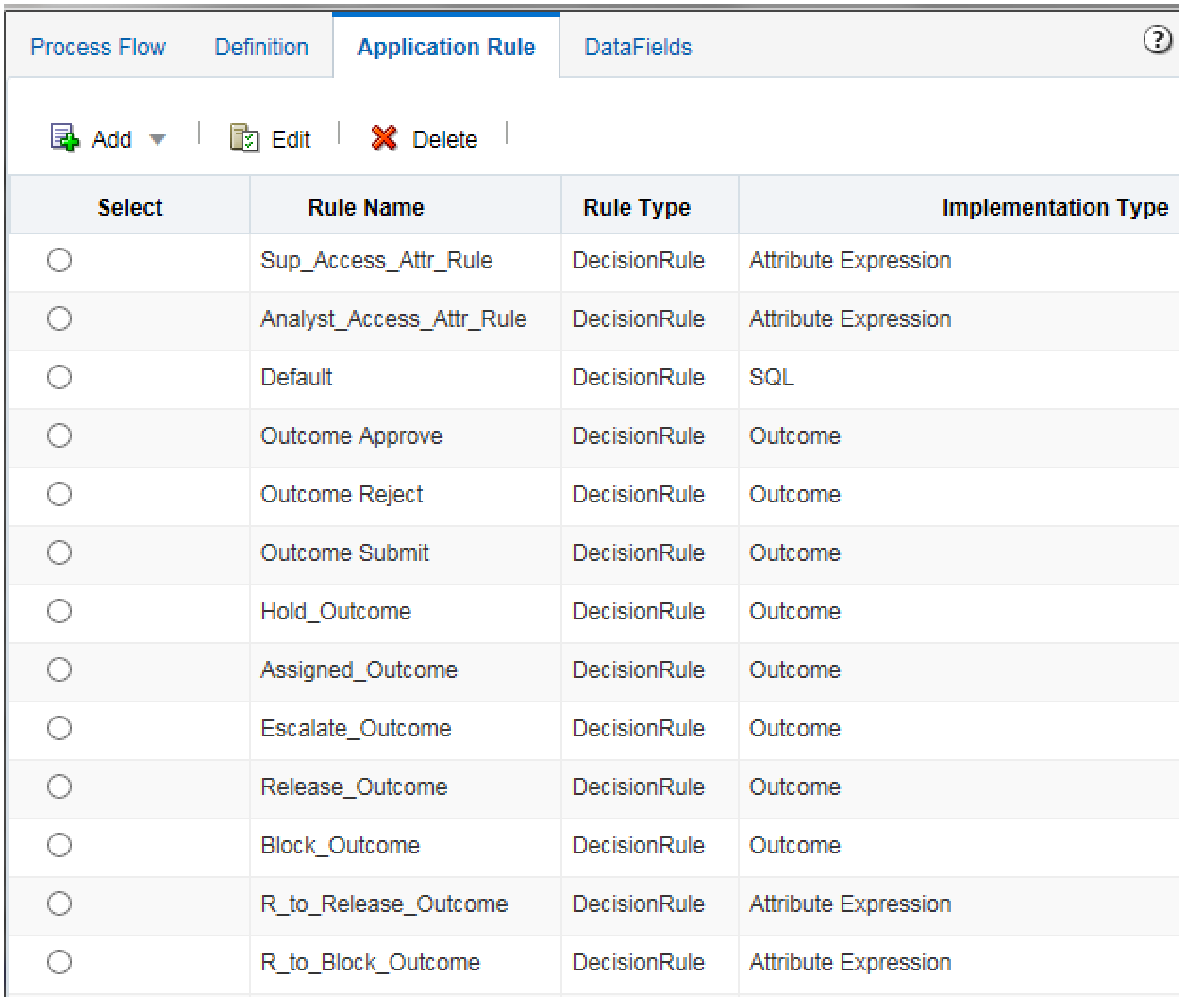
To expand the window, click **Navigation Menu** ≡.

3.2.4.1 Configuring the Transaction Currency

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

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

Figure 11: Application Rule Subtab



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

2. To change the currency for a released transaction, select **R_to_Release_Outcome**. To change the currency for a blocked transaction, select **R_to_Block_Outcome**.
3. Click **Edit**.
4. Click inside the **TF_Currency** drop-down list and select the required currency.
5. Click **Save**.

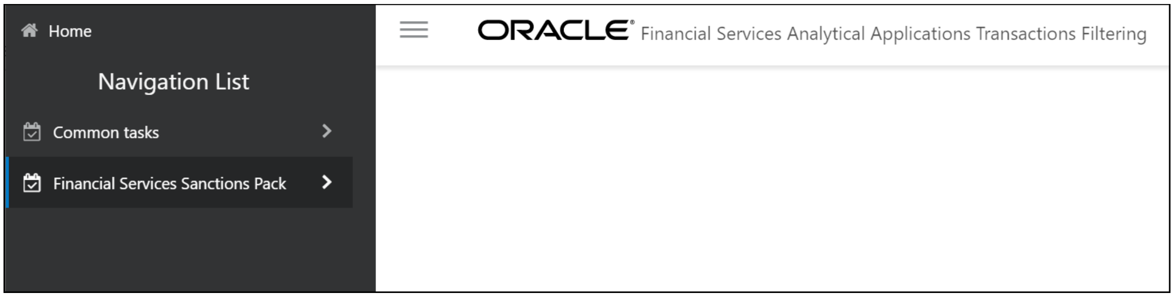
3.2.5 FEDWIRE Configuration Admin Menu

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

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

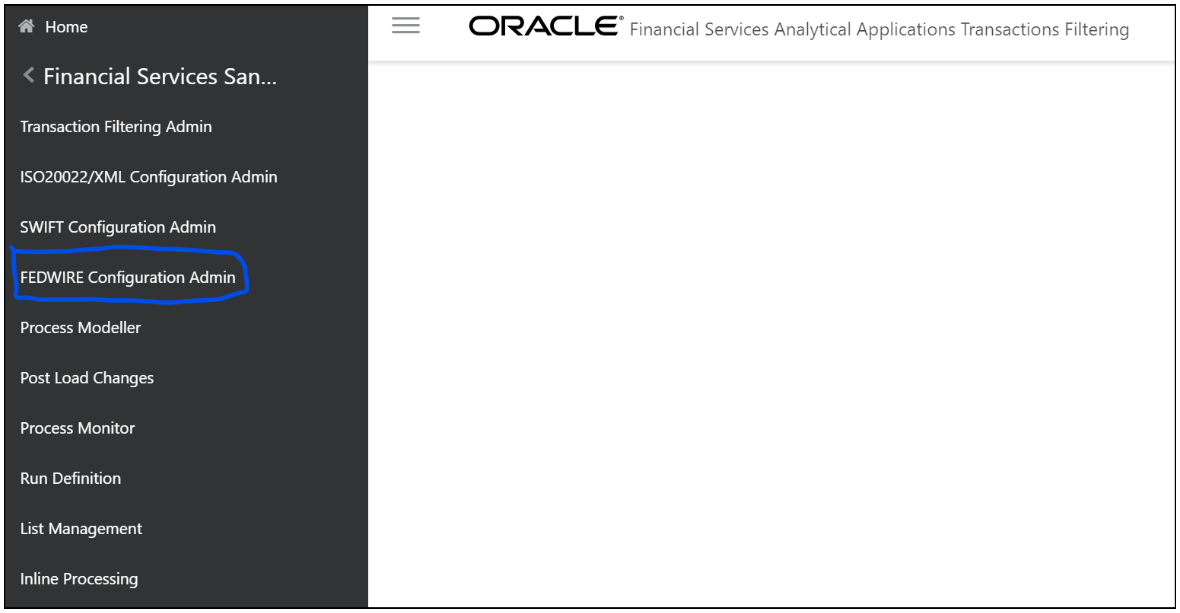
1. Click **Financial Services Sanctions Pack**.

Figure 12: Financial Services Sanctions Pack Menu


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

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

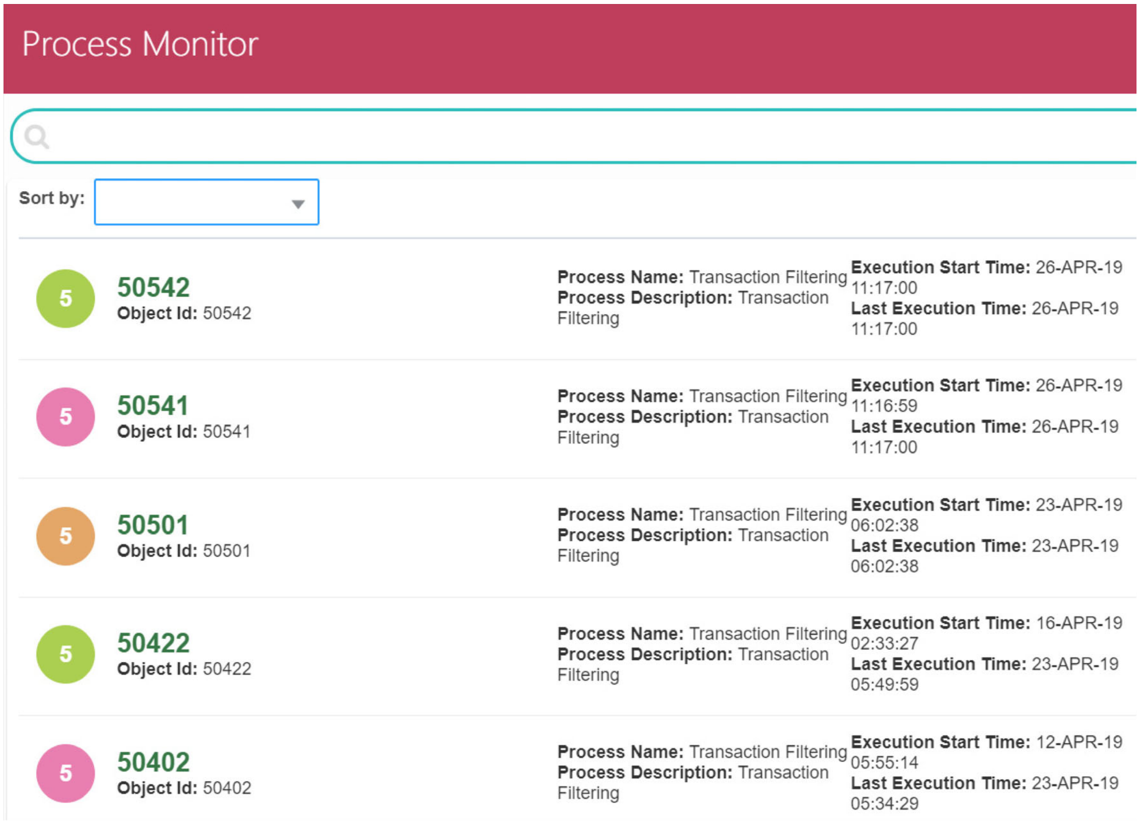
Figure 13: FEDWIRE Configuration Admin Sub-menu


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 14: Process Monitor Menu Page



Process Monitor

Sort by:

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** ☰.

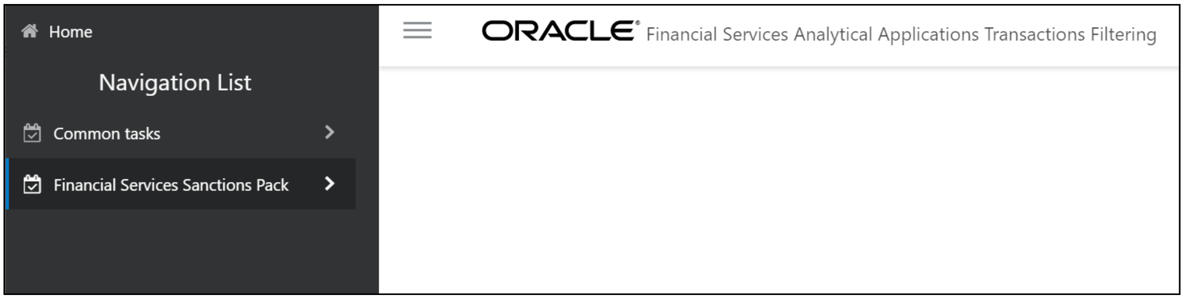
3.2.7 Run Definition Menu

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 **Financial Services Sanctions Pack**.

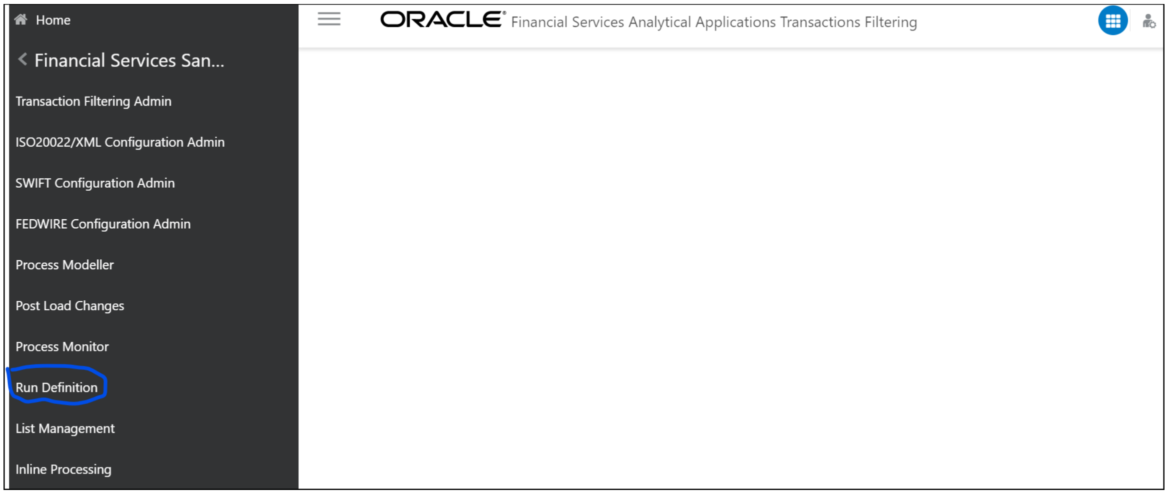
Figure 15: Financial Services Sanctions Pack Menu



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

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

Figure 16: 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

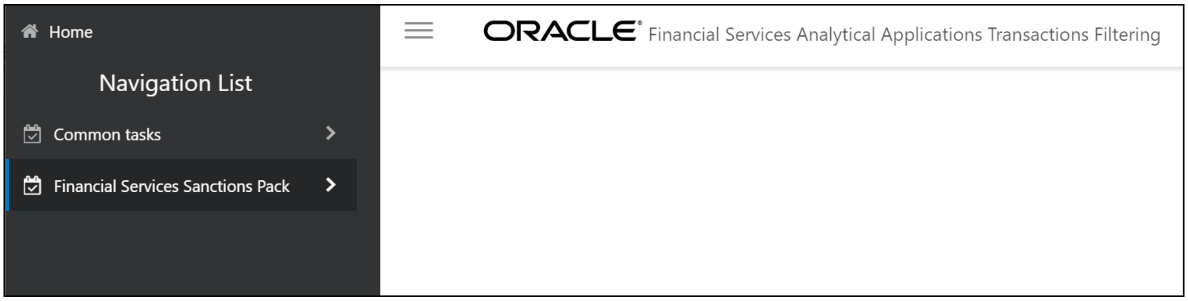
3.2.8 List Management Menu

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:

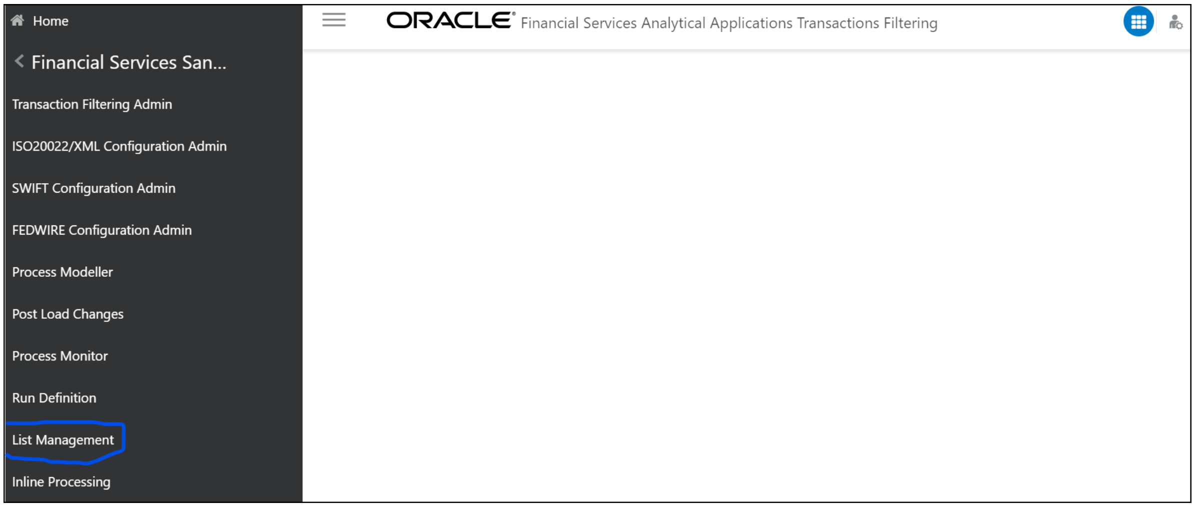
1. Click **Financial Services Sanctions Pack**.

Figure 17: Financial Services Sanctions Pack Menu


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

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

Figure 18: 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

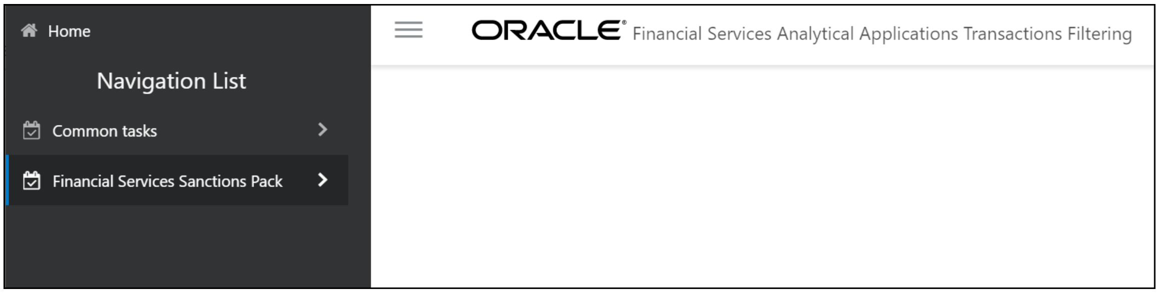
3.2.9 Inline Processing Menu

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:

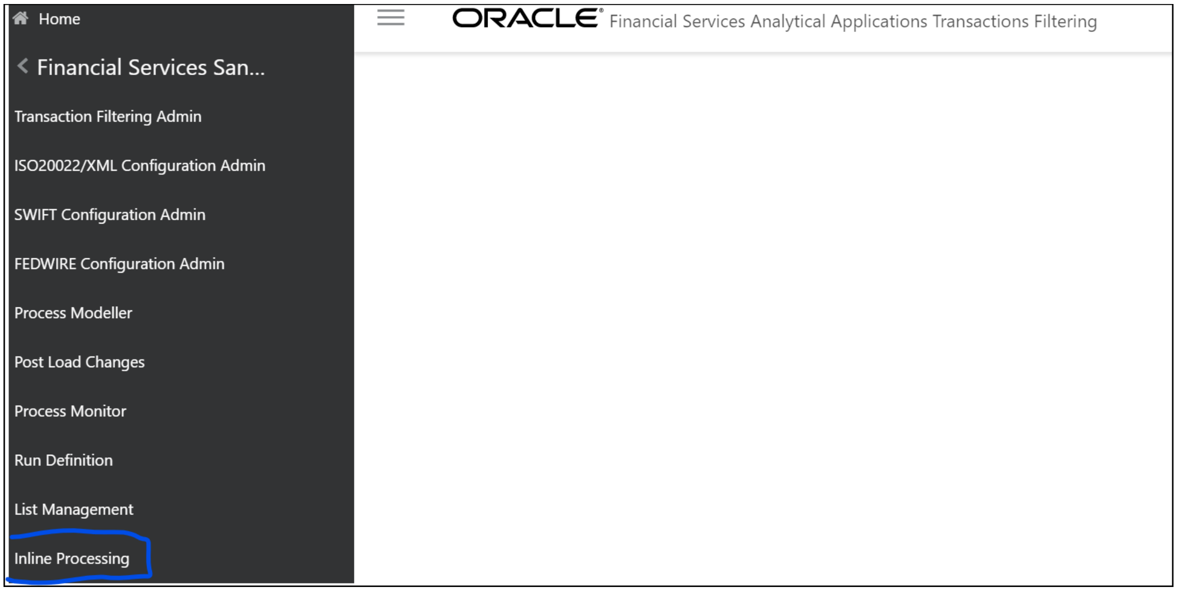
1. Click **Financial Services Sanctions Pack.**

Figure 19: Financial Services Sanctions Pack Menu


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

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

Figure 20: 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):

- 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

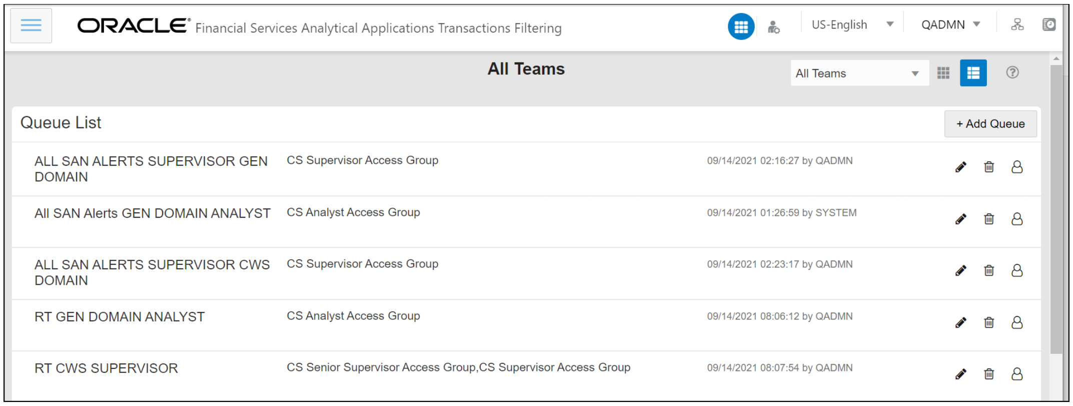
1. Log in to the application as Analyst, Supervisor, or Senior Supervisor.
2. Select the Financial Services Analytical Applications Transaction Filtering.
3. From the Application Navigation List, select Queue Management.

You can select the **hamburger** ☰ 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 21: 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 + 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.

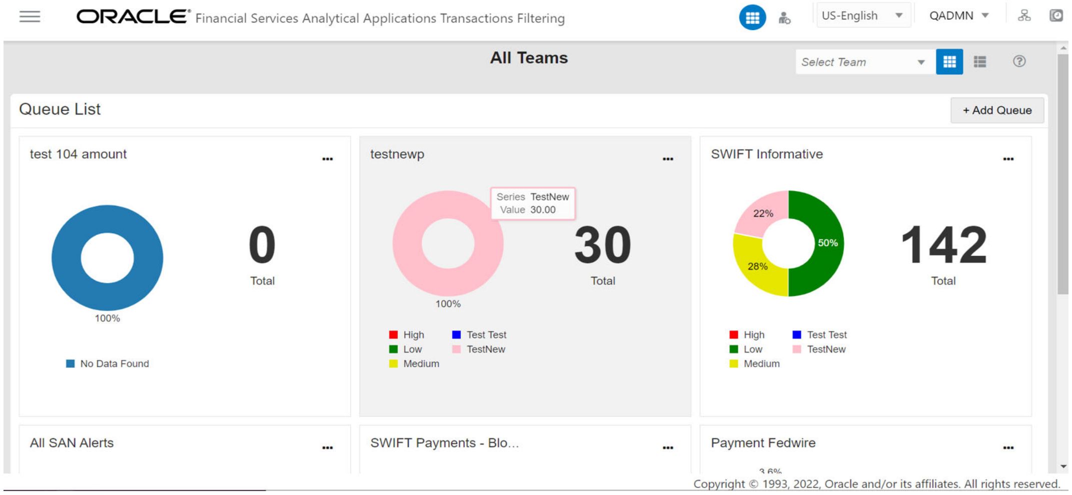
NOTE If the User Group is selected as the **All Teams** in the **Select Teams** menu, then the Queue Admin cannot sort the priority of the Queues.

3.3.2 Grid View

You can select the **thumbview** ▦ 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 22: Queue List in Grid View



NOTE Only 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:

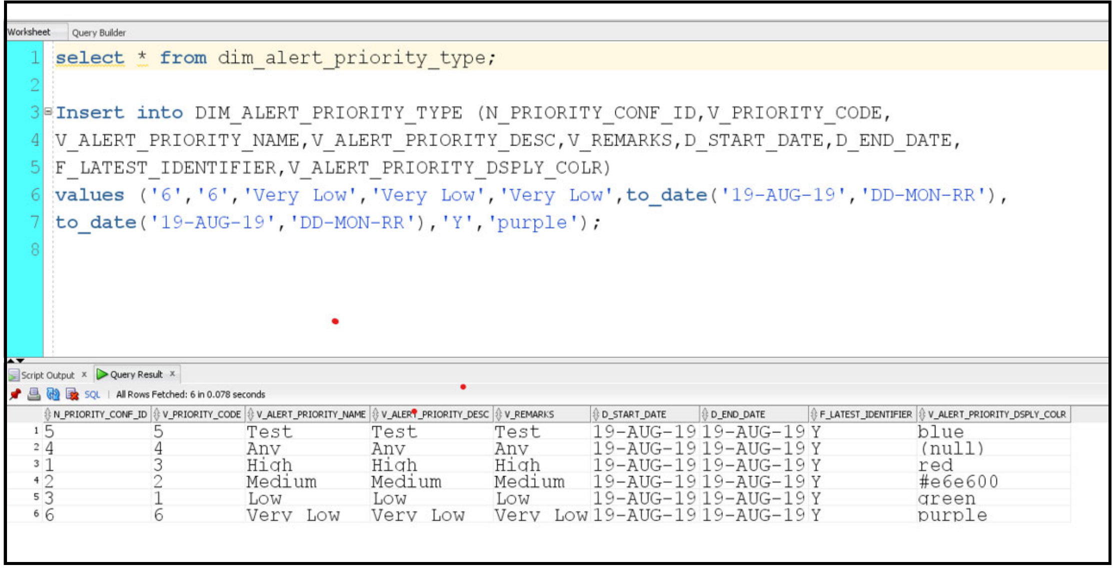
- **+Add Queue**: Click + Add Queue button top-right in the Queue List to add a new queue. (only for Queue Admin.)
- **Delete:** Click the Ellipsis menu and then select Delete and click **Yes** to delete the queue.
- **Edit:** Click the Ellipsis menu and then select Edit to edit the queue details and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

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 23: `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');
```

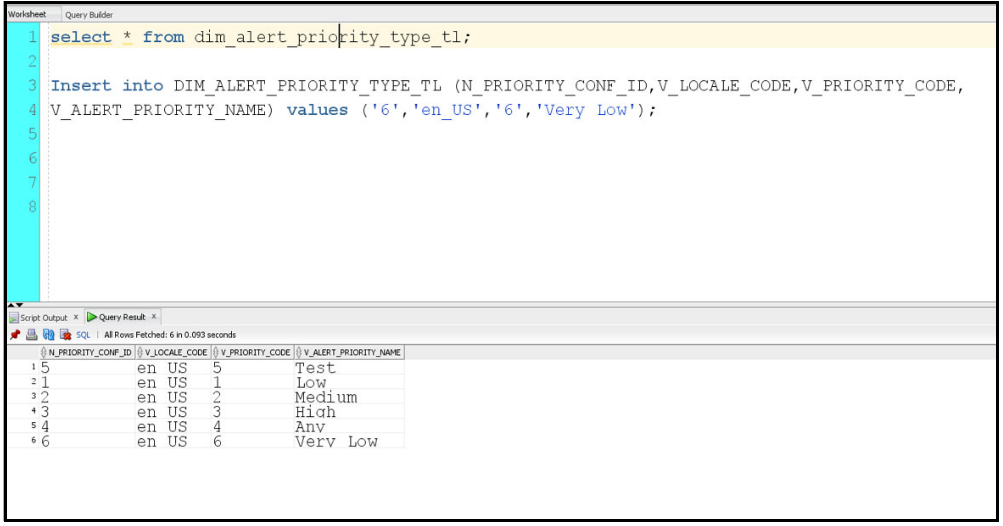
All Rows Fetched: 6 in 0.078 seconds

	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 24: `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

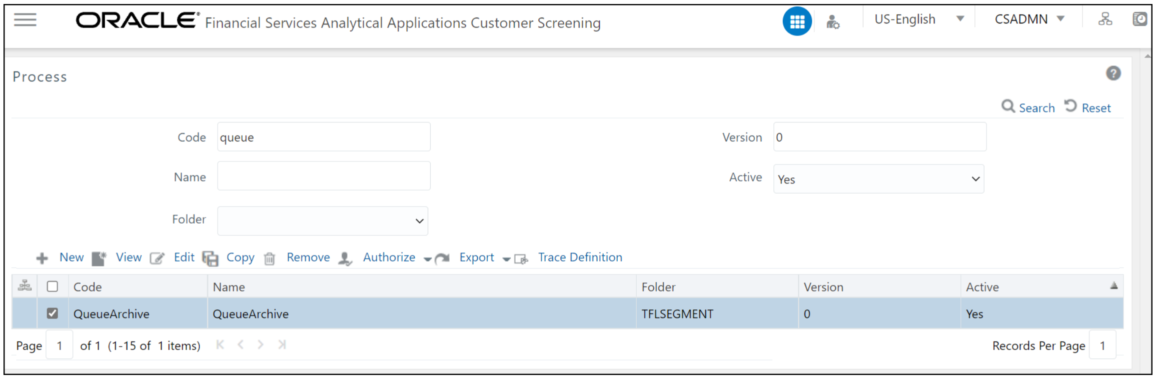
	N_PRIORITY_CONF_ID	V_LOCALE_CODE	V_PRIORITY_CODE	V_ALERT_PRIORITY_NAME
1	5	en_US	5	Test
2	1	en_US	1	Low
3	2	en_US	2	Medium
4	3	en_US	3	High
5	4	en_US	4	Any
6	6	en_US	6	Very Low

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 `QueueArchive`.

Figure 25: Process Page



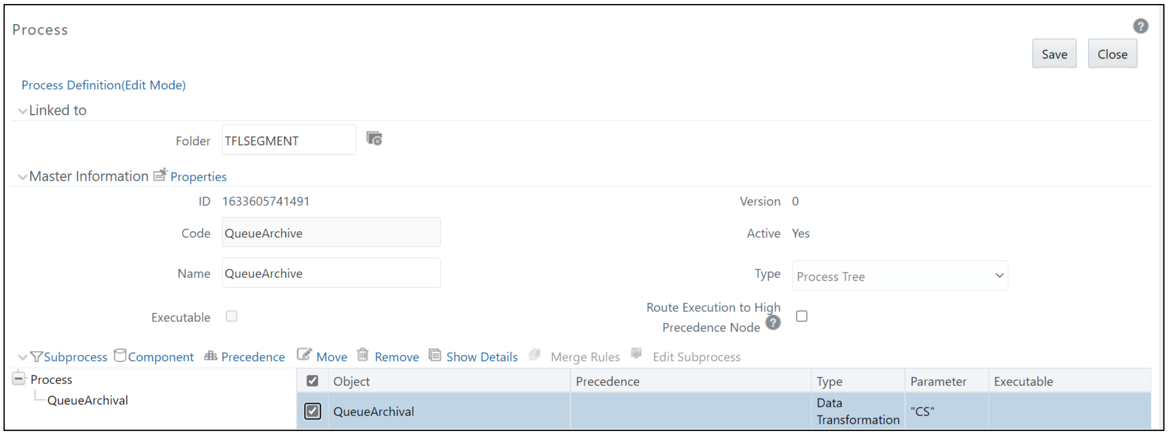
Code: queue
Version: 0
Name:
Active: Yes
Folder:

☐	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 26: Process Definition (Edit Mode)

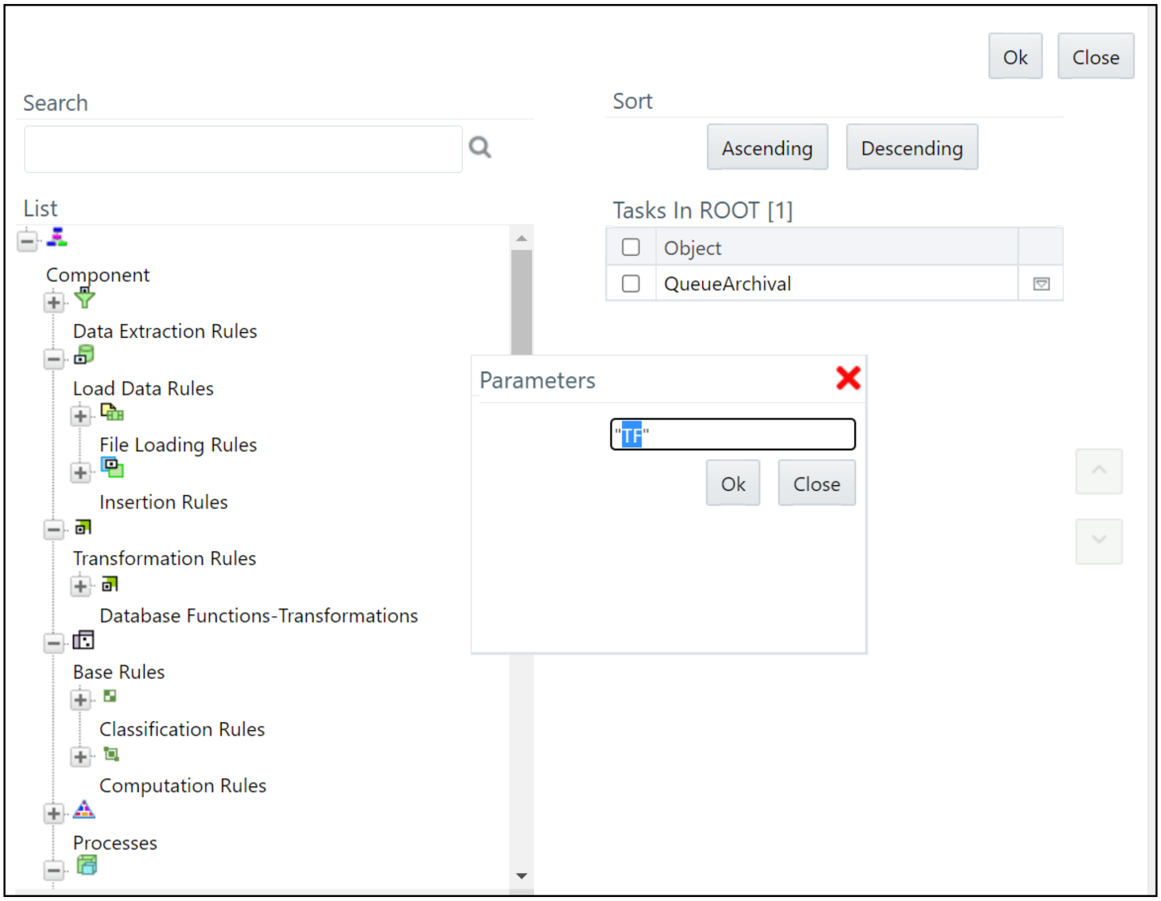


Folder: TFLSEGMENT
ID: 1633605741491
Version: 0
Code: QueueArchive
Active: Yes
Name: QueueArchive
Type: Process Tree
Executable: ☐
Route Execution to High Precedence Node: ☐

☑	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 27: Component Selector Window



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

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

3.4 Troubleshooting Your Display

If you experience problems logging into Oracle Financial Services 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 Settings are enabled.
4. Click **Settings** to open the **Pop-up Blocker Settings** dialog box.
5. In the **Pop-up Blocker Settings** dialog box, enter the URL of the application in the text area.
6. Click **Add**. The URL appears in the **Allowed Sites** list.
7. Click **Close**, then click **Apply** to save the settings.
8. Click **OK** to exit the **Internet Options** dialog box.

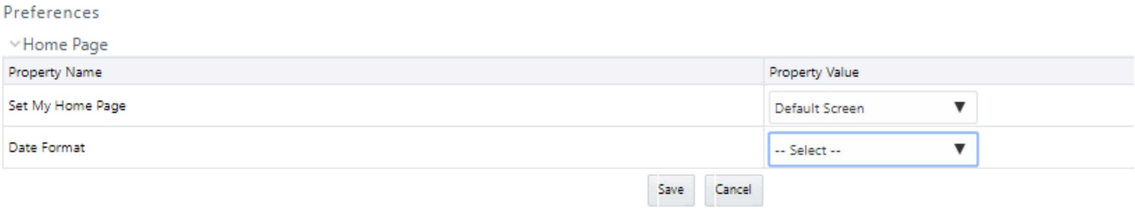
3.4.7 Setting Preferences

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 28: Preferences Page



Preferences

Home Page

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

1. 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.

2. 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.
3. Click **Save** to save your preferences.

4 Managing User Administration

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

4.1 About User Administration

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

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

4.2 Managing User Administration

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

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

Table 3: User Administration

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

4.2.1 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. The following table describes the predefined User Roles and corresponding User Groups.

Table 4: User Group-Role Mapping

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

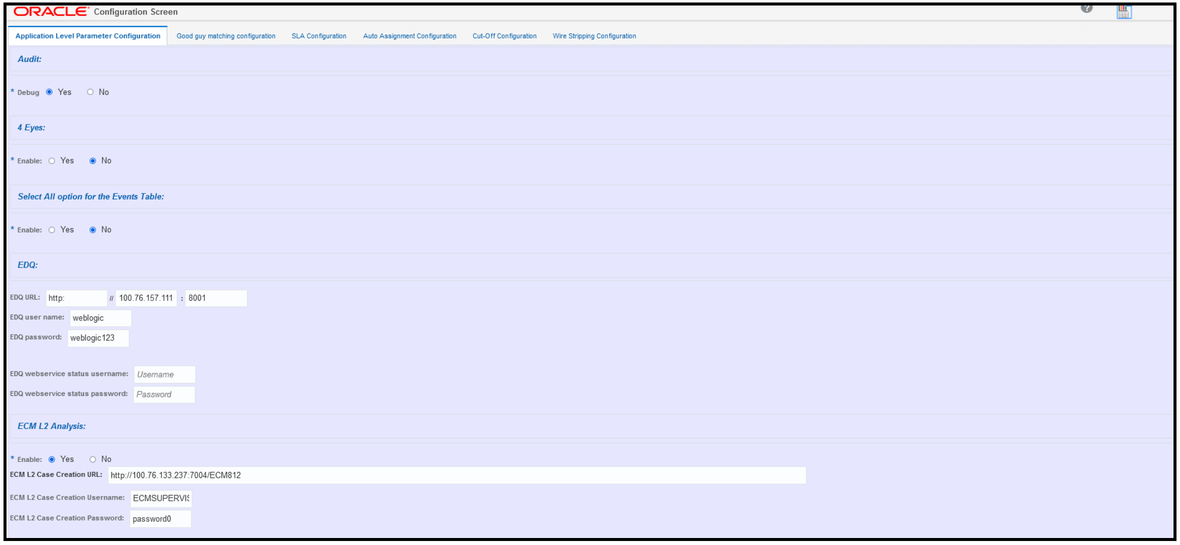
5.1 Configuring the Application Level Parameters

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, 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 29: 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

EDQ:

EDQ URL: http: // 100.76.157.111 : 8001
EDQ user name: weblogic
EDQ password: weblogic123

EDQ webservice status username: Username
EDQ webservice status password: Password

ECM L2 Analysis:

* Enable: ● Yes ○ No
ECM L2 Case Creation URL: http://100.76.133.237:7004/ECM812
ECM L2 Case Creation Username: ECMSUPERVIS
ECM L2 Case Creation Password: password0

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

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

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

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

> **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 **EDQ** section, provide the following values:
   - **EDQ URL** in the following format:

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

   - **EDQ user name**: The default username is displayed. You can update the username if required.
   - **EDQ password**: The default password is displayed. You can update the password if required.
   - **EDQ webservice status username**
   - **EDQ webservice status password**
7. 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 Number>/<Context>`
   - **ECM Case Creation user name**: Enter the ECM username.
   - **ECM Case Creation password**: Enter the ECM password.
8. 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.
9. 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.

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

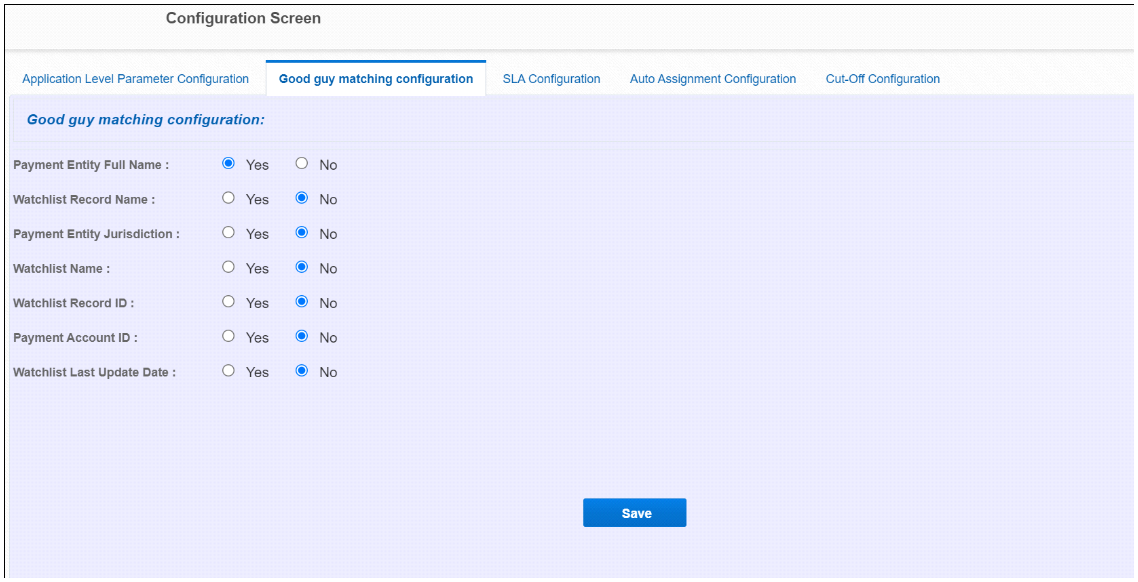
5.2 Configuring the Good Guy Matching Parameters

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 30: 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.

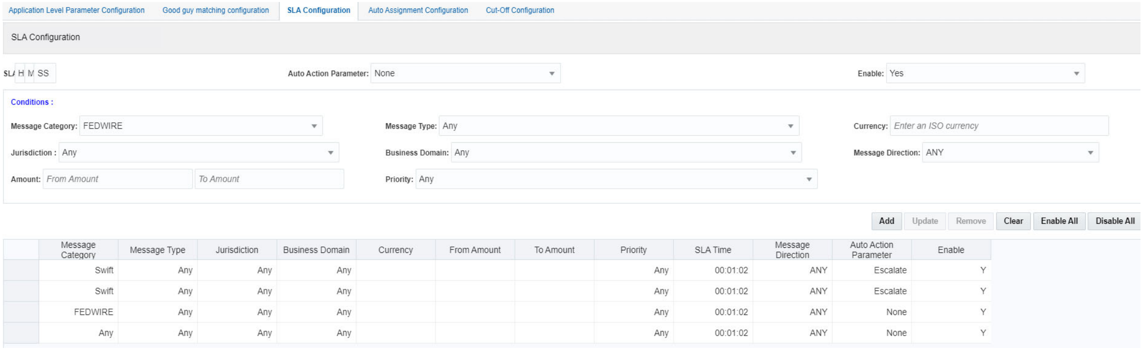
You can set an automatic action to be taken by the system if the alert is not investigated within the defined SLA using the **Auto Action Parameter** field (this is an optional step). For example, if you select **Escalate**, then the alert is escalated to the Supervisor after the SLA time is passed. 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 31: 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

SL/ 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.

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

Table 5: General Actions

To...	Do this...
Add a configuration	Click **Add**. The values appear in a tabular format.
Update a configuration	Select the configuration you want to update, update the value of one or more fields, and click **Update**. The updated value is displayed in the table.
Remove a configuration	Select the configuration you want to remove and click **Remove**. The selected configuration is removed from the table.
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/business domain are displayed. You can manually assign an alert if, for example, the Analyst to whom the alert is assigned is on leave. In this case, the Supervisor moves the status of the alert from **ASSIGNED** to **HOLD** in the Investigation User Interface. The Analyst can self-assign the alert using the lock/unlock feature. For more information on the Investigation User Interface, see the **Managing Transaction Filtering** chapter in the Oracle Financial Services Transaction Filtering User Guide.
- **Automatic assignment**: Alerts are automatically assigned to the selected user role and respective user IDs. When you auto-assign an alert, the alert is automatically assigned to all users who belong to the selected role. You can use two options: load balancing or load balancing along with specific criteria, to assign the alert.

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

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

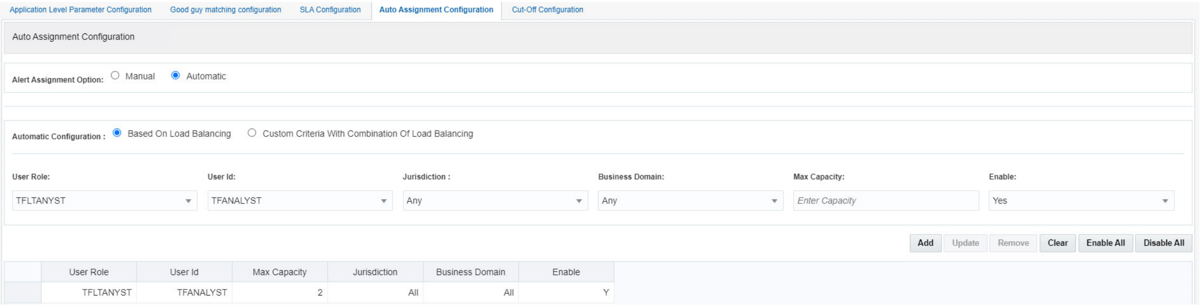
To configure an alert to be assigned manually or automatically, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering** 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 32: 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

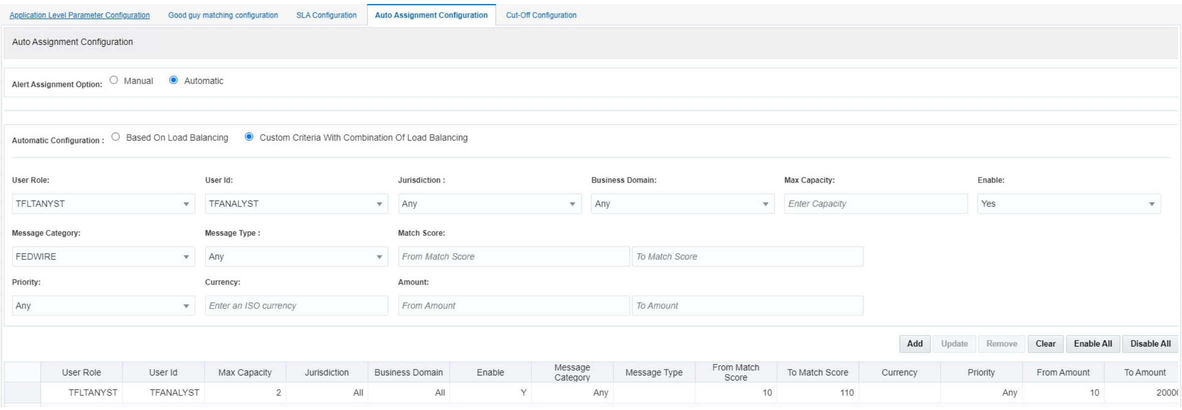
Automatic Configuration : ● Based On Load Balancing ○ Custom Criteria With Combination Of Load Balancing

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


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

Message Category:	Message Type :	Match Score:	
FEDWIRE	Any	From Match Score	To Match Score

Priority:	Currency:	Amount:	
Any	Enter an ISO currency	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 Criteria With Combination Of Load Balancing**:

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

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

Table 6: General Actions

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

5.5 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.

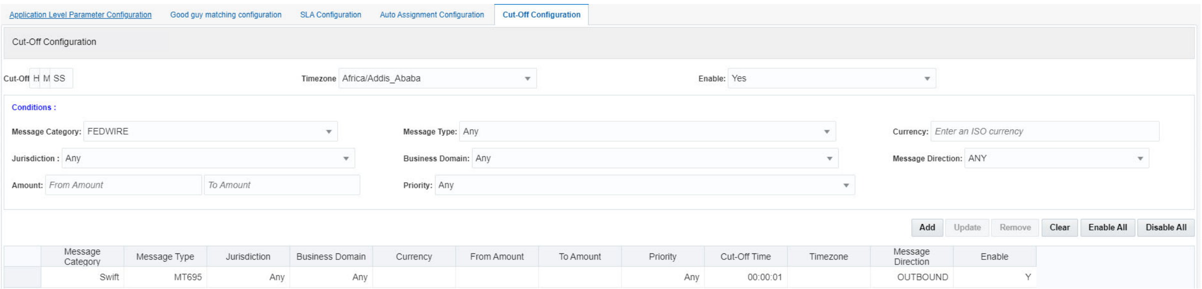
When the cut-off time is set for an alert, the alert displays the time in *green* in the Investigation User Interface until the cut-off time is passed. After the cut-off time is passed, that is, the alert becomes overdue and is not investigated within the defined cut-off time, then the alert displays 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 34: Cut-Off 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

Cut-Off Configuration

Cut-Off: H M SS
Timezone: Africa/Addis_Ababa
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	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 7: 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.

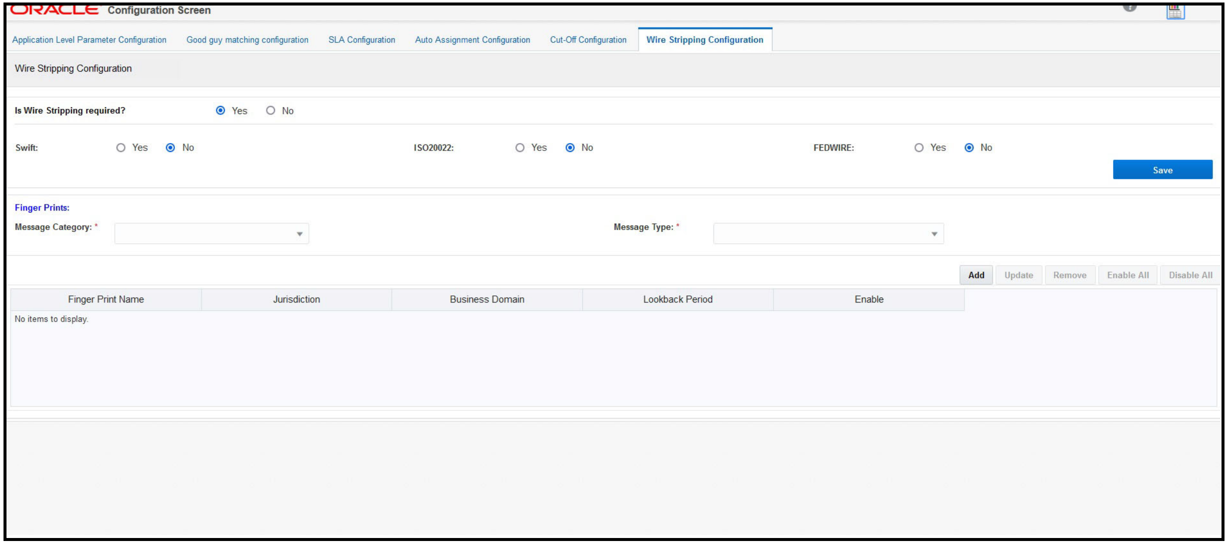
When a message is blocked or rejected by the sanctions team, the transaction is stored in the database of blocked transactions (the property of the transaction is configurable) with a unique identifier code or Fingerprint assigned. Using the Fingerprint, identical wire transfers are identified with variable 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 35: 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 fingerprint.

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 message type that you selected.

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

   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.

b. 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 combination.

c. 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**.

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

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

f. 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:

1. To configure the business data attribute for SWIFT or Fedwire message category, follow the below steps:

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

b. Insert the parameters in the columns. For more information See Data Model Reference Guide.

c. To enable a particular business data attribute in the Fingerprint, add **Y** for the selected business data in the `F_ENABLE_FOR_FINGER_PRINT` column.

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

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

b. Insert the parameters in the columns. For more information See Data Model Reference Guide.

c. To enable the business data attribute in the Fingerprint, add **Y** for the business data in the `F_ENABLE_FOR_FINGER_PRINT` column.

2. After configuring and executing the above step, you must add required conditions for the business 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` column from `DIM_MESSAGE_CATEGORY` table.

— `N_CONDITION_ID`: For the conditions required for the new business data, refer `N_CONDITION_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 lon 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

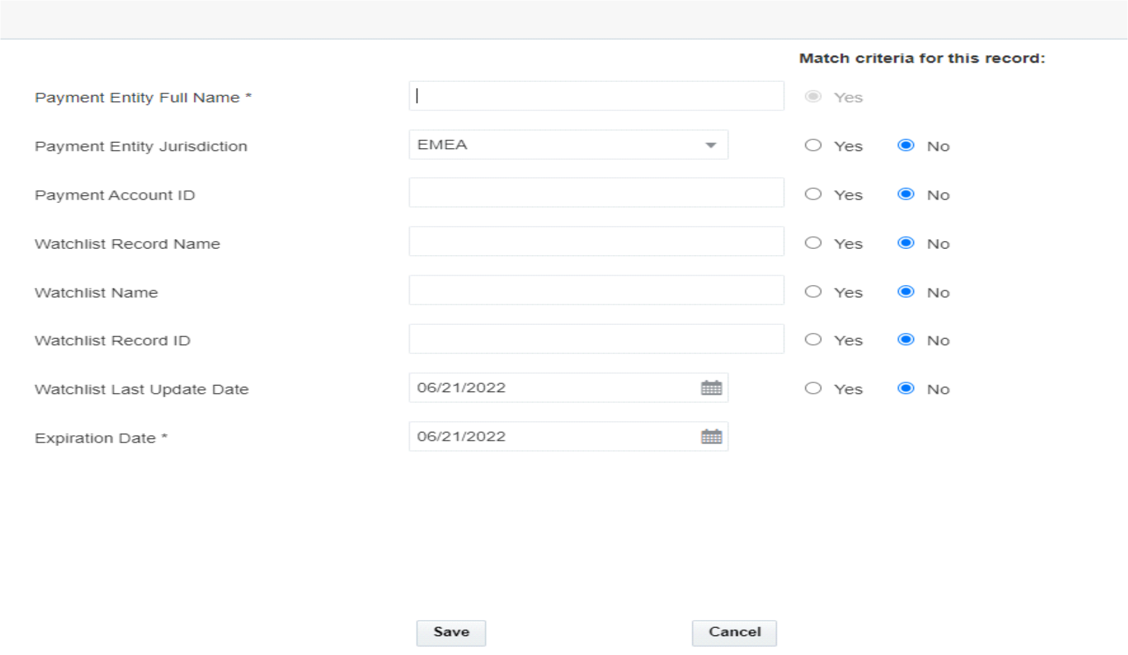
Apart from adding a good guy record using the process mentioned in the **Good Guy/White List Matching** section in the Oracle Financial Services Transaction Filtering User Guide, you can also manually add a record to the `FCC_WHITELIST` table, for example, if the record is a trusted customer.

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 36: 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**.

5.9.2.1 Updating the Status of an Expired Alert

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

5.9.3 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 hashcode 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 hashcode 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.

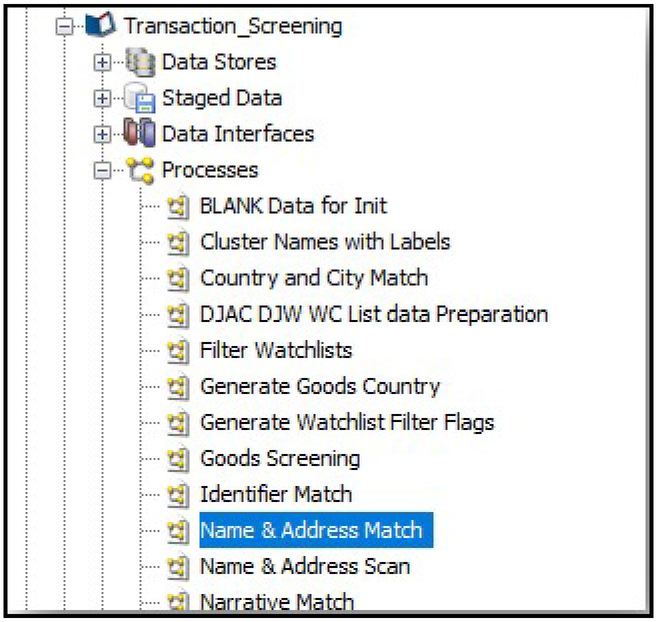
This functionality is expected to work for all types of lists - 3rd party lists and internal lists. This means an analyst should be able to mark a good guy based on an internal list match.

5.9.5 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.

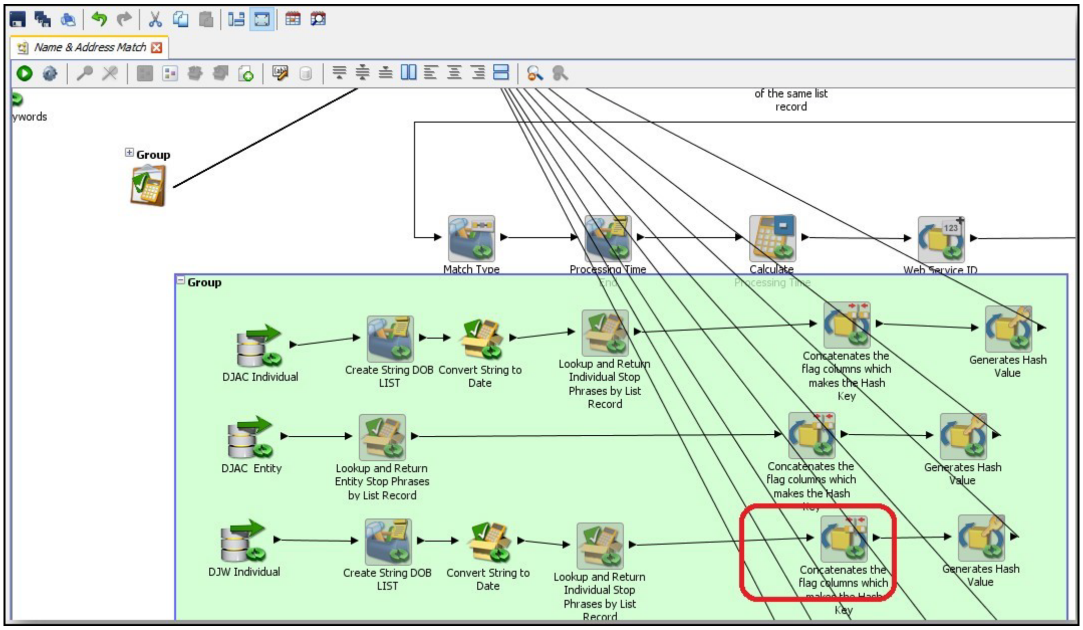
Figure 37: Transaction Screening Project



- 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**.

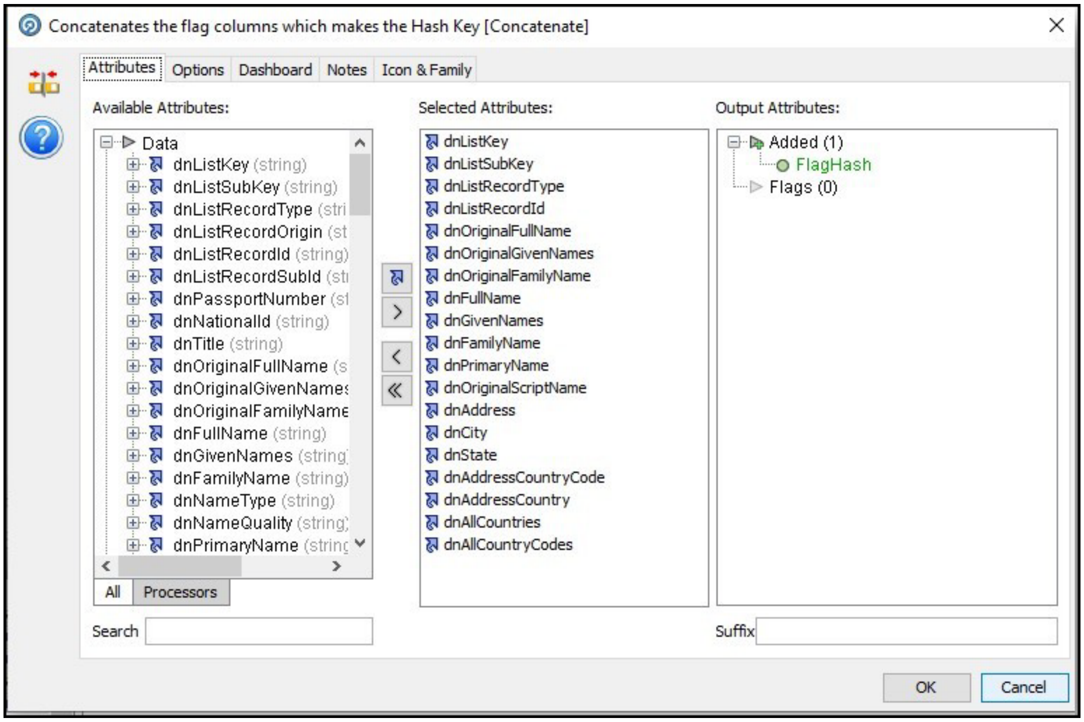
Figure 38: Name and Address Match


Name & Address Match
ywords
of the same list
record
Group
Match Type
Processing Time
Calculate
Processing Time
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 39: Attributes for Concatenates the flag columns which makes the Hash Key



Concatenates the flag columns which makes the Hash Key [Concatenate]

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

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

3. Map user groups to the appropriate jurisdiction and business domain. To do this, run the query `SELECT * FROM DOMAIN_JUR_GRP_MAP` and do the mapping in the `DOMAIN_JUR_GRP_MAP` table 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 available in the fsi_rt_al_msg_tag table. If the customer wants to use any field as a jurisdiction or business domain from this table, then an SQL query must be written in the Setup_Rt_Param table to extract the respective column.

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

5.11.2 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 popup which appears, select the versions that you want to compare.
4. Click **Configuration**.
5. In the popup which appears, select the differences only and click **OK**.
6. In the same window, select **Start Comparison**. This gives all changes between the two files.

For more information, see Oracle Enterprise Data Quality Documentation.

5.13 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_Utility/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 10: 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: 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_Utility/config` directory.
2. Open the `Dynamic.properties` file and update the placeholders as shown:

Table 12: 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.
##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 command.

```
./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 13: 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 command.

```
./ import.sh SEPA.
```

5.15 Configuring JMS Correlation ID

JMS message has two properties (column) called Correlation ID and Message Identifier.

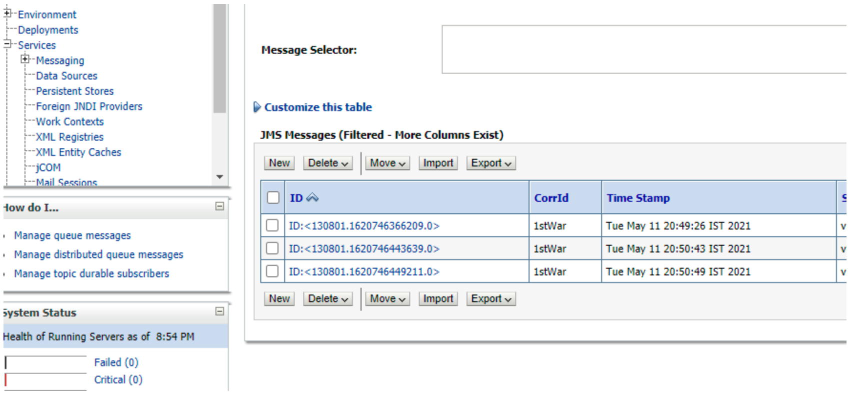
To set the Correlation ID, use the following sample code:

`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 40: JMS Message Output Queue



Message Selector:

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 Webservices 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:

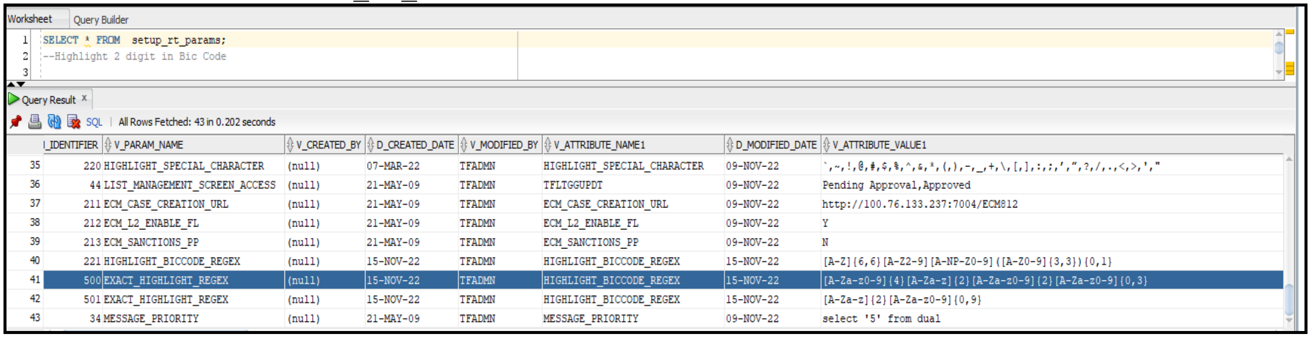
1. Access the Atomic Schema and access the `SETUP_RT_PARAMS` table.
2. Insert the attribute value for the required parameters in the table.

For example, to consider the matched data for BIC, follow the below steps:

1. Access the Atomic Schema and access the `SETUP_RT_PARAMS` table.
2. 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 41: `SETUP_RT_PARAMS` **Table**



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

All Rows Fetched: 43 in 0.202 seconds

	_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 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 is:

- `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.

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 displayed.

> **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

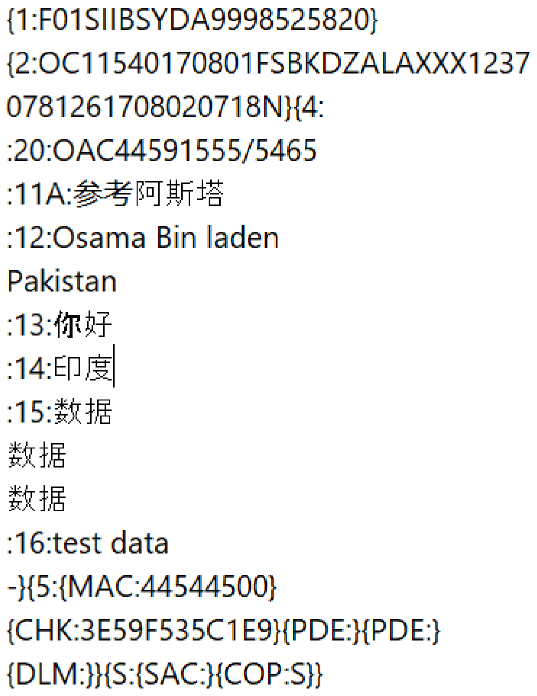
This window allows you to edit the status, field names, and expressions of the different JSON parameters in the message.

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 42: 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}}
```

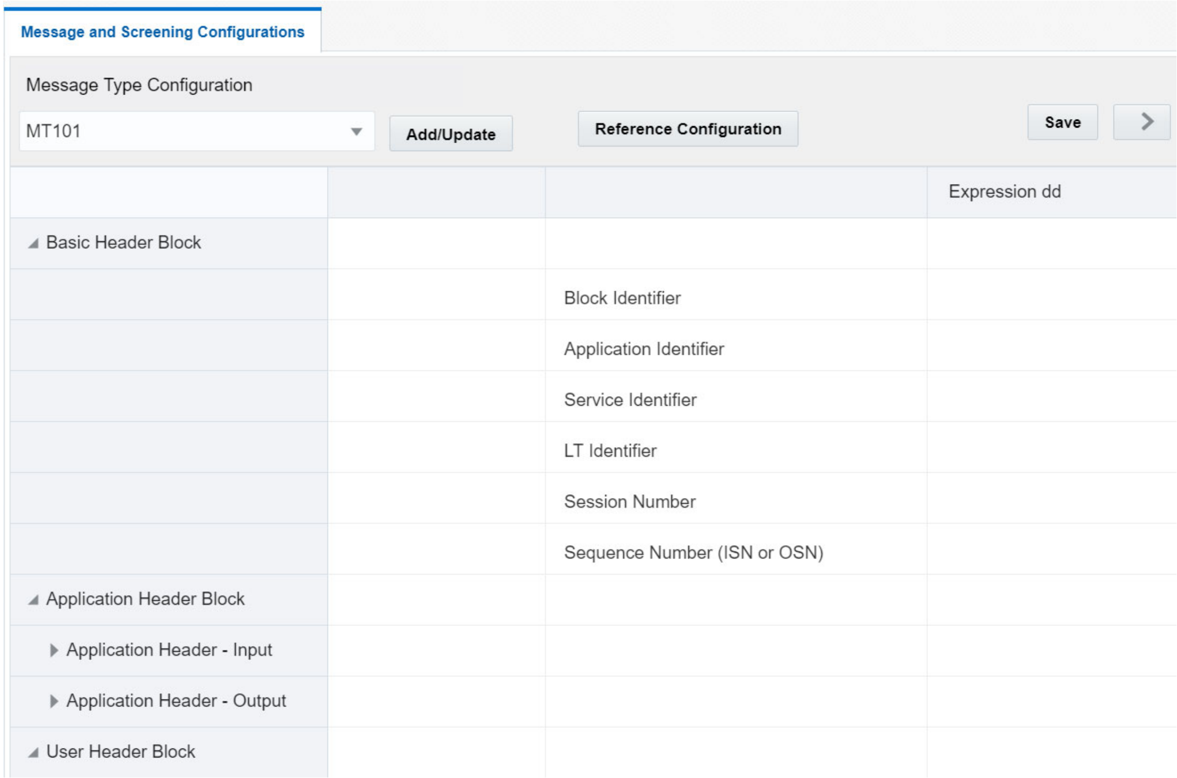
In this example, C11 can be either 11 or 11A and not 111. So, the tag can either start with two numbers or two numbers and one alphabet. The value in the 11A tag represents 100k in the JSON expression, and the value in the 15 tag represents `100*100k` in the JSON expression.

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 43: Message and Screening Configurations Window for SWIFT



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**.

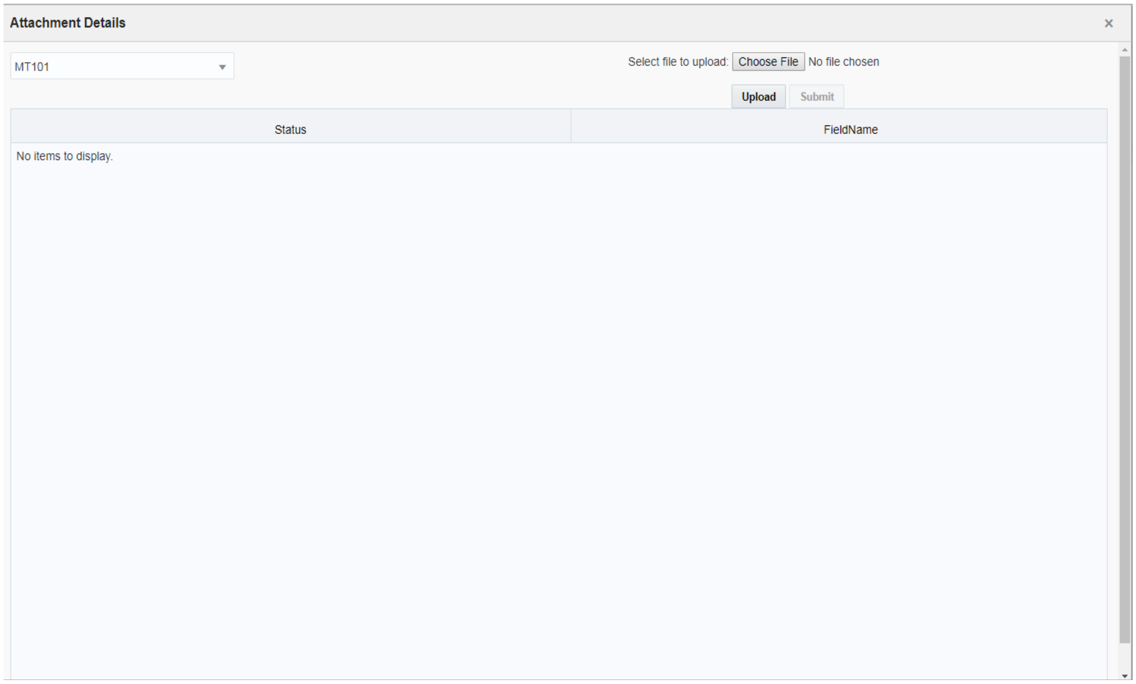
6.1.1 Adding or Updating a New Message Type

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 44: Attachment Details Window



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

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

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

For more information 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

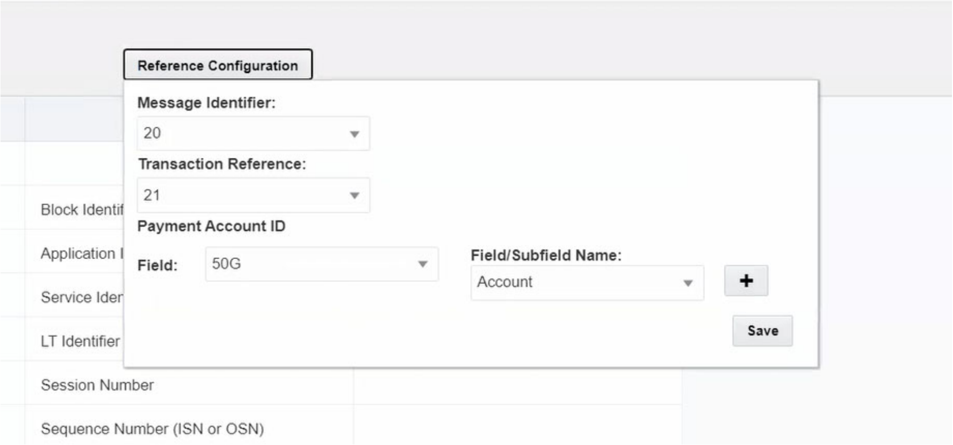
Any message which contains message references or transaction references, or both, must be configured.

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 45: Reference Configuration Window



Message Identifier: 20

Transaction Reference: 21

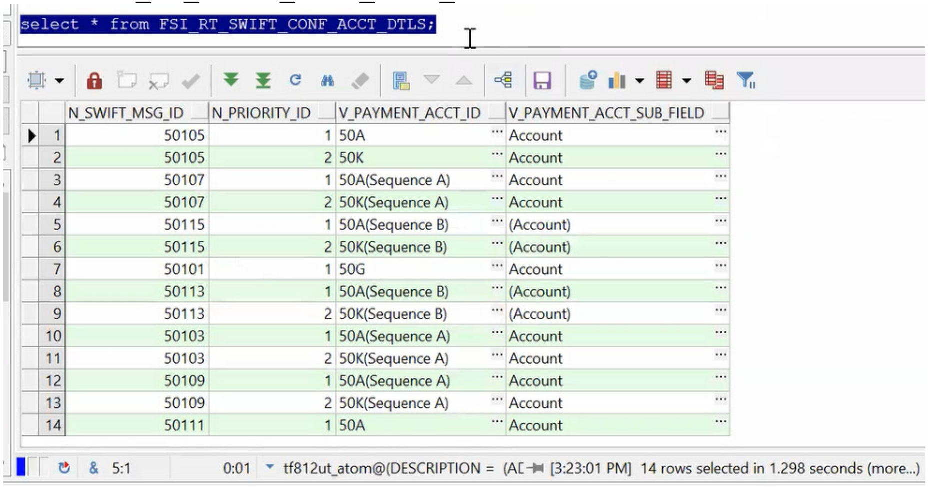
Payment Account ID

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 46: `FSI_RT_SWIFT_CONF_ACCT_DTLS` Table



```
select * from FSI_RT_SWIFT_CONF_ACCT_DTLS;
```

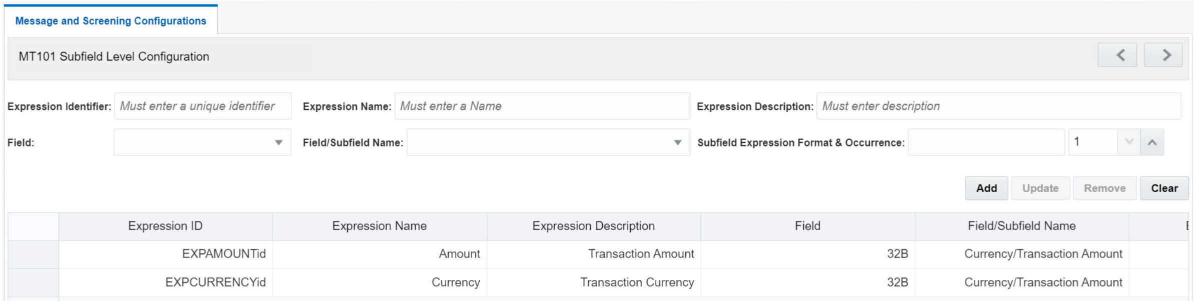
	N_SWIFT_MSG_ID	N_PRIORITY_ID	V_PAYMENT_ACCT_ID	V_PAYMENT_ACCT_SUB_FIELD
1	50105	1	50A	Account
2	50105	2	50K	Account
3	50107	1	50A(Sequence A)	Account
4	50107	2	50K(Sequence A)	Account
5	50115	1	50A(Sequence B)	(Account)
6	50115	2	50K(Sequence B)	(Account)
7	50101	1	50G	Account
8	50113	1	50A(Sequence 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 47: <Message Type> Subfield Level Configuration Window


Message and Screening Configurations
MT101 Subfield Level Configuration
Add
Update
Remove
Clear

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** Add. Enter values in the following fields:

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

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

Table 14: 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** Add.
Update button	To update an existing subfield, click the name of the subfield. After you make the changes, click **Update** Update **.**
Remove button	To remove an existing subfield, click the name of the subfield and click **Remove** Remove **.**
Clear button	To clear the data in these fields, click **Clear** Clear.

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

You can configure the subfield in two ways:

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

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

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

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

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

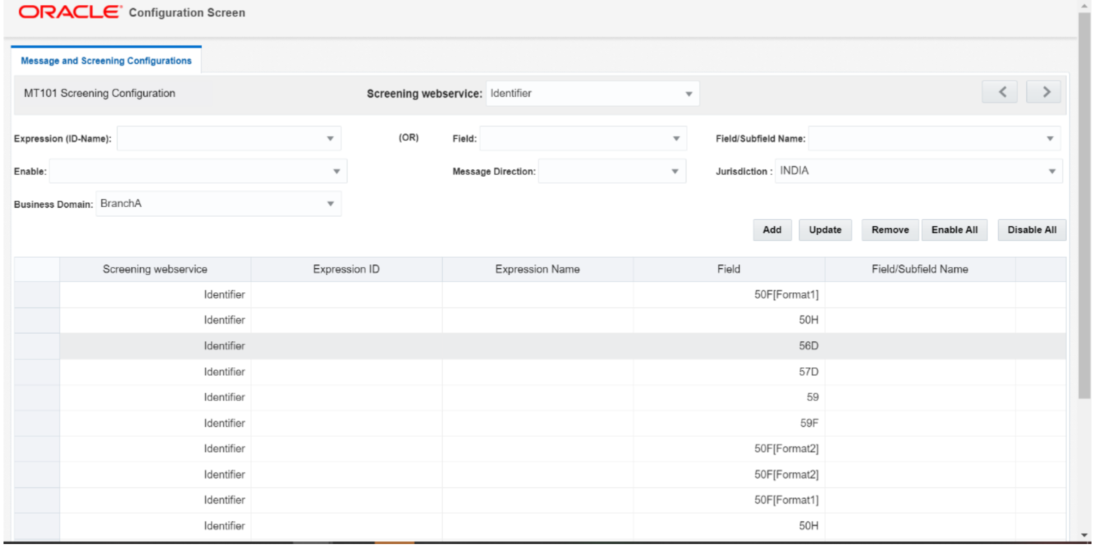
  In this example, if you want to configure the country code for `field 57,` then you can configure `2!a` from Identifier Code expression as a country code by giving unique names in the **Subfield Expression Identifier**, **Subfield Name**, and **Subfield Description** fields.

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

6.3 <Message Type> Screening Configuration Window

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

Figure 48: <Message Type> Screening Configuration Window


ORACLE Configuration Screen
Message and Screening Configurations
Add
Update
Remove
Enable All
Disable All

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

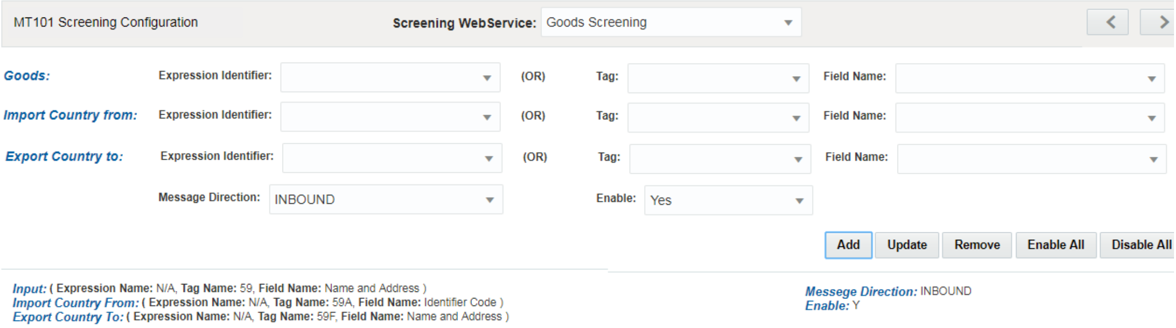
Fields	Field Description
Screening WebService	Select a screening web service from the drop-down list. This field lists all the supported matching web services in the **Transaction Filtering** application. The following web services are available: - Identifier - Country and City - Goods Screening - Name 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.
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 15: 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** Add.
Update button	To update a web service, select the web service that you want to update and click **Update** Update.
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** Remove.
Enable All button	To enable all web services, click **Enable All** Enable All.
Disable All button	To disable all web services, click **Disable All** Disable All.

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

Figure 49: 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 16: Fields in the Goods Web Service Window

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

6.3.1 Enabling or Disabling a Web Service

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

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

Table 17: Web Services 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

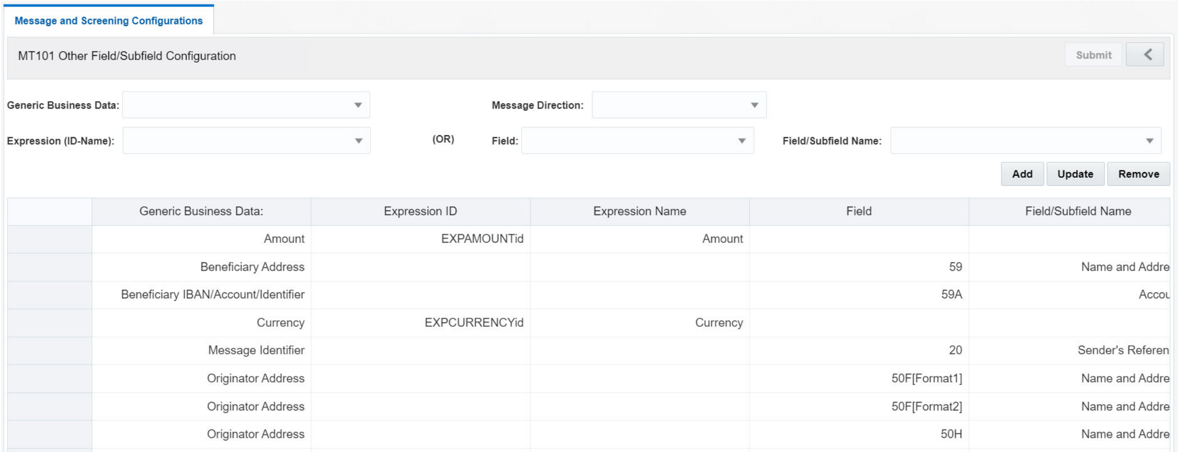
Data for the Trade goods and Trade port web services are taken from a reference table. To populate data for these web services, do this:

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 50: <Message Type> Other Field/Subfield Configuration Window



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

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

Table 18: 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** .

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

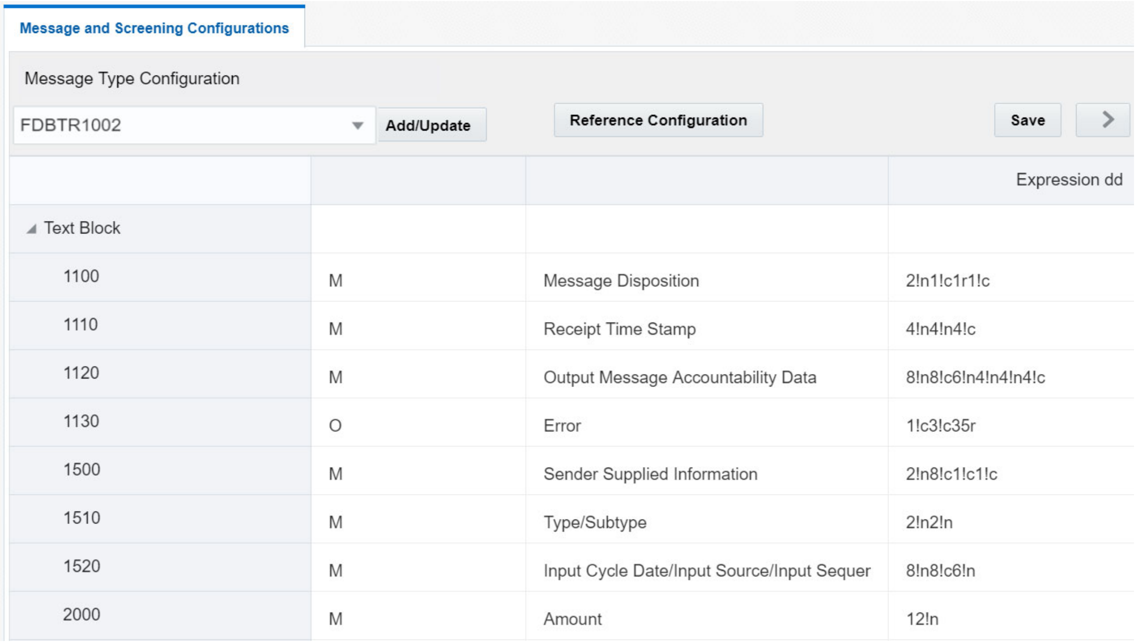
7 Configuring the Fedwire Message Parameters

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 displayed.

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

Figure 51: 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

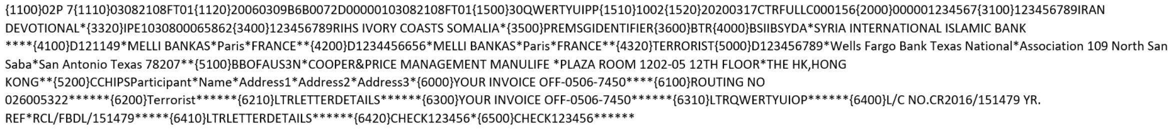
7.1 Message Type Configuration Window

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:

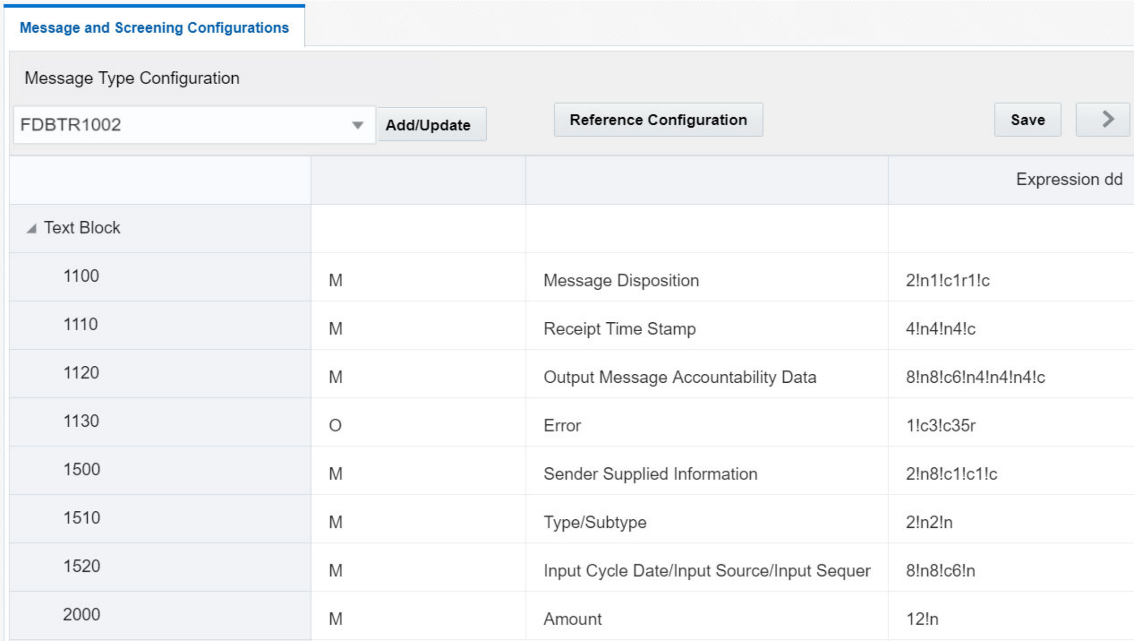
Figure 52: Sample Fedwire Message



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

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

Figure 53: Message and Screening Configurations tab for Fedwire



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

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.

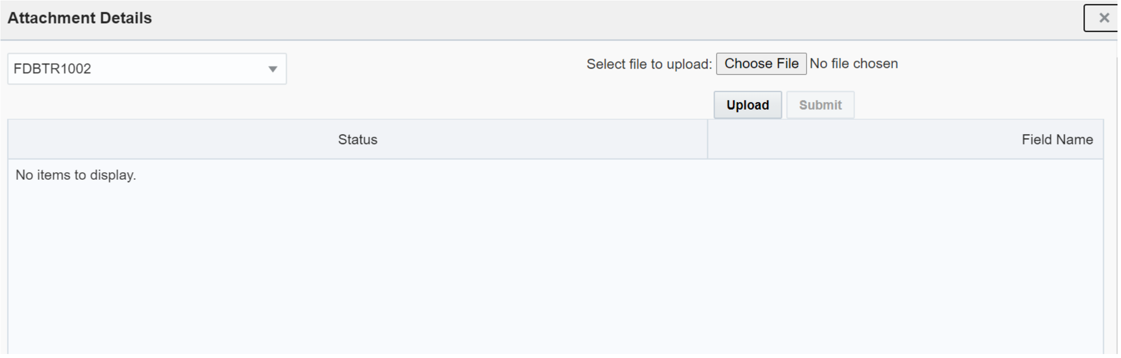
To edit a parameter, click the parameter name. After you make the changes, click **Save**.

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 54: Attachment Details Window



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

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

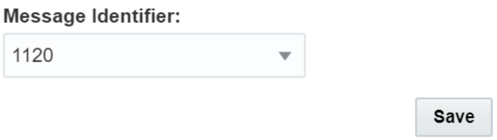
4. Click **Upload**.
5. Click **Submit**. The message is displayed in the following table as <Message Type_draft>.

   For 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 55: Reference Configuration Window

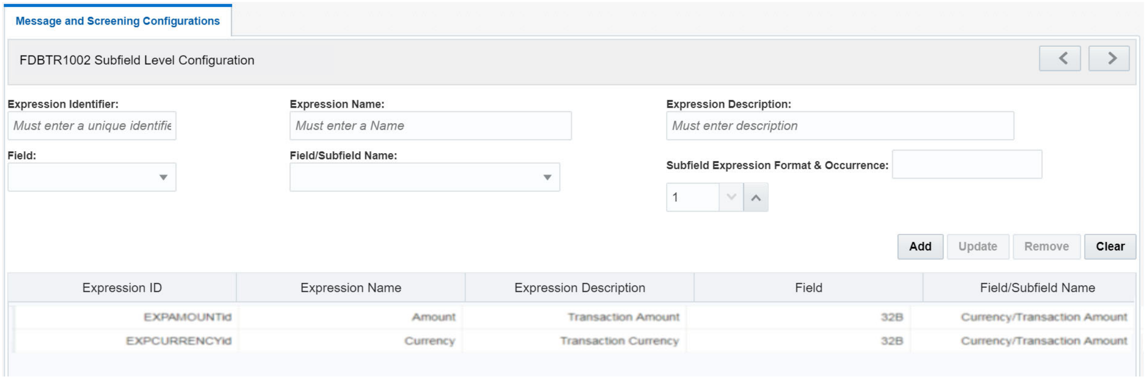


For the **Message Reference** field, a unique identifier must be configured at the message level for all message categories. For the Transaction Reference field, a unique identifier must be configured at the transaction level only if applicable for the specific message category.

7.2 <Message Type> Subfield Level Configuration Window

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

Figure 56: <Message Type> Subfield Level Configuration Window



Message and Screening Configurations
FDBTR1002 Subfield Level Configuration
<
>
Add
Update
Remove
Clear

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** Add. Enter values in the following fields:

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

Fields	Field Description
Expression Identifier	Enter a unique identifier. It must begin with an alpha character and must not contain any spaces. This is a mandatory field.
Expression Name	Enter a name for the expression. The name must be in capital letters. This is a mandatory field.
Expression Description	Enter a description for the Expression. This is a mandatory field.
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.
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** Add.
Update button	To update an existing subfield, click the name of the subfield. After you make the changes, click **Update** Update.
Remove button	To remove an existing subfield, click the name of the subfield and click **Remove** Remove.
Clear button	To clear the data in these fields, click **Clear** Clear.

You can configure the subfield in two ways:

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

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

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

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

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

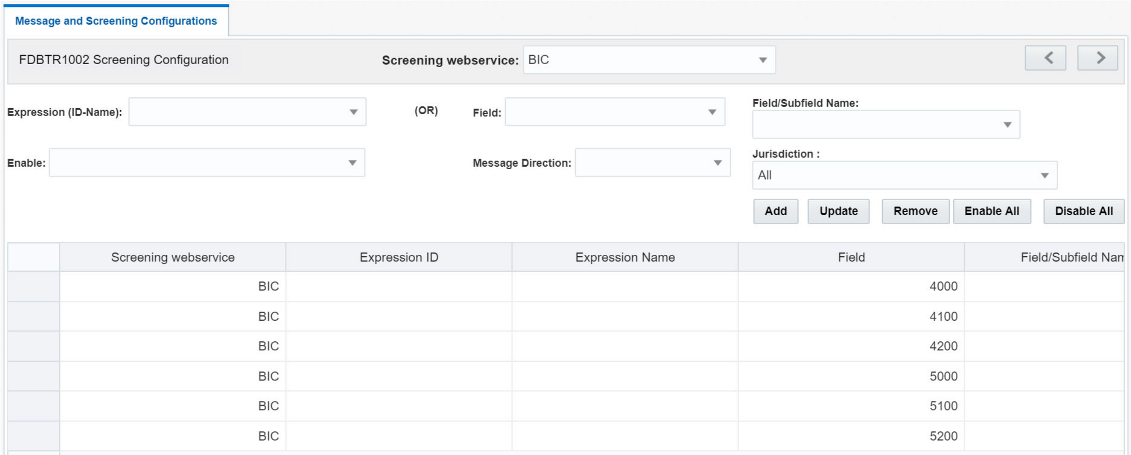
  1.In this example, if you want to configure the country code for `field 57,` then you can configure `2!a` from Identifier Code expression as a country code by giving unique names in the **Subfield Expression Identifier**, **Subfield Name**, and **Subfield Description** fields.

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

7.1 <Message Type> Screening Configuration Window

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

Figure 57: <Message Type> Screening Configuration Window



FDBTR1002 Screening Configuration

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

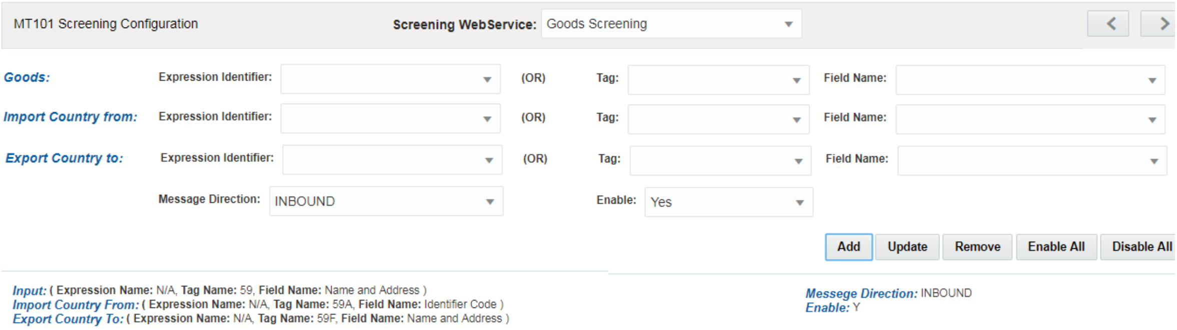
Fields	Field Description
Screening WebService	Select a screening web service from the drop-down list. This field lists all the supported matching web services in the **Transaction Filtering** application. The following web services are available: · BIC · Country and City · Goods Screening · Name and Address · Narrative or Free Text Information · Port Screening The fields for all web services except Goods Screening are as shown here. For information on the fields for Goods Screening, see .
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** Add .
Update button	To update a web service, select the web service that you want to update and click **Update** Update .
Remove button	To remove a web service, select the web service that you want to remove and click **Remove** Remove .

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

Fields	Field Description
Enable All button	To enable all web services, click **Enable All** Enable All.
Disable All button	To disable all web services, click **Disable All** Disable All.

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

Figure 58: 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 21: Fields in the Goods Web Service Window

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

7.1.1 Enabling or Disabling a Web Service

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

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

Table 22: Web Services used in Transaction Filtering

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

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

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

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

7.1.2 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**.

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

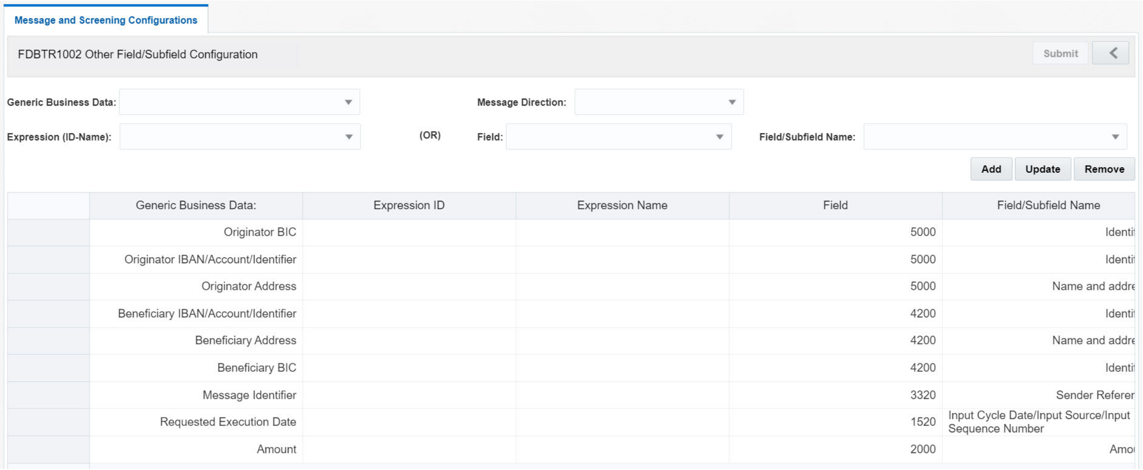
Data for the Trade goods and Trade port web services are taken from a reference table. To populate data for these web services, do this:

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**.

7.2 <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 59: Other Field/Subfield Configuration Window



FDBTR1002 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
	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: Fields in the <Message Type> Other Field/Subfield Configuration Window

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

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

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.

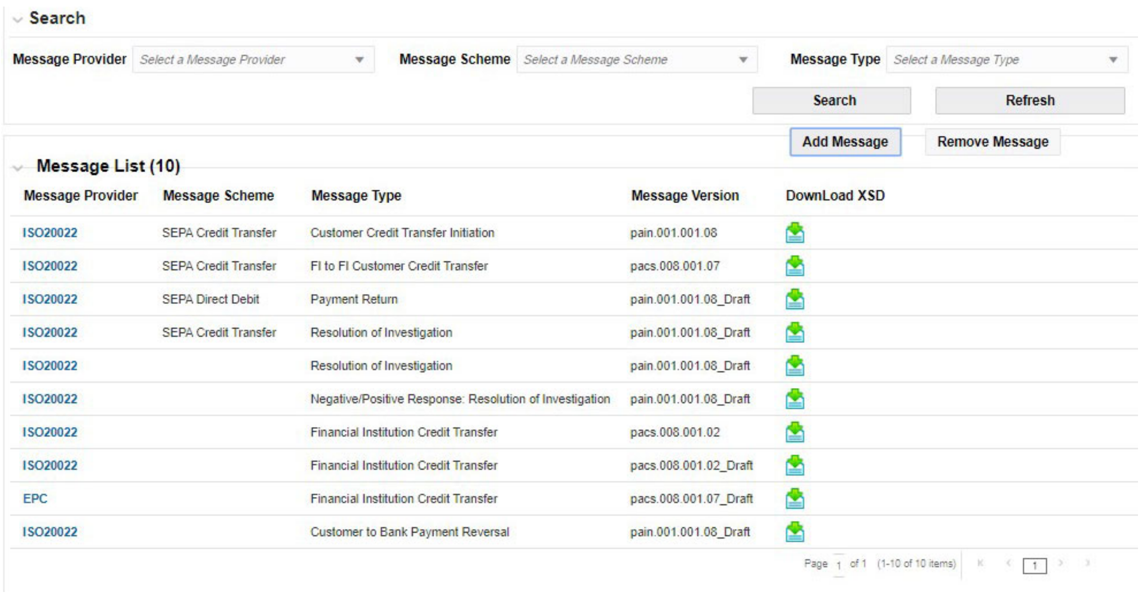
> **NOTE** The XPath of an element is the logical structure or hierarchy of the element within the XSD file.

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 60: Configuration Window - ISO20022



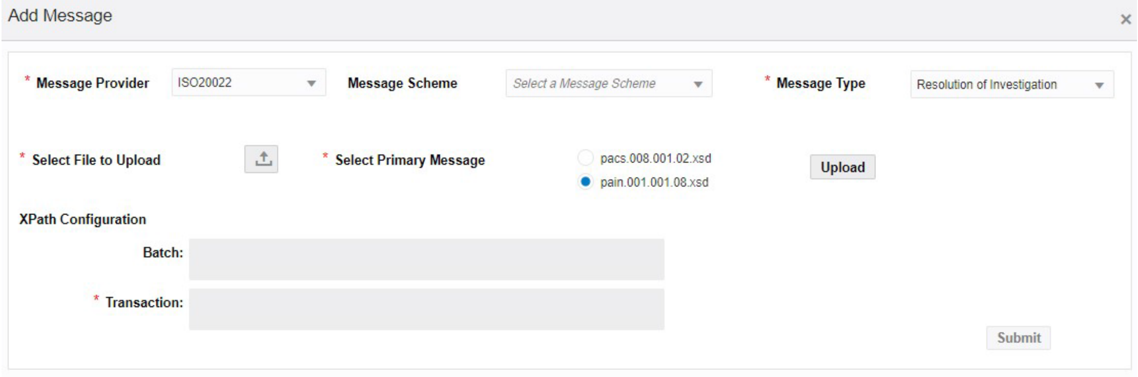
Message List (10)

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	⭳

The Message List displays the XSD files associated with each message provider /scheme/message type combination. Click the link in the **Message Provider** column to view the transaction XPaths for the message for every screening type. You can download the XSD for a message by clicking **Download** ⭳ 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 61: 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

XPath Configuration

Batch:

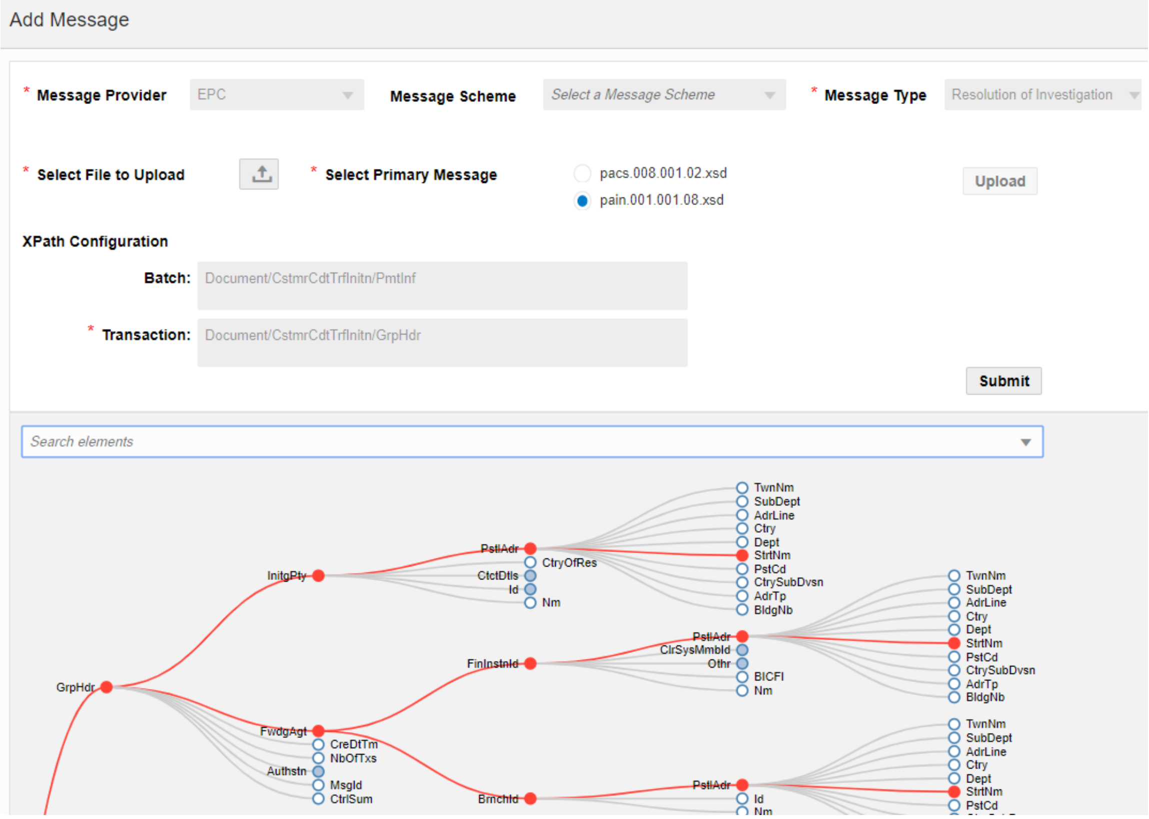
* Transaction:

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

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

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

Figure 62: 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

XPath Configuration

Batch: Document/CstmrCdtTrfInitn/PmtInf

* Transaction: Document/CstmrCdtTrfInitn/GrpHdr

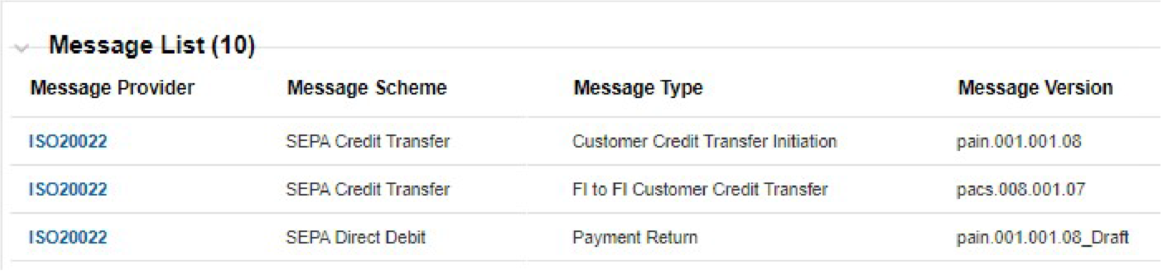
If you want to see the XPath of an element, select the element from the drop-down field. In the example window, the XPath for the StrNm element is highlighted in red.

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

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

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

Figure 63: Message List Window

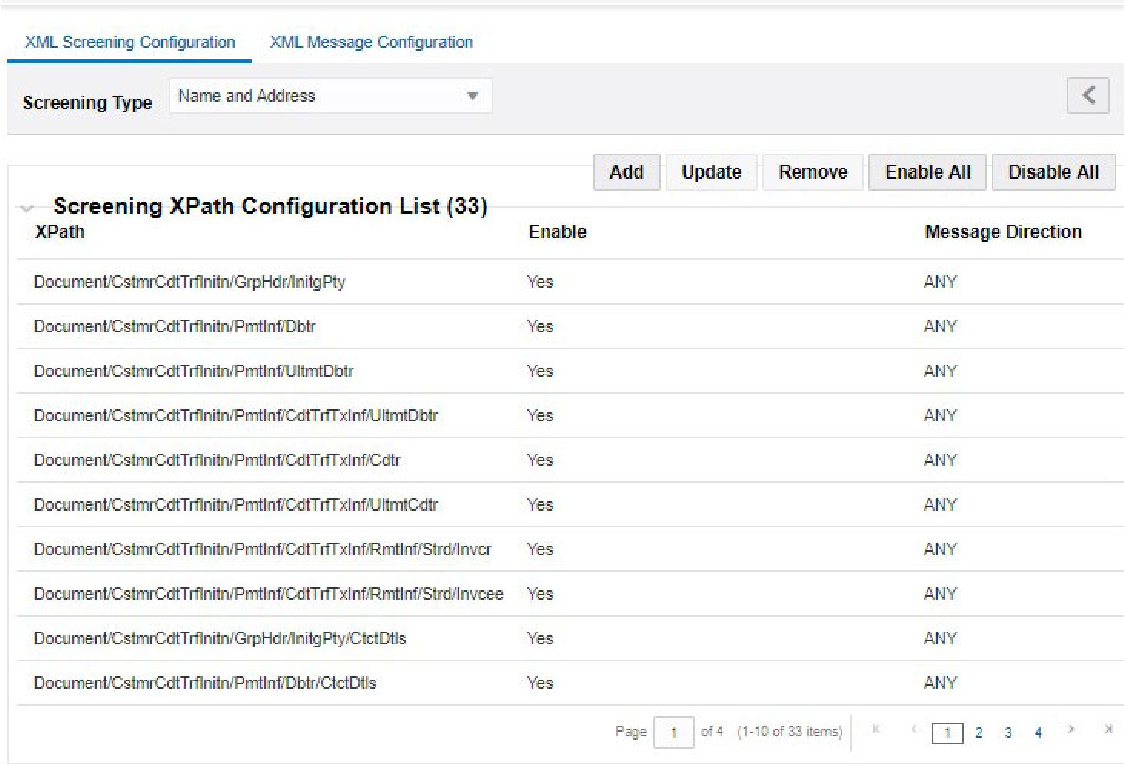


Message List (10)

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

Figure 64: Message List Window


XML Screening Configuration
XML Message Configuration
Add
Update
Remove
Enable All
Disable All
Page 1 of 4 (1-10 of 33 items)
1 2 3 4

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

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

Table 24: Other Actions

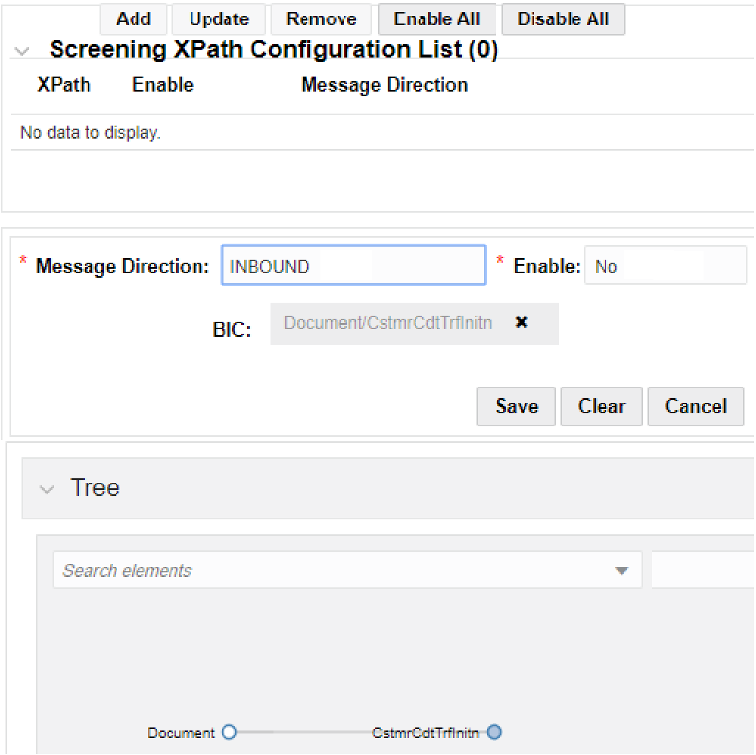
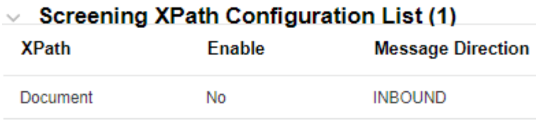
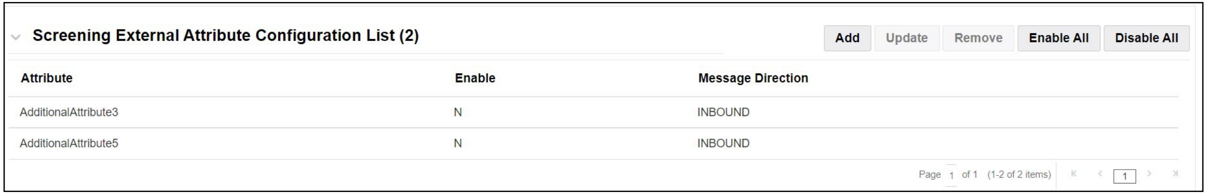
To...	Do this...
Add a web service configuration	Click **Add**. The following fields appear: **Figure 65: Add a web service configuration**  Add Update Remove Enable All Disable All Save Clear Cancel Tree Screening XPath Configuration List (0) XPath Enable Message Direction No data to display. * Message Direction: INBOUND * Enable: No BIC: Document/CstmrCdtTrfInitn ✖ Search elements 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 66: 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 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 XPath Configuration List** section.

Table 24: Other Actions

To...	Do this...
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 provider link. To add the screening configuration of External Attribute, select the Attributes under the **Screening External Attribute Configuration** list. The **Screening External Attribute Configuration** list is displayed.

Figure 67: 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:

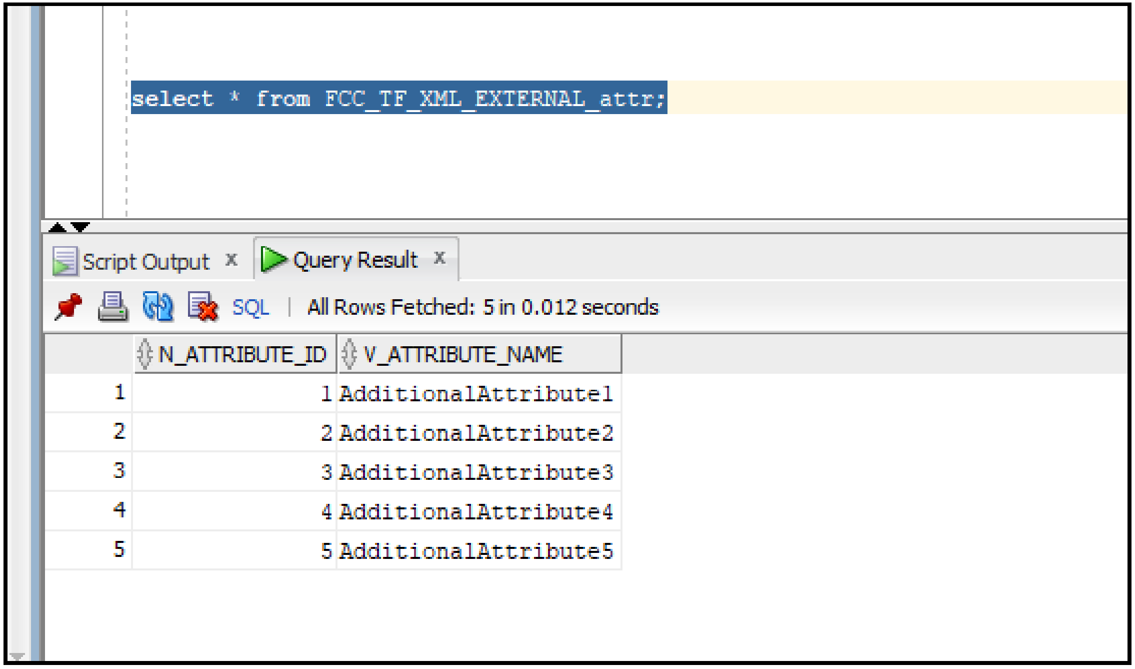
> **NOTE** The **Add** button will only appear when the user configures the FCC_TF_XML_EXTERNAL_ATTR and FCC_TF_XML_EXTERNAL_ATTR_MLS tables. Refer the following examples.

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 68: Example 1



```
select * from FCC_TF_XML_EXTERNAL_attr;
```

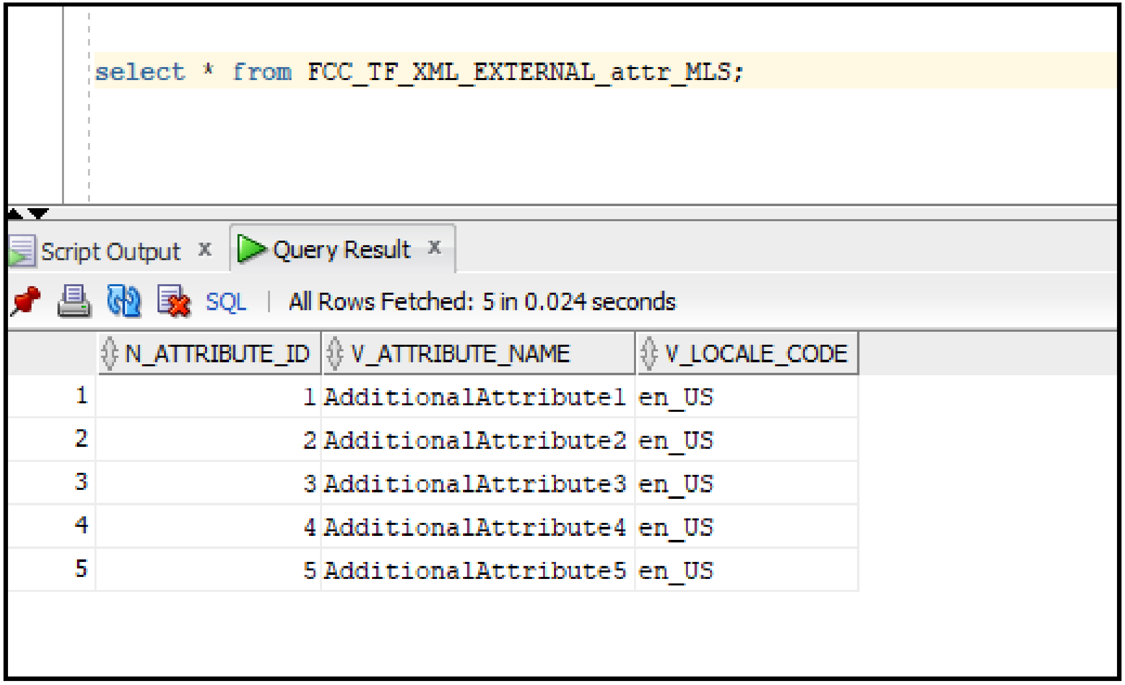
	N_ATTRIBUTE_ID	V_ATTRIBUTE_NAME
1	1	AdditionalAttribute1
2	2	AdditionalAttribute2
3	3	AdditionalAttribute3
4	4	AdditionalAttribute4
5	5	AdditionalAttribute5

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 69: Example 2



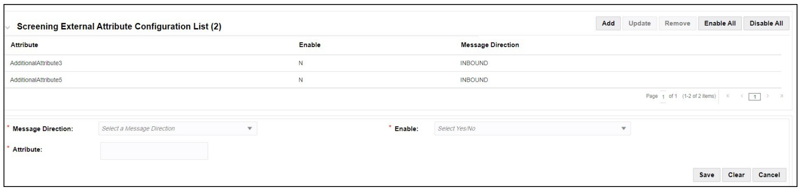
```
select * from FCC_TF_XML_EXTERNAL_attr_MLS;
```

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

The following table describes how to take additional actions.

Table 25: Other Actions

To...	Do this...
Add an external attribute configuration	Click **Add**. The following fields appear: **Figure 70: 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**.
Disable all web service configurations	Click **Disable All**.

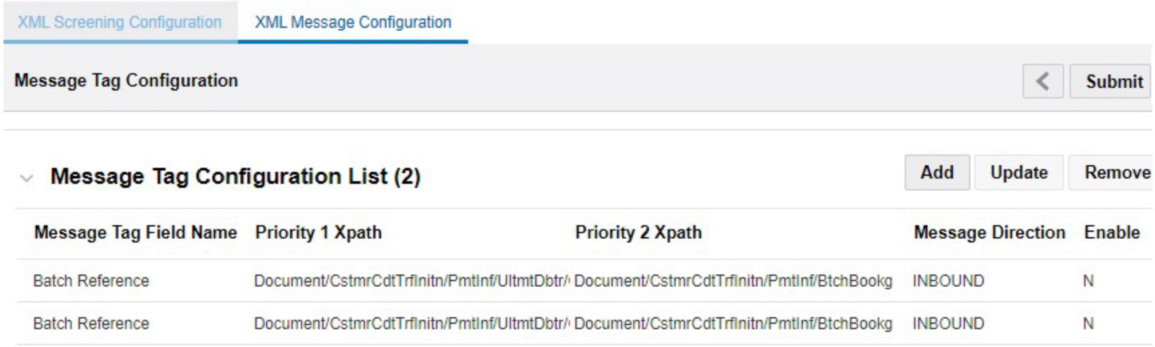
1. After configuring the External Attributes, give the following attribute names (Same attribute names which are populated in the above tables) in message posting jsp.

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 71: XML Message Configuration Tab



XML Screening Configuration
XML Message Configuration
Message Tag Configuration
<
Submit
Message Tag Configuration List (2)
Add
Update
Remove

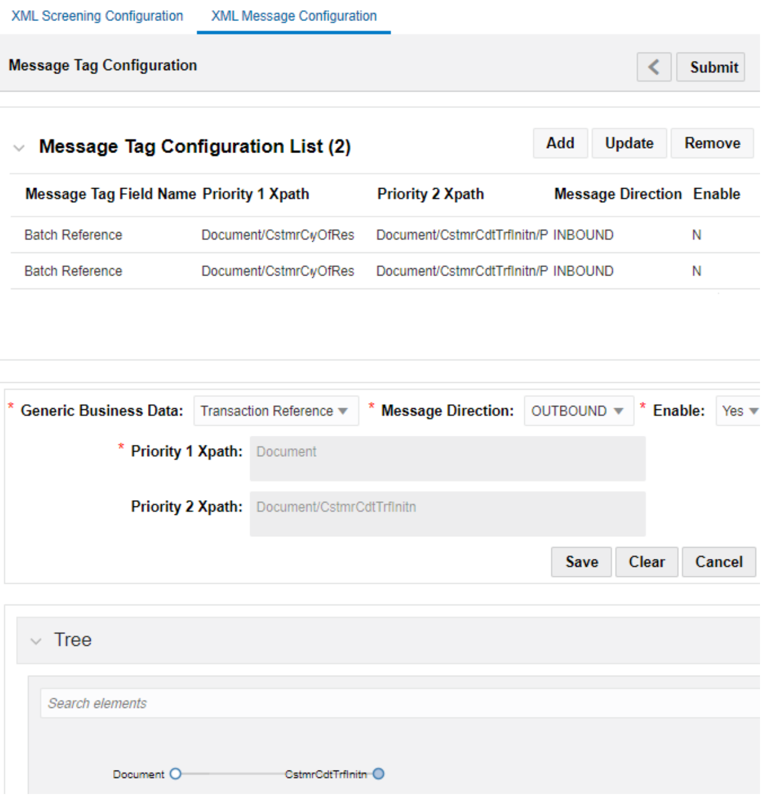
Message Tag Field Name	Priority 1 Xpath	Priority 2 Xpath	Message Direction	Enable
Batch Reference	Document/CstmrCdtTrfInitn/PmtInf/UltmtDbtr/	Document/CstmrCdtTrfInitn/PmtInf/BtchBookg	INBOUND	N
Batch Reference	Document/CstmrCdtTrfInitn/PmtInf/UltmtDbtr/	Document/CstmrCdtTrfInitn/PmtInf/BtchBookg	INBOUND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

You can also perform the following actions:

Table 26: Other Actions

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

<b>Figure 72: Add a message configuration</b>



Message Tag Configuration List (2)

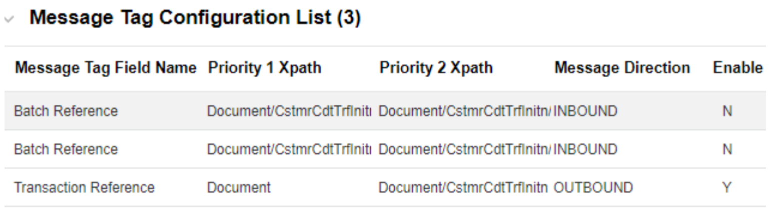
<table>
<tr><th>Message Tag Field Name</th><th>Priority 1 Xpath</th><th>Priority 2 Xpath</th><th>Message Direction</th><th>Enable</th></tr>
<tr><td>Batch Reference</td><td>Document/CstmrCyOfRes</td><td>Document/CstmrCdtTrfInitn/P</td><td>INBOUND</td><td>N</td></tr>
<tr><td>Batch Reference</td><td>Document/CstmrCyOfRes</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 73: 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 Configuration List</b> section.</td></tr>
</table>

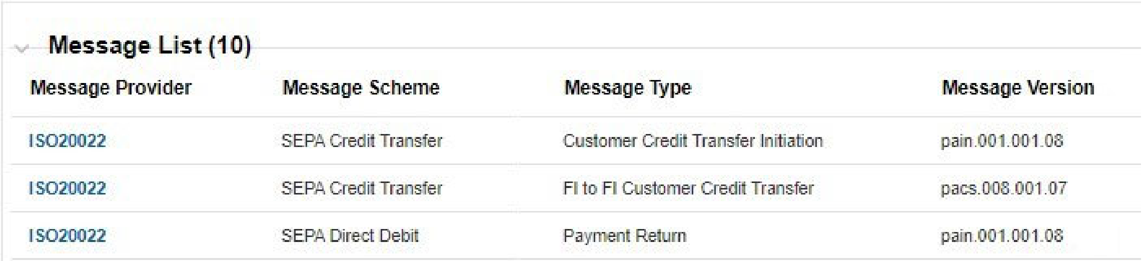
Table 26: Other Actions

To...	Do this...
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 74: 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`

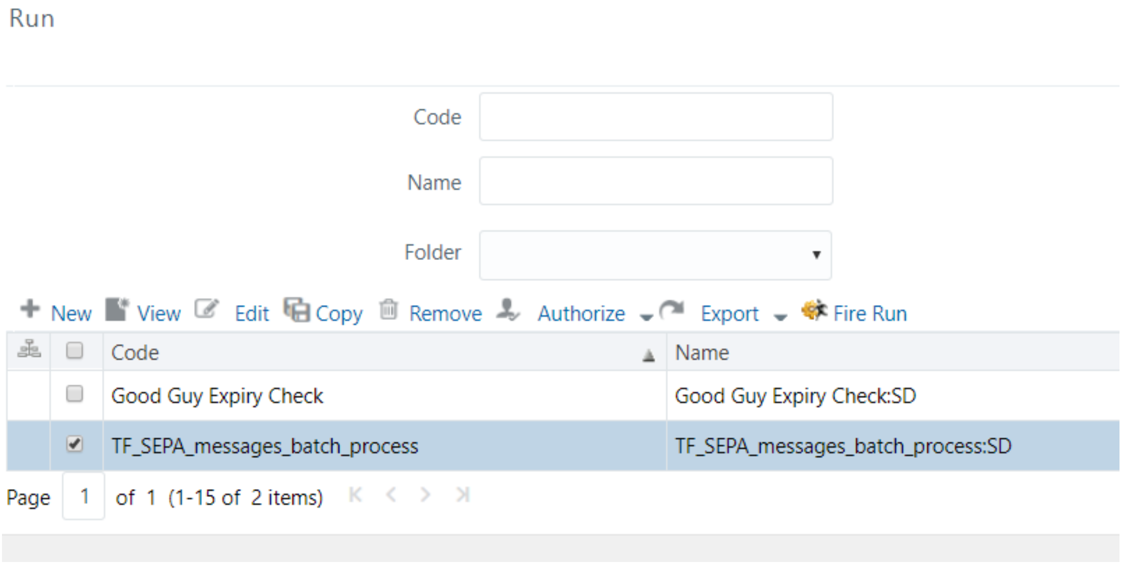
  For example, `/scratch/fccmappchef/SANC807/SANC807/ficdb/log/TF_XML`

> **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 75: Run Page



Run

Code

Name

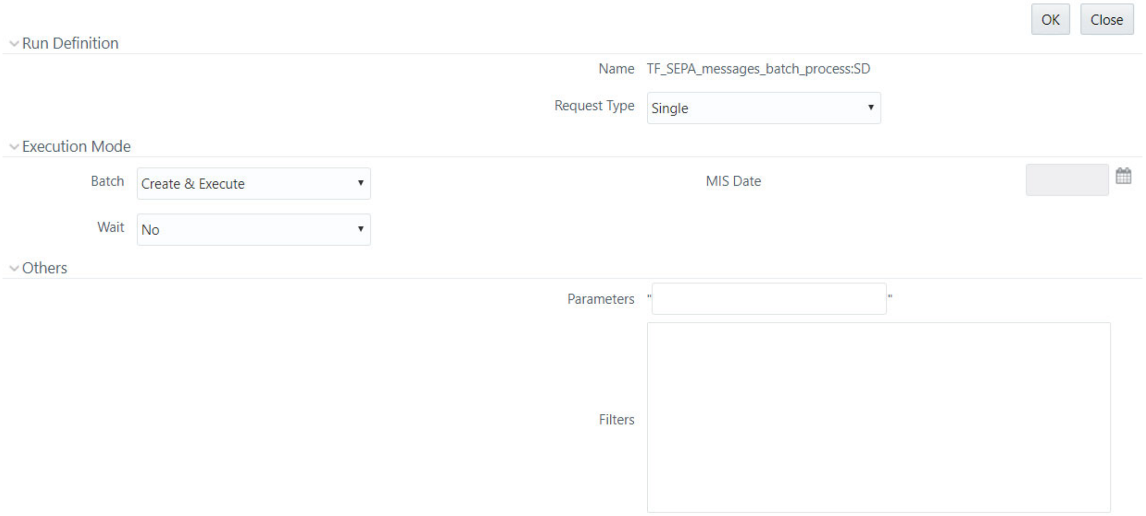
Folder ▾

	□	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 76: Fire Run Page



Run Definition

Name TF_SEPA_messages_batch_process:SD

Request Type Single

Execution Mode

Batch Create & Execute

MIS Date

Wait No

Others

Parameters " "

Filters

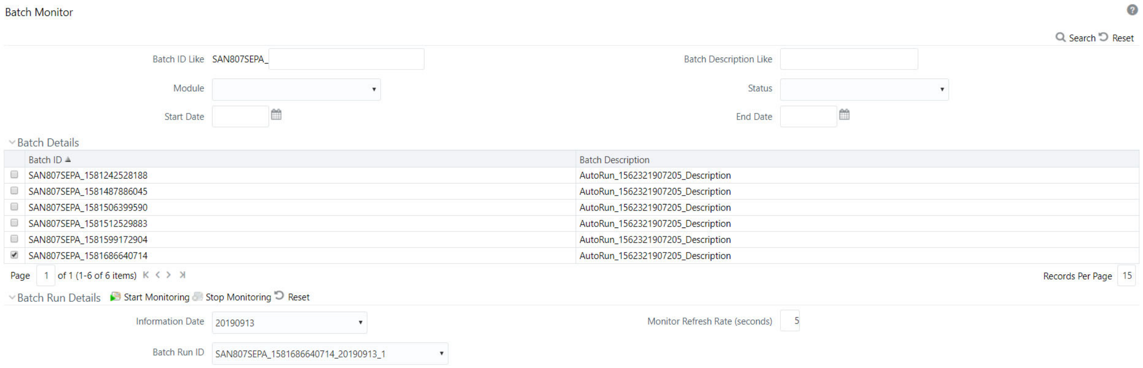
3. Select **Single** as the **Request Type**.
4. Select **Create & Execute** in the **Batch** field. The **MIS Date** field is displayed.
5. Select the date on which you want to execute the run. This date must be the same as the folder you create before you run the ISO20022 batch. In the example shown, 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 77: Batch Monitor Page



Batch ID Like SAN807SEPA_

Batch Description Like

Module

Status

Start Date

End Date

Batch Details

	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

Batch Run Details

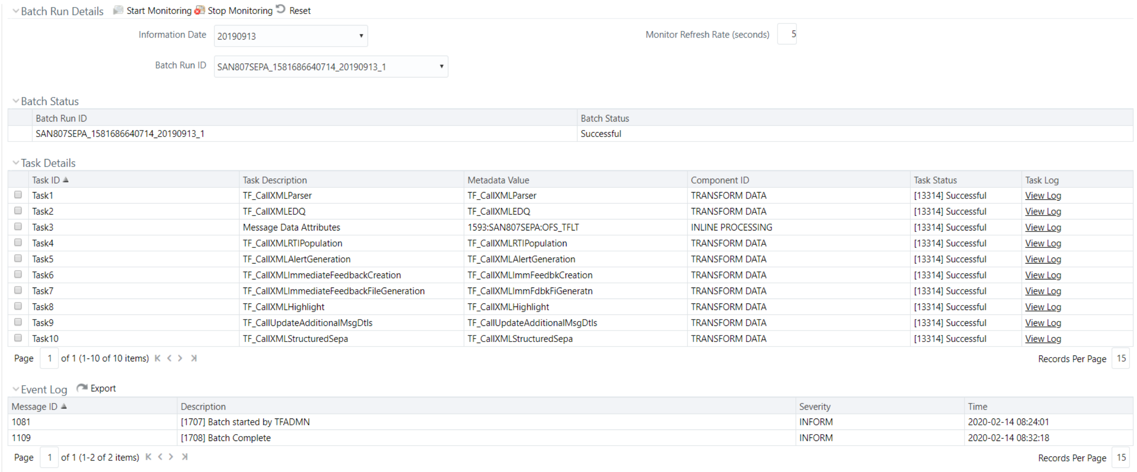
Information Date 20190913

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 78: Tasks in the Batch Monitor Page



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 27: 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_CallXMLImmediate-FeedbackCreation	Populates the feedback table.
Task7	TF_CallXMLImmediate-FeedbackFileGeneration	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.

Table 27: Task Details

Task ID	Task Name	Task Description
Task10	TF_CallXMLStructuredSepa	Populates the data in the Structured Message tab in the Investigation User Interface.

8.2 Audit Queries

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

Table 28: Audit Queries for ISO20022

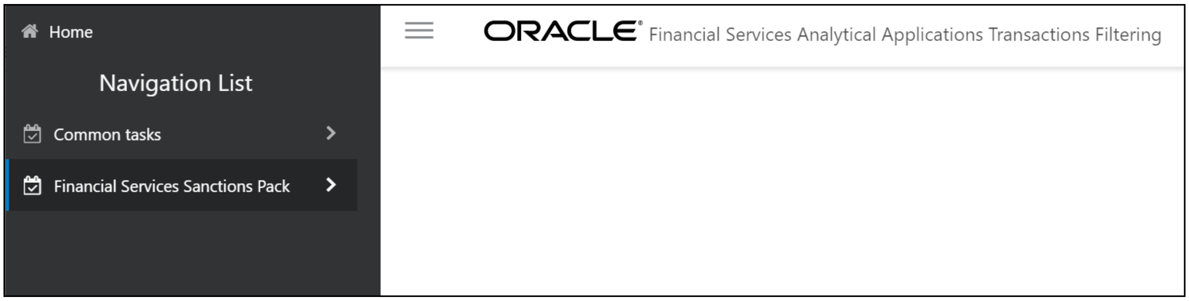
Table Name	Query	Description
FCC_TF_XML_XSD_CONF	Select * from FCC_TF_XML_XSD_CONF_HIST	Run this query to see the history of all the actions that have been performed.
FCC_TF_XML_MSG_TAG_FLD_XPATH	Select * from FCC_TF_XML_MSG_TAG_FLD_XPATH _HIST	Run this query to see the history of all the actions performed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

9 Configurations for the US NACHA Batch Process

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

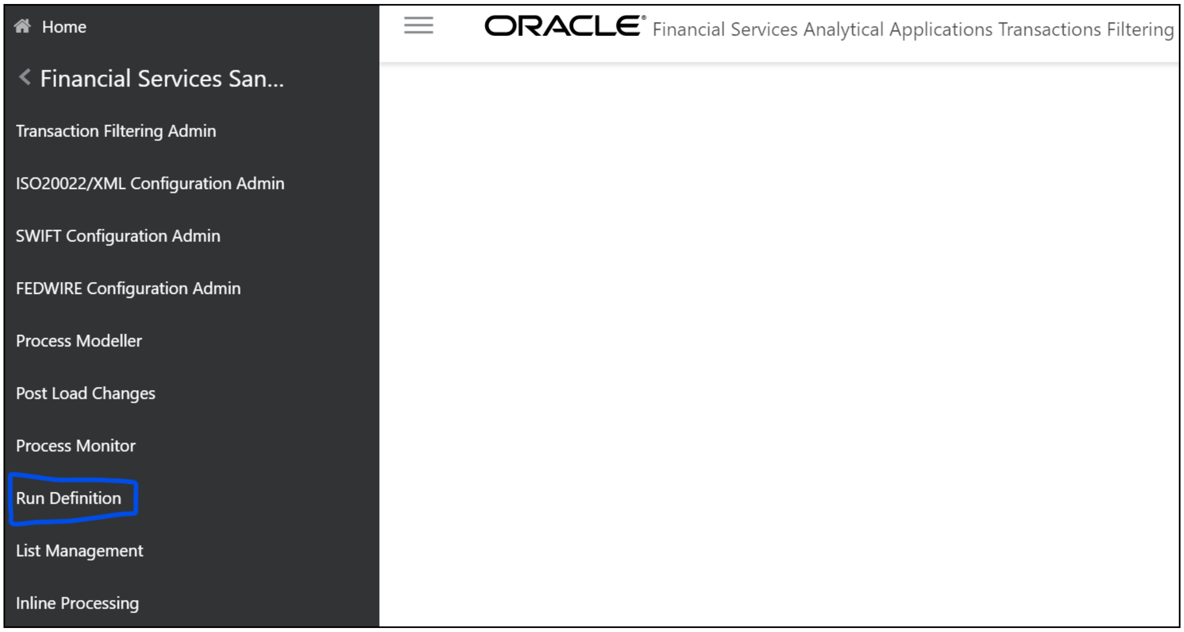
1. On the **Financial Services Analytical Applications Transactions Filtering** landing page, click **Financial Services Sanctions Pack.**

Figure 79: Financial Services Sanctions Pack Menu


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

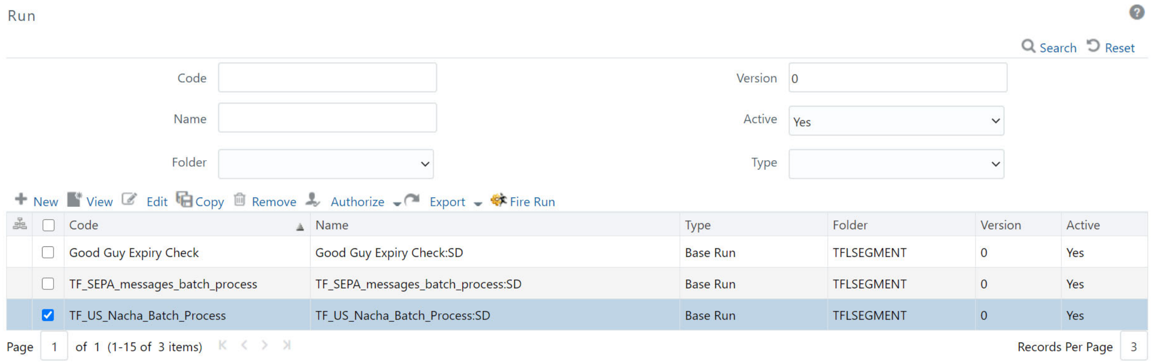
2. Click **Run Definition.** The **Run page** is displayed.

Figure 80: 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 81: Run Page



Run

Search Reset

Code

Version 0

Name

Active Yes

Folder

Type

New View Edit Copy Remove Authorize Export Fire Run

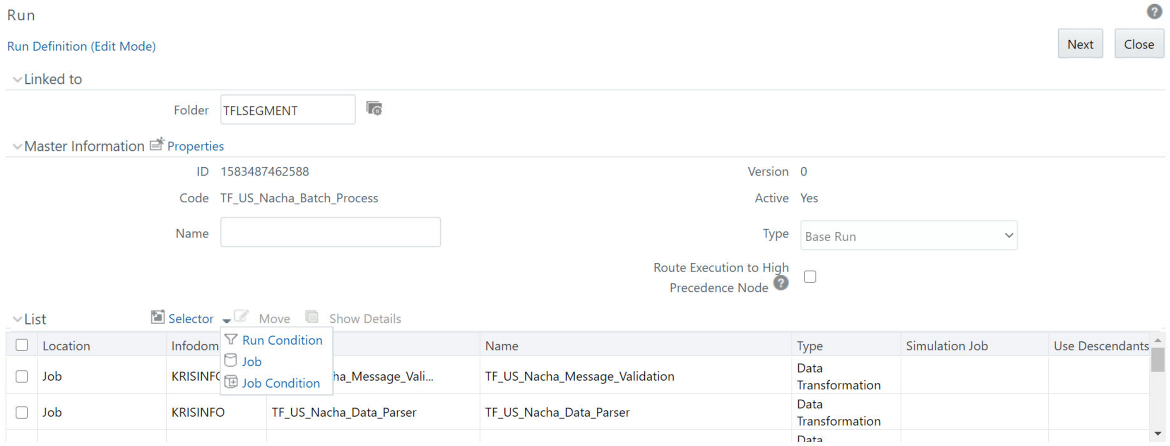
	Code	Name	Type	Folder	Version	Active
□	Good Guy Expiry Check	Good Guy Expiry Check:SD	Base Run	TFLSEGMENT	0	Yes
□	TF_SEPA_messages_batch_process	TF_SEPA_messages_batch_process:SD	Base Run	TFLSEGMENT	0	Yes
☑	TF_US_Nacha_Batch_Process	TF_US_Nacha_Batch_Process:SD	Base Run	TFLSEGMENT	0	Yes

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 82: Run Definition (Edit Mode)



Run

Run Definition (Edit Mode)

Next Close

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 □

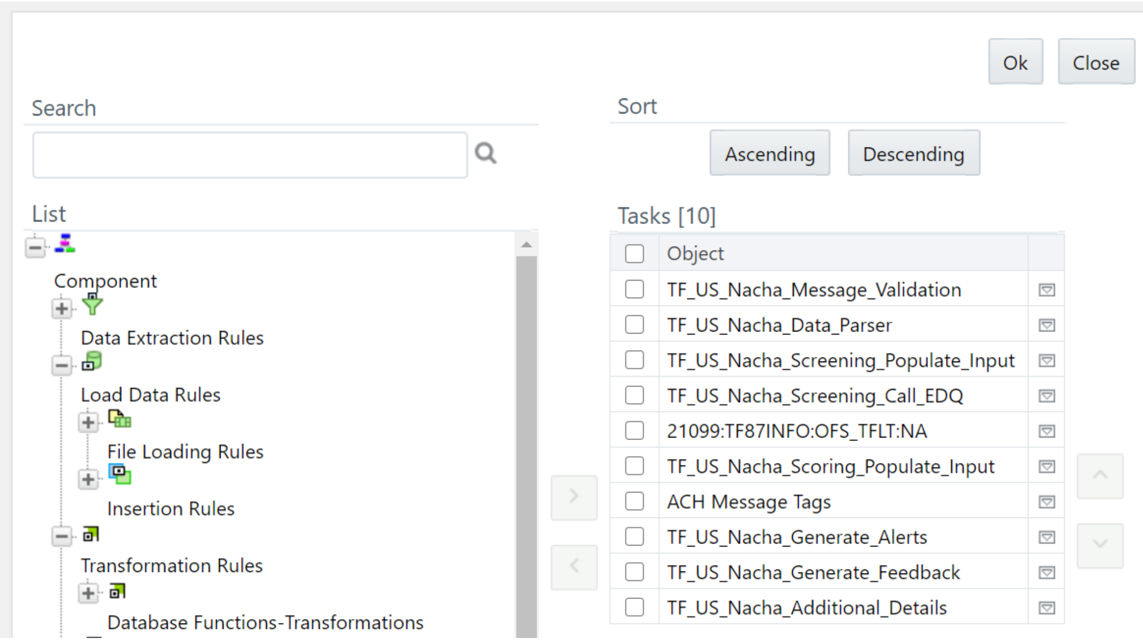
List

Selector Move Show Details

□	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 Selector** window is displayed.

Figure 83: Component Selector Window

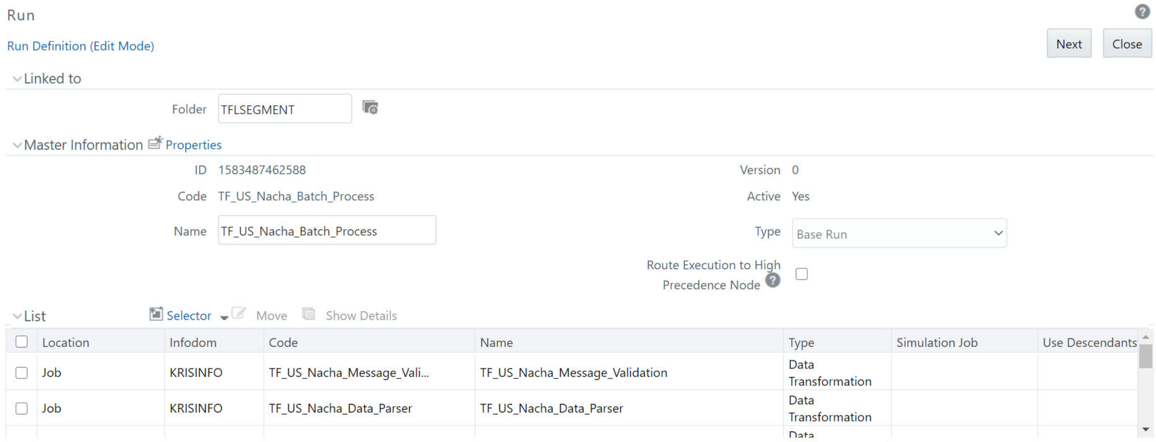


Tasks [10]

	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 84: Run Definition (Edit Mode) – Batch Name



Folder TFLSEGMENT

ID 1583487462588

Code TF_US_Nacha_Batch_Process

Name TF_US_Nacha_Batch_Process

Version 0

Active Yes

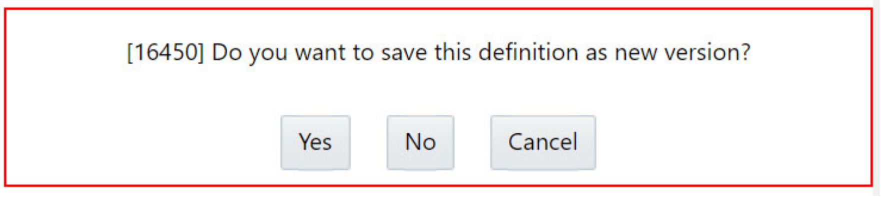
Type Base Run

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 85: 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.

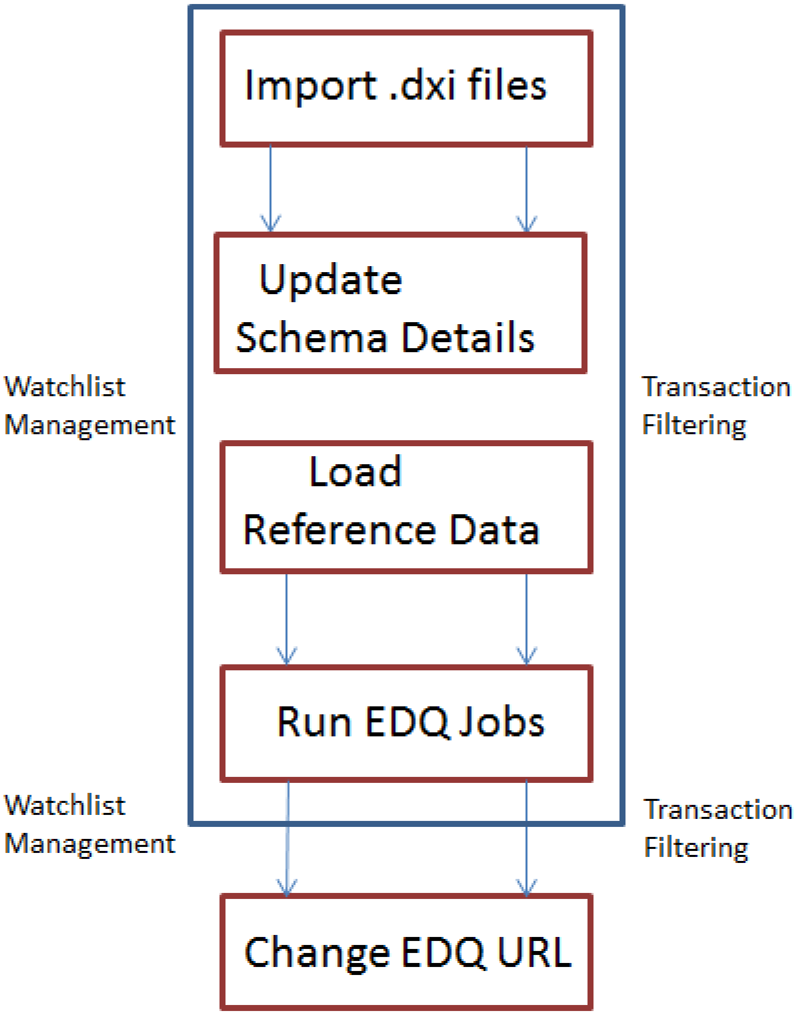
- Set the workunitexecutor.outputThreads value to a number which is greater than the number of cpu-cores and number of connection to write results and staged data to the database to tune IO heavy real-time process. This is particularly useful when the database machine is more powerful than the EDQ server.
- 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:+UseAdaptive-SizePolicy -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:

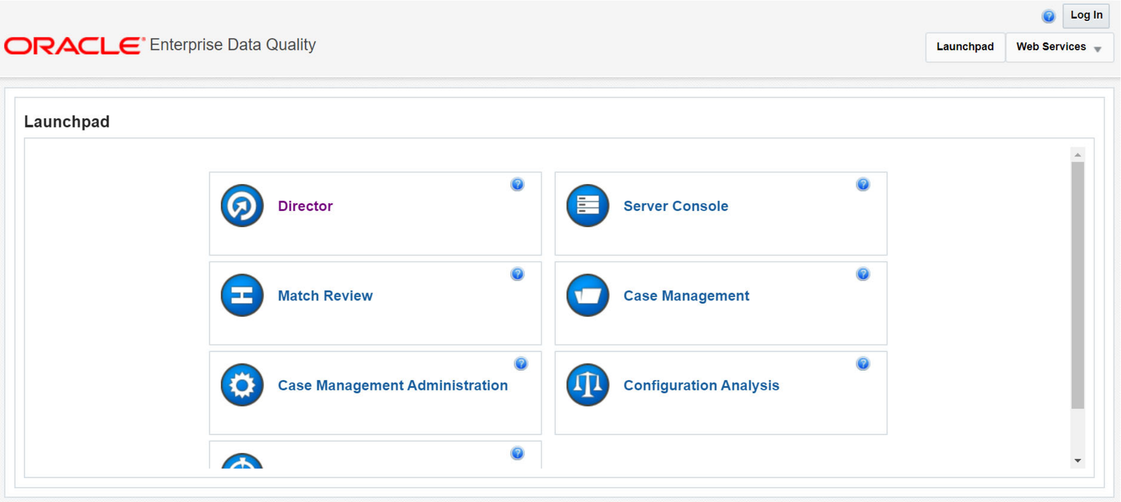
Figure 86: Enterprise Data Quality (EDQ) Configuration Steps



To configure EDQ, follow these steps:

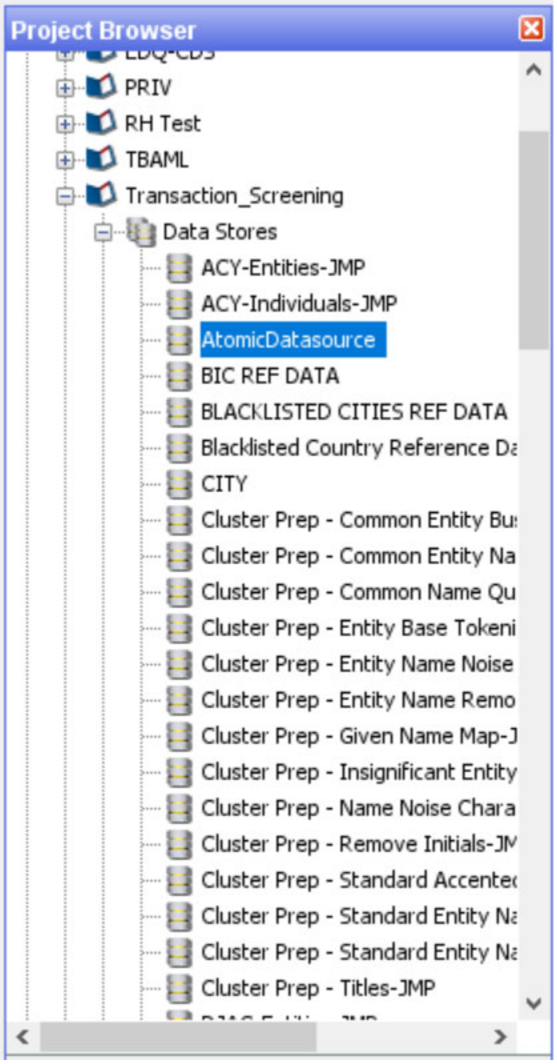
1. Import the `Watchlist Management.dxi` file from the `FIC_HOME/SanctionsCommon` path.
2. Import the `Transaction_Screening.dxi` file from the `FIC_HOME/Transaction_Processing` path (This is for SWIFT messages only).
3. Import the `Transaction_Screening_SEPA.dxi` file from the `FIC_HOME/Transaction_Processing` 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 the **Edit Data Store** window, follow these steps:
   - Go to the EDQ URL and open the **Director** menu. The **Director** landing page appears.

Figure 87: Director Menu in EDQ



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

Figure 88: Project Browser Pane

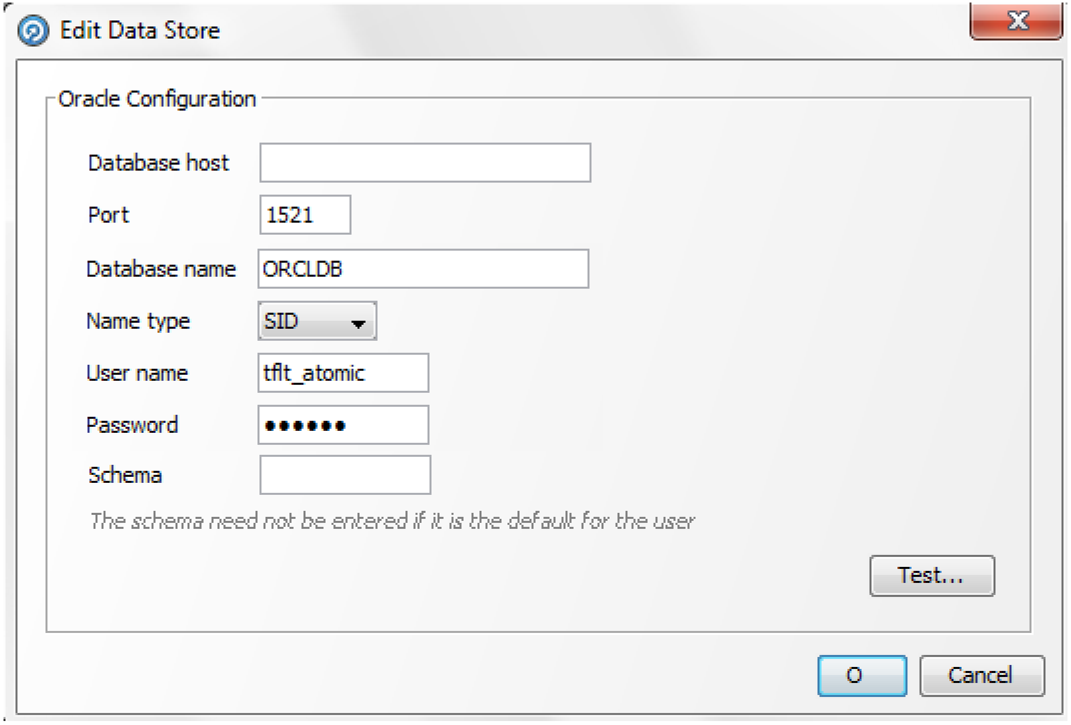


Project Browser

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

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

Figure 89: Edit Data Store Window



Oracle Configuration

Database host:

Port: 1521

Database name: ORCLDB

Name type: SID

User name: tflt_atomic

Password: ●●●●●●

Schema:

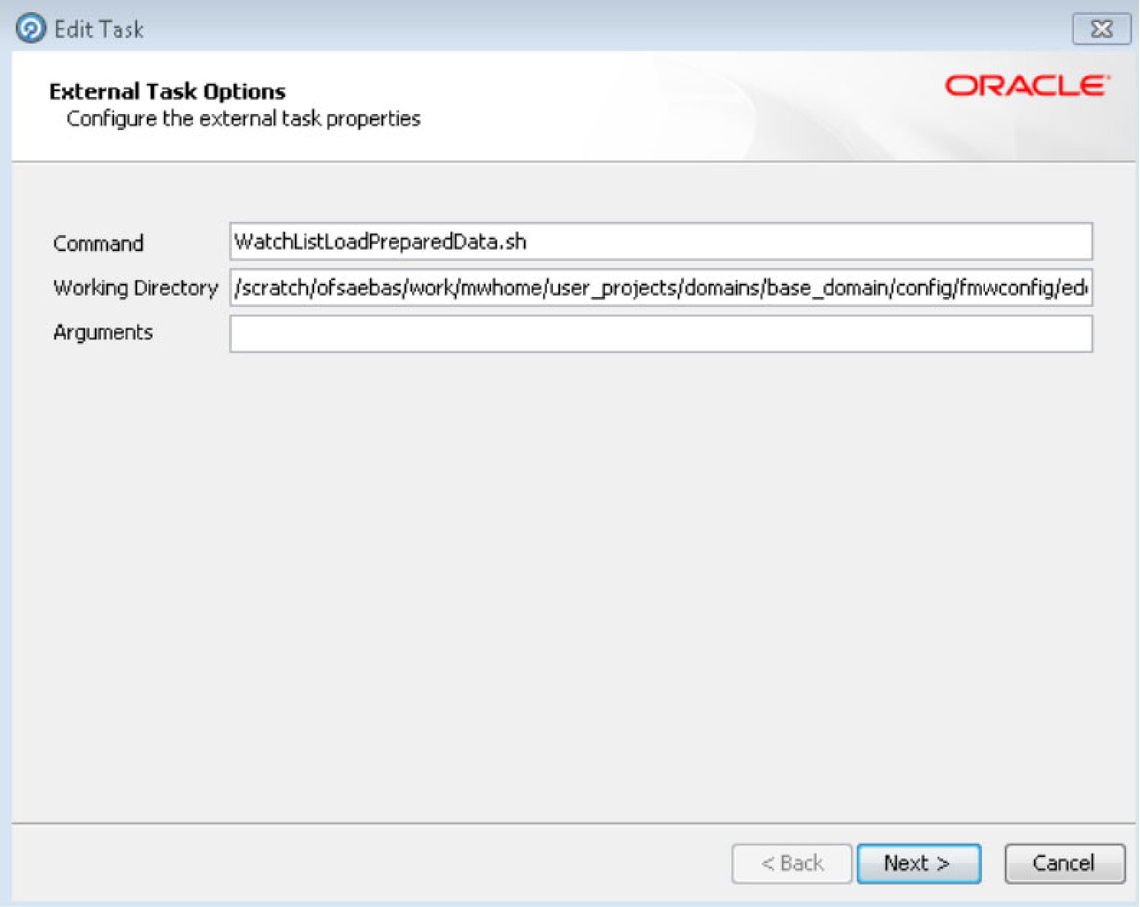
The schema need not be entered if it is the default for the user

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 90: Edit Task Window



External Task Options

Configure the external task properties

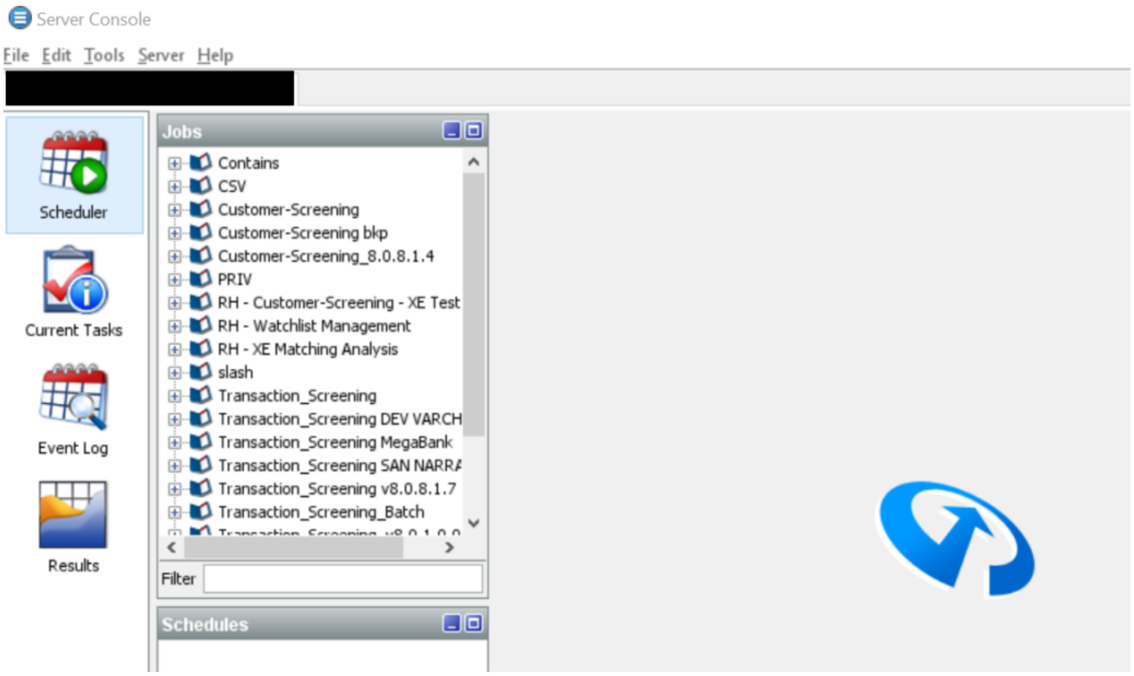
Command: WatchListLoadPreparedData.sh

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 91: Server Console Menu in EDQ


[redacted]
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

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 Configuring 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 `watchlist-management.properties` Run Profile, follow these steps:

1. Move your private watch list data to the staging area by setting `phase.PRIV\ -\ Stage\ reference\ lists.enabled` to **Y**.
2. Set `phase.PRIV\ -\ Prepare\ without\ filtering.enabled` to **Y** to prepare the private watch list without filtering.

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

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

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

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

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

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

stageddata.ACY\ Sources.visible = Y

stageddata.ACY_All.visible = Y

stageddata.ACY_Sources.visible = Y

10.2.2.2.2 Configuring Match Rules

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

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

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

```
phase.*.process.*.[I010O]\ Exact\ name\ only.san_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.*.[I010O]\ Exact\ name\ only.san_rule_en-
abled = false
```

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

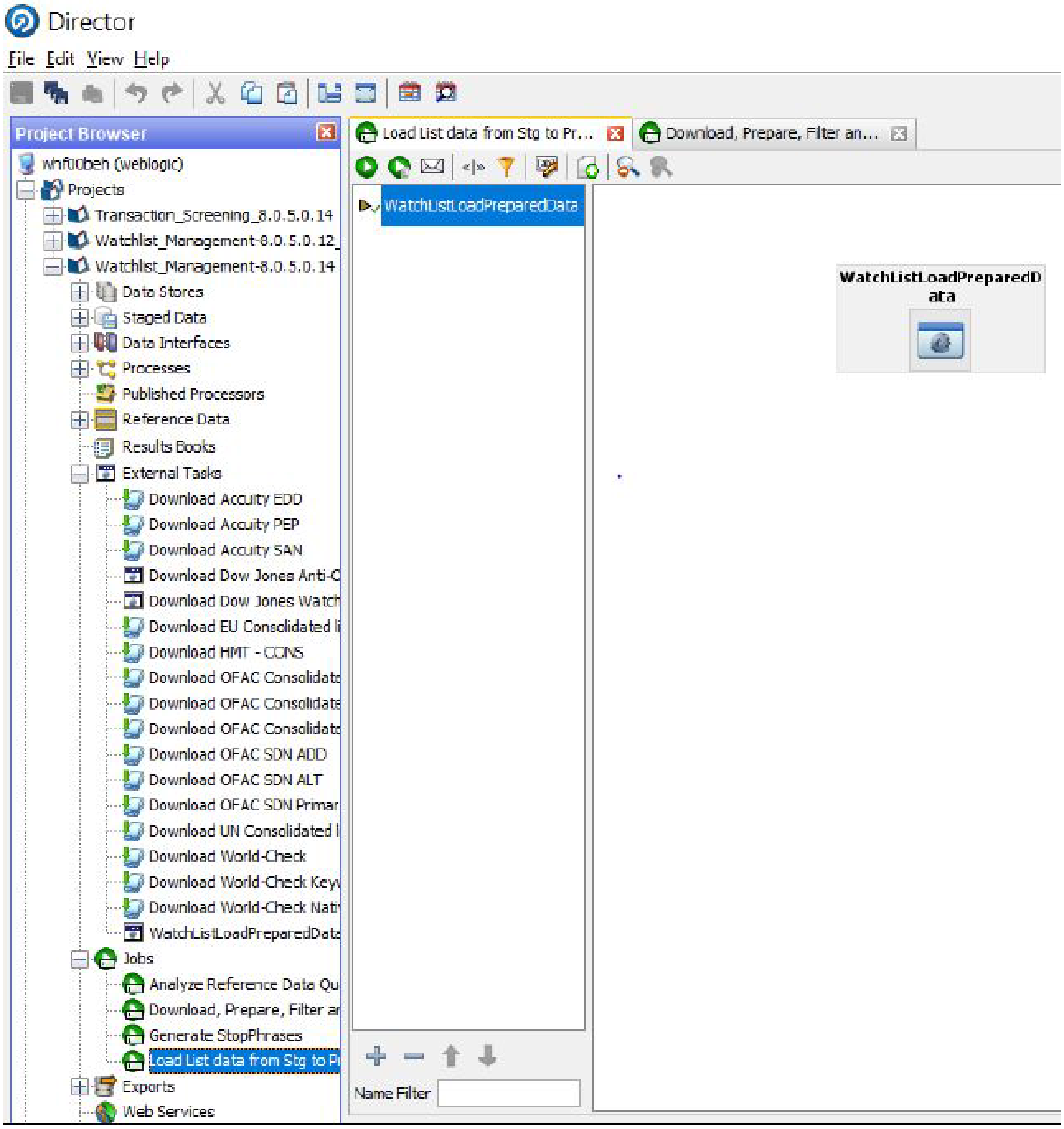
10.2.2.2.3 Configuring Jobs

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

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

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

Figure 92: 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 P
Exports
Web Services
Load List data from Stg to Pr...
Download, Prepare, Filter an...
WatchListLoadPreparedData
WatchListLoadPreparedD ata
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.

10.2.2.3.1 Enabling Watch List Filtering

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

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

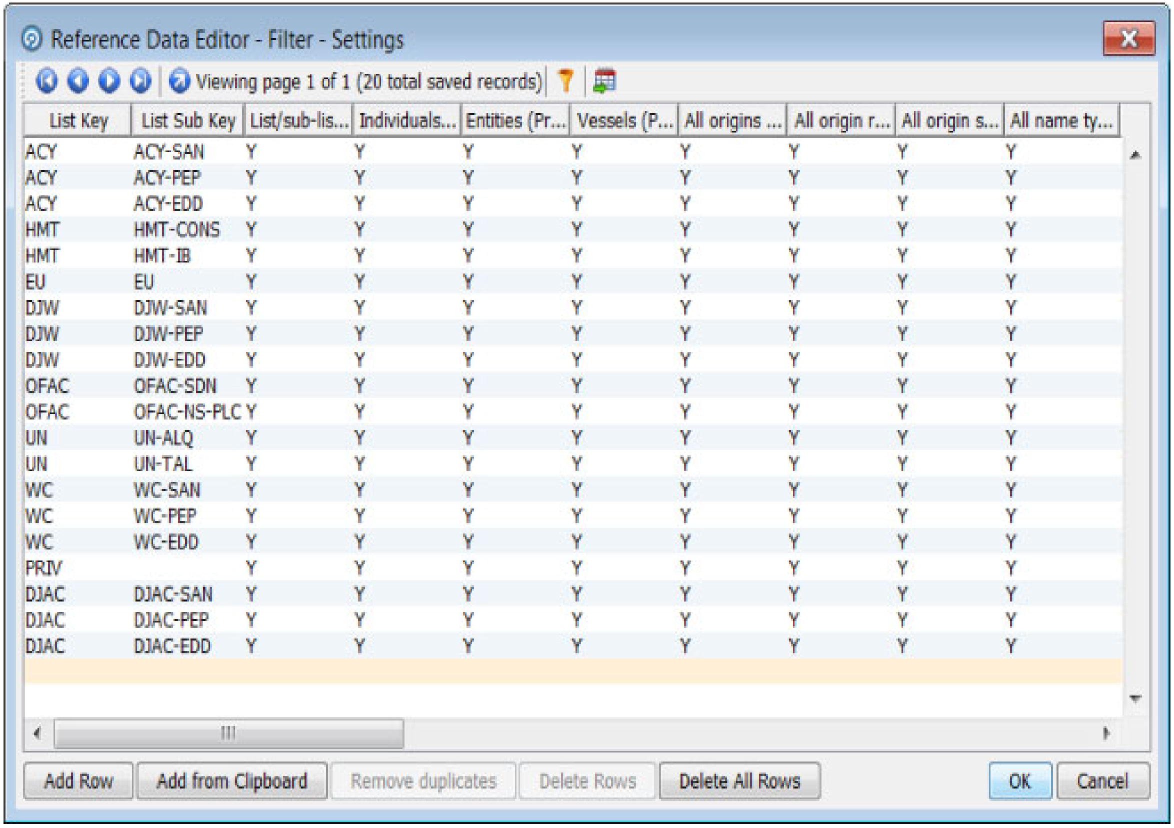
10.2.2.3.2 Configuring Watch List Filtering

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

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

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

Figure 93: Reference Data Editor - Filter - Settings Window



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

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

All the reference data filters are set to **Y** by default, except `Linked Profiles` which is set to **N**. No actual filtering is performed on watch list data unless these settings are changed.

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

Broadly speaking, watch list filtering falls into four categories:

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

10.2.2.3.3 Primary and Secondary Filtering, and Linked Records

- Primary filtering - These filters are used to return all profiles that match the criteria specified.
- Linked Profiles - If this value is set to **Y**, then all profiles linked to those captured by Primary filters are also captured. An example is a filter configured to capture all Sanctions and their related PEPs.
- Secondary filtering - These filters are applied to further filter any linked profiles that are returned.

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

10.2.2.3.4 Setting Multiple Values for Primary and Secondary Filters

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

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

To filter using one or more of these options, set the relevant value in the `Filter - Settings` reference data to **N**, and then make further changes to the corresponding reference data.

> **NOTE** When you set the `Filter - Settings` reference data to **N**, only the records that match the values set in the corresponding reference data are included. For example, if you set the value of `All name qualities` to **N** in `Filter - Settings`, then you can determine which name qualities must be included for each watch list in the `Filter - Primary Name Qualities` reference data. For instance, if you include a row for high-quality names in the EU watch list, but you do not include rows for medium-quality and low-quality names for this watch list, then only records with high-quality names are included in the watch list.

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

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

10.2.2.3.5 Filtering World-Check Data

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

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

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

1.1.1.15.0.0.4Setting Filtering options in the Run Profiles

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

```
phase.WC\ -\ Prepare\ without\ filtering.enabled = N
phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 1).enabled = Y
phase.WC\ -\ Prepare\ with\ filtering\ (Part\ 2).enabled = Y
In the watchlist-screening.properties Run Profile, set the World-Check
filtering phases as follows:
phase.WC\ -\ Load\ without\ filtering.enabled = N
phase.WC\ -\ Load\ with\ filtering\ (Part\ 1).enabled = Y
phase.WC\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y
```

10.1.1.1.6 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:
    - List Key - WC
    - List Sub Key - WC-SAN
    - 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.

10.1.1.1.7 Setting Secondary Filters in the Transaction_Screening Project

To set secondary filters, follow these steps:

1. Open the `Transaction_Screening` project, and expand the reference data link.
2. Locate the `Filter - Settings` reference data file, and double-click to open it.
3. Set the `Deceased` value in the `WC-SAN` row to **N**.

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

10.1.1.1.8 Screening All Data Using Sanctions Rules

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

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

10.1.1.2 Viewing Reference Data for Web Services

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

- Goods prohibition reference data is available in `fcc_prohibiton_goods_ref_data`
- Ports prohibition reference data is available in `fcc_port_ref_data`
- Bad BICs reference data is available in `dim_sanctioned_bic`
- Stop Keywords reference data is available in `dim_stop_keywords`
- Blacklisted Cities reference data is available in `dim_sanctioned_city`
- Blacklisted Countries reference data is available in `dim_sanctioned_country`

10.1.1.2.1 Bad BICs Reference Data

The following columns are available in the template for BICs:

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

Sample Data for Sanctioned BICs

The following table provides examples based on BICs:

Table 29: Sample Data for Sanctioned BICs

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

10.1.1.2.2 Blacklisted Cities Reference Data

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

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

Sample Data for Sanctioned Cities

The following table provides examples for blacklisted cities:

Table 30: Sample Data for Sanctioned Cities

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

10.1.1.2.3 Blacklisted Countries Reference Data

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

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

Sample Data for Sanctioned Countries

The following table provides sample data for blacklisted countries:

Table 31: 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 JUM-HURIYAH AL IRAQIYAH, AL IRAQ	OFAC (Office of Foreign Assets Control)	90

Table 31: Sample Data for Sanctioned Countries

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

10.1.1.2.4 Stop Keywords Reference Data

The following columns are available in the template for keywords:

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

Sample Data for Sanctioned Stop Keywords

The following table provides examples based on keywords:

Table 32: Sample Data for Sanctioned Stop Keywords

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

10.1.1.2.5 Goods Prohibition Reference Data

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

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

Sample Data for Prohibited Goods

The following table provides sample data for prohibited goods:

Table 33: Sample Data for Prohibited Goods

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

10.1.1.2.6 Ports Prohibition Reference Data

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

- Record ID: This column displays the record serial number for the prohibited port. The record ID is unique for every port.
- Country: This column displays the name of the country where the prohibited port is located.
- Port Name: This column displays the name of the prohibited port.
- Port Code: This column displays the code of the prohibited port.
- Port Synonyms: This column displays the synonym of the prohibited port.

Sample Data for Prohibited Ports

The following table provides sample data for prohibited ports:

Table 34: 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 Sevastopol
3	New Zealand	Dunedin	NZ ORR	Otago Harbour
4	New Zealand	Ravensbourne	NZ ORR	Otago Harbour

10.1.1.3 Extending Prohibition Screening

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

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

- Edit the appropriate screening process, to create the necessary match rules and clusters for the new attribute.

11 Configuring Risk Scoring Rules

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

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.

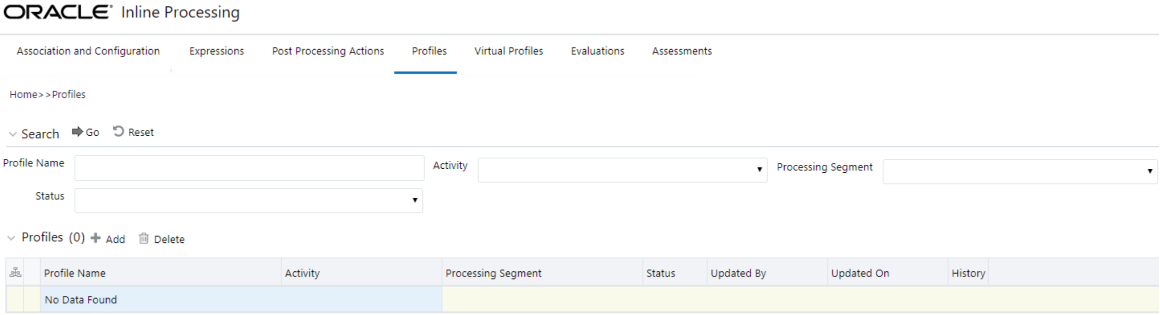
> **NOTE** The screenshots shown for these steps are taken for existing tables. You can perform similar steps for newly added tables.

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. Profiles can be based on different grouping entities (For example, account and customer) and can be filtered to only look at specific types of transactions. Profiles can also be based on time (last three months) or activity counts (last 100 transactions). For more information on Profiles, see the **Managing Profiles** chapter in the Oracle Financial Services Inline Processing Engine User Guide.

Figure 94: Profiles Menu



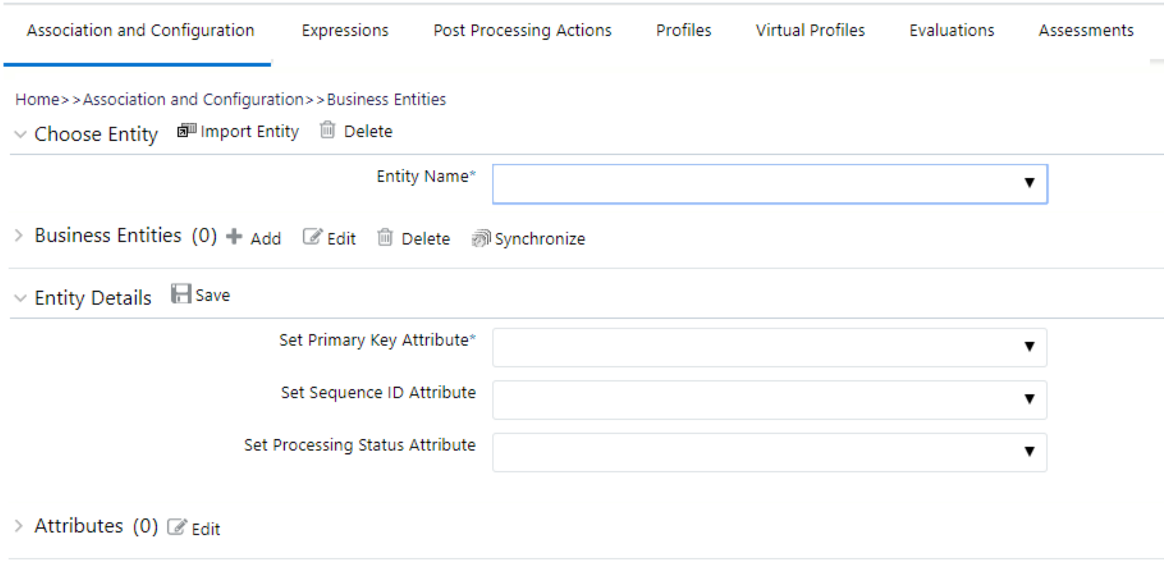
Profile Name	Activity	Processing Segment	Status	Updated By	Updated On	History
No Data Found						

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:

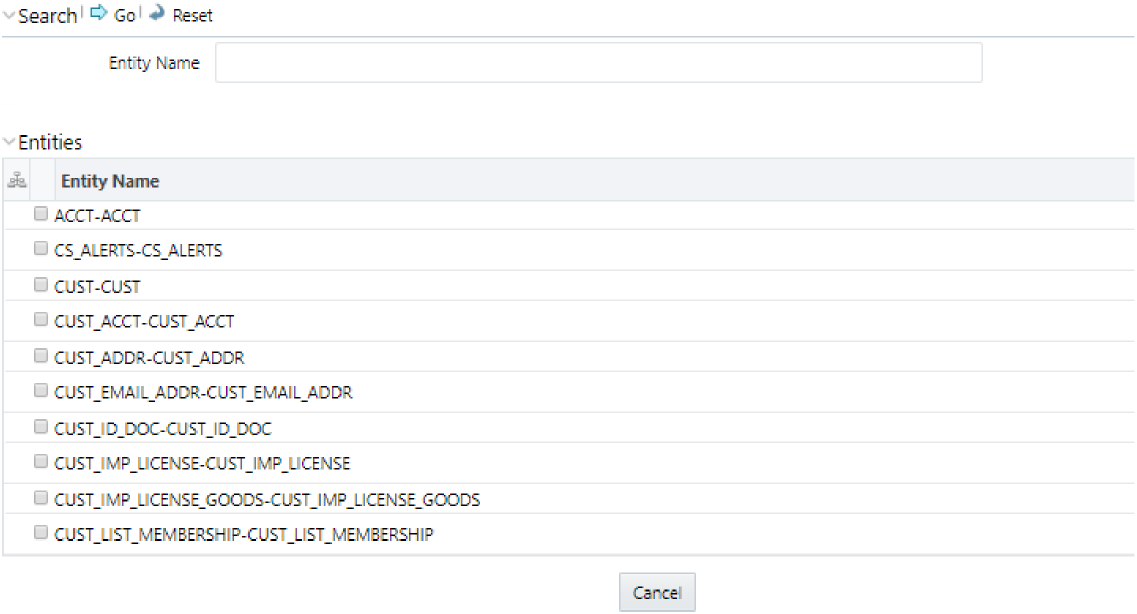
   - Click the **Association and Configuration** menu**,** then click the **Business Entities** sub-menu.
   - Select the Business Entity you want to import.
   - Click **Import Entity** Import Entity.

Figure 95: Import Table Action



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

Figure 96: Entities List



	Entity Name
□	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 35: 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.

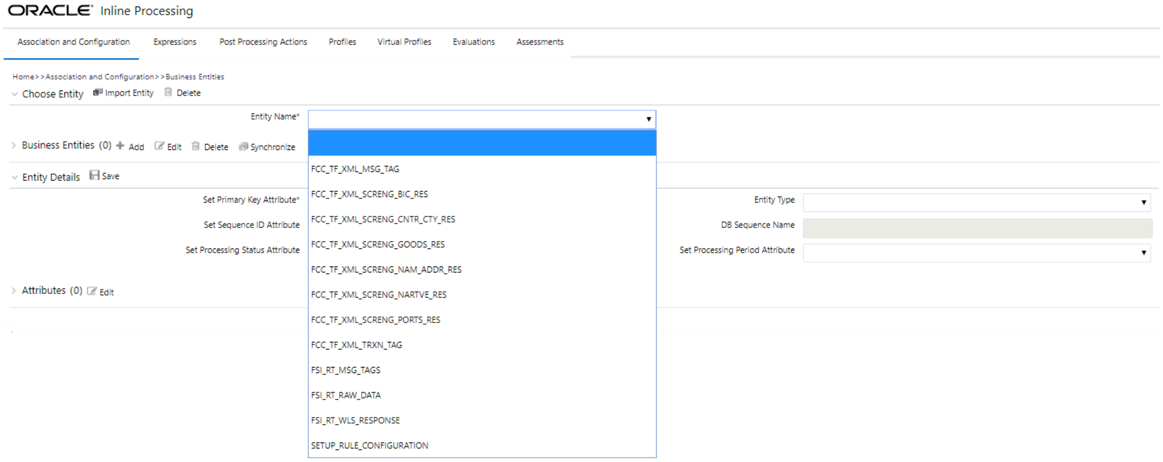
Table 35: Business Entity Fields

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.
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 97: Entities List



Entity Name*

Set Primary Key Attribute*

Set Sequence ID Attribute

Set Processing Status Attribute

Entity Type

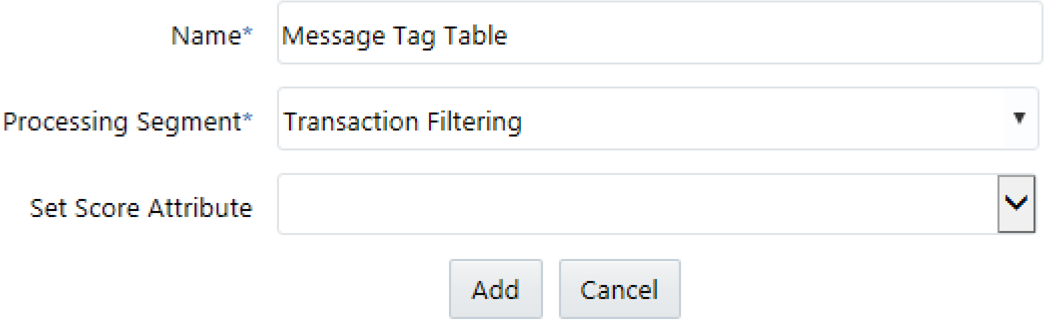
DB Sequence Name

Set Processing Period Attribute

- Click **Add**.

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

Figure 98: Business Entity attributes



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

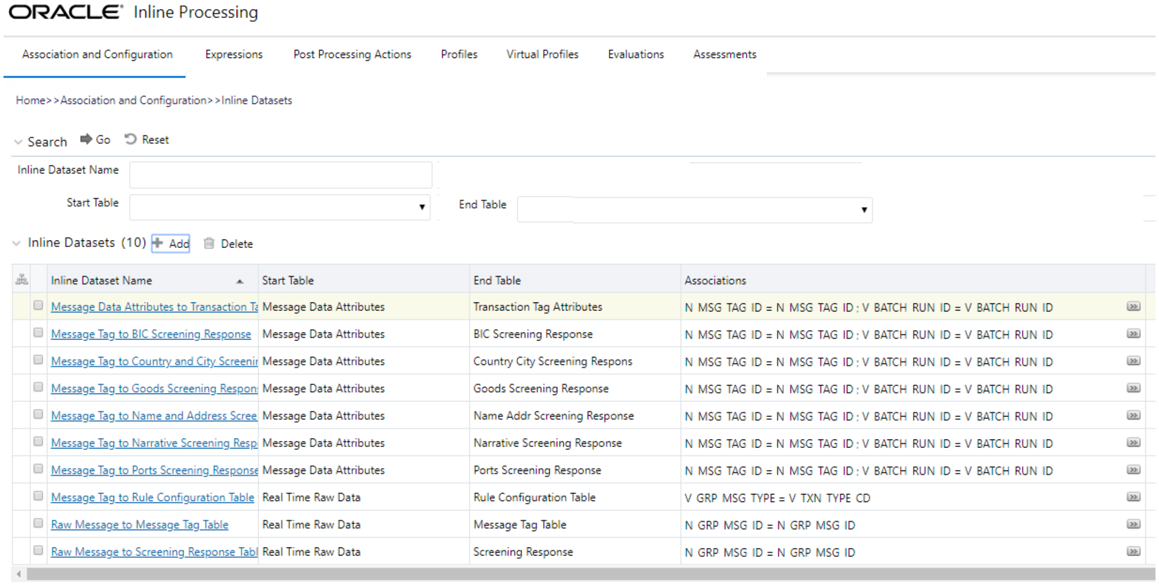
3. Click **Add**. The new parameter is added to the list of Business Entities on the **Business Entities** page.

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 Dataset, you must define at least one join.

   To add a join, follow these steps:

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

Figure 99: Inline Datasets page



Inline Dataset Name

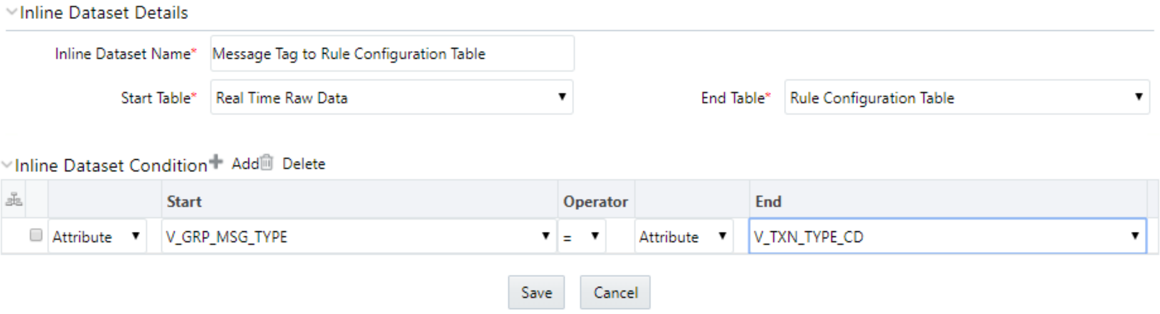
Start Table ▾ End Table ▾

Inline Datasets (10) Add Delete

	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 Screenir	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 100: Inline Datasets Attributes



Inline Dataset Name* Message Tag to Rule Configuration Table

Start Table* Real Time Raw Data ▾ End Table* Rule Configuration Table ▾

		Start	Operator		End
□	Attribute ▾	V_GRP_MSG_TYPE ▾	= ▾	Attribute ▾	V_TXN_TYPE_CD ▾

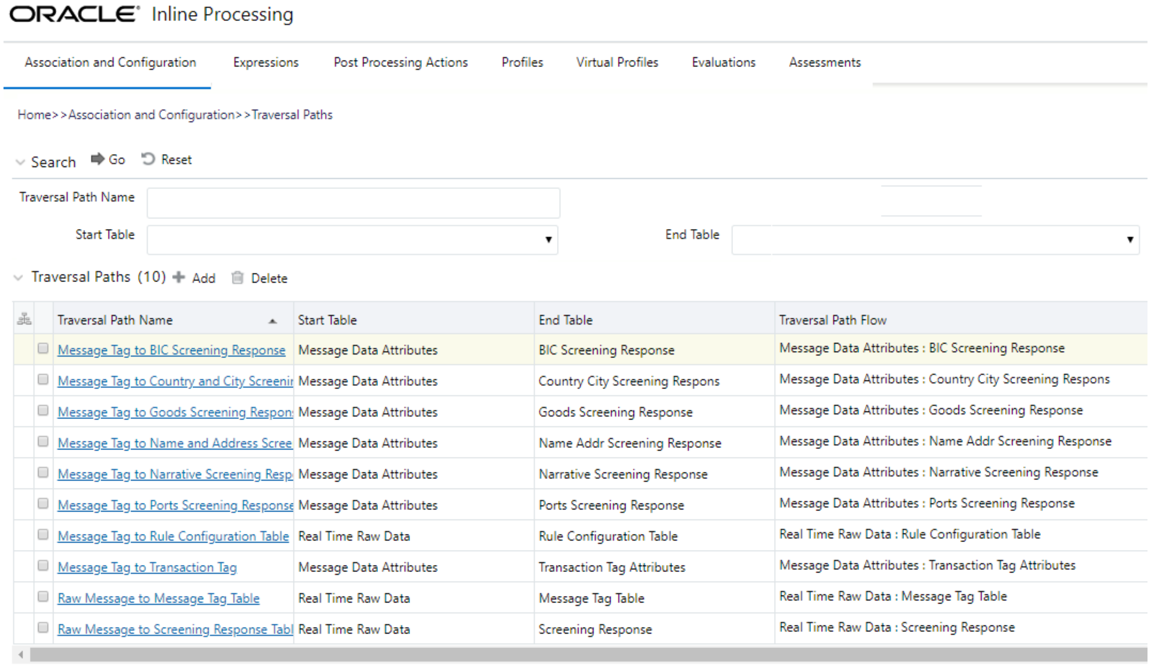
- Click **Add**.
- Click **Save**. The new dataset is added to the list of Inline Datasets on the **Inline Datasets** page. For more information on inline datasets, see the **Managing Inline Datasets** section in the Oracle Financial Services Inline Processing Engine User Guide.

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 101: Traversal Paths Page



Traversal Path Name

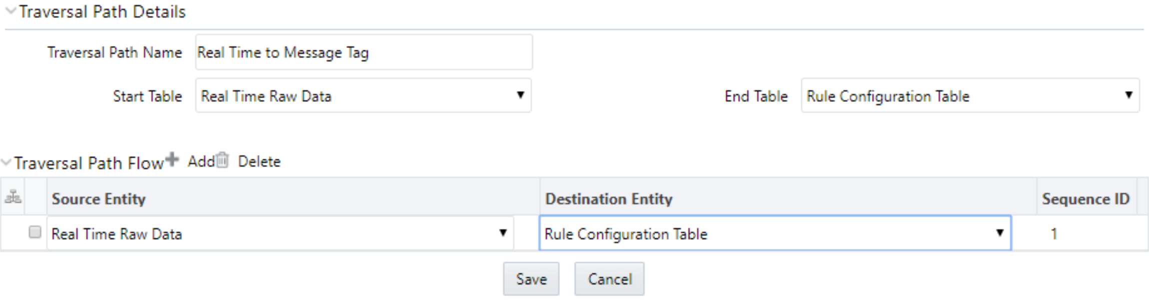
Start Table ▾ End Table ▾

Traversal Paths (10)

	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 102: Traversal Paths Attributes



Traversal Path Name: Real Time to Message Tag

Start Table: Real Time Raw Data ▾ End Table: Rule Configuration Table ▾

	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.

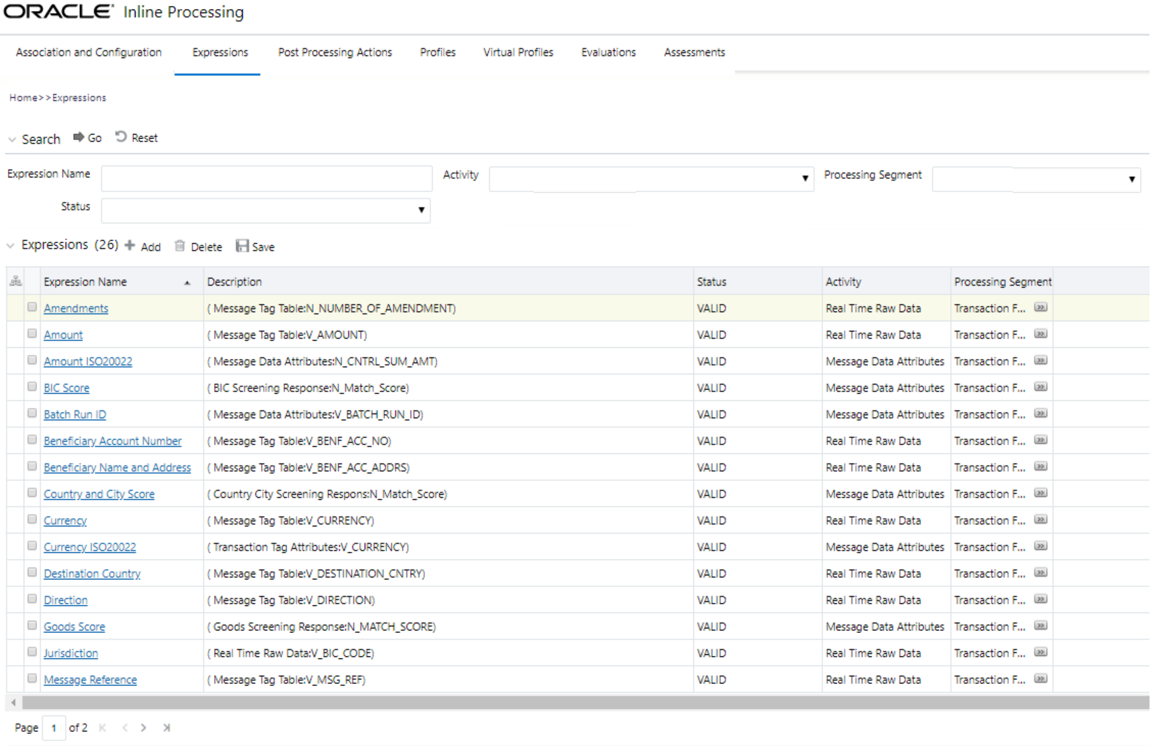
2. Add an Expression on the *risk score* column of the newly created business entity which is to be scored as a risk parameter from the **Expressions** menu. An expression is used as a filter when creating evaluations or profiles. Expressions must only be created on the activity table on which an evaluation 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 103: Expressions Page



ORACLE Inline Processing

Expression Name
Activity
Processing Segment
Status

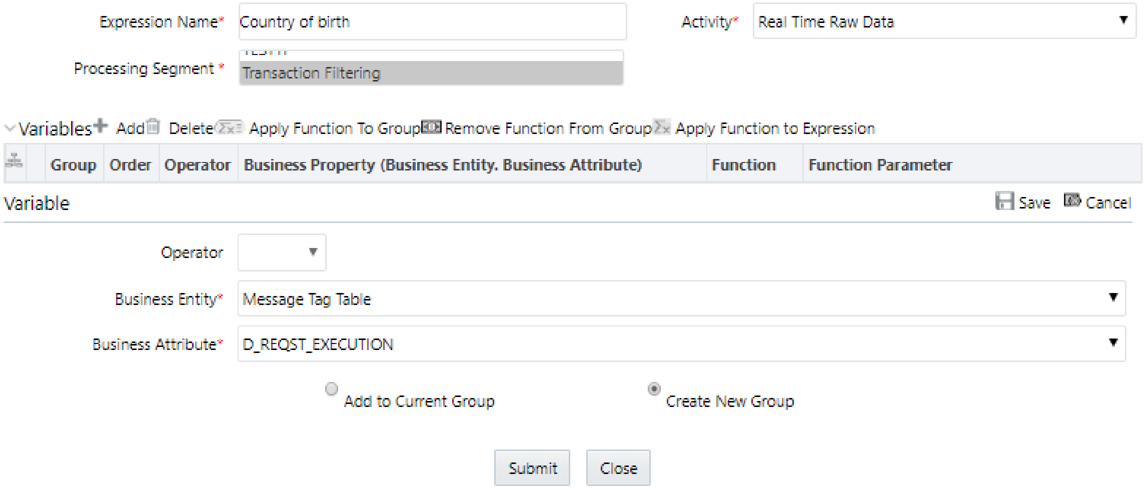
Expressions (26)

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 104: First Expression Attributes



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

Variables

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

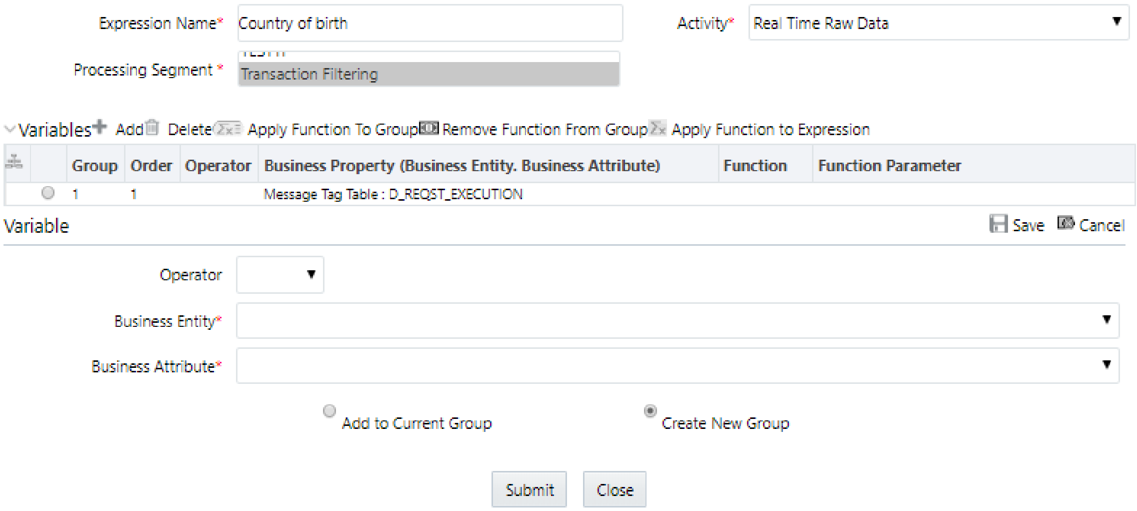
Variable

Operator	
Business Entity*	Message Tag Table
Business Attribute*	D_REQST_EXECUTION

○ Add to Current Group ● Create New Group

- 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 105: First Expression Displayed



Expression Name* Country of birth

Activity* Real Time Raw Data

Processing Segment * Transaction Filtering

Variables

Group	Order	Operator	Business Property (Business Entity. Business Attribute)	Function	Function Parameter
1	1		Message Tag Table : D_REQST_EXECUTION		

Variable

Operator

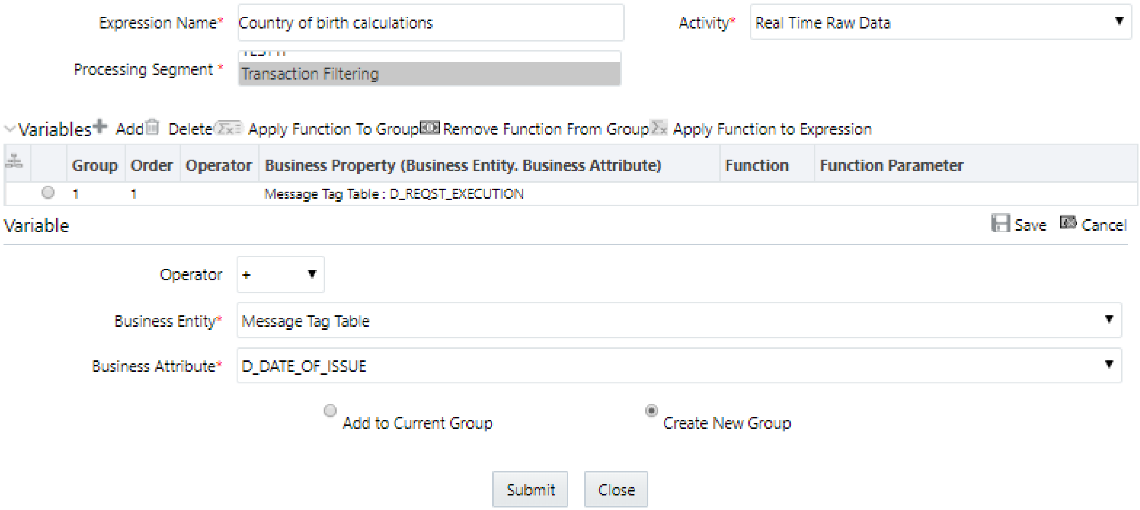
Business Entity*

Business Attribute*

○ Add to Current Group ● Create New Group

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

Figure 106: Second Expression Attributes



Expression Name* Country of birth calculations

Activity* Real Time Raw Data

Processing Segment * Transaction Filtering

Variables

Group	Order	Operator	Business Property (Business Entity. Business Attribute)	Function	Function Parameter
1	1		Message Tag Table : D_REQST_EXECUTION		

Variable

Operator +

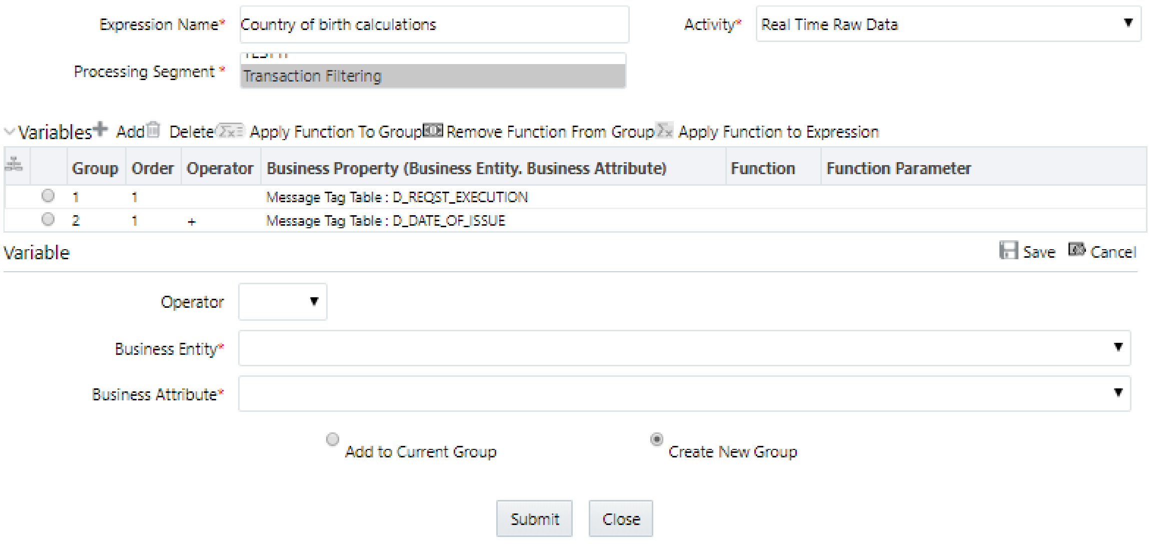
Business Entity* Message Tag Table

Business Attribute* D_DATE_OF_ISSUE

○ Add to Current Group ● Create New Group

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

Figure 107: 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 36: ISO20022 Risk-Currency VS Amount Threshold Evaluation Filters

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

- **Risk- High Risk Party Evaluation**

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

Table 37: Risk- High-Risk Party Evaluation Filters

Sl.No	Filter Name	Filter Clause
	Beneficiary Account Number	(Message Tag Table:V_BENF_ACC_NO) = (Rule Configuration Table:V_COND1)
	Rule Name	(Rule Configuration Table:V_RISK_RULE_CODE) = 'TF_HIGH_RSK_PARTY'
	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) = 'MT700'
	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 38: Risk-Currency VS Amount Threshold Evaluation Filters

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

Sl.No	Filter Name	Filter Clause
	Currency	(Message Tag Table:V_CURRENCY) = (Rule Configuration Table:V_COND1)
	Destination Country	(Message Tag Table:V_DESTINATION_CNTRY) = (Rule Configuration Table:V_COND2)

Table 39: Risk-Currency VS Destination Country Evaluation Filters

Sl.No	Filter Name	Filter Clause
	Direction	(Message Tag Table:V_DIRECTION) in ('INBOUND','OUTBOUND')
	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) = (Rule Configuration Table:V_TXN_TYPE_CD)
	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 configured then add a risk score of 20.

NOTE This score is configurable.

Table 40: Risk-High Risk Destination Country Evaluation Filters

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

Sl.No	Filter Name	Filter Clause
	Amount	(Message Tag Table:V_AMOUNT) >= 10000
	Currency	(Message Tag Table:V_CURRENCY) = 'EUR'
	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) in ('MT101', 'MT103', 'MT202COV', 'MT202')
	Direction	(Message Tag Table:V_DIRECTION) = 'INBOUND'
	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 42: Risk-Trade Amendments Evaluation Filters

Sl.No	Filter Name	Filter Clause
	Message Type	(Real Time Raw Data:V_GRP_MSG_TYPE) = 'MT707'
	Direction	(Message Tag Table:V_DIRECTION) in (('INBOUND','OUTBOUND'))
	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 different match scores in EDQ.

NOTE

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

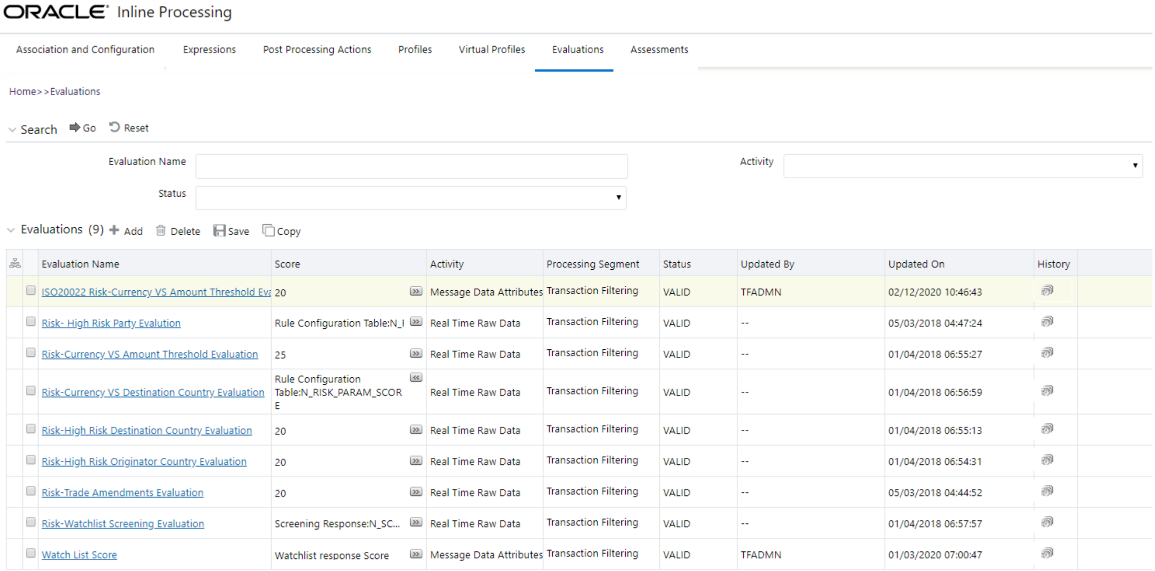
Table 43: Watch List Score Filters

Sl.No	Filter Name	Filter Clause
	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
	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 108: Evaluations Page



Evaluation Name:

Activity:

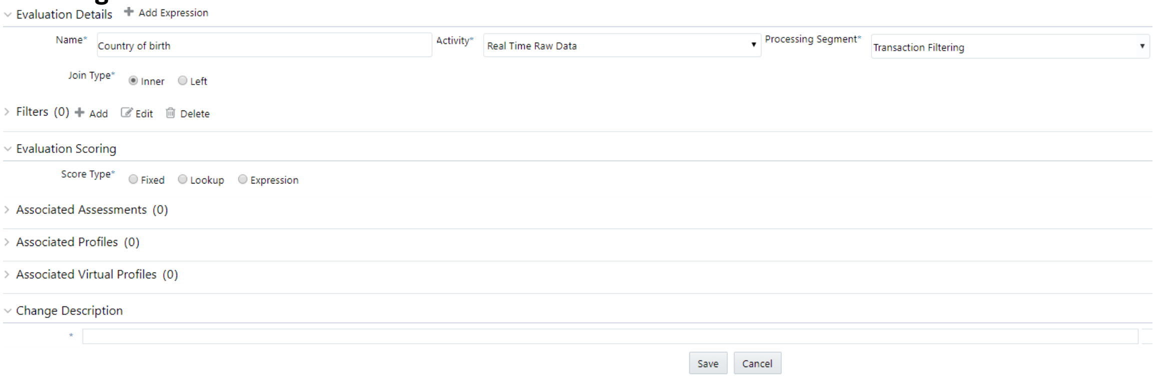
Status:

Evaluations (9)

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 109: Evaluations Attributes



Name*: Country of birth

Activity*: Real Time Raw Data

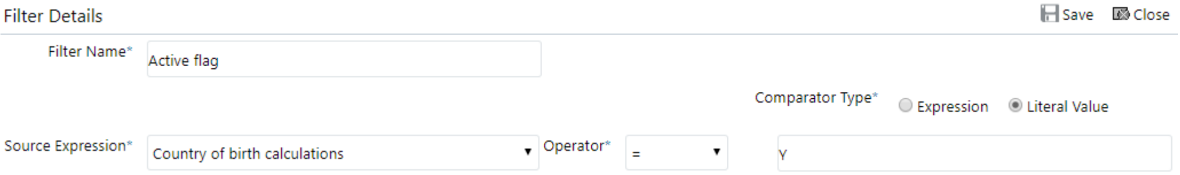
Processing Segment*: Transaction Filtering

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 110: Evaluations Filters



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.

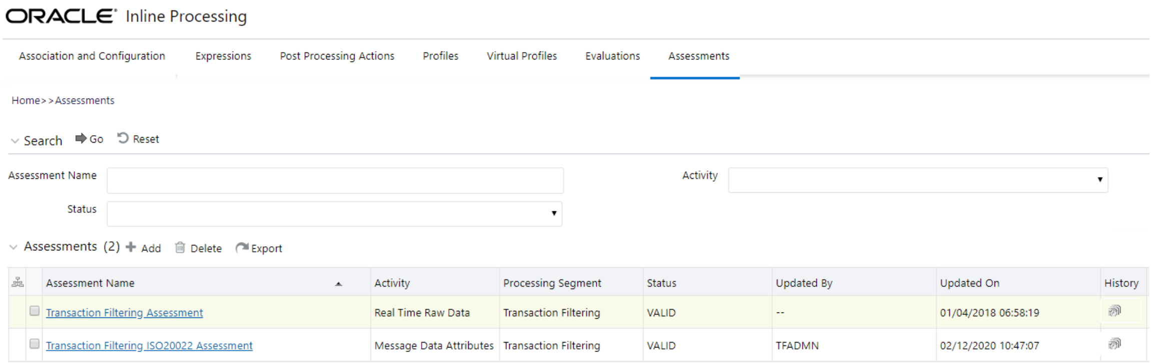
The risk score is calculated at the assessment level is as follows:

- 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 111: Assessments Page

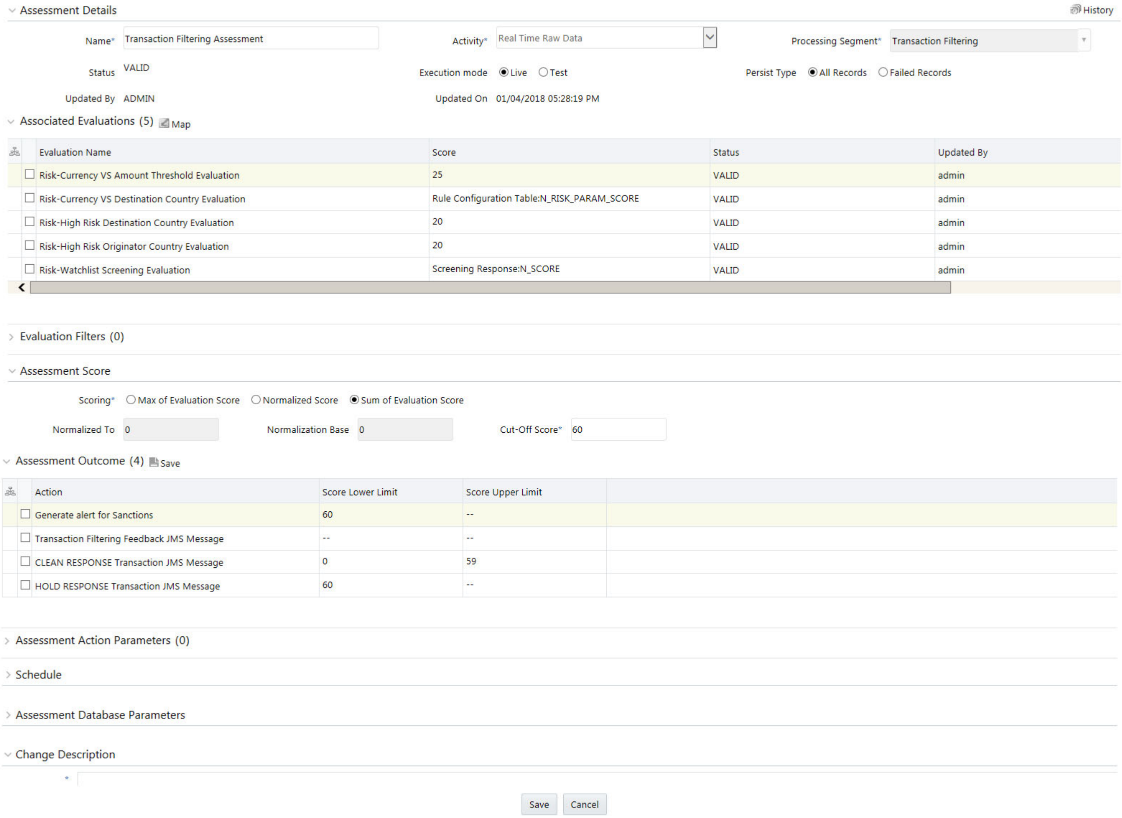


Assessments (2)

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 112: 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

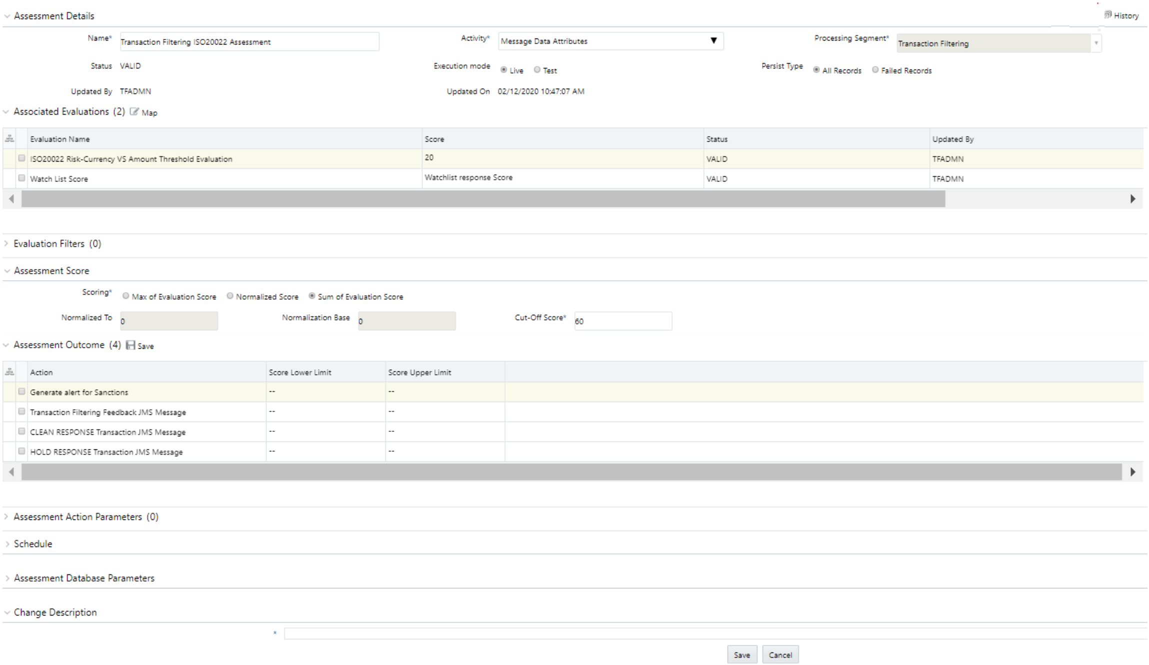
Assessment Database Parameters

Change Description

*

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

Figure 113: 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) Map

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) Save

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 Appendix A: Watch Lists

Monitoring transactions against watch lists of sanctioned individuals and companies, internal watch lists, and other commercial lists of high-risk individuals and organizations is a key compliance requirement for financial institutions worldwide. These watch lists help financial institutions identify customers who are sanctioned, live in sanctioned countries and any inbound or outbound transactions associated with these customers.

L.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

L.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

L.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.

L.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.

L.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.

L.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.

L.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.

L.8 Accuity Watch List

The Accuity Global watch list is a subscription-based service. The Accuity website states:

Accuity's proprietary collection of watch list screening databases is an aggregation of specially designated individuals and entities compiled from dozens of regulatory and enhanced due diligence lists from around the world. The global watch list provides the ideal framework for your Transaction Filtering and interdiction filtering processes.

Accuity provides its aggregated data as a set of three lists as follows:

- The Regulatory Due Diligence (RDD) lists which cover sanctioned entities and individuals. The Accuity Group File can also be used in conjunction with this list.

- Enhanced Due Diligence (EDD) lists which cover entities and individuals who are not part of the regulatory sanctions lists, but whose activities may need to be monitored
- The Politically Exposed Persons (PEPs) Due Diligence Database, and covering PEPs

Any or all the lists can be downloaded and used separately or in conjunction with each other. For more information, see the Accuity website.

L.8.1 Using the Accuity Group File

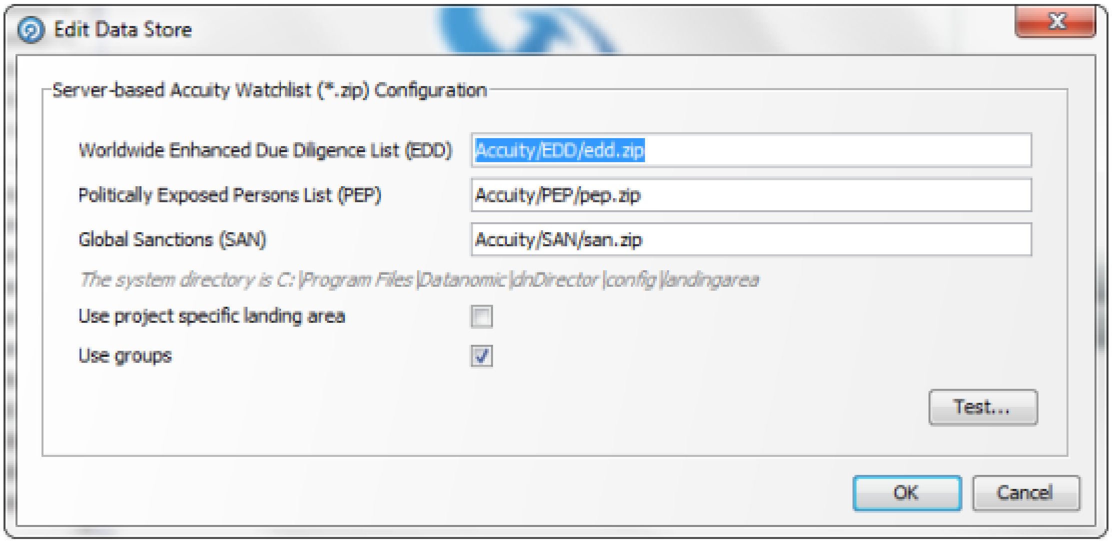
The Accuity global Watchlist is created by aggregating multiple watch lists. As such, any given individual or entity may be represented in the watch list by multiple entries using the `GROUP.XML` file.

In the `GROUP.XML` file, all records which represent the same individual or entity are collected into groups, and each group is assigned a unique group ID. The group ID has a unique identifier to differentiate it from the original record identifier in Enterprise Case Management (ECM). Records that are not included in the group use their original Accuity record ID with a different identifier to indicate that they are single records.

> **NOTE** Only entities and individuals on the Regulatory Due Diligence (RDD) watch lists are included in the group file.

The group file allows you to generate cases on individuals who are grouped together, instead of generating cases on separate individuals. Groups are used by default. To change this, open **Accuity Data Store** in the **Watch List Management** project and deselect the **Use groups** option.

Figure 114: Edit Data Store Window



Edit Data Store

Server-based Accuity Watchlist (*.zip) Configuration

Worldwide Enhanced Due Diligence List (EDD): Accuity/EDD/edd.zip

Politically Exposed Persons List (PEP): Accuity/PEP/pep.zip

Global Sanctions (SAN): Accuity/SAN/san.zip

The system directory is C:\Program Files\Datanomic\dnDirector\config\landingarea

Use project specific landing area ☐

Use groups ☑

If you choose to use the group file but it is not present in your downloaded data, an error is generated.

L.8.2 New Alerts Resulting from Use of the Group File

Using the group file causes the original list ID for an entry to be replaced with the appropriate group ID. The list ID is used in the alert key, so changes to the list ID will result in new alerts being raised for existing, known relationships. There are two main scenarios in which this may occur:

Individuals or entities are moved into, out of, or between groups by Accuity, new alerts are generated for existing relationships.

> **NOTE** Use of the group file may result in new alerts being raised for existing relationships if the group file structure is changed by Accuity. There is at present no way to circumvent this issue.

The Use Groups setting is changed after cases and alerts have already been generated. The setting for the Use Groups option must be selected during the implementation phase of the project. After screening has started, it must not be changed unless necessary. Changing this setting is likely to result in duplication of existing alerts with a new alert ID.

L.9 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.

L.9.1 Individual Private Watch List Input Attributes

This section lists the PLI fields used for individuals. In addition to the prescribed fields, fifty customizable input attributes are available for individual private watch lists, out of which forty are string attributes, five are date attributes and five are number attributes. They are available for any additional inputs required by your private watch list.

The following table lists the individual PLI fields in order, the data format expected for each field, and notes on their use in screening:

Figure 115: Individual Private Watch List Input Attributes

Field Name	Expected Data Format	Notes
ListSubKey	String	This field is used to identify the source list of the watch list record (for example, Private List, Accounting Private List, Financial Private List, and so on). It is included in the alert key.
ListRecordType	String	NA
ListRecordOrigin	String	This field is used to record the provenance of a record when it is part of a consolidated list.
ListRecordId	String	[Mandatory attribute] This attribute is not used as part of the matching process, but it must be populated with a unique identifier.
PassportNumber	String	This is an optional field that may be used to capture the passport numbers of customers or individuals for use in the review process. Passport numbers are not used in the default screening rules.
NationalId	String	This is an optional field that may be used to capture customer National IDs for use in the review process. The National IDs of customers and individuals must not use in the default screening rules.
Title	String	This field must contain the titles of customers or individuals (such as Mr/Mrs/Dr/Herr/Monsieur). It is used to derive gender values where gender is not already stated and is used during the review process. Avoid putting titles in the name fields.
FullName	String	[Mandatory attribute] The individual matching process is based primarily on the name supplied for the individual. Either a full name, a pair of given and family names, or an original script name must be submitted to the screening process for screening to proceed.
GivenName	String	
FamilyName	String	

Figure 115: Individual Private Watch List Input Attributes

Field Name	Expected Data Format	Notes
NameType	String	This is an optional field used in the review process only. Multiple names may exist for the same person. The Name Type, therefore, denotes if the name is the primary name of the listed party, or an additional name (such as an Alias, or Alternate Spelling). If two Private list records were derived from a single source with multiple names (such as Mrs. Louise Wilson née Hammond being split into two records, Louise Wilson and Louise Hammond) you may wish to denote one as the primary name and one as a maiden or alias name.
NameQuality	String	This field may be assigned a value of Low, Medium, or High to indicate the quality of the individual name. High is used for Primary names and specified good/high-quality aliases.
PrimaryName	String	For alias records, this field indicates the main name for that record.
OriginalScriptName	String	[Mandatory attribute] The individual matching process is based primarily on the name supplied for the individual. Either a full name, a pair of given and family names, or an original script name must be submitted to the screening process for screening to proceed. If you populate the Original Script Name, then you will also need to enable two facets of Match processor configuration that are disabled by default: the Original Script Name Cluster and some or all of the Match Rules that include Original script name in their name. To adapt the Match Processor configuration, you will need to open the Transaction screening project within the Director user interface and make the changes to every process used during the Transaction Filtering installation.
Gender	String	The value supplied must be either ‘M’ or ‘F’. The gender is not used directly in the matching process, but optionally, the value of the Gender field can be used by the elimination rules to eliminate poor matches.
Occupation	String	This is an optional field that may be used to eliminate records with "safe" occupations, in the review process and risk scoring. Note that customer occupations are not matched against list occupations using the default screening rules.

Figure 115: Individual Private Watch List Input Attributes

Field Name	Expected Data Format	Notes
DateofBirth	String, representing a date, in the format 'YYYYMMDD'; day, month, and year are required.	[Recommended attribute] Birth date information can be used in matching to identify particularly strong matches or to eliminate matches that are too weak.
YearofBirth	String, in the format 'YYYY'.	NA
Deceased Flag	String	If populated, this optional field must contain either **Y** or **N**.
DeceasedDate	String, representing a date, in the format 'YYYYMMDD'.	If populated, this optional field must contain either the current date or a date in the past.
Address1	String	These are optional fields that may be used in the review process.
Address2	String	
Address3	String	
Address4	String	
City	String	[Recommended attribute] City data is used to strengthen potential match information.
State	String	
Postal Code	String	
AddressCountryCode	String; ISO 2-character country code.	[Recommended attribute] Address country data is used to strengthen potential match information.
ResidencyCountryCode	String; ISO 2-character country code.	[Recommended attribute] The country of residence can be used in optional country prohibition screening.
CountryOfBirthCode	String; ISO 2-character country code.	NA
NationalityCountryCodes	String; comma separated list of ISO 2-character country codes.	[Recommended attribute] The nationality can be used in optional country prohibition screening.
ProfileHyperlink	String; a hyperlink to an Internet or intranet resource for the record.	This field may contain a hyperlink to an Internet or intranet resource that can provide reviewers with additional information about the individual.
RiskScore	Number, between 0 and 100	This field is included where the risk score for a customer is calculated externally.
RiskScorePEP	Number, between 0 and 100	A number indicating the relative 'riskiness' of the Individual, considered as a PEP. The risk score is expressed as an integer between 1 and 100, with Higher numbers indicating a higher risk.

Figure 115: Individual Private Watch List Input Attributes

Field Name	Expected Data Format	Notes
AddedDate	String, representing a date, in the format 'YYYYMMDD'	These are optional fields for use in the review process.
LastUpdatedDate	String, representing a date, in the format 'YYYYMMDD'	
DataConfidenceScore	Number, between 0 and 100	
DataConfidenceComment	String	
InactiveFlag	String	If populated, this optional field must contain either **Y** or **N.**
InactiveSinceDate	String, representing a date, in the format 'YYYYMMDD'	If populated, this optional field must contain either the current date or a date in the past.
PEPclassification	String	This field can be used to indicate the type of PEP (for example, whether the individual is part of an international organization or government, and at what level). It can be used to filter watch list records and is primarily used by the World-Check watch list, but could be used by a private watch list if required.
customString1 to customString40	String	Fifty custom fields are provided in the private list data interface for individuals. Forty of these are intended to hold string data, five hold dates, and five numeric data. The interface file is a comma-separated value (`.csv`) file, and so all fields intrinsically contain strings. However, during the processing of Private watch lists, the custom date and number fields are checked to ensure that they include appropriate data, and warning messages are provided as output if they do not.
customDate1 to customDate5		
customNumber1 to customNumber5		

L.9.2 Entity Private Watch List Input (PLI) Attributes

This section lists the PLI fields used for entities. In addition to the prescribed fields, fifty customizable input attributes are available for individual private watch lists, out of which forty are string attributes, five are date attributes and five are number attributes. They are available for any additional inputs required by your private watch list.

The following table lists the individual PLI fields in order, the data format expected for each field, and notes on their use in screening:

Table 44: Entity Private Watch List Input Attributes

Field Name	Expected Data Format	Notes
ListSubKey	String	This field is used to identify the source list of the watch list record (for example, Private List, Accounting Private List, Financial Private List, and so on). It is included in the alert key.
ListRecordType	String	[Mandatory attribute]This field is used when filtering alerts, to determine whether the record is a sanctions or PEP record. It must contain a value of SAN, PEP, or a combination of these values. If you want to include a combination of values, the values must be comma-separated and enclosed by double quotation marks. For example: "SAN, PEP".
ListRecordOrigin	String	This field is used to record the provenance of a record when it is part of a consolidated list.
ListRecordId	String	[Mandatory attribute] This attribute is not used as part of the matching process, but it must be populated with a unique identifier.
RegistrationNumber	String	This is an optional field that may be used to capture entity registration numbers for use in the review process. Note that entity registration numbers are not used for matching in the default screening rules.
EntityName	String	[Mandatory attribute] The entity matching process is based primarily on the name supplied for the entity. An entity name or original script name must be submitted to the screening process for screening to proceed.
NameType	String	This is an optional field used in the review process only. Multiple names may exist for the same person. The Name Type, therefore, denotes if the name is the primary name of the listed party, or an additional name (such as an Alias, or Alternate Spelling). If two private list records were derived from a single source with multiple names (such as Mrs. Louise Wilson née Hammond being split into two records, Louise Wilson and Louise Hammond) you may wish to denote one as the primary name and one as a maiden or alias name.

Table 44: Entity Private Watch List Input Attributes

Field Name	Expected Data Format	Notes
NameQuality	String	This field may be assigned a value of Low, Medium, or High to indicate the quality of the individual name. High is used for Primary names and specified good or high-quality aliases.
PrimaryName	String	For alias records, this field indicates the main name for that record.
OriginalScriptName	String	[Mandatory attribute] The individual matching process is based primarily on the name supplied for the individual. Either a full name, a pair of given and family names, or an original script name must be submitted to the screening process for screening to proceed. If you populate the Original Script Name, then you will also need to enable two facets of Match processor configuration that are disabled by default. The Original Script Name Cluster and some or all the Match Rules that include Original script name in their name. To adapt the Match Processor configuration, you will need to open the Transaction screening project within the Director user interface and make the changes to every process used during the Transaction Filtering installation.
AliasIsAcronym	String	If this field is set to **Y**, this flags an alias as an acronym as opposed to a full entity name. Leaving the field blank or setting it to any other value does not affect screening (that is, an alias is a full entity name). This flag is used during matching.
VesselIndicator	String	This field must be set to Y if the entity is a vessel (a ship). It must be left empty or set to **N** if the entity is not a vessel.
VesselInfo	String	If the entity is a vessel, you can populate this field with information about it: for example, its call sign, type, tonnage, owner, flag, and so on.
Address1	String	These are optional fields that may be used in the review process.
Address2	String	
Address3	String	
Address4	String	
City	String	[Recommended attribute] City data is used to strengthen potential match information.
State	String	
Postal Code	String	

Table 44: Entity Private Watch List Input Attributes

Field Name	Expected Data Format	Notes
AddressCountryCode	String; ISO 2-character country code.	[Recommended attribute] Address country data is used to strengthen potential match information.
ResidencyCountryCode	String; ISO 2-character country code.	[Recommended attribute] The entity's registration country can be used in optional country prohibition screening.
OperatingCountryCodes	String; ISO 2-character country code.	[Recommended attribute] Any of the entity's operating countries can be used in optional country prohibition screening.
ProfileHyperlink	String; a hyperlink to an Internet or intranet resource for the record.	This field may contain a hyperlink to an Internet or intranet resource that can provide reviewers with additional information about the individual.
RiskScore	Number, between 0 and 100	This field is included where the risk score for a customer is calculated externally.
RiskScorePEP	Number, between 0 and 100	A number indicating the relative ‘riskiness’ of the individual, considered as a PEP. The risk score is expressed as an integer between 1 and 100, with higher numbers indicating a higher risk.
AddedDate	String, representing a date, in the format 'YYYYMMDD'	These are optional fields for use in the review process.
LastUpdatedDate	String, representing a date, in the format 'YYYYMMDD'	
DataConfidenceScore	Number, between 0 and 100	
DataConfidenceComment	String	
InactiveFlag	String	If populated, this optional field must contain either **Y** or **N**.
InactiveSinceDate	String, representing a date, in the format 'YYYYMMDD'	If populated, this optional field must contain either the current date or a date in the past.
PEPclassification	String	This field can be used to indicate the type of PEP (for example, whether the individual is part of an international organization or government, and at what level). It can be used to filter watch list records and is primarily used by the World-Check watch list, but could be used by a private watch list if required.

Table 44: Entity Private Watch List Input Attributes

Field Name	Expected Data Format	Notes
customString1 to customString40	String	Fifty custom fields are provided in the private list data interface for individuals. Forty of these are intended to hold string data, five hold dates, and five numeric data. The interface file is a comma-separated value (`.csv`) file, and so all fields intrinsically contain strings. However, during the processing of Private watch lists, the custom date and number fields are checked to ensure that they include appropriate data, and warning messages are provided as output if they do not.
customDate1 to customDate5	String, representing a date, in the format 'YYYYMMDD'	
customNumber1 to customNumber5	Number	

13 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 45: Activities for System Audit

Activity Identifier	Activity Name	Activity Sequence
1	Raw Message Processing	1
2	Message Parser Processing	2
3	watch list Processing	3
4	Alert Manager Processing	4
5	Hold	5
6	Assigned	6
7	Escalated	7
8	Recommend to Block	8
9	Block	9
10	Recommend to Release	10
11	Release	11
12	Reject	12

B.2 Steps for System Audit Activities

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

Table 46: Steps for System Audit Activities

Step Identifier	Activity Name	Step Name	Step Sequence	Status
1	Raw Message Processing	Record the receipt of the raw message	1	Y
2	Raw Message Processing	Raw Message persisted into structure table	2	N
3	Message Parser Processing	Raw Message parsed	1	N
4	Message Parser Processing	Parsed Raw Message persisted into structure table	2	N
5	watch list Processing	Matching data prepared	1	N
6	watch list Processing	Matching Engine Invoked	2	Y
7	watch list Processing	Scoring Engine Invoked	3	Y
8	watch list Processing	Scoring performed	4	Y

Table 46: Steps for System Audit Activities

Step Identifier	Activity Name	Step Name	Step Sequence	Status
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

14 Appendix C: Process Modeller Framework (PMF) Configurability

This appendix contains information on the steps required to configure the ready-to-use Process Modeller Framework (PMF) workflow. On the **Process Modeller** page, click the transaction that you want to configure and follow the steps in the following sequence. For information on how to access the **Process Modeller** page, see the Process Modeller Menu.

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 available, see the **Components for Designing Your Process Flow** chapter in the Oracle Financial Services Analytical Applications Infrastructure Process Modelling Framework (PMF) Orchestration Guide.
3. Double-click **Human Task** .
4. In the Activity dialog, provide the following information:
   - A unique activity name in the **Activity Name** field. After you provide a name, it appears after the icon on the **PMF** page.
   - The activity description in the **Activity Description** field.
   - The current status of the transaction in the **Status** field.
   - The next status of the transaction in the **Outcomes** field.
5. Click **Transitions** and then click **Add**.
   - In the **Add New Transition** dialog, provide the following information:
   - A unique transition name in the **Transition Name** field.
   - The destination status of the transaction in the **Connected To** field.
   - The execution or decision rule for a status in the **Decision Rule** field. Here you need to map the specific rule to the current status or create the rule according to the business requirement.
   - The order of the transaction in the **Order** field.

   You can also configure the fields in the **Action and Notifications** subtabs. For more information, see the **Action Tab for Creating Tasks/Notification** section in 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.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.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.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.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.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_STATUS_TL` table must be a combination of one of the following values:
>
> - The value provided in `v_sanction_status_name` in `dim_sanctions_status` table and the name of the transaction workflow invoked for entry 1.
> - The value provided in `v_sanction_status_name` in `dim_sanctions_status` table and the name of the transaction workflow completed for entry 2.

C.5 Configurations Required for the setup_rt_params Table

To configure the table in the ATOMIC schema, follow these steps:

1. Provide the function code in the `v_attribute_value1` column where `v_attribute_name1 = 'TF_ FUNCTION_CODES'`.
2. Provide the status codes according to the `v_attribute_name1` value in the `v_attribute_value1` column where `v_attribute_name1 = 'TF_FUNCTION_AND_STATUS_CODES'`.
3. Provide all status codes in the `v_attribute_value1` column against each function code in the `v_attribute_name1` column. This displays the dynamic status filter.
4. Provide the code for each status to be displayed to the user for that function code in the `v_attribute_value1` column.
5. Provide the code for each status to be displayed to the user in the *Transaction Summary* window in the `v_attribute_value2` column.
6. Provide the code for each action that must be displayed to the user for that transaction in the `v_attribute_value3` column.
7. To create an order for the transactions, follow these steps:

- 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.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.<XREF>
2. Provide the activity name as mentioned in step 4 of the Configuring the Human Task in the PMF Page <XREF>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.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.8 Other Configurations

The user group is now created. After it is created, follow these steps:

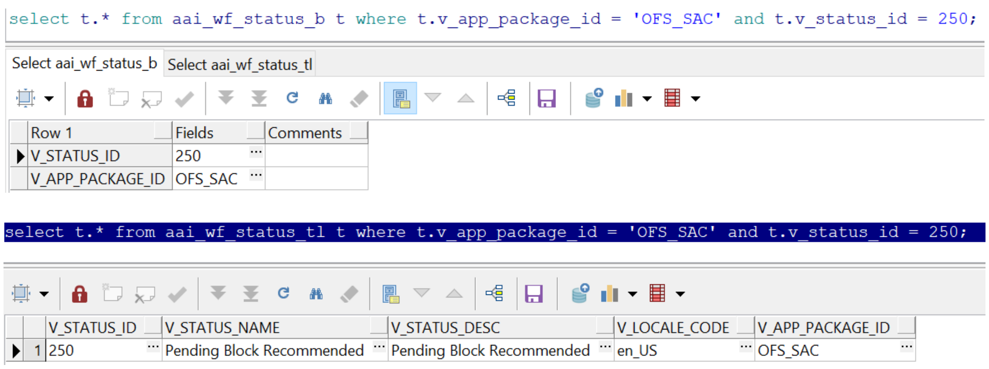
1. Map the group in the `domain_jur_grp_map` table.
2. Login to the Config schema.
3. Run the `select * from cssms_folder_function_map` query.
4. Add the new function to the `Transaction Filter` folder (TransactionFiltering `TFLTADMIN`).
5. Run the `select t.v_access_code,t.v_menu_id from aai_menu_b 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.

15 Appendix 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 116: Example 1



```
select t.* from aai_wf_status_b t where t.v_app_package_id = 'OFS_SAC' and t.v_status_id = 250;
```

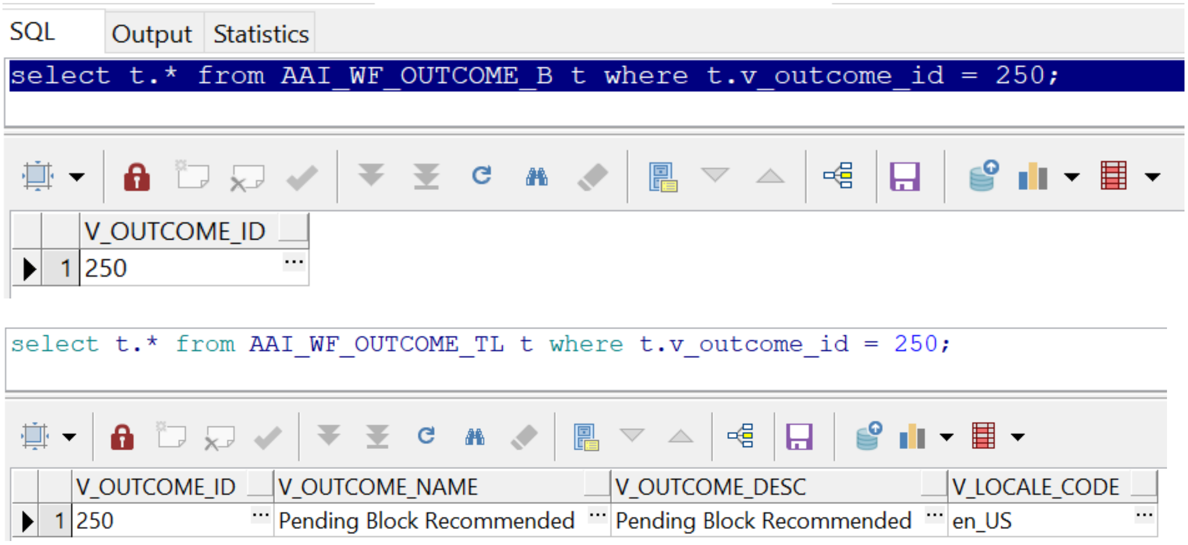
Row 1	Fields	Comments
V_STATUS_ID	250	
V_APP_PACKAGE_ID	OFS_SAC	

```
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_OUTCOME_TL table and provide other columns data.

Figure 117: Example 2



```
select t.* from AAI_WF_OUTCOME_B t where t.v_outcome_id = 250;
```

	V_OUTCOME_ID
1	250

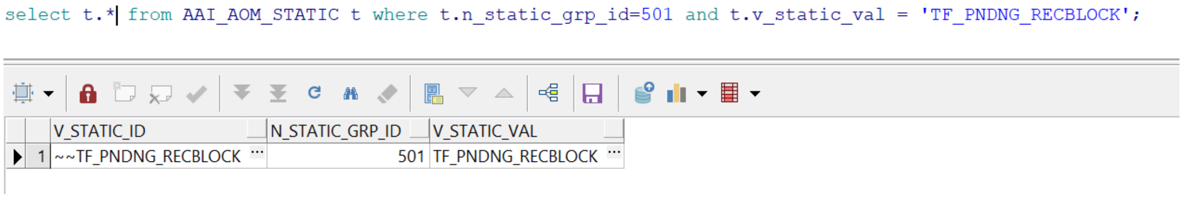
```
select t.* from AAI_WF_OUTCOME_TL t where t.v_outcome_id = 250;
```

	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_ACTION` drop-down list while adding new Application rule.

   ·§Select `* from AAI_AOM_STATIC t where t.n_static_grp_id=501;`

Figure 118: 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*

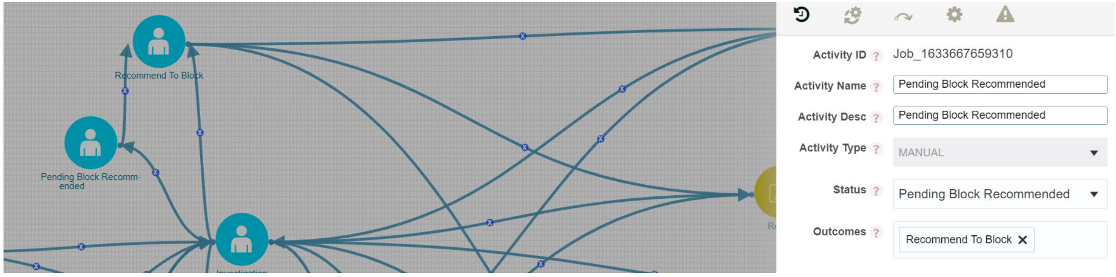
   Activity Description

   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 119: 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.

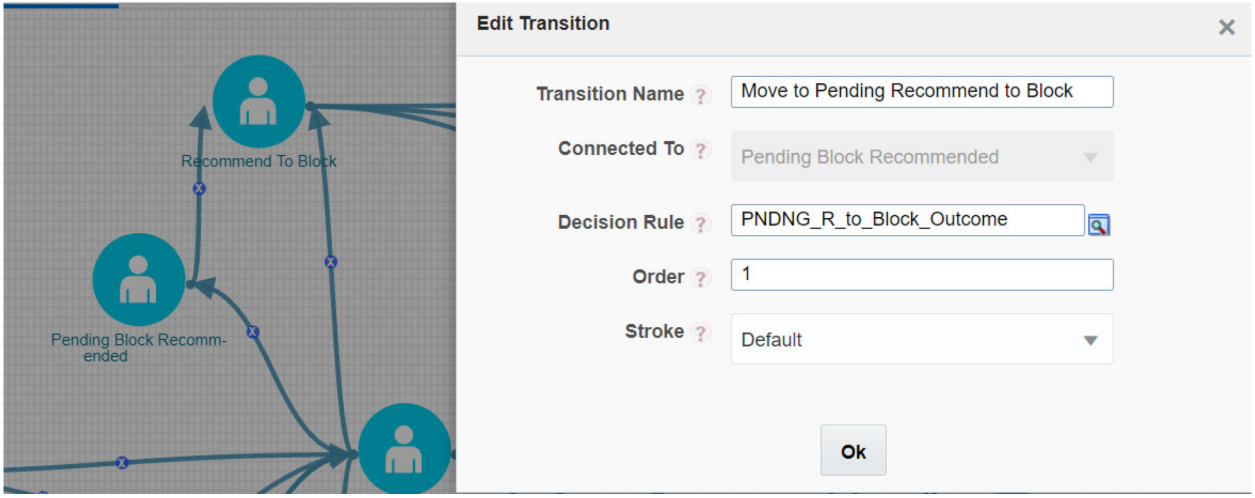
   Decision Rule - Map to decision rule for particular status.

   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 120: Edit Transaction – Pending Block Recommended



Edit Transition

Transition Name: Move to Pending Recommend to Block

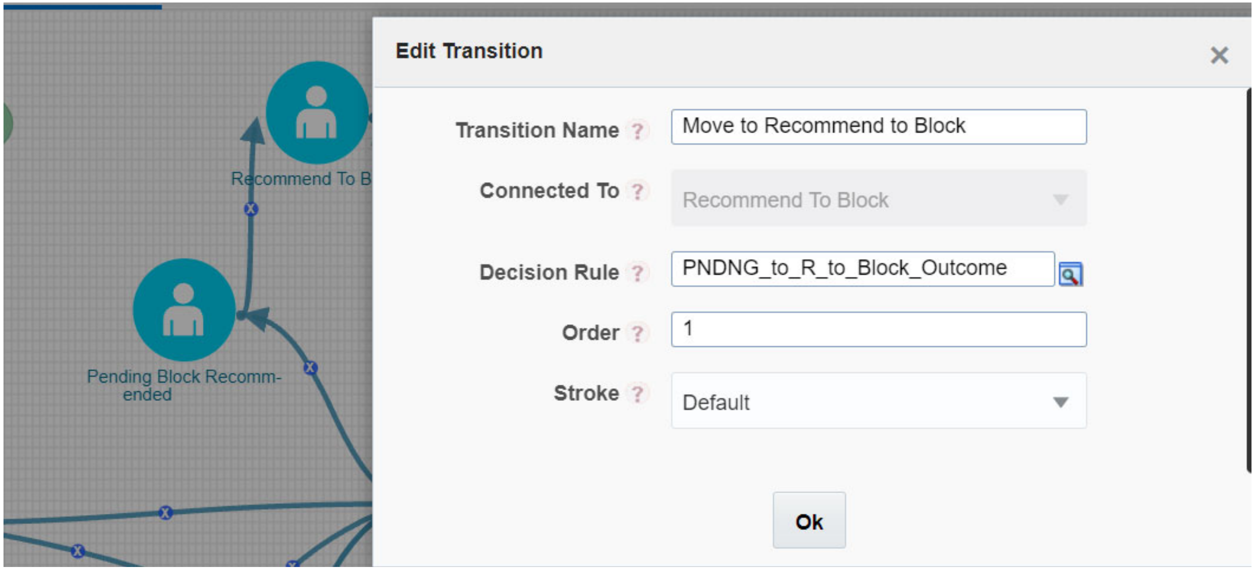
Connected To: Pending Block Recommended

Decision Rule: PNDNG_R_to_Block_Outcome

Order: 1

Stroke: Default

Figure 121: 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

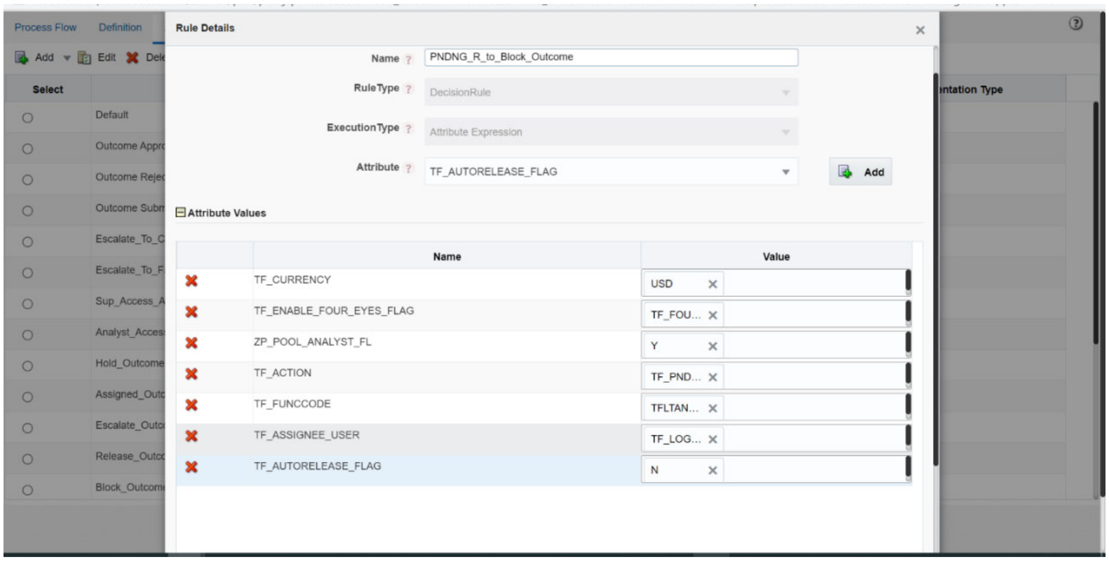
Order: 1

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 122: Rule Details – Decision Rule 1



Name: PNDNG_R_to_Block_Outcome

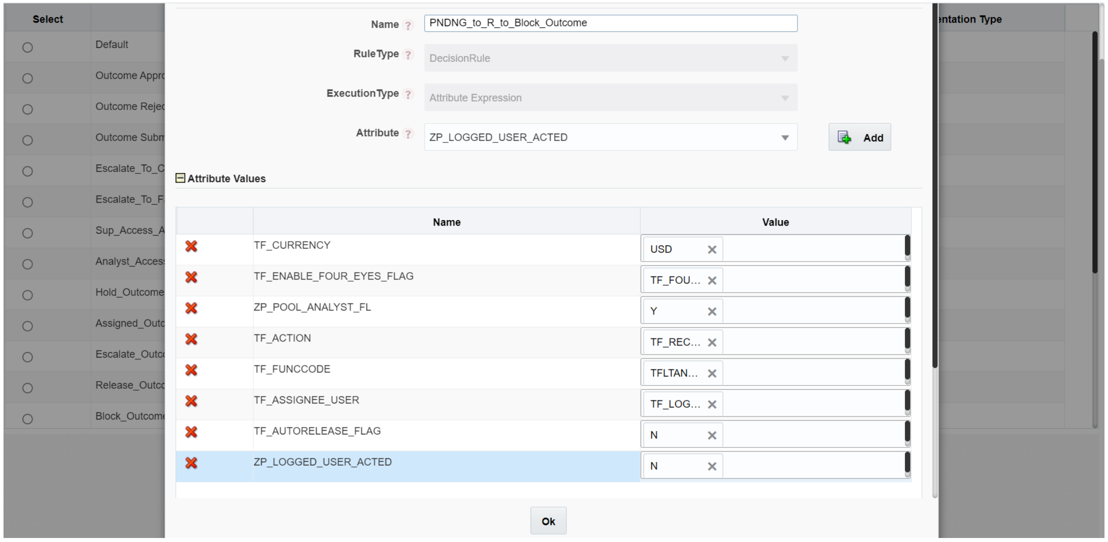
RuleType: DecisionRule

ExecutionType: Attribute Expression

Attribute: TF_AUTORELEASE_FLAG

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 123: Rule Details – Decision Rule 2



Name: PNDNG_to_R_to_Block_Outcome

RuleType: DecisionRule

ExecutionType: Attribute Expression

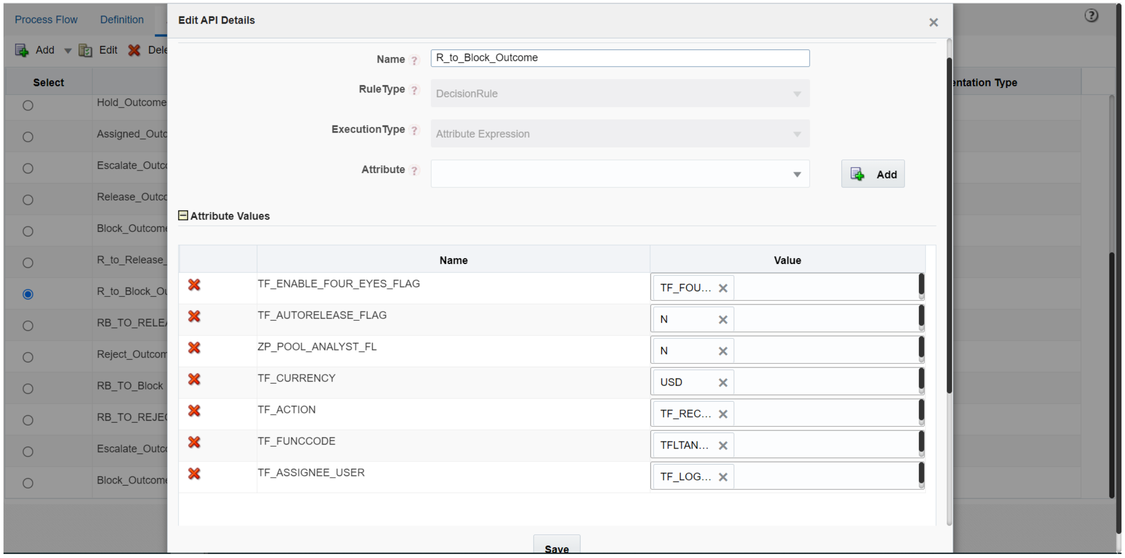
Attribute: ZP_LOGGED_USER_ACTED

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 124: Edit API Details



Edit API Details

Name: R_to_Block_Outcome

RuleType: DecisionRule

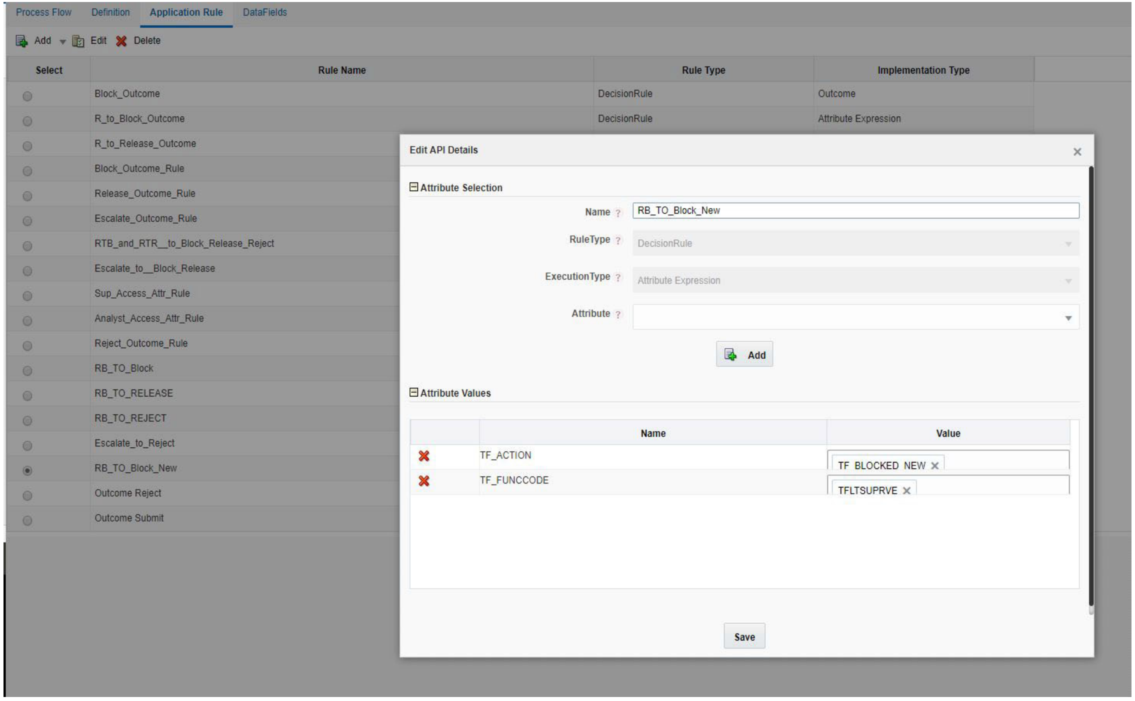
ExecutionType: Attribute Expression

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 125: 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		

Edit API Details

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:
   i. select * `from setup_rt_params where V_PARAM_NAME = 'TF_FUNCTION_AND_STATUS_CODES' and V_ATTRIBUTE_NAME1 = 'TFLTANYSE';`
   ii. Append `V_ATTRIBUTE_VALUE3` with the newly added Pending review Status.

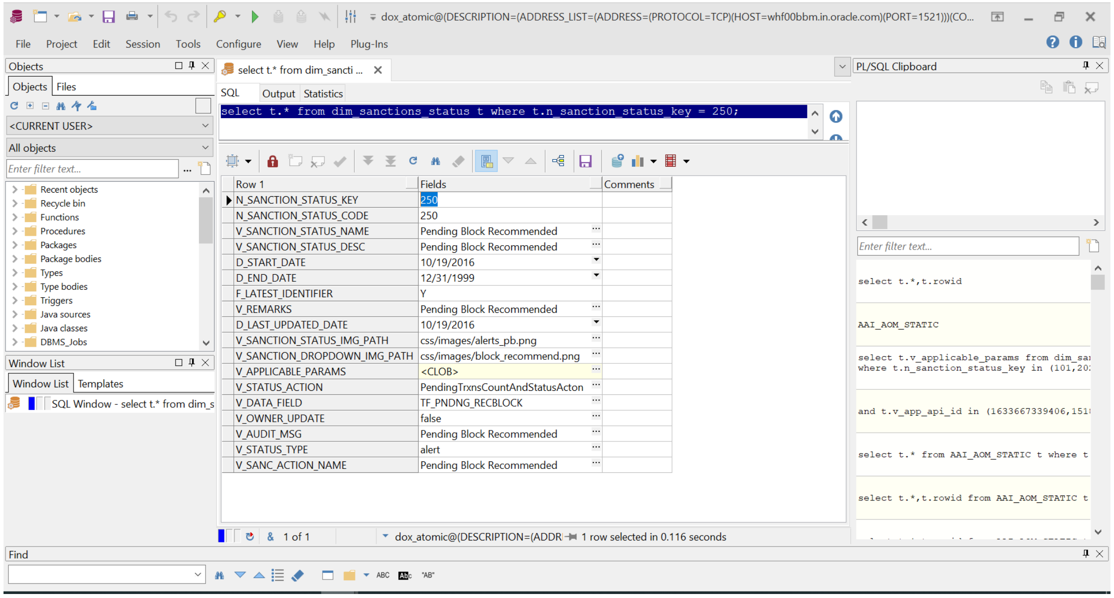
iii. Example: 2,96

> **NOTE**
> - To get the `V_ATTRIBUTE_VALUE3`; refer the `dim_sanctions_status` table.
> - This is the Customized example for Pending Review (96) to be added manually.

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 126: 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

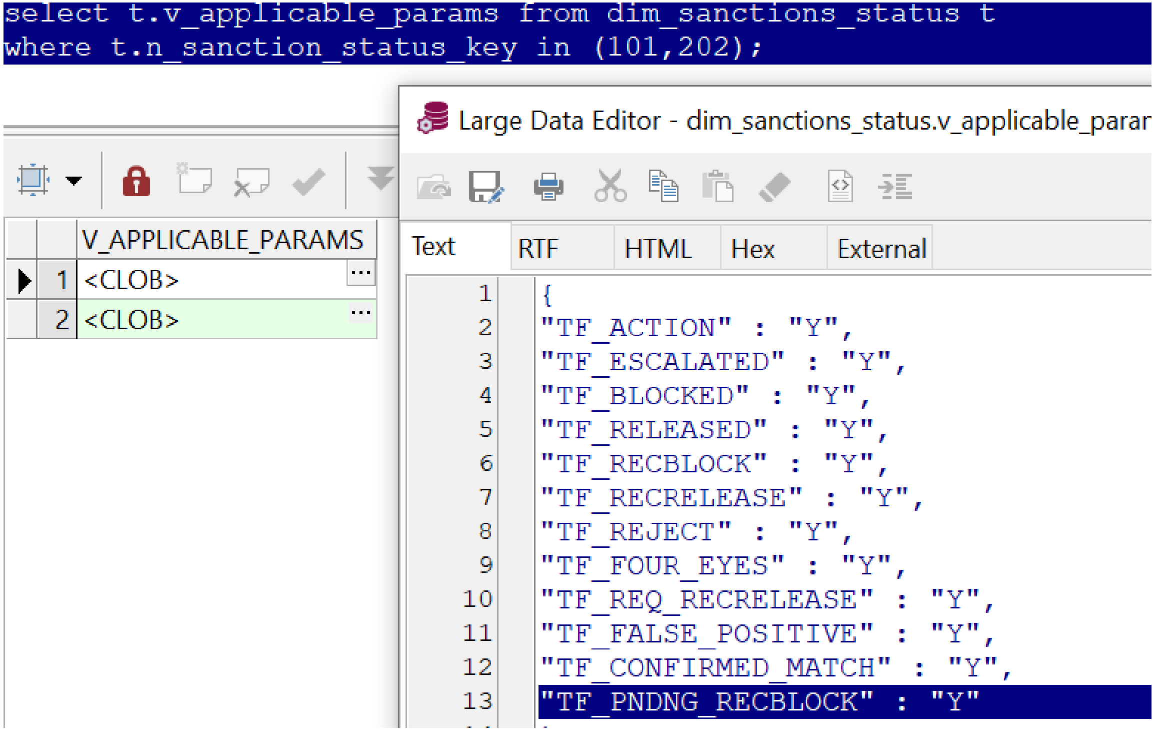
```
select t.*,t.rowid

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 127: Applicable Params



```
select t.v_applicable_params from dim_sanctions_status t
where t.n_sanction_status_key in (101,202);
```

```
{
"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 47: 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 48: `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.

16 Appendix E: Delta Watch List Configurations

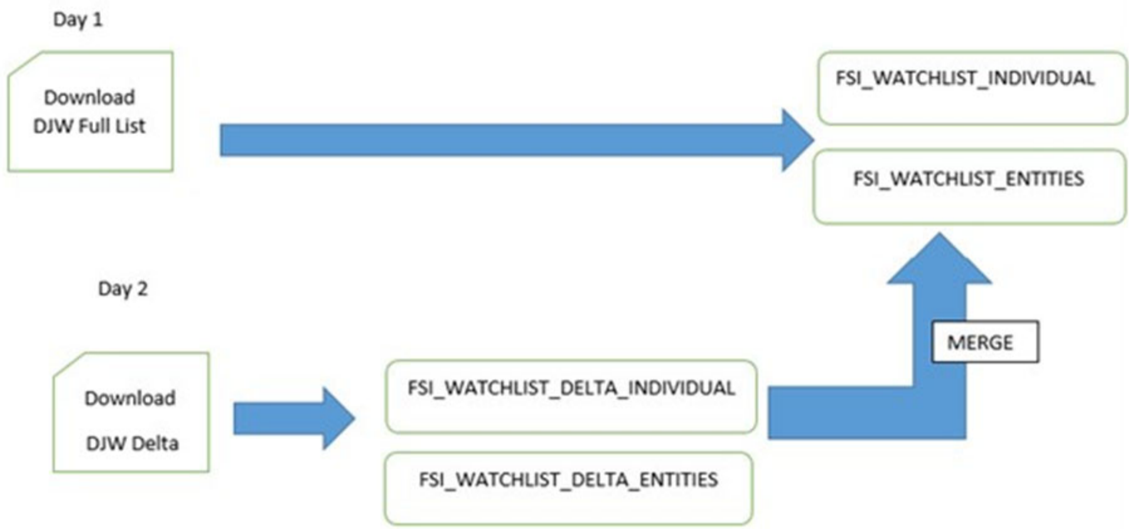
NOTE These configurations are performed when you do not want to download the full watch list, and only want to download the delta watch list. This helps to reduce the download time and is not part of the screening process.

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 128: 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.*.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`.
- Set `phase.*.export.*.ind_table_name` = `FSI_WATCHLIST_DELTA_INDIVIDUAL`.
- Set `phase.*.export.*.entities_table_name` = `FSI_WATCHLIST_DELTA_ENTITIES`.
- `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

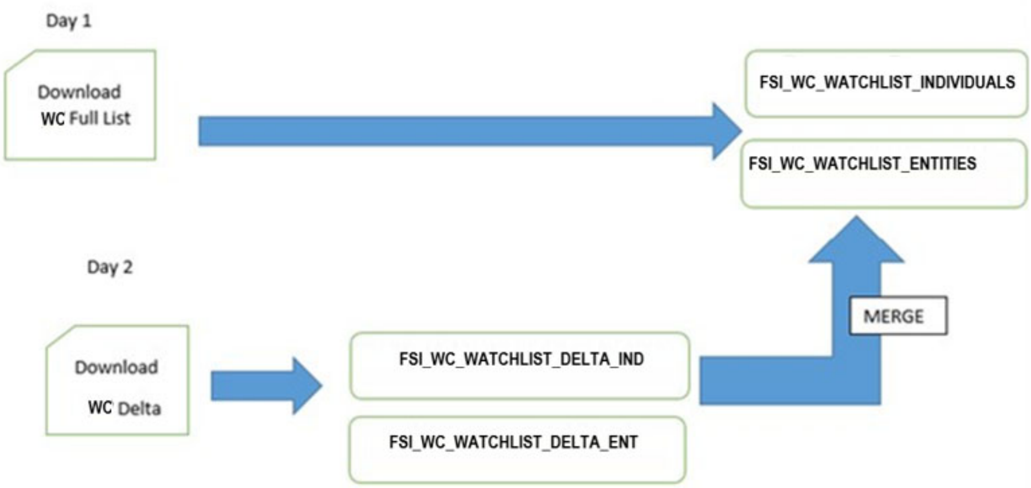
NOTE These configurations are performed when you do not want to download the full watch list, and only want to download the delta watch list. This helps to reduce the download time and is not part of the screening process.

Customer Screening recommends that you always use the full watch list during the screening process. Due to the clustering strategy, which is implemented in the screening process, you must not download the delta watch list. There are certain cases in which you must download the delta watch list files, for example, if the full watch list files are not yet available for download or if you want to save time.

Customers who download the delta watch list files must first download the full watch list files and then download the delta watch list files. The delta watch list is then merged into the full watch list before screening.

The following image shows the information flow for the delta watch list:

Figure 129: Flow for Delta Watch List


Day 1
Download
WC Full List
FSI_WC_WATCHLIST_INDIVIDUALS
FSI_WC_WATCHLIST_ENTITIES
Day 2
MERGE
Download
WC Delta
FSI_WC_WATCHLIST_DELTA_IND
FSI_WC_WATCHLIST_DELTA_ENT

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 properties:`
   - `phase.WC\ -\ Load\ without\ filtering.enabled = N`
   - `phase.WC\ -\ Load\ without\ filtering\ DB.enabled = Y`

   `To run the full watch list with filtering, set the following properties:`
   - `phase.WC\ -\ Load\ with\ filtering\ (Part\ 1).enabled = N`

   - `phase.WC\ -\ Load\ with\ filtering\ (Part\ 1)\ DB.enabled = Y`
   - `phase.WC\ -\ Load\ with\ filtering\ (Part\ 2).enabled = Y`

2. Set the following properties in the `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.`

17 Appendix F: Message Categories and Message Types

A user of the Transaction Filtering application can use the following message categories:

- SWIFT Message Types
- ISO20022 Message Types
- Fedwire Message Types
- US NACHA Message Types

Each message category has different message types defined. The following tables list the message categories and associated message types.

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 49: SWIFT Message Types

1	MT101	**2**	MT103	**3**	MT110	**4**	MT202
5	MT202COV	**6**	MT700	**7**	MT701	**8**	MT707
9	MT103STP	**10**	MT105	**11**	MT111	**12**	MT112
13	MT190	**14**	MT191	**15**	MT192	**16**	MT195
17	MT196	**18**	MT198	**19**	MT199	**20**	MT210
21	MT290	**22**	MT291	**23**	MT292	**24**	MT295
25	MT296	**26**	MT298	**27**	MT299	**28**	MT300
29	MT399	**30**	MT400	**31**	MT410	**32**	MT412
33	MT455	**34**	MT490	**35**	MT491	**36**	MT492
37	MT495	**38**	MT496	**39**	MT498	**40**	MT499
41	MT536	**42**	MT590	**43**	MT591	**44**	MT599
45	MT606	**46**	MT607	**47**	MT671	**48**	MT699
49	MT711	**50**	MT720	**51**	MT721	**52**	MT730
53	MT734	**54**	MT742	**55**	MT747	**56**	MT750
57	MT752	**58**	MT754	**59**	MT756	**60**	MT760
61	MT767	**62**	MT768	**63**	MT769	**64**	MT790
65	MT791	**66**	MT795	**67**	MT796	**68**	MT798
69	MT799	**70**	MT802	**71**	MT895	**72**	MT896

Table 49: SWIFT Message Types

73	MT899	74	MT910	75	MT950	76	MT995
77	MT996	78	MT998	79	MT999	80	MT107
81	MT204	82	MT416	83	MT420	84	MT430
85	MT516	86	MT526	87	MT581	88	MT592
89	MT608	90	MT705	91	MT710	92	MT792
93	MT801	94	MT900	95	MT320	96	MT604
97	MT605	98	MT732	99	MT740	100	MT940
101	MT942	102	MT985	103	MT986	104	MT890
105	MT895	106	MT896	107	MT899	108	MT900
109	MT910	110	MT940	111	MT942	112	MT950
113	MT985	114	MT986	115	MT995	116	MT996
117	MT998	118	MT999	119	MT102	120	MT104
121	MT200	122	MT203	123	MT456	124	MT708
125	MT321	126	MT540	127	MT541	128	MT542
129	MT543	130	MT544	131	MT305	132	MT396
133	MT568	134	MT596	135	MT696	*136*	MT304
137	MT350	138	MT362	139	MT566	140	MT765

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 50: ISO20022 Message Types

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						

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 51: Fedwire Message Types

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 52: US NACHA Message Types

1	IAT	**2**	CTX	**3**	BOC	**4**	RCK
5	POP	**6**	WEB	**7**	CCD	**8**	TEL
9	PPD	**10**	ARC	**11**	CIE		

18 Appendix G: Invoking the PMF Workflow from backend

This appendix describes invoking the Process Modeller Framework (PMF) workflow from the backend for the alert.

Table53 provides the PMF workflow invoking parameters.

Table 53: 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;
```

19 Appendix H: JMS Cluster Environment Creation

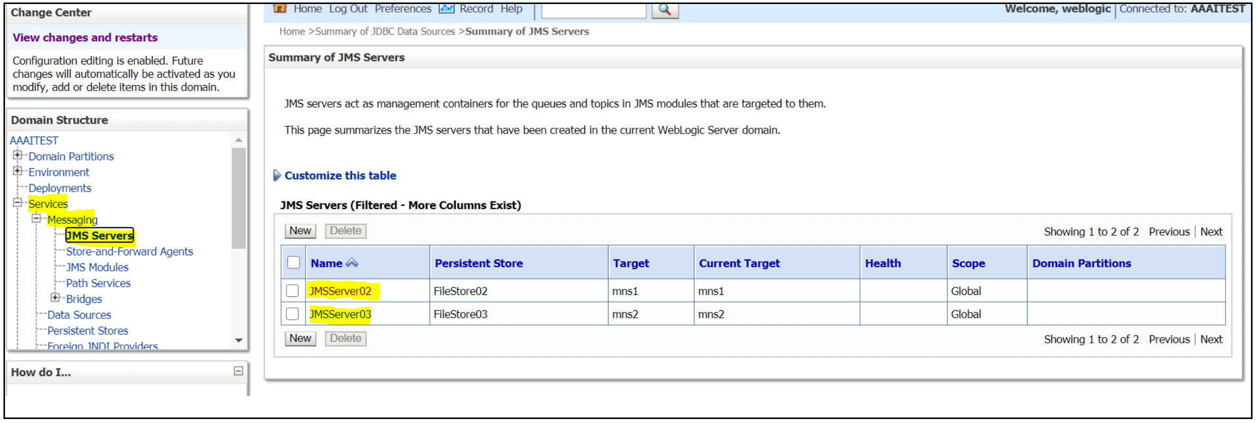
JMS servers act as management containers for the queues and topics in JMS modules that are targeted to them. JMS cluster servers in a domain work together to provide a more scalable and reliable application platform than a single server. A cluster appears to its clients as a single server, but it is a group of servers acting as one.

19.1 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 130: Weblogic Console Page



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...
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITEST
Home >Summary of JDBC Data Sources >Summary of JMS Servers
Summary of JMS Servers
Customize this table
New Delete
Showing 1 to 2 of 2 Previous Next

JMS servers act as management containers for the queues and topics in JMS modules that are targeted to them.

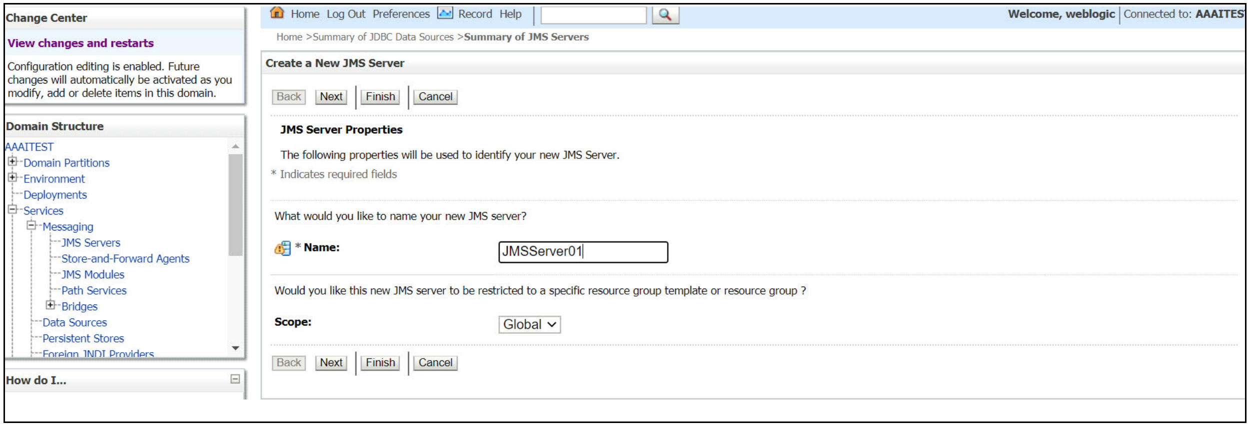
This page summarizes the JMS servers that have been created in the current WebLogic Server domain.

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 131: JMS Server Properties Page



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...
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITES
Home >Summary of JDBC Data Sources >Summary of JMS Servers
Create a New JMS Server
Back Next Finish Cancel

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?

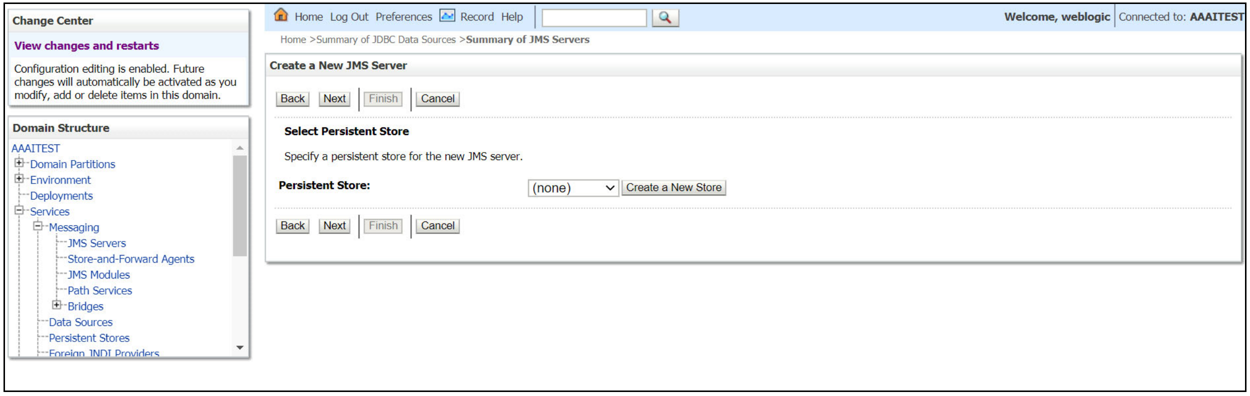
* Name: JMSServer01

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 132: Select Persistent Store 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

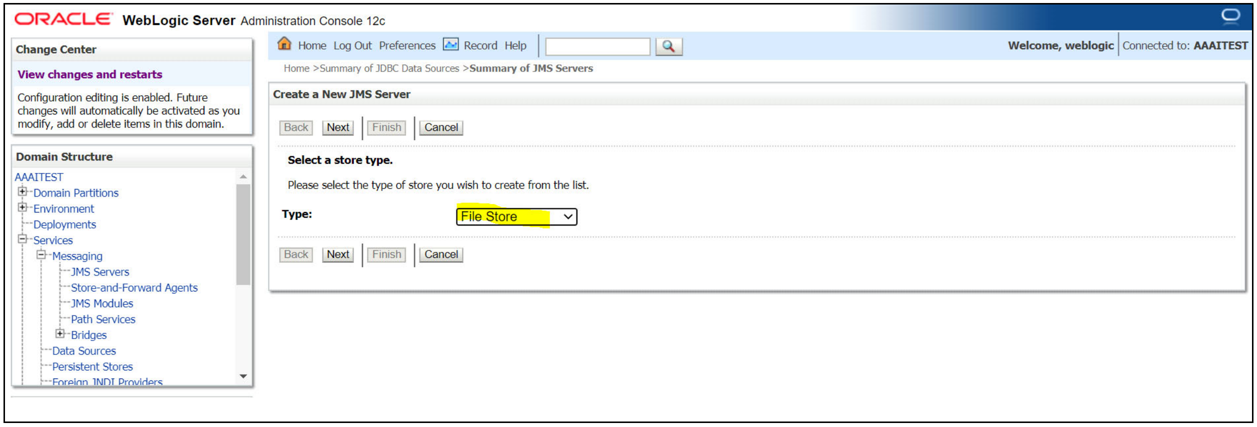
Select Persistent Store

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 133: 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.

Create a New JMS Server

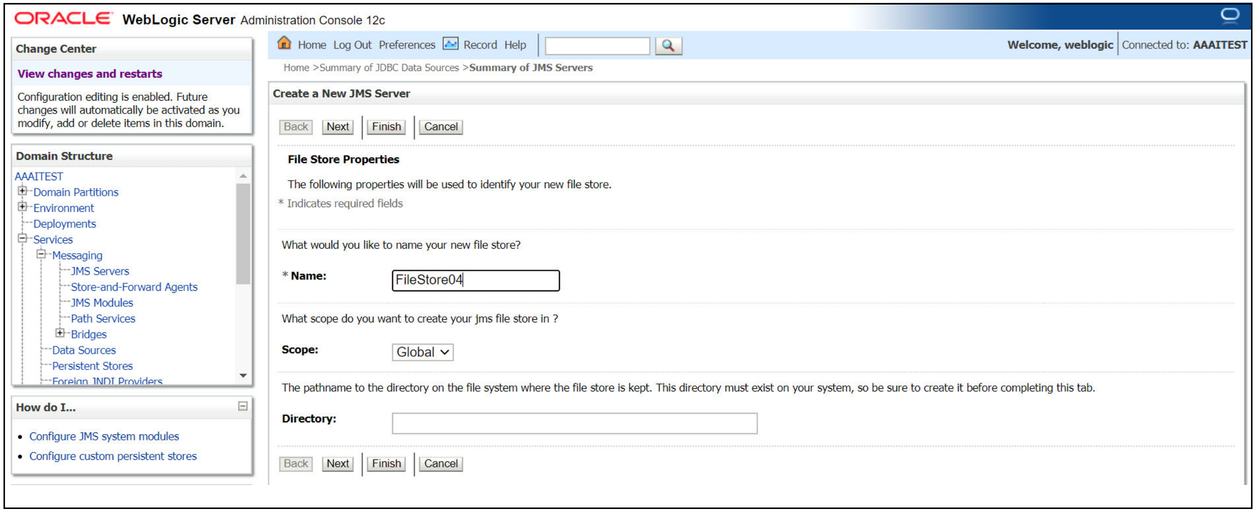
Select a store type.

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 134: File Store Properties page


ORACLE WebLogic Server Administration Console 12c
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 JMS system modules
Configure custom persistent stores
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITEST
Home >Summary of JDBC Data Sources >Summary of JMS 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 Server

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

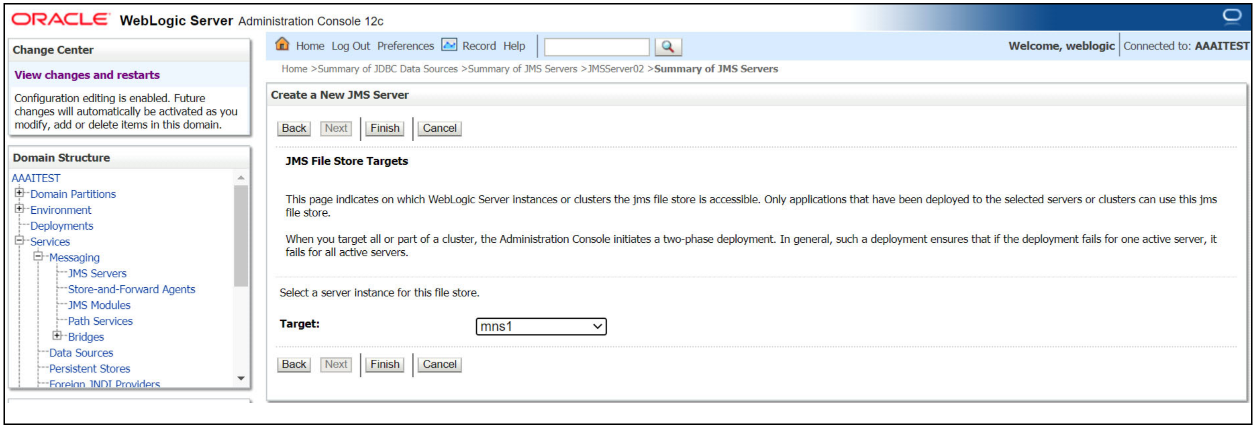
The pathname to the directory on the file system where the file store is kept. This directory must exist on your system, so be sure to create it before completing this tab.

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 135: JMS File Store Targets page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

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.

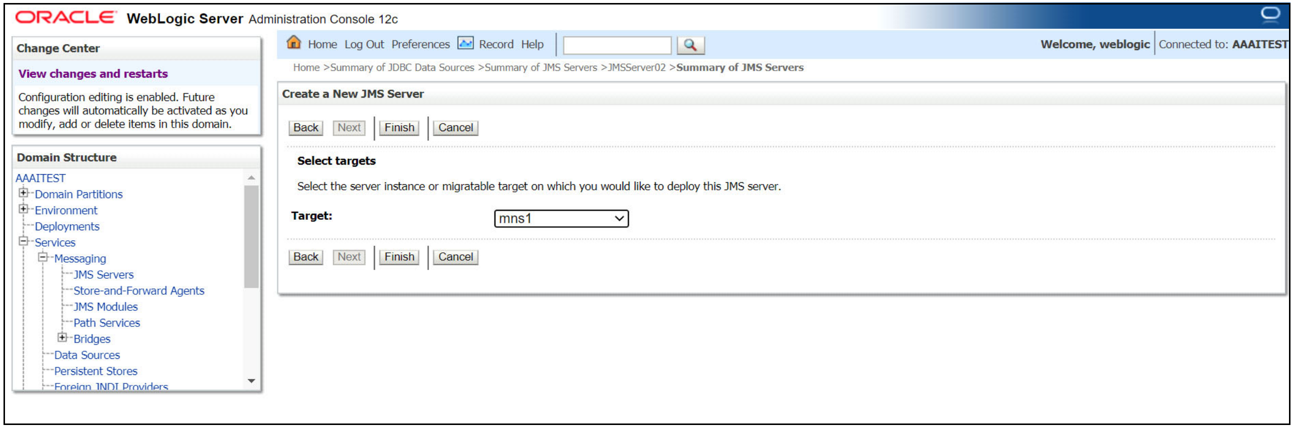
Select a server instance for this file store.

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 136: Select targets page



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Select targets

Select the server instance or migratable target on which you would like to deploy this JMS server.

Target: mns1

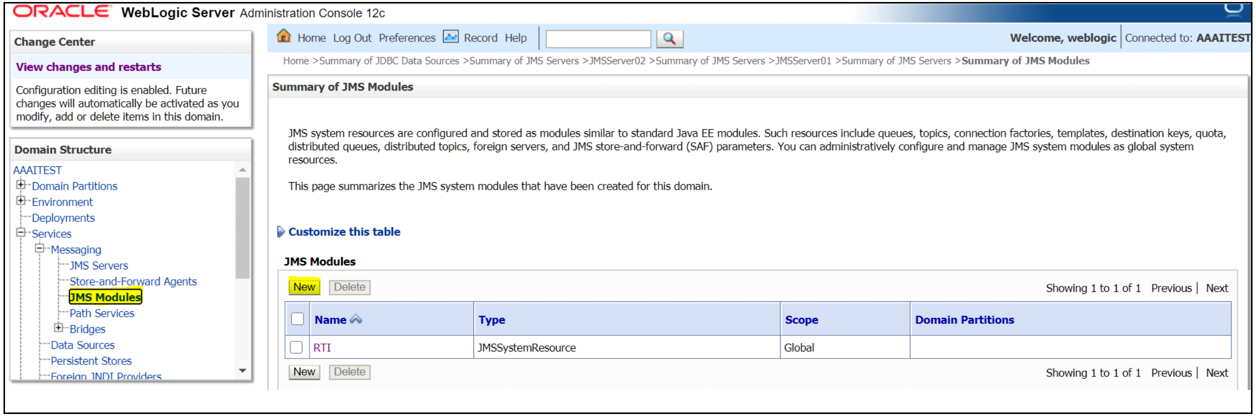
19.2 JMS Module Creation

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 137: Weblogic Console 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 >JMSServer01 >Summary of JMS Servers >Summary of JMS Modules
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
Customize this table
New
Delete
Showing 1 to 1 of 1 Previous | Next

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

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.

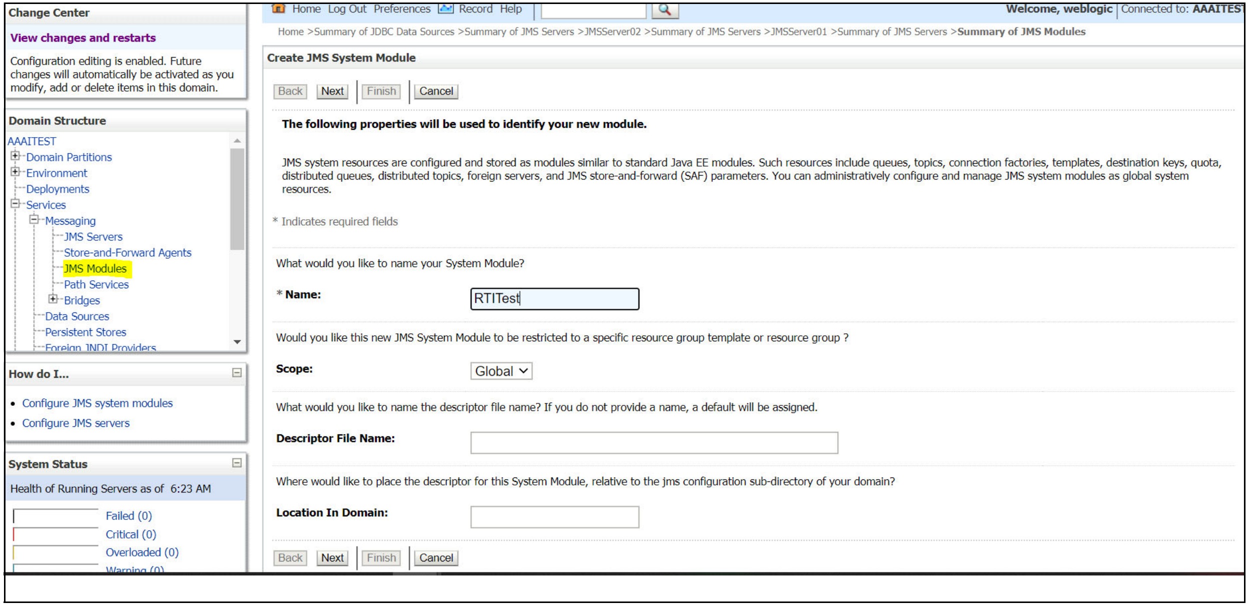
This page summarizes the JMS system modules that have been created for this domain.

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 138: Create JMS System Module Page



Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITES
Home >Summary of JDBC Data Sources >Summary of JMS Servers >JMSServer02 >Summary of JMS Servers >JMSServer01 >Summary of JMS Servers >Summary of JMS Modules
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 JMS system modules
Configure JMS servers
System Status
Back
Next
Finish
Cancel

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

Failed (0)
Critical (0)
Overloaded (0)
Warning (0)

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:

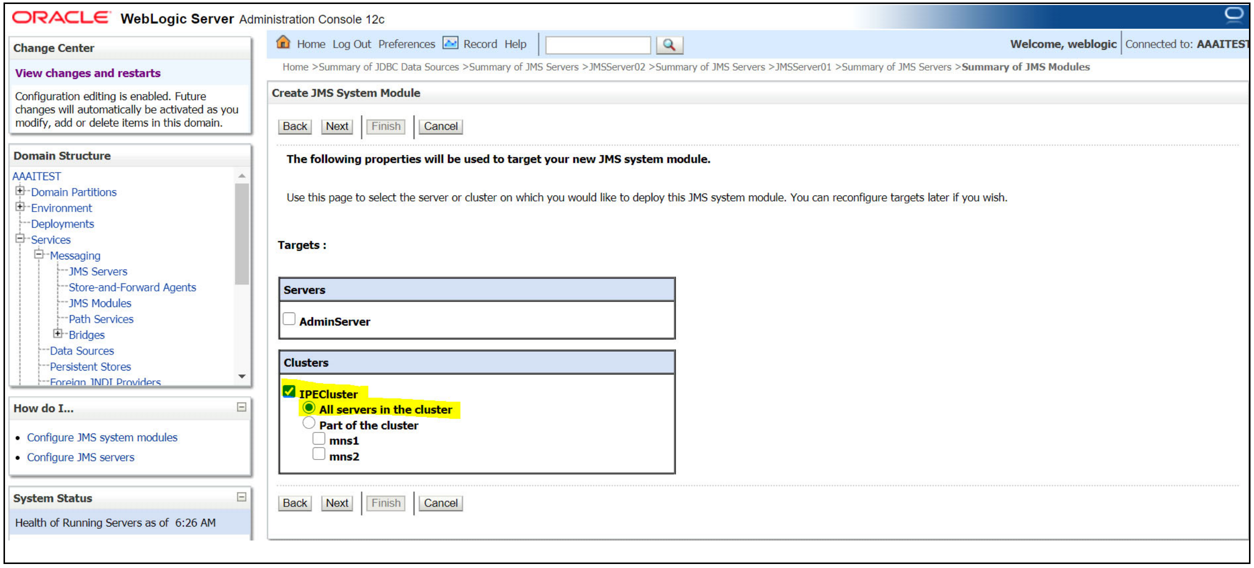
Where would like to place the descriptor for this System Module, relative to the jms configuration sub-directory of your domain?

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 139: Create JMS System Module


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 >JMSServer01 >Summary of JMS Servers >Summary of JMS Modules
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 JMS system modules
Configure JMS servers
System Status
Health of Running Servers as of 6:26 AM
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 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

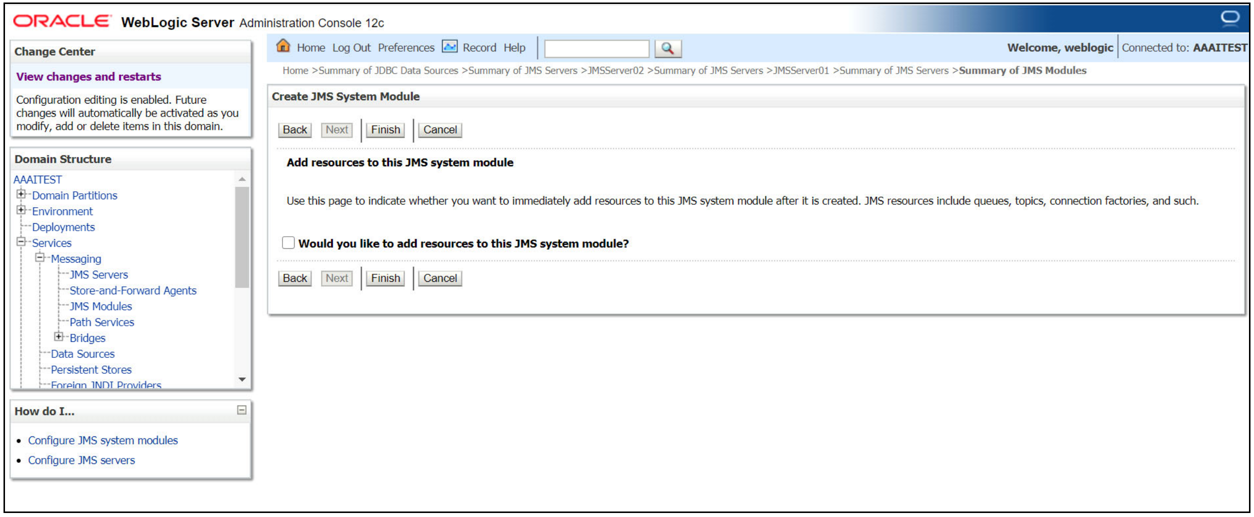
□ mns1

□ 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 140: Create JMS System Module


ORACLE WebLogic Server Administration Console 12c
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 JMS system modules
Configure JMS servers
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 >JMSServer01 >Summary of JMS Servers >Summary of JMS Modules
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 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?

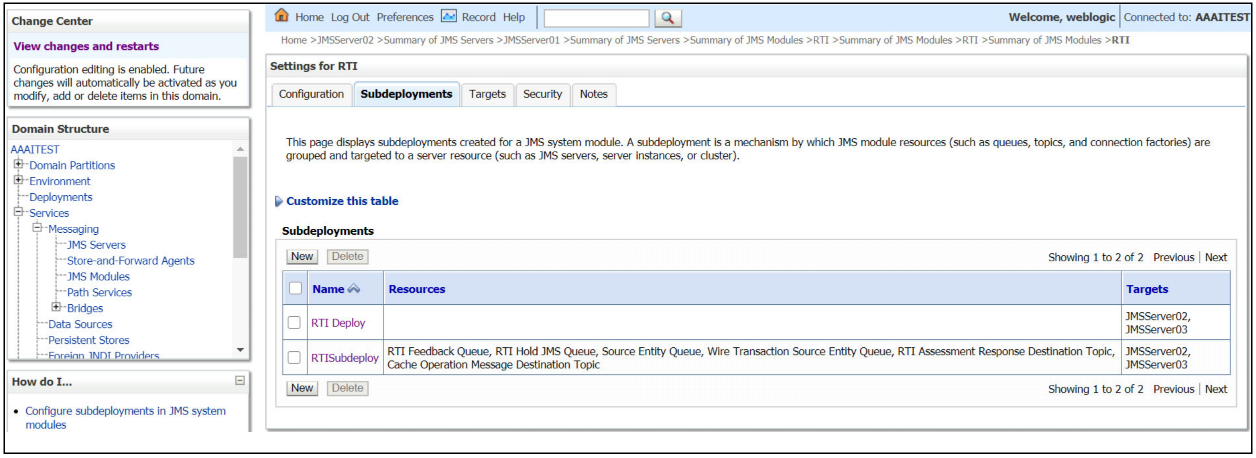
19.3 Sub-Deployment Creation

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 141: Settings for 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 subdeployments in JMS system modules
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: AAAITEST
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
Configuration
Subdeployments
Targets
Security
Notes
Customize this table
New Delete
Showing 1 to 2 of 2 Previous | Next

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

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).

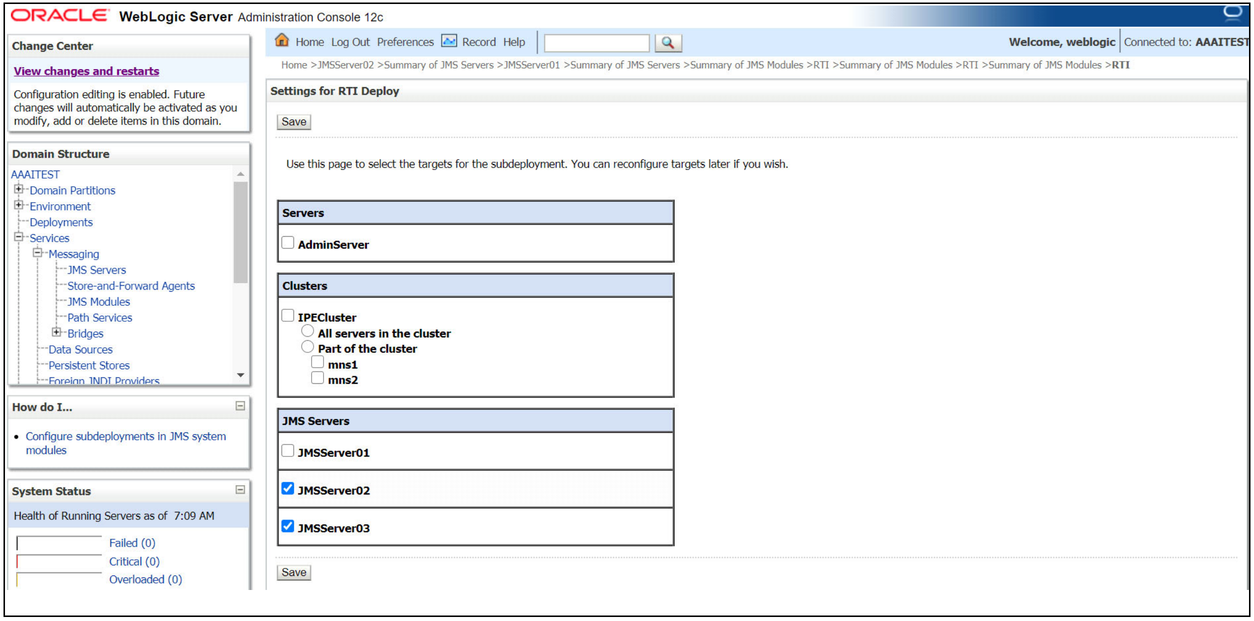
Subdeployments

☐	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 142: Settings for RTI Deploy Page



ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help | Welcome, weblogic | Connected to: AAAITEST

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**

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 subdeployments in JMS system modules

System Status

Health of Running Servers as of 7:09 AM

Failed (0)
Critical (0)
Overloaded (0)

Settings for RTI Deploy

Save

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**

Save

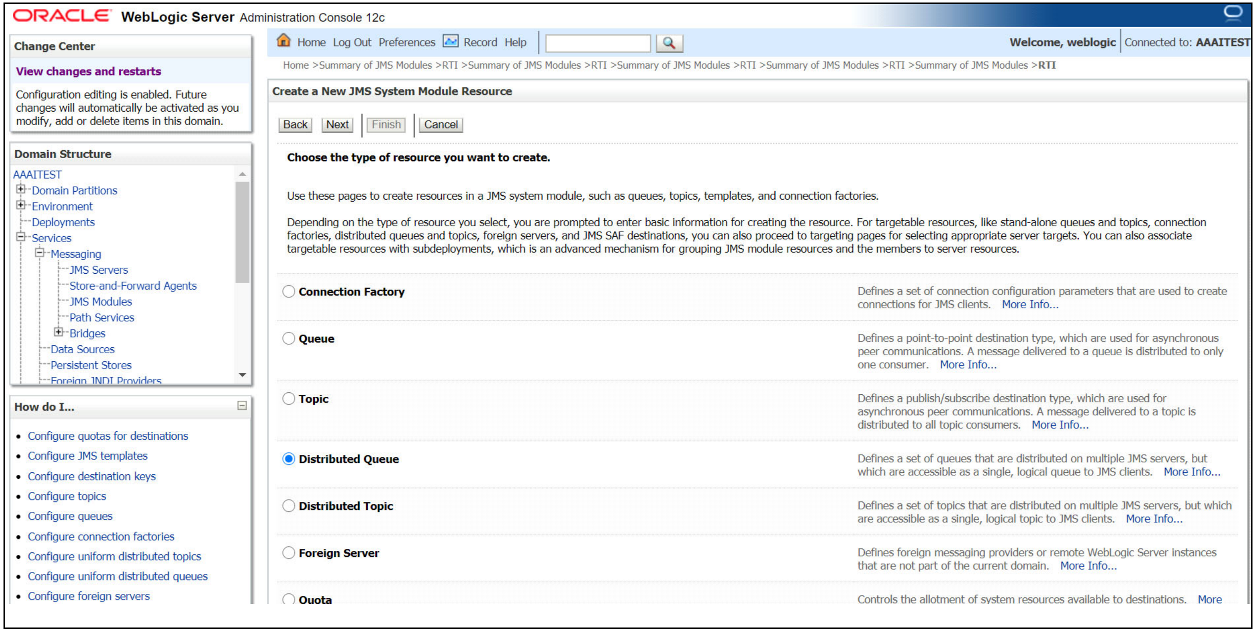
19.4 Distributed Queues Creation

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 Chapter 19.7 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 143: 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

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

Create a New JMS System Module Resource

Back | Next | Finish | Cancel

Choose the type of resource you want to create.

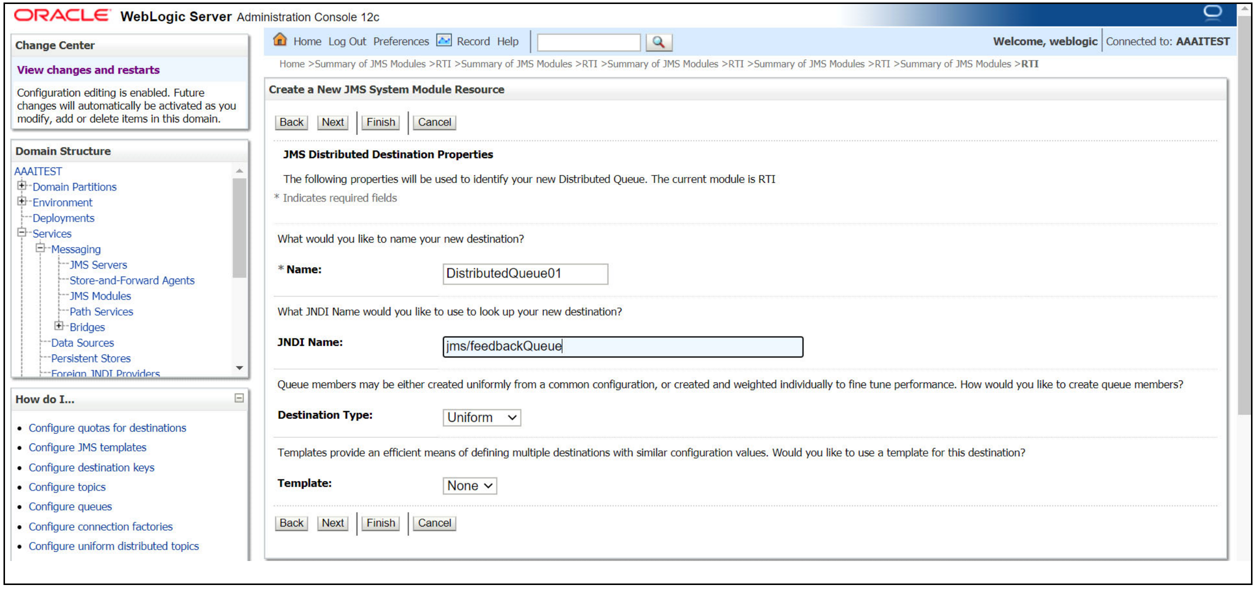
Use these pages to create resources in a JMS system module, such as queues, topics, templates, and connection factories.

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 144: 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

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

Create a New JMS System Module Resource

Back | Next | Finish | Cancel

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

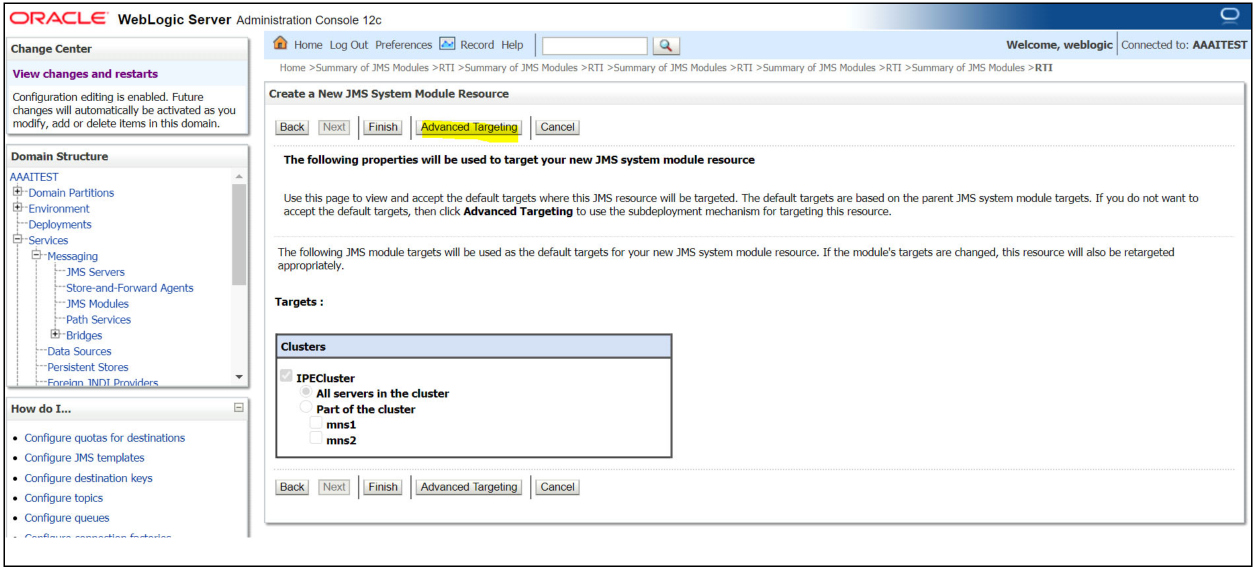
Templates provide an efficient means of defining multiple destinations with similar configuration values. Would you like to use a template for this destination?

Template: None

Back | Next | Finish | Cancel

6. Select **Advanced Targeting**.

Figure 145: 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

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**

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 :

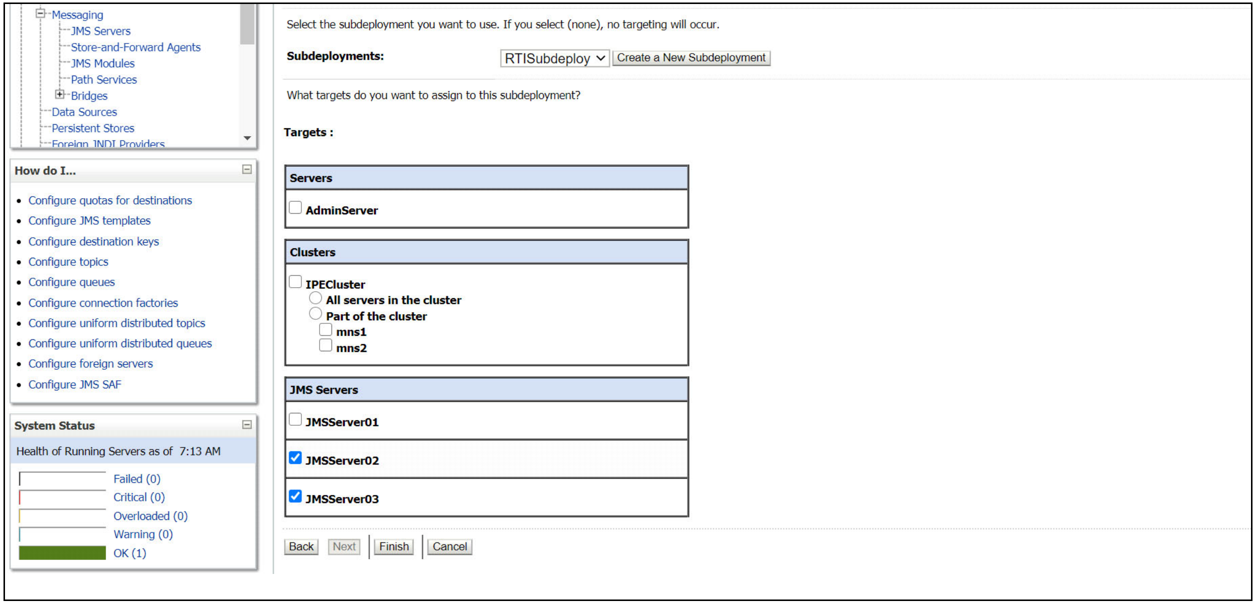
Clusters

☑ **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 146: Create a New JMS System Module Resource page



- 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
- Configure JMS SAF

System Status

Health of Running Servers as of 7:13 AM

Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)

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**

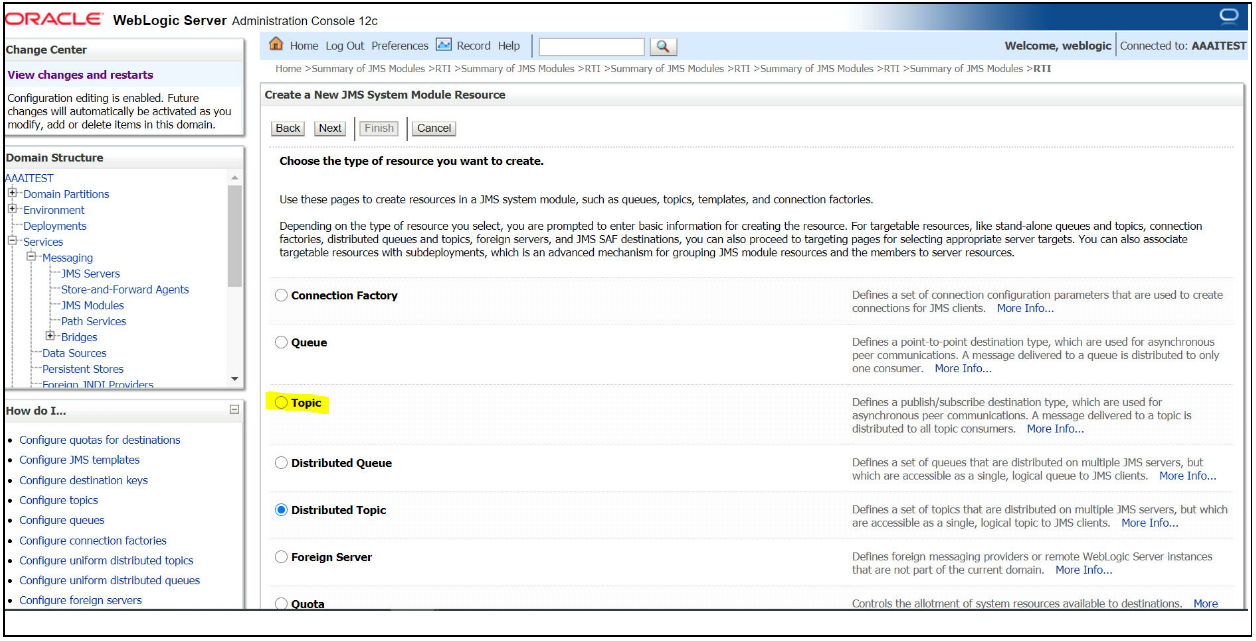
19.5 Distributed Topic Creation

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 147: Create a New JMS System Module Resource page


ORACLE 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
Back
Next
Finish
Cancel
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

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.

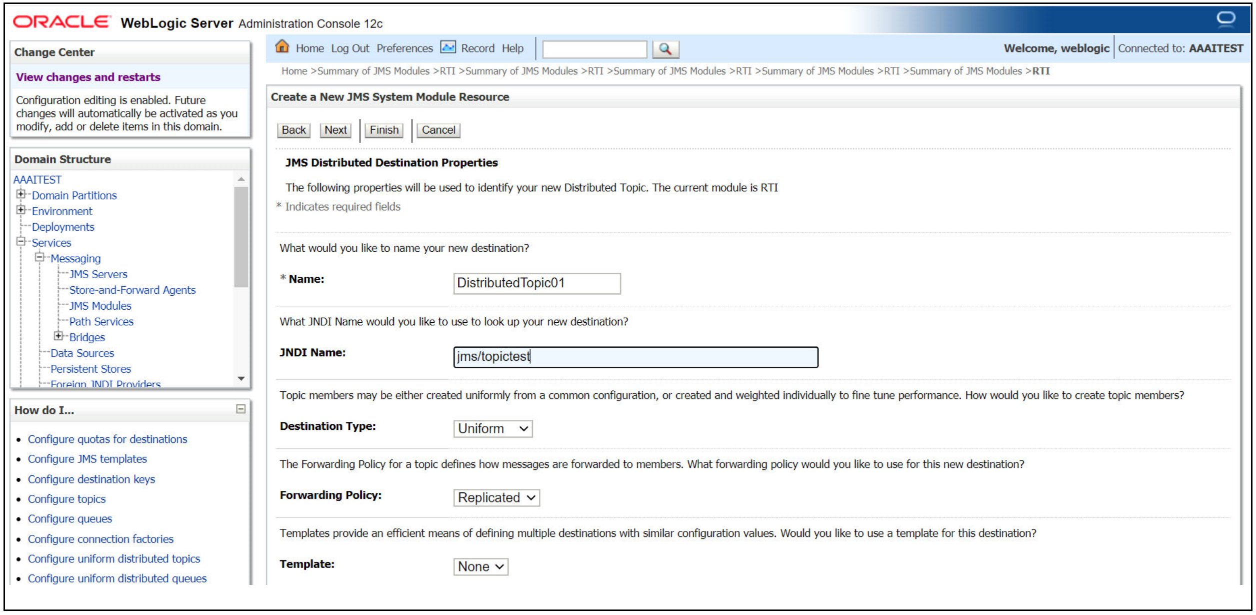
Use these pages to create resources in a JMS system module, such as queues, topics, templates, and connection factories.

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 148: 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
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

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?

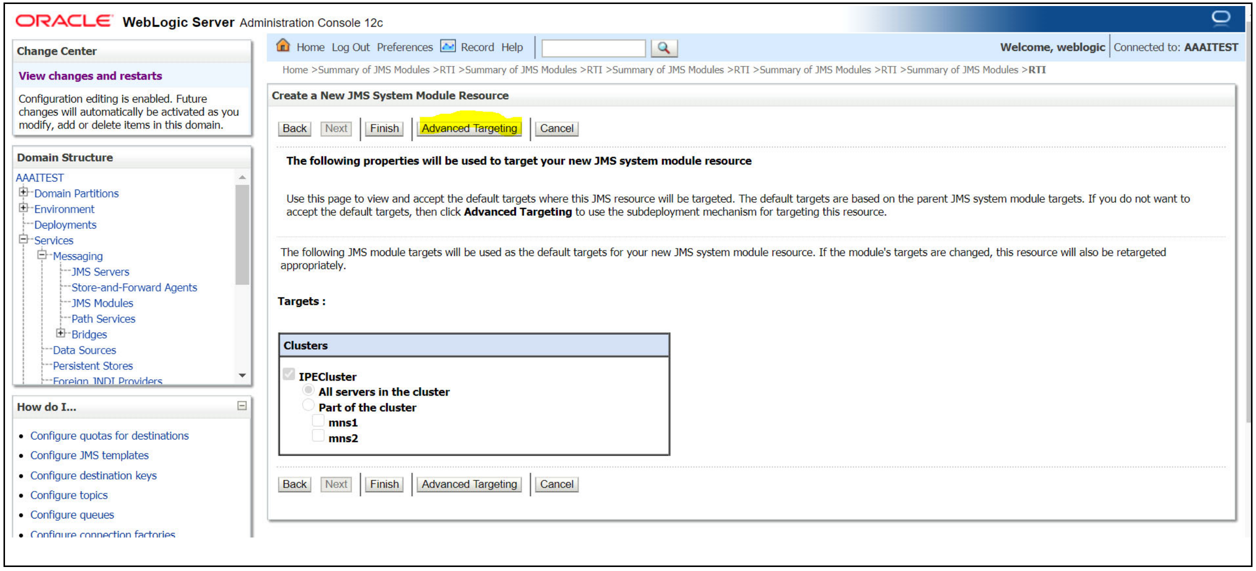
Forwarding Policy: Replicated

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 149: 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 :

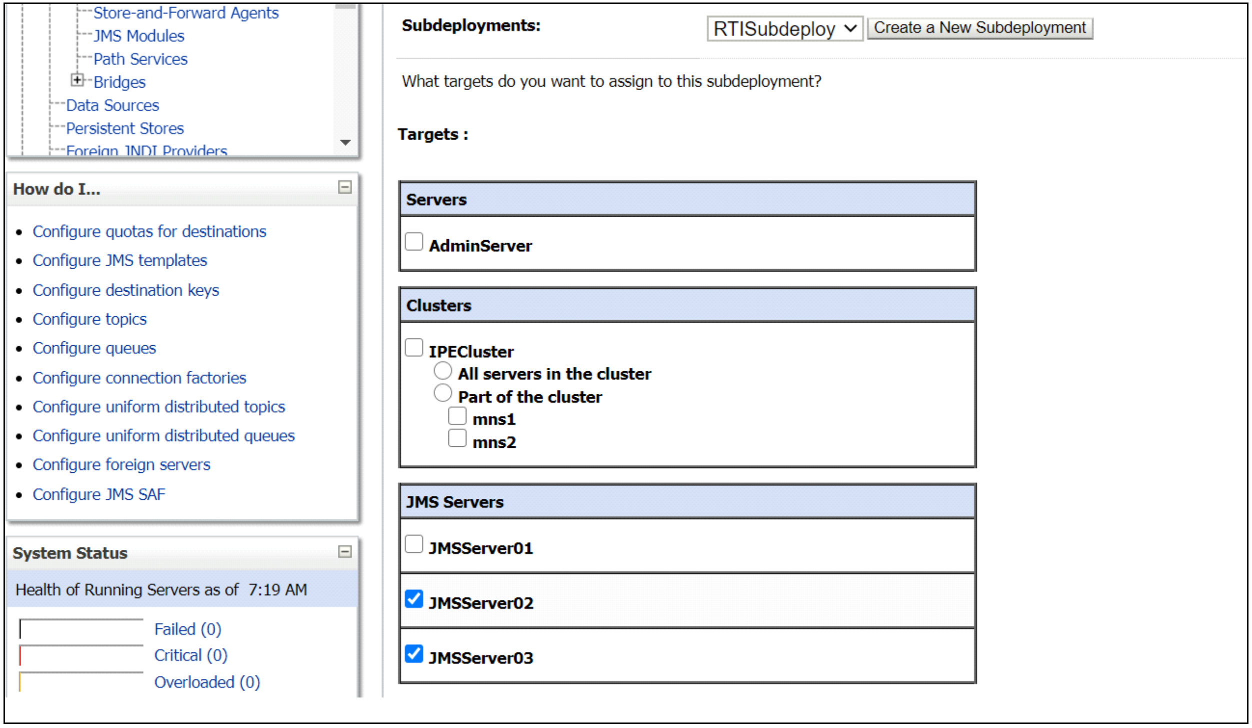
Clusters

☑ 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 150: Create a New JMS System Module Resource page


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
Configure JMS SAF
System Status
Health of Running Servers as of 7:19 AM
Failed (0)
Critical (0)
Overloaded (0)
Create a New Subdeployment

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**

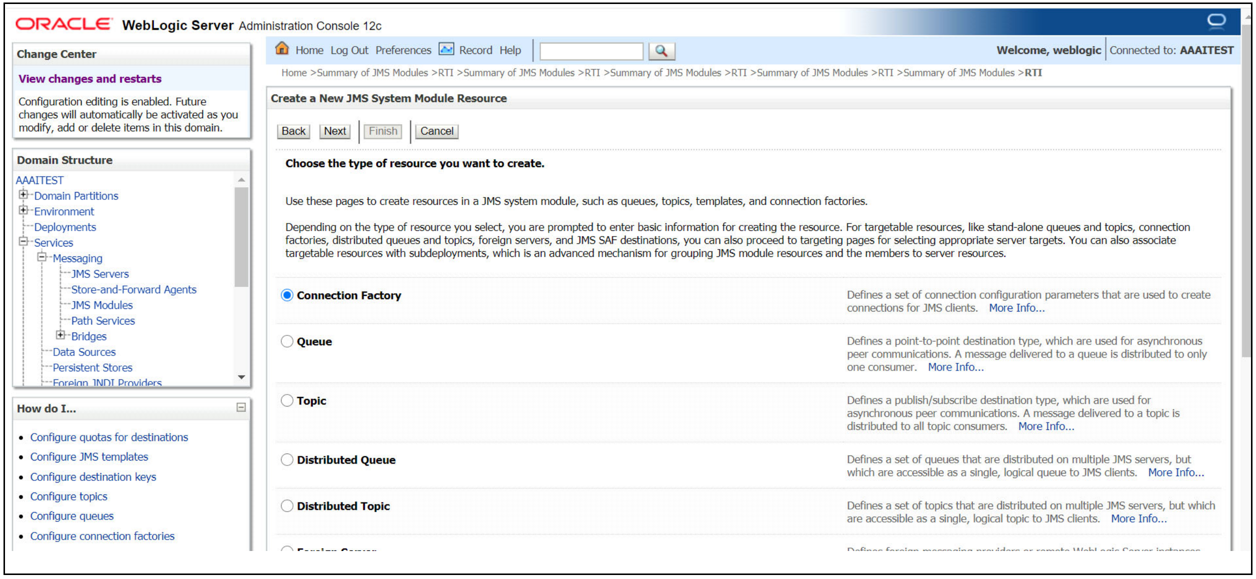
19.6 Connection Factory Creation

To create the Connection Factory, follow these steps:

> **NOTE** Connections 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 **Connection Factory** from **Create a New a JMS System Module Resource** page.

Figure 151: Create a New JMS System Module Resource page


ORACLE WebLogic Server Administration Console 12c
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
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

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.

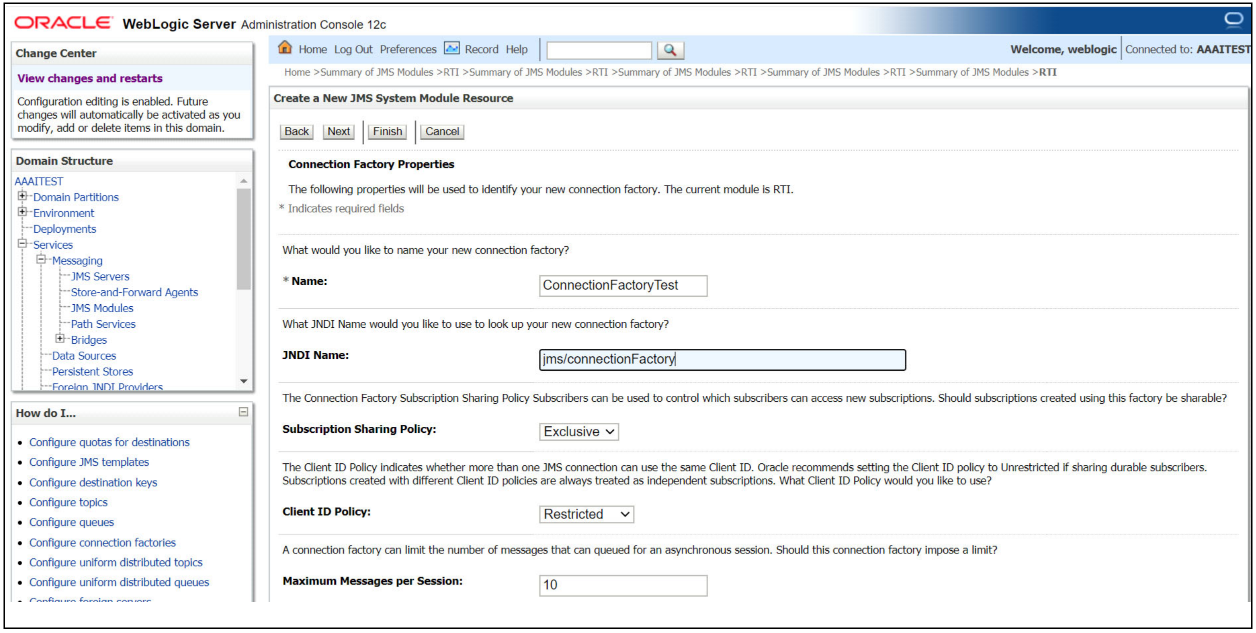
Use these pages to create resources in a JMS system module, such as queues, topics, templates, and connection factories.

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 152: Connection Factory Properties page


ORACLE WebLogic Server Administration Console 12c
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
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

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?

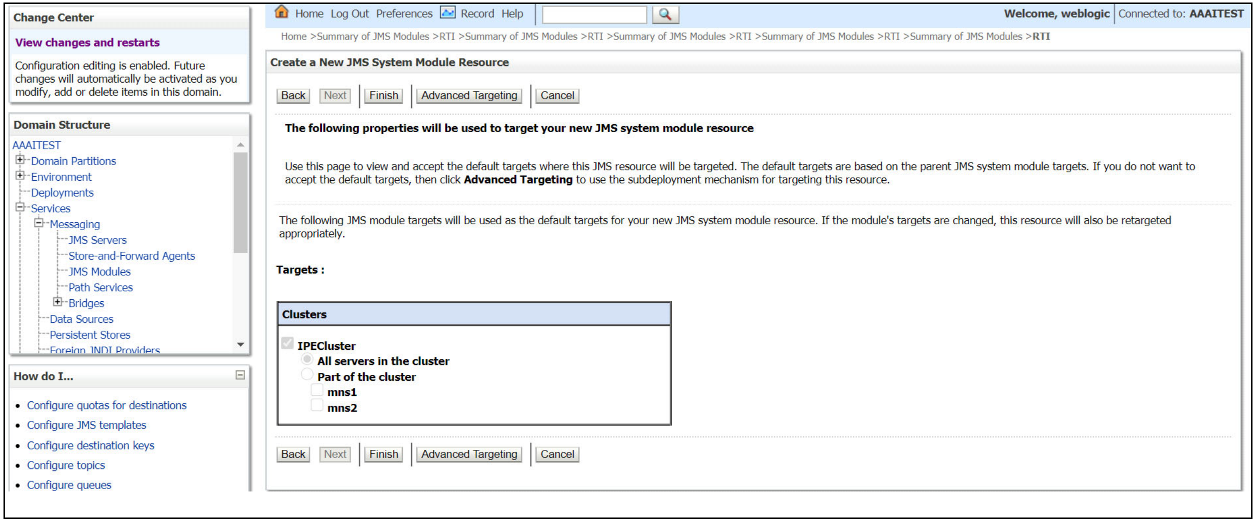
Client ID Policy: Restricted

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 153: 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 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.

19.7 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.

Table 54 provides the information about the JMS queues for SWIFT, Fedwire and ISO2022 message types.

Table 54: 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

20 Appendix 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`.

21 Appendix J: Configurations for the Bearer Token

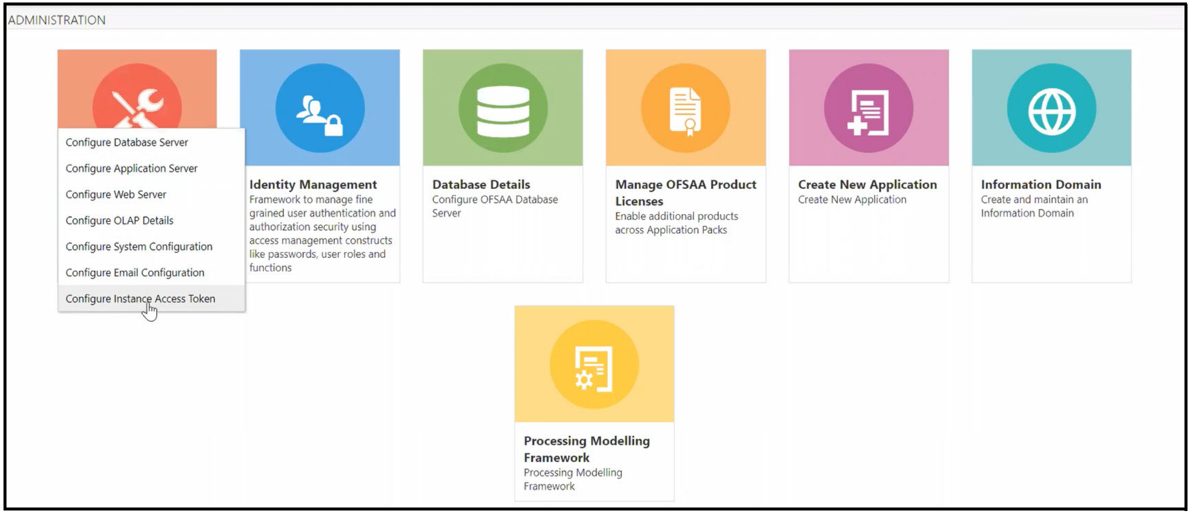
- The following section takes you through the process of generating a token and using it to get the individual or entity JSON, depending on the API request. A token is used to authorize the request.
- You can begin by generating a password for the user who sends the request. After the password is generated, 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.

21.1 Generate User Password

To generate a password for the user, follow these steps:

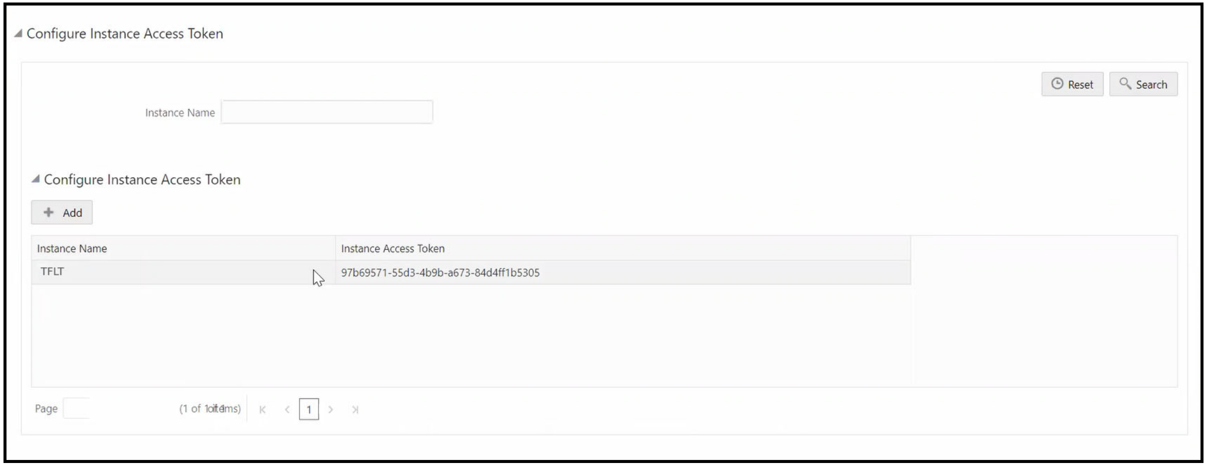
1. Log in as a system administrator.
2. Click **System Configuration** in the **Administration** page and select **Configure Instance Access Token**. The **Configure Instance Access Token** window is displayed.

Figure 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.

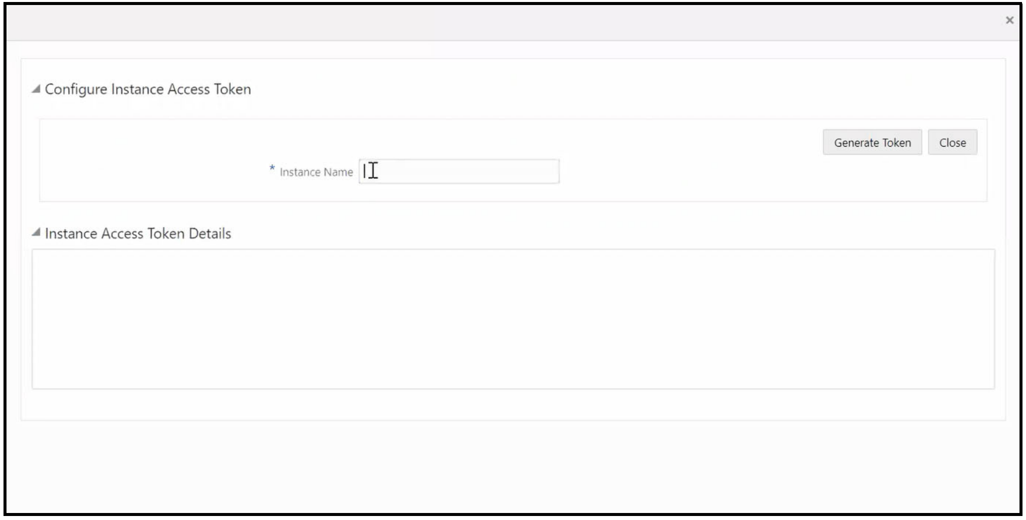
Figure 2: Configure Setup Access Token


Configure Instance Access Token
Reset
Search
Instance Name
Configure Instance Access Token
Add
Page
(1 of 1 items)
1

Instance Name	Instance Access Token
TFLT	97b69571-55d3-4b9b-a673-84d4ff1b5305

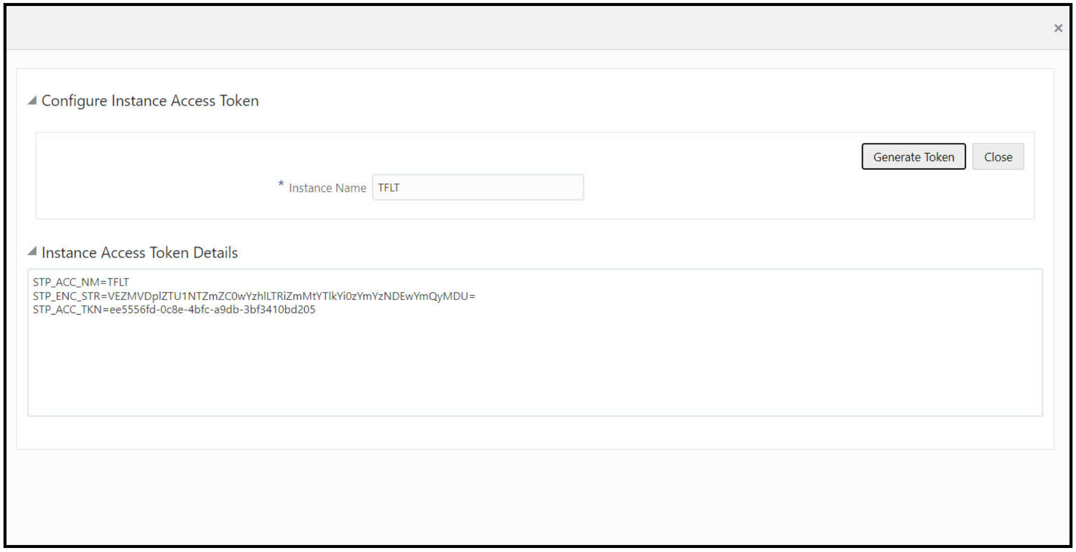
4. Enter the username in the **Instance Name** field and click **Generate Token**. The token is displayed in the **Instance Access Token Details** section.

Figure 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 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.

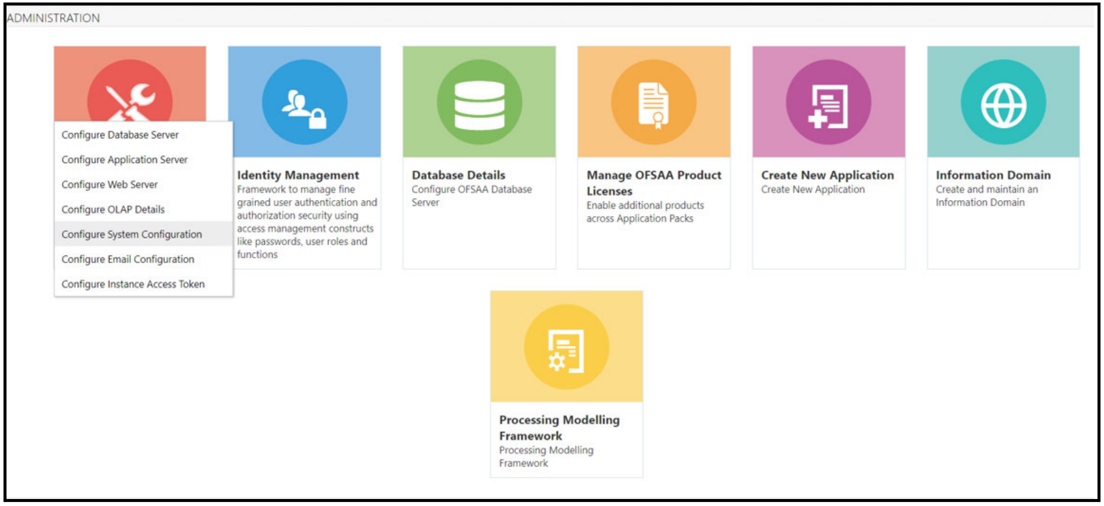
6. Click **Close** ✕ and log out as the system administrator.

21.2 Change Token Validity

To generate a password for the user, follow these steps:

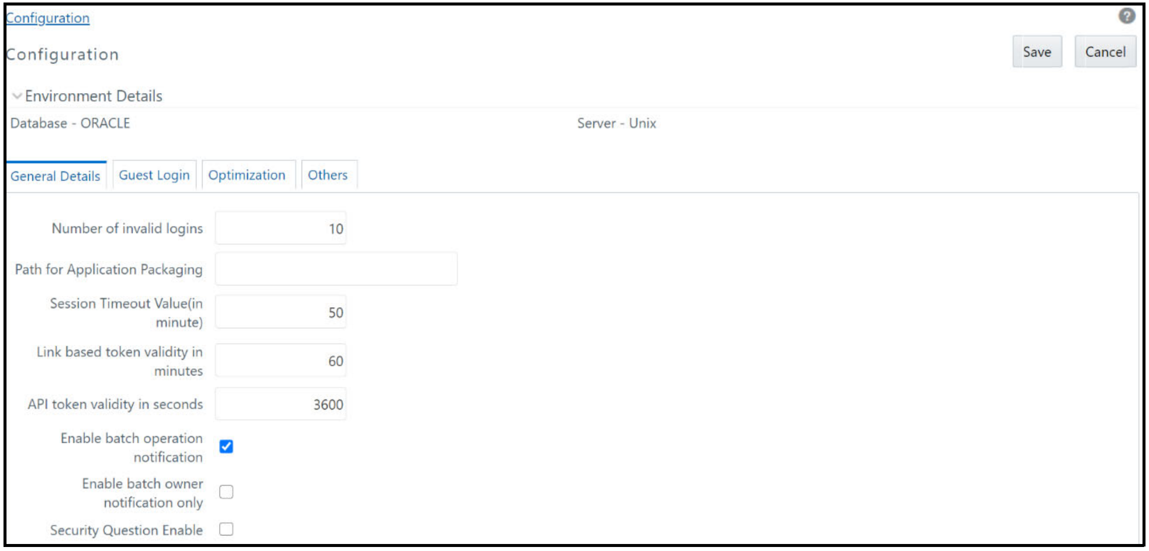
1. Log in as a system administrator.
2. Click **System Configuration** in the **Administration** page and select **Configure System Configuration**. The **Configuration** window is displayed.

Figure 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 6: Configuration window with the API token validity in seconds field shown



Configuration

Configuration

Environment Details

Database - ORACLE

Server - Unix

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**.

21.3 Generate Token

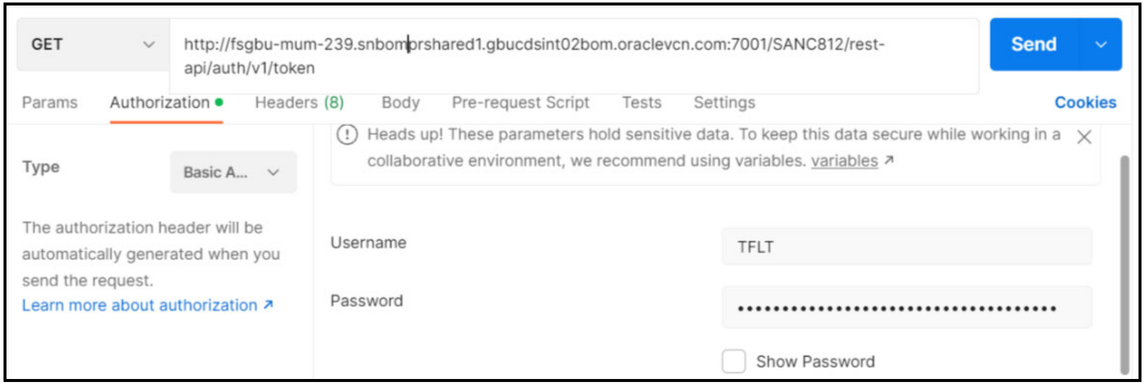
After the password is generated, you can generate the token. To generate the token, open your API client and follow these steps:

> **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 7: Request



GET http://fsgbu-mum-239.snbomprshared1.gbucdsint02bom.oraclevcn.com:7001/SANC812/rest-api/auth/v1/token

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. variables

Type: Basic A...

The authorization header will be automatically generated when you send the request.

Learn more about authorization

Username: TFLT

Password: ••••••••••••••••••••••••••••••••••••

☐ Show Password

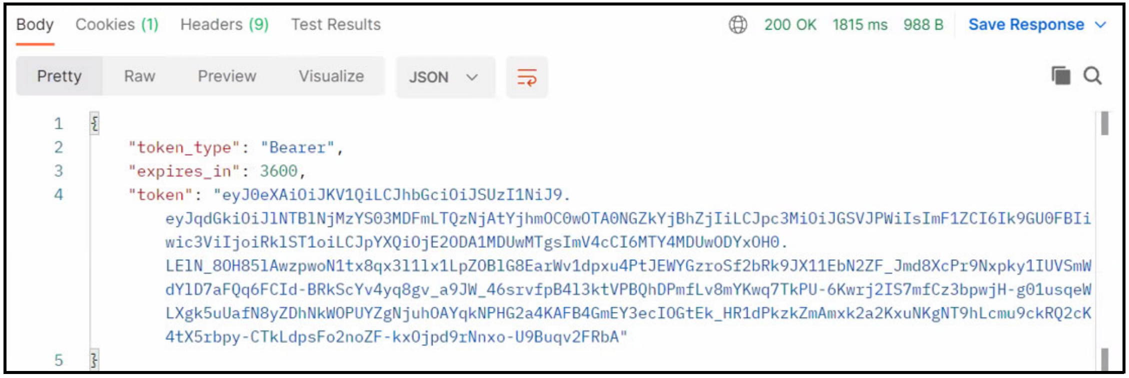
3. Select the **Authorization** menu and then select the **TYPE** as **Basic Auth**.

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 8: Response



```
{
    "token_type": "Bearer",
    "expires_in": 3600,
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
        eyJqdGkiOiJlNTBlNjMzYS03MDFmLTQzNjAtYjhmOC0wOTA0NGZkYjBhZjIiLCJpc3MiOiJGSVJPWiIsImF1ZCI6Ik9GU0FBIi
        wic3ViIjoiRklST1oiLCJpYXQiOjE2ODA1MDUwMTgsImV4cCI6MTY4MDUwODYxOH0.
        LElN_8OH85lAwzpwoN1tx8qx3l1lx1LpZOBlG8EarWv1dpxu4PtJEWYGzroSf2bRk9JX11EbN2ZF_Jmd8XcPr9Nxpky1IUVSmW
        dYlD7aFQq6FCId-BRkScYv4yq8gv_a9JW_46srvfpB413ktVPBQhDPmfLv8mYKwq7TkPU-6Kwrj2IS7mfCz3bpwjH-g01usqeW
        LXgk5uUafN8yZDhNkWOPUYZgNjuhOAYqkNPHG2a4KAFB4GmEY3ecIOGtEk_HR1dPkzkZmAmxk2a2KxuNKgNT9hLcmu9ckRQ2cK
        4tX5rbpy-CTkLdpsFo2noZF-kx0jpd9rNnxo-U9Buqv2FRbA"
}
```

21.4 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

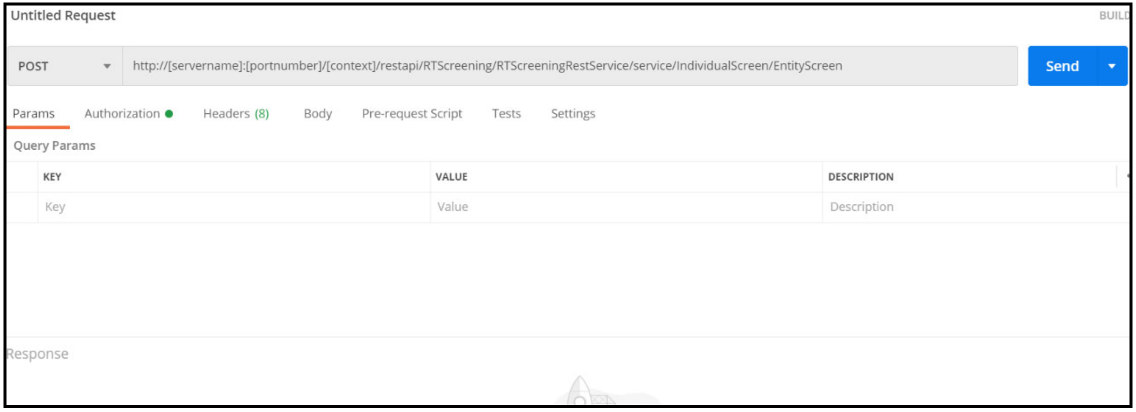
- You may use the desktop version of the Postman client to perform these steps. Postman is an open-source, collaborative platform for API development. For more information, see Postman Docs.
- You can also use any other API client, such as cURL. For more information, see REST APIs for Oracle Database.

3. 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/postMessageToQueue?queueName=sourceFedEntityQueue&msgCheckFlag=N`

Figure 9: Request



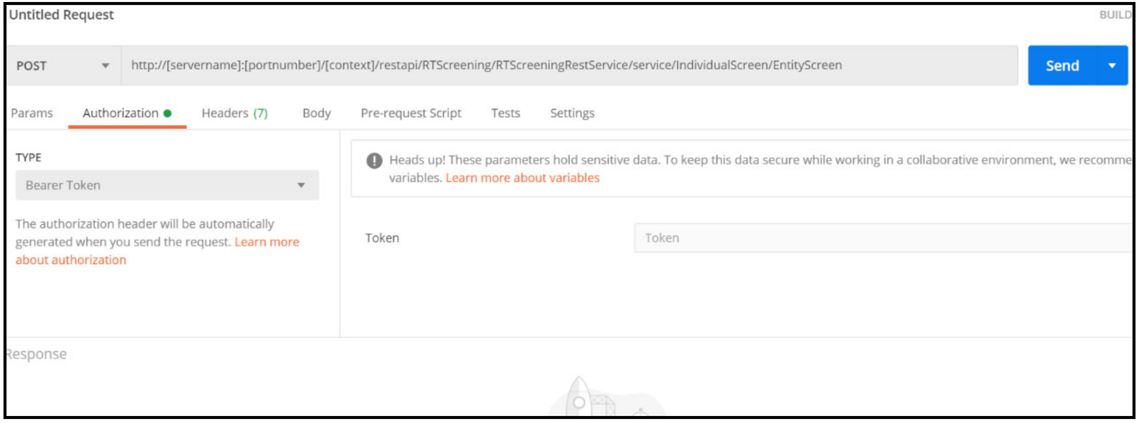
POST http://[servername]:[portnumber]/[context]/restapi/RTScreening/RTScreeningRestService/service/IndividualScreen/EntityScreen

Query Params

KEY	VALUE	DESCRIPTION
Key	Value	Description

4. In the **Authorization** menu, select the **TYPE** as **Bearer Token**.

Figure 10: Authorization



POST http://[servername]:[portnumber]/[context]/restapi/RTScreening/RTScreeningRestService/service/IndividualScreen/EntityScreen

TYPE: Bearer Token

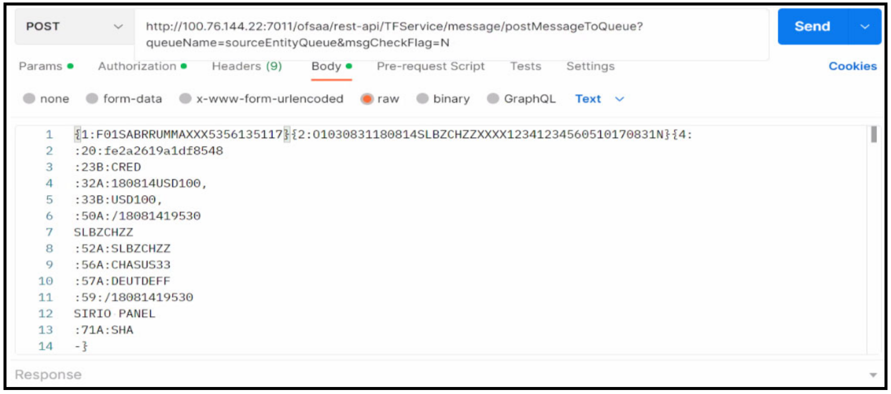
The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recomme variables. Learn more about variables

Token: Token

5. Paste the token generated in the **Token** field.
6. Select **Body** tab and select **raw**.
7. Insert the message in the text field.
8. Click **Send**.

Figure 11: Body Tab



POST http://100.76.144.22:7011/ofsaa/rest-api/TFService/message/postMessageToQueue?queueName=sourceEntityQueue&msgCheckFlag=N

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL Text

```
{1:F01SABRRUMMAXXX5356135117}{2:01030831180814SLBZCHZZXXXX12341234560510170831N}{4:
:20:fe2a2619a1df8548
:23B:CRED
:32A:180814USD100,
:33B:USD100,
:50A:/18081419530
SLBZCHZZ
:52A:SLBZCHZZ
:56A:CHASUS33
:57A:DEUTDEFF
:59:/18081419530
SIRIO PANEL
:71A:SHA
-}
```

OFSAA Support Contact Details

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

Send Us Your Comments

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

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

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.