Oracle FCCM Transaction Filtering Cloud Service

Administration Guide





Oracle FCCM Transaction Filtering Cloud Service Administration Guide, Release 24.2.1

F90359-03

Copyright © 2015, 2024, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Contents

Related Resources Help Audience Documentation Accessibility Diversity and Inclusion Conventions Comments and Suggestions	,
Audience Documentation Accessibility Diversity and Inclusion Conventions	,
Documentation Accessibility Diversity and Inclusion Conventions	,
Diversity and Inclusion Conventions	
Conventions	\
	,
Comments and Suggestions	\
Introduction	
Application Level Parameter	
Exemption Configuration	
3.1 Exemption List Management	3-:
3.1.1 Select Columns	3-
3.1.2 Filter	3-3
3.1.3 Rows Per Page	3-3
3.1.4 Format	3-3
3.1.5 Save Report	3-3
3.1.6 Reset	3-4
3.1.7 Download	3-4
3.2 Adding an Exemption	3-4
3.2.1 Adding a Exemption through Case Management	3-4
3.2.2 Adding a Exemption through TF Administration	3-!
3.2.2.1 Approving or Rejecting Alerts	3-
ISO Configuration Admin	
4.1 Configuring the ISO20022 Message Parameters	4-:



4.1.1	Running the ISO20022 Batch
-------	----------------------------

A.2 ISO20022 Message Types

Fedwire Message Types

4-4

5.1 Mes	sage and Screening Configurations Window	5-
5.1.1	Adding or Updating a New Message Type	5-
5.1.2	Configuring the References	5-
5.2 <me< td=""><td>ssage Type> Subfield Level Configuration Window</td><td>5-</td></me<>	ssage Type> Subfield Level Configuration Window	5-
5.3 <me< td=""><td>essage Type> Screening Configuration Window</td><td>5-</td></me<>	essage Type> Screening Configuration Window	5-
5.3.1	Enabling or Disabling a Web Service	5-
5.3.2	Updating and Removing a Web Service	5-
5.3.3	Populating Data for the Trade Goods and Trade Port Web Services	5-
5.4 <me< th=""><th>ssage Type> Other Field/Subfield Configuration Window</th><th>5-</th></me<>	ssage Type> Other Field/Subfield Configuration Window	5-
6.1 Mes	sage Type Configuration Window	6-
6.1.1	Adding or Updating a New Message Type	•
0.1.1	Adding or opdating a New Meddage Type	6-
6.1.2	Configuring Message and Transaction References	
6.1.2		6-
6.1.2 6.2 <me< td=""><td>Configuring Message and Transaction References</td><td>6- 6-</td></me<>	Configuring Message and Transaction References	6- 6-
6.1.2 6.2 <me< td=""><td>Configuring Message and Transaction References essage Type> Subfield Level Configuration Window</td><td>6- 6-</td></me<>	Configuring Message and Transaction References essage Type> Subfield Level Configuration Window	6- 6-
6.1.2 6.2 <me 6.3 <me< td=""><td>Configuring Message and Transaction References essage Type> Subfield Level Configuration Window essage Type> Screening Configuration Window</td><td>6- 6- 6- 6-</td></me<></me 	Configuring Message and Transaction References essage Type> Subfield Level Configuration Window essage Type> Screening Configuration Window	6- 6- 6- 6-
6.1.2 6.2 <me 6.3 <me 6.3.1</me </me 	Configuring Message and Transaction References essage Type> Subfield Level Configuration Window essage Type> Screening Configuration Window Enabling or Disabling a Web Service	6- 6- 6- 6-
6.1.2 6.2 <me 6.3 <me 6.3.1 6.3.2 6.3.3</me </me 	Configuring Message and Transaction References essage Type> Subfield Level Configuration Window essage Type> Screening Configuration Window Enabling or Disabling a Web Service Updating and Removing a Web Service	6- 6- 6- 6- 6-
6.1.2 6.2 <me 6.3 <me 6.3.1 6.3.2 6.3.3</me </me 	Configuring Message and Transaction References essage Type> Subfield Level Configuration Window essage Type> Screening Configuration Window Enabling or Disabling a Web Service Updating and Removing a Web Service Populating Data for the Trade Goods and Trade Port Web Services	6· 6· 6· 6· 6·
6.1.2 6.2 <me 6.3 <me 6.3.1 6.3.2 6.3.3 6.4 <me< td=""><td>Configuring Message and Transaction References essage Type> Subfield Level Configuration Window essage Type> Screening Configuration Window Enabling or Disabling a Web Service Updating and Removing a Web Service Populating Data for the Trade Goods and Trade Port Web Services</td><td>6- 6- 6- 6- 6- 6-</td></me<></me </me 	Configuring Message and Transaction References essage Type> Subfield Level Configuration Window essage Type> Screening Configuration Window Enabling or Disabling a Web Service Updating and Removing a Web Service Populating Data for the Trade Goods and Trade Port Web Services	6- 6- 6- 6- 6- 6-



A.3

A-2

A-3

Preface

Transaction Filtering Administratin Guide provides instructions that can help you use the Oracle Financial Services Transaction Filtering Cloud Service (OFS TF CS) application.

Related Resources

For more information, see these Oracle resources:

- Oracle Public Cloud: http://cloud.oracle.com
- Community: Use https://community.oracle.com/customerconnect/ to get information from experts at Oracle, the partner community, and other users.
- Training: Take courses on Oracle Cloud from https://education.oracle.com/oracle-cloud-learning-subscriptions.

Help

Use Help Icon to access help in the application. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. Not all pages have help icons. You can also access the https://docs.oracle.com/en/ to find guides and videos.

Audience

This document is intended for users who are responsible for provisioning and activating Oracle FCCM Cloud Service or for adding other users who would manage the services, or for users who want to develop Oracle Cloud applications.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. 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.



Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an e-mail to: https://support.oracle.com/portal/.



1

Introduction

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, or Fedwire category.

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

Application Level Parameter

Use the Application Level Parameter tab to configure the parameters for the Transaction Filtering application.

To configure the parameters, follow these steps:

- 1. Navigate to the Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service landing page.
- 2. Click Transaction Filtering Administration. The Transaction Filtering Administration page is displayed.
- 3. Click **Application Level Parameter** to display the configuration page.
- 4. In the Retrigger section, enter the value for Retrigger Time Interval (in minutes) and Retry Count.
- 5. Click **Save** to save the configuration.



Exemption Configuration

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 exemption list.

To enable or disable the exemption parameters, follow these steps:

- Navigate to the Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service landing page.
- Click Transaction Filtering Administration. The Transaction Filtering Administration page is displayed.
- 3. Click **Exemption Configuration** to display the configuration page. The following exemption parameters are available in the exemption configuration page:
 - 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**.

- Watchlist Record Name
- · Payment Entity Jurisdiction
- Watchlist Name
- Watchlist Record ID
- Payment Account ID
- Select Yes to enable the parameter and select No to disable the parameter.
- 5. Click **Save** to save the changes.

3.1 Exemption List Management

The exemption list provides the exemption summary and corresponding parameter information. User with Reviewer, and Supervisor roles can access the data but only users with Supervisor role can manage the lists under the exemption list Summary.

As a Supervisor, to access the Exemption List follow these steps:

- Login to the Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service application as a Supervisor.
- 2. Click Transaction Filtering Administration, and select Exemption List. The Exemption summary page is displayed.

You can search for a record using the following criteria in the Exemption list page.

Exemption ID

- Payment Entity Full Name
- Payment Account ID
- Jurisdiction
- Watchlist Record Name
- Watchlist Record ID
- Expiry Date
- Status
- Expiration Status
- Date Added

Click on the **Exemption ID** hyper link for match history, review and manage the exemption data. You can perform following actions on the details page.

- Change Record Parameters: Click to edit the record information.
- View Change History: Click to view the change history of the record.
- Comments: Click to type your comment for the record and click save to add the comment.
- Delete: Click to delete the exemption record.
- **Approve**: Click to Approve the exemption record. the status changes from Exemption Pending status to Approved.
- **Reject**: Click to reject the exemption record. the status changes from Exemption Pending status to Rejected.

Click on the Action button to perform the following action:

- Select Columns
- Filter
- Rows Per Page
- Format
- Save Report
- Reset
- Download

3.1.1 Select Columns

You can use the Select Column action to select the parameters to display in the exemption list UI. To add new column to the View or delete the column from the View, select the required column from the Do Not Display list or Display in Report list and use the following icon to move columns:

- Use icon to move all Columns from the Do Not Display list to the Display in Report list to add new columns
- Use icon to move the selected Columns from the **Do Not Display** list to the **Display in Report** list to add new columns



- Use icon to move the selected Columns from the **Display in Report** list to the **Do Not Display** list to delete the columns
- Use icon to move All Columns except Alert ID from **Display in Report** list to the **Do Not Display** list to delete the columns

3.1.2 Filter

You can filter the data to be displayed by selecting one of the criteria as mentioned in the Exemption Filter. You can also reset the filter criteria by clicking the **Clear** button. To apply the filter end the following fields and click **Apply**:

- Filter by Column
 - Column
 - Operator
 - Expression
- Filter by Row
 - Name
 - Filter Expression
 - Column Aliases
 - Function/Operators

3.1.3 Rows Per Page

You can use the Rows Per Page action to set the number exemption records per page.

3.1.4 Format

You can use the Format action to customize the exemption record UI view. Following formating actions are available:

- Sort
- Control Break
- Highlight
- Compute
- Aggregate
- Chart
- Group By
- Pivot

3.1.5 Save Report

You can use the **Save** action to save the report settings. Enter the name, description and click on the **Apply** button to save the report setting. You can also reset the saved report by clicking the **Clear** button.



3.1.6 Reset

You can use the Reset action to restore report to the default settings.

3.1.7 Download

You can use the Download action t download the exemption report. The following report download formats are available:

- CSV
- HTML
- Excel
- PDF
- Sent as Email

3.2 Adding an Exemption

You can add the exemption record through the following ways:

- Transaction Filtering Administration
- Case Management

3.2.1 Adding a Exemption through Case Management

The Analyst can add the exemption record in the Case Investigation User Interface. It then goes to the Supervisor for approval. If the Supervisor approves the exemption record, it is added to the exemption list. For more information on case investigation, see Oracle FCCM Cloud Services Case Investigation guide.

To add a new exemption record follow the subsequent steps:

- Navigate to Case Search and List Window. The Case Search and List page displays as a tab with a list of all open cases and a tab with a list of all open cases currently assigned to the logged in user.
- 2. Select the case by clicking the corresponding **Case ID** hyper link to view the details. The Case Details page is displayed.
- In the Events list of the Case Details page, select one or more check boxes associated with events and click Add to Exemption. The Add to Exemption configuration page is displayed.
- 4. Select the part of text to be added in exemption list click move icon.
- 5. Click **Clear** to delete the selected part of the name.
- 6. Select the Expiry Date.
- Click Submit for Approval to submit the allow list name for approval or Click Cancel to close the window.

The exemption record is then send to the Supervisor for approval. The Supervisor can approve or reject the alert by clicking Actions.



3.2.2 Adding a Exemption through TF Administration

To add a new exemption record follow the subsequent steps:



Only the Supervisor can perform this action.

- 1. Login to the Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service application as a Supervisor.
- Click Transaction Filtering Administration, and select Exemption List. The Exemption summary page is displayed.
- 3. Click **Add New Record**. The Add exemption page is displayed.
- 4. Enter the subsequent parameters:
 - Payment Details
 - Payment Full Name: Enter the record name.
 - Payment Entity Jurisdiction: You can either enter a jurisdiction name or select from the drop-down list.
 - Payment Account ID: Enter the identifier.
 - Watchlist Details
 - Watchlist Record Name: Enter the origin record name.
 - Watchlist Name: Enter the name of the origin.
 - Watchlist Record ID: Enter the record ID.
 - Date
 - Expiration Date: Select the expiration date
- Click Save to add the new exemption record to exception list. Click Cancel to close the Add exception page.

✓ Note:

The newly added exemption record have Approved status.

3.2.2.1 Approving or Rejecting Alerts

To approve or reject the case as a Supervisor, follow these steps:

- Login to the Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service application as a Supervisor.
- 2. Click **Transaction Filtering Administration**, and select **Exemption List**. The Exemption summary page is displayed.
- 3. Click on the **Exemption ID** hyper link to display the summary page.

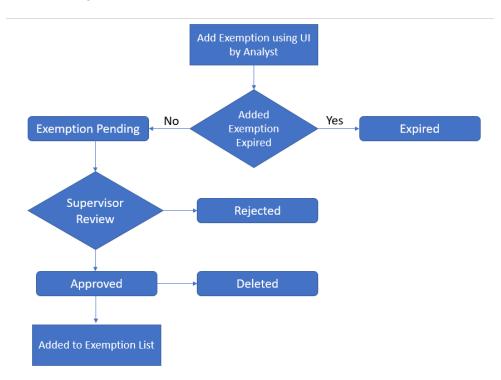


4. Click Approve to approve the case or click Reject to reject the case. If the Supervisor approves the case, the status changes from Exemption Pending status to Approved. If the Supervisor rejects the case, the status changes from Exemption Pending status to Rejected.



It is mandatory to add comments after the case is approved or rejected.

Figure 3-1 Case Investigation UI Workflow to add a Exemption Record to the Good Guy List





4

ISO Configuration Admin

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.



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

4.1 Configuring the ISO20022 Message Parameters

To configure the ISO20022 message parameters, follow these steps:

- 1. Navigate to the Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service landing page.
- 2. Click **Transaction Filtering Administration**. The Transaction Filtering Administration page is displayed.
- 3. Click **ISO Configuration Admin**. The Configuration window is displayed.
 - 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.
- 4. To upload a new XSD file, click Add Message. An Attachment Details dialog box opens.
- 5. 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.
- 6. 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.

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.



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.

- 7. Click **Submit**. The ISO20022 parameter name appears in the Message List section with Draft attached to the parameter name.
- 8. 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.

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 4-1 Other Actions

То	Do this
Add a web service configuration	Click Add . The Add a web service configuration fields is displayed.
	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.
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.
Enable all web service configurations	Click Enable All.
Disable all web service configurations	Click Disable All.

9. 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. In this tab, you can view the details of the attribute name, enable status, and message direction details.



Table 4-2 Other Actions

То	Do this
Add an external attribute configuration	Click Add. The Add an External Attribute configuration fields is displayed: 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.

10. 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

11. To view the message tag configurations for a field, click the XML Message Configuration tab. You can also perform the following actions:

Table 4-3 Other Actions

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



Table 4-3 (Co	ont.) Other	Actions
---------------	-------------	---------

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

12. Click **Submit**. The ISO20022 parameter name is updated in the **Message List** without _**Draft**.

4.1.1 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.



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

The directory structures for OUTBOUND and INBOUND are as follows: ##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUTBOUND/INPUT ##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC MIS_DATE##/INBOUND/INPUT

For example,

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

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

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



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

##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUTBOUND/
VAL ERROR

##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/INBOUND/
VAL ERROR

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

##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUTBOUND/
PRCSNG ERROR

##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/INBOUND/
PRCSNG ERROR

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

##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUTBOUND/
VAL ERROR

##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/INBOUND/
VAL ERROR

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

##FTPSHARE_PATH##/SANCINFO/STAGE/SEPA/inputXML/##FIC_MIS_DATE##/OUTBOUND/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.

- 3. Navigate to the Run page.
- 4. Select the TF_SEPA_messages_batch_process batch and click Fire Run. The Fire Run page is displayed.
- 5. Select Single as the Request Type.



- 6. Select Create & Execute in the Batch field. The MIS Date field is displayed.
- 7. 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.

8. 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.
- 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.



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

Table 4-4 Task Details

Task ID	Task Name	Task Description
Task1	TF_CallXMLParser	Parses the XML data into the pre-processing tables.
Task2	TF_CallXMLEDQ	Calls EDQ data to check if there are any matches.
Task3	Message Data Attributes	NA
Task4	TF_CallXMLRTIPopulation	Moves data from the ISO20022 configuration tables to the SWIFT configuration tables to generate OBI reports.
Task5	TF_CallXMLAlertGeneration	Creates alerts and loads data into the alert tables.
Task6	TF_CallXMLImmediateFeed backCreation	Populates the feedback table.
Task7	TF_CallXMLImmediateFeed backFileGeneration	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.



Table 4-4 (Cont.) Task Details

Task ID	Task Name	Task Description
Task9	TF_CallUpdateAdditionalMs gDtls	Populates the post- processing alert table with the additional details provided for the alert.
Task10	TF_CallXMLStructuredSepa	Populates the data in the Structured Message tab in the Investigation User Interface.



5

SWIFT Configuration Admin

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

- 1. Navigate to the Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service landing page.
- Click Transaction Filtering Administration. The Transaction Filtering Administration page is displayed.
- Click SWIFT Configuration Admin. The Message and Screening Configurations tab is displayed.



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

5.1 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.

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

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**.

5.1.1 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.
- 3. To upload an attachment, click Choose File. You can upload only one attachment at a time.



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>.

5.1.2 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.

5.2 < Message Type > Subfield Level Configuration Window

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

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



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

Table 5-1 Fields in the <Message Type> Subfield Level Configuration Window

- 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:

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

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

• By configuring the element level data within the subfield expression: Do this if you want to further configure any data out of the subfield. In this example, if you want to configure the country code for field 57, then you can configure 2!a from Identifier



Code expression as a country code by giving unique names in the **Subfield Expression Identifier**, **Subfield Name**, and **Subfield Description fields**.

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

5.3 < Message Type> Screening Configuration Window

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

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

Table 5-2 Fields in the <Message Type> Screening Configuration Window

Fields	Field Description	
Screening WebService	Select a screening web service from the drop-down list. This field lists all the supported matching web services in the Transaction Filtering application. The following web services are available: 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.	
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 adbusinesd descriptions for the jurisdictions.	
Add button	To add a web service, provide the required values in the fields shown above and click Add icon.	



Table 5-2 (Cont.) Fields in the <Message Type> Screening Configuration Window

Fields	Field Description
Update button	To update a web service, select the web service that you want to update and click Update icon.
Remove button	To remove a web service, select the web service that you want to remove and click Remove icon.
Enable All button	To enable all web services, click Enable All icon.
Disable All button	To disable all web services, click Disable All icon.

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:

Table 5-3 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 icon.
Update button	To update a web service, select the web service that you want to update and click Update icon.
Remove button	To remove a web service, select the web service that you want to remove and click Remove icon.
Enable All button	To enable all web services, click Enable All icon.
Disable All button	To disable all web services, click Disable All icon.

5.3.1 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 <code>[WEBSERVICE_IDS]</code> placeholder with the corresponding web service ID. The web services and the corresponding IDs are shown here:

Table 5-4 Web Services in Transaction Filtering

Web Service	Web Service ID
Name and Address	Name and Address
BIC	BIC



Table 5-4 (Cont.) Web Services in Transaction Filtering

Web Service	Web Service ID
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.

5.3.2 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**.

5.3.3 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:

- 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.
- 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.
- Click Run.



5.4 < 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.

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 5-5 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 icon.
Update button	To update a web service, select the web service that you want to update and click Update icon.
Remove button	To remove a web service, select the web service that you want to remove and click Remove icon.

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



6

FED Configuration Admin

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

- 1. Navigate to the Oracle Financial Services Crime and Compliance Management Anti Money Laundering Cloud Service landing page.
- 2. Click Transaction Filtering Administration. The Transaction Filtering Administration page is displayed.
- Click FED Configuration Admin. The Message and Screening Configurations tab is displayed.



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

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

6.1 Message Type Configuration Window

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

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

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

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

- Status: This column mentions whether the field is Mandatory (M) or Optional (O).
- FieldName: This column describes the name of the given field as per Fedwire standards.
- **Expression**: This column depicts the field structure in terms of expression. For example, if the field is a data type, then the maximum length of the field is displayed.

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

6.1.1 Adding or Updating a New Message Type

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

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



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>.

6.1.2 Configuring Message and Transaction References

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

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

6.2 < Message Type > Subfield Level Configuration Window

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

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

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

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



Table 6-1 (Cont.) Fields in the <Message Type> Subfield Level Configuration Window

Fields	Field Description
Subfield Expression Format and 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 icon.
Update button	To update an existing subfield, click the name of the subfield. After you make the changes, click Update icon.
Remove button	To remove an existing subfield, click the name of the subfield and click Remove icon.
Clear button	To clear the data in these fields, click Clear icon.

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:

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

```
Option A:

[/1!a][/34x] (Party Identifier)

4!a2!a2!c[3!c] (Identifier Code)
```

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.

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



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

Fields	Field Description		
Screening WebService	Select a screening web service from the drop-down list. This field lists all the supported matching web services in the Transaction Filtering application. The following web services are available: BIC Country and City Goods Screening Name and Address Narrative or Free Text Information Port Screening The fields for all web services except Goods Screening are as shown here.		
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 adbusinesd descriptions for the jurisdictions.		
Add button	To add a web service, provide the required values in the fields shown above and click Add icon.		
Update button	To update a web service, select the web service that you want to update and click Update icon.		
Remove button	To remove a web service, select the web service that you want to remove and click Remove icon.		
Enable All button	To enable all web services, click Enable All icon.		
Disable All button	To disable all web services, click Disable All icon.		

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:



Table 6-3 Fields in the Goods Web Service Window	Table 6-3	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 icon.
Update button	To update a web service, select the web service that you want to update and click Update icon.
Remove button	To remove a web service, select the web service that you want to remove and click Remove icon.
Enable All button	To enable all web services, click Enable All icon.
Disable All button	To disable all web services, click Disable All icon.

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 <code>[WEBSERVICE_IDS]</code> placeholder with the corresponding web service ID. The web services and the corresponding IDs are shown here:

Table 6-4 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

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.
- 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.

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

Table 6-5 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.
· · · · · · · · · · · · · · · · · · ·	



Table 6-5 $\,$ (Cont.) Fields in the <Message Type> Other Field/Subfield Configuration Window

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

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



A

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

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

A.1 SWIFT Message Types

For the SWIFT message category, the message types are out-of-the-box. The unsupported message types must to added using the SWIFT Administration tool.

Table A-1 SWIFT Message Types

No	Message Type	No	Message Type	No	Message Type	No	Message Type
1	MT101	2	MT102	3	MT103	4	MT103STP
5	MT104	6	MT105	7	MT107	8	MT110
9	MT111	10	MT112	11	MT190	12	MT191
13	MT192	14	MT195	15	MT196	16	MT198
17	MT199	18	MT200	19	MT201	20	MT202
21	MT202COV	22	MT203	23	MT204	24	MT205
25	MT205COV	26	MT210	27	MT290	28	MT291
29	MT292	30	MT295	31	MT296	32	MT298
33	MT299	34	MT300	35	MT304	36	MT305
37	MT306	38	MT320	39	MT321	40	MT350
41	MT362	42	MT395	43	MT396	44	MT399
45	MT400	46	MT410	47	MT412	48	MT416
49	MT420	50	MT430	51	MT455	52	MT456
53	MT490	54	MT491	55	MT492	56	MT495
57	MT496	58	MT498	59	MT499	60	MT515
61	MT516	62	MT526	63	MT536	64	MT537
65	MT540	66	MT541	67	MT542	68	MT543
69	MT544	70	MT545	71	MT546	72	MT547
73	MT548	74	MT564	75	MT566	76	MT568
77	MT581	78	MT590	79	MT591	80	MT592
81	MT595	82	MT596	83	MT599	84	MT604
85	MT605	86	MT606	87	MT607	88	MT608
89	MT671	90	MT695	91	MT696	92	MT699

Table A-1 (Cont.) SWIFT Message Types

No	Message Type	No	Message Type	No	Message Type	No	Message Type
93	MT700	94	MT701	95	MT705	96	MT707
97	MT708	98	MT710	99	MT711	100	MT720
101	MT721	102	MT730	103	MT732	104	MT734
105	MT740	106	MT742	107	MT747	108	MT750
109	MT752	110	MT754	111	MT756	112	MT759
113	MT760	114	MT765	115	MT767	116	MT768
117	MT769	118	MT790	119	MT791	120	MT792
121	MT795	122	MT796	123	MT798	124	MT799
125	MT801	126	MT802	127	MT824	128	MT890
129	MT895	130	MT896	131	MT899	132	MT900
133	MT910	134	MT940	135	MT942	136	MT950
137	MT985	138	MT986	139	MT995	140	MT996
141	MT998	142	MT999				

A.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 A-2 ISO20022 Message Types

No	Message Type	No	Message Type	No	Message Type	No	Message Type
1	camt.026.0 01.09	2	camt.027.0 01.09	3	camt.028.0 01.11	4	camt.029.0 01.11
5	camt.031.0 01.06	6	camt.032.0 01.04	7	camt.033.0 01.06	8	camt.038.0 01.04
9	Camt.050.0 01.05	10	camt.052.0 01.08	11	camt.052.0 01.10	12	camt.053.0 01.08
13	camt.053.0 01.10	14	camt.054.0 01.08	15	camt.054.0 01.09	16	camt.054.0 01.10
17	camt.056.0 01.10	18	camt.060.0 01.05	19	camt.060.0 01.06	20	camt.087.0 01.08
21	pacs.002.0 01.12	22	Pacs.003.0 01.02	23	pacs.003.0 01.10	24	Pacs.004.0 01.09
25	pacs.004.0 01.12	26	Pacs.008.0 01.02	27	Pacs.008.0 01.07	28	Pacs.008.0 01.08
29	pacs.008.0 01.11	30	Pacs.009.0 01.08	31	pacs.009.0 01.10	32	Pacs.010.0 01.03
33	pacs.010.0 01.05	34	pacs.028.0 01.05	35	Pain.001.00 1.08	36	Pain.001.00 1.09

A.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 A-3 Fedwire Message Types

No	Message Type	No	Message Type	No	Message Type	No	Message Type
1	FDBTR1000	2	FDBTR1002	3	FDBTR1008	4	FDBTR1600
5	FDBTR1602	6	FDCKS1600	7	FDCKS1602	8	FDCTP1000
9	FDCTP1002	10	FDCTP1008	11	FDCTP1600	12	FDCTP1602
13	FDCTR1000	14	FDCTR1002	15	FDCTR1008	16	FDCTR1600
17	FDCTR1602	18	FDDEP1600	19	FDDEP1602	20	FDFFR1600
21	FDFFR1602	22	FDFFS1600	23	FDFFS1602		

