Oracle FCCM Transaction Filtering Cloud Service

Administration Guide

Release 25.08.01
G40819-01
August 2025

Oracle FCCM Transaction Filtering Cloud Service Administration Guide, Release 25.08.01

G40819-01

Contents

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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

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.

3
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:

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 **Exemption Configuration** to display the configuration page. The following exemption parameters are available in the exemption configuration page:
   - payment entity full name

     > **Note**
     >
     > 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
4. 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:

1. 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:

1. 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.
3. 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.
7. 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:

> **Note**
>
> 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.
2. 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
5. 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.

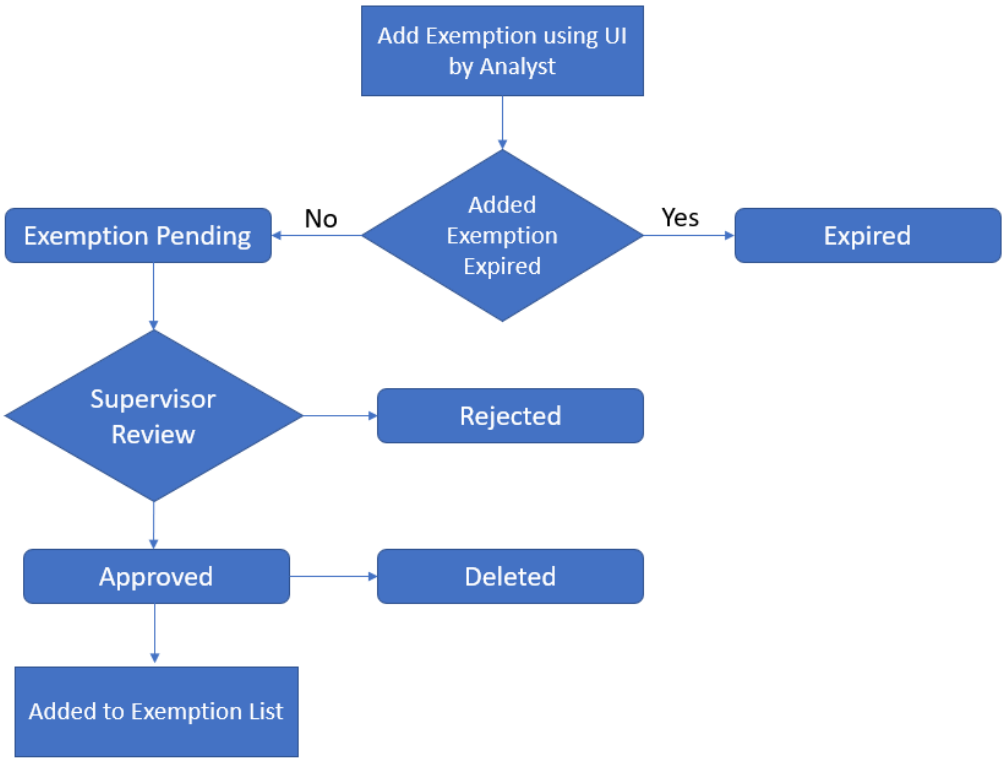
3.2.2.1 Approving or Rejecting Alerts

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

1. 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.

> **Note**
>
> 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.

> **Note**
>
> 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.

> **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.

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

To...	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

To...	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

```
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");
```

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

To...	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 (Cont.) Other Actions

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

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

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.
2. Click **Transaction Filtering Administration**. The **Transaction Filtering Administration** page is displayed.
3. 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

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.

> **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>`.

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:

Table 5-1 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.

Table 5-1 (Cont.) Fields in the <Message Type> Subfield Level Configuration Window

Fields	Field Description
Field	This field displays a complete list of fields in the drop-down for the given message type. Select the field from this drop-down field to configure the expression.
Field/Subfield Name	This field displays the respective field name or subfield options for the field that was previously selected. Select the subfield from the drop-down list.
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.

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.
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.

Table 5-3 (Cont.) Fields in the Goods Web Service Window

Fields	Field Description
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 `[WEBSERVICE_IDS]` 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
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:

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**.

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.
3. Click **FED 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 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.

> **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>`.

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.
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.

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

Fields	Field Description
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.

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

Fields	Field Description
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

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 `[WEBSERVICE_IDS]` 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.
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.

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.
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**.

7

Run the ISO20022 Batch Screening

The ISO20022 transaction messages are processed in bulk using batches such as “**ISO20022BatchScreening**” and “**ISOBatchScreeningToCaseManagement**”. Input Transaction Files are accepted in `.json` format and it can be either single json file with list of all transactions or multiple json files with list of transactions. Input transactions are processed, screened, and the feedback file is generated in the .json format.

For managing the above batches, refer Transaction Filtering Screening Batches Details.

Operations of ISO20022 Batches:

1. **ISO20022BatchScreening** – This batch performs Download the Transaction files from Object Storage, Load the transactions into tables, Parse the raw messages, Transform data, Load transformed data to Matching Engine, Screen the Data against Watchlist and create Events, Generate Score, Make HOLD/CLEAN decision along with Exemption/Alert Suppression, Generate TF immediate Feedback and Upload to Object Storage, Highlight Raw Message, and Create TF Alerts.
2. **ISOBatchScreeningToCaseManagement** – This batch performs Generate Cases for created Alerts using Case Management Tasks and Update TF Feedback with Case Id.

7.1 Prerequisites

1. Access the Object Storage Pre-authenticated URL form Admin Console. For more information see Access the Object Storage Pre-authenticated URL.
2. Setup the upload Transaction Files to Object Storage Utility.
   a. In any Linux environment, create a new folder. E.g. ISO20022_Batch_InputData_Upload_Utility.
   b. Change the directory inside the newly created folder.
   c. Create a file named “cto.sh” and paste the below contents.

```
#!/bin/bash
filename='filename.txt'

n=1
tdate=$1

echo "Entered FIC MIS Date is: " $tdate
objstore="<<OBJECT_STORAGE_PAR_URL>>"

echo "Start Copy files to Object Store"
while read line; do
    trimmed_line=$(echo "$line" | sed 's/^[[:space:]]*//;s/
[[:space:]]*$//')
    #printf "line='%s'\n" $line
    #printf "trimmed_line='%s'\n" $trimmed_line
    sfile="@"$tdate"_"$trimmed_line".json"
    dfile=$objstore$tdate"_"$trimmed_line".json"
```

```
        curl -X PUT --data-binary $sfile $dfile
        echo "File" $n ":" $sfile
        echo "File" $n ":" $dfile
    n=$((n+1))
done < $filename
    swfile="@"$tdate"_filewatcher.txt"
    dwfile=$objstore$tdate"_filewatcher.txt"
        curl -X PUT --data-binary $swfile $dwfile
        echo "File" $n ":" $swfile
echo "End of Copy files to Object Store"
```

Where <<OBJECT_STORAGE_PAR_URL>> is the URL string obtained from Admin Console.

d. Create a file named “filename.txt” and add the file contents as follows:
For Single input file:

```
RUN<<RUN_NUMBER>>_STG_TRANSACTIONS_ENTRY_1
```

Where <<RUN_NUMBER>> is the positive number used for batch Run.

For Multiple input files:

```
RUN<<RUN_NUMBER>>_STG_TRANSACTIONS_ENTRY_1
RUN<<RUN_NUMBER>>_STG_TRANSACTIONS_ENTRY_2
RUN<<RUN_NUMBER>>_STG_TRANSACTIONS_ENTRY_3
```

> **Note**
>
> i. The new line is mandatory at the end of last file name.
>
> ii. Default Batch accepts only STG_TRANSACTIONS_ENTRY file pattern. To change this, clone the following pipelines (Data Loading File Transfer Transaction Filtering and Load Transaction Filter Data) and change the input parameter “**fileName**” value in external service. Then Clone the associated jobs, attach the cloned pipeline and Save the job. Then, Change the Task Parameter “**$JOBNAME$**” value in two tasks “**DataLoadingFileTransfer**” and “**TransFilterPipeline**” respectively. Refer Pipeline Designer user guide.

7.2 Steps to Run a ISO20022 Batch

1. Create a file named `<<BATCH_DATE>_RUN<<RUN_NUMBER>>_STG_TRANSACTIONS_ENTRY_<<DIGIT>>.json`.

   Where

   - `<BATCH_DATE>` is date used for “ISO20022BatchScreening” Batch run. Format:yyyyMMdd.
   - `<RUN_NUMBER>`is Any Positive number used for “ISO20022BatchScreening” Batch run.
   - `<DIGIT>` is Any Positive number to represent the uniqueness of file. E.g.20241017_RUN1_ STG_TRANSACTIONS_ENTRY_1.json

> **Note**
>
> You can create multiple input json files for single batch run.

2. File contents must be in valid json format.
   a. Example of Single Transaction in a file.

```
[
      {
"rawMessage":"<<RAW_MESSAGE_STRING>>",
"businessDomainCode":"GEN",
"jurisdictionCode":"AMEA",
"messageDirection":"INBOUND",
"additionalData" :
        {
        "MESSAGE_DIRECTION":"INBOUND"
        }
    }
]
```

   b. Example of Multiple Transactions in a file.

```
[
      {
"rawMessage":"<<RAW_MESSAGE_STRING>>",
"businessDomainCode":"GEN",
"jurisdictionCode":"AMEA",
"messageDirection":"INBOUND",
"additionalData" :
        {
        "MESSAGE_DIRECTION":"INBOUND"
        }
},
{
"rawMessage":"<<RAW_MESSAGE_STRING>>",
"businessDomainCode":"GEN",
"jurisdictionCode":"AMEA",
"messageDirection":"INBOUND",
"additionalData" :
        {
        "MESSAGE_DIRECTION":"INBOUND"
        }
}
]
```

3. Once the files are created, and place the input files inside the **ISO20022_Batch_InputData_Upload_Utility** folder.
4. Create an empty filewatcher text file named “<<BATCH_DATE>>_filewatcher.txt" inside the utility folder.

   Where <BATCH_DATE> is date used for “ISO20022BatchScreening” Batch run. Format:yyyyMMdd.

> **Note**
>
> a. The File Watcher text file with corresponding batch date is mandatory for the batch to run.
>
> b. If any input files created for a new date, filewatcher should also be created with same date.

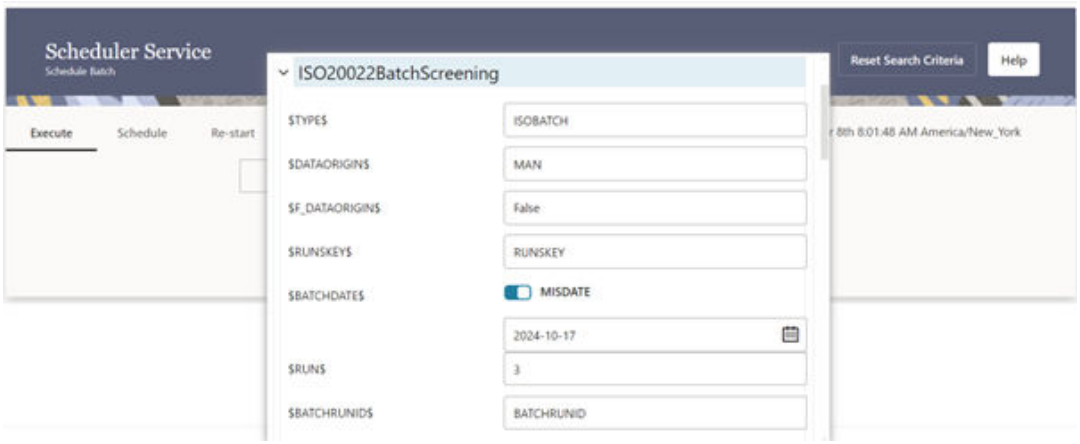
5. Add the prefix name of input json files in `filename.txt`. Refer to the Prerequisties section to add the file name prefixes.
6. To upload the input data files to Object storage, Open the terminal, and run `./cto.sh <<BATCH_DATE>>`

   For Example: ./cto.sh 20241017

> **Note**
>
> a. The **cto.sh** file contains Object Storage PAR URL as a variable “objstore”. This URL get refreshed every day in admin console. Use the latest Object Storage PAR URL from admin console using Access the Object Storage Pre-authenticated URLAccess the Object Storage Pre-authenticated URL.

7. Once the input file upload is successful, Open Application URL and Navigate to **Batch Administration>Scheduler**.
8. In the **Schedule Service** Screen, click ‘**Schedule Batch**’ Navigation and under **Execute** Tab, then select the Batch as “**ISO20022BatchScreening**”.
9. Click **Edit Parameters** button. The Edit Dynamic Params Dialog appears.

Figure 7-1 Edit Parameters



10. Under the Batch Parameters, for Param $BATCHDATE$, enable MISDATE and select the date as <<BATCH_DATE>> which is given in the input file name.
11. For Param RUN, enter the <<RUN_NUMBER>> which is given in input file name.
12. Click **Save**.
13. To run the batch, click the **Execute** button.

14. A confirmation popup appears. Click the **Monitor** button to monitor the batch.
15. Once the batch is successful, call the following API with appropriate headers to get the download URL.

    ```
    GET <<BASE_URL>>/feedback-service/iso20022-batch/getFeedbackParURL?
    runNumber=<<RUN_NUMBER>>&batchDate=<<BATCH_DATE>>
    ```

    Refer API Documentation for More Information.

    > **Note**
    >
    > The Download URL expiry date is 15 days. If any expiry happens, use the Following API to get the new Download URL.
    >
    > ```
    > POST <<BASE_URL>>/feedback-service/iso20022-batch/
    > uploadFeedbackToObjectStorage?
    > runNumber=<<RUN_NUMBER>>&batchDate=<<BATCH_DATE>>
    > ```

16. Using the URL, download the immediate feedback zip file which contains json file(s) with content as transaction token, input data, and feedback data for each transaction.
17. Then, navigate to Schedule Batch and under Execute tab, select the batch as “ISOBatchScreeningToCaseManagement”.

    > **Note**
    >
    > a. Make sure the “$DATAORIGIN$” Batch Parameter used is same in both the batches.
    >
    > b. As a pre-requisite for ISOBatchScreeningToCaseManagement Batch, “Maintenance” batch must be executed once in a setup for corresponding “$DATAORIGIN$” before triggering the above batch. It is a one-time activity in the application.

18. Then, click **Execute**.
19. Click **Monitor** to monitor the batch.
20. Once the batch is successful, cases are generated for given transactions.
21. Use the Following Feedback API to get the feedback with case Id or to get the final feedback.

    ```
    GET <<BASE_URL>>/feedback-service/Feedback/findByID?
    messageType=3&transactionToken=<<TRANSACTION_TOKEN>>
    ```
    Where `<TRANSACTION_TOKEN>>` - It can be obtained in immediate Feedback json file for each transaction.

    Refer API Documentation for More Information.

Table 7-1 Task Details for ISO20022BatchScreening

Task ID	Task Name	Task Description
Task1	StartDataLoad	Starts the Batch

Table 7-1 (Cont.) Task Details for ISO20022BatchScreening

Task ID	Task Name	Task Description
Task2	DataLoadingFileTransfer	Downloads Input Files from the Object Storage and Transfers it to the FSS (File Storage Service) location.
Task3	DataLoadingFileScanner	Scans the files in the FSS location for virus detection.
Task4	TransFilterPipeline	Reads the data from json files in the FSS location and insert the data into the batch repository and the batch transaction tables.
Task5	TransactionInputProcess	Fetches the input data from the batch transaction table, then processes it and insert them into pre-processing tables.
Task6	ISO20022DataTransform	Transforms the input data for provided rules under each webservice and persists them into transformed table.
Task7	TransactionSourceDataLoad	Loads the transformed data as indexes into Matching Engine.
Task8	ISO20022BulkMatching	Performs screening of data, scoring, decision making, generating Immediate Feedback, highlighting Raw data, and Creating TF Alerts.
Task9	GatherStats	Gathers statistics for the loaded tables.
Task10	EndDataLoad	Ends the Batch.

Note

a. Both batches must be run successfully, one after the other.

b. If the batch run fails because of the server down issue, you must try to restart the batch. It will re-start from the failed task.

c. Re-run option will create a new run for the batch with new batch run Id.

7.3 Purge Batches Available for ISO20022 Batch

Purge Batches are used to delete the data for particular batch run ID if required in case of any batch failures.

For more information see thePurge Batch details topic in the Pipleline Designer guide.

1. **PurgeISO20022BatchTables**

   Click **Edit Parameters**, enter Task Parameter "**$FCCMBATCHRUNID$**" with corresponding Batch Run Id for "**ISO20022BatchScreening**", then save and execute the Batch.

2. **PurgeCMTables**

Click **Edit Parameters**, enter Task Parameter "**$FCCMBATCHRUNID$**" with corresponding Batch Run Id for "**ISOBatchScreeningToCaseManagement**", then save and execute the Batch.

> **Note**
>
> Make sure the "$DATAORIGIN$" batch param used here is same as in ISO20022 Batches.

8
Run the NACHA Batch Screening

The NACHA transaction messages can be processed in bulk using batches such as “**NACHABatchScreening**” and “**NACHABatchScreeningToCaseManagement**”. Input Transaction Files are accepted in the .json format and it can be either single json file with list of all transactions or multiple json files with list of transactions. Input transactions will be processed, screened and feedback file will be generated in the .json format.

For managing the above batches, refer Transaction Filtering Screening Batches Details.

Operations of NACHA Batches:

1. **NACHABatchScreening** – – This batch performs Download the Transaction files from Object Storage, Load the transactions into tables, Parse the raw messages, Transform data, Load transformed data to Matching Engine, Screen the Data against Watchlist and create Events, Generate Score, Make HOLD/CLEAN decision along with Exemption/Alert Suppression, Generate TF immediate Feedback and Upload to Object Storage, Highlight Raw Message, and Create TF Alerts.
2. **NACHABatchScreeningToCaseManagement** – This batch performs Generate Cases for created Alerts using Case Management Tasks and Update TF Feedback with Case Id.

8.1 Prerequisites

1. Access the Object Storage Pre-authenticated URL form Admin Console. For more information see Access the Object Storage Pre-authenticated URL.
2. Setup the upload Transaction Files to Object Storage Utility.
   a. In any Linux environment, create a new folder. E.g. NACHA_Batch_InputData_Upload_Utility.
   b. Change the directory inside the newly created folder.
   c. Create a file named “cto.sh” and paste the below contents.

```
#!/bin/bash
filename='filename.txt'

n=1
tdate=$1

echo "Entered FIC MIS Date is: " $tdate
objstore="<<OBJECT_STORAGE_PAR_URL>>"

echo "Start Copy files to Object Store"
while read line; do
    trimmed_line=$(echo "$line" | sed 's/^[[:space:]]*//;s/
[[:space:]]*$//')
    #printf "line='%s'\n" $line
    #printf "trimmed_line='%s'\n" $trimmed_line
    sfile="@"$tdate"_"$trimmed_line".json"
    dfile=$objstore$tdate"_"$trimmed_line".json"
```

```
        curl -X PUT --data-binary $sfile $dfile
        echo "File" $n ":" $sfile
        echo "File" $n ":" $dfile
    n=$((n+1))
done < $filename
    swfile="@"$tdate"_filewatcher.txt"
    dwfile=$objstore$tdate"_filewatcher.txt"
        curl -X PUT --data-binary $swfile $dwfile
        echo "File" $n ":" $swfile
echo "End of Copy files to Object Store"
```

Where <<OBJECT_STORAGE_PAR_URL>> is the URL string obtained from Admin Console.

d. Create a file named “filename.txt” and add the file contents as follows:
For Single input file:

```
RUN<<RUN_NUMBER>>_ACH_STG_TRANSACTIONS_ENTRY_1
```

Where <<RUN_NUMBER>> is the positive number used for batch Run.

For Multiple input files:

```
RUN<<RUN_NUMBER>>_ACH_STG_TRANSACTIONS_ENTRY_1
RUN<<RUN_NUMBER>>_ACH_STG_TRANSACTIONS_ENTRY_2
RUN<<RUN_NUMBER>>_ACH_STG_TRANSACTIONS_ENTRY_3
```

> **Note**
>
> i. The new line is mandatory at the end of last file name.
>
> ii. Default Batch accepts only STG_TRANSACTIONS_ENTRY file pattern. To change this, clone the following pipelines (Nacha Data Loading File Transfer and Nacha Load Transaction Filter Data) and change the input parameter “**fileName**” value in external service. Then Clone the associated jobs, attach the cloned pipeline and Save the job. Then, Change the Task Parameter “**$JOBNAME$**” value in two tasks “**NachaDataLoadingFileTransfer**” and “**NachaLoadTransactionFilterData**” respectively. Refer Pipeline Designer user guide.

8.2 Steps to Run a NACHA Batch

1. Create a file named <<BATCH_DATE>_RUN<<RUN_NUMBER>>_ACH_STG_TRANSACTIONS_ENTRY_<<DIGIT>>.json.

   Where

   - <BATCH_DATE> is date used for “NACHABatchScreening” Batch run. Format:yyyyMMdd.
   - <RUN_NUMBER>is Any Positive number used for “NACHABatchScreening” Batch run.
   - <DIGIT> is Any Positive number to represent the uniqueness of file. E.g.20251017_RUN1_ ACH_STG_TRANSACTIONS_ENTRY_1.json

> **Note**
>
> You can create multiple input json files for single batch run.

2. File contents must be in valid json format.
   a. Example of Single Transaction in a file.

```
[
      {
"rawMessage":"<<RAW_MESSAGE_STRING>>",
"businessDomainCode":"GEN",
"jurisdictionCode":"AMEA",
"messageDirection":"INBOUND",
"additionalData" :
        {
        "MESSAGE_DIRECTION":"INBOUND"
        }
    }
]
```

   b. Example of Multiple Transactions in a file.

```
[
      {
"rawMessage":"<<RAW_MESSAGE_STRING>>",
"businessDomainCode":"GEN",
"jurisdictionCode":"AMEA",
"messageDirection":"INBOUND",
"additionalData" :
        {
        "MESSAGE_DIRECTION":"INBOUND"
        }
},
{
"rawMessage":"<<RAW_MESSAGE_STRING>>",
"businessDomainCode":"GEN",
"jurisdictionCode":"AMEA",
"messageDirection":"INBOUND",
"additionalData" :
        {
        "MESSAGE_DIRECTION":"INBOUND"
        }
}
]
```

3. Once the files are created, and place the input files inside the **NACHA_Batch_InputData_Upload_Utility** folder.
4. Create an empty filewatcher text file named “<<BATCH_DATE>>_filewatcher.txt" inside the utility folder.

   Where <BATCH_DATE> is date used for “NACHABatchScreening” Batch run. Format:yyyyMMdd.

> **Note**
>
> a. The File Watcher text file with corresponding batch date is mandatory for the batch to run.
>
> b. If any input files created for a new date, filewatcher should also be created with same date.

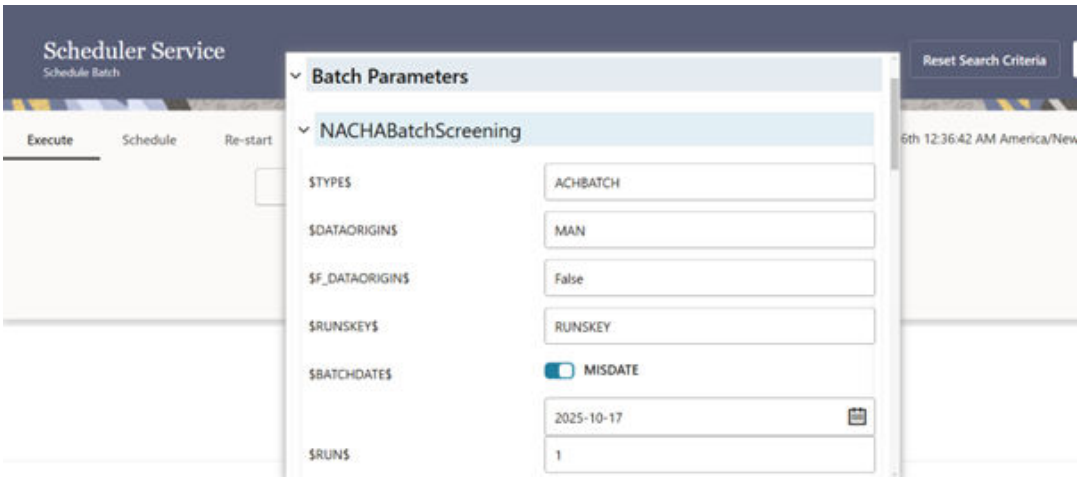
5. Add the prefix name of input json files in `filename.txt`. Refer to the Prerequisties section to add the file name prefixes.
6. To upload the input data files to Object storage, Open the terminal, and run `./cto.sh <<BATCH_DATE>>`

   For Example: ./cto.sh 20251017

> **Note**
>
> a. The **cto.sh** file contains Object Storage PAR URL as a variable “objstore”. This URL get refreshed every day in admin console. Use the latest Object Storage PAR URL from admin console using Access the Object Storage Pre-authenticated URLAccess the Object Storage Pre-authenticated URL.

7. Once the input file upload is successful, Open Application URL and Navigate to **Batch Administration>Scheduler**.
8. In the **Schedule Service** Screen, click ‘**Schedule Batch**’ Navigation and under **Execute** Tab, then select the Batch as “**NACHABatchScreening**”.
9. Click **Edit Parameters** button. The Edit Dynamic Params Dialog appears.

Figure 8-1 Edit Parameters



10. Under the Batch Parameters, for Param $BATCHDATE$, enable MISDATE and select the date as <<BATCH_DATE>> which is given in the input file name.
11. For Param RUN, enter the <<RUN_NUMBER>> which is given in input file name.
12. Click **Save**.

13. To run the batch, click the **Execute** button.
14. A confirmation pop-up appears. Click the **Monitor** button to monitor the batch.
15. Once the batch is successful, call the following API with appropriate headers to get the download URL.

    ```
    GGET <<BASE_URL>>/feedback-service/batch/getFeedbackParURL?
    runNumber=<<RUN_NUMBER>>&batchDate=<<BATCH_DATE>>&batchType=ACHBATCH
    ```

    Refer API Documentation for More Information.

    > **Note**
    >
    > The Download URL expiry date is 15 days. If any expiry happens, use the Following API to get the new Download URL.
    >
    > ```
    > POST <<BASE_URL>>/feedback-service/batch/
    > uploadFeedbackToObjectStorage?
    > runNumber=<<RUN_NUMBER>>&batchDate=<<BATCH_DATE>>&batchType=ACHBATCH
    > ```

16. Using the URL, download the immediate feedback zip file which contains json file(s) with content as transaction token, input data, and feedback data for each transaction.
17. Then, navigate to Schedule Batch and under Execute tab, select the batch as “NACHABatchScreeningToCaseManagement”.

    > **Note**
    >
    > a. Make sure the “$DATAORIGIN$” Batch Parameter used is same in both the batches.
    >
    > b. As a pre-requisite for NACHABatchScreeningToCaseManagement Batch, “Maintenance” batch must be executed once in a setup for corresponding “$DATAORIGIN$” before triggering the above batch. It is a one-time activity in the application.

18. Then, click **Execute**.
19. Click **Monitor** to monitor the batch.
20. Once the batch is successful, cases are generated for given transactions.
21. Use the Following Feedback API to get the feedback with case Id or to get the final feedback.

    ```
    GET <<BASE_URL>>/feedback-service/Feedback/findByID?
    messageType=3&transactionToken=<<TRANSACTION_TOKEN>>
    ```
    Where `<TRANSACTION_TOKEN>>` - It can be obtained in immediate Feedback json file for each transaction.

    Refer API Documentation for More Information.

Table 8-1 Task Details for NACHABatchScreening

Task ID	Task Name	Task Description
Task1	StartDataLoad	Starts the Batch

Table 8-1 (Cont.) Task Details for NACHABatchScreening

Task ID	Task Name	Task Description
Task2	NachaDataLoadingFileTransfer	Downloads Input Files from the Object Storage and Transfers it to the FSS (File Storage Service) location.
Task3	NachaDataLoadingFileScanner	Scans the files in the FSS location for virus detection.
Task4	NachaLoadTransactionFilterDat a	Reads the data from json files in the FSS location and insert the data into the batch repository and the batch transaction tables.
Task5	NachaTransactionInputProcess	Fetches the input data from the batch transaction table, then processes it and insert them into pre-processing tables.
Task6	NachaDataTransform	Transforms the input data for provided rules under each webservice and persists them into transformed table.
Task7	NachaSourceDataLoad	Loads the transformed data as indexes into Matching Engine.
Task8	NachaBulkMatching	Performs screening of data, scoring, decision making, generating Immediate Feedback, highlighting Raw data, and Creating TF Alerts.
Task9	EndDataLoad	Ends the Batch.

Note

a. Both batches must be run successfully, one after the other.

b. If the batch run fails because of the server down issue, you must try to restart the batch. It will re-start from the failed task.

c. Re-run option will create a new run for the batch with new batch run Id.

8.3 Purge Batches Available for NACHA Batch

Purge Batches are used to delete the data for particular batch run ID if required in case of any batch failures.

For more information see thePurge Batch details topic in the Pipleline Designer guide.

1. **PurgeNachaBatchTables**

   Click **Edit Parameters**, enter Task Parameter "**$FCCMBATCHRUNID$**" with corresponding Batch Run Id for "**NACHABatchScreening**", then save and execute the Batch.

2. **PurgeCMTables**

Click **Edit Parameters**, enter Task Parameter "**$FCCMBATCHRUNID$**" with corresponding Batch Run Id for "**NACHBatchScreeningToCaseManagement**", then save and execute the Batch.

> **Note**
>
> Make sure the "$DATAORIGIN$" batch param used here is same as in NACHA Batches.

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
- NACHA 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.026.001.09	2	camt.027.001.09	3	camt.028.001.11	4	camt.029.001.11
5	camt.031.001.06	6	camt.032.001.04	7	camt.033.001.06	8	camt.038.001.04
9	Camt.050.001.05	10	camt.052.001.08	11	camt.052.001.10	12	camt.053.001.08
13	camt.053.001.10	14	camt.054.001.08	15	camt.054.001.09	16	camt.054.001.10
17	camt.056.001.10	18	camt.060.001.05	19	camt.060.001.06	20	camt.087.001.08
21	pacs.002.001.12	22	Pacs.003.001.02	23	pacs.003.001.10	24	Pacs.004.001.09
25	pacs.004.001.12	26	Pacs.008.001.02	27	Pacs.008.001.07	28	Pacs.008.001.08
29	pacs.008.001.11	30	Pacs.009.001.08	31	pacs.009.001.10	32	Pacs.010.001.03
33	pacs.010.001.05	34	pacs.028.001.05	35	Pain.001.001.08	36	Pain.001.001.09

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		

A.4 NACHA Message Types

For the NACHA message category, the following message types are the ready-to-use message types that you can use after you log in.

NACHA message types:

- CTX
- IAT
- RCK
- PPD
- CCD
- TEL
- WEB
- POP
- CIE
- ARC
- BOC