Oracle® Financial Crime and Compliance Management Cloud Service

Using Pipeline Designer

Release 24.2.1
F93581-01
January 2015

Oracle Financial Crime and Compliance Management Cloud Service Using Pipeline Designer, Release 24.2.1

F93581-01

Primary Authors: (primary author), (primary author)

Contributing Authors: (contributing author), (contributing author)

Contributors: (contributor), (contributor)

Contents

5 Managing Scenario Pipelines

6 Managing Scoring Pipelines

7 Managing Customer Screening Pipelines

8 Managing Transaction Filtering Pipelines

9 Configuring KYC Risk

10 Managing KYC Onboarding Pipelines

11 Managing KYC Batch Pipelines

12 Managing KYC Risk Factor Pipelines

13 Configuring Customer Watchlists

14 Managing Watch List Pipelines

15 Managing Threshold Sets

16 Extending the Data Model

17 Managing Data Extraction API Pipelines

18 Using Jobs

19 Managing Batches

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.

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.

This documentation is in preproduction status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

1 Preface

This preface introduces information sources that can help you use the application.

The following sections provide information that can help you use the application.

Audience

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

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.

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.

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/.

2 Overview

Oracle Financial Crime and Compliance Management Cloud Services use the Pipeline Designer to create, configure, and manage pipelines.

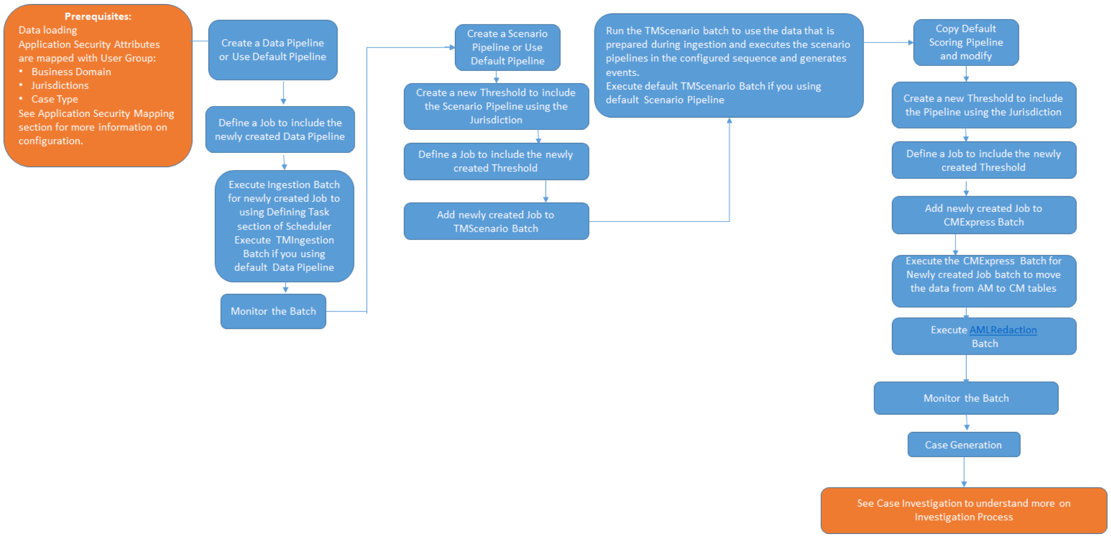
A pipeline is an embedded data processing engine that runs inside the application to filter, transform, and migrate data on-the-fly. Pipelines are a set of data processing elements called widgets connected in series, where the output of one widget is the input to the next element.

The types of pipelines are:

- Data Pipelines
- Scenario Pipelines
- Scoring Pipelines
- Customer Screening Pipelines
- KYC Onboarding Pipelines
- Watch List Pipelines

In addition, the application also includes ready-to-use pipelines to process Customer, Account, and Transaction datasets for scenarios to be run. Loading the datasets includes the ability to run data quality checks on the data.

Figure 2-1 Pipeline Workflow


Prerequisites:
Data loading
Application Security Attributes are mapped with User Group:
• Business Domain
• Jurisdictions
• Case Type
See Application Security Mapping section for more information on configuration.
Create a Data Pipeline or Use Default Pipeline
Define a Job to include the newly created Data Pipeline
Execute Ingestion Batch for newly created Job to using Defining Task section of Scheduler Execute TMIngestion Batch if you using default Data Pipeline
Monitor the Batch
Create a Scenario Pipeline or Use Default Pipeline
Create a new Threshold to include the Scenario Pipeline using the Jurisdiction
Define a Job to include the newly created Threshold
Add newly created Job to TMScenario Batch
Run the TMScenario batch to use the data that is prepared during ingestion and executes the scenario pipelines in the configured sequence and generates events.
Execute default TMScenario Batch if you using default Scenario Pipeline
Copy Default Scoring Pipeline and modify
Create a new Threshold to include the Pipeline using the Jurisdiction
Define a Job to include the newly created Threshold
Add newly created Job to CMExpress Batch
Execute the CMExpress Batch for Newly created Job batch to move the data from AM to CM tables
Execute AMLRedaction Batch
Monitor the Batch
Case Generation
See Case Investigation to understand more on Investigation Process

3

Getting Started

You must import the pre-configured pipelines into your implementation. Then you can create and edit pipelines to meet your implementation's requirements.

This section explains how to perform the initial import of pre-configured pipelines during setup, and how to upload and download pipelines to the application.

Importing Pipelines

Administrators are responsible for uploading pre-configured pipelines once during initial setup.

This is a mandatory step. You must upload these pipelines to the environment as part of the initial setup, using the **Import Pipelines** feature.

1. Navigate to the **Applications** landing page.
2. Click the Navigation Menu ☰ to access the **Navigation List**. The Navigation List displays the list of modules.
3. Click **Pipeline Administration**. The Administration page is displayed.
4. Follow these steps:
    - **(Mandatory) Import metadata**
        a. Click **Import Metadata**. The metadata is imported and a confirmation message is displayed.
    - **Import all ready-to-use pipelines**
        a. Select **Import All Pipelines** in the Import Pipelines pane. By default, the Import All Pipelines check box is selected.
        b. Click **Import**. All the ready-to-use pipelines are imported.
    - **Import selected pipelines:**
        a. Enter the required version of the pipeline to import in the Versions drop-down list. The latest version displays by default.
        b. Select the required pipelines to import from the **Pipelines** drop-down list.
        c. Click **Import**. The selected pipelines are imported.

> **Note:**
>
> If you attempt to upload a pipeline which has already been imported, an error message will display.

Downloading Pipelines

The Download/Upload Pipelines feature enables you to download and upload the pipelines available in the application.

The pipelines are saved in JSON format which can be uploaded again to the application.

1. Navigate to the **Administration** page.
2. Click **Download**. The Download Pipeline dialog box displays.
3. Enter the required version of the pipeline to download in the **Pipeline Version** field. You can only enter numerals here.
4. Select the required pipeline to download from the **Pipelines** drop-down list.
5. Click **Download**. The Status dialog box displays *Download Complete*.

Uploading Pipelines

The Upload Pipelines feature enables you to upload the pipelines available in the application.

The Upload Pipelines feature enables you to upload the pipelines available in the application.

1. Navigate to the Administration page.
2. Click **Upload**. The Upload Pipeline dialog box displays.
3. Enter the version of the pipeline to upload in the **Pipeline Version** field. You can only enter numerals here.
4. Select the pipeline to upload from your machine using the **Choose File** button.
5. Click **Upload**. The Status dialog box displays *Upload Complete*.

Copying Pipelines

After importing the ready-to-use pipelines to the application, you may want to configure them to meet your specific business needs.

In order to customize these pipelines, you must first create a copy of those pipelines and save it as a new pipeline. You can then configure the newly copied pipeline according to your requirements.

1. Navigate to the Pipeline Designer page.
2. Click **Copy** ⧉ corresponding to the pipeline that you want to modify. The Copy Pipeline dialog box is displayed.
3. Provide the details as described in the following table.

Table 3-1 Fields for Copying Pipelines and their Descriptions

Field	Description
Pipeline to Copy	Displays the name of the pipeline that you want to copy.
Copy As	Enter the name for the new pipeline that you want to create by copying the existing pipeline.
Description	Enter the description for the pipeline.
Add Search Tags	Enter the keywords for the pipeline. These keywords can be used as search tags while searching for a pipeline. Search tags are also used to group pipelines of the same type. These search tags appear as filters in the pipeline page.
Type	Displays the type of pipeline, such as Watchlist, Scenario, Scoring, Staging Data Loading, or Data Transformation.

> **Note:**
>
> Do not update the Type of data loading, such as SCD, Full load, or Merge

4. Click **Submit**. The pipeline is copied.

Creating Pipelines

You can create a new pipeline and then configure the pipeline based on your needs.

To create a new pipeline, follow these steps:.

1. Navigate to the Pipeline Designer page.
2. Click **Add** ⊞in the upper-right corner. The New Pipeline dialog box is displayed.
3. Provide the details as described in the following table.

Table 3-2 Fields for Creating Pipelines and their Descriptions

Field	Description
Name	Enter the name for the pipeline.
Description	Enter the description for the pipeline.
Add Search Tags	Enter the keywords for the pipeline. These keywords can be used as search tags while searching for a pipeline. Search tags are also used to group pipelines of the same type. These search tags appear as filters in the Pipeline page.
Type	Select the type of pipeline as either Scenario, Scoring, Data Loading, or Data.

4. Click **Create**. A new pipeline is created and displayed in the Pipeline page. You can perform the required configurations in the newly created pipeline.

Configuring Pipelines

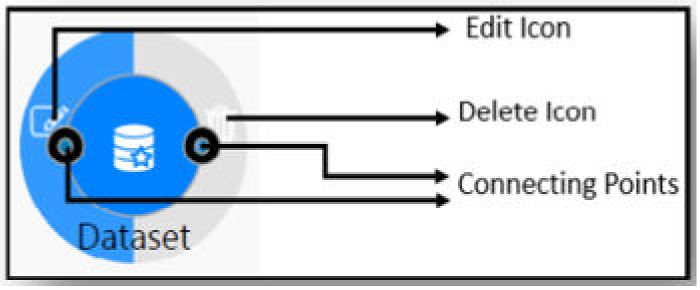
You can configure pipelines that you have created as your requirements change.

To configure pipelines, follow these steps.

> **Note:**
>
> Pre-configured pipelines cannot be edited. You can only edit user-defined pipelines.

1. Navigate to the Pipeline Designer page.
2. Click the name of the pipeline that you want to configure. The pipeline opens in the Pipeline Designer page.
3. Drag and drop the required widgets from the widgets pane located in the upper-right corner of the designer pane.
4. Hover over a widget and click **Edit** ✎ to configure a widget.

Figure 3-1 Dataset Widget Details



For more information on the widgets in the various types of pipelines, see the following sections:

- Widgets in Data Pipelines
- Widgets in Scenario Pipeline
- Widgets in Scoring Pipelines
- Widgets in Customer Screening Pipelines
- Widgets in Transaction Filtering Pipelines
- Widgets in KYC Onboarding Pipelines
- Widgets in KYC Batch Pipelines
- Widgets in KYC Risk Factor Pipelines
- Widgets in Watch List Pipelines

5. Click and hold the connecting point of a widget, and drag and drop to the connecting point of another widget to connect the widgets. If you do not connect the widgets to complete the flow of the pipeline, your pipeline will not work as expected.
6. Click **Save** ✓.The Pipeline Save dialog box is displayed.

Editing Pipeline Descriptions

You can edit the description and search tags for user-created pipelines.

To edit the description and search tags, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Click **Edit** ✎ corresponding to the pipeline that you want to modify. The Edit Pipeline dialog box is displayed.
3. Modify the required details.

> **Note:**
>
> Pre-configured pipelines cannot be edited. You can only edit user-defined pipelines

Deleting Pipelines

You can delete a pipeline, if required for your implementation.

To delete a pipeline, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Click **Delete** 🗑 corresponding to the pipeline that you want to delete. The selected pipeline is deleted.

Downloading Metadata Snippet

The Metadata snippet shows how your scenario pipeline is configured, in detail.

The Metadata snippet contains information about the pipeline such as the name, description, the dataset the scenario is using, segments and evaluations configured for the scenario, and so on. In addition, it provides the pipeline diagram. This metadata can be used to help auditors understand the logic and parameters of your scenario, as it is currently configured.

> **Note:**
>
> This feature is available only for Scenario Pipelines.

1. Navigate to the Pipeline Designer page.

2. Click **Download** corresponding to the scenario pipeline for which you want to download the metadata snippet. The metadata snippet for the selected pipeline is downloaded in .html format.

4 Managing Data Pipelines

Data pipelines prepare filtered data which can be used to create and run scenarios.

Data pipelines prepare data by selecting and joining data sources to create virtual tables of data, adding derived attributes to data, running derivations on the data to determine the risk associated with the entity, and so on.

Data pipelines are categorized according to function, into the following types:

- Data pipelines which prepare the data and make it compatible for use in Oracle FCCM Cloud products.
- Data pipelines which move the evented data to Case Management (CM) for further action.

Pre-configured Data Pipelines

FCCM TM Cloud Service provides a set of pre-configured data pipelines.

The application comes with the following ready-to-use data pipelines:

Data Pipelines which prepare data:

- Account Data Movement Pipeline
- Case Dat
- a Movement Pipeline
- City Data Load
- Country Data Load
- Customer Data Movement Pipeline
- Transaction Data Movement Pipeline
- Event Data Movement Pipeline
- Evented Account Data Movement Pipeline
- Evented Customer Data Movement Pipeline
- Evented External Entity and Derive Address Data Movement Pipeline
- Evented Transaction Data Movement Pipeline
- External Entity and Derive Address Data Movement Pipeline
- Goods Data Load
- Load Additional Account Data
- Load Account Anticipatory Profile Data
- Load Account Data
- Load Account Group Data
- Load and Prepare Watchlists

- Load Customer Add On Data
- Load Customer Anticipatory Profile Data
- Load Customer Data
- Load Customer Mapping Data
- Load Identifier
- Load Intermediate Account and Transaction Data
- Load Transaction Data and Derive External Entities and Risk
- Derive Risk and Load Supplementary Information
- Load Account Staging Data
- Load Customer Staging Data
- Load Transaction Staging Data
- Load Watchlist Staging Data
- Data Loading File Transfer
- Data Loading File Scanner
- Data Truncate Holiday Master
- Data Loading File Transfer Holiday Data
- Load Holiday Master Data
- Load Correspondent Bank
- Port Data Load
- StopKeyword Watchlist

Data Pipelines which move data to Case Management:

- Load Account Business Data to Case Management
- Load Calendar Data
- Load Case Data
- Load Customer Business Data to Case Management
- Load Evented Account Data to Case Management
- Load Evented Customer Data to Case Management
- Load Evented External Entity and Derived Address Data to Case Management
- Load Evented Transaction Data to Case Management
- Load Event Data to Case Management
- Load External Entity and Derived Address Data to Case Management
- Load Scenario Data to Case Management
- Load Transaction Business Data to Case Management
- Load Trusted Pair Data

Data Pipelines which prepare data for Investigation Hub:

- Business Data Load for CS
- Business Data Load for KYC

- Data Loading File Transfer CS
- Data Loading File Transfer KYC

Pipelines which are used to maintain data:

- Apply Redaction Policy
- Create Batch Redaction Policy
- Drop Batch Redact Policy
- Delete Business Data
- Delete Case Management Data
- Delete Staging Data

Widgets in Data Pipelines

Depending on the pipeline type, specific widgets are available in the widgets pane of the pipeline.

The following table describes the widgets available in Data pipelines. For more information about the widgets available in Scenario Pipelines, see Widgets in Scenario Pipeline.

Table 4-1 Data Pipeline – Widgets and Descriptions

Widget	Name	Description
🛢	Dataset	Use this widget to add a Dataset. Datasets correspond to the contents of a single database table which can be a staging table, business table, or a table that has been created by a data pipeline. A data pipeline must always begin with a Dataset widget.
▼	Filter	Use this widget to filter the data in the pipeline to use a subset of the data records which are available. On applying a filter, all data matching the filter conditions are obtained. This allows you to search and analyze behaviors of interest.
⊞	Join	Use this widget to combine or group multiple tables using various join operators.
⚙	Persist	Use this widget to write data to database tables so that it can be used in other pipelines.
⧉	External Service	Use this widget to add an external service. External Services perform actions on the data, such as loading or moving the data, or performing a virus scan.

Creating External Service

External Service refers to an existing set of services that the customer can use to derive the risk of certain business entities, configure data movement for case management, create events, and so on.

A business entity refers to parameters such as customer, account, transaction, and so on. To create an external service, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Drag and drop the External Service widget from the widgets pane to the designer pane.
3. Hover over the External Service widget and click **Edit** ✎. The External Service pane is displayed.
4. Select the external service from the Name drop-down list.
5. Based on the external service selected, the following details are auto-populated:
   - The description for the external service is auto-displayed in the Description field.
   - The corresponding details of the selected external service are displayed in a table. The details include parameter names and parameter values associated with the External Service.
6. Click **Save** ✓ to save the changes. The external service is created.

   You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see Common Tasks.

Creating Filters Using the Filter Widget

The Filter widget defines criteria that filter the data in the pipeline to use a subset of the data records which are available.

On applying a filter, the data matching the filter conditions are obtained which can be used to search and analyze behaviors of interest. To create a filter, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Drag and drop the Filter widget from the widgets pane to the designer pane.
3. Hover on the Filter widget and click **Edit** ✎. The Filter pane is displayed.
4. Enter the name for the filter in the **Name** field.
5. Navigate to the **Filter** pane. The Output pane is displayed.
6. Configure the filter. For more information, see Configuring Filters.

Creating Joins

The Join widget enables you to combine or group multiple tables using various join operators.

To create a join, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Drag and drop the Join widget from the widgets pane to the designer pane.
3. Hover on the Join widget and click **Edit** ✎. A dialog box is displayed.
4. Enter the name in the **Name** field.
5. Follow these steps in the **Output** pane:
   a. Select the required tables from the drop-down lists on the left-hand side and right-hand side that you want to join.
   b. Select the join operators to join the two tables. For more information, see Join Operators.
6. Add a Join condition to the Join table to save the widget.
7. To add a condition, click **Add +** on the right (Add Group and then Add Condition) and specify rules for the condition. You can add multiple groups and multiple conditions under each group.
8. Click **Save** ✓ to save the changes. The join widget is created.
9. You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see Common Tasks.

Join Operators

Join operators are used to join tables in the Output pane.

Join operators are used to join tables in the Output pane. The following types of join operators are available:

- **Inner Join:**The Inner Join selects all rows from both participating tables as long as there is a match between the columns.
- **Left Join:** The Left Join returns all rows from the left table, with the matching rows in the right table.
- **Right Join:** The Right Join returns all rows from the right table, with the matching rows in the left table.
- **Full Join:** The Full Join combines the results of both the left and right outer joins and returns all rows from the tables on both sides

Creating Persist

The Persist widget enables you to write data to database tables so that it can be used in other pipelines.

This widget is used to map columns of the source table to a destination table. The Persist widget helps you to map attributes from the input datasets to the target table which will be stored.
To create a persist, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Drag and drop the Persist widget from the widgets pane to the designer pane.
3. Hover on the Persist widget and click **Edit** ✎. A dialog box is displayed.
   - (Optional) <Enter one of the user's choices while performing this step.>
   - (Optional) <Enter another of the user's choices while performing this step.>
4. Provide the details as described in the following table:

Table 4-2 Persist Widget Details

Field	Description
Save As	Enter the name for the Persist widget.
Source Datasets	Displays the list of datasets that are linked to the persist widget.
Target Table	Select the target table to which you want to map the columns in the source dataset tables.

Table 4-2 (Cont.) Persist Widget Details

Field	Description
Type	Select the type of mapping that you want to implement for the columns in the target table.The following options are available: • Full Load: This option enables you to truncate the existing data in the target table and load with new data from the source datasets. • SCD: This option represents a slowly changing dimension. This option is used to map data from source datasets to the target table with both current and historical data stored in the target table. . You can select the following options: – Surrogate: Values of this type are typically generated incremental keys. For example, Sequence IDs. – Unique: Use this type for values which are unique across the dataset. For example, Customer Identifiers. – Type 2: Use this type for values which may be changed or added to. For example, Customer Names. Values of this type compare both current and historical data to provide the latest record as active. Historical values will be marked inactive. – Direct: Use this type for values which should consider only the current data for this record. For example, Data Origin. • Incremental: This option is used to map data from the source dataset to a target table in an incremental manner. Incremental mapping adds new entries in addition to the existing data. • Merge: This option is used to map data from source dataset to target table such that both current and historical data are stored and incremental data is also stored. • Generate CSV: This option is used to configure the headers of the source dataset and map the source columns with target column headers with user preference names. This provides insight into the source dataset, which can then be downloaded as a .csv file using the Get Object PAR API. For more information on the Get Object PAR API, see Rest API for FCCM Cloud Service.
Join	Available only if you have connected multiple datasets. For information on Joining datasets, see section Creating Join, beginning at Step 5.
Hints	Hints provide a mechanism to direct the optimizer to choose a certain query execution plan based on the specific criteria.Select the **Type of SQL Operation** from the drop-down list and provide a hint in the **Hints** field.

5. Follow these steps in the Map pane:

   a. Select the source dataset from the drop-down list on the left-hand side. The columns in the table that are associated with the selected source dataset are listed on the left-hand side.

> **Note:**
>
> The source dataset table is referred to as **Source Entity**, the columns in the Source Entity are referred to as **Source Column**.

b. Select the target table on the right-hand side. The columns in the target table are listed on the right-hand side.

> **Note:**
>
> The target dataset table is referred to as the Target Entity, the columns in the Target Entity are referred to as the Target Column.

c. To Automap, click the link icon. Source and target columns are auto-mapped based on Column Names and Data Types.

d. To map source and target columns manually, select a source column, target column, and then click **Expand** ▶ .

> **Note:**
>
> You must select columns of the same data type

The source column is mapped to the target column. The mapping details are displayed in the table on the right-hand side.

e. To add a condition to the target column, click **Add +** and use the Expression Builder to create the condition.The result is displayed in the target column on the right pane.

f. You can also import source and target columns from an Excel sheet. Click **Choose File** and select the Excel sheet.

g. You can also export the mapped source and target columns to Excel using **Export**.

You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see Common Tasks.

Creating Datasets Using the Dataset Widget

The dataset widget enables you to select and filter data sources for use in the later stages of the pipeline.

A data pipeline must always begin with a dataset. Datasets correspond to the contents of a single database table which can be a staging table, business table, or a table that has been created by a data pipeline.Using the dataset widget, you can select any available staging table, name the dataset, perform DQ (data quality) checks on one, multiple, or all columns of the selected staging table, and filter the output by defining conditions for one, multiple, or all columns of the selected staging table using one of three methods: Expression Builder, Tables, or Text. When multiple columns are selected, the OR logic is applied to filter the outputs.

To create a dataset, follow these steps:

1. Navigate to the **Pipeline Designer** page.
2. Drag and drop the Dataset widget from the widgets pane in the upper-right corner of the designer pane.
3. Hover on the Dataset widget and click **Edit** ✎. Provide details as described in the following table:

Table 4-3 Dataset Widget Details

Field	Description
Name	Enter the name for your dataset.
Tables	Select a table from the Tables drop-down list. This list consists of all the staging tables that are available. The columns of the selected table are displayed in the Attributes pane. The attributes include the Logical Name, Column name, and Column Type.

Table 4-3 (Cont.) Dataset Widget Details

Field	Description
Enable DQ check	Select this option to enable the data quality check for the table. You can select each column of the table, specify checks such as range, length, LOV, and null check, and save the rule after naming it. Based on the rule, checks are performed on the columns of the selected staging table to filter out information you do not require.To specify DQ rules, follow these steps: a. Click **Add** + next to the **Enable DQ** check option. b. Under **Master DQ**, select one or multiple Primary Key options. All columns of the selected staging table are listed for you to select. c. Under **DQ Rules**, select a column from the **Available Columns** list. This list contains all columns of the selected staging table. d. Enter a rule name for the selected column of the staging table and specify the following checks for this rule: • **Range Check DQ Rules:**Specify the following range checks: – Is Range Check Required: Select Yes or No. If you select No, jump to the length check rule. If you select Yes, provide a value in the **Minimum Value** field. – Is Provided Minimum Value Inclusive: Select Yes or No. – Maximum Value: Provide a value in the **Maximum Value** field. – Is Provided Maximum Value Inclusive: Select Yes or No. • **Length Check DQ Rules:** Specify Is Length Check Required: Select Yes or No. If you select No, jump to the LOV check rule. If you select Yes, provide a value each in the **Minimum Length** and **Maximum Length** fields. • **LOV Check DQ Rules:** Specify is LOV Check Required: Select Yes or No. If you select No, jump to the Null Check DQ rule. If you select Yes, provide the LOV values in the **LOV Values** field. • **Null Check DQ Rules**: Specify the following Null check DQ rules: – Is NULL Check Required: Select Yes or No. If you select No, jump to the Is Null Value Allowed rule. If you select Yes, provide the null default value in the **Null Default Values** field. – Is NULL Value Allowed: Select Yes or No. If you select No, provide the null default value in the **Null Default Values** field. • **Referential Check DQ Rules**: Specify if Is Referential Check Required. Select Yes or No. If you select Yes, select the name of the table and column that the DQ Rule will refer to when verifying the data.

Table 4-3   (Cont.) Dataset Widget Details

Field	Description
	Note: You must select a value for these checks, either Yes or No. e. Click **Save** to save your DQ rule. f. Repeat these steps to define DQ rules for all the columns of the table based on your requirement.

4. Click **Save** ✓ to save the changes. The dataset is created and is visible on the canvas. It is also available for use in the Dataset pane.

5. To reuse a dataset you have created, click the **Dataset** icon 📄 on the upper-left corner to view the Dataset pane. Click **Expand** to open the list to display the available datasets including the ones you have created. Click the dataset name you want and drag it into the canvas of the Pipeline Designer.

   You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see Common Tasks.

5

Managing Scenario Pipelines

Scenario Pipelines enable you to create scenarios by defining behavior that consists of events in a predetermined order. Scenarios are used to identify behaviors of interest, potentially problematic behaviors with respect to securities, regulations, and possible money-laundering activities.

Scenario Pipelines enable you to create scenarios by defining behavior that consists of events in a predetermined order. You can use these events to thread multiple data streams together. Scenarios are used to identify behaviors of interest, potentially problematic behaviors with respect to securities, regulations, and possible money-laundering activities.

These scenarios consider whether the geographical location or entities involved warrant enhanced scrutiny; monitor activity between accounts, customers, correspondents, and other entities to reveal relationships that could indicate efforts to launder funds; address sudden, significant changes in transaction activity that could indicate money laundering or fraud; and detect other types of activities that are considered potentially suspicious or indicative of money laundering.

As part of configuring a scenario pipeline, parameters are defined, which are then tuned in the Threshold Manager.

Pre-configured Scenario Pipelines

FCCM TM Cloud Service provides a set of pre-configured pre-configured scenario pipelines.

The application comes with the following ready-to-use, pre-configured scenario pipelines:

- Structuring - Potential Structuring in Cash and Equivalents - Customer Focus
- Structuring - Deposits Withdrawals of Mixed Monetary Instruments - Customer Focus
- Structuring - Avoidance of Reporting Thresholds - Account Focus
- Structuring - Avoidance of Reporting Thresholds - Customer Focus
- Structuring - Avoidance of Reporting Thresholds - External Entity Focus
- Transactions in Round Amounts - Account Focus
- Rapid Movement of Funds All Activity - Account Focus
- Escalation in Inactive Account - Account Focus
- CIB Significant Change From Previous Average Activity - Account Focus
- CIB Significant Change From Previous Peak Activity - Account Focus
- CIB High Risk Geography Activity - Account Focus
- CIB Foreign Activity - Account Focus
- CIB Product Utilization Shift - Account Focus
- Transactions in Round Amounts EFT - External Entity Focus
- Transactions in Round Amounts MI - External Entity Focus

- Focal High Risk Entity - Account Focus
- Focal High Risk Entity - Customer Focus
- Focal High Risk Entity - External Entity Focus
- Patterns of Funds Transfers Between Internal Accounts and Customers - Customer Focus
- Patterns of Funds Transfers Between Customers and External Entities - Customer Focus
- High Risk Counter Party - Account Focus
- High Risk Counter Party - Customer Focus
- High Risk Counter Party - External Entity Focus
- High Risk Geography - Account Focus
- High Risk Geography - External Entity Focus
- Large Depreciation of Account Value - Account Focus
- Large Reportable Transactions - External Entity Focus
- Large Reportable Transaction - Customer Focus
- Possible Currency Transaction Report - Customer Focus
- Possible Currency Transaction Report - External Entity Focus
- Hub and Spoke - Customer Focus
- Hub and Spoke - External Entity Focus
- Rapid Movement of Funds - Customer Focus
- Rapid Loading and Redemption of Stored Value Cards - Account Focus
- Rapid Loading and Redemption of Stored Value Cards - Customer Focus
- Anomalies in ATM Bank Card Foreign Transactions – Account Focus
- Anomalies in ATM Bank Card Foreign Transactions – Customer Focus
- Anomalies in ATM, Bank Card: Excessive Withdrawals - Account Focus
- Anomalies in ATM, Bank Card: Excessive Withdrawals - Customer Focus
- Single or Multiple Cash Transactions - Large Significant Transactions - Customer Focus
- Early Payoff or Paydown of a Credit Product - Account Focus
- Early Payoff or Paydown of a Credit Product - Customer Focus
- Early Closure of Term Account - Account Focus
- Policies with Large Early Removal - Customer Focus
- Insurance Policies with Refunds - Customer Focus

For detailed information about these scenario pipelines, see the Technical Scenario Description.

Widgets in Scenario Pipelines

Depending on the pipeline type, specific widgets are available in the widgets pane.

The following table describes these widgets and the sequence in which the widgets can be placed from start to end in a scenario pipeline.

Table 5-1 Scenario Pipeline – Widgets and Descriptions

Sequence	Widget	Name	Description	Precedence	Additional Information
1		High Level Dataset (HLD)	Use this widget to add a High Level Dataset. Essentially, this is the data that is used to detect unusual or suspicious behavior.	N/A	A scenario pipeline must always begin with an HLD widget.
2		Episode	Use this widget to add an Episode. Episodes allow you to generate events which meet specific criteria. For example, if the sum of consecutive transactions fall under the specified range, it is considered an episode. If the number of episodes crosses specified number of thresholds, an event will be generated.	1	An episode is not mandatory in a scenario pipeline.
3		Risk Indicator	Use this widget to add a Risk Indicator. Risk indicators help determine the overall risk of transactions and parties and aid users working with events.	1	
4		Segment	Use this widget to add a Segment. Segments allow you to set different values for meeting evaluations based on specified attributes. Using segments helps generate events based on applying different values to risk indicators and evaluations.	3	A segment is not mandatory in a scenario pipeline, but a scenario pipeline can contain multiple segments that can either be connected in a sequential or parallel manner.

Table 5-1 (Cont.) Scenario Pipeline – Widgets and Descriptions

Sequence	Widget	Name	Description	Precedence	Additional Information
5	⊞	Evaluation	Use this widget to add an Evaluation. Evaluations are used to define conditions for the measures that are defined in the risk indicator. Evaluations perform logical comparisons against these conditions to generate events	3,4	
6	◎	Create Event	Use this widget to create an Event. An event is a record of one or more pattern matches in a detection run, which is a signal for further investigation.	5	A scenario pipeline must always end with a Create Event widget.

Using High Level Dataset

You must add a high level dataset to begin a scenario pipeline.

To add a high level dataset and begin a scenario pipeline, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Click Widgets ≡ on the upper left corner. The list of pre-configured HLDs is displayed. FCCM TM Cloud Service comes with the following pre-configured High Level Datasets (HLD).
   - External Entity Transaction
   - Transaction by Customer
   - Transaction by Account
3. Drag and drop the required HLD to the designer pane.
4. Hover on the HLD widget and click **Edit** ✎. A dialog box is displayed.
5. Specify the required details.
6. Click **Save** ✓ to save the changes. The HLD is saved.

   You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see Common Tasks.

   Add Additional High Level Datasets
   You can add multiple conditions within the dataset to be considered by the scenario when detecting behaviors of interest. This can help improve the accuracy

of your detection results and reduce false positives. For more information, see Adding Additional Threshold Conditions.

Managing Risk Indicator

Risk Indicator is a measure used to indicate the overall risk involved in an activity.

Relevant data is compared against a set of risk indicators to identify the early signals of increasing risk exposures in various areas of an enterprise. In this context "Risk" refers not only to derived risk values (geography, watchlist, entity, and so on) but also to certain behaviors that constitute risk relative to the activity being monitored. For example, the total transaction amount of wires involved in a hidden relationship represents a risk that can be measured based on applying configurable limits that are applicable to the scenario pipeline.

Creating a Risk Indicator

You can create new risk indicators for scenario pipelines.

1. Navigate to the Pipeline Designer page.
2. Drag and drop the Risk Indicator widget from the widgets pane to the designer pane.
3. Hover on the Risk Indicator widget and click **Edit** ✎. The Risk Indicators pane is displayed.
4. Click **Move All** » on the left-hand side. The Risk Indicators Available pane is displayed with the list of risk indicators.
5. Provide the details as described in the following table:

Table 5-2 Risk Indicator Widget Details

Field	Description
Risk Indicator	Enter the risk indicator name.
Method	Select the method to obtain the risk indicator output. The available methods are Aggregation and Expression

- If you have selected the **Aggregation** method, provide the following details:
  - Aggregator: Select an aggregator from the drop-down list.
  - Attribute: Select an attribute from the drop-down list.
  - Group by: Select a Group-by clause.
  - Look Back: Select the required lookback option and provide the required details. You can further configure the Look Back period for the risk indicator when building the expression.

> **Note:**
>
> When configuring the LookBack Period in the Expression Builder, you must use the keyword "lookbackperiod".

        - Filter Attribute: Select filter attribute.
        - Filter Operator: Select filter operator.
        - Filter Value: Select the required filter value option and provide the required details.
    - If you have selected the **Expression** method, follow these steps:
        a. Add an expression by clicking **Add** ⊞. The Expression Builder dialog box is displayed.
        b. Select the Attribute, Runtime Parameters, and Operators. The resulting condition is displayed in the Condition field.

6. Click **Save** to create the measure or **Save & Attach** to create and also attach the measures to the risk indicators used.

   You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see Common Tasks.

Attaching Risk Indicator

You must attach the required risk indicator for it to take effect.

To attach a risk indicator, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Drag and drop the Risk Indicator widget from the widgets pane to the designer pane.
3. Hover on the Risk Indicator widget and click **Edit** ✎. A dialog box is displayed.
4. Click **Move All** » on the left-hand side. The Risk Indicators Available pane is displayed with a list of available risk indicators.
5. Click **Move** › corresponding to the risk indicator that you want to attach. The selected risk indicator is moved to the Risk Indicators Used pane.
6. Click **Save** ✓ to save the changes. The Risk Indicator is attached

Editing Risk Indicator

You can edit risk indicators which you have created.

Only user-configured measures can be edited. You cannot edit pre-configured measures. To modify details of a risk indicator, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Select the Risk Indicator widget that you want to modify.
3. Hover on the Risk Indicator widget and click **Edit** ✎. A dialog box is displayed.
4. Click **Move All** » on the left-hand side. The Risk Indicators Available pane is displayed with the list of available risk indicators.

5. Click the Risk Indicator that you want to modify and click **Edit**.
6. Modify the required details.
7. Click **Save**. The Risk Indicator is modified.

Creating Episodes

Episodes are used by structuring scenarios to generate events which meet specific criteria, based on runtime parameters.

For example, if the sum of consecutive transactions fall under the specified range, it is considered an episode. If the number of episodes crosses the specified threshold, then an event will be generated.
To create an episode, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Drag and drop the Episode widget from the widgets pane to the designer pane, after a High Level Dataset.
3. Hover on the Episode widget and click **Edit** ✎. The Episode window displays any existing conditions.
4. Select options from the drop-down lists to edit existing conditions.
5. Select options from the **List of Conditions** to add additional conditions for consideration by the scenario. Configure these conditions by selecting options from the drop-down lists.
6. Click **Add** ⊞ to add a new runtime parameter which can be used by the conditions.
    a. Enter the name for the runtime parameter in the **Name** field.
    b. Enter a description for the runtime parameter in the **Description** field.
    c. Select a Datatype for the runtime parameter from the **Datatype** drop-down list.
    d. Enter any default values for the runtime parameter.
    e. Click **OK** to save the runtime parameter.
7. Click **Save** ✓ to save the changes.

    You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see Common Tasks.

Creating Segments

A segment enables you to segregate data based on defined conditions.For example, risk levels.

A segment can be defined where both the effective risk of the focal entity and the risk of the associated activity determine if the behavior meets a High Risk, Medium Risk or Regular Risk definition. Risk indicator triggering levels can be set according to the segment. Using segments allows for generating events based on applying different values to risk indicators and evaluation based on how a party fits within a defined segment.
To create a segment, follow these steps:

1. Navigate to the Pipeline Designer page.

2. Drag and drop the Segment widget from the widgets pane to the designer pane.
3. Hover on the Segment widget and click **Edit** ✎. A dialog box is displayed.
4. Enter the name for the Segment in the **Name** field.
5. Click **Add** ⊞ corresponding to the Output pane to open the segment group. You can add multiple groups and multiple conditions under each group.
6. Select the dataset or Risk Indicator you want to add conditions for.
7. Select a column and operator (=,>, <, <=, >=, <>, LIKE, and so on) to configure the conditions.

   For example: (Effective Risk >= $Effective_Risk)

   The following table describes the columns available.

Table 5-3 Segment Column Details

Column	Dataset	Description
Net Worth Amount	Customer	The net worth required for generating an event using this segment.
Customer Age	Customer	The number of calendar days that an account has been opened. This is used to determine whether an account is new or seasoned.
Customer Number	Customer	The number of customers required for generating this event.
Effective Risk	Customer	The effective risk level specified for the conditional thresholds to decide which set of threshold values would be applied in event generation.
From Party Credit Debit Indicator	Transaction	Identifier of whether this transaction represents credits to the account or debits from the sending account.
From Party Identifier	Transaction	Identifier for the party sending the transaction.
To Party Identifier	Transaction	Identifier for the party receiving the transaction.
Party Identifier	Transaction	Identifier for this party as it appears on this transaction. This might be a financial institution identifier (for example, ABA number or BIC) or other standard industry identifier (such as, TIN or account number).
Transaction Number	Transaction	Number of transactions to be considered or calculated as part of the logic.
Transaction Amount	Transaction	Monetary value of the funds involved this transaction.
Left Entity	Transaction	Originator of the transaction.

Table 5-3 (Cont.) Segment Column Details

Column	Dataset	Description
Right Entity	Transaction	Beneficiary of the transaction.
Both Party Internal Account Identifier	Transaction	Identifier of whether or not both parties involved in this transaction are internal accounts.
Credit Debit Indicator	Transaction	Identifier of whether this transaction represents credits to the account or debits from this account.
Activity Risk	Transaction	Activity risk level specified for the conditional thresholds to decide which set of threshold values is applied in event generation.
Counterparty	Transaction	Counterparty associated with this transaction.
Geography Risk	Transaction	Identifier of the level of risk associated with the geographic characteristics of this transaction. Firms have used account addresses and customer information (for example, citizenship) to determine the level of risk.
Total_Debit_Amount	Risk Indicator	Aggregate amount of debit transactions involved required to trigger an event, expressed in base currency.
Activity_Risk	Risk Indicator	Calculated on the transaction for each party based on the risk of the entity on the other side of the transaction as well as channel being used.
Total_Credit_Count	Risk Indicator	Total number of credit transactions required to trigger an event.
Total_Debit_Count	Risk Indicator	Count of debit transactions required to trigger an event.
Distinct_Counterparties_ for_Incoming	Risk Indicator	Total number of distinct originators crediting money into the focal customer's accounts.
Distinct_Counterparties_ for_Outgoing	Risk Indicator	Total number of distinct originators debiting money from the focal customer's accounts.
Total_Credit_Amount	Risk Indicator	Aggregate amount of credit transactions involved required to trigger an event.

8. Click **Save** ✓ to save the changes. The segment is created.

Creating Evaluations

Evaluations are used to define conditions for the measures that are defined in the risk indicator.

Evaluations perform logical comparisons against these conditions to generate events. To create an evaluation, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Drag and drop the **Evaluations** widget from the widgets pane to the designer pane.
3. Hover on the Evaluations widget and click **Edit** ✎. A dialog box is displayed.
4. Enter the name for the evaluation in the **Name** field.
5. Click **Add** ⊞ corresponding to the Output pane to open the evaluation group. You can add multiple groups and multiple conditions under each group. The values which display in the Output pane are typically thresholds which can be managed in the Threshold Editor.

   For more information on configuring a filter, see Configuring Filter.
6. Click **Save** ✎ to save the changes.

   You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see Common Tasks.

Creating Events

An event is a record of one or more pattern matches in a detection run, which is a signal for further investigation.

In Scenario Pipelines, the Create Event widget is the final part of the pipeline and is used to produce an event. An event is a record of one or more pattern matches in a detection run, which is a signal for further investigation. An event is also a unit of work in which a focus appears to have exhibited behavior of interest, along with the supporting information. A focus represents a business entity around which activity is reviewed and aggregated. For example customer, account or external entity. Events can be generated from a pattern matching specific source events, a sequence of events, trends, conditions, or context.
To create an event, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Drag and drop the **Create Event** widget from the widgets pane to the designer pane.
3. Hover on the Create Event widget and click **Edit** ✎. A dialog box is displayed.
4. Verify the details and click Save ✓ to save the changes.

   The Create Event widget is created.

6

Managing Scoring Pipelines

A Scoring Pipeline is used to calculate Event and Correlation scores, and define Decision Rules for case promotion.

Logical conditions are used to define the Event and Correlation scores. These logical conditions are grouped in Rules.

Scoring can be performed on events or correlations. The Pre-Case score is the sum of score of all events and the correlation. Events are promoted to case based on decision rules which run on the pre-case score calculated earlier.

After creating the Jurisdiction in the system, create a pre-case decision rule in the scoring pipeline with respect to the Case Type, Jurisdiction combination. You need to take a copy of the existing pipeline and create the decision rule.

> **Note:**
>
> You cannot use the default ECMProcess Batch unless you configure a Case Scoring Pipeline and associate it with the Batch.

Scoring Pipeline Operations

A scoring pipeline has the following major operations:

- Correlation Scoring: Scoring each correlation based on the defined rules and condition.
- Event Scoring: Scoring each event based on the defined rules and condition.
- Moving Scoring Data: The result of the event scoring and correlation scoring rule sets are moved to the related tables in Case Management and then the Pre-Case score is calculated.
- Pre-case Decision: Rules defining a threshold through which decision to promote a correlation to a case is taken.

Pre-configured Rules in Scoring Pipelines

FCCM TM Cloud Service provides a set of pre-configured scoring pipelines.

The application comes with the following set of ready-to-use scoring pipelines.

- Rules in Correlation Scoring Pipelines
- Rules in Event Scoring Pipelines
- Rules in Pre-case Decisions

>

Rules in Correlation Scoring Pipeline

The following table lists the ready-to-use Correlation Scoring Pipeline Rules.

Table 6-1   Correlation Scoring Pipeline Rules

Rule Name	Condition Details
Correlation score for high number of events	If Event Count> 10, then Score is 50.
Correlation score for low number of events	If Event Count > 3 and Event Count <= 5 , then Score is 30.
Correlation score for medium number of events	If Event Count > 5 and Event Count <= 10 , then Score is 40.
High bucket for total transaction amount	If Total Transaction Amount >= 500001, then Score is 50
Medium bucket for total transaction amount	If Total Transaction Amount >= 100001 and Total Transaction Amount < 500001, then Score is 20.
Lower bucket for total transaction amount	If Total Transaction Amount >= 50000 and Total Transaction Amount < 100001, then Score is 20.

Rules in Event Scoring Pipeline

The following table lists the ready-to-use Event Scoring Pipeline Rules.

Table 6-2   Event Scoring Pipeline Rules

Rule Name	Condition Details
High bucket score for total transaction amount	If Total Transaction Amount>= 100001, then Score is 40.
Lower bucket score for total transaction amount	If Total Transaction Amount >= 0 and Total Transaction Amount < 50001, then Score is 20.
Medium bucket score for total transaction amount	If Total Transaction Amount >= 50001 and Total Transaction Amount < 100001, then Score is 30.

Rules in Pre-case Decision

The following table lists the ready-to-use Pre-case Scoring Pipeline Rules.

Table 6-3   Pre-Case Scoring Pipeline Rules

Rule Name	Condition Details
AML_SURV	Threshold Score =70 and Jurisdiction Code = AMEA

> **Note:**
>
> These ready-to-use scoring pipelines are not editable. You can make a copy of the pipeline and edit the scoring rules.

Widgets in Scoring Pipelines

Depending on the pipeline type, specific widgets are available in the widgets pane. The following table describes these widgets and the sequence in which the widgets can be placed from start to end in a scoring pipeline.

The following table lists the widgets available in a scoring pipeline.

Table 6-4 Scoring Pipeline - Widgets and Descriptions

Widget	Name	Description
⚙	Correlation Scoring	Use this widget to set a Correlation Score. The correlation scoring rule is driven by the events that are part of the correlation. For more information, see Defining a Correlation Scoring.
◎	Event Scoring	Use this widget to set an Event Score. For more information, see Defining an Event Scoring.
⧉	External Services	Use this widget to move the scoring data. For more information, see External Service
✓	Pre-Case Decision	Use this widget to define threshold value and if the pre-case score crosses this threshold value, the correlation is promoted to case. For more information, see Defining a Pre-case Scoring.

Creating Scoring Pipelines

You can create new scoring pipelines as needed for your implementation.

1. Navigate to the Pipeline Designer page.
2. Follow the steps provided in Creating Pipelines to create a new scoring pipeline.
3. Drag and drop the Scoring Widgets from the widgets pane in the upper-right corner to the designer pane. It is recommended to use the Standard flow.
4. Connect the widgets in the order provided.
5. Hover on the scoring widget and click **Edit** ✎.
6. Define the scoring pipeline components, as shown in the following sections.
   1. Correlation Scoring
   2. Event Scoring
   3. External Service
   4. Pre-case Decision

Defining Correlation Scoring Rule

Step 1: Create rules for Correlation Scoring

To create rules for Correlation Scoring, follow these steps:

1. Hover on the Correlation Scoring widget ⚙ and click **Edit** ✎. The Ruleset Details window is displayed for the Correlation Scoring widget.

   (Optional) <Enter a step example.>

2. Provide the details as described in the following table.

Table 6-5 Fields to Define Correlation Scoring Pipeline

Field	Description
Ruleset Name	Enter the name for the correlation scoring rule.
Ruleset Description	Enter the description for the correlation scoring rule.
Scoring Aggregation Type	Select the scoring aggregation type from the Scoring Aggregation Type drop-down list. There are three Score Aggregation Types: • SUM: This option calculates the sum of the scores among the associated rules and assigns it as the final score. • MIN: This option calculates the minimum score among the associated rules and assigns it as the score. • MAX: This option calculates the maximum score among the associated rules and assigns it as the score.
Rules	Define the conditions using the Rules section for scoring. For more information, see the Adding a Rule section.

3. To add a rule, click **Add** ⊞ on the left (Rules pane) and specify conditions for the rule. You can add multiple rules and multiple conditions under each rule. For more information, see the Adding a Rule section.

4. Click **Save** ✓ to save the changes.

5. Add more rules as needed to define all the rules for Correlation Scoring.

   You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see the Common Tasks section.

Defining Event Scoring Rule

Step 2: Create rules for Event Scoring

Complete the steps in Defining Correlation Scoring

To define an event scoring, follow these steps:

1. Hover on the Event Scoring widget and click Edit . The Ruleset Details window is displayed for the Event Scoring widget.
2. Provide the details as described in the following table.

Table 6-6 Fields to Define Event Scoring Pipeline

Field	Description
Ruleset Name	Enter the name for the event scoring rule.
Ruleset Description	Enter the description for the event scoring rule.
Scoring Aggregation Type	Select the scoring aggregation type from the Scoring Aggregation Type drop-down list. There are three Score Aggregation Types: • SUM: This option calculates the sum of the scores among the associated rules and assigns it as the final score. • MIN: This option calculates the minimum score among the associated rules and assigns it as the score. • MAX: This option calculates the maximum score among the associated rules and assigns it as the score.
Rules	Define the conditions using the Rules section for scoring. For more information, see the Adding a Rule section.

3. To add a rule, click **Add** on the left (Rules pane) and specify conditions for the rule. You can add multiple rules and multiple conditions under each rule. For more information, see the Adding a Rule section.
4. Click **Save** to save the changes.
5. Add more rules as needed to define all the rules for Correlation Scoring.

   You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see the Common Tasks section.

Move Scoring Data using External Services

Step 3: Move Scoring Data using External Services

Complete the steps in Defining Correlation Scoring and the steps in Defining Event Scoring.

In Scoring pipelines, the External Services widget is a persist widget that moves the data from the rule set result table to the main scoring tables. This means that scoring data will move from the FCC_M_CM_RULESET_RESULT table to the FCC_CM_CORRELATION_SCORE table for correlation scoring and the FCC_CM_EVENT_SCORE table for event scoring, respectively.
Before moving the data to the main scoring table, data will be stored in the CC_M_CM_RULESET_RESULT table from event scoring and correlation scoring. You cannot make any changes in this widget.

> **Note:**
>
> For more information about the Persist widget, see Creating a Persist.

Pre-case scoring is performed on event scoring and correlation scoring.

For example, if there are Event A, Event B, and Event C in the system, then the pre-case score is the sum of Event A + Event B + Event C + Correlation Score.

> **Note:**
>
> If the pre-case score does not cross the promote to case threshold, it remains only in the pre-case layer.

To move the scoring data after creating a correlation scoring widget and defining the correlation and event scoring rules, follow these steps:

1. Hover on the External Service widget and click **Edit** . The External Service window is displayed.
2. Select **Move Scoring Data** from the **Name** drop-down list.

Define Pre-Case Decision

Step 4: Define Pre-Case Decision Thresholds

Complete the steps in Defining Correlation Scoring, the steps in Defining Event Scoring, and the steps in Move Scoring Data using External Services.

Correlations are promoted to cases based on decision rules which run on the pre-case score calculated earlier. Use the Pre-Case Decision widget to define threshold values. If the pre-case score crosses the configured threshold values, the correlation is promoted to case.
To define threshold values, follow these steps:

1. Hover on the Pre-case Decision widget and click **Edit** . The Pre Case Decision window is displayed.
2. Provide the details as described in the following table:

Table 6-7 Fields to Define Pre-Case Decisions

Field	Description
Case Type	Select the case type from Case Type drop-down list. For example: AML_SURV and so on.
Jurisdiction	Select a Jurisdiction.

Table 6-7 (Cont.) Fields to Define Pre-Case Decisions

Field	Description
Threshold Score	Enter the threshold score. If pre-case score exceeds the threshold score, then it gets promoted to case.

3. Click **Save** ✓ from the **Add Rule** section.
4. Click **Save** again ✓ from the top-corner of the window to save the changes. After defining the rule, the Scoring page is displayed.
   - Click **Edit** ✎ to edit the rule.
   - Click **Delete** 🗑 to delete the rule.

Adding Scoring Rules

Rules are logical comparisons against conditions that result in a score.

To add a rule, follow these steps:

1. Navigate to the **Rules** section of the Scoring page.
2. Enter a name for this rule.
3. Define the conditions. You can add multiple conditions.
   - Left Expression: Select the expression on which rule must be operated. The following two types are available:
     - Profiles: are an aggregation of information. Profiles can be based on different grouping entities and can be filtered to only look at kinds of transactions. By default, Event Count, Total Transaction Count and Total Transaction Amount profiles are available. You can also use filters on profile. For more information, see Adding Filters.
     - Attributes: this list is the group of data condition such as correlation, generated events, and so on.
     - Operator: select the operator from the Operator drop-down list for the expression and also the expression that it is to be operated on. The available operators are IN, =, >, <, <=, >=, and <>.
   - Right Expression: Provide the value on which the left expression and operators will work
4. Click **Save** ✓ to save the Rule.

Use Cases

Example of Correlation Scoring

Correlation Scoring use case.

In this example, the correlation scoring rule-based Event Count and Total Transaction Amount is defined as follows:

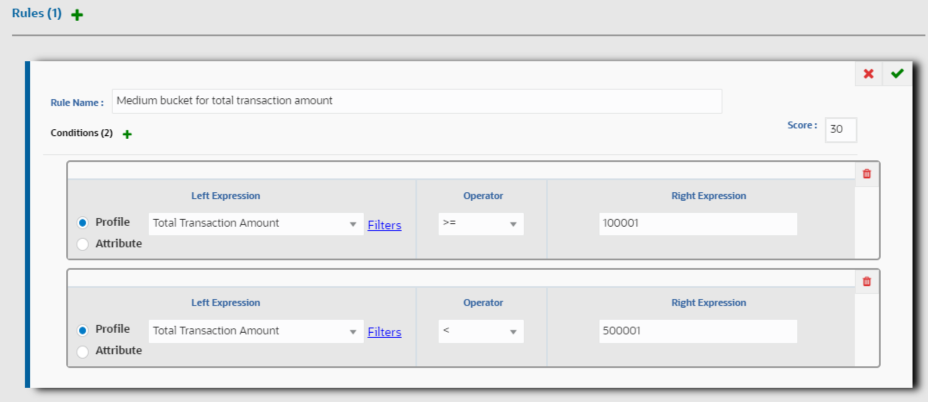
- Correlation 1: Total Transaction Amount = 170000, Event Count =3
- Correlation 2: Total Transaction Amount = 180000, Event Count = 7
- Correlation 3: Total Transaction Amount = 50000, Event Count = 8

1. Define a rule (Rule1) with the score 30 based on the following conditions:
   - Conditions: Transaction Amount >= 100001 and Transaction Amount < 500001
   - Result: Correlation 1 and Correlation 2 will be assigned a score as 30
2. Define a rule (Rule2) with the score 50 based on the following conditions:
   - Conditions: Event Count > 5 and Event Count < = 10
   - Result: Correlation 2 and Correlation 3 will be assigned a score as 50.

Follow these steps to define this use case:

1. Add a rule (Rule1) using **Add** ✚ from the Rules window. The Rules window is displayed.
   a. Enter the **Rule Name**, **Description**, and **Score** as 30.
   b. Define **condition 1** and **condition 2** as Transaction Amount >= 100001 and Transaction Amount < 500001.

Figure 6-1 Example of Correlation Scoring – Condition 1



Rules (1) ✚

Rule Name : Medium bucket for total transaction amount

Conditions (2) ✚

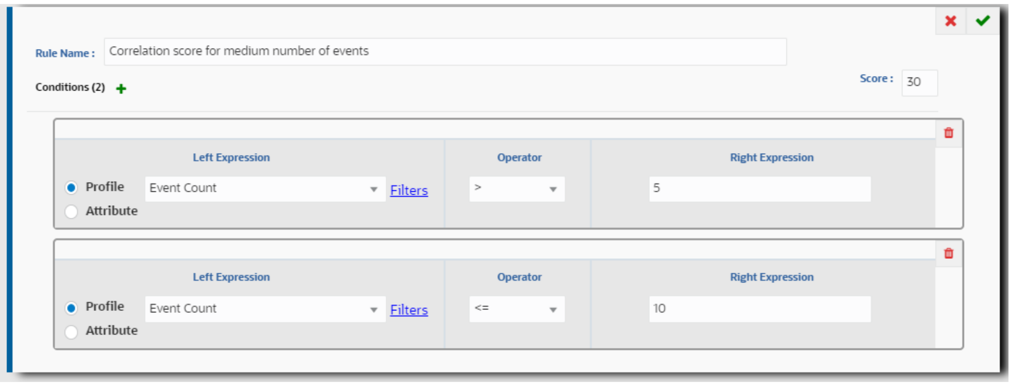
Score : 30

Left Expression			Operator	Right Expression
● Profile ○ Attribute	Total Transaction Amount	Filters	>=	100001
● Profile ○ Attribute	Total Transaction Amount	Filters	<	500001

   c. Click **Save** ✓.

2. Add a rule (Rule2) using **Add** ✚ from the Rules window The Rules window is displayed.
   a. Enter the **Rule Name** and **Score** as 50.
   b. Define **condition 1** and **condition 2** as Event Count > 5 and Event Count < = 10

Figure 6-2 Example of Correlation Scoring – Condition 2



Rule Name : Correlation score for medium number of events

Conditions (2)

Score : 30

Left Expression		Operator	Right Expression
● Profile ○ Attribute	Event Count	>	5
● Profile ○ Attribute	Event Count	<=	10

c. Click **Save** ✓.

After defining the scoring rules, the total correlation score will be calculated based on the Score Aggregation Type. The Score Aggregation Types are described in the following table.

Table 6-8 Score Aggregation Types

Aggregation Type	Correlation 1	Correlation 2	Correlation 3
SUM	30	30+50=80	50
MIN	30	30	50
MAX	30	50	50

Example of Event Scoring

Event Scoring use case.

The following example shows how to create a rule based on the Total Transaction Amount and Jurisdiction conditions:

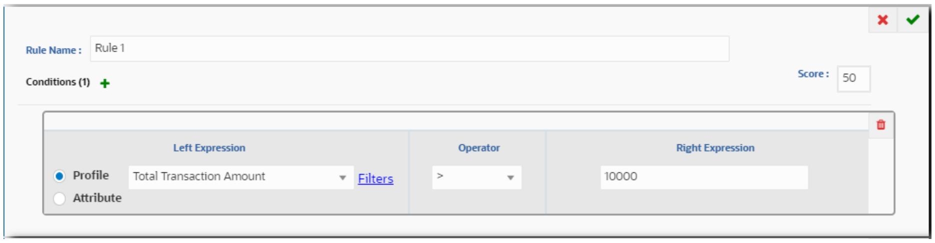
- Event 1: Total Transaction Amount = 17500, Jurisdiction code = AMEA
- Event 2: Total Transaction Amount = 4000, Jurisdiction code = INDA
- Event 3: Total Transaction Amount = 5000, Jurisdiction code = EMEA

1. Define a rule (Rule 1) with the score 50 based on the following conditions:
   - Conditions: When Total Transaction Amount > 10000
   - Result: Event 1 and Event 2 will be assigned a score as 50
2. Define a rule (Rule 2) with the score 30 based on the following conditions:
   - Conditions: Total Transaction Amount < = 10000
   - Result: Event 3 will be assigned a score as 30
3. Define a rule (Rule 3) with the score 20 based on the following conditions:
   - Conditions: Jurisdiction code = AMEA
   - Result: Event 1 will be assigned a score as 20

Follow these steps to define this use case:

1. Add a rule (Rule1) using **Add** ➕ from the Rules window. The Rules window is displayed.
   a. Enter the **Rule Name** and **Score** as 50.
   b. Define the **Condition 1** as Total Transaction Amount >10000

   Figure 6-3 Example of Event Scoring – Rule 1

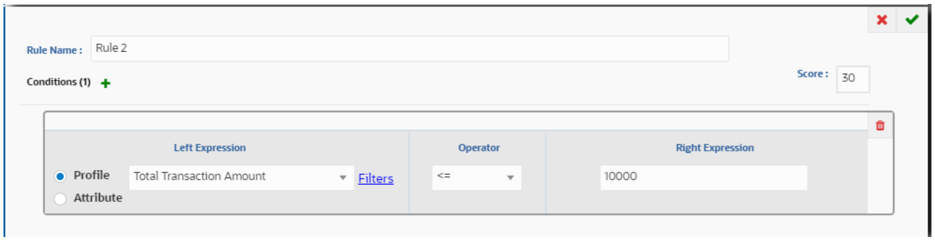
   Rule Name : Rule 1
   Score : 50
   Conditions (1) +

Left Expression			Operator	Right Expression
● Profile ○ Attribute	Total Transaction Amount	Filters	>	10000

   c. Click **Save** ✓.

2. Add a rule (Rule 2) using **Add** ➕ from the Rules window. The Rules window is displayed.
   a. Enter the **Rule Name** and **Score** as 30.
   b. Define **Condition 1** as Total Transaction Amount < = 10000.

   Figure 6-4 Example of Event Scoring – Rule 2

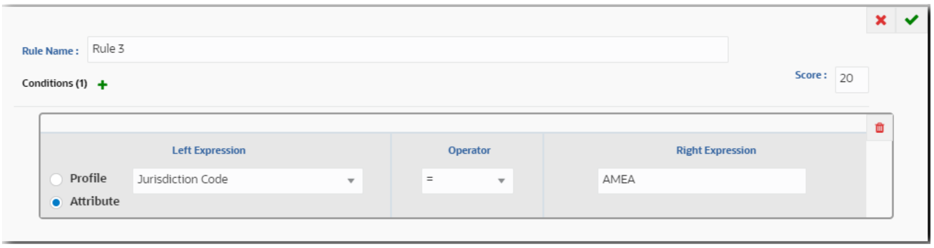
   Rule Name : Rule 2
   Score : 30
   Conditions (1) +

Left Expression			Operator	Right Expression
● Profile ○ Attribute	Total Transaction Amount	Filters	<=	10000

   c. Click **Save** ✓.

3. Add a rule (Rule 3) using **Add** ➕ from the Rules window. The Rules window is displayed.
   a. Enter the **Rule Name** and **Score** as 20.
   b. Define the **Condition 1** as Jurisdiction code = AMEA.

   Figure 6-5 Example of Event Scoring – Rule 3

   Rule Name : Rule 3
   Score : 20
   Conditions (1) +

Left Expression		Operator	Right Expression
○ Profile ● Attribute	Jurisdiction Code	=	AMEA

c. Click **Save** ✓.

After defining the scoring rules, the total event score will be calculated based on the Score Aggregation Type. The Score Aggregation Types are described in the following table.

Table 6-9 Event Score Aggregation Types

Aggregation Type	Event 1	Event 2	Event 3
SUM	50+20	50	30
MIN	20	50	30
MAX	50	50	30

7

Managing Customer Screening Pipelines

Customer Screening pipelines allow you to load data and screen entities in batch and real time.

Organizations need to effectively and efficiently screen their customers to successfully meet anti-bribery, anti-corruption, export control, and other legal regulations as well as all current anti-money laundering and counter-terrorist financing legislation. Customer Screening pipelines allow you to load data and screen entities in batch and real time.

> **Note:**
>
> **ATTENTION:** Customer Screening pipelines are only available if your firm has implemented Oracle FCCM Customer Screening Cloud Service.

Pre-configured Customer Screening Pipelines

FCCM TM Cloud Service provides a set of pre-configured customer screening pipelines.

The application comes with the following ready-to-use customer screening pipelines:

- Load Customer Add On Data
- Load Customer Data
- Load Customer Mapping Data
- Individual Batch Screening
- Individual Real Time Screening
- Entity Real Time Screening
- Individual 314 A Batch Screening
- Entity 314 A Batch Screening
- Loading Screening AE Decision

Import the ready-to-use pipelines to the application. To configure pipelines, you must create a copy of an imported pipeline and save it as a new pipeline. For more information, see Copying Pipelines.

> **Note:**
>
> After importing the ready-to-use pipelines to the application, you must refresh the existing copied pipeline with the latest version.

Widgets in Customer Screening Pipelines

Depending on the pipeline type, specific widgets are available in the widgets pane of the pipeline

The following table describes the widgets available in Customer Screening pipelines.

Table 7-1 Customer Screening Pipeline – Widgets and Descriptions

Widget	Name	Description
🛢	Entity	Use this widget to link to data that has been loaded into indexes for matching. An entity can be an individual, organization, and so on.
👥	Request JSON	Use this widget to view the available request attributes in real time screening.
☑	Matching Rules	Use this widget to configure how matching occurs for a set of data.
⧉	External Service	Use this widget to add an external service. External Services perform actions on the data, such as loading or moving the data, or performing a virus scan.
⚙	Alert Decision	Use this widget to define which customer and watchlist attributes changes should be considered for further review.
⚙	Auto Elimination Rules	Use this widget to enable or disable the event type (SAN/PEP/EDD/PRB) for auto-elimination.

Using Entity Widget

The Entity widget links to data that has been loaded into indexes for matching.

The **Entity** widget 🛢 is similar to the Dataset widget used in other pipelines, except that instead of reading data from a table it links to data that has been loaded into indexes for matching. The **Entity** widget allows you to specify the entity name and displays the associated columns that are available. You can also specify if the entity is the source or target for the matching. All screening pipelines must specify a single source and target.

Using the Request JSON Widget

The Request JSON widget displays the available request attributes in Real Time Screening.

The Request JSON widget also allows you to specify if the entity is the source or target for matching. All screening pipelines must specify a single source and target.

Using the Matching Rules Widget

The Matching Rules widget enables you to define the matching configuration for a set of data.

The data that must be matched by each widget depends on the source and target set in the Entity widgets linked to the Matching Rules widget. The source and target data can be filtered if a subset of data is to have this matching configuration applied. This allows you to provide different matching configurations for different types of watchlist records and different jurisdictions and domains. Each matching ruleset contains the name, description, scoring aggregation used, the threshold value for the overall rule set and one or more rules.

Rules are configured using the Matching Ruleset window. Matches are generated based on a defined set of attributes for each rule. A weighted average of the score is generated for each of the attribute level matches. There are two types of matching services :

- Real-Time query processing
- Bulk query processing

In Real-Time query processing, a string value given in the UI is matched against a column in the target table. Customer Screening explicitly passes the strings as values in the request which forms “the strings to be matched” against “all the values in a column name”. Then, based on the matches received for the source string from the search engine, the score and the feature vector for the matched strings (source and target) are generated. Scores which exceed the configured thresholds are taken and collected.

Provide the following values for each rule:

- Source attribute
- Target attribute
- Match type (The Match Types table provides some examples)
- Scoring Method (This can be one of the following:)
  - Levenshtein: The Levenshtein Distance (LD) or edit distance provides the distance, or the number of edits (deletions, insertions, or substitutions) needed to transform the source string into the target string. For example, if the source string is Mohamed and the target string is Mohammed, then the LD = 1, because there is one edit (insertion) required to match the source and target strings.
  - Jaro Winkler: The Jaro Winkler similarity is the measure of the edit distance between two strings. For example, if the source string is Mohammed Ali and the target string is Mohammed Ali, then the similarity = 1.

  - Reverse Jaro Winkler: In the Reverse Jaro Winkler, matches are generated even if the string is reversed. For example, if the source string is Mohammed Ali and the target string is Ali Mohammed, then the similarity = 1.
  - Individual SAN: The details are provided in the Matching Guide.
  - Entity SAN: The details are provided in the Matching Guide.
  - Individual PEP: The details are provided in the Matching Guide.
  - Entity PEP: The details are provided in the Matching Guide.
  - Individual EDD: The details are provided in the Matching Guide.
  - Entity EDD: The details are provided in the Matching Guide.
- Set threshold value: If this value is crossed then the attribute is considered for matching
- Weightage assigned to the attribute (total of all attributes within a rule must equal 1)
- Must check box (optional): If this check box is selected, then there must be a match on this attribute; if not, no matches are generated for this rule.

Each combination of attributes in the match rule will be scored. If the threshold for an attribute is greater than the specified attribute level threshold then the score contributes to the overall score. If data is null for either the source or target attribute a score of 50 is given. Attribute level scores are multiplied by the weightage and then added to get the weighted average score for the customer and watchlist record. If the score is greater than the rule threshold, then the record is considered for matching.

If there are two or more rules in the ruleset then the maximum score is taken. If this score is greater than the threshold defined for the ruleset, than the two records are a match.

Table 7-2 Match Types

Logic Used	Description	Example
Exact	Considers two values and determines whether or not they match exactly. Applies only if Exact Match is selected. It does not apply when using Fuzzy Match.	If the source attribute is “John smith” and target attribute is “John smith”, then the match is an exact match.

Table 7-2   (Cont.) Match Types

Logic Used	Description	Example
Character Edit Distance (CED)	Considers two String tokens and determines how closely they match each other by calculating the minimum number of character edits (deletions, insertions and substitutions) needed to transform one value into the other. For entities, stop words are not considered.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the CED is 1 since the letter 'h' is missing between the source attribute and target attribute. If the entity names are Oracle Financial Corporation and Finance Orcl Pvt. Ltd., then only Oracle Financial and Finance Orcl are considered for matching as corporation, Pvt., and Ltd. are stop words. The CED for Orcl is 2 and CED for finance is 3, so the overall CED is 3.
Character Match Percentage (CMP)	Determines how closely two values match each other by calculating the Character Edit Distance between two String tokens and considering the length of the shorter of the two tokens, by character count.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the CMP is calculated using the formula (length of shorter string – CED) * 100 /length of longer string. In this case, it is (9-1) * 100/8 = 77.77%.

Table 7-2 (Cont.) Match Types

Logic Used	Description	Example
Word Edit Distance (WED)	Determines how well multi-word String values match each other by calculating the minimum number of word edits (word insertions, deletions and substitutions) required to transform one value to another.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the WED is calculated by checking the number of words that did not match with the target words after allowing for character tolerance, which is the number of words in the source attribute that did not match the target attribute. For example, the source string is Yohan Russel Smith and target string is Smith Johaan Rusel. First, we determine the CED for each word: • Yohan matches with Johann with a CED of 2 • Russel matches with Rusel with a CED of 1 • Smith matches with Smith with a CED of 0 • If we consider a character tolerance of 1, we can observe the following: • Russel with a character tolerance of 1 matches with Rusel. • Smith with a character tolerance of 0 matches with Smith. • Yohan with a character tolerance of 2 does not match with Johann as the character tolerance is 1. Based on these observations, we can conclude that one word does not match. This means that the WED is 1.
Word Match Percentage (WMP)	Determines how closely, by percentage, two multi-word values match each other by calculating the Word Edit Distance between two Strings, and also taking into account the length of the longer or the shorter of the two values, by word count.	The WMP is calculated using the formula (WMC/minimum word length) * 100. If the source attribute is “John smith” and target attribute is “Jon smith”, then the WMP is calculated as (2/5) * 100 = 40 %.

Table 7-2   (Cont.) Match Types

Logic Used	Description	Example
Word Match Count (WMC)	Determines how closely two multi-word values match each other by calculating the Word Edit Distance between two Strings, and also taking into account the length of the longer or the shorter of the two values, by word count.	The WMC is like WED, with the difference being that WMC gives the number of matches between 2 words and WED gives the number of words that did not match between 2 words. If the source attribute is “John smith” and target attribute is “Jon smith”, then the WMC is 2 as two words have matched (allowing for the character tolerance).
Exact String Match	Considers two String values and determines whether or not they match exactly.	
Abbreviation	Checks if the first character matches with the first character of source and target values.	
Starts With	Compares two values and determines whether either value starts with the whole of the other value. It therefore matches both exact matches and matches where one of the values starts the same as the other but contains extra information	
Jaro Winkler or Reverse Jaro Winkler	The Jaro Winkler similarity is the measure of the edit distance between two strings.Click here for more information. In the Reverse Jaro Winkler, matches are generated even if the string is reversed. For example, if the source string is Mohammed Ali and the target string is Ali Mohammed, then the similarity = 1.	If the source string is Mohammed Ali and the target string is Mohammed Ali, then the similarity = 1.
Levenshtein	The Levenshtein Distance (LD) or edit distance provides the distance, or the number of edits (deletions, insertions, or substitutions) needed to transform the source string into the target string. Click here for more information.	For example, if the source string is Mohamed and the target string is Mohammed, then the LD = 1, because there is one edit (insertion) required to match the source and target strings.

Adding Rulesets

Use the Matching Rules widget to add new rulesets.

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the Matching Rules widget and click **Edit**. Provide the following details:
   - Ruleset Name: Enter the name for your ruleset. This is a mandatory field.
   - Description: Enter the description of the ruleset. This is a mandatory field.
   - Scoring Aggregation Type: Select the scoring type. Currently, only **Maximum** is available.
   - Set Threshold: Enter the threshold value for the ruleset.
   - Source: Select **Filter** to add values for the source entity in the Add Source Entity Filters window.
     a. To add a value, click **Add** and provide the required attribute, operator, and value. Attributes can be Business Domain Code, Customer Type Code, or Jurisdiction Code. Enter the value based on the attribute. For example, a value for jurisdiction code can be JC1.
     b. Click **Save** to save the values or click **Close** to go back to the Matching Ruleset window.
   - Target: Select **Filter** to add values for the target entity in the Add Source Entity Filters window.
     a. To add a value, click **Add** and provide the required attribute, operator, and value. Attributes can be Business Domain Code, Customer Type Code, or Jurisdiction Code. Enter the value based on the attribute. For example, a value for jurisdiction code can be JC1.
     b. Click **Save** to save the values or click **Close** to go back to the Matching Ruleset window.
   - Rules: Select Add to add a rule for the ruleset.
   - Name: Enter the rule name.
   - Description: Enter the description of the ruleset. This is a mandatory field.
   - Rule Threshold: Enter the threshold value for the rule.
   - Mappings: Select Add to add a matching configuration for the rule.
   - Source Attribute: Select one or more source attributes from the customer record that must be matched.
   - Target Attribute: Select one or more attributes from the watch list against which matching is performed.
   - Match Type: Select the matching type. The following match types are available:

  - Exact
  - Fuzzy
  - Date
- Scoring Method: Select the scoring method if you have selected the match type as Fuzzy. The scoring methods described in the Using Matching Rules widget section are available:
- Threshold: Enter the threshold score.
- Weightage: Enter the weightage.
- Condition: If this check box is selected, then this condition must be met for matching.

3. Click Save ✓ to save the changes. The rule is created and is visible on the canvas. It is also available for use in the Matching Ruleset window.

   When you have finished looking through the fields and want to go back to the Pipeline Designer window, click Close ✖ to close the window. Finally, click Save ✓ to save the updates made.

Using the Alert Decision Widget

The Alert Decision widget enables you to define which customer and watchlist attributes changes should be considered for further review.

Screening happens periodically and generates alerts for new customers and watchlist records, and where important data has changed and the alert needs to be reviewed again.

The **Alert Decision** widget ⚙ enables you to define which customer and watchlist attributes changes should be considered for further review. Attributes can be set to re-alert based on whether the data has changed or only when it has caused the score to increase.

Configuring Alert Attributes

Attributes can be set to re-alert based on whether the data has changed or only when it has caused the score to increase.

1. Navigate to the Pipeline Designer page.
2. Drag and drop the Alert Decision widget ⚙ from the widgets pane in the upper-right corner of the designer pane.
3. Hover on the Alert Decision widget and click **Edit** ✎.
4. (Optional) Add a source attribute into the list of attributes where a change will trigger a re-alert.

   a. Select the attribute from the Source Attributes table and click **Move** › to move the selected attribute to the Selected Source Attributes table.

   b. You can also move multiple source attributes by selecting the applicable attributes from the Source Attributes table and clicking **Move All** » to move the selected attributes to the Selected Source Attributes table.
   c. The same steps can be repeated for target attributes and Re-alert on Score Increase.
5. Click **Save** ✓ to save the changes.

Using Auto Elimination Rules Widget

Auto Elimination rules are designed to reduce False Positives so that analysts will be provided only the events requiring a manual intervention.

Using the auto-elimination pre-set rules, you can use the Auto Elimination Rules widget to mark the events automatically as False Positive.

> **Note:**
>
> No new Auto-Elimination rules can be created in the application.

The cases and associated events generated go through the auto-elimination rules widget. If any of the auto-elimination rules are applicable as per pre-defined rule sets, those events are filtered and auto-eliminated. The auto-eliminated events will have the event decision as False Positive, and the corresponding matched rule will be added as the comment. You cannot reopen the auto-eliminated event.

Auto-elimination rules can be enabled or disabled anytime and can be enabled based on the event type (SAN/PEP/EDD/PRB). If any auto-elimination rule applies for an event, the remaining rules are not executed.

The folllowing table the auto-elimination rules and their priorities.

Table 7-3 Auto-Elimination Rules

Rule Priority	Rule Name	Description
1	Difference in date of birth	Where the Date of Birth differs between customer and watchlist
2	Difference in year of birth	Where the Year of Birth is greater than 2 years between customer and watchlist
3	Difference in gender and country	Where the Gender differs and there are no matching Countries across any of the date available in the customer and the Watchlist Profile
4	Difference in gender	Where the Gender differs between customer and watchlist

Table 7-3 (Cont.) Auto-Elimination Rules

Rule Priority	Rule Name	Description
5	Difference in nationality	Where the Nationality/ Citizenship differs between customer and watchlist
6	Difference in country	Where there are no matching Countries across any of the data available between customer and watchlist
7	Difference in year of birth when there is a relationship to PEP as Son or Daughter or Child	Where the Alert is against a Relative and Close Associate of the PEP, the relationship to the PEP is Son/Daughter/ Child
8	Difference in year of birth when there is a relationship to PEP as Mother or Father	Where the Alert is against a Relative and Close Associate of a PEP, the relationship to the PEP is Mother/Father

Evaluation Logic Used by Matching

The Customer Screening Matching Service uses evaluation logic to determine whether individuals and entities match the watch list.

Evaluation logic is the foundation for a sub-rule. A sub-rule is a combination of the evaluation logic with an AND condition. The overall score for an individual or entity is the weighted average of all the individual attribute scores.

Consider two source attributes available for matching individuals: customer last name and customer full name. The customer last name is matched with a watch list **Family Name** record and customer full name is matched with a watch list **Full Name** & **Alias Name** record using fuzzy matching. The threshold score is as configured by the user and weightage is as configured by the user. A JSON is generated when the batch is run and passed to the Matching Service.

The Entity rules work the same way as the Individual rules, except that the entity rules or logic only applies to companies and corporations.The following table provides some examples of evaluation logic for SAN, PEP, and EDD.

Table 7-4 Customer Screening Evaluation Logic

Logic Used	Description	Example
Exact	Considers two values and determines whether or not they match exactly. Applies only if Exact Match is selected. It does not apply when using Fuzzy Match.	If the source attribute is “John smith” and target attribute is “John smith”, then the match is an exact match.

Table 7-4 (Cont.) Customer Screening Evaluation Logic

Logic Used	Description	Example
Character Edit Distance (CED)	Considers two String tokens and determines how closely they match each other by calculating the minimum number of character edits (deletions, insertions and substitutions) needed to transform one value into the other. For entities, stop words are not considered.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the CED is 1 since the letter 'h' is missing between the source attribute and target attribute. If the entity names are Oracle Financial Corporation and Finance Orcl Pvt. Ltd., then only Oracle Financial and Finance Orcl are considered for matching as corporation, Pvt., and Ltd. are stop words. The CED for Orcl is 2 and CED for finance is 3, so the overall CED is 3.
Character Match Percentage (CMP)	Determines how closely two values match each other by calculating the Character Edit Distance between two String tokens and considering the length of the shorter of the two tokens, by character count.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the CMP is calculated using the formula (length of shorter string – CED) * 100 /length of longer string. In this case, it is (9-1) * 100/8 = 77.77%.

Table 7-4 (Cont.) Customer Screening Evaluation Logic

Logic Used	Description	Example
Word Edit Distance (WED)	Determines how well multi-word String values match each other by calculating the minimum number of word edits (word insertions, deletions and substitutions) required to transform one value to another.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the WED is calculated by checking the number of words that did not match with the target words after allowing for character tolerance, which is the number of words in the source attribute that did not match the target attribute. For example, the source string is Yohan Russel Smith and target string is Smith Johaan Rusel. First, we determine the CED for each word: • Yohan matches with Johann with a CED of 2 • Russel matches with Rusel with a CED of 1 • Smith matches with Smith with a CED of 0 • If we consider a character tolerance of 1, we can observe the following: • Russel with a character tolerance of 1 matches with Rusel. • Smith with a character tolerance of 0 matches with Smith. • Yohan with a character tolerance of 2 does not match with Johann as the character tolerance is 1. Based on these observations, we can conclude that one word does not match. This means that the WED is 1.
Word Match Percentage (WMP)	Determines how closely, by percentage, two multi-word values match each other by calculating the Word Edit Distance between two Strings, and also taking into account the length of the longer or the shorter of the two values, by word count.	The WMP is calculated using the formula (WMC/minimum word length) * 100. If the source attribute is “John smith” and target attribute is “Jon smith”, then the WMP is calculated as (2/5) * 100 = 40 %.

Table 7-4 (Cont.) Customer Screening Evaluation Logic

Logic Used	Description	Example
Word Match Count (WMC)	Determines how closely two multi-word values match each other by calculating the Word Edit Distance between two Strings, and also taking into account the length of the longer or the shorter of the two values, by word count.	The WMC is like WED, with the difference being that WMC gives the number of matches between 2 words and WED gives the number of words that did not match between 2 words. If the source attribute is “John smith” and target attribute is “Jon smith”, then the WMC is 2 as two words have matched (allowing for the character tolerance).
Exact String Match	Considers two String values and determines whether or not they match exactly.	
Abbreviation	Checks if the first character matches with the first character of source and target values.	
Starts With	Compares two values and determines whether either value starts with the whole of the other value. It therefore matches both exact matches and matches where one of the values starts the same as the other but contains extra information	
Jaro Winkler	The Jaro Winkler similarity is the measure of the edit distance between two strings.	If the source string is Mohammed Ali and the target string is Mohammed Ali, then the similarity = 1.

8 Managing Transaction Filtering Pipelines

Organizations need to effectively and efficiently screen their transactions to successfully meet antibribery, anti-corruption, export control, and other legal regulations as well as all current anti-money laundering and counter-terrorist financing legislation.

Oracle Financial Services Transaction Filtering Cloud Service (TFCS) enables organizations to scan payment messages and identify individuals, entities, prohibited lists, private watchlists, and Stop keywords that may be sanctioned in relation to a transaction that is processed.

Transaction Filtering pipelines are used to configure watchlist data for screening.

Pre-configured Transaction Filtering Pipelines

FCCM TF Cloud Service provides a set of pre-configured Transaction Filtering pipelines.

The application comes with the following ready-to-use Transaction Filtering pipelines:

> **Note:**
>
> Transaction Filtering pipelines are only available if your firm has implemented Oracle FCCM Transaction Filtering Cloud Service.

- Swift And Fedwire Screening
- ISO Screening
- StopKeyword Watchlist
- City Data Load
- Country Data Load
- Goods Data Load
- Port Data Load
- Load Identifier

Import the ready-to-use pipelines to the application. To configure pipelines, you must create a copy of an imported pipeline and save it as a new pipeline.

Widgets in Transaction Filtering Pipelines

Depending on the pipeline type, specific widgets are available in the widgets pane of the pipeline.

The following table describes the widgets available in Transaction Filtering pipelines.

Table 8-1 Widgets in Transaction Filtering Pipelines

Widget	Name	Description
	Decision	Use this widget to define which transaction and watchlist attributes changes should be considered clean or should be moved as a case.
	Data Transformation	Use this widget to generate the transformed input before sending to the matching rule.
	Entity	Use this widget to link to data that has been loaded into indexes for matching. An entity can be an individual, organization, and so on.
	Input JSON	Use this widget to view the available input attributes in Transaction Screening.
	Matching Rules	Use this widget to configure how matching occurs for a set of data.
	Scoring	The Scoring widget enables you to see the type of transaction which is being assessed and the risk category score associated with the transaction.
	External Service	Use this widget to add an external service. External Services perform actions on the data, such as loading or moving the data, or performing a virus scan.

About the Decision Widget

The Decision widget enables you to define which transaction and watchlist attributes changes should be considered clean or should be generated as a case.

Screening happens periodically and generates alerts for new transactions and watchlist records. Screening also occurs when important data has changed and the alert needs to be reviewed again. The Decision widget enables you to define which transaction and watchlist attributes changes should be considered clean or should be generated as a case.

About the Data Transformation Widget

The Data Transformation widget generates a transformed input by removing special characters.

This transformed input is then sent to the matching rule widget. Other than period (.) and comma (,), all special characters are removed.

About the Entity Widget

The Entity widget is similar to the Dataset widget used in other pipelines, except that instead of reading data from a table it links to data that has been loaded into indexes for matching.

The Entity widget allows you to specify the entity name and displays the associated columns that are available. You can also specify if the entity is the source or target for the matching. All screening pipelines must specify a single source and target.

About the Input JSON Widget

The Input JSON widget displays the available request attributes in Transaction Screening.

You can also specify if the entity is the source or target for matching.All screening pipelines must specify a single source and target.

Using the Matching Rules Widget

The Matching Rules widget enables you to define the matching configuration for a set of data.

The data that must be matched by each widget depends on the source and target set in the Entity widgets linked to the Matching Rules widget. The source and target data can be filtered if a subset of data is to have this matching configuration applied. This allows you to provide different matching configurations for different types of watchlist records and different jurisdictions and domains. Each matching ruleset contains the name, description, scoring aggregation used, the threshold value for the overall rule set and one or more rules.

Rules are configured using the Matching Ruleset window. Matches are generated based on a defined set of attributes for each rule. A weighted average of the score is generated for each of the attribute level matches. There are two types of matching services :

- Real-Time query processing
- Bulk query processing

In Real-Time query processing, a string value given in the UI is matched against a column in the target table. Customer Screening explicitly passes the strings as values in the request which forms “the strings to be matched” against “all the values in a column name”. Then, based on the matches received for the source string from the search engine, the score and the feature vector for the matched strings (source and target) are generated. Scores which exceed the configured thresholds are taken and collected.

Provide the following values for each rule:

- Source attribute
- Target attribute
- Match type (The Match Types table provides some examples)
- Scoring Method (This can be one of the following:)
  - Levenshtein: The Levenshtein Distance (LD) or edit distance provides the distance, or the number of edits (deletions, insertions, or substitutions) needed to transform the source string into the target string. For example, if the source string is Mohamed and the target string is Mohammed, then the LD = 1, because there is one edit (insertion) required to match the source and target strings.
  - Jaro Winkler: The Jaro Winkler similarity is the measure of the edit distance between two strings. For example, if the source string is Mohammed Ali and the target string is Mohammed Ali, then the similarity = 1.
  - Reverse Jaro Winkler: In the Reverse Jaro Winkler, matches are generated even if the string is reversed. For example, if the source string is Mohammed Ali and the target string is Ali Mohammed, then the similarity = 1.
  - Individual SAN: The details are provided in the Matching Guide.
  - Entity SAN: The details are provided in the Matching Guide.
  - Individual PEP: The details are provided in the Matching Guide.
  - Entity PEP: The details are provided in the Matching Guide.
  - Individual EDD: The details are provided in the Matching Guide.
  - Entity EDD: The details are provided in the Matching Guide.
- Set threshold value: If this value is crossed then the attribute is considered for matching
- Weightage assigned to the attribute (total of all attributes within a rule must equal 1)
- Must check box (optional): If this check box is selected, then there must be a match on this attribute; if not, no matches are generated for this rule.

Each combination of attributes in the match rule will be scored. If the threshold for an attribute is greater than the specified attribute level threshold then the score contributes to the overall score. If data is null for either the source or target attribute a score of 50 is given. Attribute level scores are multiplied by the weightage and then added to get the weighted average score for the customer and watchlist record. If the score is greater than the rule threshold, then the record is considered for matching.

If there are two or more rules in the ruleset then the maximum score is taken. If this score is greater than the threshold defined for the ruleset, than the two records are a match.

Table 8-2 Match Types

Logic Used	Description	Example
Exact	Considers two values and determines whether or not they match exactly. Applies only if Exact Match is selected. It does not apply when using Fuzzy Match.	If the source attribute is “John smith” and target attribute is “John smith”, then the match is an exact match.
Character Edit Distance (CED)	Considers two String tokens and determines how closely they match each other by calculating the minimum number of character edits (deletions, insertions and substitutions) needed to transform one value into the other. For entities, stop words are not considered.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the CED is 1 since the letter 'h' is missing between the source attribute and target attribute. If the entity names are Oracle Financial Corporation and Finance Orcl Pvt. Ltd., then only Oracle Financial and Finance Orcl are considered for matching as corporation, Pvt., and Ltd. are stop words. The CED for Orcl is 2 and CED for finance is 3, so the overall CED is 3.
Character Match Percentage (CMP)	Determines how closely two values match each other by calculating the Character Edit Distance between two String tokens and considering the length of the shorter of the two tokens, by character count.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the CMP is calculated using the formula (length of shorter string – CED) * 100 /length of longer string. In this case, it is (9-1) * 100/8 = 77.77%.

Table 8-2 (Cont.) Match Types

Logic Used	Description	Example
Word Edit Distance (WED)	Determines how well multi-word String values match each other by calculating the minimum number of word edits (word insertions, deletions and substitutions) required to transform one value to another.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the WED is calculated by checking the number of words that did not match with the target words after allowing for character tolerance, which is the number of words in the source attribute that did not match the target attribute. For example, the source string is Yohan Russel Smith and target string is Smith Johaan Rusel. First, we determine the CED for each word: • Yohan matches with Johann with a CED of 2 • Russel matches with Rusel with a CED of 1 • Smith matches with Smith with a CED of 0 • If we consider a character tolerance of 1, we can observe the following: • Russel with a character tolerance of 1 matches with Rusel. • Smith with a character tolerance of 0 matches with Smith. • Yohan with a character tolerance of 2 does not match with Johann as the character tolerance is 1. Based on these observations, we can conclude that one word does not match. This means that the WED is 1.
Word Match Percentage (WMP)	Determines how closely, by percentage, two multi-word values match each other by calculating the Word Edit Distance between two Strings, and also taking into account the length of the longer or the shorter of the two values, by word count.	The WMP is calculated using the formula (WMC/minimum word length) * 100. If the source attribute is “John smith” and target attribute is “Jon smith”, then the WMP is calculated as (2/5) * 100 = 40 %.

Table 8-2 (Cont.) Match Types

Logic Used	Description	Example
Word Match Count (WMC)	Determines how closely two multi-word values match each other by calculating the Word Edit Distance between two Strings, and also taking into account the length of the longer or the shorter of the two values, by word count.	The WMC is like WED, with the difference being that WMC gives the number of matches between 2 words and WED gives the number of words that did not match between 2 words. If the source attribute is “John smith” and target attribute is “Jon smith”, then the WMC is 2 as two words have matched (allowing for the character tolerance).
Exact String Match	Considers two String values and determines whether or not they match exactly.	
Abbreviation	Checks if the first character matches with the first character of source and target values.	
Starts With	Compares two values and determines whether either value starts with the whole of the other value. It therefore matches both exact matches and matches where one of the values starts the same as the other but contains extra information	
Jaro Winkler or Reverse Jaro Winkler	The Jaro Winkler similarity is the measure of the edit distance between two strings.Click here for more information. In the Reverse Jaro Winkler, matches are generated even if the string is reversed. For example, if the source string is Mohammed Ali and the target string is Ali Mohammed, then the similarity = 1.	If the source string is Mohammed Ali and the target string is Mohammed Ali, then the similarity = 1.
Levenshtein	The Levenshtein Distance (LD) or edit distance provides the distance, or the number of edits (deletions, insertions, or substitutions) needed to transform the source string into the target string. Click here for more information.	For example, if the source string is Mohamed and the target string is Mohammed, then the LD = 1, because there is one edit (insertion) required to match the source and target strings.

About the Scoring Widget

The Scoring widget enables you to see Transaction Filtering's pre-configured matching rules set.

With respect to the matching rule a score is generated. If the value exceeds the frequency score (the default value is 60) a Alert/Case is generated. If the score is less than the frequency score then the transaction is considered as clean.

Using the External Service Widget

The External Service is used if a case must be created for the particular risk assessment.

External Service refers to an existing set of services that the customer can use to derive the risk of certain business entities, configure data movement for case management, create events, and so on. The External Service widget is used if a case must be created for the particular risk assessment.

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the External Service widget and click Edit . The External Service window is displayed.
3. Select the external service name. The Description, Input Parameter Name, Input Parameter Values, Output Parameter Name, and Output Parameter Value details are displayed based on the selected External Service.
4. You can add or remove the Input Parameter values using the Add and Remove icons.
    - To add the Input Parameters, click **Add** in the Input Parameter section, and click on the Input Parameter Name and Input Parameter Values column to enter the name and value details.
    - To remove the Input Parameters, select the Parameter from the list and click **Remove** .
5. You can add or remove the Output Parameter values using the Add and Remove icons.
    - To add the Output Parameters, click **Add**in the Input Parameter section, and click on the Input Parameter Name and Input Parameter Values column to enter the name and value details.
    - To remove the Output Parameters, select the Parameter from the list and click **Remove**.
6. Click **Save** ✓ to save the values.

   To return to the Pipeline Designer window, click **Close** ✗to close the window.

   Finally, click **Save** ✓to save the updates made.

Evaluation Logic Used by Matching

The Customer Screening Matching Service uses evaluation logic to determine whether individuals and entities match the watch list.

Evaluation logic is the foundation for a sub-rule. A sub-rule is a combination of the evaluation logic with an AND condition. The overall score for an individual or entity is the weighted average of all the individual attribute scores.

Consider two source attributes available for matching individuals: customer last name and customer full name. The customer last name is matched with a watch list **Family Name** record and customer full name is matched with a watch list **Full Name** & **Alias Name** record using fuzzy matching. The threshold score is as configured by the user and weightage is as configured by the user. A JSON is generated when the batch is run and passed to the Matching Service.

The Entity rules work the same way as the Individual rules, except that the entity rules or logic only applies to companies and corporations.The following table provides some examples of evaluation logic for SAN, PEP, and EDD.

Table 8-3 Customer Screening Evaluation Logic

Logic Used	Description	Example
Exact	Considers two values and determines whether or not they match exactly. Applies only if Exact Match is selected. It does not apply when using Fuzzy Match.	If the source attribute is “John smith” and target attribute is “John smith”, then the match is an exact match.
Character Edit Distance (CED)	Considers two String tokens and determines how closely they match each other by calculating the minimum number of character edits (deletions, insertions and substitutions) needed to transform one value into the other. For entities, stop words are not considered.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the CED is 1 since the letter 'h' is missing between the source attribute and target attribute. If the entity names are Oracle Financial Corporation and Finance Orcl Pvt. Ltd., then only Oracle Financial and Finance Orcl are considered for matching as corporation, Pvt., and Ltd. are stop words. The CED for Orcl is 2 and CED for finance is 3, so the overall CED is 3.
Character Match Percentage (CMP)	Determines how closely two values match each other by calculating the Character Edit Distance between two String tokens and considering the length of the shorter of the two tokens, by character count.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the CMP is calculated using the formula (length of shorter string – CED) * 100 /length of longer string. In this case, it is (9-1) * 100/8 = 77.77%.

Table 8-3 (Cont.) Customer Screening Evaluation Logic

Logic Used	Description	Example
Word Edit Distance (WED)	Determines how well multi-word String values match each other by calculating the minimum number of word edits (word insertions, deletions and substitutions) required to transform one value to another.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the WED is calculated by checking the number of words that did not match with the target words after allowing for character tolerance, which is the number of words in the source attribute that did not match the target attribute. For example, the source string is Yohan Russel Smith and target string is Smith Johaan Rusel. First, we determine the CED for each word: • Yohan matches with Johann with a CED of 2 • Russel matches with Rusel with a CED of 1 • Smith matches with Smith with a CED of 0 • If we consider a character tolerance of 1, we can observe the following: • Russel with a character tolerance of 1 matches with Rusel. • Smith with a character tolerance of 0 matches with Smith. • Yohan with a character tolerance of 2 does not match with Johann as the character tolerance is 1. Based on these observations, we can conclude that one word does not match. This means that the WED is 1.
Word Match Percentage (WMP)	Determines how closely, by percentage, two multi-word values match each other by calculating the Word Edit Distance between two Strings, and also taking into account the length of the longer or the shorter of the two values, by word count.	The WMP is calculated using the formula (WMC/minimum word length) * 100. If the source attribute is “John smith” and target attribute is “Jon smith”, then the WMP is calculated as (2/5) * 100 = 40 %.

Table 8-3 (Cont.) Customer Screening Evaluation Logic

Logic Used	Description	Example
Word Match Count (WMC)	Determines how closely two multi-word values match each other by calculating the Word Edit Distance between two Strings, and also taking into account the length of the longer or the shorter of the two values, by word count.	The WMC is like WED, with the difference being that WMC gives the number of matches between 2 words and WED gives the number of words that did not match between 2 words. If the source attribute is “John smith” and target attribute is “Jon smith”, then the WMC is 2 as two words have matched (allowing for the character tolerance).
Exact String Match	Considers two String values and determines whether or not they match exactly.	
Abbreviation	Checks if the first character matches with the first character of source and target values.	
Starts With	Compares two values and determines whether either value starts with the whole of the other value. It therefore matches both exact matches and matches where one of the values starts the same as the other but contains extra information	
Jaro Winkler	The Jaro Winkler similarity is the measure of the edit distance between two strings.	If the source string is Mohammed Ali and the target string is Mohammed Ali, then the similarity = 1.

9

Configuring KYC Risk

Transaction Monitoring can assess the KYC Risk of customers by calculating the KYC Risk Score through Oracle's Know Your Customer Cloud Service (KYC CS), or by providing KYC risk values using staging data.

> **Note:**
>
> Only one configuration method can be used in your implementation. Both methods cannot be deployed together.

By default, Transaction Monitoring is configured to read customer KYC risk information from Oracle KYC CS. Additional configuration is not required. For more information about KYC Pipelines, see Managing KYC Onboarding Pipelines and Managing KYC Batch Pipelines.

To provide customer KYC risk values from staging data, such as from STG_PARTY_MASTER.N_KYC_RISK, you must change the mapping in the ‘Load Customer Data’ pipeline from Direct to Type2. For steps on how to change the mapping, see Changing KYC Risk to Staging Data.

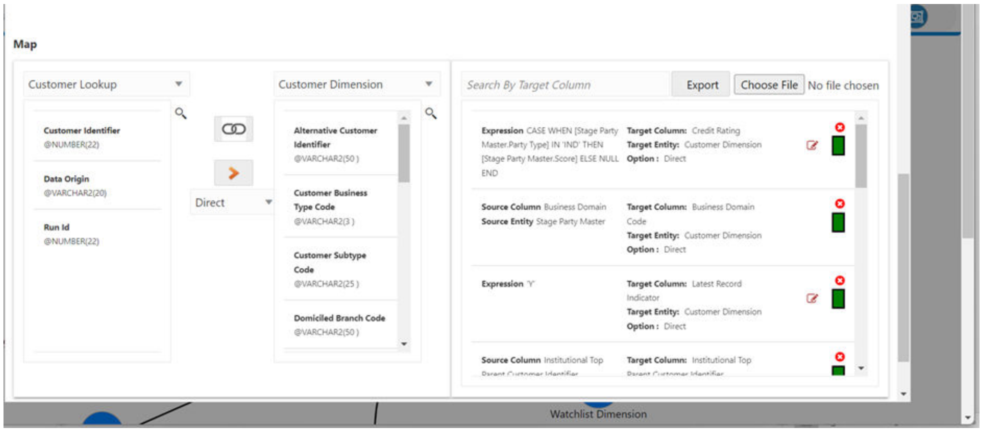
Changing KYC Risk to Staging Data

To provide customer KYC risk values from staging data, such as from STG_PARTY_MASTER.N_KYC_RISK, you must change the mapping in the ‘Load Customer Data’ pipeline from Direct to Type2.

To change the mapping, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Search for and open the **Load Customer Data** pipeline.
3. Copy and rename the pipeline, following the steps in Copying Pipelines.
4. In the new pipeline, open the Customer Dimension_1 Persist widget and scroll until you reach the **Map** panel.

Figure 9-1   Map panel



Customer Identifier @NUMBER(22)
Data Origin @VARCHAR2(20)
Run Id @NUMBER(22)

Alternative Customer Identifier @VARCHAR2(50)
Customer Business Type Code @VARCHAR2(3)
Customer Subtype Code @VARCHAR2(25)
Domiciled Branch Code @VARCHAR2(50)

Expression CASE WHEN [Stage Party Master.Party Type] IN 'IND' THEN [Stage Party Master.Score] ELSE NULL END **Target Column:** Credit Rating **Target Entity:** Customer Dimension **Option :** Direct

Source Column Business Domain **Source Entity** Stage Party Master **Target Column:** Business Domain Code **Target Entity:** Customer Dimension **Option :** Direct

Expression 'Y' **Target Column:** Latest Record Indicator **Target Entity:** Customer Dimension **Option :** Direct

Source Column Institutional Top Parent Customer Identifier **Target Column:** Institutional Top Parent Customer Identifier

5. Enter **Customer KYC risk** in the **Search by Target Column** search field. The following mapping displays:Expression NVL([Stage Party Master.Customer Kyc Risk Number] , ‘ 0 ‘)
   - Target Column: Customer Kyc Risk Number
   - Target Entity: Customer Dimension
   - Option: Direct
6. Click **Remove** ✖ to remove the mapping.
7. Replace the Customer Lookup mapping by selecting **Stage Party Master** from the drop-down list.
8. Select **Customer Kyc Risk Number** from the available list values.
9. In the Customer Dimension mapping, select **Customer Kyc Risk Number** from the available list of values.
10. Build the expression by following these steps:

    a. Click **Add Expression** ⊞.

    b. Enter **NVL** in the Condition field and then select an Opening bracket “ **(** “.

    c. Select the **Select Attributes** checkbox.

    d. Select **Stage Party Master** from the Dataset drop-down list.

    e. Select **Customer Kyc Risk Number** from the Attribute drop-down list.

    f. Select a “ **,** ” comma and type “ **0** “ in the Condition text field, then select a closing bracket “ **)** “.

    g. Click **Save** ✓ to save the new expression.

    NVL([Stage Party Master.Customer Kyc Risk Number] , 0)
11. Change the mapping option from Direct to **Type2** in the drop-down list and click **Map** .
12. Verify the mapping is correct by typing Customer KYC risk in the Search by Target Column search field. The mapping should be displayed as follows:

    Expression NVL([Stage Party Master.Customer Kyc Risk Number] , 0)

Target Column: Customer Kyc Risk Number

Target Entity: Customer Dimension

Option: Type2

13. Click **Save** ✓ to save the Customer Dimension_1 Persist widget.
14. In the Pipeline Designer page, click **Save**to save all updates.

10

Managing KYC Onboarding Pipelines

Oracle Financial Crime and Compliance Management Know Your Customer Cloud Service uses KYC Onboarding pipelines to assess and evaluate prospects.

> **Note:**
>
> KYC Onboarding pipelines are only available if your firm has implemented Oracle FCCM Know Your Customer Cloud Service.

Widgets in KYC Onboarding Pipelines

Depending on the pipeline type, specific widgets are available in the widgets pane of the pipeline.

The following table describes the widgets available in KYC Onboarding pipelines.

Table 10-1 KYC Onboarding Pipeline Widgets

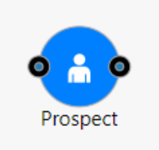
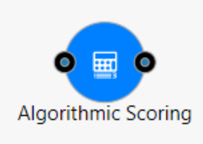
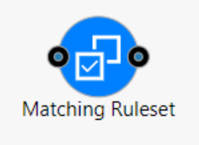
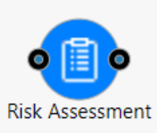
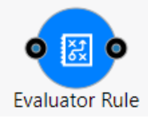
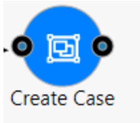
Widget	Name	Description
	Prospect	Use this widget to view the list of all attributes that are part of real-time KYC API Onboarding request.
	Algorithmic Scoring	Use this widget to understand the type of prospect which is being assessed and the risk category score associated with the prospect.
	Business Check	Use this widget to score for a business check rule associated with the prospect.
	Matching Ruleset	Use this widget to configure watchlist rules for various customer types to be screened against different watchlist types (Sanctions, PEP, EDD).
	Risk Assessment	Use this widget to set the threshold scores for a prospect and related jurisdiction.

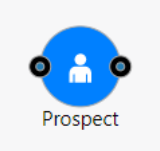
Table 10-1 (Cont.) KYC Onboarding Pipeline Widgets

Widget	Name	Description
	Evaluator Rule	Use this widget to determine the final risk score for each prospect type based on the KYC risk score and business check risk score values.
	Create Case/External Service	Use this widget to configure External Pipeline service for case creation.

Using the Prospect Widget

Use the Prospect widget to view all the fields and the corresponding values that are available in the Prospect JSON.

To view the details of the Prospect JSON, follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the Prospect widget  and click **Edit** ✎. The KYC Prospect window is displayed.

   To view the field details, click a hyperlinked value. When you first access the window, not all fields are visible. To view more fields, click **Expand** ▶.

   To return to the Pipeline Designer window, click **Close** ✖ to close the window.

   Finally, click **Save** ✓ to save the updates made.

Using the Algorithmic Scoring Widget

The Algorithmic Scoring widget enables you to see the type of prospect or customer which is being assessed and the risk category score associated with the prospect or customer.

The jurisdiction must be mapped to the pipeline. Based on the mapped jurisdiction, the pipeline is displayed in the scoring table of the Algorithmic Scoring window.

> **Note:**
>
> The pipeline can be used ONLY if you provide the Account opening jurisdiction value in the onboarding JSON.

To create a scoring rule, follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the Scoring Rule widget and click **Edit** . The KYC Scoring window is displayed.
3. Select a customer type. Click **Add** to add a new risk category. A new row is displayed.
4. Provide the following details as described in the following table:

Table 10-2 Scoring Rule Widgets

Field	Description
Risk Category Name *	Enter a risk category name.
Weightage*	Enter the weightage you want the new risk category to have. The total of all risk category weightages must equal 100.
Risk Elements	Click **Add** to add a risk element to the risk category. **Note:** Do not add a Risk Element that is Deactivated in the Risk Element Configuration window. For more information, See Configure KYC Administration Data.
Attributes Risk Scores*	To add a risk score for all attributes of the rule, follow these steps: a. Click **Lookup** . The Lookup Scores View Screen window is displayed. b. Enter the risk score in the **Default Score Value** field. c. Click **Populate** . The risk scores are added for all the attributes.
Weightage*	Enter the weightage you want the new risk element to have. The total of all risk element weightages must equal 100.
Default Risk Score*	Enter the default risk score for the risk element. If you do not add a default score, it is added by the system.

5. Click **Save** to save the changes.

> **Note:**
>
> **ATTENTION:**You must add risk scores for the attributes of all risk elements in order to save the risk score.

After you add a rule, you can edit the risk elements.

- Click **Edit** ✎ in line with the risk category you want to edit. Edit icons are displayed against each risk element.
- Click **Edit** ✎in line with the weightage and default risk score of the risk element you want to edit and click**Save** ✓
- Click **Delete** 🗑 to delete the risk category or an individual risk element.
- When you have finished looking through the fields and want to go back to the Pipeline Designer window, click **Close** ✖to close the window. Finally, click **Save** ✓to save the updates made.

Using the Business Check Widget

The Business Check widget shows the score for a business check rule associated with the prospect or customer.

Each business check value has a risk score associated with it. To create a business check, follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover on the Business Check widget and click **Edit** ✎ . The Business Check window is displayed.
3. Select a prospect or customer type.
4. Click **Add**➕ to add a new business check. A new row is displayed.
5. Provide details as described in the following table:

Table 10-3 Business Check Widget Fields

Field	Description
Rule Name	Select the rule name. **Note:** Do not add a Rule Element that is Deactivated in the Risk Element Configuration window. For more information, See Configure KYC Administration Data.
Value	To add a risk score for all attributes of the rule, follow these steps: a. Click **Lookup** ⚖ . The Lookup Scores View Screen window is displayed. b. Enter the risk score in the **Populate Default Score Value** field. c. Click **Populate** →. The risk scores are added for all the attributes.
Default Risk Score	Enter the default risk score. If you do not add a default score, it is added by the system.

6. Click **Save** ✓ to save the values. You can also click **Reset** to reset the values in the fields.

> **Note:**
>
> **ATTENTION:**You must add risk scores for the attributes of all risk elements in order to save the risk score.

After you add a rule, you can edit the risk elements.

- Click **Edit** ✎ in line with the risk category you want to edit. Edit icons are displayed against each risk element.
- Click **Edit** ✎ in line with the weightage and default risk score of the risk element you want to edit and click**Save** ✓
- Click **Delete** 🗑 to delete the risk category or an individual risk element.

- When you have finished looking through the fields and want to go back to the Pipeline Designer window, click **Close** ✖ to close the window. Finally, click **Save** ✔ to save the updates made.

Using the Risk Assessment Widget

The Risk Assessment widget enables you to set the threshold scores for a prospect and related jurisdiction using the Risk Assessment Category window.

The Risk Assessment Score is the maximum score of the KYC risk score and Business Check score.

> **Note:**
>
> You must save your changes after adding the scores.

For each jurisdiction, when you provide the range of scores for a risk category, they must cover all numbers from 0 to 100. Also, the minimum score of the next risk category must be one number more than the maximum score of the previous risk category. For example:

- The minimum score for the first risk category is 0, and the maximum score for the same risk category is 40.
- The minimum score for the next risk category is 41, and the maximum score for the same risk category is 80.
- The minimum score for the next risk category is 81, and the maximum score for the same risk category is 100.

To create a scoring rule, follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the Risk Assessment widget and click **Edit** ✎. The Risk Assessment Category window is displayed.
3. Select a prospect type.
4. Click **Add** ➕ to add a new risk assessment category.
5. Provide details as described in the following table:

Table 10-4 Risk Assessment Widget Fields

Field	Description
Category Name*	Select the category name.

Table 10-4 (Cont.) Risk Assessment Widget Fields

Field	Description
Risk Assessment Score >= *	Enter the minimum risk assessment score. After you add a score, you can edit the value by clicking **Edit** ✎ in line with the score you want to edit, updating the new score, and clicking **Save** ✓. Click **Delete** 🗑 to delete the score.
Risk Assessment Score <=*	Enter the maximum risk assessment score. After you add a score, you can edit the value by clicking **Edit** ✎ in line with the score you want to edit, updating the new score, and clicking **Save** ✓. Click **Delete** 🗑 to delete the score.

To return to the Pipeline Designer window, click **Close** ✖ to close the window. Finally, click **Save** ✓ to save the updates made.

Using the Matching Rules Widget

The Matching Rules widget enables you to define the matching configuration for a set of data.

The data that must be matched by each widget depends on the source and target set in the Entity widgets linked to the Matching Rules widget. The source and target data can be filtered if a subset of data is to have this matching configuration applied. This allows you to provide different matching configurations for different types of watchlist records and different jurisdictions and domains. Each matching ruleset contains the name, description, scoring aggregation used, the threshold value for the overall rule set and one or more rules.

Rules are configured using the Matching Ruleset window. Matches are generated based on a defined set of attributes for each rule. A weighted average of the score is generated for each of the attribute level matches. There are two types of matching services :

- Real-Time query processing
- Bulk query processing

In Real-Time query processing, a string value given in the UI is matched against a column in the target table. Customer Screening explicitly passes the strings as values in the request which forms “the strings to be matched” against “all the values in a column name”. Then, based on the matches received for the source string from the search engine, the score and the feature vector for the matched strings (source and target) are generated. Scores which exceed the configured thresholds are taken and collected.

Provide the following values for each rule:

- Source attribute
- Target attribute

- Match type (The Match Types table provides some examples)
- Scoring Method (This can be one of the following:)
  - Levenshtein: The Levenshtein Distance (LD) or edit distance provides the distance, or the number of edits (deletions, insertions, or substitutions) needed to transform the source string into the target string. For example, if the source string is Mohamed and the target string is Mohammed, then the LD = 1, because there is one edit (insertion) required to match the source and target strings.
  - Jaro Winkler: The Jaro Winkler similarity is the measure of the edit distance between two strings. For example, if the source string is Mohammed Ali and the target string is Mohammed Ali, then the similarity = 1.
  - Reverse Jaro Winkler: In the Reverse Jaro Winkler, matches are generated even if the string is reversed. For example, if the source string is Mohammed Ali and the target string is Ali Mohammed, then the similarity = 1.
  - Individual SAN: The details are provided in the Matching Guide.
  - Entity SAN: The details are provided in the Matching Guide.
  - Individual PEP: The details are provided in the Matching Guide.
  - Entity PEP: The details are provided in the Matching Guide.
  - Individual EDD: The details are provided in the Matching Guide.
  - Entity EDD: The details are provided in the Matching Guide.
- Set threshold value: If this value is crossed then the attribute is considered for matching
- Weightage assigned to the attribute (total of all attributes within a rule must equal 1)
- Must check box (optional): If this check box is selected, then there must be a match on this attribute; if not, no matches are generated for this rule.

Each combination of attributes in the match rule will be scored. If the threshold for an attribute is greater than the specified attribute level threshold then the score contributes to the overall score. If data is null for either the source or target attribute a score of 50 is given. Attribute level scores are multiplied by the weightage and then added to get the weighted average score for the customer and watchlist record. If the score is greater than the rule threshold, then the record is considered for matching.

If there are two or more rules in the ruleset then the maximum score is taken. If this score is greater than the threshold defined for the ruleset, than the two records are a match.

Table 10-5 Match Types

Logic Used	Description	Example
Exact	Considers two values and determines whether or not they match exactly. Applies only if Exact Match is selected. It does not apply when using Fuzzy Match.	If the source attribute is “John smith” and target attribute is “John smith”, then the match is an exact match.

Table 10-5 (Cont.) Match Types

Logic Used	Description	Example
Character Edit Distance (CED)	Considers two String tokens and determines how closely they match each other by calculating the minimum number of character edits (deletions, insertions and substitutions) needed to transform one value into the other. For entities, stop words are not considered.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the CED is 1 since the letter 'h' is missing between the source attribute and target attribute. If the entity names are Oracle Financial Corporation and Finance Orcl Pvt. Ltd., then only Oracle Financial and Finance Orcl are considered for matching as corporation, Pvt., and Ltd. are stop words. The CED for Orcl is 2 and CED for finance is 3, so the overall CED is 3.
Character Match Percentage (CMP)	Determines how closely two values match each other by calculating the Character Edit Distance between two String tokens and considering the length of the shorter of the two tokens, by character count.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the CMP is calculated using the formula (length of shorter string – CED) * 100 /length of longer string. In this case, it is (9-1) * 100/8 = 77.77%.

Table 10-5 (Cont.) Match Types

Logic Used	Description	Example
Word Edit Distance (WED)	Determines how well multi-word String values match each other by calculating the minimum number of word edits (word insertions, deletions and substitutions) required to transform one value to another.	If the source attribute is “John smith” and target attribute is “Jon smith”, then the WED is calculated by checking the number of words that did not match with the target words after allowing for character tolerance, which is the number of words in the source attribute that did not match the target attribute. For example, the source string is Yohan Russel Smith and target string is Smith Johaan Rusel. First, we determine the CED for each word: • Yohan matches with Johann with a CED of 2 • Russel matches with Rusel with a CED of 1 • Smith matches with Smith with a CED of 0 • If we consider a character tolerance of 1, we can observe the following: • Russel with a character tolerance of 1 matches with Rusel. • Smith with a character tolerance of 0 matches with Smith. • Yohan with a character tolerance of 2 does not match with Johann as the character tolerance is 1. Based on these observations, we can conclude that one word does not match. This means that the WED is 1.
Word Match Percentage (WMP)	Determines how closely, by percentage, two multi-word values match each other by calculating the Word Edit Distance between two Strings, and also taking into account the length of the longer or the shorter of the two values, by word count.	The WMP is calculated using the formula (WMC/minimum word length) * 100. If the source attribute is “John smith” and target attribute is “Jon smith”, then the WMP is calculated as (2/5) * 100 = 40 %.

Table 10-5 (Cont.) Match Types

Logic Used	Description	Example
Word Match Count (WMC)	Determines how closely two multi-word values match each other by calculating the Word Edit Distance between two Strings, and also taking into account the length of the longer or the shorter of the two values, by word count.	The WMC is like WED, with the difference being that WMC gives the number of matches between 2 words and WED gives the number of words that did not match between 2 words. If the source attribute is “John smith” and target attribute is “Jon smith”, then the WMC is 2 as two words have matched (allowing for the character tolerance).
Exact String Match	Considers two String values and determines whether or not they match exactly.	
Abbreviation	Checks if the first character matches with the first character of source and target values.	
Starts With	Compares two values and determines whether either value starts with the whole of the other value. It therefore matches both exact matches and matches where one of the values starts the same as the other but contains extra information	
Jaro Winkler or Reverse Jaro Winkler	The Jaro Winkler similarity is the measure of the edit distance between two strings.Click here for more information. In the Reverse Jaro Winkler, matches are generated even if the string is reversed. For example, if the source string is Mohammed Ali and the target string is Ali Mohammed, then the similarity = 1.	If the source string is Mohammed Ali and the target string is Mohammed Ali, then the similarity = 1.
Levenshtein	The Levenshtein Distance (LD) or edit distance provides the distance, or the number of edits (deletions, insertions, or substitutions) needed to transform the source string into the target string. Click here for more information.	For example, if the source string is Mohamed and the target string is Mohammed, then the LD = 1, because there is one edit (insertion) required to match the source and target strings.

Using the Evaluator Rule Widget

The Evaluator Rule widget enables you to set the threshold scores for the case creation for a customer type.

Additionally, it allows an optional configuration to mark case creation whenever there is a change in the current vs last risk category for the customer. To create an evaluator rule, follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the Evaluator Rule widget and click **Edit** ✎ . The Evaluator window displays.
3. Select a customer type. The criteria for case creation displays.
4. Click Edit to update the score.
   - Update the threshold risk score for case creation in the **Risk Assessment Score >=** field. If the Risk assessment score of the customer is equal or above the score in this field then the customer is marked for case creation.
   - Update the **Create Case (if change in current vs last risk category**) field accordingly with the available options on when to mark for the case creation. **Not Applicable** is the default option chosen.
5. Click **Save** ✓ to save the values.

   To return to the Pipeline Designer window, click **Close** ✖to close the window.

   Finally, click **Save** ✓to save the updates made.

Using the External Service Widget

The External Service is used if a case must be created for the particular risk assessment.

External Service refers to an existing set of services that the customer can use to derive the risk of certain business entities, configure data movement for case management, create events, and so on. The External Service widget is used if a case must be created for the particular risk assessment.

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the External Service widget and click Edit . The External Service window is displayed.
3. Select the external service name. The Description, Input Parameter Name, Input Parameter Values, Output Parameter Name, and Output Parameter Value details are displayed based on the selected External Service.
4. You can add or remove the Input Parameter values using the Add and Remove icons.

- To add the Input Parameters, click **Add** in the Input Parameter section, and click on the Input Parameter Name and Input Parameter Values column to enter the name and value details.
- To remove the Input Parameters, select the Parameter from the list and click **Remove** .

5. You can add or remove the Output Parameter values using the Add and Remove icons.
   - To add the Output Parameters, click **Add**in the Input Parameter section, and click on the Input Parameter Name and Input Parameter Values column to enter the name and value details.
   - To remove the Output Parameters, select the Parameter from the list and click **Remove**.
6. Click **Save** ✓ to save the values.

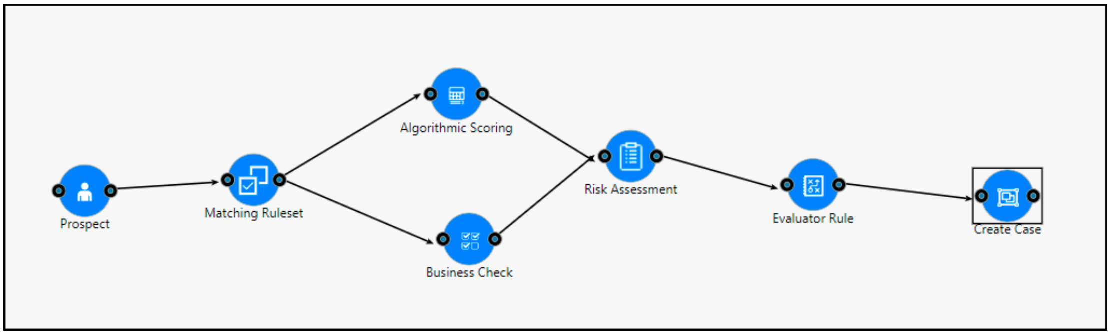
   To return to the Pipeline Designer window, click **Close** ✗to close the window. Finally, click **Save** ✓to save the updates made.

Process Flow of KYC OnboardingWidgets

KYC Onboarding widgets must be updated in a specific sequence

Widgets in KYC Onboarding pipelines must be placed in the following sequence.

Figure 10-1 Widgets in KYC Onboarding Pipelines



1. Prospect
2. Matching Ruleset
3. Algorithmic Scoring and Business Check
4. Risk Assessment
5. Evaluator Rule
6. Create Case

After you have updated the widgets, click **Save** ✓.

Note:

You cannot delete a widget from an existing KYC Onboarding pipeline. Create a new pipeline without the widget to ensure your data ingests correctly.

11 Managing KYC Batch Pipelines

Oracle Financial Crime and Compliance Management Know Your Customer Cloud Service uses KYC Batch pipelines to assess and evaluate customers.

> **Note:**
>
> KYC Batch pipelines are only available if your firm has implemented Oracle FCCM Know Your Customer Cloud Service.

> **Note:**
>
> To use the out-of-the-box batch pipelines, first copy the pipeline, and then customize as required.

Widgets in KYC Batch Pipelines

Depending on the pipeline type, specific widgets are available in the widgets pane of the pipeline.

The following table describes the widgets available in KYC Batch pipelines.

Table 11-1 KYC Batch Pipeline Widgets

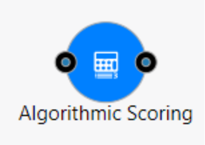
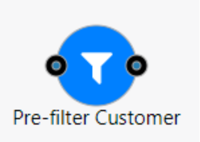
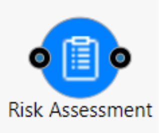
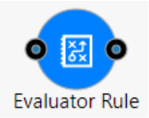
Widget	Name	Description
	Algorithmic Scoring	Use this widget to understand the type of customer being assessed and the risk category score associated with the customer.
	Pre-Filter Customer	Use this widget to filter the customers by defining various pre-filter configurations such as Attributes, Operator, and Value.
	Business Check	Use this widget to score for a business check rule associated with the customer.
	Risk Assessment	Use this widget to set the threshold scores for a customer and related jurisdiction.

Table 11-1 (Cont.) KYC Batch Pipeline Widgets

Widget	Name	Description
	Evaluator Rule	Use this widget to determine the final risk score for each prospect type based on the KYC risk score and business check risk score values.

Using the Algorithmic Scoring Widget

The Algorithmic Scoring widget enables you to see the type of prospect or customer which is being assessed and the risk category score associated with the prospect or customer.

The jurisdiction must be mapped to the pipeline. Based on the mapped jurisdiction, the pipeline is displayed in the scoring table of the Algorithmic Scoring window.

> **Note:**
>
> The pipeline can be used ONLY if you provide the Account opening jurisdiction value in the onboarding JSON.

To create a scoring rule, follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the Scoring Rule widget and click **Edit** ✎ . The KYC Scoring window is displayed.
3. Select a customer type. Click **Add**⊞ to add a new risk category. A new row is displayed.
4. Provide the following details as described in the following table:

Table 11-2 Scoring Rule Widgets

Field	Description
Risk Category Name *	Enter a risk category name.
Weightage*	Enter the weightage you want the new risk category to have. The total of all risk category weightages must equal 100.

Table 11-2 (Cont.) Scoring Rule Widgets

Field	Description
Risk Elements	Click **Add** ➕ to add a risk element to the risk category. **Note:** Do not add a Risk Element that is Deactivated in the Risk Element Configuration window. For more information, See Configure KYC Administration Data.
Attributes Risk Scores*	To add a risk score for all attributes of the rule, follow these steps: a. Click **Lookup** ⚖ . The Lookup Scores View Screen window is displayed. b. Enter the risk score in the **Default Score Value** field. c. Click **Populate** ➔. The risk scores are added for all the attributes.
Weightage*	Enter the weightage you want the new risk element to have. The total of all risk element weightages must equal 100.
Default Risk Score*	Enter the default risk score for the risk element. If you do not add a default score, it is added by the system.

5. Click **Save** ✓ to save the changes.

> **Note:**
>
> **ATTENTION:**You must add risk scores for the attributes of all risk elements in order to save the risk score.

After you add a rule, you can edit the risk elements.

- Click **Edit** ✎ in line with the risk category you want to edit. Edit icons are displayed against each risk element.
- Click **Edit** ✎ in line with the weightage and default risk score of the risk element you want to edit and click**Save** ✓

- Click **Delete** to delete the risk category or an individual risk element.
- When you have finished looking through the fields and want to go back to the Pipeline Designer window, click **Close** to close the window. Finally, click **Save** to save the updates made.

Using the Pre-Filter CustomerWidget

The Pre-filter Customer widget filters the pool of customers list based on the customer type and configured criteria such as Jurisdiction, Age of Customer, business risk and geographical risks.

To configure the Pre-Filter Customer Configuration, follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the Pre-Filter Customer widget and click **Edit** . The Pre-Filter Customer window displays.
3. Select a batch type. Select a customer type (s) and then select selected customer type.
4. Click **Add** to add a new pre-filter attributes. A new row is displayed.
5. Provide the following details as described in the following table:

Table 11-3 Pre-Filter Customer Attributes

Field	Description
Attribute Name	Select the attribute name as Jurisdiction or Age of Customer.
Operator	Select the operator from the drop-down menu. The options which display will be populated based on the selected attribute name.
Values	• If the attribute selected as Jurisdiction, then select one or more values from the drop-down menu. • If the attribute selected as Age of Customer, then enter the amount of time the customer has been a customer of the Financial Institution.

6. Click **Save** to save the changes.

   After you add a Customer Pre-filter Configuration, you can edit the pre-filter configurations.

   - Click **Edit** in line with the configuration you want to edit and update the new configuration. Click**Save** to save the updates made.

- Click **Delete** 🗑 to delete the score.
- To return to the Pipeline Designer window, click **Close** ✖to close the window. Finally, click **Save** ✓to save the updates made.

Daily Batches Configurations

KYC Daily Batches have specific configurations available.

KYC Daily Batches have specific configurations available. The following configurations are only available for the Daily batches:

- By default, Periodic Review is enabled. You cannot disable it.
- By default, New Account Review is enabled. You can disable it, if required.
- By default, Accelerated Re-Review is enabled. You can disable Accelerated Re-Review, if required. This also disables all the sub-level configurations. If required, you can disable any of the following individually.
  - Change Log (enabled by default)
  - Case Investigation (disabled by default)
  - Regulatory Report Filing (disabled by default)

> **Note:**
>
> The case count is considered between the current batch and the last batch run.

1. Click **Add**⊞ to add a new Case Investigation configuration.
2. Provide the details as described in the following table.

Table 11-4 ARR Rule Definition Attributes

Field	Description
ARR Rule Name	Enter name for the ARR rule. For example, Suspicious AML Case.
Case Type	Select a case type from the drop-down. For example, AML case
Primary Entity	Select the primary entity for the selected case type. For example, Customer.
Count (>=)	Enter the count ranging between 1 and 1000.
Status	Select the appropriate status for the selected case type. You can select multiple status for the same case type.
Action Reason	Select an action reason for the selected case type. You can select multiple reasons for the same case. This field is optional.

3. Click **Save** ✓ to save the changes.

Click **Copy** to copy all the configurations from one customer type to another customer type.

Regulatory Report Filing Configurations

Regulatory Report filings have specific configurations available.

Regulatory Report filings have specific configurations available.

> **Note:**
>
> The report count is considered between the current batch and the last batch run.

1. Click **Add** to add a new Regulatory Report Filing configuration.
2. Provide the details as described in the following table.

Table 11-5 Regulatory Report Filing Attributes

Field	Description
ARR Rule Name	Enter name for the ARR rule. For example, Unusual SAR Filing.
Regulatory Report	Select the appropriate regulatory report for the respective Jurisdiction. For example, CTR/SAR/STR.
Entity Focus	Select the appropriate entity focus. For example, Customer.
Count (>=)	Enter the count ranging between 1 and 1000.

3. Click **Save** to save the changes.

Using the Business Check Widget

The Business Check widget shows the score for a business check rule associated with the prospect or customer.

Each business check value has a risk score associated with it. To create a business check, follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover on the Business Check widget and click **Edit** . The Business Check window is displayed.
3. Select a prospect or customer type.
4. Click **Add** to add a new business check. A new row is displayed.

5. Provide details as described in the following table:

Table 11-6 Business Check Widget Fields

Field	Description
Rule Name	Select the rule name. **Note:** Do not add a Rule Element that is Deactivated in the Risk Element Configuration window. For more information, See Configure KYC Administration Data.
Value	To add a risk score for all attributes of the rule, follow these steps: a. Click **Lookup** . The Lookup Scores View Screen window is displayed. b. Enter the risk score in the **Populate Default Score Value** field. c. Click **Populate**. The risk scores are added for all the attributes.
Default Risk Score	Enter the default risk score. If you do not add a default score, it is added by the system.

6. Click **Save** to save the values. You can also click **Reset** to reset the values in the fields.

> **Note:**
>
> **ATTENTION:**You must add risk scores for the attributes of all risk elements in order to save the risk score.

After you add a rule, you can edit the risk elements.

- Click **Edit** in line with the risk category you want to edit. Edit icons are displayed against each risk element.
- Click **Edit** in line with the weightage and default risk score of the risk element you want to edit and click**Save**
- Click **Delete** to delete the risk category or an individual risk element.

- When you have finished looking through the fields and want to go back to the Pipeline Designer window, click **Close** ✖ to close the window. Finally, click **Save** ✓ to save the updates made.

Using the Risk Assessment Widget

The Risk Assessment widget enables you to set the threshold scores for a prospect and related jurisdiction using the Risk Assessment Category window.

The Risk Assessment Score is the maximum score of the KYC risk score and Business Check score.

> **Note:**
>
> You must save your changes after adding the scores.

For each jurisdiction, when you provide the range of scores for a risk category, they must cover all numbers from 0 to 100. Also, the minimum score of the next risk category must be one number more than the maximum score of the previous risk category. For example:

- The minimum score for the first risk category is 0, and the maximum score for the same risk category is 40.
- The minimum score for the next risk category is 41, and the maximum score for the same risk category is 80.
- The minimum score for the next risk category is 81, and the maximum score for the same risk category is 100.

To create a scoring rule, follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the Risk Assessment widget and click **Edit** ✎. The Risk Assessment Category window is displayed.
3. Select a prospect type.
4. Click **Add** ➕ to add a new risk assessment category.
5. Provide details as described in the following table:

Table 11-7 Risk Assessment Widget Fields

Field	Description
Category Name*	Select the category name.

Table 11-7 (Cont.) Risk Assessment Widget Fields

Field	Description
Risk Assessment Score >= *	Enter the minimum risk assessment score. After you add a score, you can edit the value by clicking **Edit** ✎ in line with the score you want to edit, updating the new score, and clicking **Save** ✓. Click **Delete** 🗑 to delete the score.
Risk Assessment Score <=*	Enter the maximum risk assessment score. After you add a score, you can edit the value by clicking **Edit** ✎ in line with the score you want to edit, updating the new score, and clicking **Save** ✓. Click **Delete** 🗑 to delete the score.

To return to the Pipeline Designer window, click **Close** ✖ to close the window. Finally, click **Save** ✓ to save the updates made.

Using the Evaluator Rule Widget

The Evaluator Rule widget enables you to set the threshold scores for the case creation for a customer type.

Additionally, it allows an optional configuration to mark case creation whenever there is a change in the current vs last risk category for the customer. To create an evaluator rule, follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the Evaluator Rule widget and click **Edit** ✎ . The Evaluator window displays.
3. Select a customer type. The criteria for case creation displays.
4. Click Edit to update the score.
   - Update the threshold risk score for case creation in the **Risk Assessment Score >=** field. If the Risk assessment score of the customer is equal or above the score in this field then the customer is marked for case creation.
   - Update the **Create Case (if change in current vs last risk category**) field accordingly with the available options on when to mark for the case creation. **Not Applicable** is the default option chosen.
5. Click **Save** ✓ to save the values.

To return to the Pipeline Designer window, click **Close** ✖ to close the window.

Finally, click **Save** ✔ to save the updates made.

12
Managing KYC Risk Factor Pipelines

Oracle Financial Crime and Compliance Management Know Your Customer Cloud Service uses KYC Risk Factor pipelines to assess and evaluate customers based on their transactions.

> **Note:**
>
> KYC Batch pipelines are only available if your firm has implemented Oracle FCCM Know Your Customer Cloud Service.

Widgets in KYC Risk Factor Pipelines

Depending on the pipeline type, specific widgets are available in the widgets pane of the pipeline.

The following table describes the widgets available in KYC Risk Factor pipelines.

> **Note:**
>
> The widgets used in this pipeline are the same widgets used for Scenario pipelines. For more information on specific widgets, refer to Widgets in Scenario Pipelines.

Table 12-1 KYC Risk Factor Pipelines Widgets and Descriptions

Name	Description	
	High Level Dataset (HLD)	Use this widget to add a High Level Dataset. Essentially, this is the data that is used to detect unusual or suspicious behavior.
	Risk Indicator	Use this widget to add a Risk Indicator. Risk indicators help determine the overall risk of transactions and parties and aid users working with events.
	Create Event	Use this widget to create an Event. An event is a record of one or more pattern matches in a detection run, which is a signal for further investigation.

Using High Level Dataset

You must add a high level dataset to begin a scenario pipeline.

To add a high level dataset and begin a scenario pipeline, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Click Widgets ☰ on the upper left corner. The list of pre-configured HLDs is displayed. FCCM TM Cloud Service comes with the following pre-configured High Level Datasets (HLD).
   - External Entity Transaction
   - Transaction by Customer
   - Transaction by Account
3. Drag and drop the required HLD to the designer pane.
4. Hover on the HLD widget and click **Edit** ✎. A dialog box is displayed.
5. Specify the required details.
6. Click **Save** ✓ to save the changes. The HLD is saved.

   You can perform certain tasks that are common in all the widgets, such as edit, delete, filter, and so on. For more information, see Common Tasks.

   Add Additional High Level Datasets
   You can add multiple conditions within the dataset to be considered by the scenario when detecting behaviors of interest. This can help improve the accuracy of your detection results and reduce false positives. For more information, see Adding Additional Threshold Conditions.

Using High Level Dataset in KYC Risk Factor Pipelines

For KYC Risk Factor pipelines, use only the Transaction by Customer High level dataset.

Refer to Using High Level Dataset (HLD) to understand how to use the High Level Dataset in a pipeline. For KYC Risk Factor pipelines, use only the Transaction by Customer High level dataset.

The Transaction Type filter is mandatory to include in the Transaction by Customer widget for KYC Risk Factor pipelines. You can add additional filters as required.

For more information about how to configure a specific risk factor, refer to Managing Risk Indicator

Attaching Risk Indicator

You must attach the required risk indicator for it to take effect.

To attach a risk indicator, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Drag and drop the Risk Indicator widget from the widgets pane to the designer pane.
3. Hover on the Risk Indicator widget and click **Edit** ✎. A dialog box is displayed.

4. Click **Move All** » on the left-hand side. The Risk Indicators Available pane is displayed with a list of available risk indicators.

5. Click **Move** > corresponding to the risk indicator that you want to attach. The selected risk indicator is moved to the Risk Indicators Used pane.

6. Click **Save** ✓ to save the changes. The Risk Indicator is attached

Creating Events

An event is a record of one or more pattern matches in a detection run, which is a signal for further investigation.

In Scenario Pipelines, the Create Event widget is the final part of the pipeline and is used to produce an event. An event is a record of one or more pattern matches in a detection run, which is a signal for further investigation. An event is also a unit of work in which a focus appears to have exhibited behavior of interest, along with the supporting information. A focus represents a business entity around which activity is reviewed and aggregated. For example customer, account or external entity. Events can be generated from a pattern matching specific source events, a sequence of events, trends, conditions, or context.
To create an event, follow these steps:

1. Navigate to the Pipeline Designer page.
2. Drag and drop the **Create Event** widget from the widgets pane to the designer pane.
3. Hover on the Create Event widget and click **Edit** ✎. A dialog box is displayed.
4. Verify the details and click Save ✓ to save the changes.

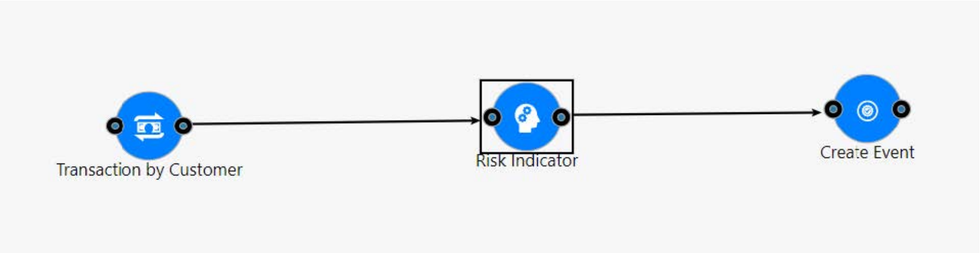
   The Create Event widget is created.

Process Flow of KYC Risk Factor Widget

KYC Risk Factor widgets must be updated in a specific sequence.

All widgets are mandatory in KYC Risk Factor pipelines.

Figure 12-1 KYC Risk Factor Pipeline Widgets



1. High Level Dataset,

2. Risk Indicator
3. Create Event

After you have updated the widgets, click **Save** ✓.

> **Note:**
>
> You cannot delete a widget from an existing KYC Risk Factor pipeline. Instead copy a pipeline and edit it or create a new pipeline as in the above sequence for this pipeline type.

> **Note:**
>
> When first opening the Create Event widget, it will be blank for this pipeline type but it is mandatory.

Using Risk Factor Pipelines

Risk factor pipelines work to risk assess a customer based on their transaction history.

To implement Transaction-based KYC Assessments on customers, follow these steps:

1. Configure the Risk Factor pipeline.
2. Configure the Threshold and Job. Refer to Managing Threshold Sets and Using Jobs for more information.
3. Attach the new task with the created pipeline job along with the calendar task to the batch as shown in the following sequence.
    a. LoadKYCCustomerInterestedParties
    b. Calendar
    c. KYCScenarioBasedRiskFactors
    d. KYCProcessingAccountData
4. Configure the risk indicator ranges for behavioral risk in the Behavioral Risk Indicator menu. Refer to the Behavioral Risk Indicator section in Configuring Dimension Data.
5. Configure the Risk Elements for the risk indicator by adding the applicable customer type, KYC check and Mapping lookup. Refer to the Risk Element Conguration section inConfiguring Dimension Data.
6. Add the rules in Business Check and Algorithmic Scoring as necessary.

    After running the batches, the customers are scored using the configuration in the above widget.

Performing KYC Assessments Without Transaction-based Scenarios

You can opt out of risk assessing customers based on their transaction history.

To conduct KYC assessments without transaction based scenarios, follow these steps.

1. Do not add any rules related to KYC Risk Factors in Algorithmic Scoring and Business Check Scoring Widgets.
2. Remove the tasks Calendar, KYCScenarioBasedRiskFactor tasks from the KYCDeploymentInitiation and KYCDaily batches.

13 Configuring Customer Watchlists

Transaction Monitoring can be configured to assess the watchlist scores of customers from either Private Watchlists, fed through staging data, or External Watchlists provided through integration with Oracle's Customer Screening Cloud Services.

> **Note:**
>
> Only one configuration method can be used in your implementation. Both methods cannot be deployed together.

Configuring Watchlist Score Integration

You can configure which type of watchlist score your implementation will use.

To configure the type of watchlist score integration your implementation will use, follow these steps:

> **Note:**
>
> Only one configuration method can be used in your implementation. Both methods cannot be deployed together.

1. Navigate to the Applications landing page.
2. Click the **Navigation Menu** ☰ to access the Navigation List. The Navigation List displays the list of modules.
3. Click **Transaction Monitoring Administration**. The Administration page is displayed..>
4. Choose the type of watchlist to integrate:
   - Select **Private Watchlist** if a private watchlist is maintained by Financial Institution and fed into Transaction Monitoring staging watchlist tables.
   - Select **External Watchlist** if Financial Institutions use Oracle FCCM Customer Screening Cloud Services to screen customers against external watchlist such as Dow Jones, World-Check.
5. Click **Save**. A confirmation message displays.

   For more information about Customer Screening Pipelines, see Managing Watch List Pipelines.

14 Managing Watch List Pipelines

Watch List pipelines are used to download and ingest free and subscription-based watch lists for screening entities, and third-party data sources for inclusion in the graph for Investigation Hub.

Depending on your implementation, pre-configured watch list pipelines are provided.

Pre-configured Watch List Pipelines

Pre-configured watch list pipelines are provided depending on your implementation.

Pre-configured Watch List Pipelines for Customer Screening

The following watch list pipelines are available if your firm has implemented Oracle FCCM Customer Screening Cloud Service:

- OFAC Watchlist Load
- Private Watchlist Load
- WC Premium Plus Watchlist Load
- WC Premium Watchlist Load
- WC Standard Watchlist Load
- DJW Watchlist Load
- EU Watchlist Load
- UN Watchlist Load
- HMT Watchlist Load

Import the ready-to-use pipelines to the application. To configure pipelines, you must create a copy of an imported pipeline and save it as a new pipeline.

> **Note:**
>
> In order to ensure that you always have the latest metadata available, rerun the watch list batches, such as OFAC or private watchlist, after applying the hotfix pipeline and get the latest metadata loaded in your search engine. For information on how to apply the hotfix pipeline and update your data, contact Oracle Support.

Watch List Pipelines for Transaction Filtering

The following watch list pipelines are available if your firm has implemented Oracle FCCM Transaction Filtering Cloud Service:

- StopKeyword Watchlist
- City Data Load

- Country Data Load
- Goods Data Load
- Port Data Load
- Load Identifier

Import the ready-to-use pipelines to the application. To configure pipelines, you must create a copy of an imported pipeline and save it as a new pipeline.

> **Note:**
>
> In order to ensure that you always have the latest metadata available, rerun the watch list batches, such as OFAC or private watchlist, after applying the hotfix pipeline and get the latest metadata loaded in your search engine. For information on how to apply the hotfix pipeline and update your data, contact Oracle Support.

Watch List Pipelines for Investigation Hub

The Investigation Hub application comes with the following pipeline which allows for the inclusion of ICIJ data in the global graph:

- IcijDataIngestion

Widgets in Watch List Pipelines

Depending on the pipeline type, specific widgets are available in the widgets pane of the pipeline.

The following table describes the widgets available in Watch List pipelines.

Table 14-1 Watch List Pipelines Widgets and Descriptions

Widget	Name	Description
⬇	Watch List Management	Use this widget to add a watch list and provide credentials for that watch list.
⚙	Watch List Data Movement	This widget is not in use at this time.
📋	Watchlist Categorization	Use this widget to categorize the World Check and Dow Jones watch list records which must be matched to Sanctions (SAN), Enhanced Due Diligence (EDD) and Political Exposed persons (PEP) records.
▼	Filter Watch List Data	Use this widget to select, filter, and include or exclude watch list records from screening.
⧉	External Service	Use this widget to add an external service. External Services perform actions on the data, such as loading or moving the data.

Watch List Management Widget

The Watch List Management widget enables you to set the URLs for downloading watchlist data in .CSV format and to enter a username and password, if applicable.

To set your watchlist management credentials follow these steps:

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover on the Watch List Management widget ⬇ and click Edit . The Watchlist Details window appears.
3. In the List Provider drop-down list, select the watchlist and associated sub-list (if applicable) you want to use.

Table 14-2 Watch List Management Widget Details

Field	Description
File	Enter the file name of the watch list file.
Description	Enter the description for the watch list.
URL	Enter the URL where the watch list is stored. **Note:** The URL must be in .zip or a tar.gz file format.
Username	Enter your user name which can be used to access and download the watch list.
Password	Enter the password which can be used to access and download the watch list.

4. Click **Save** ✓ to save the changes.

   To return to the Pipeline Designer window, click **Close** ✖ to close the window. Finally, click **Save** ✓ to save the updates made.

Watch List Data Movement Widget

The Watchlist Data Movement widget displays how the data is mapped from the Source Datasets into the Target tables on a column level.

⚙ This information helps administrators bring transparency to the data that is being screened.

> **Note:**
>
> This widget is not in use at this time.

Watch List Categorization Widget

Use the Watch list Categorization widget to categorize the watch list records which must be matched to Sanctions (SAN), Enhanced Due Diligence (EDD) and Political Exposed persons (PEP) records.

You can use the Watchlist Categorization widget on the World-Check and Dow Jones watch lists.

- The World-Check watch list is a collection of data on Politically Exposed Persons (PEPs) and heightened risk individuals and organizations from around the world to help identify and manage financial, regulatory and reputational risk.
- The Dow Jones watch list is also a collection of data on senior PEPs, their relatives and close associates as well as national and international sanctions lists, and profiles of persons linked to high profile crime.

The World Check Categorization and Dow Jones Categorization windows display two toggle buttons: one to enable or disable the PEP/ State-Owned Entities (SoE)/ Instrumentalities of State (IOS) records and another to enable or disable the SAN and EDD records. If you enable both the toggle buttons, then all PEP/SoE/IOS and SAN/EDD records are included during the screening process. If you disable both the toggle buttons, then no SAN/EDD or PEP/SoE records are included during the screening process.

> **Note:**
>
> Both toggle buttons are enabled by default.

Enable the Include SAN/EDD Records for Screening toggle button to view all records and associated watch lists. To move all records to the SAN category, enable the toggle button in line with the watch list name.

Filter Watch List Data Widget

Use the Filter Watch List widget to select, filter, and include or exclude watch list records from screening.

Use the Filter Watchlist widget to do the following:

- Select SAN and EDD watch list records in the Watch List Categorization window.
- Include or exclude countries or watch lists for further filtering, if you have included them under SAN and EDD.
- Select the PEP types for screening if you have included PEP and SoE records.

- Filter the watch list records by customer type, name type and status.

> **Note:**
>
> SAN records are given priority over PEP records and PEP records are given priority over EDD records. For example, if a specific record is categorized as SAN and PEP, they are screened against SAN matching rules and not PEP matching rules.

If the **Include PEP/SoE for Screening toggle button** is disabled in the Watch List Categorization window, the PEP tab and related records are not displayed.

You must select **Yes** to view the filter fields. If you select **No**, all records selected in the Watch List Categorization window are not considered for screening. Select **Include** to screen specific records or select **Exclude** to avoid screening specific records during the screening process.

NorwayOFACNorwayCountry TypeOFACList Type

> **Note:**
>
> - All check boxes are selected by default.
> - Typically, all SAN watch lists records are pushed for screening in order to eliminate the possibility of high-risk individuals going undetected. Select **Yes** only if you want to reduce the time taken for screening and the number of alerts that must be investigated.

Using the External Service Widget

The External Service is used if a case must be created for the particular risk assessment.

External Service refers to an existing set of services that the customer can use to derive the risk of certain business entities, configure data movement for case management, create events, and so on. The External Service widget is used if a case must be created for the particular risk assessment.

1. In the Pipeline Designer page, select the pipeline you want to edit. The Pipeline Designer window appears.
2. Hover over the External Service widget and click Edit . The External Service window is displayed.
3. Select the external service name. The Description, Input Parameter Name, Input Parameter Values, Output Parameter Name, and Output Parameter Value details are displayed based on the selected External Service.
4. You can add or remove the Input Parameter values using the Add and Remove icons.
   - To add the Input Parameters, click **Add** in the Input Parameter section, and click on the Input Parameter Name and Input Parameter Values column to enter the name and value details.
   - To remove the Input Parameters, select the Parameter from the list and click **Remove** .

5. You can add or remove the Output Parameter values using the Add and Remove icons.
   - To add the Output Parameters, click **Add**in the Input Parameter section, and click on the Input Parameter Name and Input Parameter Values column to enter the name and value details.
   - To remove the Output Parameters, select the Parameter from the list and click **Remove**.
6. Click **Save** ✓ to save the values.

   To return to the Pipeline Designer window, click **Close** ✖to close the window.

   Finally, click **Save** ✓to save the updates made.

15

Managing Threshold Sets

FCCM TM Cloud Service uses tunable Thresholds to change variable values for scenarios.

When scenarios are created or installed, thresholds are established. Once the application is in the production environment, you can use the Threshold Editor to modify threshold values of user-created scenarios, and create and edit threshold sets to fine-tune how that scenario finds matches, without changing the values defined at the dataset or pattern level. These thresholds are applied to scenarios to find matches. Using this tool, you can enter a new value for a threshold (within a defined range) or reset the thresholds to their sample values.

Threshold sets allow you to run the same scenario multiple times against a variety of sources (for example, currencies, or jurisdictions) with separate threshold values for each source.

> **Note:**
>
> - Changing threshold values can generate significantly more or fewer alerts, depending upon the modifications made.
> - Pre-configured threshold sets cannot be edited or deleted. You can only edit or delete user-defined threshold sets or copies of pre-configured threshold sets.

Accessing Threshold Sets

You can access the threshold sets through the Threshold Manager.

To access the All Threshold Sets page and view threshold sets, follow these steps:

1. In the Navigation List menu, select **Pipeline Administration**.
2. Select **Threshold Manager**. The All Threshold Sets page displays the complete list of threshold sets available in your implementation.
3. Select the check box for the threshold set you want to view, or click the threshold set name to view the threshold set details.

Copying a Threshold Set

Copy an existing threshold set before modifying the values.

To copy and modify an existing threshold set, follow these steps:

1. Navigate to the Threshold Manager page.
2. Select the check box for the threshold set you want to copy.
3. Click **Copy** . The Copy Threshold Set window displays.
4. Enter the following values:

a. Enter a **Name** for this threshold set.

b. The scenario associated with this threshold set displays additional configurable parameters. These parameters are specific to the selected scenario.

c. Select one or more **Jurisdictions** for this threshold set using the drop-down list. Jurisdiction refers to the division of data in the database based on criteria such as geographical boundaries, legal entities, and so on.

d. Enter the **Lookback Period** for this threshold set. Lookback period refers to the number of seconds, minutes, hours, or days to lookback from the current date or time to create a time window which is used to consider cases for correlation.

e. Enter the **Frequency Period** for this threshold set. Frequency period refers to how frequently the scenario should be run.

f. Enter any **Comments** you have for this threshold set.

g. Enter the threshold values you want this threshold set to be updated with in the **New Value** field.

5. Click **Save** ✓ to save the values.

Creating a Threshold Set

You can create new threshold sets in the Threshold Editor.

To create a new threshold set, follow these steps:

1. Navigate to the **Threshold Editor** page.
2. Click **Add** ⊞in the top right corner. The New Threshold Set page is displayed.
3. Enter the following values:

   a. Enter a **Name** for this threshold set.

   b. The scenario associated with this threshold set displays additional configurable parameters. These parameters are specific to the selected scenario.

   c. Select one or more **Jurisdictions** for this threshold set using the drop-down list. Jurisdiction refers to the division of data in the database based on criteria such as geographical boundaries, legal entities, and so on.

   d. Enter the **Lookback Period** for this threshold set. Lookback period refers to the number of seconds, minutes, hours, or days to lookback from the current date or time to create a time window which is used to consider cases for correlation.

   e. Enter the **Frequency Period** for this threshold set. Frequency period refers to how frequently the scenario should be run.

   f. Enter any **Comments** you have for this threshold set.

   g. Enter the threshold values you want this threshold set to be updated with in the **New Value** field.

4.

- Click **Save** ✓ to save the values. A new threshold set is created and a message displays: *New Threshold Set created successfully*.
- Click **Save & Simulate**. A new threshold set is created, and the Create Simulator Conditions page displays. For more information about the Threshold Simulator, see Threshold Simulator.

Editing Threshold Sets

You can modify user-defined threshold sets in the Threshold Editor.

To edit a threshold set, follow these steps:

> **Note:**
>
> Pre-configured threshold sets cannot be edited or deleted. You can only edit or delete user-defined threshold sets.

1. Navigate to the Threshold Editor page. The existing threshold sets are displayed.
2. Select the check box corresponding to the threshold set you want to edit.
3. Click **Edit** ✎. The Edit Threshold page is displayed.

   Alternatively, you can click **Edit** when viewing a threshold set in the View Threshold Set window.
4. Modify the required details.
   a. Select one or more **Jurisdictions** for this threshold set using the drop-down list. Jurisdiction refers to the division of data in the database based on criteria such as geographical boundaries, legal entities, and so on.
   b. Enter the **Lookback Period** for this threshold set. Lookback period refers to the number of seconds, minutes, hours, or days to lookback from the current date or time to create a time window which is used to consider cases for correlation.
   c. Enter the **Frequency Period** for this threshold set. Frequency period refers to how frequently the scenario should be run.
   d. Enter any **Comments** you have for this threshold set.
   e. Enter the threshold values you want this threshold set to be updated with in the **New Value** field.

   > **Note:**
   >
   > You can modify the values of the existing parameters only, you cannot add new parameters.
5.
   - Click **Save** ✓ to save the values. A new threshold set is created and a message displays: *New Threshold Set created successfully*.

- Click **Save as New** to save the edited threshold set as a new threshold set. The New Threshold window opens. Enter a name for the threshold set and click **Save**. A new threshold set is created and a message displays: *New Threshold Set created successfully*.
- Click **Save & Simulate**. A new threshold set is created, and the Create Simulator Conditions page displays. For more information about the Threshold Simulator, see Threshold Simulator.

Adding Additional Threshold Conditions

In order to improve the accuracy of your detection results and reduce false positives, you can add additional threshold conditions to detect only those behaviors which meet a combination of specific criteria.

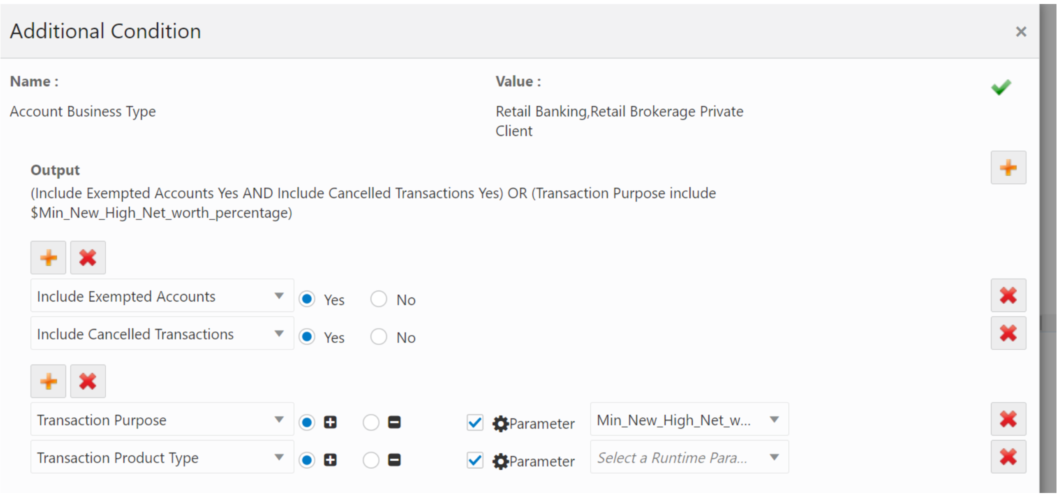
To add additional threshold conditions to a high level dataset, follow these steps:

1. Navigate to the scenario you want to further define in the Pipeline Designer by selecting **Pipeline Administration**, then **Pipeline Designer**, and selecting the scenario pipeline. The Pipeline Designer displays for the scenario.
2. Select **Edit** in the High Level Dataset widget. The Threshold Editor displays for this dataset.
3. Select **Add Additional High Level Dataset** for the threshold that you wish to define further, for example, Account Business Type. The Additional Condition window opens for this threshold.
4. Click **Add**. Under Output, click **Add** again.
5. Select an item from the drop-down list to include in the threshold conditions for this scenario. Modify the details as desired. The Output section displays the new condition.

   To add additional threshold conditions, if desired, click **Add** and select another item from the drop-down list.

   Clicking **Add** under output from the same condition joins these conditions as an AND condition. Clicking **Add** from the right hand side of the Additional Condition window joins the conditions as an OR condition. The following image provides an example:

Figure 15-1   Sample High Level Dataset Output



Additional Condition

Name : Account Business Type

Value : Retail Banking,Retail Brokerage Private Client

Output
(Include Exempted Accounts Yes AND Include Cancelled Transactions Yes) OR (Transaction Purpose include $Min_New_High_Net_worth_percentage)

Include Exempted Accounts ● Yes ○ No

Include Cancelled Transactions ● Yes ○ No

Transaction Purpose ● ⊞ ○ ⊟ ☑ Parameter Min_New_High_Net_w...

Transaction Product Type ● ⊞ ○ ⊟ ☑ Parameter *Select a Runtime Para...*

You can continue to add and select threshold conditions until you are satisfied with the granularity of the threshold conditions.

6. When you have finished adding all the threshold conditions, click **Save**.

Deleting Threshold Sets

You can delete user-defined threshold sets in the Threshold Editor.

To delete a threshold set, follow these steps:

> **Note:**
>
> Pre-configured threshold sets cannot be edited or deleted. You can only edit or delete user-defined threshold sets.

1. Navigate to the Threshold Editor page. The existing threshold sets are displayed.
2. Select the check box corresponding to the threshold set you want to delete.
3. Click **Delete** . A message displays: *Are you sure you want to delete <threshold set>?*
4. Enter the reason for deletion in the **Your Comment** box. This is mandatory.
5. Click **Delete**. The threshold set is deleted.

About Threshold Simulator

The Threshold Simulator is used to run selected scenario pipelines against the selected threshold sets to find the matches obtained from these combinations.

These matches enable you to identify the events generated for the combination on a specified date. This can be helpful when you want to see which events would be generated with different threshold settings and be able to explain why your scenario is configured as it is, such as during audits.

View Simulator Conditions

You can view Simulator Conditions using the Threshold Manager.

To view simulator conditions for a threshold set, follow these steps:

1. In the Navigation List menu ≡, select **Pipeline Administration**.
2. Select **Threshold Manager**. The All Threshold Sets page displays.
3. In the All Thresholds page, select the check box corresponding to the threshold set you want to view simulation details for.
4. Click **Simulation History** ⟲. The Simulation Details for this threshold set opens as a new tab.
5. Click the **Simulation Run ID** for the simulation you want to view conditions for. The View Threshold Set pop-up window displays the details of this threshold set.

   If you want to make modifications to these conditions, click **Edit & Simulate** . The Edit Threshold Set pop-up window displays. Follow the steps in Edit Simulator Conditions to make these changes.

Edit Simulator Conditions

You can edit Simulator Conditions using the Threshold Manager.

To edit existing simulator conditions for a threshold set, follow these steps:

1. In the All Thresholds page, select the check box corresponding to the threshold set you want to edit.
2. Click **Simulation History** ⟲. The Simulation Details for this threshold set opens as a new tab.
3. Select the check box corresponding to the **Simulation Run ID** for the simulation you want to edit.
4. Click **Edit** ✎. The Edit Simulator Conditions pop-up window displays.

   Alternatively, you can access the Edit Simulator Conditions window by clicking **Edit & Simulate** in the View Simulator Conditions window.
5. To make modifications to these conditions, update the following values:
   a. Select one or more **Jurisdictions** for this threshold set using the drop-down list. Jurisdiction refers to the division of data in the database based on criteria such as geographical boundaries, legal entities, and so on.
   b. Enter the **Lookback Period** for this threshold set. Lookback period refers to the number of seconds, minutes, hours, or days to lookback from the current date or time to create a time window which is used to consider cases for correlation.

   c. Enter the **Frequency Period** for this threshold set. Frequency period refers to how frequently the scenario should be run.

   d. Enter the threshold values you want this threshold set to be updated with in the **New Value** field. Select the Batch Date as the date for the data you want to test the thresholds against. This can be the current date or a past date.

   e. Enter the Data Origin.

6. Click **Save & Simulate** to run the modified simulation. After running a simulation, the Simulator History window displays the result with the number of event matches and details of each event. You can view the following details:
   - Simulation ID: ID for this simulation run.
   - Data Origin: Data Origin of the data set the simulated scenario conditions are run against.
   - Jurisdiction: Jurisdiction the simulated scenario conditions are run for.
   - Batch Date: Date the simulated scenario conditions are run for.
   - Results: Number of event matches generated by the simulated scenario conditions during the run.
   - Event Details: Details for each event generated by the simulated scenario conditions during the run.
     - Event ID
     - Focus Name
     - Focus Type
     - Highlights

Viewing Simulation Details

When a threshold set simulation has completed, you can view the details of all thresholds in this simulation and their results in the Simulation Details.

This allows you to determine whether your threshold set is generating the expected detection results or if further modification is required.You can also view the Simulation Details for all runs of a threshold set which has been previously run. To open the Simulation Details, follow these steps:

1. In the All Thresholds page, select the check box corresponding to the threshold set you want to view simulation details for.
2. Click **Simulation History** ⟲. The Simulation Details for this threshold set opens as a new tab. You can view the following details:
   - Simulation Run: ID for this simulation run with the scenario name.
   - Jurisdiction: Jurisdiction the simulated scenario conditions are run for.
   - Run Date and Time: Date and time the simulation was run.
   - User ID: User who ran the simulation.

   You can export the results of the threshold set simulation runs in .xlsx format by selecting the check boxes for one or more simulation runs and clicking **Export Results**.

You can delete a simulation run by selecting the check boxes for one or more simulation runs and clicking **Delete**. The Delete pop-up window displays: *Are you sure you want to delete <Simulation ID>*? Enter a comment and click **Delete**. A confirmation message displays.

To return to the All Threshold Sets tab, click the **All Thresholds List** tab.

Creating New Simulator Conditions

You can create new Simulator Conditions using the Threshold Manager.

To create new simulator conditions for a threshold set, follow these steps:

1. In the **All Thresholds** page, select the check box corresponding to the threshold set you want to create new simulator conditions for.
2. Click **Simulation History** . The Simulation Details for this threshold set opens as a new tab.
3. Click **Open Simulator**. The Create Simulator Condition pop-up window displays.

   Alternatively, you can access the Create Simulator window by clicking **Open Simulator** in the All Thresholds page. The Create Simulator Condition pop-up window displays.
4. Create the simulator conditions by providing the following details:
   a. Select the required scenario from the **Select Scenario** drop-down list.
   b. Select the required threshold set from the **Select Threshold** drop-down list.
   c. Select the **Batch Date** as the date for the data you want to test the thresholds against. This can be the current date or a past date.
   d. Enter the **Data Origin**.
5. Click **Save**.

> **Note:**
>
> If the simulation run fails, you can retrigger the simulation for successful run.

Running Existing Threshold Sets

You can run a simulation for existing scenario threshold sets.

To run the threshold simulator for an existing scenario threshold set, follow these steps:

1. In the All Thresholds page, select the check box corresponding to the threshold set you want to run the simulator for.
2. Click **Open Simulator**. The Simulator Conditions pop-up window displays.

   Alternatively, you can also run existing threshold set from the Simulation Details tab by clicking Open Simulator. The Simulator Conditions pop-up window displays.
3. Provide the following details:

a. Select the **Batch Date** as the date for the data you want to test the thresholds against. This can be the current date or a past date.

b. Enter the **Data Origin**.

c.

d. Select one or more **Jurisdictions** for this threshold set using the drop-down list. Jurisdiction refers to the division of data in the database based on criteria such as geographical boundaries, legal entities, and so on.

e. Enter the **Lookback Period** for this threshold set. Lookback period refers to the number of seconds, minutes, hours, or days to lookback from the current date or time to create a time window which is used to consider cases for correlation.

f. Enter the **Frequency Period** for this threshold set. Frequency period refers to how frequently the scenario should be run.

g. Enter any comments you have for this threshold set.

h. Enter the threshold values you want for this threshold set in the **New Value** field.

4. Click **Save & Simulate** to run the modified simulation. After running a simulation, the Simulator History window displays the result with the number of event matches and details of each event. You can view the following details:

   - Simulation ID: ID for this simulation run.
   - Data Origin: Data Origin of the data set the simulated scenario conditions are run against.
   - Jurisdiction: Jurisdiction the simulated scenario conditions are run for.
   - Batch Date: Date the simulated scenario conditions are run for.
   - Results: Number of event matches generated by the simulated scenario conditions during the run.
   - Event Details: Details for each event generated by the simulated scenario conditions during the run.
     - Event ID
     - Focus Name
     - Focus Type
     - Highlights

> **Note:**
>
> If the simulation run fails, you can retrigger the simulation for successful run.

Viewing Simulation Details

When a threshold set simulation has completed, you can view the details of all thresholds in this simulation and their results in the Simulation Details.

This allows you to determine whether your threshold set is generating the expected detection results or if further modification is required.You can also view the Simulation Details for all runs of a threshold set which has been previously run. To open the Simulation Details, follow these steps:

1. In the All Thresholds page, select the check box corresponding to the threshold set you want to view simulation details for.
2. Click **Simulation History**. The Simulation Details for this threshold set opens as a new tab. You can view the following details:
   - Simulation Run: ID for this simulation run with the scenario name.
   - Jurisdiction: Jurisdiction the simulated scenario conditions are run for.
   - Run Date and Time: Date and time the simulation was run.
   - User ID: User who ran the simulation.

   You can export the results of the threshold set simulation runs in .xlsx format by selecting the check boxes for one or more simulation runs and clicking **Export Results**.
   You can delete a simulation run by selecting the check boxes for one or more simulation runs and clicking **Delete**. The Delete pop-up window displays: *Are you sure you want to delete <Simulation ID>*? Enter a comment and click **Delete**. A confirmation message displays.

   To return to the All Threshold Sets tab, click the **All Thresholds List** tab.

16
Extending the Data Model

Oracle provides an extensive data model which is used to populate the fields in the user interface for the application.

If an Oracle client captures additional Customer, Account, or Transaction data which they would like to include in the application or needs to quickly adjust their coverage to address emerging risks and topologies, users who are mapped to the "Data Model Admin Group" can designate additional columns or attributes to capture this data in the customized data model extension tables.

> **Note:**
>
> This feature is currently available to extend Stage tables only.

Adding New Data Model Columns

You can add additional data model columns to Staging tables.

To add a new column to extend your data model, follow these steps:

1. Under Pipeline Administration, select **Data Model Extension**. The FCCM Cloud Service Data Model Extension page displays.
2. Provide the required details for your new column.
   - Select the entity type of the data you are adding from the **Select Entity** drop-down list. You can choose from the following tables:
     - **Customer** populates the STG_PARTY_MASTER_EXT table.
     - **Account** populates the STG_CASA_EXT table.
     - **Transaction** populates the STG_CASA_TXNS_EXT table.
   - The **Primary Keys** field is automatically populated with the primary keys for this field. You cannot edit this field.
   - Enter a **Logical Name** for the column you want to add, for example, Passport Number. This name must be under 50 characters.
   - Enter the **New Attribute Name**. This will be the physical name of the column. For example, V_PASSPORT_NUMBER.
   - Select the **Data Type** from the drop-down list:
     - Number
     - Varchar2
     - Date
     - Timestamp

- Enter the allowable **Data Type Length** for the column. For example, 20. This should be at least as long as the maximum expected value for the column you are adding.
- Select whether **Data Type Constraints** will apply to the column from the drop-down list. Selecting **Unique** means that values provided in this column cannot be repeated.
- Select the type of **Environment** you want to create this column for. You can select one or both options.
  - Selecting **Stage** adds this column to the data provided by Oracle customers.
  - Selecting **Business** adds this column to the data which can be configured to process the data or to populate the UI. This feature is not enabled fully at this time.

3. Click **Add** to add this column to the data model extension table, for example STG_PARTY_MASTER_EXT.
4. Enter **Comments** to explain why you are creating this column.
5. Click **Submit**. The Attribute details for all custom fields added to Stage tables, or both the Stage and Business tables, display on the right side pane. Columns added to Business tables only will not display in this section.

   When you have successfully added all columns you need, click **Download Sample CSV** to download a sample data model table containing all the customized columns along with the default columns provided by Oracle. Use this sample file to help you provide data in the proper format. For more information on Oracle's default sample .csv format, see Sample Templates files.
   More information about the default data model and how to load data into the application can be found in Using FCCM Cloud Service Data Loading.

17

Managing Data Extraction API Pipelines

Data Extraction API pipelines allow you to build queries to extract data from your FCCM cloud implementation.

Using the Query Builder, you can define views and expose the final results as REST APIs for downloading the results as JSON.

Widgets in Data Extraction API Pipelines

Depending on the pipeline type, specific widgets are available in the widgets pane of the pipeline.

The following table describes the widgets available in Data Extraction API pipelines.

Table 17-1   Data Extraction API Pipeline – Widgets and Descriptions

Widget	Name	Description
🛢	Dataset	Use this widget to add a Dataset. Datasets correspond to the contents of a single database table which can be a staging table, business table, or a table that has been created by a data pipeline. A data extraction pipeline must always begin with a Dataset widget.
⚙	API Forge	Use this widget to define the API which will be used to extract the data. The APIForge widget cannot be changed.

Creating Data Extraction API Pipelines

You can create a data extraction API pipeline using the API Forge widget to define the API which will be used to extract the data.

You must first create a new pipeline. Follow the steps in Creating Pipelines to create a new pipeline, with the Pipeline Type as **API Pipeline**.

1. Navigate to the Pipeline Designer page.
2. Open your newly created API Pipeline.
3. Drag and drop the **Dataset** 🛢 widget from the widgets pane in the upper-right corner of the designer pane. You can add multiple datasets to each pipeline.
4. Hover on the Dataset widget and click **Edit**. ✎
5. Provide the details as described in the following table.

Table 17-2   Dataset Widget Details

Field	Description
Name	Enter the name for your dataset.
Tables	Select a table from the Tables drop-down list. This list consists of all the staging tables that are available. The columns of the selected table are displayed in the Attributes pane. The attributes include the Logical Name, Column name, and Column Type.

6. Click **Save** ✓ to save the changes. The dataset is created and is visible on the canvas. It is also available for use in the Dataset pane.
7. Drag and drop the **API Forge** ⚙ widget from the widgets pane in the upper-right corner of the designer pane.
8. Hover on the API Forge widget and click **Edit**.✎
9. Provide the details as described in the following table. Click on the + icon to add rows as needed.

Table 17-3   API Forge Details

Field	Description
Name	Enter the name for this API.
URI	Enter the URI to be used in API Execution. This must be unique to this API Forge widget.
Source Dataset	The datasets that are connected to the ForgeAPI Widget display.

10. Enter the following **Input Parameters**. Click on the + icon to add rows as needed.
    - **Key**: Enter the JSON Key to be passed in the request Object. This Input Parameter displays in the Join/Filter conditions under the Expression builder and is also given as a value during the API call, as shown in the sample payload.
    - **Datatype**: Select the datatype for the Key from the following options:
      - String
      - Date
      - Number

      This Input Parameter displays in the Join/Filter conditions under the Expression builder and sets the value during the API call.
11. Provide the following **Join** information. This section only displays when more than one dataset is connected to the APIForge widget.
    - **Parent Dataset**: Select the Parent Dataset as required for the desired output.

- **Relation**: Displays the relation type between the parent and child as Has Many [For every parent entity, there can be 0..n child entities].
- **Child Dataset**: Select the Child Dataset as required for the desired output.
- **Join Conditions**: You can add multiple join conditions on the parent and child datasets. Use the drop-down lists to select:
  - **Datasets**: Select from the table names.
  - **Attributes**: Select from the column names
  - **Operator**: Select an operator to connect the Datasets and Attributes.

  Click on the + icon to add join conditions as needed.
- **Join Condition Modes**: Define the mode of the join condition between the tables. You can select:
  - **Exp**: Use this option when one dataset is Entity and the other is Expression. The Expression Builder displays.
  - **Text**: Use this option when one dataset is Entity and the other is static text
  - **Table**: Use this option when both datasets selected are tables.

12. Provide the following **Filter** information.
    - **Filter Conditions**: You can apply filters to datasets based on specific criteria. Select the dataset to apply the filter on and use the drop-down lists to select:
      - **Datasets**: Select from the table names.
      - **Attributes**: Select from the column names
      - **Operator**: Select an operator to connect the Datasets and Attributes.

      Click on the + icon to add filter conditions as needed.
    - **Filter Condition Modes**: Define the mode of the filter condition between the tables. You can select:
      - **Exp**: Use this option when one dataset is Entity and the other is Expression. The Expression Builder displays.
      - **Text**: Use this option when one dataset is Entity and the other is static text
      - **Table**Use this option when both datasets selected are tables.
13. Map and configure the Output Parameters.
    - Select the Dataset Name from the drop-down list to populate the attributes in the dataset
    - Select fields which you want to display in the output from the source datasets and click **Map** › .
    - Assign valid JSON keys for each mapped field to structure the output.
14. Check the sample payload to ensure the setup aligns with your requirements. If changes are required, you can edit the necessary settings using the steps above. After making changes, click **Regenerate Payload** to refresh the sample payload.
15. Click **Save** ✓ to save the changes.
16. In the Pipeline Designer page, click **Save** to save all updates.

Executing Data Extraction APIs

After creating the data extraction API pipeline using the API Forge widget, you can use the API to extract the data.

Before working with APIs, verify that you have the following:

- Access to FCCM Cloud service.
- Appropriate user privileges to access the services.
- Technical and functional knowledge to understand and execute the REST APIs and configuration knowledge.
- Knowledge of REST concepts, JSON, browser-based REST client.
- Knowledge of an interactive and automatic tool for verifying the APIs such as Postman.

Create one or more data extraction API pipelines using the API Forge widget

After creating a data extraction API pipeline using the API Forge widget, you can use the API to extract the data.

1. Generate the Access Token by following the steps found in Authentication.
2. Open Postman or another relevant tool.
3. Configure your authorization.
   a. Copy the Access token you generated above.
   b. Go to the **Authorization** tab and select the Type as **Bearer Token** (Access token).
   c. Replace the token with the Access token you generated above.
4. Provide the sample input payload generated by your Data Extraction API pipeline.
   a. Copy the sample input payload generated by your Data Extraction API pipeline.
   b. Go to the Request **Body** tab and paste the sample input payload.
5. Send a request using the GET method by replacing the Post URL with the Generated URI from your Data Extraction API pipeline.

   > **Note:**
   >
   > A unique URI will be generated for each APIForge widget in the pipeline.

6. Trigger the API request. You can change the parameters from the input payload at any time.

   The extracted records display in the Response Body.

Note:

By default, the number of records extracted is limited to 500. To extract more records, use the **Offset** parameter to extract records 501-1000, 10001-1500, and so on.

18 Using Jobs

The application uses jobs to define the instructions for executing the data pipelines or scenario pipelines against threshold sets, for example, running a scenario or loading data.

These jobs can be included in batches (groups of jobs) which run at configured intervals against the selected threshold to detect and generate events. This allows the jobs to run automatically, without requiring your involvement. Jobs can also be used to monitor the execution of jobs.

Creating Jobs

You can create new jobs to run in batches.

To create a new job, follow these steps:

1. Navigate to the OFS Transaction Monitoring page.
2. Click ≡ to access the Navigation List. The Navigation List displays the list of modules.
3. Click **Jobs** in the Navigation List. The Jobs page opens in a new window.
4. Click **Expand** in the upper-right corner. The Create Job pane is displayed.
5. Provide the details as described in the following table:

Table 18-1 Fields to Create Jobs

Field	Description
Job Name	Enter the name for the job.
Pipeline Type	Select the pipeline type for which you want to create the job. The available options are Data and Scenario.
Pipeline	Select the pipeline from the drop-down list for which you want to create a job.
Threshold	Applicable only when the Pipeline Type selected is Scenario. Select the threshold set from the drop-down list. The drop-down list displays the list of thresholds that are created for the selected scenario pipeline. The job is run against the selected threshold to detect and generate events.

6. Click **Save** ✓to save the changes. A new job is created and displayed in the Jobs page.

Editing Jobs

You can edit or delete user-defined jobs

To edit a job, follow these steps:

> **Note:**
>
> Pre-configured jobs cannot be edited or deleted. You can only edit or delete user-defined jobs.

1. Navigate to the **Jobs** page.
2. Click on the Job that you want to modify and click corresponding to the job that you want to modify.
3. Modify the required details in the Edit Job pane on the right-hand side.
4. Click **Save** ✓to save the changes. The job is modified.

Deleting Jobs

You can edit or delete user-defined jobs

To delete a job, follow these steps:

> **Note:**
>
> Pre-configured jobs cannot be edited or deleted. You can only edit or delete user-defined jobs.

1. Navigate to the Jobs page.
2. Click **Delete** corresponding to the job that you want to delete. The job is deleted.

Viewing Execution History

Execution History enables you to view the complete history of job execution, such as the start and end time of the job execution, status of the job execution, log messages generated during job execution, and so on. This will help you see how your jobs are progressing and detect any recurring issues.

To view the execution history, follow these steps:

1. On the Jobs page, click the job for which you want to view the execution history.
2. The Execution History pane at the bottom of the page displays the historical information of the selected job. The details include the Batch ID, the date and time during which a job is executed, status of the job execution, and so on.
3. Click **Monitor Execution** corresponding to the batch ID for which you want to view more information of a batch.

> **Note:**
>
> Some batch IDs may display more than one execution. View the Execution History for the most recent execution to see how your jobs are progressing.

4. The Execution Monitor page is displayed in a new window. The page contains the following details:
   - The pipeline for which the job is created. The widgets in the pipeline are represented in different colors. Widgets are color coded to indicate the widget type and status of the job.
   - Log messages generated during the execution of the pipeline.

   > **Note:**
   >
   > You can click the **Create Event** widget to display the Log Messages window. When working with a Scenario Pipeline, you can click the **Add Hint** option to add hints. Hints provide a mechanism to direct the optimizer to choose a certain query execution plan based on the specific criteria.

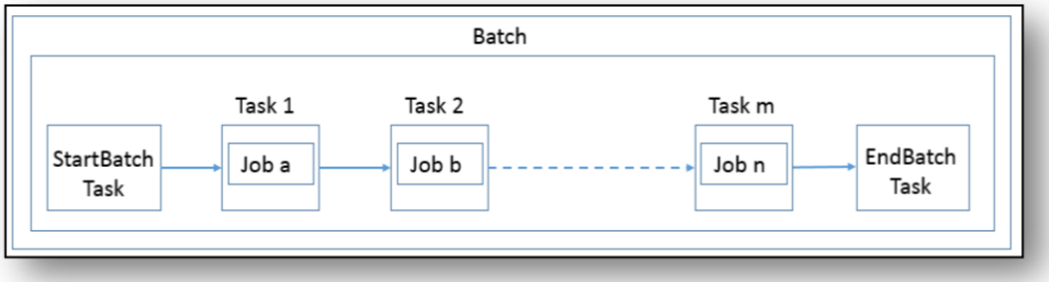
5. Click the widget marked as complete (with a check mark) to view the Log Messages dialog box with detailed information of the widget.

19 Managing Batches

A batch is a group of jobs that are scheduled to run at a defined interval of time, in sequence, automatically, without user involvement.

Oracle FCCM Cloud Service uses the Scheduler Service to create, schedule, execute and manage batches. A batch is a group of jobs that are scheduled to run at a defined interval of time, in sequence, automatically, without user involvement. Each batch begins with a StartBatch, includes any additional jobs that should be run in this batch, and then completes with the Endbatch.

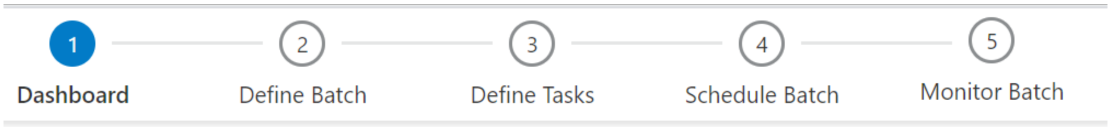
Figure 19-1   Flow of Batch



To execute the batches, use the Schedule Batch feature in the Scheduler Service. For more information, see Scheduler Service. You can use the Scheduler Service to first define the batch, then define which tasks should be included in this batch.

Next, you must schedule the batch. When the batch runs, you can monitor the batch to verify it is executing as intended. Click the Batch Scheduling Flow to navigate through the Scheduler Service.

Figure 19-2   Scheduler Service -- Batch Scheduling Flow

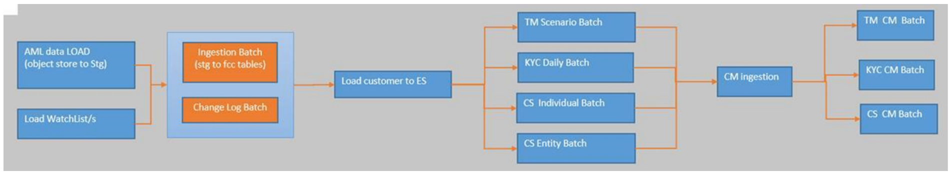


Possible Batch Flow

Possible batch flow for an Oracle client who has subscribed to Oracle FCCM Transaction Monitoring Cloud Service, Oracle FCCM Know Your Customer Cloud Service, and Oracle FCCM Customer Screening Cloud Service.

The following figure provides a possible batch flow for an Oracle client who has subscribed to Oracle FCCM Transaction Monitoring Cloud Service, Oracle FCCM Know Your Customer Cloud Service, and Oracle FCCM Customer Screening Cloud Service.

Figure 19-3 Possible MultiProduct Batch Flow



The batch order shown above should be maintained. Batches shown in parallel can be executed and purged in any order.

> **Note:**
>
> - Batch purge order should always be maintained in the reverse order of execution for batches shown in series in the batch flow diagram.
> - If an Ingestion batch is run for a given mis_date and dataorigin, CMIngestion must be run with the same mis_date and dataorigin before running a new Ingestion batch for a different date.

Pre-Configured Batches

The application contains certain pre-configured batches that can be used to run the default data. You must create new batches to run customer-specific data.

Execute the pre-configured batches in the sequence provided in each table.

Pre-configured TM Batches

Table 19-1 Pre-configured Transaction Monitoring Batches

Sequence	Batch Name	Purpose
1	AMLDataLoad	Loads client data.
2	AMLHolidayMasterDataLoad	Loads Holiday and Non-Working day data.
3	Ingestion	Loads data from staging tables to business tables.
4	TMScenario	Uses the data that is prepared during ingestion and executes the scenario pipelines to generate events.
5	CMIngestion	Loads the data to Case Management Business tables.

Table 19-1 (Cont.) Pre-configured Transaction Monitoring Batches

Sequence	Batch Name	Purpose
6	AMLtoCaseManagement	Loads Event and Business data to Case Management tables.

Note:

The FinancialCrimeGlobalGraph batch for Investigation Hub should be executed after the ICIJ and TM/CM batches.

Pre-configured CS Batches

Table 19-2 Pre-configured Customer Screening Batches

Sequence	Batch Name	Purpose
1	AMLDataLoad	Loads client data.
2	Ingestion	Loads data from staging tables to business tables.
3	• CustomerFullLoad • CustomerDeltaLoad	Loads data into the search engine and creates the index.
4	• WLHMTLoad • WLDJWLoad • WLDJWDeltaLoad • WLWCPREMIUMLoad • WLWCPREMIUMDeltaLoad • WLWCSTANDARDLoad • WLWCSTANDARDDeltaLoad • WLOFACLoad • WLUNLoad • WLEULoad • WLPRIVATELoad	Downloads the respective advanced or private watchlist data and loads it into a search engine index.

Table 19-2 (Cont.) Pre-configured Customer Screening Batches

Sequence	Batch Name	Purpose
5	- IndividualScreening - EntityScreening - Individual314aScreening - Entity314aScreening - IndividualDIScreening - EntityDIScreening - IndividuDIal314aDIScreening - Entity314aDIScreening - CountryWatchlistLoad	Runs the matching rules and generates the events. **Note:** This is an out-of the box sample batch. You can create your own batch with specific parameters.
6	ScreeningToCaseManagement	Creates cases for the alerts.

Pre-configured TF Batches

Table 19-3 Pre-configured Transaction Filtering Batches

Sequence	Batch Name	Purpose
1	AMLDataLoad	Loads client data.
2	Ingestion	Loads data from staging tables to business tables.
3	- WLHMTLoad - WLDJWLoad - WLDJWDeltaLoad - WLWCPREMIUMLoad - WLWCPREMIUMDeltaLoad - WLWCSTANDARDLoad - WLWCSTANDARDDeltaLoad - WLOFACLoad - WLUNLoad - WLEULoad - WLPRIVATELoad	Downloads the respective advanced or private watchlist data and loads it into a search engine index.
4	- CityWatchlistLoad - CountryWatchlistLoad - GoodsWatchlistLoad - PortWatchlistLoad - IdentifierWatchlistLoad - StopKeyWordWatchlistLoad	Downloads the respective advanced or private watchlist data and loads it into a search engine index.

Pre-configured KYC Batches for Deployment Initiation

Table 19-4 Pre-configured KYC Batches for Deployment Initiation

Sequence	Batch Name	Purpose
1	AMLDataLoad	Loads client data.
2	Ingestion	Loads data from staging tables to business tables.
3	KYCCustomerFullLoad	Loads KYC data into the search engine and creates the index.
4	• WLHMTLoad • WLDJWLoad • WLDJWDeltaLoad • WLWCPREMIUMLoad • WLWCPREMIUMDeltaLoad • WLWCSTANDARDLoad • WLWCSTANDARDDeltaLoad • WLOFACLoad • WLUNLoad • WLEULoad • WLPRIVATELoad	Download the respective advanced or private watchlist data and loads it into a search engine index.
5	• KYCIndividualScreening • KYCEntityScreening	Runs the matching rules and generates the events. **Note:** This is an out-of the box sample batch. You can create your own batch with specific parameters.
6	KYCDeploymentInitiation	KYC is done for the Customers and the customers who are to be further investigated are decided.
7	CMIngestion	Loads the data to Case Management Business tables.
8	KYCToCaseManagement	Customers who require investigation are pushed to the Case Manager.

Pre-configured Batches for KYC Daily

Table 19-5 Pre-configured Batches for KYC Daily

Sequence	Batch Name	Purpose
1	AMLDataLoad	Loads client data.
2	CustomerChangeLog	Identifies changes in the Customer's Details. These customers are picked up for KYC.
3	Ingestion	Loads data from staging tables to business tables.
4	• WLHMTLoad • WLDJWLoad • WLDJWDeltaLoad • WLWCPREMIUMLoad • WLWCPREMIUMDeltaLoad • WLWCSTANDARDLoad • WLWCSTANDARDDeltaLoad • WLOFACLoad • WLUNLoad • WLEULoad • WLPRIVATELoad	Download the respective advanced or private watchlist data and loads it into a search engine index. If this batch has already been run once, rerunning this batch is required only if there is new Watchlist data. **Note:** If this batch has already been run once, rerunning this batch is required only if there is new Watchlist data.
5	KYCDaily	KYC is done for the Customers and the customers who are to be further investigated are decided.
6	CMIngestion	Loads the data to Case Management Business tables.
7	KYCToCaseManagement	Customers who require investigation are pushed to the Case Manager.

AMLDataLoad Batch Details

The AMLDataLoad batch loads data provided in the .csv templates into staging tables, which prepare the data for loading into the business tables.

This batch must be run before Ingestion.The following table provides the tasks that are configured for the AMLDataLoad batch. These tasks must be executed in the following order:

Table 19-6 AMLDataLoad Batch Details

Sequence	Tasks for AMLDataLoad Batch	Jobs for AMLDataLoad Batch	Pipelines for AMLDataLoad Batch
1	StartDataLoad	Not Applicable	Not Applicable
2	WatchlistPipeline	Load Watchlist Staging Data	Load Watchlist Staging Data
3	TransactionPipeline	Load Transaction Staging Data	Load Transaction Staging Data
4	CustomerPipeline	Load Customer Staging Data	Load Customer Staging Data
5	AccountPipeline	Load Account Staging Data	Load Account Staging Data
6	InsurancePipeline	Load Insurance Staging Data	Load Insurance Staging Data
7	GatherStats	DLGatherStats	Gather Staging Data Statistics
8	EndDataLoad	Not Applicable	Not Applicable

Note:

Data Loading via Object Storage supports two versions of FSDF, namely, the latest version (8.1.2.4) and the previous version (8.0.8). To specify which FSDF version the template you are using to upload data to Object Storage is compatible with, you must update the parameters in the AMLDataLoad batch as follows:

- **$VERSION$:** Set this parameter to the FSDF version the template you are using to upload data to Object Storage is compatible with.
  As of release 24.2.1, the default for existing customers is **808**. New implementations and existing customers who have migrated to the latest FSDF version must set this value to **8124**. For more information, see Uploading Data Files.

Ingestion Batch Details

The Ingestion batch runs the data pipelines, filters the data and prepares the data for further processing.

Therefore, the Ingestion batch must be run before the TMScenario batch.

This batch loads the data from the staging tables to the business tables in the specified order. The loading process receives, transforms, and loads Market, Business, and Reference data that is required for event detection.

The following table provides the tasks that are configured for the Ingestion batch. These tasks must be executed in the following order:

Table 19-7 Ingestion Batch Details

Sequence	Tasks for Ingestion Batch	Jobs for Ingestion Batch	Pipelines for Ingestion Batch
1	StartBatch	Not Applicable	Not Applicable
2	ACCTTRXNINT	Load Intermediate Account and Transaction Data	Load Intermediate Account and Transaction Data
3	WatchList	Load and Prepare Watchlists	Load and Prepare Watchlists
4	Customer	Load Customer Data	Load Customer Data
5	CustomerAddData	Load Customer Add On Data	Load Customer Add On Data
6	AnticipatoryProfile	Load Customer Anticipatory Profile Data	Load Customer Anticipatory Profile Data
7	Account	Load Account Data	Load Account Data
8	AccountGroup	Load Account Group Data	Load Account Group Data
9	AccountAddData	Load Additional Account Data	Load Additional Account Data
10	AcctAnticipatoryProfile	Load Account Anticipatory Profile Data	Load Account Anticipatory Profile Data
11	CustMapData	Load Customer Mapping Data	Load Customer Mapping Data
12	SupplyInfo	Derive Risk and Load Supplementary Information	Derive Risk and Load Supplementary Information
13	Transaction	Load Transaction Data and Derive External Entities and Risk	Load Transaction Data and Derive External Entities and Risk
14	TrustedPair	Load Trusted Pair Data	Load Trusted Pair Data
15	LoanData	Load Loan Data	Load Loan Data
16	InsuranceData	Load Insurance Data	Load Insurance Data
17	CleanAMTempTables	CleanAMTempTables	Not Applicable
18	EndBatch	Not Applicable	Not Applicable

Note:

- Clients using Oracle FCCM KYC Cloud Service in an integrated TM & KYC setup must populate the FCC_CUST_KYC_RISK table via KYC Batch to calculate the KYC Risk Score.
- Oracle FCCM Transaction Monitoring Cloud Service considers the customer’s KYC Risk Score as of the prior day.

TMScenario Batch Details

The TMScenario batch uses the data that is prepared during ingestion and executes the scenario pipelines in the configured sequence to generate events.

For detailed information about the pre-configured scenarios, see the Technical Scenario Description.

> **Note:**
>
> You cannot run the TMScenario batch before running the Ingestion batch.

The following table provides the tasks that are configured for the TMScenario batch. These tasks can be executed in the order required by your implementation, but must begin with a StartBatch, followed by Calendar, then the Jobs you will be running, and end with an EndBatch.

Table 19-8 TMScenario Batch Details

Sequence	Tasks for TMScenario Batch	Jobs for TMScenario Batch	Pipelines for TMScenario Batch
1	StartBatch	Not Applicable	Not Applicable
2	CALENDAR	Load Calendar Data	Load Calendar Data
3	HRECUST	Focal High Risk Entity - Customer Focus	Focal High Risk Entity - Customer Focus
4	HRGACCT	High Risk Geography - Account Focus	High Risk Geography - Account Focus
5	POSSIBLECTRCUST	Possible Currency Transaction Report - Customer Focus	Possible Currency Transaction Report - Customer Focus
6	LRTCUST	Large Reportable Transaction - Customer Focus	Large Reportable Transaction - Customer Focus
7	FTNINTCUST	Patterns of Funds Transfers Between Internal Accounts and Customers - Customer Focus	Patterns of Funds Transfers Between Internal Accounts and Customers - Customer Focus
8	FTNEXTCUSTC	Patterns of Funds Transfers Between Receiving Customers and External Entity - Customer Focus	Patterns of Funds Transfers Between Receiving Customers and External Entity - Customer Focus
9	FTNEXTCUSTD	Patterns of Funds Transfers Between Sending Customers and External Entity - Customer Focus	Patterns of Funds Transfers Between Sending Customers and External Entity - Customer Focus
10	RMFCUST	Rapid Movement of Funds - Customer Focus	Rapid Movement of Funds - Customer Focus
11	LDACCT	Large Depreciation of Account Value - Account Focus	Large Depreciation of Account Value - Account Focus
12	HREEE	Focal High Risk Entity - External Entity Focus	Focal High Risk Entity - External Entity Focus
13	HRGEE	High Risk Geography - External Entity Focus	High Risk Geography - External Entity Focus
14	LRTEE	Large Reportable Transactions - External Entity Focus	Large Reportable Transactions - External Entity Focus
15	POSSIBLECTREE	Possible Currency Transaction Report - External Entity Focus	Possible Currency Transaction Report - External Entity Focus

Table 19-8 (Cont.) TMScenario Batch Details

Sequence	Tasks for TMScenario Batch	Jobs for TMScenario Batch	Pipelines for TMScenario Batch
16	HUBSPOKE	Hub and Spoke - Customer Focus	Hub and Spoke - Customer Focus
17	HRCPAC	High Risk Counter Party - Account Focus	High Risk Counter Party - Account Focus
18	HRCPCU	High Risk Counter Party - Customer Focus	High Risk Counter Party - Customer Focus
19	HRCPEE	High Risk Counter Party - External Entity Focus	High Risk Counter Party - External Entity Focus
20	CIBFAAF	CIB Foreign Activity - Account Focus	CIB Foreign Activity - Account Focus
21	CIBHRGAAF	CIB High Risk Geography Activity - Account Focus	CIB High Risk Geography Activity - Account Focus
22	CIBSCPAAAF	CIB Significant Change From Previous Average Activity - Account Focus	CIB Significant Change From Previous Average Activity - Account Focus
23	CIBSCPPAAF	CIB Significant Change From Previous Peak Activity - Account Focus	CIB Significant Change From Previous Peak Activity - Account Focus
24	EIIAF	Escalation in Inactive Account - Account Focus	Escalation in Inactive Account - Account Focus
25	RMFAAAF	Rapid Movement of Funds All Activity - Account Focus	Rapid Movement of Funds All Activity - Account Focus
26	STRAVCRAC	Structuring - Avoidance of Reporting Thresholds Credit - Account Focus	Structuring - Avoidance of Reporting Thresholds - Account Focus
27	STRAVDBAC	Structuring - Avoidance of Reporting Thresholds Debit - Account Focus	Structuring - Avoidance of Reporting Thresholds - Account Focus
28	STRAVCRCU	Structuring - Avoidance of Reporting Thresholds Credit - Customer Focus	Structuring - Avoidance of Reporting Thresholds - Customer Focus
29	STRAVDBCU	Structuring - Avoidance of Reporting Thresholds Debit - Customer Focus	Structuring - Avoidance of Reporting Thresholds - Customer Focus
30	STRAVCREE	Structuring - Avoidance of Reporting Thresholds Credit - External Entity Focus	Structuring - Avoidance of Reporting Thresholds - External Entity Focus
31	STRAVDBEE	Structuring - Avoidance of Reporting Thresholds Debit - External Entity Focus	Structuring - Avoidance of Reporting Thresholds - External Entity Focus
32	STRDEPWDCRCU	Structuring - Deposits Withdrawals of Mixed Monetary Instruments Credit - Customer Focus	Structuring - Deposits Withdrawals of Mixed Monetary Instruments - Customer Focus
33	STRDEPWDDBCU	Structuring - Deposits Withdrawals of Mixed Monetary Instruments Debit - Customer Focus	Structuring - Deposits Withdrawals of Mixed Monetary Instruments - Customer Focus

Table 19-8 (Cont.) TMScenario Batch Details

Sequence	Tasks for TMScenario Batch	Jobs for TMScenario Batch	Pipelines for TMScenario Batch
34	TRAEFTEEF	Transactions in Round Amounts EFT - External Entity Focus	Transactions in Round Amounts EFT - External Entity Focus
35	TRAMAF	Transactions in Round Amounts - Account Focus	Transactions in Round Amounts - Account Focus
36	TRAMIEEF	Transactions in Round Amounts MI - External Entity Focus	Transactions in Round Amounts MI - External Entity Focus
37	STRPOTCRCU	Structuring - Potential Structuring in Cash and Equivalents Credit - Customer Focus	Structuring - Potential Structuring in Cash and Equivalents Credit - Customer Focus
38	STRPOTDBCU	Structuring - Potential Structuring in Cash and Equivalents Debit - Customer Focus	Structuring - Potential Structuring in Cash and Equivalents Debit - Customer Focus
39	ATMFTAC	Anomalies in ATM Bank Card - Foreign Transactions - Account Focus	Anomalies in ATM Bank Card - Foreign Transactions - Account Focus
40	ATMFTCU	Anomalies in ATM Bank Card - Foreign Transactions - Customer Focus	Anomalies in ATM Bank Card - Foreign Transactions - Customer Focus
41	LSTCU	Single or Multiple Cash Transactions - Large Significant Transactions - Customer Focus	Single or Multiple Cash Transactions - Large Significant Transactions - Customer Focus
42	HREAC	Focal High Risk Entity - Account Focus	Focal High Risk Entity - Account Focus
43	ATMEWAC	Anomalies in ATM, Bank Card- Excessive Withdrawals - Account Focus	Anomalies in ATM, Bank Card- Excessive Withdrawals - Account Focus
44	ATMEWCU	Anomalies in ATM, Bank Card- Excessive Withdrawals - Customer Focus	Anomalies in ATM, Bank Card- Excessive Withdrawals - Customer Focus
45	AFEARLYPAYOFF	Early Payoff or Paydown of a Credit Product - Account Focus	Early Payoff or Paydown of a Credit Product - Account Focus
46	CFEARLYPAYOFF	Early Payoff or Paydown of a Credit Product -Customer Focus	Early Payoff or Paydown of a Credit Product -Customer Focus
47	CleanAMTempTables	CleanAMTempTables	CleanAMTempTables
48	EndBatch	Not Applicable	Not Applicable

A copy of the TMScenario batch is provided based on the frequency which each pre-configured scenario should be run, such as Daily, Weekly, Bi-Weekly, and Monthly. These batches contain only the scenario pipelines and jobs that will be run using this frequency. For detailed information about the frequency period for pre-configured scenarios, see the

Technical Scenario Description. For information about how to set precedence for the Batch Group when creating your own scenario configuration, see Using Scheduler Services.

KYCToCaseManagement Batch Details

The DM Utility job KYCToCaseManagement moves KYC Event and Business data to Case Management tables.

> **Note:**
>
> An ECMProcess must follow only one KYCProcess.

The following table provides the tasks that are configured for the KYCToCaseManagement batch. These tasks must be executed in the following order:

Table 19-9 KYCToCaseManagement Batch Details

Sequence	Tasks for KYCToCaseManagements Batch	Jobs for KYCToCaseManagement Batch	Pipelines for KYCToCaseManagement Batch
1	ECMStartBatch	Not Applicable	Not Applicable
2	PipelineStart	Not Applicable	Not Applicable
3	LoadKYCEventData2CaseManagement	Load KYC Event Data to Case Management	Load KYC Event Data to Case Management
4	LoadKYCEventedCustomerData2CaseManagement	Load KYC Evented Customer Data to Case Management	Load KYC Evented Customer Data to Case Management
5	LoadKYCEventedAccountData2CaseManagement	Load Evented KYC Account Data to Case Management	Load Evented KYC Account Data to Case Management

Table 19-9 (Cont.) KYCToCaseManagement Batch Details

Sequence	Tasks for KYCToCaseManagements Batch	Jobs for KYCToCaseManagement Batch	Pipelines for KYCToCaseManagement Batch
6	EVCORR **Note:** For more information, see Defining Correlatio	Not Applicable	Not Applicable

Table 19-9 (Cont.) KYCToCaseManagement Batch Details

Sequence	Tasks for KYCToCaseManagements Batch	Jobs for KYCToCaseManagement Batch	Pipelines for KYCToCaseManagement Batch
	nScoringRules.		

Table 19-9 (Cont.) KYCToCaseManagement Batch Details

Sequence	Tasks for KYCToCaseManagements Batch	Jobs for KYCToCaseManagement Batch	Pipelines for KYCToCaseManagement Batch
7	SCORING **Note:** For more information, see Managing Scoring Pi	KYC Case Scoring	KYC Case Scoring

Table 19-9 (Cont.) KYCToCaseManagement Batch Details

Sequence	Tasks for KYCToCaseManagements Batch	Jobs for KYCToCaseManagement Batch	Pipelines for KYCToCaseManagement Batch
	pelines.		
8	CASEGEN	Not Applicable	Not Applicable
9	CASELOAD	Load Case Data	Load Case Data
10	PRECSUPDT	Not Applicable	Not Applicable
11	UpdateCaseDtlsToKYC	Populate Case Details to KYC	Populate Case Details to KYC
12	PipelineEnd	Not Applicable	Not Applicable
13	ECMEndBatch	Not Applicable	Not Applicable

AMLtoCaseManagement Batch Details

The DM Utility job AMLtoCaseManagement moves Event and Business data to Case Management tables.

Once the data is moved to consolidation tables, it is used for Correlation. Cases are generated after correlation.

> **Note:**
>
> You should run the TMScenario batch before running the AMLtoCaseManagement batch.

You must perform the following pre-batch configurations before executing the AMLtoCaseManagement Batch.

- Start the AMLtoCaseManagement Batch
- Correlation Case Type Mapping

The following table provides the tasks that are configured for the AMLtoCaseManagement batch. These tasks must be executed in the following order:

Table 19-10 AMLtoCaseManagement Batch Details

Sequ ence	Tasks for AMLtoCaseManagement Batch	Jobs for AMLtoCaseManagement Batch	Pipelines for AMLtoCaseManagement Batch
1	ECMSRTBTH	Not Applicable	Not Applicable
2	PL_SRT	Not Applicable	Not Applicable
3	SCRLOAD	Load Scenario Data to Case Management	Load Scenario Data to Case Management
4	EVNTPOP	Load Event Data to Case Management	Load Event Data to Case Management
5	EVCUSTLOAD	Load Evented Customer Data to Case Management	Load Evented Customer Data to Case Management
6	EVACCTLOAD	Load Evented Account Data to Case Management	Load Evented Account Data to Case Management
7	EVTRXNLOAD	Load Evented Transaction Data to Case Management	Load Evented Transaction Data to Case Management
8	EVEXTELOAD	Load Evented External Entity and Derived Address Data to Case Management	Load Evented External Entity and Derived Address Data to Case Management

Table 19-10 (Cont.) AMLtoCaseManagement Batch Details

Sequence	Tasks for AMLtoCaseManagement Batch	Jobs for AMLtoCaseManagement Batch	Pipelines for AMLtoCaseManagement Batch
9	EVCORR **Note:** For more information, see Defining Correlatio	Not Applicable	Not Applicable

Table 19-10 (Cont.) AMLtoCaseManagement Batch Details

Sequence	Tasks for AMLtoCaseManagement Batch	Jobs for AMLtoCaseManagement Batch	Pipelines for AMLtoCaseManagement Batch
	nScoringRules.		

Table 19-10   (Cont.) AMLtoCaseManagement Batch Details

Sequence	Tasks for AMLtoCaseManagement Batch	Jobs for AMLtoCaseManagement Batch	Pipelines for AMLtoCaseManagement Batch
10	SCORING **Note:** For more information, see Managing Scoring Pi	Case Scoring	Case Scoring

Table 19-10 (Cont.) AMLtoCaseManagement Batch Details

Sequence	Tasks for AMLtoCaseManagement Batch	Jobs for AMLtoCaseManagement Batch	Pipelines for AMLtoCaseManagement Batch
	pelines.		
11	CASEGEN	Not Applicable	Not Applicable
12	CASELOAD	Load Case Data	Load Case Data
13	PRECSUPDT	Not Applicable	Not Applicable
14	CleanAMTempTables	CleanAMTempTables	Not Applicable
15	ECMECND	Not Applicable	Not Applicable

Starting the AMLtoCaseManagement Batch

In order to generate cases, you must define and start the AMLtoCaseManagement batch.

Follow these steps before starting the AMLtoCaseManagement batch:

1. Navigate to the Transaction Monitoring page.
2. Click ☰ to access the Navigation List. The Navigation List displays the list of modules.
3. Click **Scheduler** in the Navigation List. The Scheduler Service page opens in a new window.
4. Click **Define Batch**.
5. Click **Copy** ⧉ to copy the pre-configured AMLtoCaseManagement batch. Update the Batch Details as needed.
6. Click **Define Tasks**. Select the copy of the AMLtoCaseManagement batch that you just created.
7. Add a Scoring pipeline to this batch and configure the Scoring rules. For information about how to create and configure scoring pipelines, see the Creating_Scoring_Pipelines section.

   > **Note:**
   >
   > A Scoring pipeline must be configured and associated with this batch, or no cases will be generated.

8. Define tasks for the ECMSRTBTH task in the AMLtoCaseManagement Batch.

9. Add the following parameters to the **ECMSRTBTH** task in the AMLtoCaseManagement Batch.

Table 19-11 Parameters in AMLtoCaseManagement Batch

Parameter Name	Expected Value
DATAORIGIN	MAN **Note:** CMCSMAN is reserved for Manual Events. Using this field to send data may result in batch failure due to the same dataOrigin of multiple events containing the same event code.
FICMISDATE	FICMISDATE
BATCHTYPE	DATA
BATCHRUNID	BATCHRUNID
component	ALL
dataorigin	MAN
sourcebatch	-
currentbatch	ALL

When the Start Batch run is executed, it loads the data to the FCC_CM_BATCH_RUN table.

Correlation Case Type Mapping

You must define the Case Type mapping before executing the AMLtoCaseManagement Batch.

This is performed using the Case Type Admin function. For more information, see the Case Types section.

Integrating with Third-Party Case Management Systems

The AMLToCMEventData batch supports integration with third-party case management systems by providing a means to extract evented data which can be loaded into an external system.

The following table provides the tasks that are configured for the AMLToCMEventData batch. These tasks must be executed in the following order:

Table 19-12 AMLToCMEventData Batch Details

Sequence	Tasks for AMLToCMEventData Batch	Jobs for AMLToCMEventData Batch	Pipelines for AMLToCMEventData Batch
1	ECMSRTBTH	Not Applicable	Not Applicable
2	PL_SRT	Not Applicable	Not Applicable
3	SCRLOAD	Load Scenario Data to Case Management	Load Scenario Data to Case Management
4	EVNTPOP	Load Event Data to Case Management	Load Event Data to Case Management
5	EVCUSTLOAD	Load Evented Customer Data to Case Management	Load Evented Customer Data to Case Management
6	EVACCTLOAD	Load Evented Account Data to Case Management	Load Evented Account Data to Case Management
7	EVTRXNLOAD	Load Evented Transaction Data to Case Management	Load Evented Transaction Data to Case Management
8	EVEXTELOAD	Load Evented External Entity and Derived Address Data to Case Management	Load Evented External Entity and Derived Address Data to Case Management
9	DropTempTables	DropTempTables	Not Applicable
10	ECMECND	Not Applicable	Not Applicable

Note:

You can find pre-configured sample data pipelines, Evented Customer Details (data extraction from a single table) and Evented Customer Details - Two Tables Join (data extraction from mutliple tables), which provide examples of the pipeline to extract data.

Run the TMCS_CSV_Export batch to generate the .csv file of the extracted data.

For information about how to download the extracted data in .csv format, see Using Object PAR in the Oracle FCCM Cloud Service Using Rest API guide.

AMLHolidayMasterDataLoad Batch Details

The AMLHolidayMasterDataLoad batch loads holiday and non-working day data into the FCC_AM_HOLIDAY_MASTER and FCC_AM_DATAORIGIN_COUNTRY_MA tables.

There are no tasks associated with this batch, however you must update the Data Origin and Batch Date parameters before running this batch.

CMIngestion Batch Details

The CMIngestion batch loads the data into the Case Management Business tables for further processing.

The CMIngestion batch must be run as the next to last batch. The following table provides the tasks that are configured for the CMIngestion batch. These tasks must be executed in the following order:

Table 19-13 CMIngestion Batch Details

Sequence	Tasks for CMIngestion Batch	Jobs for CMIngestion Batch	Pipelines for CMIngestion Batch
1	ECMSRTBTH	Not Applicable	Not Applicable
2	PL_SRT	Not Applicable	Not Applicable
3	BCUSTLOAD	Load Scenario Data to Case Management	Load Customer Business Data to Case Management
4	BACCTLOAD	Load Account Business Data to Case Management	Load Account Business Data to Case Management
5	BTRXNLOAD	Load Transaction Business Data to Case Management	Load Transaction Business Data to Case Management
6	BEXTENLOAD	Load External Entity and Derived Address Data to Case Management	Load External Entity and Derived Address Data to Case Management
7	PL_END	Not Applicable	Not Applicable
8	ECMEnd	Not Applicable	Not Applicable

FullLoadCustomer Batch Detail

The FullLoadCustomer batch loads the Customer details into the search engine.

The following table provides the list of tasks in the FullLoadCustomer batch. These tasks must be executed in the following order:

Table 19-14 FullLoadCustomer Batch Details

Sequence	Tasks for FullLoadCustomer Batch	Jobs for FullLoadCustomer Batch	Pipelines for FullLoadCustomer Batch
1	StartBatchCustomer	Not Applicable	Not Applicable
2	FullLoadCustomerTask	Full Load Customer Data To ES	Full Load Customer Data To ES
3	EndBatchCustomer	Not Applicable	Not Applicable

DeltaLoadCustomer Batch Details

The DeltaLoadCustomer batch supports Delta loading of the Customer details into the search engine.

The following table provides the list of tasks in the DeltaLoadCustomer batch. These tasks must be executed in the following order:

Table 19-15 DeltaLoadCustomer Batch Details

Sequence	Tasks for DeltaLoadCustomer Batch	Jobs for DeltaLoadCustomer Batch	Pipelines for DeltaLoadCustomer Batch
1	StartBatchCustomer	Not Applicable	Not Applicable

Table 19-15 (Cont.) DeltaLoadCustomer Batch Details

Sequence	Tasks for DeltaLoadCustomer Batch	Jobs for DeltaLoadCustomer Batch	Pipelines for DeltaLoadCustomer Batch
2	DeltaLoadCustomerTask	Delta Load Customer Data To ES	Delta Load Customer Data To ES
3	EndBatchCustomer	Not Applicable	Not Applicable

Note:

For the DeltaLoadCustomer batch, all ingestion batches must have the word 'ingestion' present as part of the batch name. If the batch name is incorrect, the data will not be loaded.

CustomerFullLoad Batch Detail

The CustomerFullLoad batch loads the Customer details into the search engine.

The following table provides the list of tasks in the CustomerFullLoad batch. These tasks must be executed in the following order:

Table 19-16 CustomerFullLoad Batch Details

Sequence	Tasks for CustomerFullLoad Batch	Jobs for CustomerFullLoad Batch	Pipelines for CustomerFullLoad Batch
1	StartBatchCustomerFullLoad	Not Applicable	Not Applicable
2	CustomerFullLoad	Customer Full Load	Customer Full Load
3	EndBatchCustomerFullLoad	Not Applicable	Not Applicable

KYCCustomerFullLoad Batch Detail

The KYCCustomerFullLoad batch loads the Customer KYC details into the search engine.

The following table provides the list of tasks in the KYCCustomerFullLoad batch. These tasks must be executed in the following order:

Table 19-17 KYCCustomerFullLoad Batch Details

Sequence	Tasks for KYCCustomerFullLoad Batch	Jobs for KYCCustomerFullLoad Batch	Pipelines for KYCCustomerFullLoad Batch
1	StartBatchKYCCustomerFullLoad	Not Applicable	Not Applicable
2	KYCCustomerFullLoad	KYC Customer Full Load	KYC Customer Full Load

Table 19-17 (Cont.) KYCCustomerFullLoad Batch Details

Sequence	Tasks for KYCCustomerFullLoad Batch	Jobs for KYCCustomerFullLoad Batch	Pipelines for KYCCustomerFullLoad Batch
3	EndBatchKYCCustomerFullLoad	Not Applicable	Not Applicable

KYCDeploymentInitiation (DI) Batch Details

The KYCDeploymentInitiation batch uses the data that is prepared during ingestion and executes the pipelines in the configured sequence to generate assessments.

The following table provides the tasks that are configured for the KYCDeploymentInitiation batch.

Note:

You can run the KYCDeploymentInitiation batch in the following ways:

- Using Multiple Data Origins in sequential batch runs.
- Using a Single Data Origin with Multiple Jurisdictions in a single batch.

Note:

ATTENTION: Slicing the customer data is mandatory before running the KYCDeploymentInitiation batch. For more information on Slicing Customer data, see the FCCM Cloud Master Data Guide.

These tasks must be executed in the following order:

Table 19-18 KYCDeploymentInitiation Batch Details

Sequence	Tasks for KYCDeploymentInitiation Batch	Jobs for KYCDeploymentInitiation Batch	Pipelines for KYCDeploymentInitiation Batch
1	StartBatch	Not Applicable	Not Applicable
2	StartDataPipelineServiceBatch	Not Applicable	Not Applicable
3	KYCClearProcessing Data	KYC Clear Processing Data	KYC Clear Processing Data
4	LoadKYCCustomerFilter	preFilterDemo	Load Deployment Initiation KYC Customers
5	LoadKYCCustomerInterestedParties	Load KYC Customer Interested Parties	Load KYC Customer Interested Parties
6	Calendar	Calendar	Calendar

Table 19-18 (Cont.) KYCDeploymentInitiation Batch Details

Sequence	Tasks for KYCDeploymentInitiation Batch	Jobs for KYCDeploymentInitiation Batch	Pipelines for KYCDeploymentInitiation Batch
7	KYCScenarioBasedRiskFactor	KYC Transaction Based Risk Factors	KYC Transaction Based Risk Factors
8	KYCProcessingAccountData	Load KYC Account Processing Data	Load KYC Customer Account Processing Data
9	KYCProcessingCustomerData	Load KYC Customer Processing Data	Load KYC Customer Processing Data
10	LoadKYCCustomerDataForScoring	Load KYC Customer Data For Scoring	Load KYC Customer Data For Scoring
11	LoadKYCCustomerMatchesDataForScoring	Load KYC Customer Matches Data For Scoring	Load KYC Customer Matches Data For Scoring
12	KYCRACreation	KYC Batch RA Creation	KYC Batch RA Creation
13	LoadKYCCustomerRiskScore	Load KYC Customer Risk Score	Load KYC Customer Risk Score
14	SlicingCompletionUpdate	KYC Customer Slicing Update	KYC Customer Slicing Update
15	EndDataPipelineBatch	Not Applicable	Not Applicable
16	EndBatch	Not Applicable	Not Applicable

KYCDaily Batch Details

The KYCDaily batch performs KYC for customers and the customers who are to be further investigated are decided.

Note:

You can run the KYCDaily batch in the following ways:

- Using Multiple Data Origins in sequential batch runs.
- Using a Single Data Origin with Multiple Jurisdictions in a single batch.

These tasks must be executed in the following order:

Table 19-19 KYCDaily Batch Details

Sequence	Tasks for KYCDaily Batch	Jobs for KYCDaily Batch	Pipelines for KYCDaily Batch
1	StartBatch	Not Applicable	Not Applicable
2	StartDataPipelineServiceBatch	Not Applicable	Not Applicable

Table 19-19 (Cont.) KYCDaily Batch Details

Sequence	Tasks for KYCDaily Batch	Jobs for KYCDaily Batch	Pipelines for KYCDaily Batch
3	KYCClearProcessingData	KYC Clear Processing Data	KYC Clear Processing Data
4	LoadKYCChangeLogData	Load KYC Change Log	Load KYC Change Log
5	LoadKYCCustomerFilter	preFilterDemo	Load Deployment Initiation KYC Customers
6	LoadKYCCustomerInterestedParties	Load KYC Customer Interested Parties	Load KYC Customer Interested Parties
7	Calendar	Calendar	Calendar
8	KYCScenarioBasedRiskFactor	KYC Transaction Based Risk Factors	KYC Transaction Based Risk Factors
9	KYCProcessingAccountData	Load KYC Account Processing Data	Load KYC Account Processing Data
10	KYCProcessingCustomerData	Load KYC Customer Processing Data	Load KYC Customer Processing Data
11	FullLoadKYCCustomerTask	Load KYC Daily Customer to ES	Load KYC Daily Customer to ES
12	KYCIndividualBatchScreening	KYC Individual Batch Screening	KYC Individual Batch Screening
13	EntityBatchScreening	KYC Customer Daily Load	KYC Customer Daily Load
14	LoadKYCCustomerDataForScoring	Load KYC Customer Data For Scoring	Load KYC Customer Data For Scoring
15	LoadKYCCustomerMatchesDataForScoring	Load KYC Customer Matches Data For Scoring	Load KYC Customer Matches Data For Scoring
16	KYCRACreation	KYC Batch RA Creation	KYC Batch RA Creation
17	LoadKYCCustomerRiskScore	Load KYC Customer Risk Score	Load KYC Customer Risk Score
18	EndDataPipelineBatch	Not Applicable	Not Applicable
19	EndBatch	Not Applicable	Not Applicable

Using External Case Management Feedback

You can create a task to consume External Case Management feedback into the KYC system.

1. Copy the existing KYCClearProcessingData task in the KYCDaily batch and give an appropriate new task name, new task code and $JOBNAME$ as **Load External System Feedback To KYC**.
2. Adjust the precedence by moving the newly created task associated to Load External System Feedback To KYC between the **LoadKYCCustomerRiskScore** and **EndDataPipelineBatch** tasks.
3. Run the KYCDaily batch.

Note:

The N_REQUEST_ID, N_RA_ID and FIC_MIS_DATE are composite primary keys. Make sure to check the following points while feeding External Case Management feedback into KYC via STG_FCC_KYC_EXT_SYS_FEEDBACK.csv file.

- The N_REQUEST_ID, N_RA_ID and FIC_MIS_DATE columns can never be null.
- The N_REQUEST_ID, N_RA_ID and FIC_MIS_DATE columns together must be unique such that for a given FIC_MIS_DATE, the N_RA_ID and N_REQUEST_ID combination cannot be repeated.
- All batch RA records must always have the N_REQUEST_ID column value as **0**.

KYCCustomerRAExport - Exporting KYC Risk Assessments

You can configure the KYCCustomerRAExport batch to export the risk assessment records.

You can configure the KYCCustomerRAExport batch to export the risk assessment records in the following ways:

- Exporting for Integration with External CRM/Case Management System
- Exporting for Bulk Export of Records Displayed on Risk Assessment UI

Exporting KYC Risk Assessments for Integration with External CRM/Case Management System

You can configure the KYCCustomerRAExport batch to export the risk assessment records into a CSV file. This file can be fed to an external CRM or Case Management System for investigation.

The following table provides the list of tasks in the KYCCustomerRAExport batch. These tasks must be executed in the following order:

Table 19-20 KYCCustomerRAExport Batch Details

Sequence	Tasks for KYCCustomerRAExport Batch	Jobs for KYCCustomerRAExport Batch	Pipelines for KYCCustomerRAExport Batch
1	StartBatch	Not Applicable	Not Applicable
2	StartDataPipelineBatch	Not Applicable	Not Applicable
3	CSVUPLOAD	KYC Customer RA Export	KYC Customer RA Export
4	EndDataPipelineBatch	Not Applicable	Not Applicable
5	EndBatch	Not Applicable	Not Applicable

Before running this batch, configure the date field of the Dataset widget of the KYC Customer RA Export pipeline as required. Valid formats are as follows:

- TRUNC(SYSDATE): Exports Risk Assessments created on the same day. Use this condition if the task is added as part of the KYCDaily or KYCDeploymentInitiation batch.
- 24-NOV-2023': Exports Risk Assessments created on that day. The format is 'DD-MON-YYYY'.
- TRUNC(TO_DATE('2023-11-24','yyyy-mm-dd')): Exports Risk Assessments created on that day. The date is given here and the date format should be in sync.

> **Note:**
>
> To execute the CSVUPLOAD task along with the KYCDaily or KYCDeploymentInitiation batch, follow these steps:
>
> 1. Create a new task in the KYCDaily or KYCDeplomentInitiation batch. (Refer to the CSVUPLOAD task in the pre-shipped KYCCustomerRAExport batch and set all the task parameters and execution URL accordingly.)
> 2. Set this task before the EndDataPipelineBatch task.

Bulk Export of Records Displayed on Risk Assessment UI

Similar to the Export Risk Assessments functionality in the KYC Customer Risk Assessment and KYC Prospect Risk Assessment screens, customer risk assessments can be exported using this batch in the form of a CSV file.

The pipeline and the job required for this Customer Risk Assessment Export are pre-configured. By default, this pipeline exports Customer/Prospect Risk Assessments generated in the last 7 days.

To export the Customer risk assessments similar to the UI, follow these steps:

1. Copy the pre-configured CSV export batch, KYCCustomerRAExport, with an appropriate new name and code.
2. In the CSVUPLOAD task of this newly copied batch, replace the value of $JOBNAME$ to Customer Risk Assessment Export and execute the batch.

To export the Prospect Risk Assessments similar to the UI, follow these steps:

1. Copy the pre-configured CSV export batch, KYCProspectRAExport, with an appropriate new name and code.
2. In the CSVUPLOAD task of this newly copied batch, replace the value of $JOBNAME$ to Prospect Risk Assessment Export and execute the batch.

> **Note:**
>
> To export Risk assessments generated in a specific date range or based on any filter already available on the KYC RA screen, these filters can be configured in the pipeline before the batch is executed.

CustomerChangeLog Batch Details

The CustomerChangeLog batch identifies which customer information has changed since the last time the batch was run.

The following table provides the list of tasks in the CustomerChangeLog batch. These tasks must be executed in the following order:

Table 19-21 CustomerChangeLog Batch Details

Sequence	Tasks for CustomerChangeLog Batch	Jobs for CustomerChangeLog Batch	Pipelines for CustomerChangeLog Batch
1	StartBatch	Not Applicable	Not Applicable
2	startDataPipeline	Not Applicable	Not Applicable
3	populateCustomerChangeLog	ChangeLog	
4	EndBatch	Not Applicable	Not Applicable

> **Note:**
>
> All columns in the changelog must be type2 in the Change Log pipelines. Visit support.oracle.com for the Customer Change Log attributes list.

Configuring Change Logs for Multiple Entities

You can configure the CustomerChangeLog pre-configured batch to execute a change log for different entities in the same batch.

By default, the CustomerChangeLog pre-configured batch has a populateCustomerChangeLog task with STG_PARTY_MASTER as the $CHGTBLNM$ parameter value. To execute a change log for different entities in the same batch, follow these steps:

1. Navigate to the **Scheduler Services**.
2. In the Scheduler Service, navigate to Define Task.
3. Select **CustomerChangeLog** from the **Batch** drop-down list.
4. Copy the **populateCustomerChangeLog** task and rename the **Task Name** and **Task Code**.
5. Edit the **$CHGTBLNM$** parameter value for any entity other than STG_PARTY_MASTER and click **Save**.
   - The parameter value for country of residence is FCC_STG_PARTY_ADDRESS_VW.
   - The parameter value for source of wealth is FCC_STG_PARTY_DETAILS_VW.

> **Note:**
>
> Each new entity of the change log must have one new task copied and edited.

6. Edit the precedence for the newly created tasks. The tasks should follow one after the other. In the end, the endDataPipeline task should have the preceding task as the nth populateCustomerChangeLog task.

1. The populateCustomerChangeLog task should be marked as the preceding task for populateCustomerChangeLog2.
2. The populateCustomerChangeLog2 task should be set as the preceding task for populateCustomerChangeLog3.
3. The populateCustomerChangeLog3 task should be the preceding task for endDataPipeline task.

This allows all the populateCustomerChangeLog tasks to be captured in one execution of the CustomerChangeLog Batch.

> **Note:**
>
> You can also run the CustomerChangeLog batch once per stage entity. To do this, set the task parameter value of populateCustomerChangeLog, such as, $CHGTBLNM$, accordingly and trigger the batch. Once that execution is complete, the same process can be repeated for other stage entities.

Transaction Filtering Watchlist Batch Details

Oracle's Transaction Filtering solution provides pre-configured batches.

Oracle's Transaction Filtering solution provides the following pre-configured batches.

- CityWatchlistLoad
- CountryWatchlistLoad
- GoodsWatchlistLoad
- PortWatchlistLoad
- IdentifierWatchlistLoad
- StopKeyWordWatchlistLoad

These batches are described in detail in the following sections.

CityWatchlistLoad Batch Details

The CityWatchlistLoad batch downloads the city watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the CityWatchlistLoad batch. These tasks must be executed in the following order:

Table 19-22 CityWatchlistLoad Batch Details

Sequence	Tasks for CityWatchlistLoad Batch	Jobs for CityWatchlistLoad Batch	Pipelines for CityWatchlistLoad Batch
1	StartBatchCityList	Not Applicable	Not Applicable
2	LoadCityListData	Load City Watchlist	Load City Watchlist
3	EndBatchCityList	Not Applicable	Not Applicable

CountryWatchlistLoad Batch Details

The CountryWatchlistLoad batch downloads the country watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the CountryWatchlistLoad batch. These tasks must be executed in the following order:

Table 19-23 CountryWatchlistLoad Batch Details

Sequence	Tasks for CountryWatchlistLoad Batch	Jobs for CountryWatchlistLoad Batch	Pipelines for CountryWatchlistLoad Batch
1	StartBatchCountryList	Not Applicable	Not Applicable
2	LoadCountryListData	Load Country Watchlist	Country Data Load
3	EndBatchCountryList	Not Applicable	Not Applicable

GoodsWatchlistLoad Batch Details

The GoodsWatchlistLoad batch downloads the Goods watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the GoodsWatchlistLoad batch. These tasks must be executed in the following order:

Table 19-24 GoodsWatchlistLoad Batch Details

Sequence	Tasks for GoodsWatchlistLoad Batch	Jobs for GoodsWatchlistLoad Batch	Pipelines for GoodsWatchlistLoad Batch
1	StartBatchGoodsList	Not Applicable	Not Applicable
2	LoadGoodsListData	Load Goods Watchlist	Goods Data Load
3	EndBatchGoodsList	Not Applicable	Not Applicable

PortWatchlistLoad Batch Details

The PortWatchlistLoad batch downloads the Port watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the PortWatchlistLoad batch. These tasks must be executed in the following order:

Table 19-25 PortWatchlistLoad Batch Details

Sequence	Tasks for PortWatchlistLoad Batch	Jobs for PortWatchlistLoad Batch	Pipelines for PortWatchlistLoad Batch
1	StartBatchPortList	Not Applicable	Not Applicable
2	LoadPortListData	Load Port Watchlist	Port Data Load
3	EndBatchPortList	Not Applicable	Not Applicable

IdentifierWatchlistLoad Batch Details

The IdentifierWatchlistLoad batch downloads the Identifier watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the IdentifierWatchlistLoad batch. These tasks must be executed in the following order:

Table 19-26 IdentifierWatchlistLoad Batch Details

Sequence	Tasks for IdentifierWatchlistLoad Batch	Jobs for IdentifierWatchlistLoad Batch	Pipelines for IdentifierWatchlistLoad Batch
1	StartBatchIdentifierList	Not Applicable	Not Applicable
2	LoadIdentifierListData	Load Identifier Watchlist	Load Identifier
3	EndBatchIdentifierList	Not Applicable	Not Applicable

StopKeyWordWatchlistLoad Batch Details

The StopKeyWordWatchlistLoad batch downloads the StopKeyWord watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the StopKeyWordWatchlistLoad batch. These tasks must be executed in the following order:

Table 19-27 StopKeyWordWatchlistLoad Batch Details

Sequence	Tasks for StopKeyWordWatchlistLoad Batch	Jobs for StopKeyWordWatchlistLoad Batch	Pipelines for StopKeyWordWatchlistLoad Batch
1	StartBatchStopKeyWord	Not Applicable	Not Applicable
2	LoadStopKeyWordData	Load StopKeyWord Watchlist	StopKeyWordWatchlist
3	EndBatchStopKeyWord	Not Applicable	Not Applicable

Watchlist Batch Details

The application contains certain pre-configured watchlist batches.

The application contains the following pre-configured watchlist batches:

- CustomerFullLoad
- CustomerDeltaLoad
- WLHMTLoad
- WLDJWLoad
- WLDJWDeltaLoad
- WLWCPREMIUMLoad
- WLWCPREMIUMDeltaLoad
- WLWCSTANDARDLoad
- WLWCSTANDARDDeltaLoad
- WLOFACLoad
- WLUNLoad
- WLEULoad
- WLPRIVATELoad

CustomerDeltaLoad Batch Details

The CustomerDeltaLoad batch downloads the Customer data and loads it into a search engine index, using Delta loading.

The following table provides the list of tasks in the CustomerDeltaLoad batch. These tasks must be executed in the following order:

Table 19-28 CustomerDeltaLoad Batch Details

Sequence	Tasks for CustomerDeltaLoad Batch	Jobs for CustomerDeltaLoad Batch	Pipelines for CustomerDeltaLoad Batch
1	StartBatchCustomerDeltaLoad	Not Applicable	Not Applicable
2	CustomerDeltaLoad	Customer Delta Load	Customer Delta Load
3	EndBatchCustomerDeltaLoad	Not Applicable	Not Applicable

> **Note:**
>
> For the CustomerDeltaLoad batch, ensure the ingestion batches have the word 'ingestion' present as part of the batch name. If the batch name is incorrect, the data will not be loaded.

WLHMTLoad Batch Details

The WLHMTLoad Batch downloads the HM Treasury watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the WLHMTLoad batch. These tasks must be executed in the following order:

Table 19-29 WLHMTLoad Batch Details

Sequence	Tasks for WLHMTLoad Batch	Jobs for WLHMTLoad Batch	Pipelines for WLHMTLoad Batch
1	StartBatchWLHMTLoad	Not Applicable	Not Applicable
2	WLHMT Load	WL HMT Load	WL HMT Load
3	EndBatchWLHMTLoad	Not Applicable	Not Applicable

WLDJWLoad Batch Details

The WLDJWLoad batch downloads the Dow Jones watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the WLDJWLoad batch. These tasks must be executed in the following order:

Table 19-30 WLDJWLoad Batch Details

Sequence	Tasks for WLDJWLoad Batch	Jobs for WLDJWLoad Batch	Pipelines for WLDJWLoad Batch
1	StartBatchWLDJWLoad	Not Applicable	Not Applicable
2	WLDJWLoad	WL DJW Load	WL DJW Load
3	EndBatchWLDJWLoad	Not Applicable	Not Applicable

WLDJWDeltaLoad Batch Details

The WLDJWDeltaLoad batch downloads the Dow Jones watchlist data and loads it into a search engine index, using Delta loading.

The following table provides the list of tasks in the WLDJWDeltaLoad batch. These tasks must be executed in the following order:

Table 19-31 WLDJWDeltaLoad Batch Details

Sequence	Tasks for WLDJWDeltaLoad Batch	Jobs for WLDJWDeltaLoad Batch	Pipelines for WLDJWDeltaLoad Batch
1	StartBatchWLDJWDeltaLoad	Not Applicable	Not Applicable

Table 19-31 (Cont.) WLDJWDeltaLoad Batch Details

Sequence	Tasks for WLDJWDeltaLoad Batch	Jobs for WLDJWDeltaLoad Batch	Pipelines for WLDJWDeltaLoad Batch
2	WLDJWDeltaLoad	WL DJW Delta Load	WL DJW Delta Load
3	EndBatchWLDJWDeltaLoad	Not Applicable	Not Applicable

WLWCPREMIUMLoad Batch Details

The WLWCPREMIUMLoad batch downloads the World-Check Premium watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the WLWCPREMIUMLoad batch. These tasks must be executed in the following order:

Table 19-32 WLWCPREMIUMLoad Batch Details

Sequence	Tasks for WLWCPREMIUMLoad Batch	Jobs for WLWCPREMIUMLoad Batch	Pipelines for WLWCPREMIUMLoad Batch
1	StartBatchWLWCPREMIUMLoad	Not Applicable	Not Applicable
2	WLWCPREMIUMLoad	WL WC PREMIUM Load	WL WC PREMIUM Load
3	EndBatchWLWCPREMIUMLoad	Not Applicable	Not Applicable

WLWCPREMIUMDeltaLoad Batch Details

The WLWCPREMIUMDeltaLoad batch downloads the World Check Premium watchlist data and loads it into a search engine index, using Delta loading.

The following table provides the list of tasks in the WLWCPREMIUMDeltaLoad batch. These tasks must be executed in the following order:

Table 19-33 WLWCPREMIUMDeltaLoad Batch Details

Sequence	Tasks for WLWCPREMIUMDeltaLoad Batch	Jobs for WLWCPREMIUMDeltaLoad Batch	Pipelines for WLWCPREMIUMDeltaLoad Batch
1	StartBatchWLWCPREMIUMDeltaLoad	Not Applicable	Not Applicable
2	WLWCPREMIUMDeltaLoad	WL WC PREMIUM Delta Load	WL WC PREMIUM Delta Load
3	EndBatchWLWCPREMIUMDeltaLoad	Not Applicable	Not Applicable

WLWCSTANDARDLoad Batch Details

The WLWCSTANDARDLoad batch downloads the World-Check standard watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the WLWCSTANDARDLoad batch. These tasks must be executed in the following order:

Table 19-34 WLWCSTANDARDLoad Batch Details

Sequence	Tasks for WLWCSTANDARDLoad Batch	Jobs for WLWCSTANDARDLoad Batch	Pipelines for WLWCSTANDARDLoad Batch
1	StartBatchWLWCSTANDARDLoad	Not Applicable	Not Applicable
2	WLWCSTANDARDLoad	WL WC STANDARD Load	WL WC STANDARD Load
3	EndBatchWLWCSTANDARDLoad	Not Applicable	Not Applicable

WLWCSTANDARDDeltaLoad Batch Details

The WLWCSTANDARDDeltaLoad batch downloads the World-Check standard watchlist data and loads it into a search engine index, using Delta load.

The following table provides the list of tasks in the WLWCSTANDARDDeltaLoad batch. These tasks must be executed in the following order:

Table 19-35 WLWCSTANDARDDeltaLoad Batch Details

Sequence	Tasks for WLWCSTANDARDDeltaLoad Batch	Jobs for WLWCSTANDARDDeltaLoad Batch	Pipelines for WLWCSTANDARDDeltaLoad Batch
1	StartBatchWLWCSTANDARDDeltaLoad	Not Applicable	Not Applicable
2	WLWCSTANDARDDeltaLoad	WL WC STANDARD Delta Load	WL WC STANDARD Delta Load
3	EndBatchWLWCSTANDARDDeltaLoad	Not Applicable	Not Applicable

WLOFACLoad Batch Details

The WLOFACLoad batch downloads the Office of Foreign Assets Control (OFAC) watchlist data and loads it into a search engine index, using Delta load.

The following table provides the list of tasks in the WLOFACLoad batch. These tasks must be executed in the following order:

Table 19-36 WLOFACLoad Batch Details

Sequence	Tasks for WLOFACLoad Batch	Jobs for WLOFACLoad Batch	Pipelines for WLOFACLoad Batch
1	StartBatchWLOFACLoad	Not Applicable	Not Applicable
2	WLOFACLoad	WL OFAC Load	WL OFAC Load
3	EndBatchWLOFACLoad	Not Applicable	Not Applicable

WLUNLoad Batch Details

The WLUNLoad batch downloads the United Nations (UN) watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the WLUNLoad batch. These tasks must be executed in the following order:

Table 19-37 WLUNLoad Batch Details

Sequence	Tasks for WLUNLoad Batch	Jobs for WLUNLoad Batch	Pipelines for WLUNLoad Batch
1	StartBatchWLUNLoad	Not Applicable	Not Applicable
2	WLUNLoad	WL UN Load	WL UN Load
3	EndBatchWLUNLoad	Not Applicable	Not Applicable

WLEULoad Batch Details

The WLEULoad batch downloads the European Union (EU) watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the WLEULoad batch. These tasks must be executed in the following order:

Table 19-38 WLEULoad Batch Details

Sequence	Tasks for WLEULoad Batch	Jobs for WLEULoad Batch	Pipelines for WLEULoad Batch
1	StartBatchWLEULoad	Not Applicable	Not Applicable
2	WLEULoad	WL EU Load	WL EU Load
3	EndBatchWLEULoad	Not Applicable	Not Applicable

WLPRIVATELoad Batch Details

The WLPRIVATELoad batch downloads the private watchlist data and loads it into a search engine index.

The following table provides the list of tasks in the WLPRIVATELoad batch. These tasks must be executed in the following order:

Table 19-39 WLPRIVATELoad Batch Details

Sequence	Tasks for WLPRIVATELoad Batch	Jobs for WLPRIVATELoad Batch	Pipelines for WLPRIVATELoad Batch
1	StartBatchWLPRIVATELoad	Not Applicable	Not Applicable
2	WLPRIVATELoad	WL PRIVATE Load	WL PRIVATE Load
3	EndBatchWLPRIVATELoad	Not Applicable	Not Applicable

Screening Batches Details

The application contains certain pre-configured screening batches.

This section provides the tasks required to run the following Screening batches:

- IndividualScreening
- EntityScreening
- Individual314aScreening
- Entity314aScreening
- IndividualDIScreening
- EntityDIScreening
- IndividuDIal314aDIScreening
- Entity314aDIScreening
- ScreeningToCaseManagement

> **Note:**
>
> You can execute multiple screening batches concurrently. For more information, see Parallel Batch Execution.

IndividualScreening Batch Details

The IndividualScreening batch runs the matching rules for individuals and generates the events. This is an out-of the box sample batch. You can create your own batch with specific parameters.

The following table provides the list of tasks in the IndividualScreening batch. These tasks must be executed in the following order:

Table 19-40 IndividualScreening Batch Details

Sequence	Tasks for IndividualScreening Batch	Jobs for IndividualScreening Batch	Pipelines for IndividualScreening Batch
1	StartBatchIndScreening	Not Applicable	Not Applicable
2	IndBatchScreeningTask	IndBatchScreeningJob	IndBatchScreeningJob
3	EndBatchIndScreening	Not Applicable	Not Applicable

EntityScreening Batch Details

The EntityScreening batch runs the matching rules for entities and generates the events. This is an out-of the box sample batch. You can create your own batch with specific parameters.

The following table provides the list of tasks in the EntityScreening batch. These tasks must be executed in the following order:

Table 19-41 EntityScreening Batch Details

Sequence	Tasks for EntityScreening Batch	Jobs for EntityScreening Batch	Pipelines for EntityScreening Batch
1	StartBatchEntScreening	Not Applicable	Not Applicable
2	EntityBatchScreeningTask	EntityBatchScreeningJob	EntityBatchScreeningJob
3	EndBatchEntityScreening	Not Applicable	Not Applicable

Individual314aScreening Batch Details

The Individual314aScreening batch runs the 314a matching rules for individuals and generates the events. This is an out-of the box sample batch. You can create your own batch with specific parameters.

The following table provides the list of tasks in the Individual314aScreening batch. These tasks must be executed in the following order:

Table 19-42 Individual314aScreening Batch Details

Sequence	Tasks for Individual314aScreening Batch	Jobs for Individual314aScreening Batch	Pipelines for Individual314aScreening Batch
1	StartBatchInd314aScreening	Not Applicable	Not Applicable
2	Ind314aBatchScreening Task	Ind314aBatchScreening Job	Individual 314 A Batch Screening
3	EndBatchInd314aScreening	Not Applicable	Not Applicable

Entity314aScreening Batch Details

The Entity314aScreening batch runs the 314a matching rules for entities and generates the events. This is an out-of the box sample batch. You can create your own batch with specific parameters.

The following table provides the list of tasks in the Entity314aScreening batch. These tasks must be executed in the following order:

Table 19-43 Entity314aScreening Batch Details

Sequence	Tasks for Entity314aScreening Batch	Jobs for Entity314aScreening Batch	Pipelines for Entity314aScreening Batch
1	StartBatchEntity314aScreening	Not Applicable	Not Applicable
2	Entity314aBatchScreeningTask	Entity314aScreeningJob	Entity314aScreening
3	EndBatchEntity314aScreening	Not Applicable	Not Applicable

IndividualDIScreening Batch Details

The IndividualDIScreening batch runs the matching rules for individuals and generates the events. This batch is run during Deployment Initation (DI), that is, Day 0 or Initial screening.

The following table provides the list of tasks in the IndividualDIScreeningbatch. These tasks must be executed in the following order:

Note:

ATTENTION: You can slice the customer data and execute the slices instead of executing extensive data. The Data Slicing functionality empowers you to partition the data on the Day 0/Initial screening, facilitating the screening of smaller, more manageable chunks or slices of customer data. Consequently, this reduces resource requirements and the time needed for the screening process. For more information on Slicing Customer data, see the FCCM Cloud Master Data Guide.

Table 19-44 IndividualDIScreeningBatch Details

Sequence	Tasks for IndividualDIScreeningBatch	Jobs for IndividualDIScreeningBatch	Pipelines for IndividualDIScreeningBatch	Comment
1	StartBatchIndDIScreening	Not Applicable	Not Applicable	

Table 19-44 (Cont.) IndividualDIScreeningBatch Details

Sequence	Tasks for IndividualDIScreeningBatch	Jobs for IndividualDIScreeningBatch	Pipelines for IndividualDIScreeningBatch	Comment
2	IndBatchDIScreeningTask	IndBatchScreeningJob	IndBatchScreeningJob	Data Origin ($DATAORIGIN$) and Slice Name ($SLICENAME$) are mandatory parameters.
3	ValidateIndDIBatch	Not Applicable	Not Applicable	• Slice Name ($SLICENAME$) is a mandatory parameter. • You cannot repeat the slice name if a batch is ongoing with the same slice name. The ValidateIndDIBatch task will show an error message if you repeat the slice name in a progressing batch. After the successful execution of the batch, you can use the slice name again.
4	EndBatchIndDIScreening	Not Applicable	Not Applicable	

EntityDIScreening Batch Details

The EntityDIScreening batch runs the matching rules for entities and generates the events. This batch is run during Deployment Initation (DI), that is, Day 0 or Initial screening.

The following table provides the list of tasks in the EntityDIScreeningbatch. These tasks must be executed in the following order:

Note:

ATTENTION: You can slice the customer data and execute the slices instead of executing extensive data. The Data Slicing functionality empowers you to partition the data on the Day 0/Initial screening, facilitating the screening of smaller, more manageable chunks or slices of customer data. Consequently, this reduces resource requirements and the time needed for the screening process. For more information on Slicing Customer data, see the FCCM Cloud Master Data Guide.

Table 19-45 EntityDIScreeningBatch Details

Sequence	Tasks for EntityDIScreeningBatch	Jobs for EntityDIScreeningBatch	Pipelines for EntityDIScreeningBatch	Comment
1	StartBatchEntityDIScreening	Not Applicable	Not Applicable	
2	EntityBatchDIScreeningTask	EntityScreeningJob	EntityScreeningJob	Data Origin ($DATAORIGIN$) and Slice Name ($SLICENAME$) are mandatory parameters.
3	ValidateEntityDIBatch	Not Applicable	Not Applicable	• Slice Name ($SLICENAME$) is a mandatory parameter. • You cannot repeat the slice name if a batch is ongoing with the same slice name. The ValidateEntityDIBatch task will show an error message if you repeat the slice name in a progressing batch. After the successful execution of the batch, you can use the slice name again.

Table 19-45 (Cont.) EntityDIScreeningBatch Details

Sequence	Tasks for EntityDIScreeningBatch	Jobs for EntityDIScreeningBatch	Pipelines for EntityDIScreeningBatch	Comment
4	EndBatchEntityDIScreening	Not Applicable	Not Applicable	

IndividuDIal314aDIScreening Batch Details

The IndividuDIal314aDIScreening batch runs the matching rules for individuals and generates the events. This batch is run during Deployment Initation (DI), that is, Day 0 or Initial screening.

The following table provides the list of tasks in the IndividuDIal314aDIScreeningbatch. These tasks must be executed in the following order:

> **Note:**
>
> **ATTENTION:** You can slice the customer data and execute the slices instead of executing extensive data. The Data Slicing functionality empowers you to partition the data on the Day 0/Initial screening, facilitating the screening of smaller, more manageable chunks or slices of customer data. Consequently, this reduces resource requirements and the time needed for the screening process. For more information on Slicing Customer data, see the FCCM Cloud Master Data Guide.

Table 19-46 IndividuDIal314aDIScreeningBatch Details

Sequence	Tasks for IndividuDIal314aDIScreeningBatch	Jobs for IndividuDIal314aDIScreeningBatch	Pipelines for IndividuDIal314aDIScreeningBatch	Comment
1	StartBatchInd314aDIScreening	Not Applicable	Not Applicable	
2	Ind314aDIBatchScreeningTask	Ind314aBatchScreeningJob	Individual 314 A Batch Screening	Data Origin ($DATAORIGIN$) and Slice Name ($SLICENAME$) are mandatory parameters.

Table 19-46 (Cont.) IndividuDIal314aDIScreeningBatch Details

Sequence	Tasks for IndividuDIal314aDIScreeningBatch	Jobs for IndividuDIal314aDIScreeningBatch	Pipelines for IndividuDIal314aDIScreeningBatch	Comment
3	ValidateInd314aDIBatch	Not Applicable	Not Applicable	• Slice Name ($SLICENAME$) is a mandatory parameter. • You cannot repeat the slice name if a batch is ongoing with the same slice name. The ValidateInd314aDIBatch task will show an error message if you repeat the slice name in a progressing batch. After the successful execution of the batch, you can use the slice name again.
4	EndBatchInd314aDIScreening	Not Applicable	Not Applicable	

Entity314aDIScreening Batch Details

The Entity314aDIScreening batch runs the matching rules for individuals and generates the events. This batch is run during Deployment Initation (DI), that is, Day 0 or Initial screening.

The following table provides the list of tasks in the Entity314aDIScreeningbatch. These tasks must be executed in the following order:

> **Note:**
>
> **ATTENTION:** You can slice the customer data and execute the slices instead of executing extensive data. The Data Slicing functionality empowers you to partition the data on the Day 0/Initial screening, facilitating the screening of smaller, more manageable chunks or slices of customer data. Consequently, this reduces resource requirements and the time needed for the screening process. For more information on Slicing Customer data, see the FCCM Cloud Master Data Guide.

Table 19-47 Entity314aDIScreeningBatch Details

Sequence	Tasks for Entity314aDIScreeningBatch	Jobs for Entity314aDIScreeningBatch	Pipelines for Entity314aDIScreeningBatch	Comment
1	StartBatchEntity314aDIScreening	Not Applicable	Not Applicable	
2	Entity314aDIBatchScreeningTask	Entity314aScreeningJob	Entity314aScreening	Data Origin ($DATAORIGIN$) and Slice Name ($SLICENAME$) are mandatory parameters.
3	Validate314aEntityBatch	Not Applicable	Not Applicable	• Slice Name ($SLICENAME$) is a mandatory parameter. • You cannot repeat the slice name if a batch is ongoing with the same slice name. The Validate314aEntity task will show an error message if you repeat the slice name in a progressing batch. After the successful execution of the batch, you can use the slice name again.
4	EndBatchEntity314aDIScreening	Not Applicable	Not Applicable	

ScreeningToCaseManagement Batch Details

The ScreeningToCaseManagement batch creates cases for the alerts.

The following table provides the list of tasks in the ScreeningToCaseManagement batch. These tasks must be executed in the following order:

Table 19-48 ScreeningToCaseManagement Batch Details

Sequence	Tasks for ScreeningToCaseManagement Batch	Jobs for ScreeningToCaseManagement Batch	Pipelines for ScreeningToCaseManagement Batch
1	ECMStartBatch	Not Applicable	Not Applicable

Table 19-48 (Cont.) ScreeningToCaseManagement Batch Details

Sequence	Tasks for ScreeningToCaseManagement Batch	Jobs for ScreeningToCaseManagement Batch	Pipelines for ScreeningToCaseManagement Batch
2	CASEGEN	Not Applicable	Not Applicable
3	CASELOAD	Load Case Data	Load Case Data
4	CustomerEventEntityMap	Loading Screening Customer Event Entity Map	Loading Screening Customer Event Entity Map
5	ECMEndBatch	Not Applicable	Not Applicable
6	EVCORR	Not Applicable	Not Applicable
7	LoadingScreeningCustomersEvented	Loading Screening Customers Evented	Loading Screening Customers Evented
8	LoadingScreeningData	Loading Screening Data	Loading Screening Data
9	LoadingScreeningEvents	Loading Screening Events	Loading Screening Events
10	LoadingScreeningMatchedWatchlist	Loading Screening Matched Watchlist	Loading Screening Matched Watchlist
11	LoadingScreeningMatches	Loading Screening Matches	Loading Screening Matches
12	LoadingScreeningWatchlistEventEntityMap	Loading Screening Watchlist Event Entity Map	Loading Screening Watchlist Event Entity Map
13	LoadingscreeningWatchlistMap	Loading Screening Watchlist Map	Loading S14creening Watchlist Map
14	LoadingScreeningAEDecision	LoadingScreeningAEDecision	Loading Screening AE Decision
15	PRECSUPDT	Not Applicable	Not Applicable
16	PipelineEnd	Not Applicable	Not Applicable
17	PipelineStart	Not Applicable	Not Applicable
18	SCORING	SCREENINGSCORING	SCREENINGSCORING

Note:

After importing the latest OOB pipelines, you must refresh the existing copied ScreeningToCaseManagement batch with the latest version.

Purge Batch Details

Purge batches are used when your batch has not executed successfully to purge the data and execute the batch again.

If your batch has not executed successfully, has been explicitly interrupted or cancelled, or was put on hold during the execution process, first try to restart the batch following the steps in Restart a Batch/Batch Group If this is not successful, then you can purge the data and execute the batch again.

> **Note:**
>
> Purge batches are not a regular required activity. They should only be used when other methods to re-run the batches are not successful.

To purge the data which was partially processed during the interrupted or canceled batch execution, follow these steps:

- If the AMLDataLoad batch fails to execute, follow these steps:
  1. Run the PurgeStagingTables batch for the batch date and data origin on which the batch failed.
  2. Execute the AMLDataLoad batch for the batch date.
- If the Ingestion batch fails, follow these steps:
  1. Run the PurgeAMTables batch by providing the failed batchrunID as input parameter in the field $FCCBATCHRUNID$.
  2. Execute the Ingestion batch for the batch date.
- If any Case Management batch fails to execute, follow these steps:
  1. Run the PurgeCMTables batch by providing the failed batchrunID as input parameter in the field $FCCBATCHRUNID$.
  2. Execute the Case Management batch for the batch date.
- If the AMLToCMEventData batch fails to execute, follow these steps:
  1. Run the PurgeAMLToCMEventData batch by providing the failed batchrunID as input parameter in the field $FCCBATCHRUNID$.
  2. Execute the Curated CM batch for the batch date.
- If the KYC batch fails to execute, follow these steps:
  1. Run the PurgeKYCTables batch by providing the failed batchrunID as input parameter in the field $FCCBATCHRUNID$.
  2. Execute the KYC batch for the batch date.
- If the KYC DeploymentInitiation batch fails to execute, follow these steps:
  1. Run the PurgeKYCTables batch by providing the failed batchrunID as input parameter in the field $FCCBATCHRUNID$.
  2. Run the PurgeCustomerSlicing batch by providing the failed SliceName as input parameter in the field $SLICENAME$ and AppID as input in the field $APPID$.
- If the CS batch fails to execute, follow these steps:
  1. Run the PurgeCSTables batch by providing the failed batchrunID as input parameter in the field $FCCBATCHRUNID$.
  2. Execute the CS batch for the batch date.

> **Note:**
>
> - After executing the purge batch, the metering records for that run will get deleted. To get the updated data for the metering in the Dashboard UI, you must run AMLMetrics from the Scheduler screen. Otherwise, you must wait until the next day for the latest data to reflect in the UI.
> - If you are purging a DI batch, you must enter the exact slice name label used in the failed DI batch as the slice name ($SLICENAME$) parameter in the PurgeCSTables batch.

- If the CMIngestion batch fails to execute, follow these steps:
  1. Run the PurgeCMIngestion batch by providing the failed batchrunID as input parameter in the field $FCCBATCHRUNID$.
  2. Execute the CMIngestion batch for the batch date.

> **Note:**
>
> - The batch should not be executed for any past dates, but only for the batch date on which the batch failed.
> - Purge Batches should be run in the reverse order of batch execution. For example, if batches are run in the order of Ingestion > TMScenario > CMIngestion and AMLtoCaseManagement, then the purge batch order should be: AMLtoCaseManagement > CMIngestion > TMScenario > Ingestion.

Maintenance Batch Details

The Maintenance batch configures and creates table partitions for Common Staging Area and Transaction Monitoring business tables. This batch is run to enhance performance and maintainability.

This batch is run to enhance performance, maintainability and to support archival/ retention (planned for future release) implementation.

Partitions are created on the FIC_MIS_DATE and DATA ORIGIN parameters where applicable. You must provide the Data Origination input. The FIC_MIS_DATE partition will be created automatically by the application.

Note:

- The Maintenance batch creates the partition on FIC_MIS_DATE and DATA ORIGIN (wherever applicable). Oracle will internally handle auto-partition creation on FIC_MIS_DATE. You only need to provide Data Origin as an input parameter.
- This out of box batch should only be used during the Maintenance window and should not be copied or customized.
- Execution of this batch is mandatory before any other batches are executed.
- Skipping this Maintenance batch may impact performance and batch execution.

To run the Maintenance batch in an existing or upgrading implementation, you must provide a downtime maintenance window and run the Maintenance batch so that historical business and staging data is partitioned. To add a new data origin at another time, run the Maintenance batch in the downtime maintenance window, giving the new data origin as the input parameter.

New implementations should run the Maintenance batch after installation with the respective data origin as input to create partitions. To add a new data origin at another time, run the Maintenance batch in the downtime maintenance window, giving the new data origin as the input parameter.

The following table provides the list of tasks in the Maintenance batch. These tasks must be executed in the following order:

Table 19-49 Maintenance Batch Details

Sequence	Tasks for Maintenance Batch	Jobs for Maintenance Batch	Pipelines for Maintenance Batch
1	StartBatch	Not Applicable	Not Applicable
2	Partition_Maintenance	Partition Maintenance	Partition Maintenance
3	EndBatch	Not Applicable	Not Applicable

AMLRedaction Batch Details

The AMLRedaction batch redacts Personal Identifying Information (PII) in order to comply with General Data Protection Regulation (GDPR) regulations.

When this batch is run, PII will display in AML cases as XXXX. See Access Case Details for more information about which fields are redacted.

To provide users access to view these fields, you must map the user role to the Unredacted data function code in the Admin Console. For more information about how to map user roles, see Mapped Roles.

Right to Forget (FCCRTFDataLoadUtility) Batch Details

The FCCRTFDataLoadUtility batch redacts Personal Identifying Information (PII) in order to comply with General Data Protection Regulation (GDPR) regulations.

When this batch is run, PII for Customers listed in the FCC_RTF_SQL_QUERY table will be redacted in the UI.

> **Note:**
>
> Before executing this batch, you must update the FCC_RTF_SQL_QUERY table to provide the Customer Internal ID and other relevant details for the customers who require redaction in the correct format. Follow the steps in Executing the FCCRTFDataLoadUtility Batch before executing this batch.

The following table provides the list of tasks in the FCCRTFDataLoadUtility batch. These tasks must be executed in the following order:

Table 19-50 FCCRTFDataLoadUtility Batch Details

Sequence	Tasks for FCCRTFDataLoadUtility Batch
1	StartDataLoad
2	DataLoadingFileTransfer
3	DataLoadingFileScanner
5	FCCRTFSQLQueryDataLoad
6	RightToForgetUtility
7	GatherStats
8	EndDataLoad

Executing the FCCRTFDataLoadUtility Batch

Before executing the FCCRTFDataLoadUtility batch, certain steps are required to prepare the Customer data for redaction of Personal Identifying Information (PII).

Before executing the FCCRTFDataLoadUtility batch, certain steps are required to prepare the Customer data for redaction of Personal Identifying Information (PII).

1. Before executing the FCCRTFDataLoadUtility batch, you must update the FCC_RTF_SQL_QUERY table to provide the Customer Internal ID and other relevant details for the customers who require redaction in the correct format.

   Information on how this data should be provided can be found in the FCC_RTF_SQL_QUERY table at Sample Templates for Data Loading.

   > **Note:**
   >
   > The CSV file should follow proper naming conventions. For example, 20231129_FCC_RTF_SQL_QUERY_TAB.csv

2. Upload the FCC_RTF_SQL_QUERY.csv file you have created into Object Storage using the steps found in Uploading Data into Object Storage.
3. Execute the FCCRTFDataLoadUtility batch.
   a. In **$DATAORIGIN$**, enter the Data Origin provided in the FCC_RTF_SQL_QUERY.csv file you uploaded into Object Storage

b. In **$BATCHDATE$**, select the MISDATE associated with the FCC_RTF_SQL_QUERY.csv file you uploaded into Object Storage.

Creating and Configuring New Batches

You must create new batches to run customer-specific data.

To create and configure a new batch, follow these steps.

1. Navigate to the **Scheduler Service** page.
2. Define a batch. This option enables you to create a new batch. For more information, see Defining Batches.
3. Define a task. This option enables you to add new tasks to the selected batch definition. For information on configuring tasks for batches, see Defining Tasks.
4. Schedule a batch. This option enables you to run a batch. For more information, see Scheduling and Automating Batch/Batch Group Execution.
5. Monitor a batch. This option enables you to view the status of the executed Batch along with the details of the task. For more information, see Monitor Batches.

Defining Batches

To define batches, you must configure the batches.

The following table lists the fields which should be configured.

Table 19-51 Defining Batches

Field Name	Description	Batches for Data Redaction	Batches for Data Pipeline	Batches for Scenario Pipeline	Batches for Case Management
Batch Name	Indicates the batch name.	Configure	Configure	Configure	Configure
Batch Description	Indicates the batch description.	Configure	Configure	Configure	Configure
Service URL Name	Indicates the Service URL name.	Configure	Configure	Configure	Configure
Service URL	Indicates the Service URL.	Configure	Configure	Configure	Configure

> **Note:**
>
> You cannot run both a data pipeline and scenario pipeline in the same batch.

The following table lists the parameter details which should be configured.

Table 19-52 Parameter Details for Defining Batches

Parameter Name	Description	Batches for Data Redaction	Batches for Data Pipeline	Batches for Scenario Pipeline	Batches for Case Management
$LOADRUNID$	Indicates the load run ID.	N/A	Configure	N/A	N/A
$GROUPNAME$	Indicates the group name.	Configure	Configure	Configure	N/A
$DATAORIGIN$	Indicates the type of the source of the data.	Configure	Configure	Configure	Pre-Configured
$RUNTYPE$	Indicates the run type.	N/A	N/A	Configure	N/A
$FICMISDATE$	Indicates the date on which you want to run the batch.	Configure	Pre-Configured	Pre-Configured	Pre-Configured
$BATCHTYPE$	Indicates the type of pipeline to run as part of this batch.	Configure	Configure	Configure	Pre-Configured
$PREVMISDATE$	Indicates the date previous to the FICMISDATE	N/A	Configure	Configure	N/A
$BATCHRUNID$	Indicates the batch run ID.	Configure	Pre-Configured	Pre-Configured	Pre-Configured

Defining Tasks for Batches

To define tasks, you must configure the batches.

The following table lists the tasks which should be configured.

Table 19-53 Task Details for Defining Batches

Field Name	Description	StartBatch Task	EndBatch Task	Other Task
Task Name	Indicates the task name.	Configure	Configure	Configure
Task Description	Indicates the task description.	Configure	Configure	Configure
Task Type	Indicates the task type.	Pre-Configured	Pre-Configured	Pre-Configured
Batch Service URL	Indicates the batch service URL.	Pre-Configured	Pre-Configured	Pre-Configured
Task Service URL	Indicates the task service URL.	Configure as / StartBatch	Configure as / EndBatch	Configure as / ExecutePipeline

The following table lists the parameter which should be configured.

Table 19-54 Parameter Details for Defining Tasks

Parameter Name	Parameter Value
$GROUPNAME$	This value is obtained from the Batch Configuration.
$DATAORIGIN$	This value is obtained from the Batch Configuration.
$FICMISDATE$	This value is obtained from the Batch Configuration.
$BATCHTYPE$	This value is obtained from the Batch Configuration.
$PREVMISDATE$	This value is obtained from the Batch Configuration.
$BATCHRUNID$	This value is obtained from the Batch Configuration.
$JOBNAME$	You must add this parameter and mention the corresponding job name that you want to execute as part of this task.
component	This is applicable only for the ECM start batch task. For more information, see Starting the AMLtoCaseManagement Batch.
dataorigin	This is applicable only for the ECM start batch task. For more information, see Starting the AMLtoCaseManagement Batch.
sourcebatch	This is applicable only for the ECM start batch task. For more information, see Starting the AMLtoCaseManagement Batch.
currentbatch	This is applicable only for the ECM start batch task. For more information, see Starting the AMLtoCaseManagement Batch.

Viewing Batch Logs

Log files are generated when some services are executed as batches. You can view these log files in the View Logger.

Log files are generated when the following services are executed as batches.

- AMLDataLoad
- Ingestion
- TMScenario

You can view these log files in the View Logger.

1. In the Monitor Batch page, select one of the following batches from the **Select Batch** drop-down list
    - AMLDataLoad
    - Ingestion
    - TMScenario

2. Select the Run ID for the batch you want to view log files for from the **Run ID** drop-down list. The Batch Details display.
3. In the List View tab, click **View Logger** for the task you want to view the log files for. The View Logger window opens and displays the log for this task.

   You can download the log file by clicking **Download**.

Parallel Execution of CS Batches

You can execute multiple screening batches concurrently without waiting to complete the previous batch.

Parallel Execution of Customer Screening Batches supports the following cases of batch run:

- **Multiple Data Origins in a parallel batch run.** You can execute multiple screening batches concurrently if the screening batches have different Data Origin value. You must add $DATA_ORIGIN$ as the task parameter for the screening batch for the parallel execution.

  > **Note:**
  >
  > Data Origin is a mandatory field and Jurisdictions is an optional field.

- **Single Data Origin with Multiple Jurisdictions in a single batch**. You can execute screening batches concurrently if the screening batch have the same Data Origin and different Jurisdictions. You must add $JURISDICTION$ as the task parameter for the screening batch for the parallel execution.

  > **Note:**
  >
  > - Data Origin is a mandatory field and Jurisdictions is an optional field.
  > - If you have multiple tasks of different jurisdictions in the same screening batch do not point to the same pipeline.

20
Common Tasks

Certain tasks may apply to many different pipeline types.

This section tells how to perform the following common tasks:

Configuring Filters

You can configure a filter by defining various filter conditions.

1. Navigate to the Output pane.
2. Click **Add** corresponding to the Output pane to open the filter group. The filter group opens where you can add filter conditions.
3. Click **Add** in the Output pane to create a filter condition. The filter condition is displayed.
4. Define the filter condition. You can define the filter conditions using one of the following:
   - Expression Builder: You can form filter conditions using all the operators given in the Expression Builder. The Expression Builder is used to define free flow text filter conditions. To define a filter condition using the Expression Builder, follow these steps:
     a. Click **Exp**. The Expression Builder dialog box is displayed.
     b. Select the required Dataset, Attribute and Runtime Parameters and operators. The resulting condition is displayed in the Condition field.
     c. Click **Save** to save the changes.
   - Tables: You can define filter conditions using the various columns of tables. The columns of the two tables are compared with each other using the required operators. To define filter condition using tables, follow these steps:
     a. Click **Tables**.
     b. Select the dataset or risk indicator and column on the left-hand side and right-hand side, and then select the operator.
   - Text: You can define filter conditions using text. A particular column in a table is compared with the input text using the required operators. To define filter conditions using text, follow these steps:
     a. Click **Text**.
     b. Select a dataset and column on the left-hand side, operator, and then enter the text in the field on the right-hand side.

c. Click **Save** to save the changes.

Creating Runtime Parameters

A Runtime parameter is a variable whose value can be defined and then called from within that same pipeline.

When you define a runtime parameter, you enter the default value to use. When you create or edit a job that includes a pipeline with runtime parameters, you can specify another value to override the default.
To create a runtime parameter, follow these steps:

1. Configure a filter using the steps in Configuring Filters.
2. Define the filter condition using Expression Builder.
3. Click **Add**. The New Runtime Parameter dialog box is displayed.
4. Provide the details as described in the following table:

Table 20-1 Fields in New Runtime Parameter and their Descriptions

Field	Description
Name	Enter the name for the runtime parameter.
Datatype	Enter the datatype for the runtime parameter.
Description	Enter the description for the runtime parameter.
Default Values	Provide the default values for the runtime parameter.

5. Click **OK**.The runtime parameter is created.

Editing Widget

You can modify the settings for widgets associated with pipelines.

1. Navigate to the Pipeline Designer page.
2. Select the widget that you want to modify.
3. Hover on the widget and click **Edit** ✎. A dialog box is displayed.
4. Modify the required details.
5. Click **Save** ✓to save the changes. The widget details are modified.

Deleting Widget

You can delete widgets from pipelines.

To delete a widget, follow these steps:

1. Navigate to the Pipeline Designer page.

2. Select the widget that you want to delete.
3. Hover on the widget and click **Delete** 🗑.The Pipeline Delete dialog box is displayed.
4. Click **Confirm**. The widget is deleted.

About Audit History

The Audit History displays all changes made to pipelines or threshold configuration.

This allows you to view the changes made to a scenario before approving or rejecting the updates, and to detect and mitigate the risk of internal employee manipulation, as required by auditors and regulators. You can also filter the results to show updates made to a specific pipeline or scenario since the last tuning cycle or last regulatory exam. If needed, you can export the data in .csv format to analyze further.

Accessing Audit History

You can access the Audit History from the Navigation List.

1. In the Applications landing page, click the **Navigation Menu** ☰ to access the Navigation List. The Navigation List displays the list of modules.
2. Select **Audit History**. The Audit History page displays.

   The following table describes the columns which display in the Audit History.

Table 20-2 Columns in the Audit History

Column	Description
Component	Type of component the action was taken on. For example, Scenario Pipeline or Threshold.
Component Name	Name of the threshold or pipeline the action was taken on. For example, if you are viewing the Audit History for a scenario pipeline, the scenario name will display.
Sub Component	Type of sub component the action was taken on. For example, High Level Dataset, Evaluation, Risk Indicator and so on. If there is no sub component, this column will appear blank.
Sub Component Name	Name of the sub component the action was taken on. For example, if a scenario Risk Indicator was updated, the name of the Risk Indicator will display, such as *Total of Very High Risk Amount Percentage*.If there is no sub component, this column will appear blank.

Table 20-2 (Cont.) Columns in the Audit History

Column	Description
Action	Action that was taken. For example, Changing a pipeline name, adding or modifying widgets in the pipeline, creating or deleting a threshold set, changing threshold set configurations and so on. **Note:** • When a parameter is deleted, the Action column displays *Delete*. • When a widget or pipeline is deleted at the parent level without deleting its underlying parameters, the Action column displays *Bulk Delete*.
Current State	The current state of the component which was acted upon. Compare the Current State with the Previous State to see the change which was made.
Previous State	The previous state of the component which was acted upon. Compare the Current State with the Previous State to see the change which was made.
Updated By	User who took the action.
Date & Time	Date and Time the action was taken.

>

Filtering Audit History

The Filter option allows you to search and narrow down the results of the Audit History.

You can use a combination of these search criteria to quickly find the components you are interested in. If you don’t enter any value in any search field, it is equivalent to selecting all the criteria.
To filter the Audit History, follow these steps:

1. n the Audit History page, click **Filter** . The Filter criteria appear on the left-hand-side pane.
2. Select one or more criteria. You can filter by the following criteria:
   - Updated by
   - Action
   - Component
   - Component Name
   - From Date

- To Date