Oracle Financial Services Know Your Customer **Administration Guide**

Release 8.0.4.0.1
March 2017

ORACLE
FINANCIAL SERVICES

ORACLE

Oracle Financial Services Know Your Customer **Administration Guide**

Release 8.0.4.0.1
March 2017

Part Number: E85983-02

Oracle Financial Services Software, Inc.
1900 Oracle Way
Reston, VA 20190

Part Number: E85983-02
Second Edition (March 2017)

Trademarks
Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

Oracle Financial Services Software, Inc.
1900 Oracle Way
Reston, VA 20190
Phone: (703) 478-9000
Fax: (703) 318-6340
Internet: www.oracle.com/financialservices

Revision History

The following table describes the revision history of the Administration Guide.

Date	Edition	Description
May 2017	First edition of 8.0.4.1	Created the KYC Admin Guide.

Contents

List of Figures

List of Tables

About this Guide

This guide explains the concepts behind the Oracle Financial Services Know Your Customer (OFS KYC) application and provides comprehensive instructions for proper system administration, as well as daily operations and maintenance. This section focuses on the following topics:

Who Should Use this Guide

This *Administration Guide* is designed for use by the Administrators and Implementation consultants. Their roles and responsibilities, as they operate within OFS KYC, include the following:

- **Implementation Consultants:** Installs and configures OFS BD at a specific deployment site. The consultant also installs and upgrades any additional Oracle Financial Services solution sets, and requires access to deployment-specific configuration information. For example, machine names and port numbers.
- **System Administrator:** Configures, maintains, and adjusts the system. The System Administrator maintains user accounts and roles, monitors data management, archives data, loads data feeds, and performs post-processing tasks. In addition, the System Administrator can reload cache.

Scope of this Guide

This guide describes the physical and logical architecture of OFS KYC. It also provides instructions for maintaining and configuring OFS KYC, its subsystem components, and any third-party software required for operation.

OFS KYC provides an open and scalable infrastructure that supports rich, end-to-end functionality across all Oracle Financial Services solution sets. OFS KYC's extensible, modular architecture enables a customer to deploy new solution sets readily as the need arises.

How this Guide is Organized

The *Administration Guide* includes the following chapters:

- *About Oracle Financial Services Know Your Customer (KYC)* provides a brief overview of the Oracle Financial Services Know Your Customer and its components.
- *Managing User Administration and Security Configuration* covers the required day-to-day operations and maintenance of OFS KYC users, groups, and organizational units.
- *Maintenance Activities and Configuring Setup Parameters* describes how to configure the KYC application.
- *Managing KYC Batches* describes how to execute KYC batches.
- *Setting up Questionnaires for KYC* provides information on Questionnaires.
- The *Index* provides an alphabetized cross-reference list that helps you locate information quickly.

Where to Find More Information

For more information about OFS KYC, refer the following documents:

- *KYC Risk Assessment Guide*
- *KYC Service Guide*
- *Behavior Detection (BD) Installation Guide (IG)*
- *Behavior Detection (BD) Configuration Guide (CG)*

These documents can be found at the following OHC documentation library:
http://docs.oracle.com/cd/E60570_01/homepage.htm
You can find additional information in the following link:
http://docs.oracle.com/cd/E60058_01/homepage.htm:

- *Oracle Financial Services Analytical Applications Infrastructure (OFS AAI) User Guide*
- *Oracle Financial Services Analytical Applications Infrastructure (OFS AAI) Security Guide*

For installation and configuration information about Sun Java System, BEA, and Apache software, refer to the appropriate documentation that is available on the associated web sites.

Conventions Used in this Guide

This table lists the conventions used in this guide and their associated meanings.

Table 1. Conventions Used in this Guide

Convention	Meaning
Italics	• Names of books, chapters, and sections as references • Emphasis
Bold	• Object of an action (menu names, field names, options, button names) in a step-by-step procedure • Commands typed at a prompt • User input
`Monospace`	• Directories and subdirectories • File names and extensions • Process names • Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text
<Variable>	• Substitute input value

Abbreviations Used in this Guide

This table lists the abbreviations used in this guide and their associated descriptions.

Table 2. Abbreviations Used in this Guide

Abbreviation	Description
AML	Anti-Money Laundering
T2T	Table to Table
AAI	Analytical Applications Infrastructure
OFS	Oracle Financial Services

CHAPTER 1

About Oracle Financial Services Know Your Customer (KYC)

This chapter provides a brief overview of the Oracle Financial Services Know Your Customer (KYC) in terms of its architecture and operations.

This chapter focuses on the following topics:

KYC Overview

KYC assesses the risk a customer poses to the bank or financial institution. It is not a one-time assessment, but is a continuous process of assessing customers. Customers are assessed in different stages of their relationship with the bank. The different stages of the relationship are described in the following sections:

- Deployment Initiation
- Real Time Account on Boarding
- Account on Boarding or Default Review
- Re-review

The Oracle KYC risk assessment application is built using the OFS AAI framework. The application functions are divided into the following areas:

- Reference Data Management (Internal and External)
- On-line interface with account opening system
- Risk Assessment Engine
- Interface with Third Party Services
- System Maintenance

KYC Workflow

The following figure shows the workflow for existing customers:

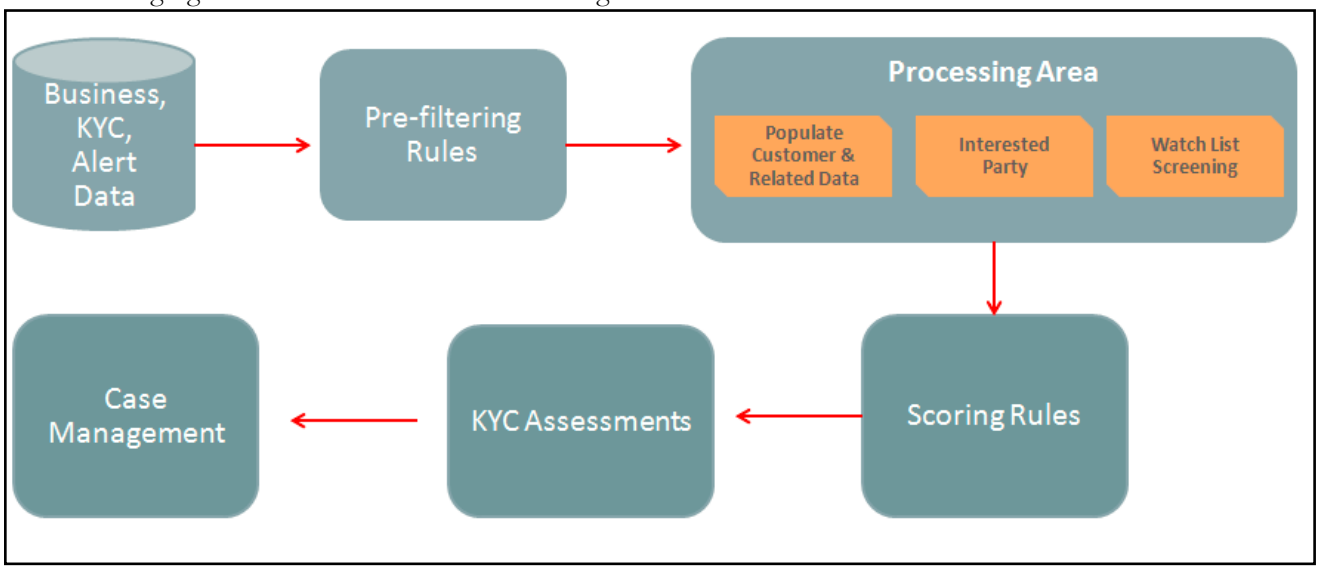


Figure 1. KYC Process Flow for Existing Customers

The following section describes the process flow:

1. Customer data is moved from the data warehouse to the processing area using BDF or T2T. This data can be account data, information related to alerts, or information specific to KYC cases.
2. All data is not moved to the processing area. It is moved using certain prefiltering rules, such as accelerated rereviews, periodic reviews, and account onboarding.
3. The processing area contains data of all customers for whom the prefiltering rules apply and for whom risk scoring needs to be done.
4. The prefiltered customers are scored using two risk assessments to get the risk score on the customer attributes: Algorithm-based risk assessments and Rule-based risk assessments. The risk score is the maximum of the Algorithm-based risk score and Rule-based risk score.
5. A risk assessment record is created for each customer who is scored. The risk assessment contains data such as the risk score, risk assessment history, and customer review details. Based on the risk score, the risk assessment can either be closed or promoted to a case.
6. A risk assessment is promoted to a case under the following conditions:

- The customer effective risk score, or the risk score, is beyond the threshold defined for due diligence.
- The watch list score of a customer is beyond the limit defined.
- The customer matches a rule defined for Rule-based risk assessments irrespective of the risk score.

CHAPTER 2

Managing User Administration and Security Configuration

This chapter provides instructions for setting up and configuring the Know Your Customer (KYC) application.

This chapter focuses on the following topics:

About User Administration

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

- Administrator permissions
- Creating and mapping users and user groups
- Loading and mapping security attributes

User Provisioning Process Flow

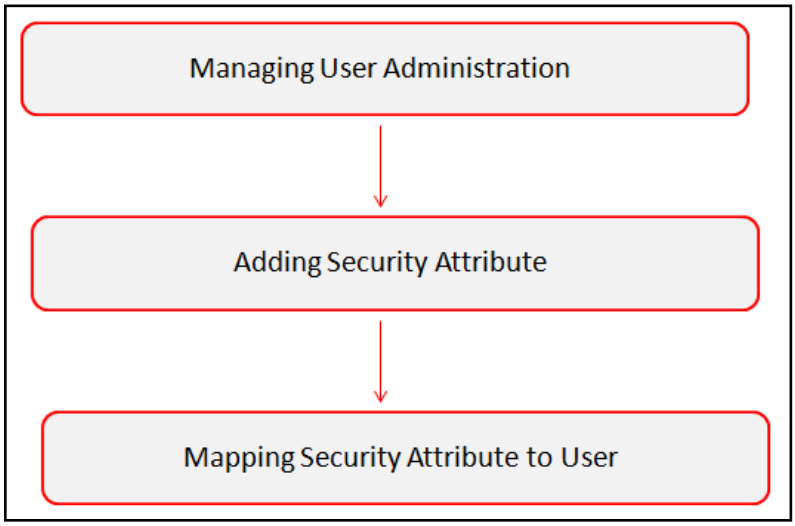


Figure 2. User Provisioning Process Flow

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

Table 3. User Provisioning Process Flow

Action	Description
Managing User Administration	Create users and map users to user groups. This allows Administrators to provide access, monitor, and administer users.
Adding Security Attributes	Load security attributes. Security attributes are loaded using either Excel or SQL scripts.
Mapping Security Attributes to Users	Map security attributes to users. This is done to determine which security attributes control the user's access rights.

Managing User Administration

This section allows you to create, map, and authorize users defining a security framework which has the ability to restrict access to the KYC application.

Managing Identity and Authorization

This section explains how to create a user and provide access to the KYC application.

This section covers the following topics:

- Managing Identity and Authorization Process Flow
- Creating and Authorizing a User
- Mapping a User with a User Group

Managing Identity and Authorization Process Flow

The following figure shows the process flow of identify management and authorization:

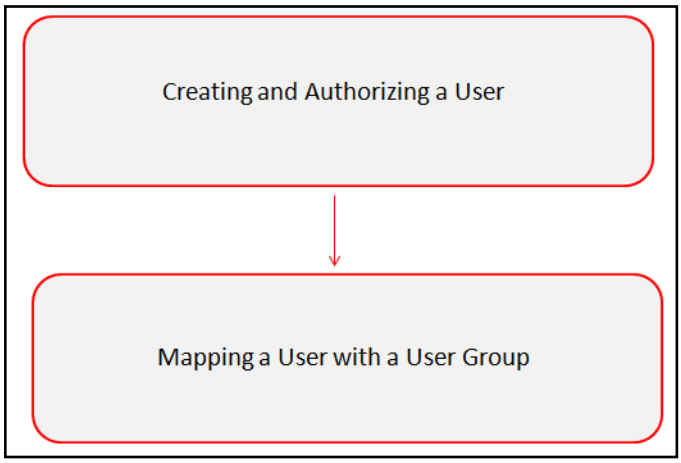


Figure 3. Managing Identity and Authorization Process Flow

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

Table 4. Administration Process Flow

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

Creating and Authorizing a User

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

Mapping a User with a User Group

This section explains how to map Users and User Groups. With this, the user has access to the privileges as per the role. The sysadm user maps a user to a user group in the KYC application.The following table describes the predefined KYC User Roles and corresponding User Groups.

Table 5. KYC Roles and User Groups

Role	Privileges
KYC Admin	• Manage the Risk Rating Parameters • Manage the KYC Installation Parameters • Manage the KYC Application Parameters • Upload the Risk Parameter Data using Excel • Perform the Rule-based Risk Assessment • Perform the Algorithm-based Risk Assessment • Perform the Real Time Account On-Boarding Risk Assessment • Perform the Accelerated Rereview • Update the Accelerated Rereview Rules • Update the Risk Assessment Category • Update the Real Time Account On-Boarding Risk Assessment Category • Update the Risk Assessment Case Priority • Update the Account Customer Role • Update the Company Type Risk Value • Update the Corporation Age Range Risk Value • Update the Country Risk Value • Update the Industry Risk Value • Update the Income Source Type Risk Value • Update the Legal Structure and Ownership Risk Value • Update the Markets Served Risk Value • Update the Negative News Range Risk Value • Update the Occupation Range Risk Value • Update the Products Offered Risk Value • Update the Relationship Period Risk Value • Search and View the List of Rules • Copy the values from one jurisdiction to other • View the Risk Rating Model • Search and View the Model, Rule-based, or RAOR-based risk parameters • Edit the weights of the parameters • Copy the values from one jurisdiction to other • Edit the values of the individual parameters

Table 5. KYC Roles and User Groups

Role	Privileges
KYC Supervisor	• View the KYC Cases • Perform the Rule-based Risk Assessment • Perform the Algorithm-based Risk Assessment • Perform the Real Time Account On-Boarding Risk Assessment • Update the Accelerated Rereview Rules • Update the Risk Assessment Category • Update the Real Time Account On-Boarding Risk Assessment Category • Update the Risk Assessment Case Priority • Update the Account Customer Role • Update the Company Type Risk Value • Update the Corporation Age Range Risk Value • Update the Country Risk Value • Update the Industry Risk Value • Update the Income Source Type Risk Value • Update the Legal Structure and Ownership Risk Value • Update the Markets Served Risk Value • Update the Negative News Range Risk Value • Update the Occupation Range Risk Value • Update the Products Offered Risk Value • Update the Relationship Period Risk Value • View the Related Risk Assessments • Update the Accelerated Review Rules • Search and View the List of Rules • Update the Risk Rating Model • Search and View the Model, Rule-based, or RAOR-based risk parameters • Update the Risk Value
KYC Relationship Manager	• Update the KYC Assessments • Search for Risk Assessments • View the List of Risk Assessment • Verify or Update the Customer Details
KYC Analyst	• View the KYC Cases • View the Third Party Verification tab • Verify the Third Party Results • View the Risk Information Tab • View the Related Risk Assessments

Adding Security Attributes

This section explains about security attributes, the process of uploading security attributes, and mapping security attributes to users in the KYC application.

This section covers the following topics:

About Security Attributes

Security Attributes are those attributes which help an organization classify their users based on their geographical location, jurisdiction, and business domain in order to restrict access to the data that they can view.

You must first provide the user with access privileges, so the user can perform activities throughout various functional areas in the KYC application.

Types of Security Attributes

The following are the security attributes:

- Jurisdiction
- Business Domain
- Scenario Group
- Case Type
- Organization

Jurisdiction

KYC applications use Jurisdictions to limit user access to data in the database. Records from the Oracle client that the Ingestion Manager loads must be identified with a jurisdiction, users of the application must be associated with one or more jurisdictions. In the KYC application, users can only view assessments associated with jurisdictions to which they have access. You can also use a jurisdiction to divide data in the database. For example:

- **Geographical:** Division of data based on geographical boundaries, such as countries and states.
- **Organizational:** Division of data based on different legal entities that compose the client's business.
- **Other:** Combination of geographic and organizational definitions. In addition, it is client driven and can be customized.

Business Domain

Business domains are used for data access controls similar to jurisdiction but have a different objective. The business domain can be used to identify records of different business types (For example, Private Client vs. Retail customer), or to provide more granular restrictions to data such as employee data. The list of business domains in the application resides in the `KDD_BUS_DMN` table. The application tags each data record provided through the Ingestion Manager to one or more business domains. It also associates users with one or more business domains in a similar fashion. If a user has access to any of the business domains that are on a business record, the user can view that record.

The business domain field for users and data records is a multi-value field. For example, you define two business domains:

- **a:** Private Client
- **b:** Retail Banking

A record for an account that is considered both has `BUS_DMN_SET=ab`. If a user can view business domain **a** or **b**, the user can view the record. You can use this concept to protect special classes of data, such as data about executives of the firm. For example, you can define a business domain as *e: Executives*.

You can set this business domain with the employee, account, and customer records that belong to executives. Thus, only specific users of the application have access to these records. If the executive's account is identified in the Private Client business domain as well, any user who can view Private Client data can view the executive's record. Hence, it is important not to apply too many domains to one record.

The application also stores business domains in the KDD_CENTRICITY table to control access to Research against different types of entities. Derived External Entities and Addresses inherit the business domain set that is configured in KDD_CENTRICITY for those focus types.

Scenario Group

Scenario groups are used for data access controls. A scenario group refers to a group of scenarios in the KYC application that identify a set of scenario permissions and to which a user has access rights. Scenario groups need to be mapped to scenarios in order to view the alert details. The list of scenario groups in the application resides in the KDD_SCNRO_GRP table.

Case Type

If your firm has implemented KYC, you must establish access permissions associated with the available Case Types. The Case Type is used for data access controls similar to business domains, but has a different objective. The Case Type can be used to identify records of different case types or to provide more granular restrictions to data such as case data.

The following tables are involved in the display of the Case Type, Subclass1, and Subclass2 in the Case Management UI and are specific to the Enterprise Case Management implementation.

- KDD_CASE_TYPE_SUBTYPE – Each record in the Case Type Subtype table represents a case type available in the OFS ECM application. Cases are logically grouped to a certain type based on their behavior of interest and purpose of investigation. When generated, a case is mandatorily assigned to one of the case types for further investigation.
- KDD_SUBCLASS1 - Each record in the Case Subclass 1 table represents a subclass based on which the cases of a particular type can be grouped. On categorizing the cases based on type, they can further be grouped based on these subclasses. Case Subclass 1 provides the list of subclasses for first level grouping. Subclasses are not mandatory information for a case.
- KDD_SUBCLASS2 – Each record in the Case Subclass 2 table represents a subclass based on which the cases of a particular type can be grouped. On categorizing the cases based on type, they can further be grouped based on these subclasses. Case Subclass 2 provides the list of subclasses for second level grouping. Subclasses are not mandatory information for a case.
- KDD_TYPE_CLASS_MAP – Each record in the Case Type and Class Map table represents the set of valid combinations of Case Type, Subclass1 and Subclass2 values which can be used to group the cases for proper investigation.

Organization

Organizations are used for data access controls. Organizations are user group to which a user belongs. The list of scenario groups in the application resides in the KDD_ORG table.

Loading Security Attributes

This section covers the following topics:

Loading Security Attributes through Excel

The Excel Upload process inserts data into the appropriate dimension tables based on the pre-configured Excel Upload definitions installed during the application installation.

Note: Data which already exists must not be loaded again, as this results in failure of the upload. When uploading additional records, only the incremental records are maintained in the Excel template with the correct unique identifier key.

- All template Excel files for Excel Upload are available in `ftpshare/STAGE/Excelupload/AMCMLookupFiles`
- All date values are provided in `MM/DD/YYYY` format in the Excel worksheet.
- Whenever a record is deleted from the Excel worksheet, the complete row is deleted. This is to ensure that no blank active record exists in the Excel worksheet.
- After selecting the Excel template, preview it before uploading.

Security attributes are loaded through Excel using the following templates:

Table 6. Security Attributes and Excel Templates

Security Attribute	Excel Template
Jurisdiction	`KDD_JRSDCN.xls`
Business Domain	`KDD_BUS_DMN.xls`
Scenario Group	`KDD_SCNRO_GRP.xls`
Case type	• Case Type: KDD_CASE_TYPE_SUBTYPE **Note:** The Case Type created must pertain to its classification code, such as AML, FR, and KYC. • Case Subclass1: KDD_SUBCLASS1 • Case Subclass2: KDD_SUBCLASS2 • Case Type and Class Map: KDD_TYPE_CLASS_MAP
Organization	KDD_ORG database

Note: All Excel template files are available in: `ftpshare/STAGE/Excelupload/AMCMLookupFiles`

Uploading Excel

To upload an excel template, follow these steps:

1. Login as the KYC Administrator. The KYC application home page is displayed.

2. Click **User Security Administration**, and then click **Security Attributes Upload**. The Anti Money Laundering page is displayed.
3. In the left pane, click **Excel Upload.**
4. Browse your system and select the Excel file.
5. Select **Sheet** from Sheet drop-down list.
6. Go to the Excel-Entity Mappings section. Click Arrow icon to select one or more Mapping IDs from the dialog box. The Excel is updated.

Loading Security Attributes through SQL Scripts

This section covers the following topics:

- Loading Jurisdictions
- Loading Business Domains
- Loading Scenario Groups
- Loading Scenario Group Memberships
- Loading Organizations

Loading Jurisdictions

To load jurisdictions in the database, follow these steps:

1. Add the appropriate record to the KDD_JRSDCN database table as mentioned in *Table 7*.

Table 7. KDD_JRSDCN Table Attributes

Column Name	Description
JRSDCN_CD	Code (one to four characters) that represents a jurisdiction (For example, N for North, or S for South).
JRSDCN_NM	Name of the jurisdiction (For example, North or South).
JRSDCN_DSPLY_NM	Display name of the jurisdiction (For example, North or South).
JRSDCN_DESC_TX	Description of the jurisdiction (For example, Northern US or Southern US).

Note: The data in the KDD_JRSDCN database table is loaded through the ATOMIC schema.

2. Add records to the table by using a SQL script similar to the sample script in following figure:

```
INSERT INTO KDD_JRSDCN (JRSDCN_CD,
JRSDCN_NM,JRSDCN_DSPLY_NM,JRSDCN_DESC_TX)
VALUES ('E', 'East', 'East', 'Eastern')
```

Figure 4. Sample SQL Script for Loading KDD_JRSDCN

Note: The KDD_JRSDCN table is empty after application initialization and requires populating before the application can operate.

Loading Business Domains

To load a business domain, follow these steps:

1. Add the appropriate user record to the KDD_BUS_DMN database table as mentioned in the *Table 8*.

Table 8. KDD_BUS_DMN Table Attributes

Column Name	Description
BUS_DMN_CD	Single-character code that represents a business domain (For example, a, b, or c).
BUS_DMN_DESC_TX	Description of the business domain (For example, Institutional Broker Dealer or Retail Banking).
BUS_DMN_DSPLY_NM	Display name of the business domain (For example, INST or RET).
MANTAS_DMN_FL	Flag that indicates whether Oracle Financial Services Behavior Detection Framework specified the business domain (Y). If a BD client specified the business domain, set the flag to N.

Note: The KDD_BUS_DMN table already contains predefined business domains for the Oracle client.

2. Add more records to the table by using a SQL script similar to the sample script in the following figure:

```
INSERT INTO KDD_BUS_DMN (BUS_DMN_CD, BUS_DMN_DESC_TX,
BUS_DMN_DSPLY_NM, MANTAS_DMN_FL) VALUES ('a', 'Compliance
Employees', 'COMP', 'N');

INSERT INTO KDD_BUS_DMN (BUS_DMN_CD, BUS_DMN_DESC_TX,
BUS_DMN_DSPLY_NM, MANTAS_DMN_FL) VALUES ('b', 'Executives'
'EXEC', 'N');
```

Figure 5. Loading the KDD_BUS_DMN Table

3. Update the KDD_CENTRICITY table to reflect access to all focuses within the business domain with the following command:

```
update KDD_CENTRICITY set bus_dmn_st = 'a'
where KDD_CENTRICITY. CNTRY_TYPE_CD = 'SC'
```

Loading Scenario Groups

To load a Scenario Group, follow these steps:

1. Add the appropriate user record to the KDD_SCNRO_GRP database table as mentioned in the *Table 9*.

Table 9. KDD_SCNRO_GRP Table Attributes

Column Name	Description
SCNRO_GRP_ID	Scenario group identifier.
SCNRO_GRP_NM	Scenario Group Name

2. Add more records to the table by using a SQL script similar to the sample script in the following figure.

```
INSERT INTO KDD_SCNRO_GRP(SCNRO_GRP_ID,SCNRO_GRP_NM) VALUES
(66,'BEX');
INSERT INTO KDD_SCNRO_GRP(SCNRO_GRP_ID,SCNRO_GRP_NM) VALUES
(77,'CST');
COMMIT;
```

Figure 6. Loading the KDD_SCNRO_GRP Table

Loading Scenario Group Memberships

To load a Scenario Group Membership, follow these steps:

1. Add the appropriate user record to the KDD_SCNRO_GRP_MEMBERSHIP database table as mentioned in *Table 10*.

Table 10. KDD_SCNRO_GRP_MEMBERSHIP Table Attributes

Column Name	Description
SCNRO_ID	Scenario Identifier
SCNRO_GRP_ID	Scenario Group Identifier
SCNRO_GRP_NM	Scenario Group Name

2. Add more records to the table by using a SQL script similar to the sample script in the following figure.

```
INSERT INTO KDD_SCNRO_GRP_MEMBERSHIP
(SCNRO_ID,SCNRO_GRP_ID,SCNRO_GRP_NM) VALUES (113000016,66,'BEX') ;
INSERT INTO KDD_SCNRO_GRP_MEMBERSHIP
(SCNRO_ID,SCNRO_GRP_ID,SCNRO_GRP_NM) VALUES (113000016,77,'CST') ;
```

Figure 7. Loading the KDD_SCNRO_GRP_MEMBERSHIP Table

Loading Organizations

To load an organization in the database, follow these steps:

1. Add the appropriate user record to the `KDD_ORG` database table as mentioned in *Table 11*.

Table 11. KDD_ORG Table Attributes

Column Name	Description
ORG_CD	Unique identifier for this organization.
ORG_NM	Short name for this organization that is used for display purposes.
ORG_DESC_TX	Description of this organization.
PRNT_ORG_CD	Parent organization of which this organization is considered to be a child. **NOTE:** This references an ORG_CD in the KDD_ORG table.
MODFY_DT	Last modified date and time for this organization record.
MODFY_ID	User ID of the user who last modified this organization data. **NOTE:** This references a user in the Investigation Owner table (KDD_REVIEW_OWNER.OWNER_SEQ_ID).
COMMENT_TX	Additional remarks added by the user.

2. Add more records to the table by using a SQL script similar to the sample script in the following figure.

```
INSERT INTO KDD_ORG
(ORG_CD,ORG_NM,ORG_DESC_TX,PRNT_ORG_CD,MODFY_DT,MODFY_ID,COM
MENT_TX) VALUES ('ORG1','COMPLIANCE ORG','DEPARTMENT FOR
INVESTIGATION','ORG1 PARENT ORG','01-JUN-2014',1234,'ADDING
```

Figure 8. Loading the KDD_ORG Table

Mapping Security Attributes to Users

You can determine which security attribute controls the user's access permissions. Using this UI, an Administrator can map both Organizations and Users to different Security attributes.

To map a Security Attribute, follow these steps:

1. Login as the KYC Administrator. The KYC application home page is displayed.
2. Click **User Security Administration**, and then click **Security Attribute Administration**. The Anti Money Laundering page is displayed.
3. Hover over the Administration menu, select the User Administration sub-menu, and click **Security Attribute Administration**. The Security Attribute Administration page is displayed.
4. Select user type from Choose User Type drop-down list (Organization or User).

Note: Before proceeding with providing a user access through this UI, all necessary data is available in the appropriate database tables and the user must be created.

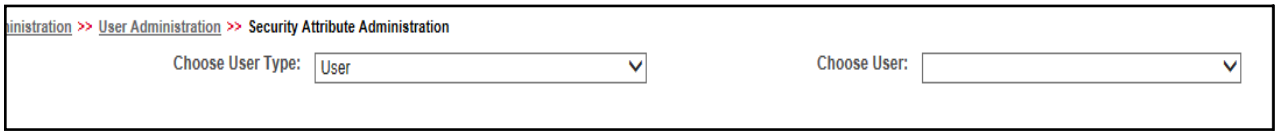


Figure 9. Security Attribute Administration

Based upon your User Type selection, the Choose User drop-down list changes. Select the user from Choose User drop-down list. The relevant Security Attribute Administration page is displayed.

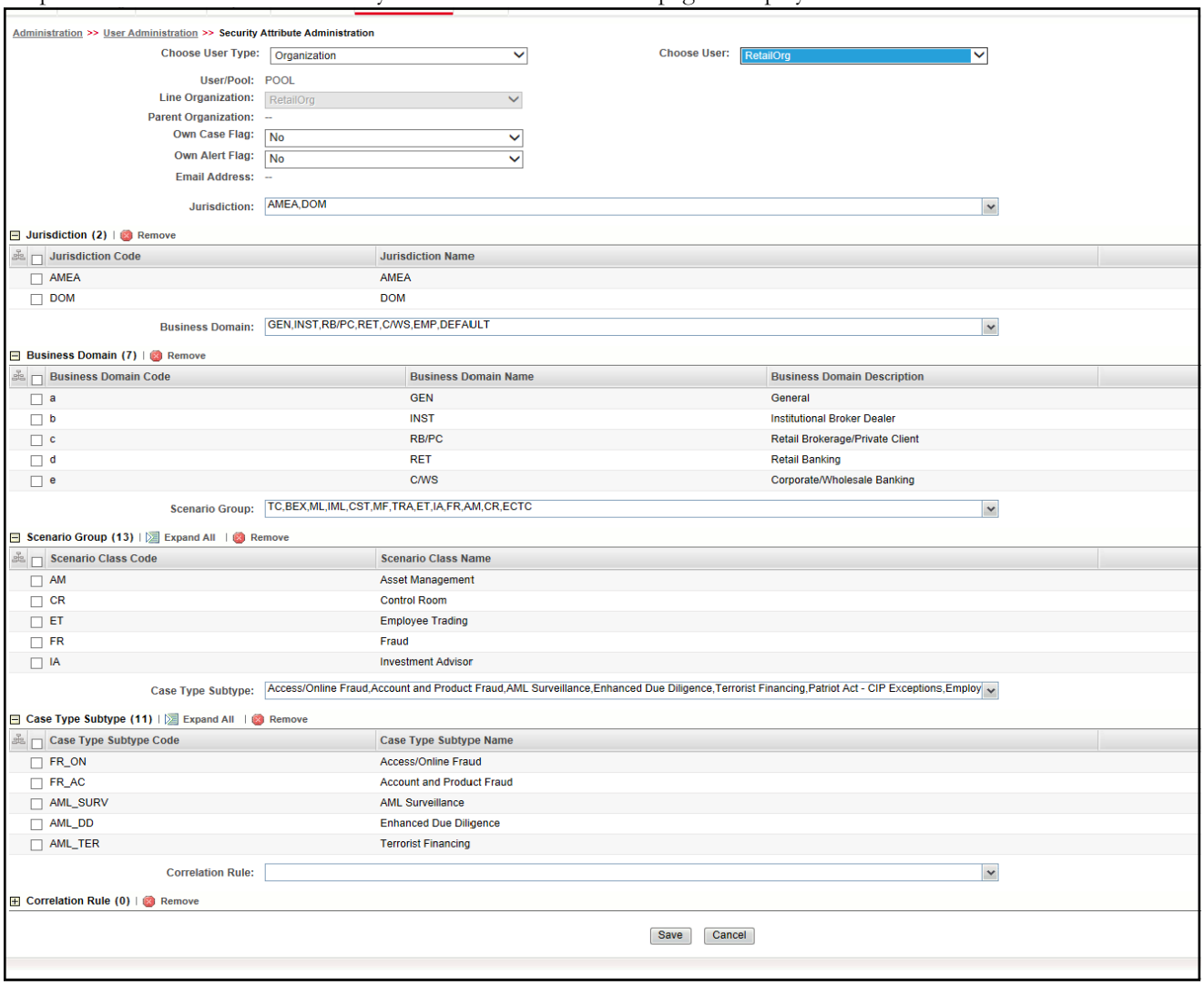


Figure 10. Security Attribute Administration

Note: In order to update the user profiles before proceeding with mapping any security attributes, select **User** from the **Choose User Type** drop-down list. When chosen, all the updates made to all the user profiles through User Maintenance UI are imported from the `CSSMS_USER_PROFILE` table of the OFS AAI ATOMIC schema to the `KDD_REVIEW_OWNER` table of the ATOMIC schema.

If you delete a user through the Security Management System screen, you must come back to the Security Attribute Administration screen and select the value **User** from the **Choose User Type** drop-down list. Then the deleted user is updated in the `KDD_REVIEW_OWNER` table against the column `actv_flg` as *N*, and that user is inactive.

Table 12. Security Attributes

Fields	Description
Organization	Select an organization from the drop-down list. A User or Organization's access to other Organizations depends on the selection(s) made for this organization parameter. For example, if a user is mapped to Org1 and Org2, it implies that this user can access alerts and cases which belong to these two organizations, provided other security attributes are also matching.
Own Case Flag	Select whether this user type owns a case flag from the drop-down list.
Own Alert Flag	Select whether this user type owns a alert flag from the drop-down list.
Note: The Own Alert and Case flag is required for taking ownership of the alerts and cases. If an alert user must perform a Promote To Case action, then the following prerequisites are fulfilled. The user is mapped to any one of the following user groups: ● Case Supervisor ● Case Analyst1 ● Case Analyst2	
Business Organization	The default Business Organization is displayed, but you can select the business organization from the drop-down list.
Jurisdictions	Select the jurisdictions from the drop-down list. Mapping of one or more jurisdictions to a user or organization allows this user or organization to access cases, alerts, watch lists, and watch list members that belong to the mapped jurisdiction. The selected jurisdictions are displayed in Jurisdictions section after you save your selection.
Business Domain	Select the business domains from the drop-down list. Mapping of one or more business domains to a user or organization allows this user or organization to access cases, alerts, watch lists, and watch list members that belong to the mapped business domains. The selected jurisdictions are displayed in Jurisdictions section after you save your selection.
Scenario Group	Select the scenario group from the drop-down list. Mapping of one or more Scenario Groups to a user or organization allows this user or organization to access alerts that belong to the mapped scenario Group. The selected jurisdictions are displayed in Jurisdictions section after you save your selection.
Case Type	Select the case type from the drop-down list. Mapping of one or more Case Types to a user or organization allows this user or organization to access cases that belong to the mapped Case Type. The selected jurisdictions are displayed in Case Types section after you save your selection.
Correlation Rule	Select the correlation rule from the drop-down list. Mapping of one or more correlation rules allows the user to view the correlations generated based on the mapped correlation. The selected jurisdictions are displayed in correlation section after you save your selection.

5. Click **Save**. The following confirmation message is displayed: *Would you like to save this action?*
6. Click **OK**. The following confirmation message is displayed: *The update operation successful.*
7. Click **OK**. The updated Security Attribute page is displayed.

Removing Security Attributes

This section allows you to delete the mapped security from the Users.

To remove security attributes, follow these steps:

1. Navigate to the Security Attributes page.
2. Select one or more check boxes in the respective security attributes such as Business Domain and Jurisdictions. Click Remove. The following confirmation message is displayed: *Are you sure you want to delete this records*?
3. Click **OK**. The selected record is deleted from the list.
4. Click **Save**. The changes are updated.

CHAPTER 3

Maintenance Activities and Configuring Setup Parameters

This chapter discusses the following topics:

- Prerequisite
- Maintenance Activities

Prerequisite

The OFS BD application pack must be installed. For information on pack installation, see *Behavior Detection Application Pack Installation Guide*.

Maintenance Activities

Oracle Financial Services KYC activities are classified into the following types:

- Initial or One time Activities
- Daily Activities

Initial or One time Activities

This section covers the following topics:

- Managing Users
- Uploading Data Using Excel
- Moving Country Data in KDD_CODE_SET_TRNLN table
- Configuring Application Parameters
- Configuring Application Installation Parameters
- Configuring Rule Based Risk Values
- Defining the Rereview Risk Thresholds
- Configuring Algorithm Based Risk Parameters
- Configuring Scores for Values in KYC Risk Assessment
- Populating Data in the KDD_CODE_SET_TRNLN Table
- Setting up Document Guidelines
- Third Party Integration

- Setting up KYC On-Boarding Service
- Scheduling KYC Batches
- Listing Holidays in the OFS AAI Administration User Interface
- Deployment Initiation Processing Based on the Implementation Requirement
- Partitioning IPE Tables

Managing Users

Users need to be created in KYC for KYC-related processing. For information on the users that need to created, see *Mapping a User with a User Group*.

For information on how to create users, see *Managing User Administration and Security Configuration*.

Uploading Data Using Excel

Note: You must upload the excel template in order to populate data into the KYC metadata tables.

The Excel upload process inserts data into the appropriate tables based on the pre-configured Excel upload definitions installed as part of the application installation. The Excel upload process fails if there are primary key violations during the upload process. When uploading data, only the incremental records are maintained in the Excel template with the correct unique identifier.
The Parameters and values for the default jurisdiction are provided in the Excel data file. New values can be added for the parameters in the Excel data files before the upload process is complete, or values can be modified in the application. For more information on uploading data using excel and the expected values for each column, see *Adding Risk Parameters for Algorithm-based Risk Assessments*.

Note: You must enter the appropriate value in the V_JRSDCN_CD column and the value must be according to the values in the `KDD_JRSDCN.JRSDCN_CD` table. For example, AMEA.

Moving Country Data in KDD_CODE_SET_TRNLN table

To add data for country so that it is available in the code set for KYC, run the following script:

```
insert into kdd_code_set_trnln select distinct 'ISOCountryCode', g.geo_cntry_cd, null,
g.geo_nm, null from GEOGRAPHY g;
Commit;
```

The following excel uploads must be performed. Each row has to be repeated for every jurisdiction.

- APPLN_RB_PROCESSING: Enter all the rule values you consider as high. The number of rows must be as many as the number of rule values for every jurisdiction.

Note: To add data for country so that it is available in the code set for KYC, run the following script:

```
insert into kdd_code_set_trnln select distinct 'ISOCountryCode',
g.geo_cntry_cd, null,
g.geo_nm, null from GEOGRAPHY g;
Commit;
```

- APPLN_REREVIEW_PARAMS: Enter the appropriate values in all the columns.
- APPLN_RISK_RATING_PARAMS: Ensure that the total weight of all the risk parameters that you have uploaded are equal to 100.
- DIM_RISK_CATEGORY: Ensure that the minimum range of consecutive rows are equal to the previous maximum range. For example, if the value in one row is 5-10, the value in the next row must be 10-15.

- DIM_RA_PRIORITY: Ensure that the minimum range of consecutive rows are equal to the previous maximum range. For example, if the value in one row is 5-10, the value in the next row must be 10-15.
- DIM_ACCT_CUST_ROLE_TYPE: Ensure that the value in the `F_CONTROLLING_ROLE` column is Y in order to consider the risk parameter for interested party calculations.

  Note: After uploading data, you can modify the values in the columns of all the excels except for the DIM_ACCT_CUST_ROLE_TYPE and DIM_RA_PRIORITY excels through the UI. All column values must be according to the data types and expected character length. Refer the sample values shown for the default jurisdiction to know what values must be provided.

Configuring Application Parameters

Initially, the default values for the application parameters are to be populated into the database (DB) during Excel upload. The parameter values can be modified in the Excel data files before the upload process is done. This can be fine tuned through the User Interface provided by logging into the application as the KYC Administrator. The entries in the Application Parameters (`Appln_Params`) are used to control the flow of the application. These parameters are Jurisdiction-specific.

The values of these parameters have an impact on the various services invoked by the application, and the work flow of the application. Multiple entries can be made for each parameter, one for each jurisdiction. For more information on how to navigate the UI and populate values for all jurisdictions, see *Configuration Guide*.

Configuring Application Installation Parameters

The Application Installation Parameters contain information about installation specific parameters which do not vary with the jurisdiction. This table has only one set of parameters for a particular installation. You can modify the values in the UI. For more information, see *Configuration Guide*.

Configuring Rule Based Risk Values

The sample values for the Rule Based Risk Assessment Parameters are populated into the DB during Excel upload. Parameters and Values for the sample jurisdiction are provided in the Excel data file. For each of the risk parameters, the rule values are updated against all valid jurisdictions.

Rule Based Risk Assessment Parameters contains information about the rules which are pre-defined and the parameter values (which can vary according to the jurisdiction). It is mandatory to update rules values for all the jurisdictions for which Rule Based Risk Assessment is used. For more information, see *Configuration Guide*.

Defining the Rereview Risk Thresholds

Sample values for the Re-Review Parameters are included as a part of the Excel upload. Excel data for all jurisdictions must have appropriate values in order for data to be available in the `KDD_JRSDCN` table.

The OFS KYC comes with pre-packaged rules based on which the Accelerated Re-Review is triggered. These rules are available in the Application Re-Review Parameters Table (`Appln_ReReview_Params`). All these 13 rules are updated for each jurisdiction using excel upload. Each record contains a rule number with which it is associated in the Re-Review Rules. Each rule can be enabled or disabled depending on the site-specific requirement. The `Appln_ReReview_Params` table specifies details such as Look Back Period, Count of Alerts, and Alert Score for the Rule.

For more information, see *Configuration Guide*.

Configuring Algorithm Based Risk Parameters

The weights for each parameter of the Algorithm-Based Risk Model are populated into the `Appln_Risk_Rating_Params` table in the DB during Excel upload.

The sample values must be fine tuned to suit the site specific requirements in the Excel data files before the Excel upload or modifying the parameter values after the Excel upload process by the KYC Administrator. For more information, see *Configuration Guide*.

Configuring Scores for Values in KYC Risk Assessment

The `PARAM_RISK_SCORE_JRSDN` table contains the risk parameter values for algorithm-based and rule-based risk parameters for all jurisdictions.

Before you configure scores, algorithm-based and rule-based parameters must be uploaded for both batch and RAOR. Each risk parameter or rule must have a corresponding code set and the same code set must be available in the `KDD_CODE_SET_TRNLN` table.

Populating Data in the KDD_CODE_SET_TRNLN Table

The data from the `KDD_CODE_SET_TRNLN` table is available in the UI when you click the Auto-Populate button in the *Risk Score for Parameter/Rule Value* page.

To access the *Risk Score for Parameter/Rule Value* page, follow these steps:

1. Navigate to the KYC home page.
2. Click **KYC Risk Assessment Configuration** in the LHS menu. The *KYC Risk Assessment Configuration* page is displayed.

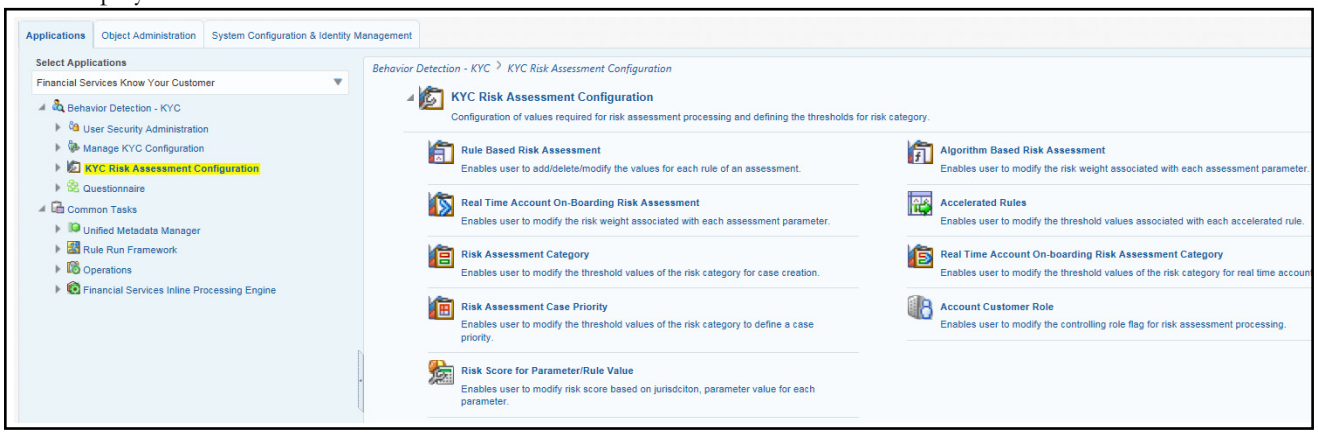


Figure 11. KYC Risk Assessment Configuration Page

3. Click **Risk Score for Parameter/Rule Value** in the RHS menu. The *Risk Score for Parameter/Value* page is displayed.

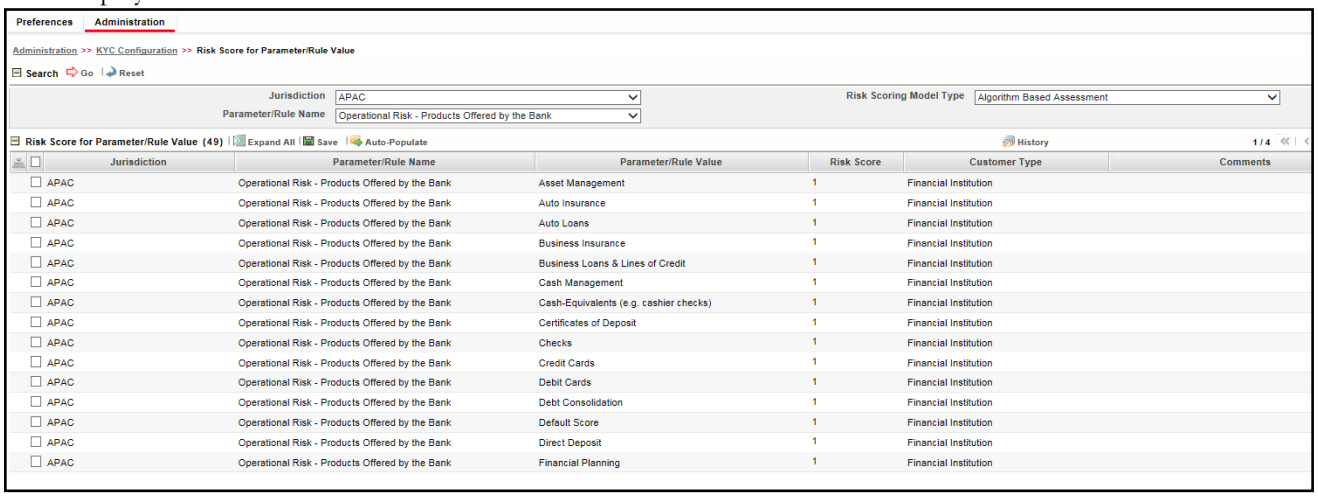


Figure 12. Risk Score for Parameter/Value Page

4. Click **Auto-Populate**. The risk scores for the parameters or rules are displayed.

Note: To configure the risk scores, you need to access the UI and make changes as required. For more information, see Configuration Guide.

Every code set has one or more seeded code values. You can add a code value in a code set or modify an existing code value in a code set.

To add a code value in a code set, execute the following script:

```
insert into KDD_CODE_SET_TRNLN (CODE_SET, CODE_VAL, SRC_SYS_CD, CODE_DISP_TX)
values ('', '', null, '');
```

To modify an existing code value in a code set, execute the following script:

```
update kdd_code_set_trnln set code_val='', code_disp_tx = '' where code_val = '' and
code_set='';
```

Setting up Document Guidelines

The internal document verification process occurs before the external identity verification is triggered to collect data for the risk assessment process. The guidelines for verification are set up as a start-up activity.

The guidelines must be entered in the Excel template available at `/ftpshare/STAGE/ExcelUpload/KYCLookupTables/ FCT_DOCS_GUIDELINES.XLS` in the `ficapp` layer.

Upload the details through the Excel upload activity.

Third Party Integration

Oracle Financial Services Know Your Customer can be integrated with external third party services for enhanced due diligence. The KYC Administrator can update the required configuration for identity verification from the UI.

For more information, see *Configuration Guide*.

Setting up KYC On-Boarding Service

KYC has a feature called Real-Time Account On-Boarding Risk (RAOR). This feature allows you to gather additional information from a customer and calculate the risk score of a customer.

The following parameters in `appln_install_params` are related to the Onboarding Service and must be configured in the KYC UI for executing a real time-service request:

- QUESTIONNAIRE_INFODOM: If the Questionnaire Infodom and the Application Infodom on which the Onboarding Service is deployed are not the same, then the infodom muts be changed accordingly.
- QUESTIONNAIRE_URI: Replace the placeholders for `<PROTOCOL>`, `<HOST_NAME>`, `<PORT>` and `<OFSAA_DOMAIN>` in the `v_attribute1_value` field with the appropriate values.
- RAOR_URI: Replace the placeholders for `<PROTOCOL>`, `<HOST_NAME>`, and `<PORT>` in the `v_attribute1_value` field with the appropriate values.
- QUESTIONNAIRE_APP_ID: The value must be `OFS_KYC`.

  For more information, see *Configuration Guide*.

Scheduling KYC Batches

After the installation is complete, login to the OFS KYC as the KYC Administrator and perform the steps mentioned in *Managing KYC Batches*.

Note: The batches are not visible in the Batch execution screen after the KYC installation is complete.

Table 13. Scheduling Batches

Criteria	Remarks
Timing of Execution of KYC batches	The KYC batches are executed only after Oracle Financial Services Behavior Detection application has completed the day's ingestion and alert generation process. This ensures that KYC has the latest customer, account, or alert information available for Risk Assessment reference. All the processing batches are EOD processing. The default review execution is scheduled as an EOD activity.
Sequence of Execution of KYC batches	The Processing of batch is in the following sequence: ● Deployment Initiation Processing - For processing the Existing customers. ● Regular Processing - For daily processing. ● EOD Processing (Feedback Processing) - For processing after the entire DI processing batch is complete. The feedback processing creates feeds for the account opening system and Oracle Financial Services Behavior Detection application. **Note:** Ensure that the feeds are scheduled as part of the data ingestion process in the account opening system and Oracle Financial Services Behavior Detection application.

Listing Holidays in the OFS AAI Administration User Interface

Use the OFS AAI Administration UI (Administration>Security Management>System Administrator >Holiday Maintenance) to setup and maintain the holiday list for the financial institution.

Deployment Initiation Processing Based on the Implementation Requirement

After installing KYC, the existing customers are to be risk assessed and processed through KYC for which Deployment Initiation is required. The Deployment Initiation Process helps the financial institution process the risk assessment of an existing customer once as a start-up process and mark them for periodic review based on the CER score.

Deployment Initiation Processing can be done in a single slot or can be executed in multiple slots (for example, Number of Customers to be processed) for managing the performance due to volume. The prerequisite for triggering the process execution involves setting up the KYC related parameters correctly using the application parameter configuration UI.

Partitioning IPE Tables

Take the back up of the IPE results tables by executing the below 3 sql statements in Atomic schema.

CREATE TABLE RTI_ASSMNT_EVAL_RESULT_TEMP AS SELECT * FROM RTI_ASSMNT_EVAL_RESULT;

CREATE TABLE RTI_ASSMNT_RESULT_TEMP AS SELECT * FROM RTI_ASSMNT_RESULT;

CREATE TABLE RTI_ASSMNT_EVAL_EXPORT_DATA_TP AS SELECT * FROM RTI_ASSMNT_EVAL_EXPORT_DATA;

Execute the below statements to Drop and Recreate (with partition) the 3 IPE results tables

```
Drop Table RTI_ASSMNT_EVAL_RESULT;
CREATE TABLE RTI_ASSMNT_EVAL_RESULT
 (
 N_RUN_ID              NUMBER(22)  ,
 N_BATCH_ID            NUMBER(22)  ,
 N_TASK_ID             VARCHAR2(100 CHAR)  ,
 N_START_TIME          TIMESTAMP ,
 N_ASSMNT_EVAL_RESULT_ID  VARCHAR2(3800 CHAR) ,
 N_ASSMNT_RESULT_ID    NUMBER(22)  ,
 N_EVAL_ID             NUMBER(22)  ,
 N_EVAL_VERSION        NUMBER(22) DEFAULT 0 ,
 N_EVAL_SCORE          NUMBER(22)  ,
 D_EVAL_TM             TIMESTAMP  ,
 N_ENTITY_SEQ_ID       VARCHAR2(3500 CHAR) ,
 N_ACTIVITY_BUS_ID     NUMBER(22)  ,
 N_ASSMT_ID            NUMBER(22)  ,
 V_THRESHOLD           VARCHAR2(100 CHAR),
 V_INFODOM             VARCHAR2(100 CHAR ) ,
 V_BATCH_RUN_ID        VARCHAR2(200 CHAR ) ,
 V_BATCH_ASSMNT_RES_ID VARCHAR2(4000 CHAR ),
 N_ASSMT_RES_EXT_REF_ID  NUMBER(22),
 V_APP_ID VARCHAR2 (20 CHAR) DEFAULT 'OFS_IPE' NOT NULL
 )PARTITION BY LIST (V_APP_ID)
SUBPARTITION BY LIST (V_BATCH_RUN_ID)
```

```
(
 PARTITION DEFAULT_PART VALUES (DEFAULT)
 (
SUBPARTITION DEFAULT_SUBPART VALUES (DEFAULT)
 )
);

Drop Table RTI_ASSMNT_RESULT;
CREATE TABLE RTI_ASSMNT_RESULT
  (
  N_RUN_ID              NUMBER(22)  ,
  N_BATCH_ID              NUMBER(22)  ,
  N_TASK_ID             VARCHAR2(100 CHAR)  ,
  N_START_TIME            TIMESTAMP ,
  N_ASSMNT_RESULT_ID   NUMBER(22)  ,
  N_ASSMT_ID          NUMBER(22) NOT NULL ,
  N_ASSMNT_VERSION      NUMBER(22) DEFAULT 0 ,
  N_ASSMNT_SCORE       NUMBER(22)  ,
  N_ENTITY_SEQ_ID      VARCHAR2(3500 CHAR) ,
  D_ASSMNT_EXEC_TM      TIMESTAMP ,
  V_ERROR_CODE         VARCHAR2(10 CHAR) ,
  V_ERROR_MSG          VARCHAR2(500 CHAR) ,
  N_ACTIVITY_BUS_ID     NUMBER(22)  ,
  V_ASSMNT_EXEC_MODE       VARCHAR2(10 CHAR)  ,
  V_ASSMNT_EXEC_RESULT     VARCHAR2(10 CHAR) ,
  N_ALERT_ID             NUMBER(22)  ,
  V_THRESHOLD               VARCHAR2(100 CHAR),
  V_INFODOM                VARCHAR2(100 CHAR ) ,
  V_BATCH_RUN_ID            VARCHAR2(200 CHAR ) ,
  V_BATCH_ASSMNT_RES_ID      VARCHAR2(4000 CHAR ),
  N_ASSMT_RES_EXT_REF_ID  NUMBER(22),
  V_APP_ID VARCHAR2 (20 CHAR) DEFAULT 'OFS_IPE' NOT NULL
 )PARTITION BY LIST (V_APP_ID)
SUBPARTITION BY LIST (V_BATCH_RUN_ID)
(
 PARTITION DEFAULT_PART VALUES (DEFAULT)
 (
SUBPARTITION DEFAULT_SUBPART VALUES (DEFAULT)
 )
);
```

```
Drop Table RTI_ASSMNT_EVAL_EXPORT_DATA;
CREATE TABLE RTI_ASSMNT_EVAL_EXPORT_DATA
(
N_RUN_ID NUMBER(22,0),
N_BATCH_ID NUMBER(22,0),
N_TASK_ID VARCHAR2(100 CHAR),
N_EVAL_ID NUMBER(22,0),
N_EVAL_VERSION NUMBER(22,0) DEFAULT 0,
N_ENTITY_SEQ_ID VARCHAR2(3500 CHAR),
N_ACTIVITY_BUS_ID NUMBER(22,0),
N_ASSMT_ID NUMBER(22,0),
V_INFODOM VARCHAR2(100 CHAR),
V_BATCH_RUN_ID VARCHAR2(200 CHAR),
V_APP_ID VARCHAR2(20 CHAR) DEFAULT 'OFS_IPE' NOT NULL ,
v_export_DATA clob
)PARTITION BY LIST (V_APP_ID)
SUBPARTITION BY LIST (V_BATCH_RUN_ID)
(
  PARTITION DEFAULT_PART VALUES (DEFAULT)
  (
SUBPARTITION DEFAULT_SUBPART VALUES (DEFAULT)
  )
);
```

Insert back the date in the IPE results table from the back up table only if requried. From a product stand up, we do not recommend this step.

Insert into RTI_ASSMNT_EVAL_RESULT select * from RTI_ASSMNT_EVAL_RESULT_TEMP;

Insert into RTI_ASSMNT_RESULT select * from RTI_ASSMNT_RESULT_TEMP;

Insert into RTI_ASSMNT_EVAL_EXPORT_DATA select * from RTI_ASSMNT_EVAL_EXPORT_DATA_TP;

To Create and Drop partition as part of Regular Processing Batch,

1.Open the RUN 'IPEKYCRun' in Edit mode, Click on 'Selector' Drop down and select 'Job'.

a.On the LHS of the pop-up, look for 'KYC_IPE_TABLE_CREATE_PARTITION' under 'Processes' and move that component to RHS

i.Select the KYC_IPE_TABLE_CREATE_PARTITION component check box in the RHS and Move it up to make it the first task.

b.On the LHS of the pop-up, look for 'KYC_IPE_DROP_PARTITION' under 'Processes' and move that component to RHS

i.Select the KYC_IPE_DROP_PARTITION component check box in the RHS and Move it down to make it the last task.

2.Click on Ok to close the pop-up and then SAVE then RUN.

To Create and Drop partition as part of Deployment Initiation Batch,

1.Open the RUN 'IPEKYCRunDI' in Edit mode, Click on 'Selector' Drop down and select 'Job'.

a.On the LHS of the pop-up, look for 'KYC_IPE_TABLE_CREATE_PARTITION' under 'Processes' and move that component to RHS

i.Select the KYC_IPE_TABLE_CREATE_PARTITION component check box in the RHS and Move it up to make it the first task.

b.On the LHS of the pop-up, look for 'KYC_IPE_DROP_PARTITION' under 'Processes' and move that component to RHS

i.Select the KYC_IPE_DROP_PARTITION component check box in the RHS and Move it down to make it the last task.

2.Click on Ok to close the pop-up and then SAVE then RUN.

Daily Activities

This section covers the following topics:

- Real-Time Account On-Boarding Risk Assessment
- Regular Processing - Account Opening Review
- Regular Processing- Accelerated Review
- Regular Processing - Re-Review or Periodic
- Feedback or Application EOD Processing

Real-Time Account On-Boarding Risk Assessment

Processing the online request from the Account On-Boarding system assists in the account opening process.

The Real Time Account On-Boarding Risk Assessment (RAOR) workflow is triggered by the request from the external account opening system.This returns a risk score to the external account opening system. The request and response is sent as a Web Service Request.

If questionnaires are chosen as part of the on-boarding service, then questionnaire-related configurations are required. KYC only provides the list of questions that need to be asked based on their configurable attributes. For information on how to invoke the service, see *KYC Service Guide*.

Regular Processing - Account Opening Review

All the accounts which were opened the previous x days and are in *Active* status are picked for risk assessment. The accounts which were opened in the last 7 days and activated the previous day are also selected. The look back period is set to x days, where x is configurable. The Account Range for Regular Processing parameter can be modified from the Application Parameters UI screen under the KYC Administration option by the KYC Administrator. For more information, see *Configuration Guide*.

Regular Processing- Accelerated Review

Accelerated Review depends on the changes in customer and account information as well the alerts behavior. The Accelerated Review Processing is executed, along with Default or Account Opening review, after the Oracle Financial Services Behavior Detection Framework alert generation is complete.

Regular Processing - Re-Review or Periodic

After every review (Account Opening Review, Deployment Initiation, or Accelerated Review), the next review date is set for the customer based on the risk assessed. Thus, customers are periodically subjected to Risk Assessment, which is essential as the risk associated with each customer may change over time.

After a case is closed, the customer's next review date is determined by adding the time period (specified for the current risk category of the case) to the processing date in line with the holiday list definition.

Re-Review Processing checks whether the Next Re-Review Date falls between the processing date and the number of days specified for the attribute in the `KYC_PERIODIC_REVIEW` parameter.

Note: The table used to specify the number of days is the `APPLN_PARAMS` table and the column where the number is provided is `V_ATTRIBUTE1_VALUE`.

A Risk Assessment is created for customers whose next review date matches with the current day's processing date. This batch is executed once every day.

Feedback or Application EOD Processing

During the execution of the regular processing batches, the risk scores at customer levels are sent to the Oracle Financial Services Alert Management application and the account opening system. The feedback batch achieves this goal by consolidating customers and their risk scores on whom the risk assessment was created, analyzed, and closed for the processing date.

The application also creates a KYC watch list feed for the Oracle Financial Services Alert Management application for the customers whose review is completed.

CHAPTER 4 Managing KYC Batches

This chapter discusses the following topics:

Note: Before you Create a batch, ensure that all the necessary batch uploads mentioned in Adding Risk Parameters are completed.

Note: A prerequisite for KYC batches is to run ingestion first.

About KYC Batches

KYC batches are run using two processes:

- Regular processes, which are run daily
- Deployment Initiation processes, which are run once

Note: With relation to 8.0.2 KYC, the equivalent batches in 8.0.4 KYC for Deployment Initiation Processing, Regular Processing, and End Of the Day Processing are 'IPEKYCRunDI', 'IPEKYCRun' and 'IPEKYCEODDI'.

Deployment Initiation Processing

This batch is to be executed only once at the time the KYC application goes live. All the sections listed under this batch are part of the Re-Review Processing Batch also. The batch is split into the following sections:

- Customer Identification for Risk Assessment
- Watch List screening
- Risk Assessment
- Auto Closure
- Promote to Case
- Customer - Risk Assessment History population

Customers are picked for processing based on the following:

- **Jurisdiction**: Oracle Financial Services clients can process the deployment workflow based on specific jurisdiction.
- **Customer Type**: Oracle Financial Services clients can also process data based on customer type.
- **Length of Relationship**: Oracle Financial Services clients can also process data based on length of relationship of the customer and this is configurable.

Note: All the above criteria for processing can be done separately or by combining them.

Refer to the KYC_DEPLOYMNT_INIT_WF parameter under the application parameter.

End of Day Processing

This topic covers the following sections:

Feedback to the Oracle Financial Services Behavior Detection Framework or Account Opening System

At the end of each day, risk scores for risk assessments that are auto-closed or closed by the compliance officer after investigation are sent to Oracle Financial Services Behavior Detection Framework and the Account Opening System through Feedback files. Watch List files and Feedback files to the Account Opening System are available after KYC End of Day (EOD) processing is complete. These files must then be scheduled for loading into Oracle Financial Services Behavior Detection Framework and the Account Opening System. The processing date is the date of KYC EOD Processing. The following files are available:

- CBS Feedback (incremental dump of processing day for Oracle Financial Services Alert Management application)
- Watch List Entry Feedback (full dump as of processing day)
- Customer - Risk Assessment Details (Incremental dump as of processing day for the Account Opening System) The delimiter for the extract file can be defined under Unified Metadata Data Integrator. Refer to the Appendix C, "Extraction Definition,".

CBS Feedback

This file contains the Customer ID and the risk score computed by the risk assessment engine. The file name is obtained by appending the processing date to GenCustDetails_ED. The Feedback Flag is updated in the FCT_CUST_RVWDTLS table. Customer Feedback is not sent unless the Business schema is present. This file is sent in the batch which runs in the subsequent days.

Table 14. CBS Feedback

SL No.	Business Name	Data Type
1	Risk Assessment ID	String
2	Customer ID	String
3	Customer Name	String
4	Customer Effective Risk Score	Number
5	Risk Assessment Closed Date	Date
6	Next Re-review Date	Date

Watch List Entry Feedback

The Watch List is generated for closed cases and where closure is recommended for the Account. The records populated in the Watch List results table for a processing date are dumped into this file. The file name is obtained by appending the processing date to GenWLSFeedback_ED.

Table 15. Watch List Feedback

SL No.	Business Name	Data Type
1	Entity Identifier Type	String
2	Entity Identifier	String
3	Watch List Identifier(Referred from Application parameter KYC_WLS_ENTRY_FILE_ID)	String
4	Watch List Entry Description Text	String

Customer - Risk Assessment Details

This file contains the Customer ID and the Risk assessment details computed by the risk assessment engine. The file name is obtained by appending the processing date to GenCustDetails_ED. This file is created for the Oracle Financial Services Behavior Detection Framework and placed in the path defined by the Configuring Customer Feedback Files parameter in the Application Parameter UI. A schedule must be created to load this file in the Customer Supplemental Attribute table of the Behavior Detection Framework application. The data provided in this file is used for calculating the Entity Risk of a customer, where the KYC Risk is one component of Entity Risk. The file contains the KYC risk score provided when a risk assessment is closed by the application or closed by the investigation officer on every processing date.

Table 16. Risk Assessment Details

SL No.	Business Name	Data Type
1	Customer ID	String
2	Customer Effective Risk Score	Number
3	Custom1Date	String
4	Custom2Date	String
5	Custom3Date	String
6	Custom1Real	String
7	Custom2Real	String
8	Custom3Real	String
9	Custom1Text	String
10	Custom2Text	String
11	Custom3Text	String
12	Custom4Text	String
13	Custom5Text	String
14	Source System	String

Customer - Risk Assessment History

The KYC application captures the history of all the risk assessments created on all the customers within a period of 12 months and would retain for x period of months. 12 months is configured by default, the administrator can update this parameter based on the client requirement. The value can be updated from the UI for the 'V_ATTRIBUTE1_VALUE' for the 'KYC_RISK_ASSESSMENT_HISTORY' parameter of the Application Install Parameters. A partition is created on the table based on the value which is updated.

Renaming and Transferring Feedback files

When a KYC review for a new account request is complete, KYC informs the Account On-Boarding System about the disposition of the review. At the disposition of a periodic or accelerated KYC review, the KYC application communicates the results of the review to the appropriate banking application used within the financial institution, such as an Account Management application. The parameters required for renaming and transferring feedback files must be configured in the `appln_install_params` table.

The Oracle Financial Services KYC application is also responsible for sharing Account, Customer, and Watch List feedback to the Oracle Financial Services Alert Management application and Oracle Flexcube application at the disposition of the KYC review.

The extract names are not compatible with the Oracle Financial Services Behavior Detection Framework file naming convention. This utility completes the following activities based on the configurations set for the implementation:

1. Moves the files to the different location in the same server.
2. Renames the files with the extension defined.
3. Maintain a copy of the extract in the history directory with its original name.
4. The utility covers the following extracts in KYC 2.0:

- GenCustDetails_ED<YYYYMMDD>
- GenWLSFeedback_ED<YYYYMMDD>

Regular Processing

The Default Account Review workflow is triggered upon request from the following external account opening system:

This section covers the following topics:

- Prefilter Rules
- Risk Assessment Initiation
- Promote to Case

OFS KYC requires an online batch interface to facilitate Watch List Scanning, Identity Verification, News Searches, and successful execution of the default review.

The Account Opening Review is executed at the end of the day and the results are computed.

There are two ways to execute the batch for Account Opening

- Regular Processing on daily basis (Combined batch with Re-Review)
- Weekly Processing on weekly basis (Combined batch with Re-Review)

Prefilter Rules

These rules comprise of accelerated re-review, periodic review, and new accounts. For more information, see *Daily Activities* section and Chapter 5 and 6 of the *Configuration Guide*.

Risk Assessment Initiation

Based on the reasons generated in the previous module, risk assessments are created for the corresponding customers. The type of risk assessment source is specified as *Accelerated Re-Review*.

Then the next Re-Review Date for each customer is compared to the day's processing date. If the two match, then a risk assessment is created for the customer with the risk assessment source specified as *Periodic Re-Review*.

There are two types of Risk Assessments:

- Rule-based Risk Assessment
- Algorithm-based Risk Assessment

Rule-based Risk Assessment

Rule-based assessment calculates a risk score based on client configurable rules. For more information about the Rule-based assessment model parameters, see *Configuration Guide*.

Rule-based assessment model supports a business process framework, which allows the bank or FI to provide different values for the pre-defined rules. All customers are first assessed using the Rule-based Assessment Model and then assessed using the Algorithm-based Assessment Model.

For Rule-based assessment, the values for each rule are provided by the Admin user. For more information about providing values for rule-based assessment, see *Adding Risk Parameters for Rule-based Risk Assessments*.

A customer can fall under one or more rules during rule-based assessment. When a customer has been matched to multiple rules, the application considers the maximum score of the matched rules.

For example, a customer has matched the Country of Citizenship and Country of Residence rules, with the values being Afghanistan and India, with a score of 45 and 60 respectively. In this case, the application considers the risk score as 60 for the customer. It also captures and displays all the rules matched.

Risk assessments created using this work flow are promoted to a case based on the risk score mentioned in the Risk Category table.

Algorithm-based Risk Assessment

Algorithm-based Assessment Model calculates the risk of customers based on different parameters which are based on customer type.

For each parameter the application checks the value provided by the customer who is being risk assessed, and retrieves the score of that value from the `PARAM_RISK_SCORE_JRSDN` table. If the value provided by the customer for a parameter is not available, then the application considers it as DEFAULT which would have a corresponding score in the `PARAM_RISK_SCORE_JRSDN` table. If the value provided by the customer is not available or the value is not provided at all, then a value of DEFAULT is assigned.

Closure Updates

After Risk Assessment, some risk assessments are eligible for Auto-Closure based on the following criteria:

- The User Review Flag of the risk category to which the risk score belongs is set to N.
- The High Risk Watch List Flag of the Risk assessment is set to N.
- The difference between the present risk score and previous risk score is less than the value specified in the parameter KYC_CHG_IN_CUST_RSK_TOLERANCE.

For all the risk assessments that satisfy the above set of conditions, the records of the risk assessed customers in the KYC Master Customer Table (Fct_Cust_Rvwdtls), is updated with all the parameters pertaining to the risk score

calculation. Subsequently, the records of all the accounts associated with the risk assessed customer are also updated with the risk scores. The threshold values for Auto-Closure can be altered by changing the value of the Application parameter mentioned above.

Promote to Case

During Risk Assessment Promotion to Case, there are possibilities of few risk assessments not being promoted to case which can be because of non-availability of data, system issues, server problems etc.

The error for the Risk Assessment not being promoted to a case is captured in the table RA_TO_CASE_ERROR. This table is available in the KYC Atomic schema. The user must identify the cause of the error and resolve the same. Once the error is rectified, these Risk Assessments are promoted to a case during the next KYC batch processing.

Running KYC Batches

For the first time after installation, you need to create batches in KYC by running a fire run.

To do a fire run, follow these steps:

1. Login as the KYC Administrator. The KYC application home page is displayed.
2. From the **Common Tasks** option, select **Rule Run Framework** in the LHS menu.
3. Click **Run**. The Run page is displayed.
4. From the List section, select the particular batch that you want to run and click **Fire Run**. The Fire Run page is displayed.

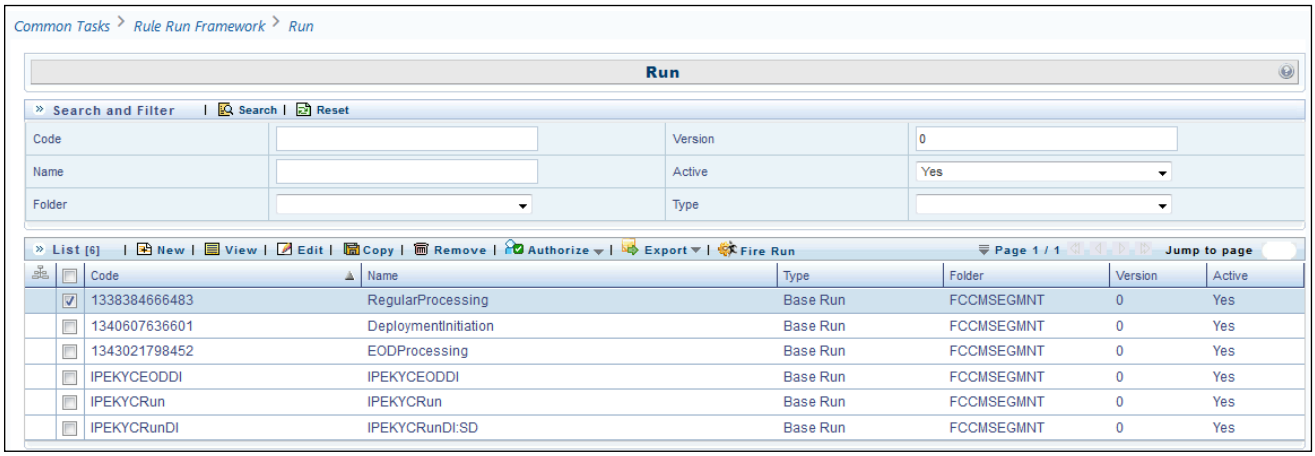


Figure 13. Running KYC Batches

5. In the Fire Run page, provide the required values.

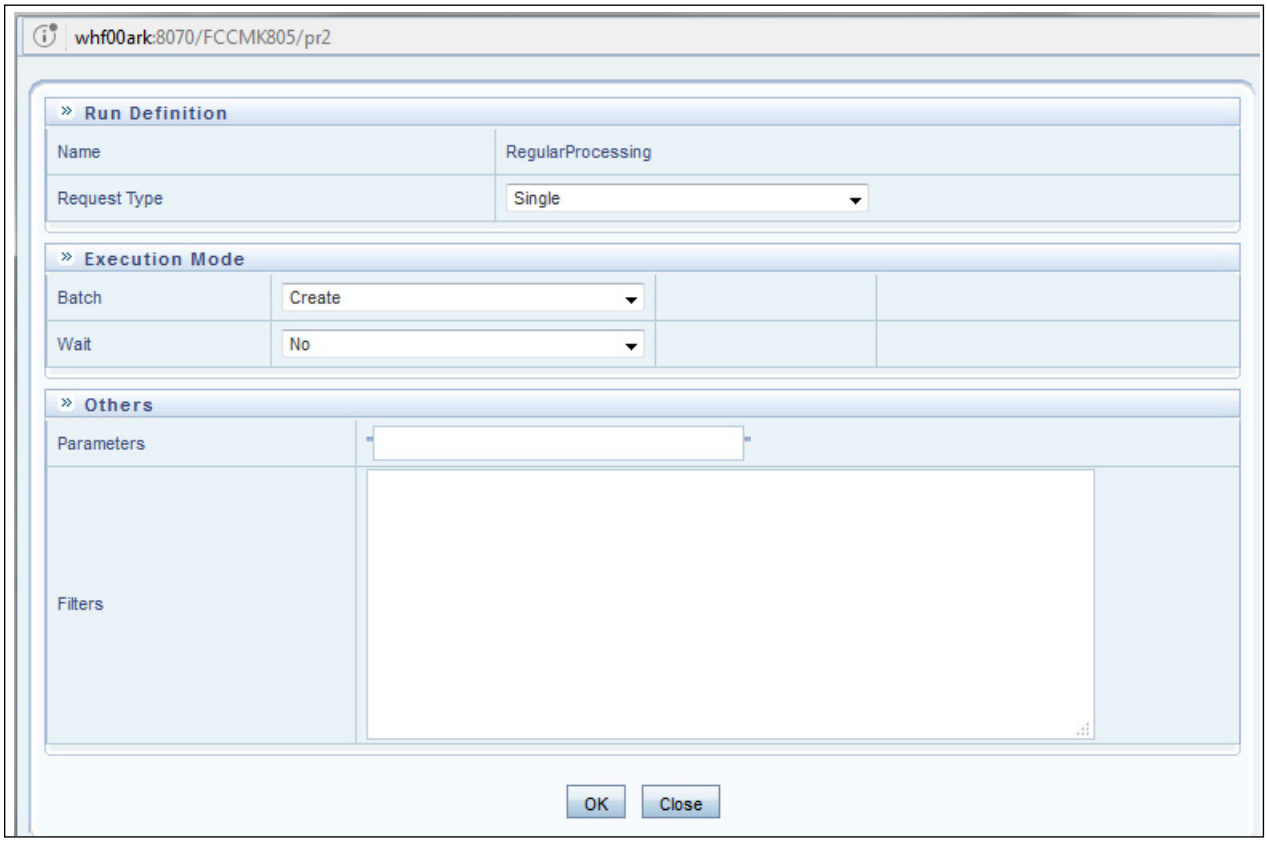


Figure 14. Fire Run

6. Click **OK**.

Running a Single Task Using a Batch

From the Batch Execution page, you can run a single task from a batch.

Note: Running a single task using a batch is not a recommended approach and must be done only for debugging a particular task.

To run a single task using a batch, follow these steps:

1. Login as the KYC Administrator. The KYC application home page is displayed.
2. From the **Common Tasks** option, select **Operations** in the LHS menu.
3. Click **Batch Execution**. The Batch Execution page is displayed.
4. From the Batch Details section, select the particular batch that you want to execute.
5. From the Task Details section, click  . The Task Mapping window is displayed.

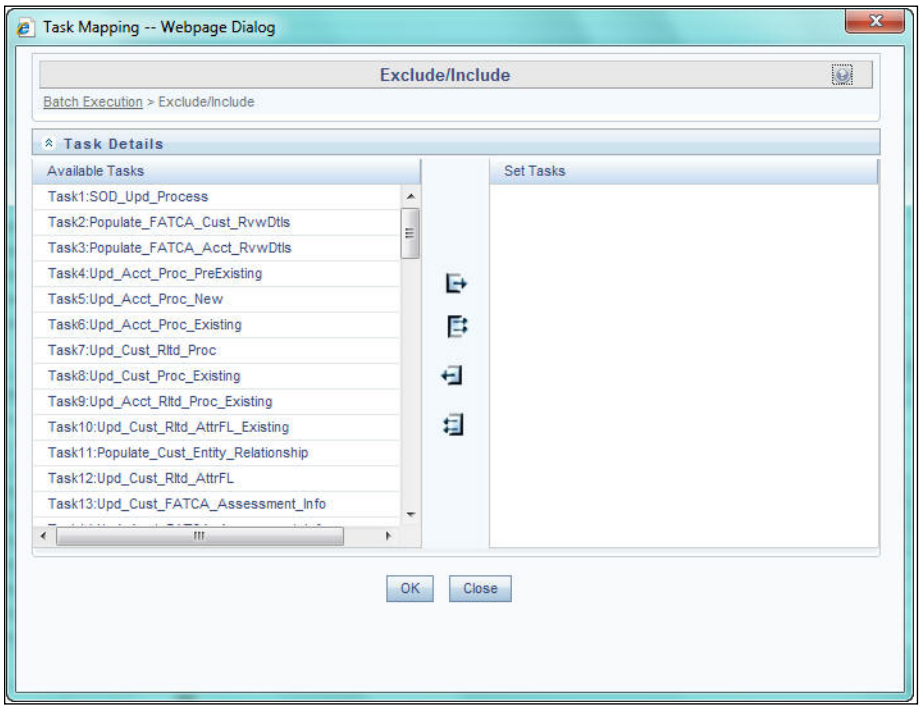


Figure 15. Running a Single Task Using a Batch

6. Retain the tasks that you want to execute under the Available Tasks section and move the rest to the Set Tasks section.
7. Click **OK**. The following warning message is displayed: *If you exclude a task, it will be skipped when executing the batch but, the precedence will not be altered. Do you want to exclude the selected task(s)?*
8. Click **OK**.
9. Click **Execute Batch**.

Scheduling a Batch

This section covers the following topics:

- Scheduling a Batch Once
- Scheduling a Daily Batch
- Scheduling a Weekly Batch
- Scheduling a Monthly Batch

Scheduling a Batch Once

To schedule a batch that you want to run only once, follow these steps:

1. Login as the KYC Administrator. The KYC application home page is displayed.
2. From the **Common Tasks** option, select **Operations** in the LHS menu.

3. Click **Batch Scheduler**. The Batch Scheduler page is displayed.
4. Select a batch that you want to schedule from the list of available batches. The Batch Scheduler section is expanded and displays additional options.
5. Click **New Schedule**.
6. Set the frequency of the new schedule as **Once**.
7. Enter the schedule time of the batch by specifying the **Start Date** and the **Run Time**.

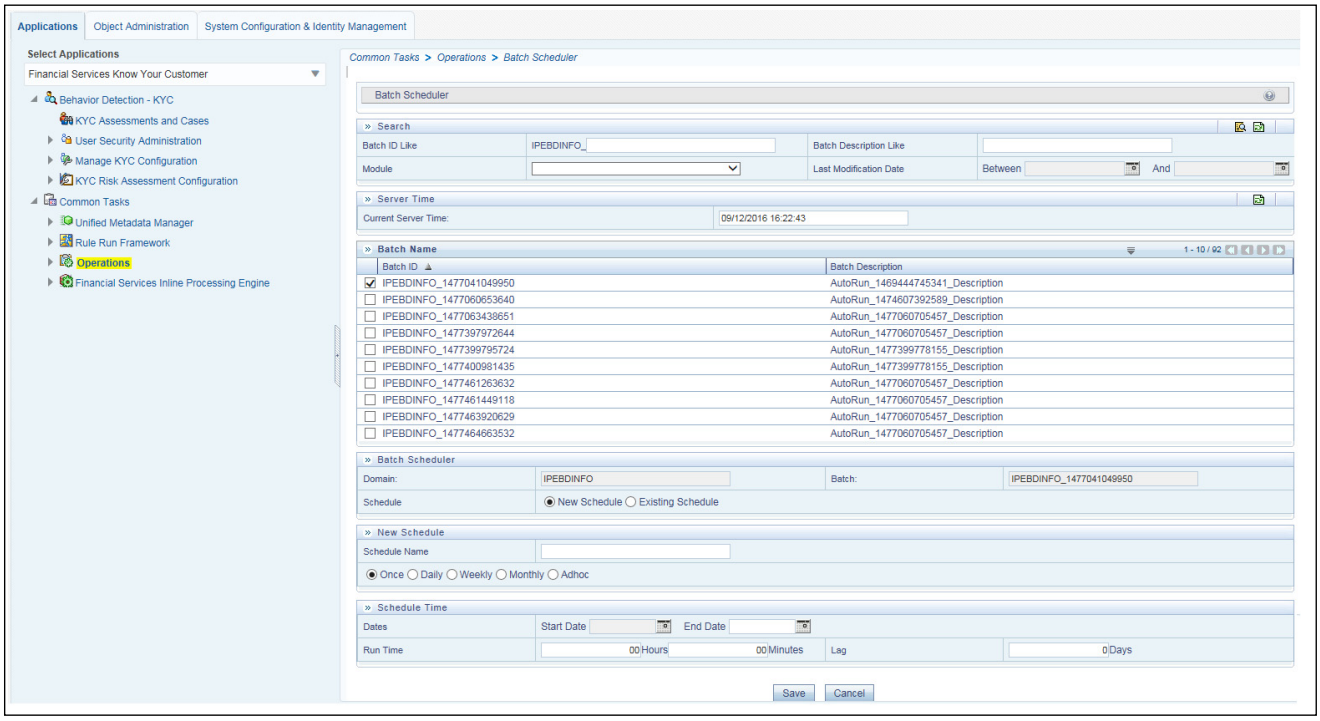


Figure 16. Scheduling a Batch Once

8. Click **Save**.

Scheduling a Daily Batch

To schedule a batch that you want to run daily, follow these steps:

1. Login as the KYC Administrator. The KYC application home page is displayed.
2. From the **Common Tasks** option, select **Operations** in the LHS menu.
3. Click **Batch Scheduler**. The Batch Scheduler page is displayed.
4. Select a batch that you want to schedule from the list of available batches. The Batch Scheduler section is expanded and displays additional options.
5. Click **New Schedule**.
6. Set the frequency of the new schedule as **Daily**.
7. Enter the schedule time of the batch by specifying the **Dates**, **Run Time**, and **Every** information.

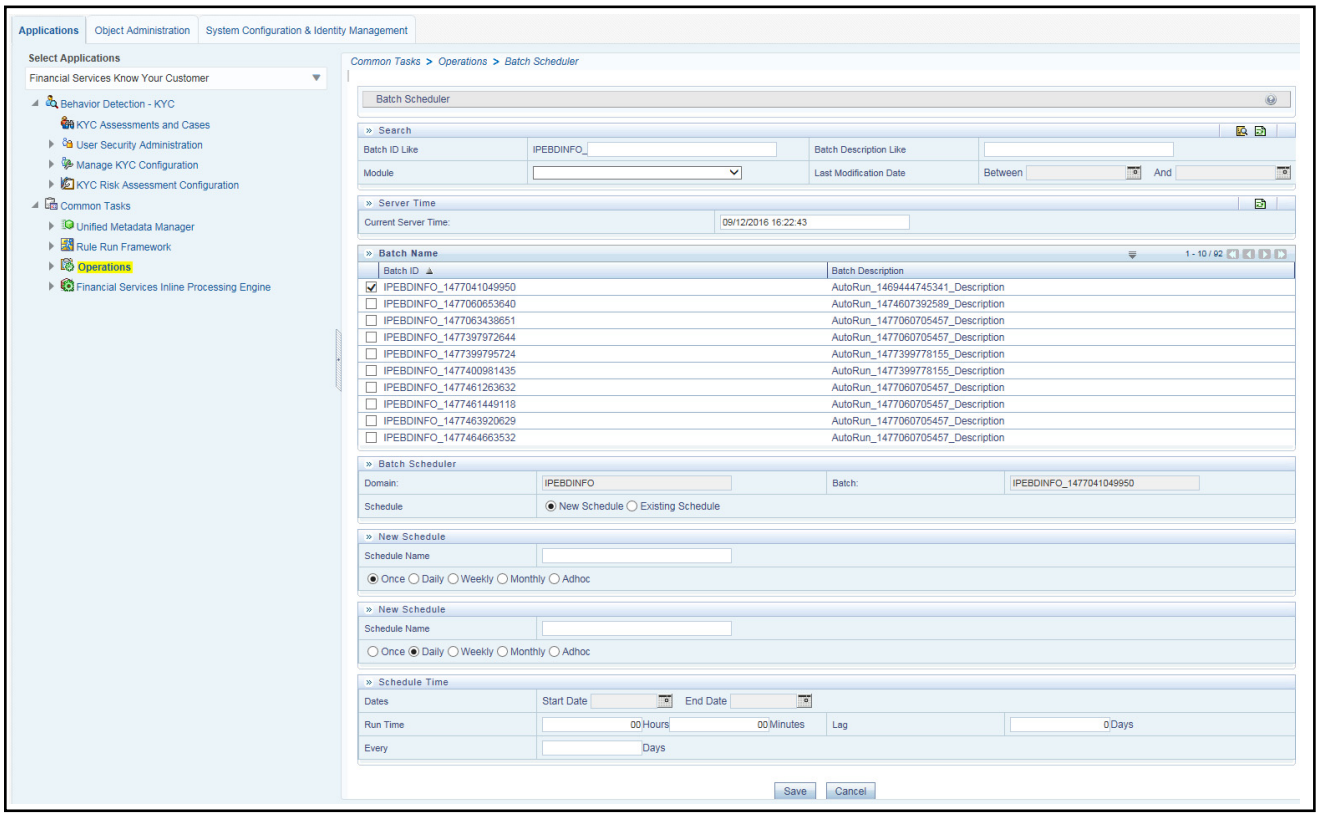


Figure 17. Scheduling a Daily Batch

8. Click **Save**.

Scheduling a Weekly Batch

To schedule a batch that you want to run weekly, follow these steps:

1. Login as the KYC Administrator. The KYC application home page is displayed.
2. From the **Common Tasks** option, select **Operations** in the LHS menu.
3. Click **Batch Scheduler**. The Batch Scheduler page is displayed.
4. Select a batch that you want to schedule from the list of available batches. The Batch Scheduler section is expanded and displays additional options.
5. Click **New Schedule**.
6. Set the frequency of the new schedule as **Weekly**.
7. Enter the schedule time of the batch by specifying the **Dates**, **Run Time**, **Every, Working days of the Week** information.

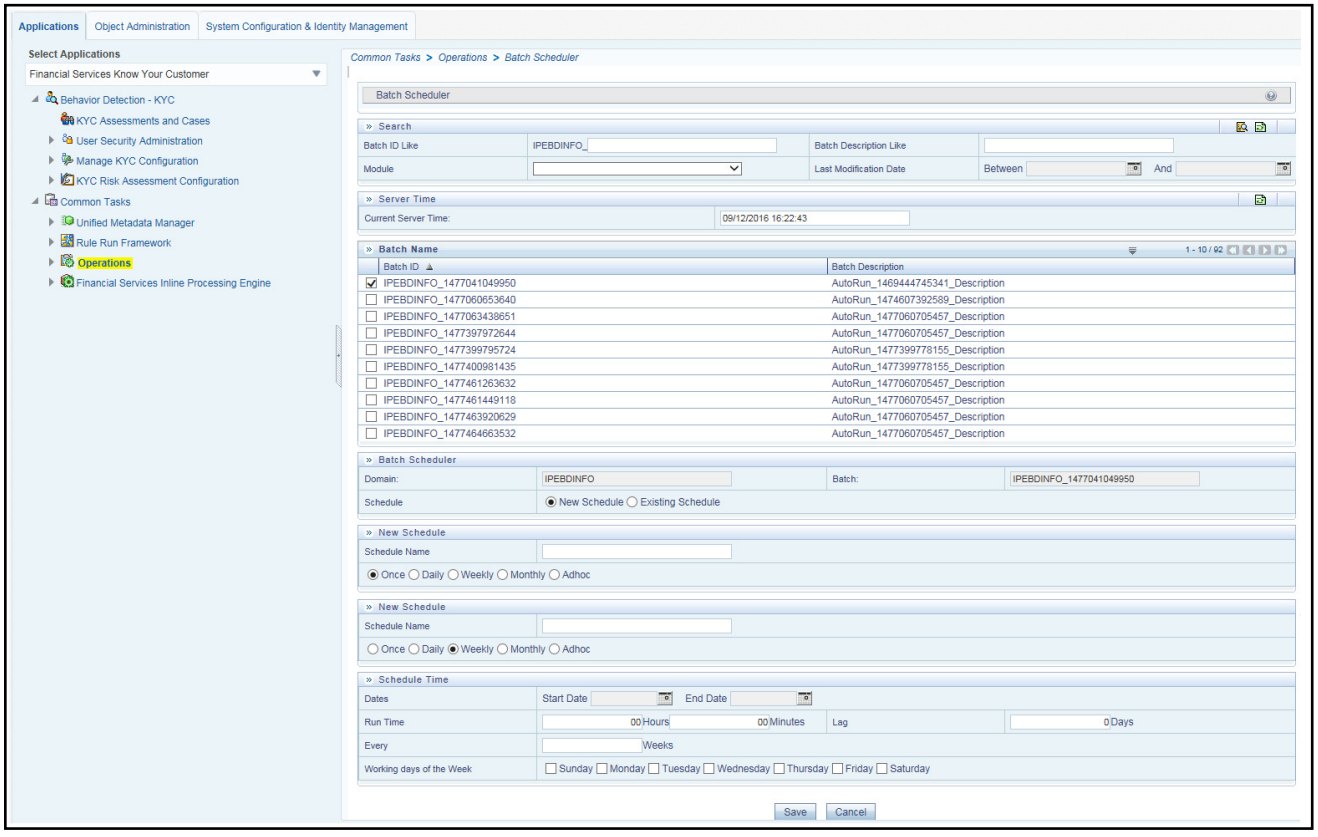


Figure 18. Scheduling a Weekly Batch

8. Click **Save**.

Scheduling a Monthly Batch

To schedule a batch that you want to run monthly, follow these steps:

1. Login as the KYC Administrator. The KYC application home page is displayed.
2. From the **Common Tasks** option, select **Operations** in the LHS menu.
3. Click **Batch Scheduler**. The Batch Scheduler page is displayed.
4. Select a batch that you want to schedule from the list of available batches. The Batch Scheduler section is expanded and displays additional options.
5. Click **New Schedule**.
6. Set the frequency of the new schedule as **Monthly**.
7. Enter the schedule time of the batch by specifying the **Dates**, **Run Time**, and **Occurrence** information.

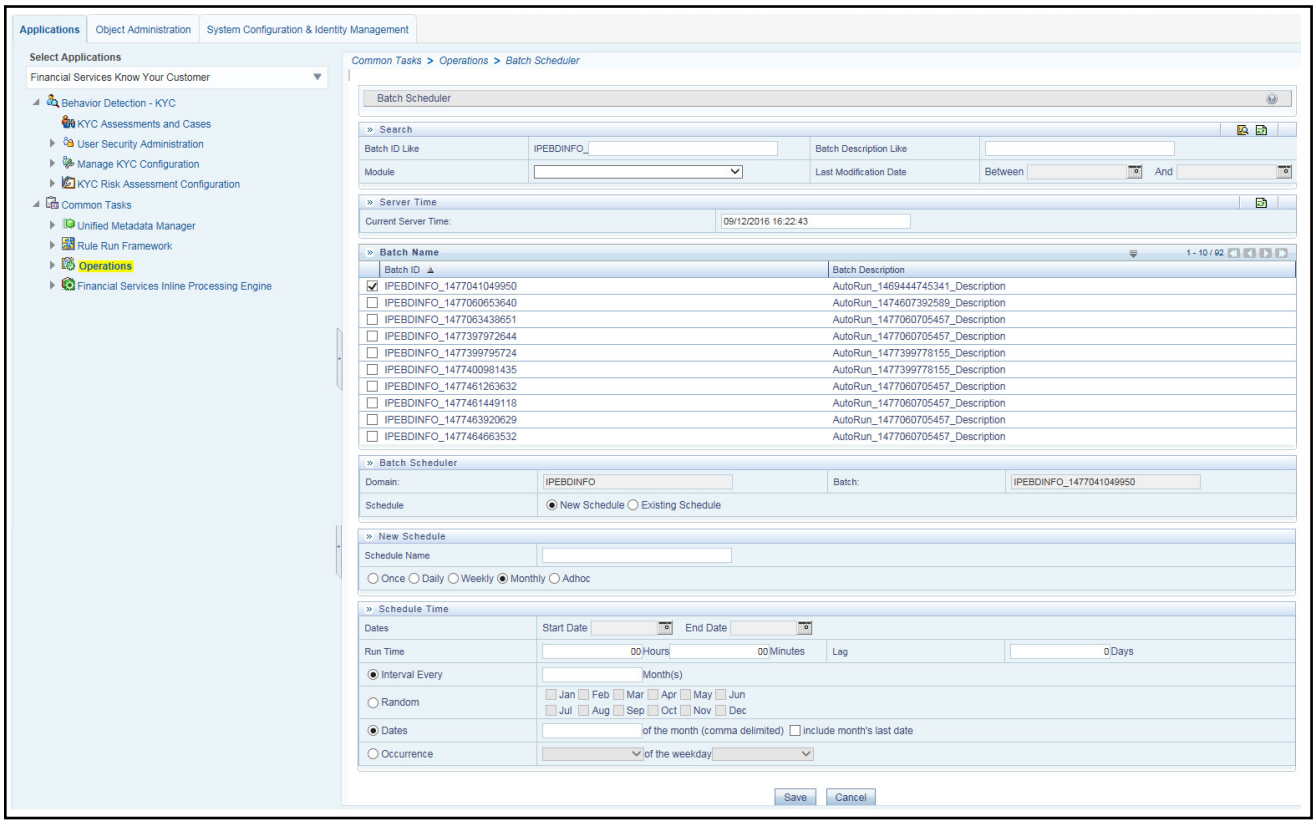


Figure 19. Scheduling a Monthly Batch

8. Click **Save**.

KYC Batch Execution Logs

Logs are created only after the batches are executed. The following types of tasks are present in the batches:

- Table 2 Table (T2T)

- Transform Data (Data transformation or DT logs)
- Promote to Case

Batch Execution Logs are based on the types of rule. The following sections describe the types of task present in the batches.

Table 2 Table (T2T)

The logs for this type of task are created in the path as follows:

```
<Ofsaai Installed Area>/ficdb/log/ t2t/KYC12DOM_1221824179931_20121122_1_Task1_ttl.log
```

The following table describes the log file:

Table 17: Table 2 Table (T2T)

Component	Description
KYC12DOM	This is the INFODOM on which the batch was executed
1221824179931	This is the ID of the RUN (batch is created once the RUN is saved)
20121122	This is the date on which the Batch was executed
1	The batch is executed for the first time on the same day
Task1	This log file is for the Task1 of the batch

Transform Data (Data transformation or DT logs)

The logs for this type of task are created in the path as follows.

The following types of definitions can be defined under data transformations:

- Executing a Stored procedure
- Executing a Shell script

The following log files are created for the Stored Procedure execution type of Transform data. The definition name is available in these log files.

- `<Ofsaai Installed Area>/ficdb/log/date/DT_KYC12DOM_1221824179931_20121123_1_Task23.log`
- `<Ofsaai Installed Area>/ficdb/log/date/RunProc_KYC12DOM_1221824179931_20121123_1_Task23.log`
- `/ftpshare/<DT_Definition_name>.log /`

The following logs are created for the Shell script type of Transform data:

```
<Ofsaai Installed Area>/ficdb/log/date/DT_KYC12DOM_1221824179931_20121123_1_Task23.log
```

Information related to the failure is inserted into the `am_log_file.logfile` which is present in the path `<Ofsaai Installed Area>/ficdb/log/`

Table 18: Shell script Transform data

Component	Description
DT	This is a product indication for the Data transformation type of log
RunProc	This indicated that the log is for running a procedure (function)
KYC12DOM	This is the INFODOM on which the batch was executed
1263964041287	This is the ID of the RUN (batch is created once the RUN is saved)
20121120	This is the date on which the Batch was executed
2	The batch is executed for the second time on the same day
Task23	This log file is for the Task23 of the batch
DT_Definition_name	A log file is created with the name of the DT definition created.

Promote to Case

If any of the risk assessments are not promoted to a case, refer to the table `RA_TO_CASE_ERROR` present in the KYC Atomic schema for the reasons for not being promoted.

CHAPTER 5 Adding Risk Parameters

This chapter discusses the following topics:

- Adding Risk Parameters for Algorithm-based Risk Assessments
- Adding Risk Parameters for Rule-based Risk Assessments

Adding Risk Parameters for Algorithm-based Risk Assessments

Before you add risk parameters, you need to:

1. Prepare the metadata in the application. For more information, see Maintenance Activities and Configuring Setup Parameters.
2. Update the sequence ID for IPE. To do this, execute the following script in the Config schema as a post installation step:
3. `Begin p_set_sequence_value('TASKS','5000000','Y'); end;`
4. For information on the post installation activities, see Installation Guide.

To add risk parameters for algorithm-based risk assessments, follow these steps:

1. Navigate to the KYC home page.
2. Click **Manage KYC Configuration** in the LHS menu.The *Manage KYC Configuration page* is displayed.

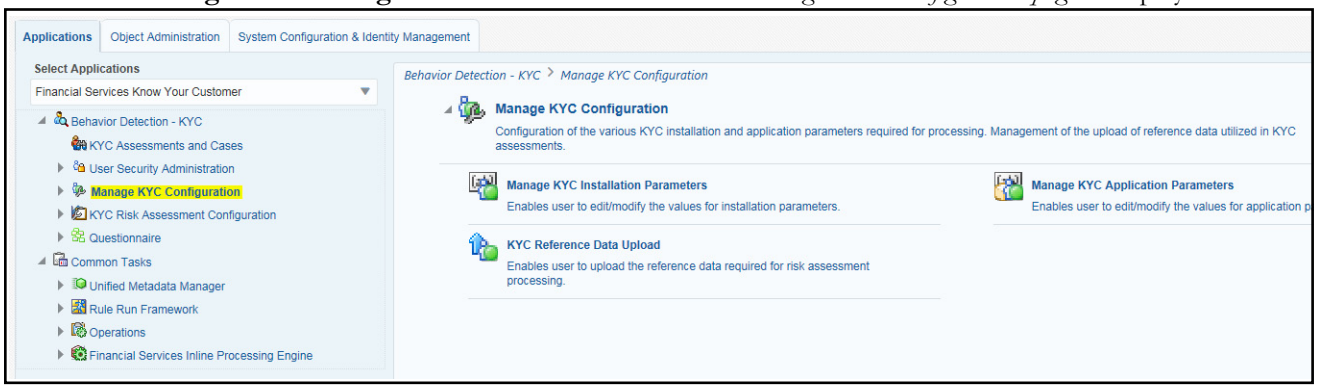


Figure 20. Manage KYC Configuration Page

3. Click **KYC Reference Data Upload** in the RHS menu. The *Administration* page is displayed.

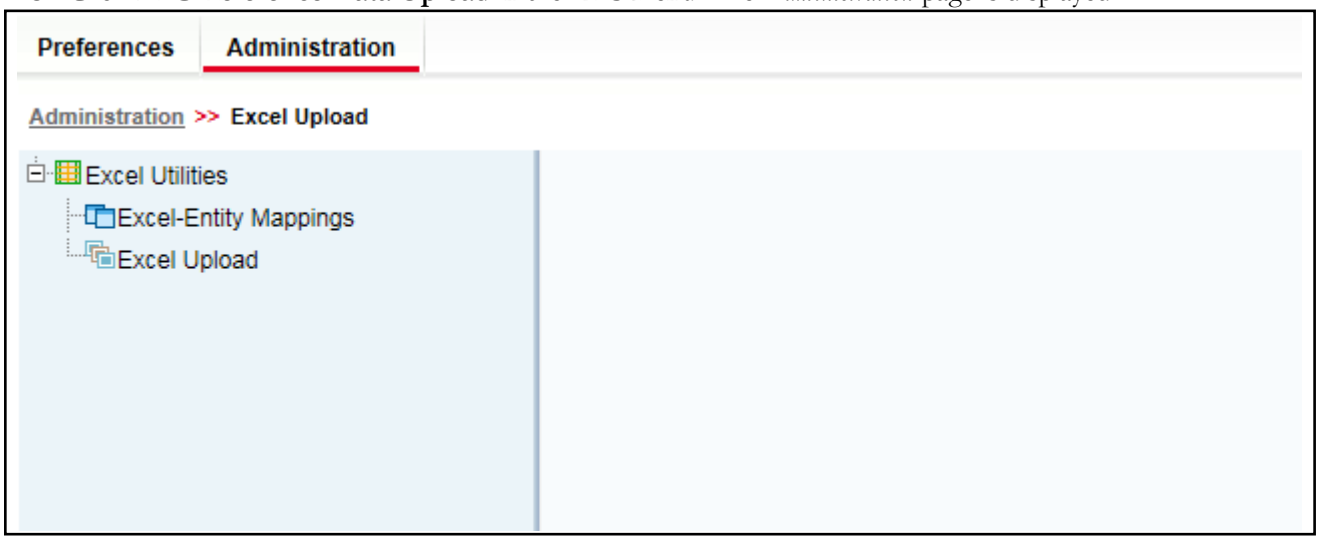


Figure 21. Administration Page

4. Click **Excel-Entity Mappings**. The *Excel-Entity Mappings* page is displayed.

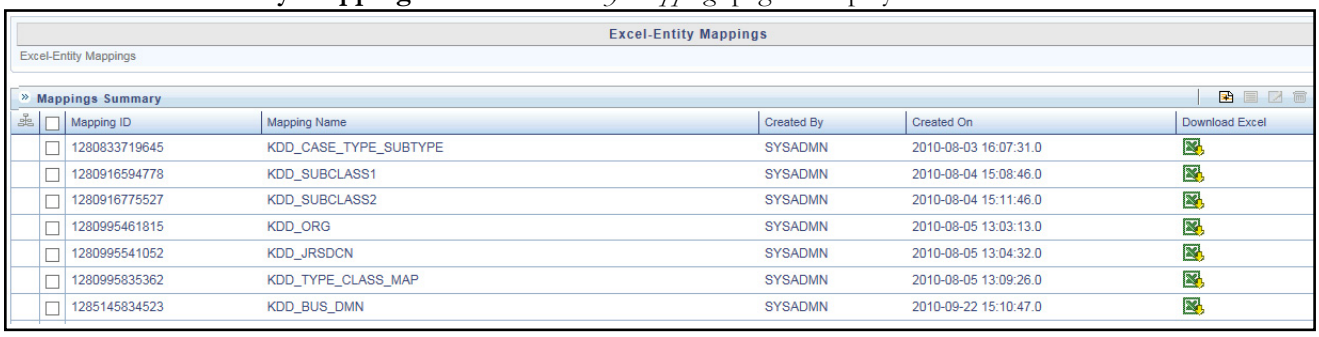


Figure 22. Excel-Entity Mappings Page

5. Download the `APPLN_RISK_RATING_PARAMS` metadata sheet and add the following details of the new risk parameter:

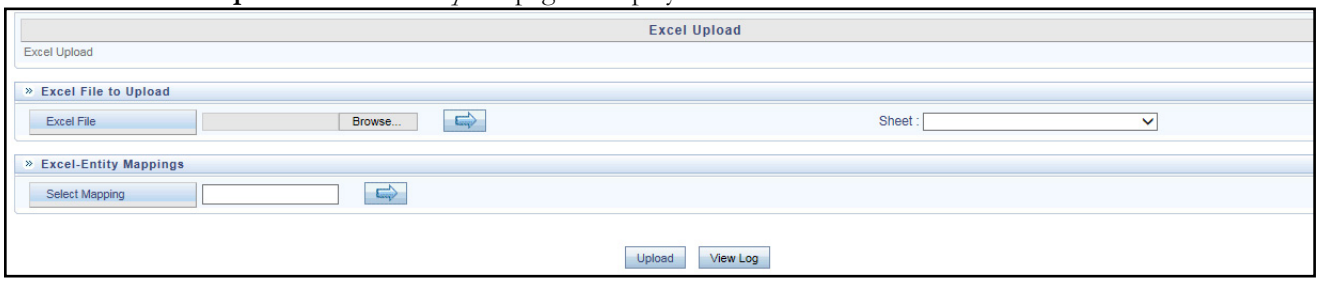
Table 19. Expected Values for APPLN_RISK_RATING_PARAMS

Parameter Name	Expected Value
V_RISK_MODEL_CODE	• For batch algorithm: The value must be CCR. • For RAOR algorithm: The value must be NRAOR.
V_RISK_MODEL_DESC	• For batch algorithm: The value must be CCR. • For RAOR algorithm: The value must be Real-time account onboarding.
V_RISK_PARAM_CODE	• For batch algorithm: The value must be Batch mode_MB_CCR_<unique value>. • For RAOR algorithm: The value must be Batch mode_MB_OB_<unique value>. **Note:** The recommended unique value must represent the new parameter being added.
V_RISK_PARAM_DESC	• For batch algorithm and RAOR algorithm: Add the appropriate description for the algorithm.

Table 19. Expected Values for APPLN_RISK_RATING_PARAMS

Parameter Name	Expected Value
V_CODE_SET	• For batch algorithm and RAOR algorithm: Provide an appropriate code set according to the KDD_CODE_SET_TRNLN.CODE_SET table. If the new parameter does not have a corresponding code set available, such as for range-based parameters, the code set needs to be manually added to the KDD_CODE_SET_TRNLN.CODE_SET table. **Note:** For non-range based parameters, Oracle recommends that you validate the new code set through the appropriate support channel. **Note:** To identify if the new parameter (<table>.<column>) has a defined code set, see the standard values column for the tables and columns that you need to add as shown in the *Financial Services Data Model Reference Guide Volume 1*.
F_ENABLE	For batch algorithm and RAOR algorithm: The value must be Y to consider the new parameter for risk scoring.
N_RISK_PARAM_WEIGHT	For batch algorithm and RAOR algorithm: The total weights of the risk parameters must add up to 100. These values need to be updated in the application.
V_JRSDCN_CD	For batch algorithm and RAOR algorithm: Provide the jurisdiction code for the new parameter. The code must be according to the values in the KDD_JRSDN table.
V_CUST_TYPE_CD	For batch algorithm and RAOR algorithm: Provide the customer codes for the parameter. The code must be one of the following: • IND: Individual • FIN: Financial Institution • ORG: Other Organization
V_CATEGORY	For batch algorithm and RAOR algorithm: The value must be KYC.

6. Click **Excel Upload**. The *Excel Upload* page is displayed.



7. Click **Browse.**
8. Select the APPLN_RISK_RATING_PARAMS metadata sheet and click the arrow. The sheet name appears in the Sheet field and a preview of the sheet details appear below.
9. In the Select Mapping field, click the arrow and select the template which contains data for the APPLN_RISK_RATING_PARAMS sheet.
10. Click **Upload**. For a successful upload, the following message is displayed:

    Successfully uploaded data into APPLN_RISK_RATING_PARAMS. Please click the View Log button to check the logs.

11. In the KYC home page, click **KYC Risk Assessment Configuration** in the LHS menu.

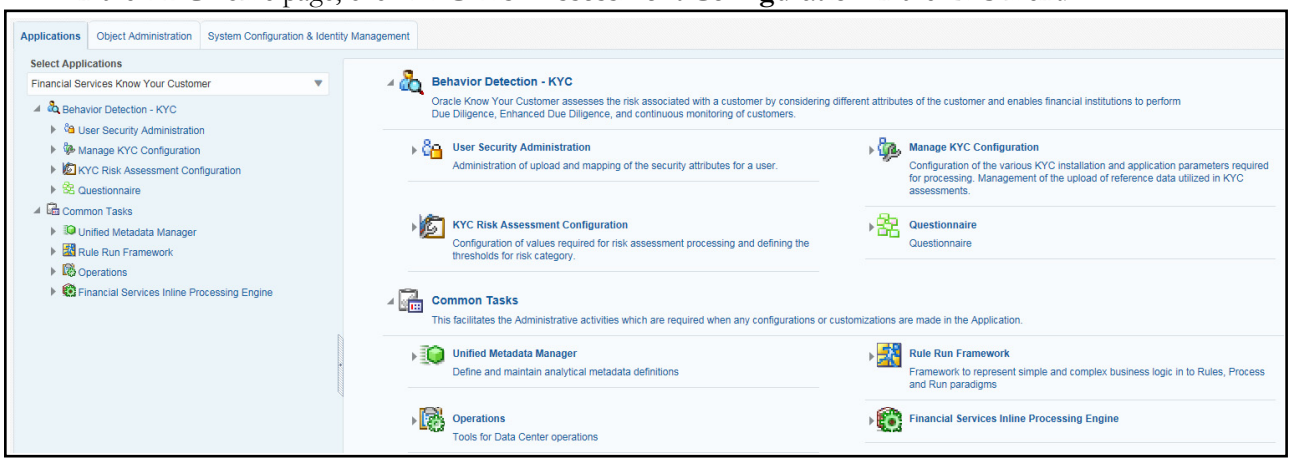


Figure 23. KYC Risk Assessment Configuration Page

12. Click **Algorithm Based Risk Assessment** in the RHS menu. The *Algorithm Based Risk Assessment* page is displayed.

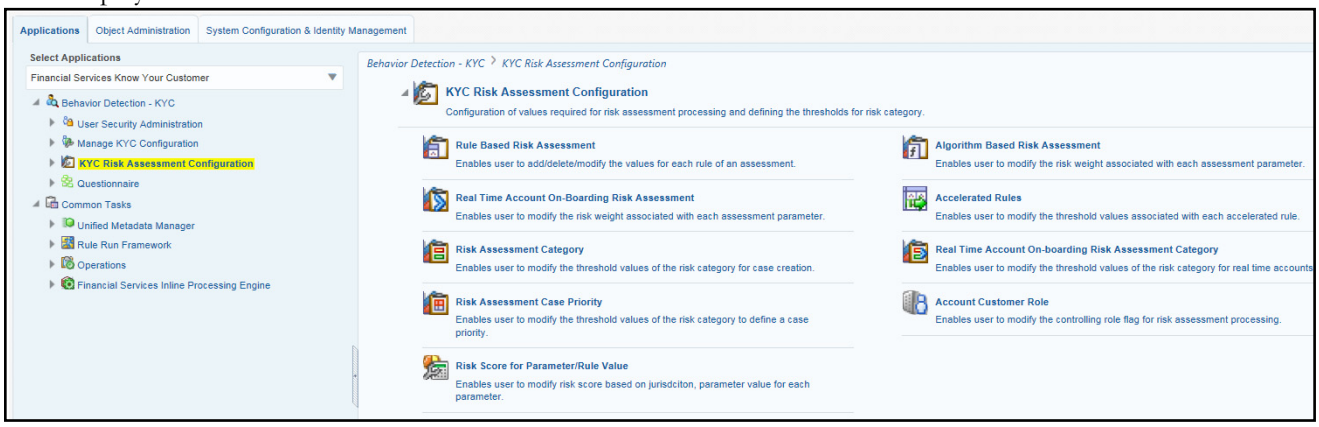


Figure 24. Algorithm Based Risk Assessment Page

13. Select the jurisdiction and make appropriate changes to the weight.

Note: The weights of all risk parameters must add to 100 for a combination of jurisdiction and customer type.

14. To view the risk score of the new parameter, click **Risk Score for Parameter/Rule Value** in the **KYC Risk Assessment Configuration** page. The Risk Score for Parameter/Rule Value page is displayed.

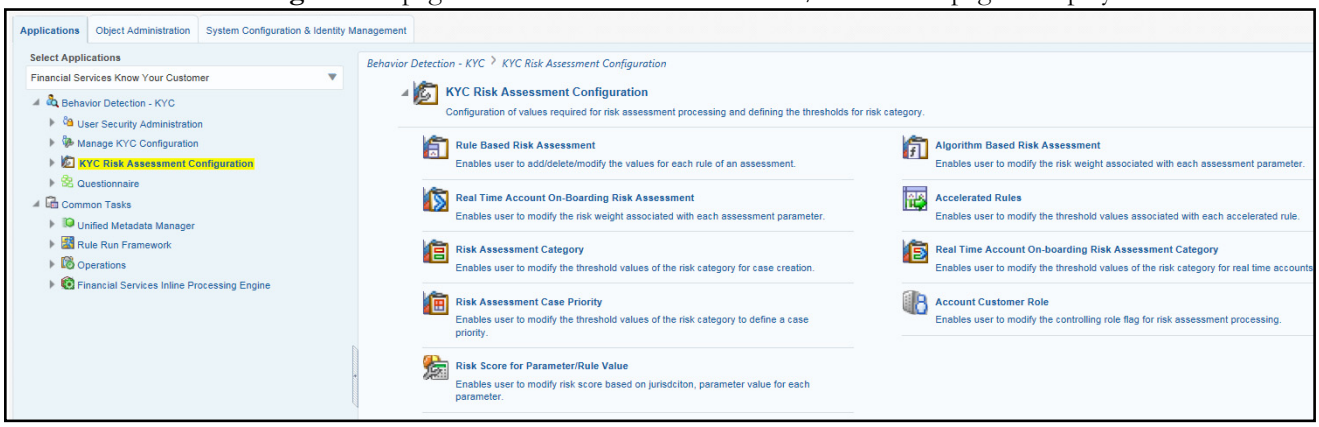


Figure 25. Risk Score for Parameter/Rule Value Page

15. Select the jurisdiction, risk scoring model type, and the newly added parameter.

Note: For Algorithm-based risk parameters, select Algorithm Based Assessment as the risk scoring model type.

16. Click **Auto-Populate** to get all the code values for the new parameter with the minimum risk score. To change the risk score, select the check box of the parameter that you want to change and enter the new risk score.

Note: After the initial preparation of the metadata, such as creating a new risk parameter, defining the risk weights, and defining the risk scores, you need to define a rule for the new risk parameter.

17. In the KYC home page, click **Financial Services Inline Processing Engine** in the LHS menu.

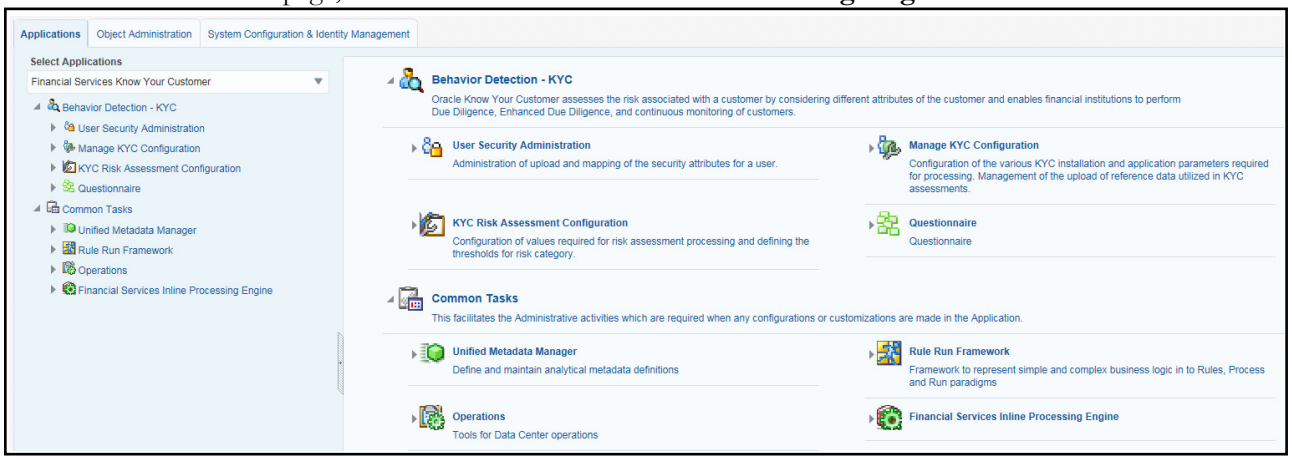


Figure 26. Financial Services Inline Processing Engine Page

18. Click **Inline Processing** in the RHS menu. The *Inline Processing* page is displayed.

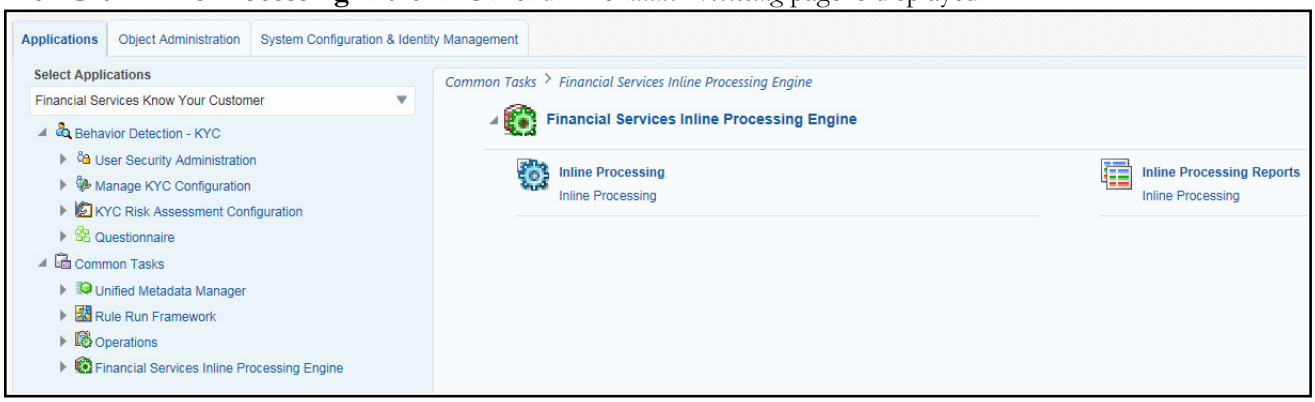


Figure 27. Inline Processing Page

19. Add a business entity on top of the `PARAM_RISK_SCORE_JRSDN` table in IPE. For example, Country of Birth. This is required because for every new risk parameter, you must indicate the source from where the risk score is derived or picked.

    To add a business entity, follow these steps:

    a. Click the **Business Entities** sub-menu in the **Association and Configuration** menu.

    b. Select the Entity Name as `PARAM_RISK_SCORE_JRSDN`.

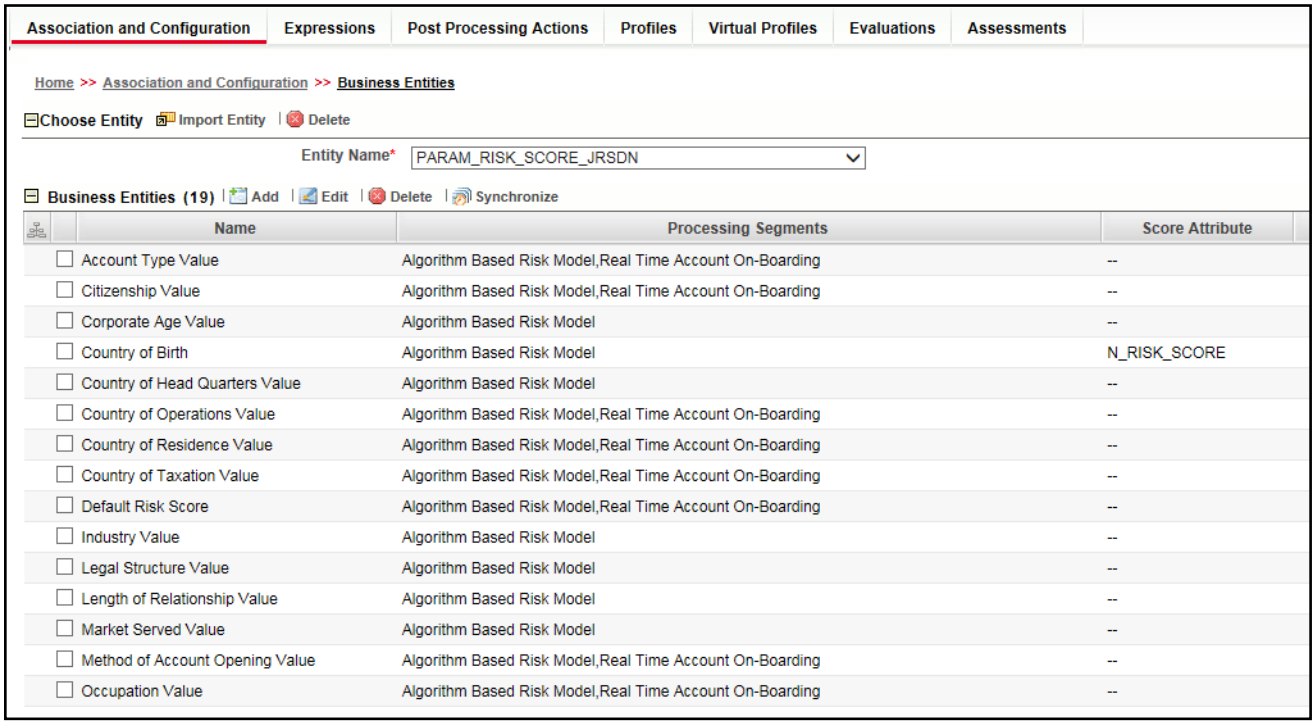


Figure 28. Business Entities Sub-Menu

    c. Click **Add**.

    d. Enter the name, processing segment, and score attribute for the business entity.

Note: For Algorithm-based risk parameters, select Algorithm Based Risk Model as the Processing Segment and N_RISK_SCORE as the set score attribute.

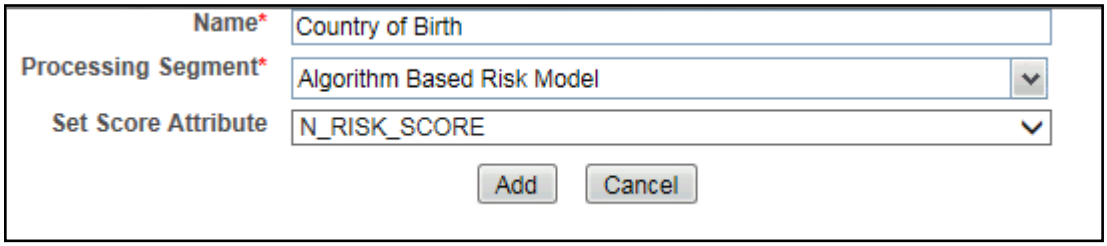


Figure 29. Adding a Business Entity

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

20. Add the following joins in IPE from the Inline Datasets sub-menu in the Association and Configuration menu:

- Algorithm-based Risk Scoring to Country of Birth: This is required to associate the risk parameter column of these two tables.
- Customer Processing to Country of Birth: This is required to associate the customer data of the new parameter to the risk score parameter table.

To create a join for Algorithm-based Risk Scoring to Country of Birth, follow these steps:

a. In the *Inline Datasets* page, click **Add**.

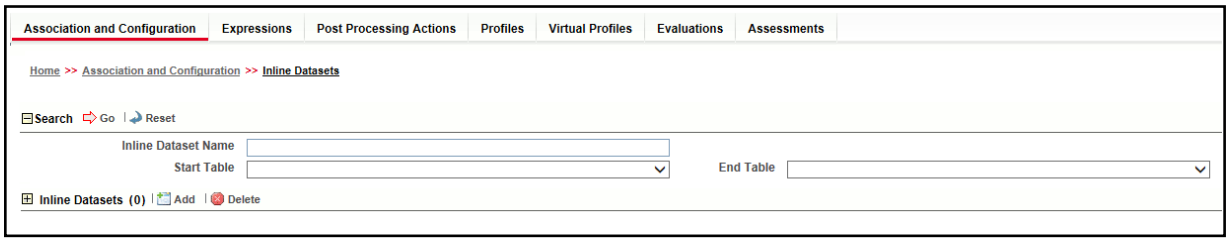


Figure 30. Inline Datasets Sub-Menu

b. Enter a name for the inline dataset.

c. In the Start Table field, select **Algorithm Based Risk Scoring**.

d. In the End Table field, select **Country of Birth**. This is the new business entity that we have created in step 19.

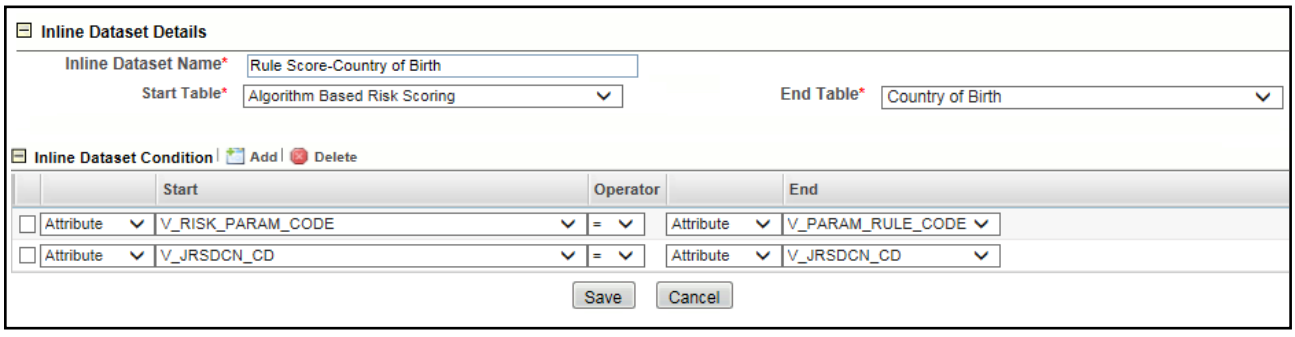


Figure 31. Adding an Inline Dataset

e. Click **Add**.

f. Select the values for the dataset condition as shown in the figure.

g. Click **Save**. The new dataset is added to the list of Inline Datasets in the Inline Datasets page.

Note: To view the results of the newly added values, use Search.

21. Add a traversal path for each join defined in the Inline Datasets sub-menu. For example, Customer Processing to Customer Account Processing through Algorithm Based Risk Scoring.

    To add a traversal path, follow these steps:

    a. Click the **Traversal Paths** sub-menu in the **Association and Configuration** menu.

    b. In the *Traversal Paths* page, click **Add**.

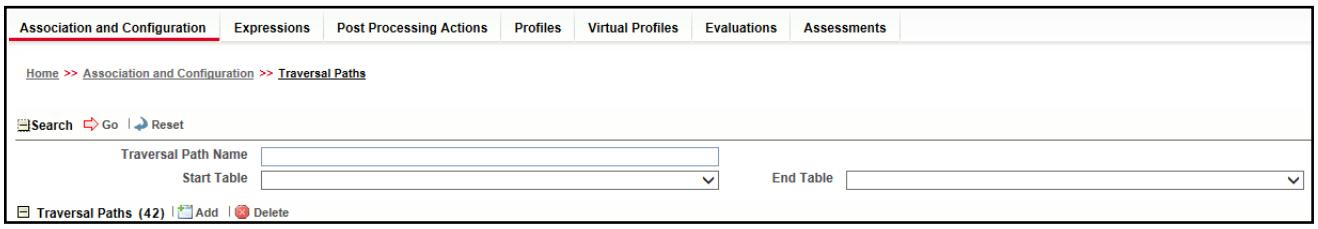


Figure 32. Traversal Paths Sub-Menu

c. Enter a name for the traversal path.

d. In the Start Table field, select Customer Processing.

e. In the End Table field, select Account Processing.

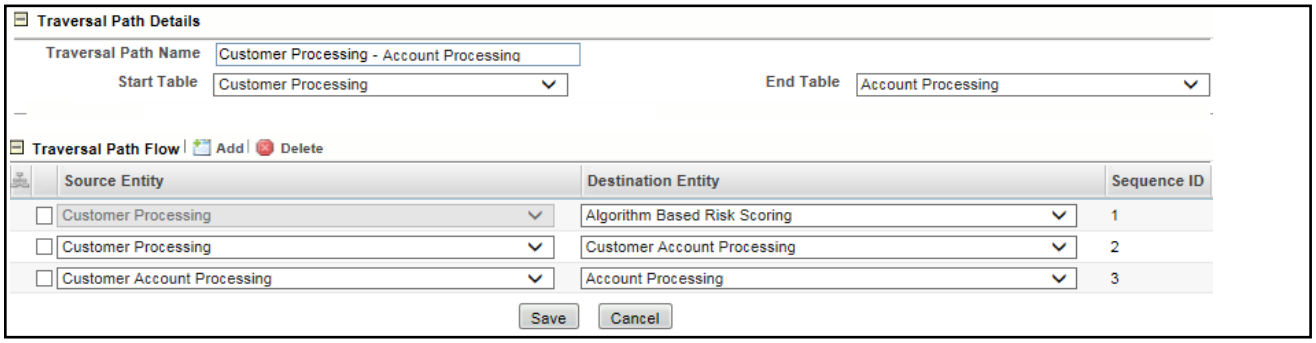


Figure 33. Adding a Traversal Path

f. Click **Add**.

g. Select the values for the traversal path flow as shown in the figure.

h. Click **Save**. The new path is added to the list of traversal paths in the Traversal Paths page.

For more information on the datasets and traversal paths used in KYC, see *Parameter Details*.

Note: The first two rows (joins) are mandatory. The remaining joins differ based on where the new parameter is stored.

Note: If the start table is Customer Processing, as in the above figure, there are usually three joins. More joins may need to be added based on how many tables data is spread across.

22. Add an Expression on the risk score column of the newly created business entity which is to be scored as a risk parameter from the Expressions menu. Two expressions need to be created:

- The first expression is for the column which holds the value of the new risk parameter
- The second expression is for the calculations that are needed to derive the risk score

Note: The business entity used in this example is Method of Account Opening.

To add an expression, follow these steps:

a. Click the **Expressions** menu.

b. In the *Expressions* page, click **Add**.

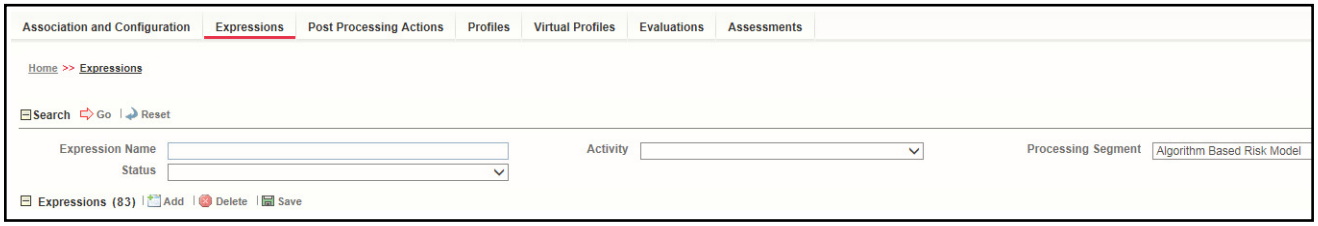


Figure 34. Expressions Menu

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

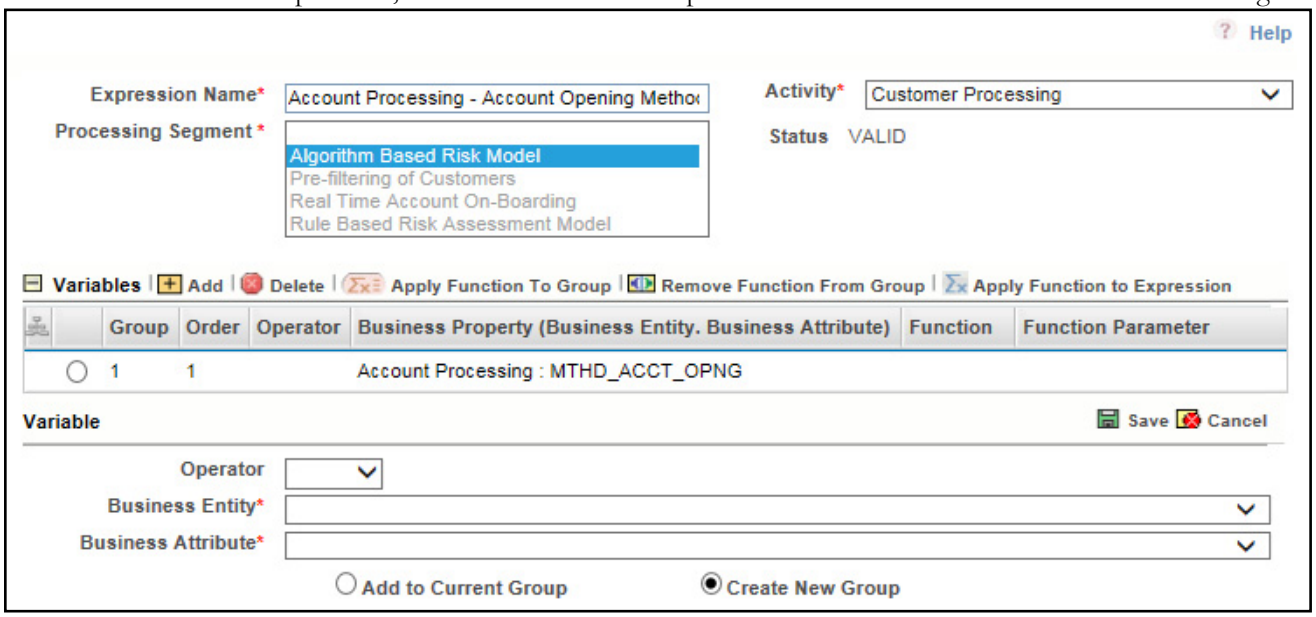


Figure 35. Adding the First Expression

d. To add a variable for the first expression, click **Add**.

e. Select the business entity and the business attribute where the value of the new parameter resides.

f. Click **Save**. The variable is displayed.

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

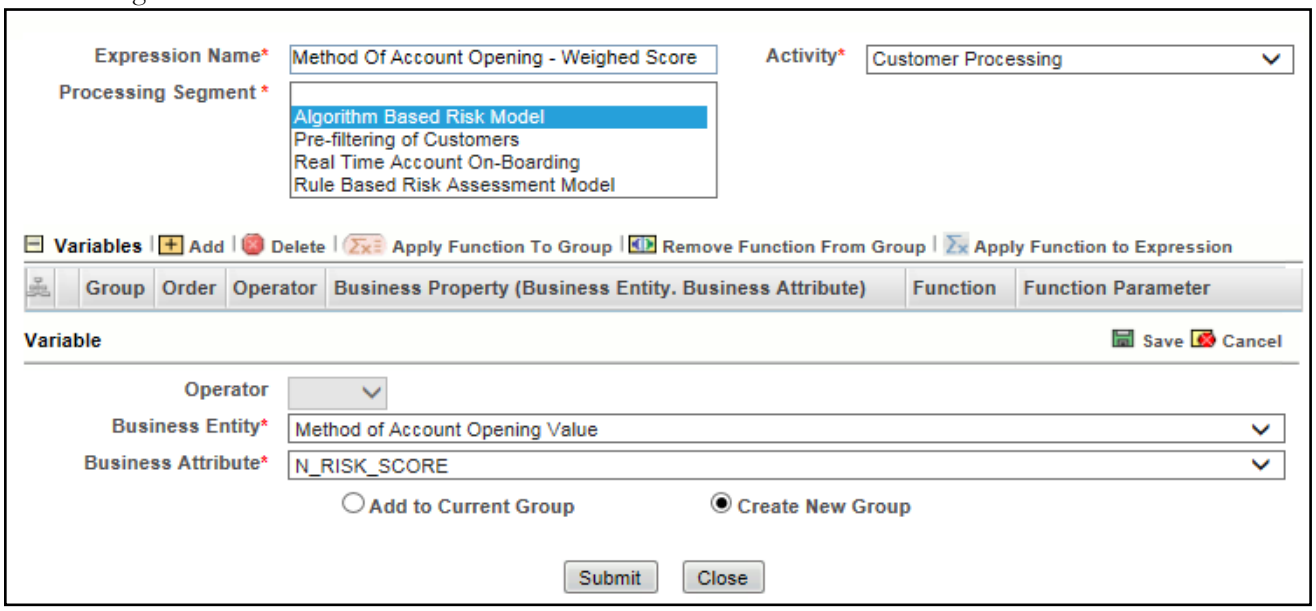


Figure 36. Adding the Second Expression

h. To add a variable for the second expression, click **Add**. For the second expression, we need to add two variables: one variable is the column which holds the risk score of the parameter, and the other variable is the column which holds the risk weight for the parameter.

i. For the first variable, select the values according to the Variable section in the above figure and click **Save**. The variable is displayed. For the second variable, select the values according to the below figure and click **Save**. The variable is displayed.

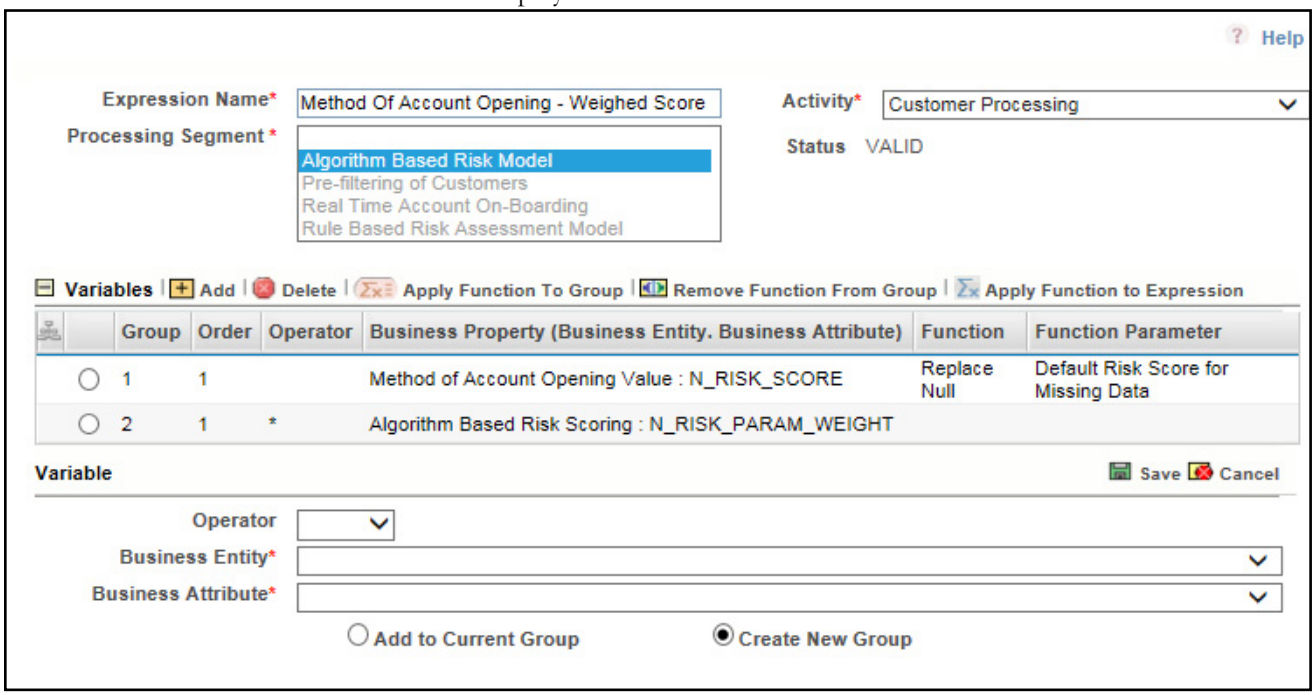


Figure 37. Adding the Second Expression - Both Variables Displayed

j. Select the Group 1 radio button.

k. Click **Apply Function To Group**.

l. In the Apply Function To Group section, select the values according to the below figure and click **Save**.

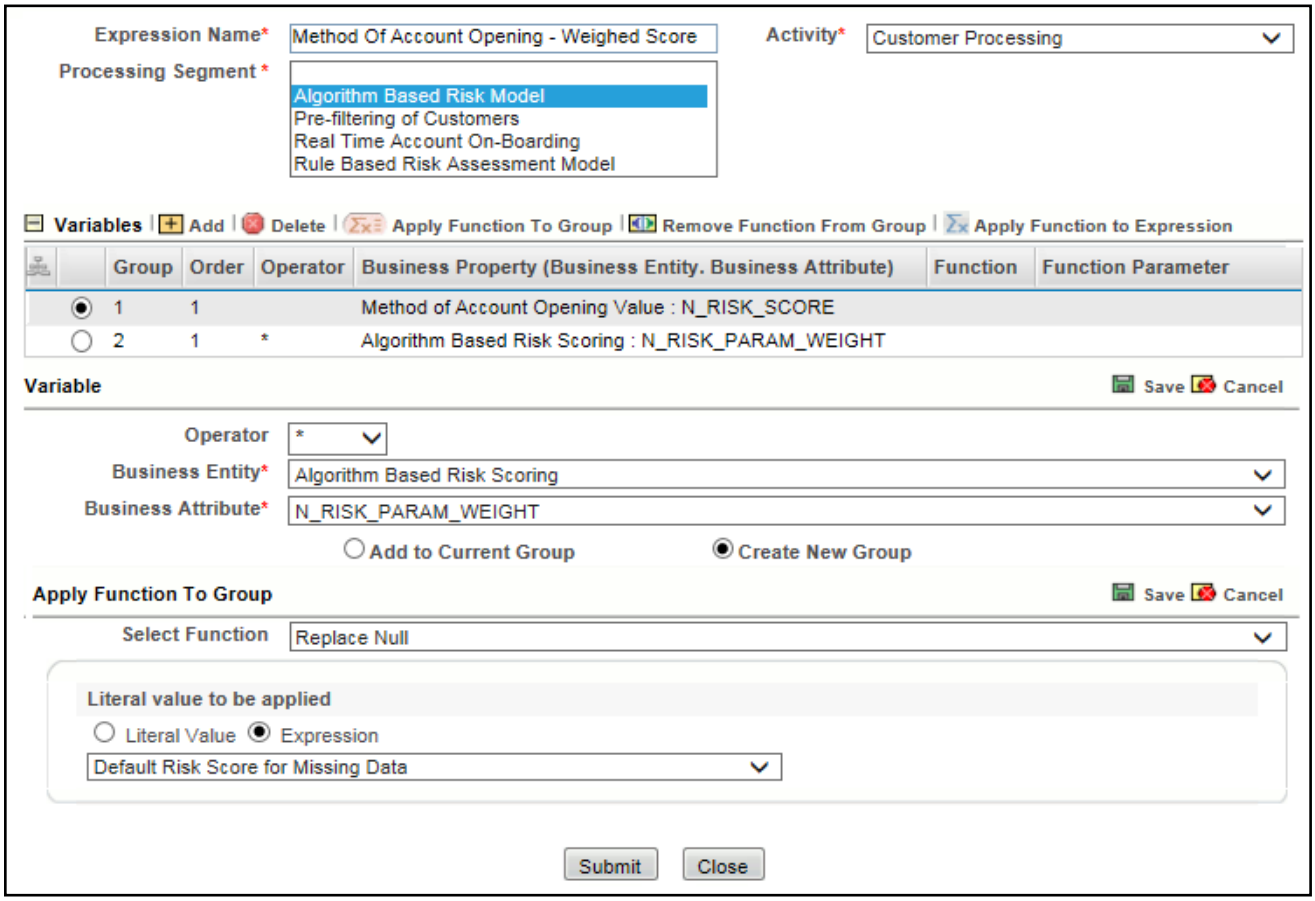


Figure 38. Adding the Second Expression - Apply Function To Group

m. Select the Group 1 radio button.

n. Click **Apply Function To Group**.

o. In the Apply Function To Group section, select the values according to the below figure and click **Save**.

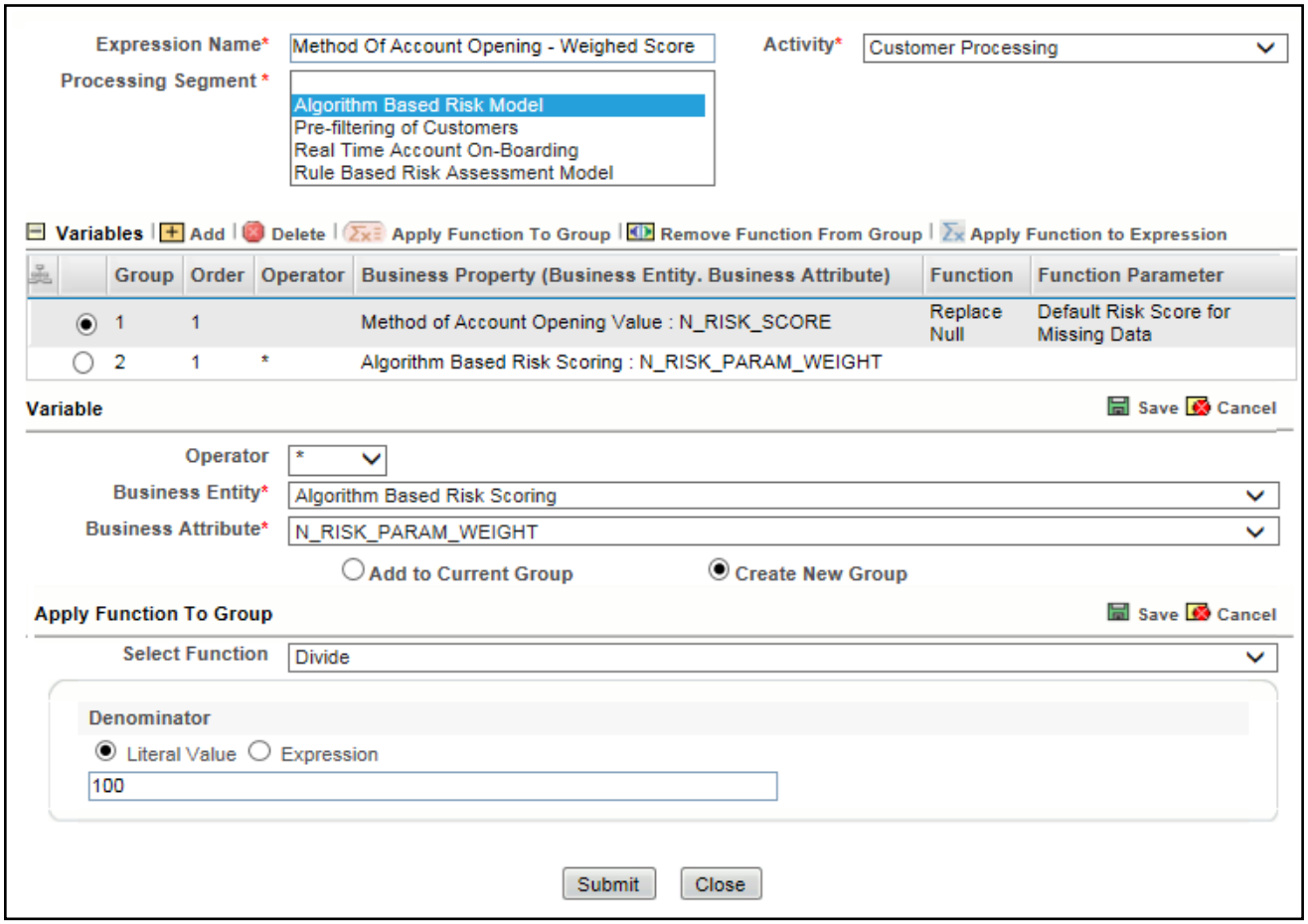


Figure 39. Adding the Second Expression - Apply Function To Group

p. Click **Submit**. The new expression is added to the list of expressions in the Expressions page.

23. Create an evaluation for the new risk parameter from the Evaluations Menu, with the same filter conditions as that of the other parameters, such as the filter details and the score type.

    To add an evaluation, follow these steps:

    a. Click the **Evaluations** menu.

    b. In the *Evaluations* page, click **Add**.

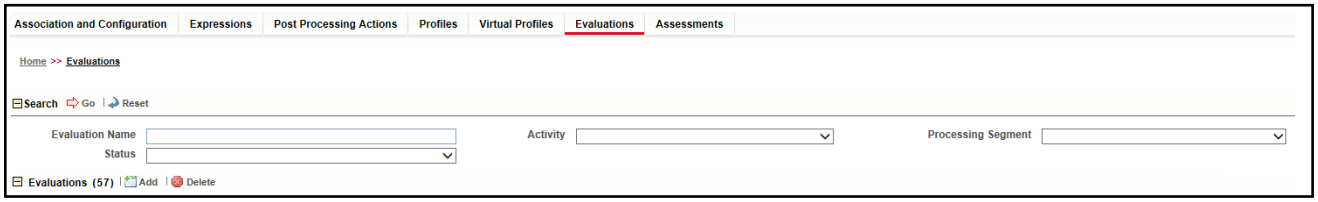


Figure 40. Evaluations Menu

c. Enter a name for the evaluation.

d. Select the Activity and Processing Segment field according to the below figure.

Note: For algorithm-based risk evaluations, the join type is always left. This allows the application to provide a default risk score.

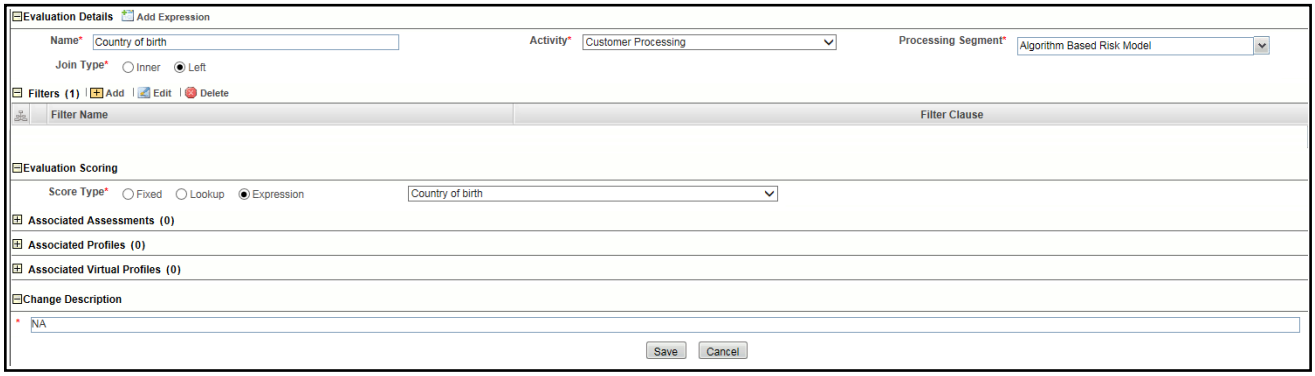


Figure 41. Adding an Evaluation

e. To add filters for the evaluation, click **Add**. You need to add two filters.

f. For the first filter, select the values according to the below figure and click **Save**:

Figure 42. Adding an Evaluation - First Filter

Note: In the Literal Value field, select the same value as provided in the F_ENABLE parameter of the APPLN_RISK_RATING_PARAMS excel sheet during upload.

g. For the second filter, select the values according to the below figure and click **Save**:

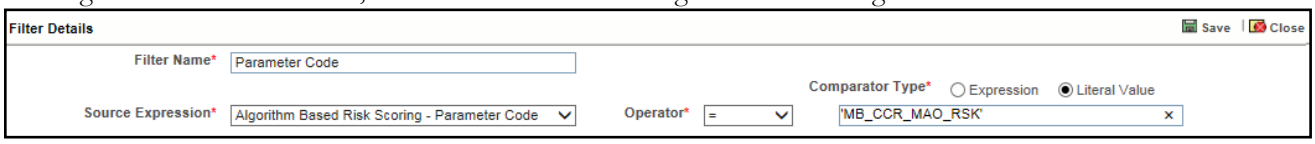


Figure 43. Adding an Evaluation - Second Filter

Note: In the Literal Value field, select the same value as provided in the V_RISK_PARAM_CODE parameter of the APPLN_RISK_RATING_PARAMS excel sheet during upload.

h. Select the expression that you have created for the calculation of the risk score.

i. Select the expression which holds data for the risk parameter in the Highlights section. This is required to get the actual value for every customer.

j. Click **Save**.

24. Map the evaluation to the existing assessment of the added parameter. To do this, run the following insert script:

```
insert into MAP_EVAL_RISK_ASSMNT_MODEL (N_EVAL_ID, N_EVAL_VRSN_NB, N_CNTRY_ID,
N_TABLE_BUS_ID, V_TABLE_PHY_NM, V_TABLE_BUS_NM, V_RISK_ASSMNT_MODEL, N_ASSMT_ID,
V_APP_ID, V_EVAL_NM, V_ACTV_FL, V_PARAM_RULE_CODE, V_CUST_TYPE_CD
```

The following are the expected values for the above script:

Parameter Name	Expected Value
N_EVAL_ID	The expected value can be retrieved by querying the `MAP_EVAL_RISK_ASSMNT_MODEL` table.
N_EVAL_VRSN_NB	0
N_CNTRY_ID	Null
N_TABLE_BUS_ID	Null
V_TABLE_PHY_NM	Null
V_TABLE_BUS_NM	Null
V_RISK_ASSMNT_MODEL	MB
N_ASSMT_ID	8000
V_APP_ID	OFS_KYC
V_EVAL_NM	<Name of the Evaluation>
V_ACTV_FL	Null
V_PARAM_RULE_CODE	<RULE CODE from APPL_RISK_RATING_PARAMS>
V_CUST_TYPE_CD	Null

25. Click **Save**.

Adding Risk Parameters for Rule-based Risk Assessments

To add risk parameters for algorithm-based risk assessments, follow these steps:

1. Navigate to the KYC home page.
2. Click **Manage KYC Configuration** in the LHS menu.

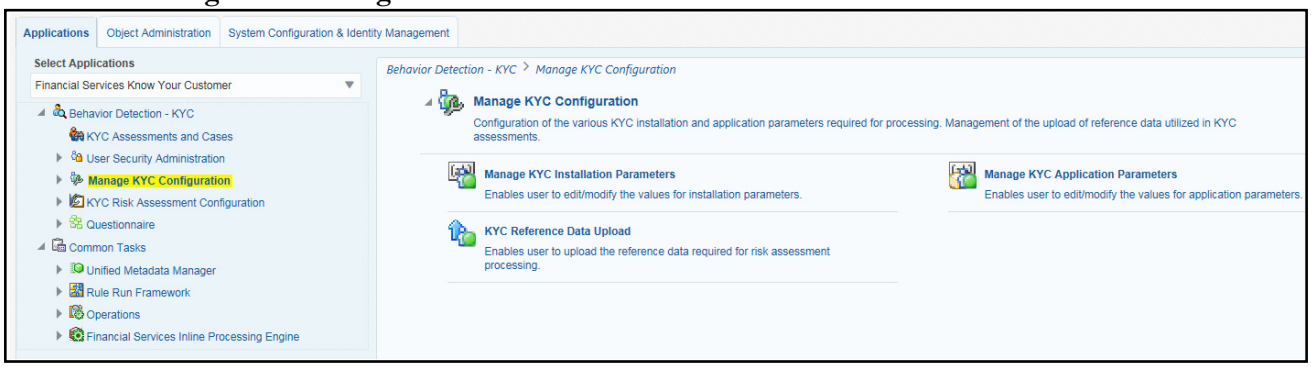


Figure 44. Manage KYC Configuration Page

3. Click **KYC Reference Data Upload** in the RHS menu. The *Administration* page is displayed.

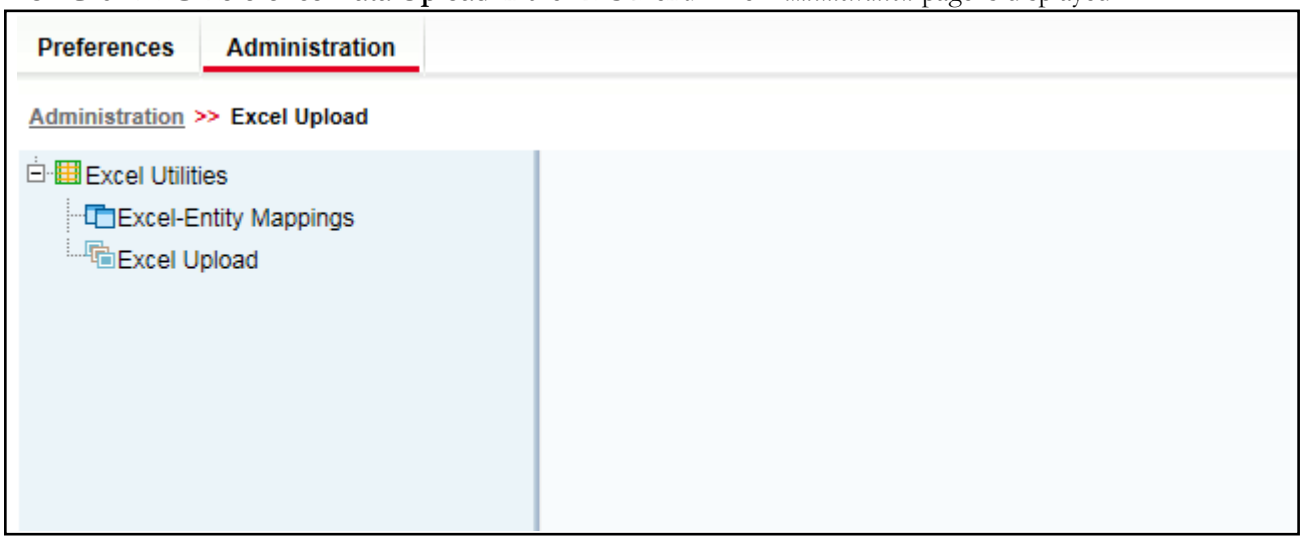


Figure 45. Administration Page

4. Click **Excel-Entity Mappings**. The *Excel-Entity Mappings* page is displayed.

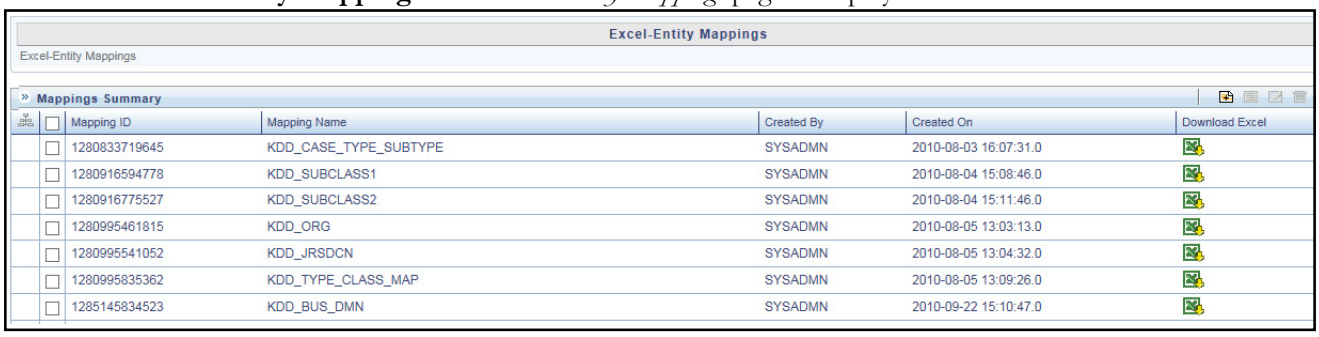


Figure 46. Excel-Entity Mappings Page

5. Download the `APPLN_RB_PROCESSING` metadata sheet and add the following details of the new risk parameter:

Table 20. Expected Values for APPLN_RB_PROCESSING

Parameter Name	Expected Value
V_RISK_ASSMT_MODEL	• For batch algorithm: The value must be RB. • For RAOR algorithm: The value must be RAORRB.
V_RB_RULE_CODE	• For batch algorithm: The value must be RB_CCR_<unique rule name code>. • For RAOR algorithm: The value must be OB_RB_CCR_<unique rule name code> **Note:** Scoring does not happen unless the rule name code is unique.
V_RB_RULE_DESC	For batch algorithm and RAOR algorithm: Enter a valid description for the rule.
F_ENABLE	For batch algorithm and RAOR algorithm: The value must be Y to consider the new parameter for risk scoring.

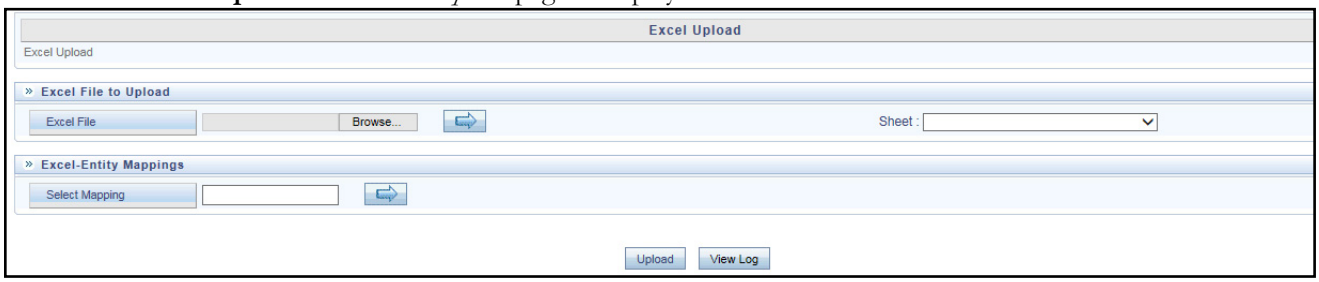
Table 20. Expected Values for APPLN_RB_PROCESSING

Parameter Name	Expected Value
V_CODE_SET	• For batch algorithm and RAOR algorithm: Provide an appropriate code set according to the KDD_CODE_SET_TRNLN.CODE_SET table. If the new parameter does not have a corresponding code set available, such as for range-based parameters, the code set needs to be manually added to the KDD_CODE_SET_TRNLN.CODE_SET table. **Note:** To identify if the new parameter (<table>.<column>) has a defined code set, see the standard values column for the tables and columns that you need to add as shown in the *Financial Services Data Model Reference Guide Volume 1*.
V_RULE_VAL_CODE	For batch algorithm and RAOR algorithm: Enter the values available in the code set.
V_JRSDCN_CD	For batch algorithm and RAOR algorithm: Provide the jurisdiction code for the new parameter. The code must be according to the values in the KDD_JRSDN table.
V_CUST_TYPE_CD	For batch algorithm and RAOR algorithm: Provide the customer codes for the parameter. The code must be one of the following: • IND: Individual • FIN: Financial Institution • ORG: Other Organization

Note: The mapped code value must be according to the code set available.

Note: During the excel upload, ensure that values are available for the above fields.

6. Click **Excel Upload**. The *Excel Upload* page is displayed.



7. Click **Browse.**
8. Select the APPLN_RISK_RATING_PARAMS metadata sheet and click the arrow. The sheet name appears in the Sheet field and a preview of the sheet details appear below.
9. In the Select Mapping field, click the arrow and select the template which contains data for the APPLN_RISK_RATING_PARAMS sheet.
10. Click **Upload**.

11. In the KYC home page, click **KYC Risk Assessment Configuration** in the LHS menu.

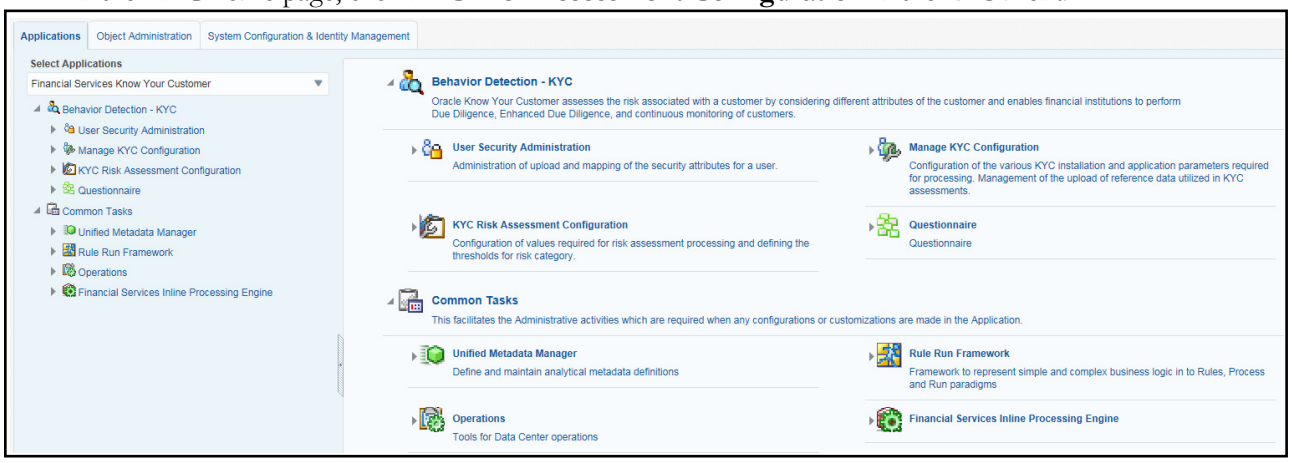


Figure 47. KYC Risk Assessment Configuration Page

12. Click **Rule Based Risk Assessment** in the RHS menu. The *Rule Based Risk Assessment* page is displayed.

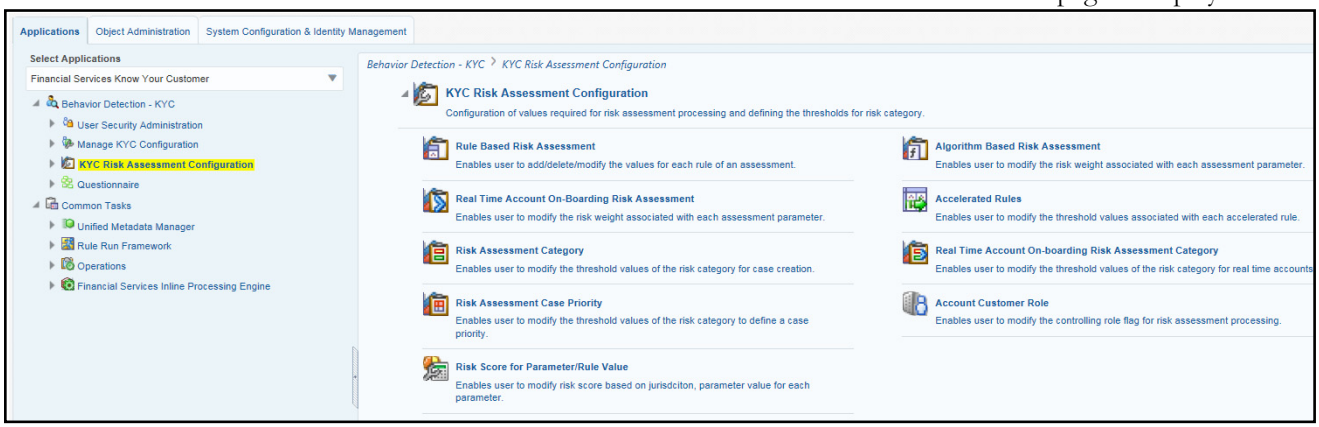


Figure 48. Rule Based Risk Assessment Page

13. Select the jurisdiction and make appropriate changes to the weight.

Note: The weights of all risk parameters must add to 100 for a combination of jurisdiction and customer type.

14. To view the risk score of the new parameter, click **Risk Score for Parameter/Rule Value** in the **KYC Risk Assessment Configuration** page. The Risk Score for Parameter/Rule Value page is displayed.

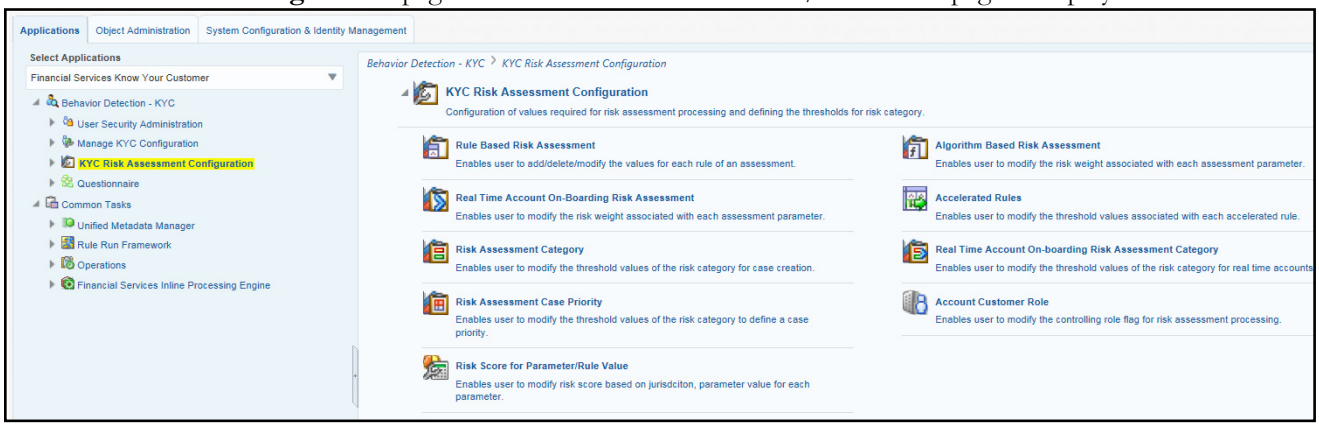


Figure 49. Risk Score for Parameter/Rule Value Page

15. Select the jurisdiction, risk scoring model type, and the newly added parameter.

Note: For Rule-based risk parameters, select Rule Based Assessment as the risk scoring model type.

16. Click **Auto-Populate** to get all the code values for the new parameter with the minimum risk score. To change the risk score, select the check box of the parameter that you want to change and enter the new risk score.

Note: After the initial preparation of the metadata, such as creating a new risk parameter, defining the risk weights, and defining the risk scores, you need to define a rule for the new risk parameter.

17. In the KYC home page, click **Financial Services Inline Processing Engine** in the LHS menu.

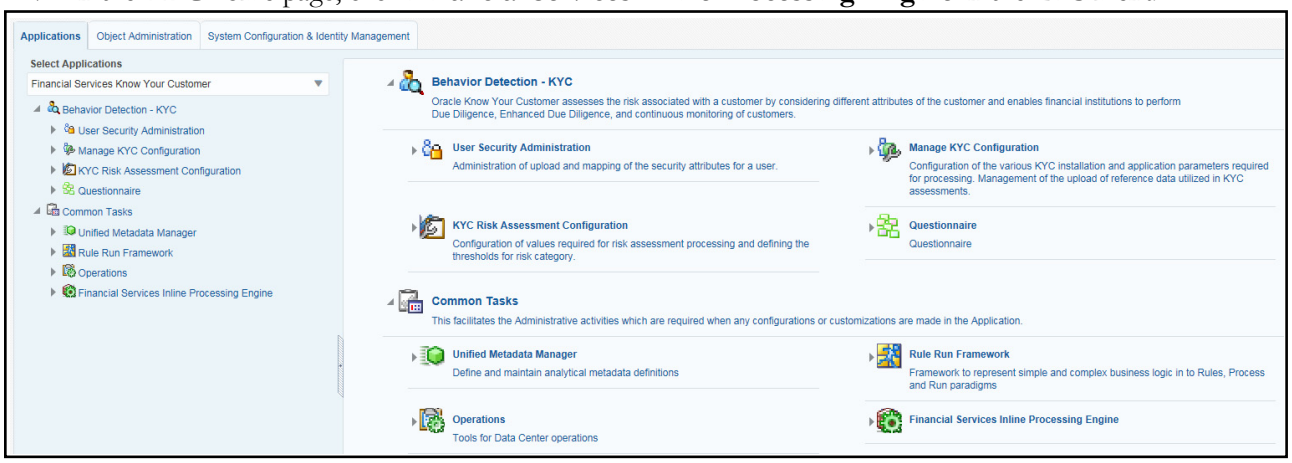


Figure 50. Financial Services Inline Processing Engine Page

18. Click **Inline Processing** in the RHS menu. The *Inline Processing* page is displayed.

Figure 51. Inline Processing Page

19. Add a business entity on top of the `PARAM_RISK_SCORE_JRSDN` table in IPE. For example, Country of Birth.

    To add a business entity, follow these steps:

    a. Click the **Business Entities** sub-menu in the **Association and Configuration** menu.

    b. Select the Entity Name as `PARAM_RISK_SCORE_JRSDN`.

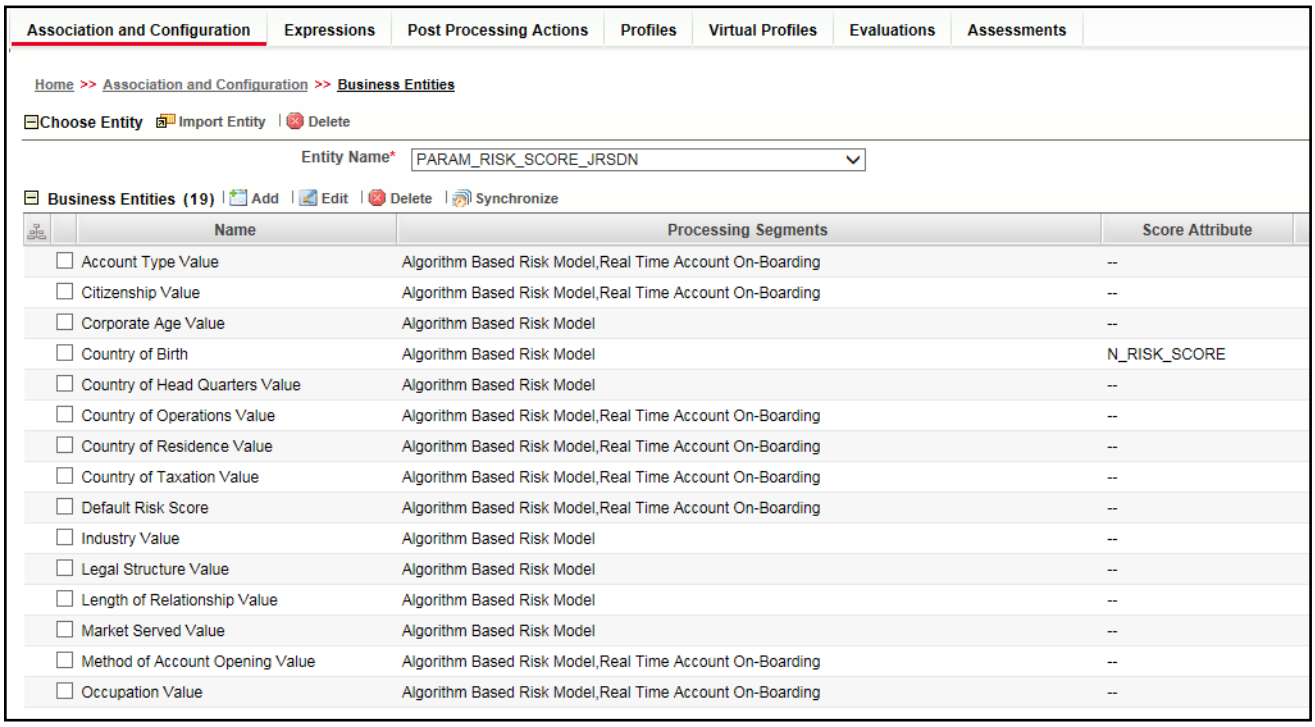
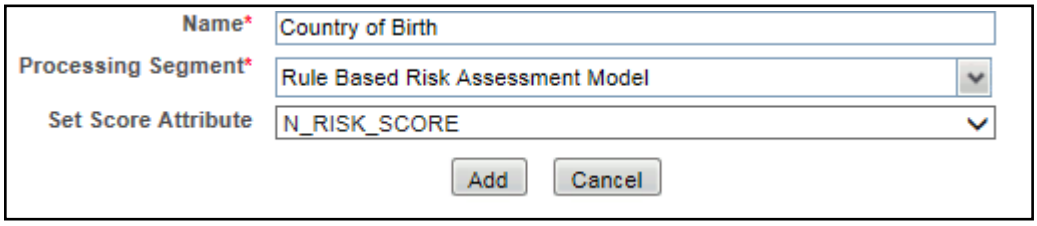


Figure 52. Business Entities Sub-Menu

c. Click **Add**.

d. Enter the name, processing segment, and score attribute for the business entity.

Note: For Rule-based risk parameters, select Rule Based Risk Assessment Model as the Processing Segment and N_RISK_SCORE as the set score attribute.



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

20. Add the following joins in IPE from the Inline Datasets sub-menu in the Association and Configuration menu:

- Rule-based Risk Scoring to Country of Birth (New Parameter virtual table). This is required to associate the risk parameter column of these two tables.
- Customer Processing to Country of Birth (New Parameter virtual table). This is required to associate the customer data of the new parameter to the risk score parameter table.

To create a join for Rule-based Risk Scoring to Country of Birth, follow these steps:

a. In the *Inline Datasets* page, click **Add**.

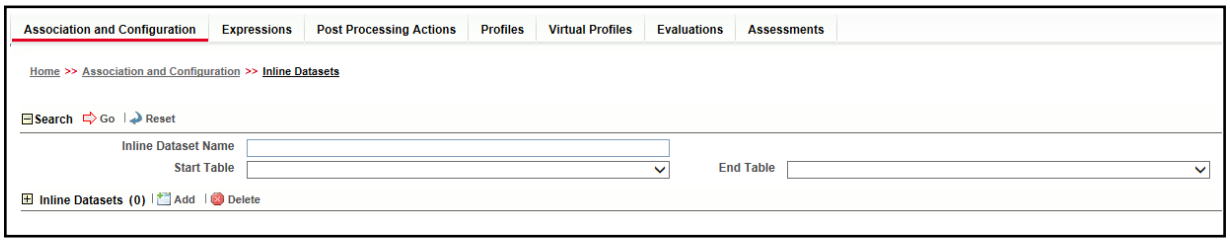


Figure 53. Inline Datasets Sub-Menu

b. Enter a name for the inline dataset.

c. In the Start Table field, select **Rule Based Risk Assessment**.

d. In the End Table field, select **Country of Birth**. This is the new business entity that we have created in step 19.

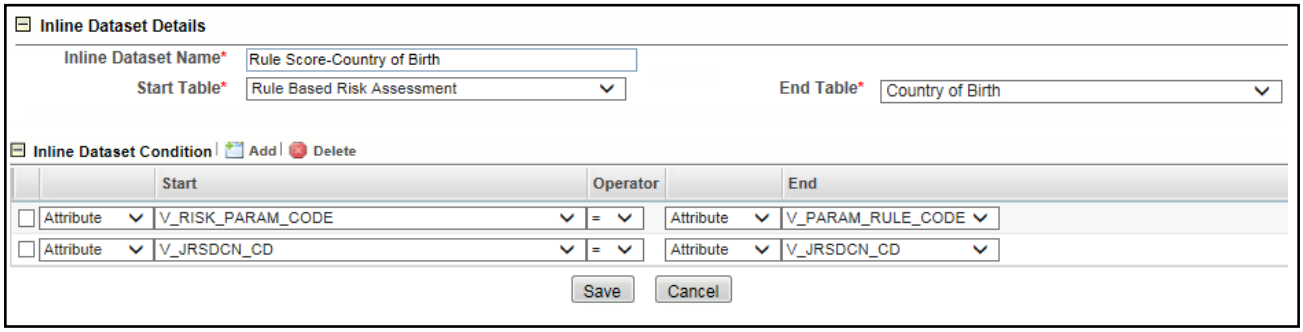


Figure 54. Adding an Inline Dataset

e. Click **Add**.

f. Select the values for the dataset condition as shown in the figure.

g. Click **Save**. The new dataset is added to the list of Inline Datasets in the Inline Datasets page.

Note: To view the results of the newly added values, use Search.

21. Add a traversal path for each join defined in the Inline Datasets sub-menu. For example, Customer Processing to Rule Based Risk Assessment through the Country of birth.

    To add a traversal path, follow these steps:

    a. Click the **Traversal Paths** sub-menu in the **Association and Configuration** menu.

    b. In the *Traversal Paths* page, click **Add**.

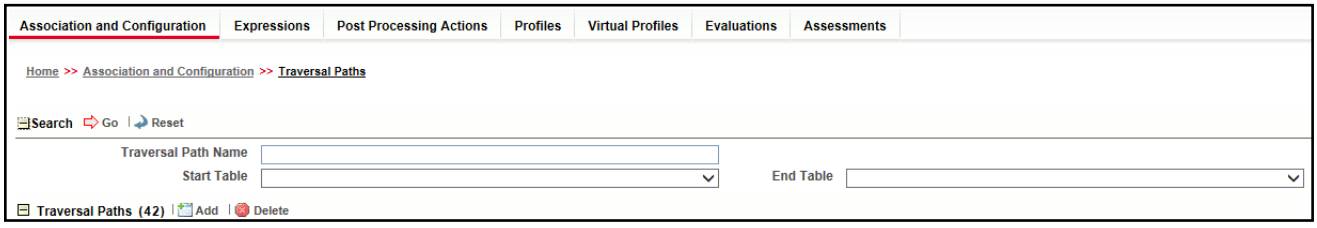


Figure 55. Traversal Paths Sub-Menu

c. Enter a name for the traversal path.

d. In the Start Table field, select Customer Processing.

e. In the End Table field, select Rule Based Risk Assessment.

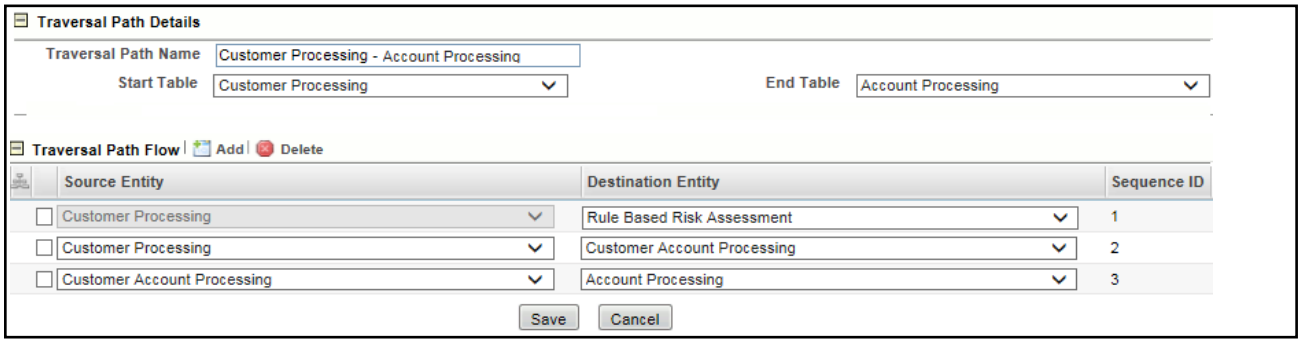


Figure 56. Adding a Traversal Path

f. Click **Add**.

g. Select the values for the traversal path flow as shown in the figure.

h. Click **Save**. The new path is added to the list of traversal paths in the Traversal Paths page.

For more information on the datasets and traversal paths used in KYC, see *Parameter Details*.

22. Add an Expression on the risk score column of the newly created business entity which is to be scored as a risk parameter from the Expressions menu. Two expressions need to be created:

- The first expression is for the column which holds the value of the new risk parameter
- The second expression is for the calculations that are needed to derive the risk score

Note: The business entity used in this example is Method of Account Opening.

To add an expression, follow these steps:

a. Click the **Expressions** menu.

b. In the *Expressions* page, click **Add**.

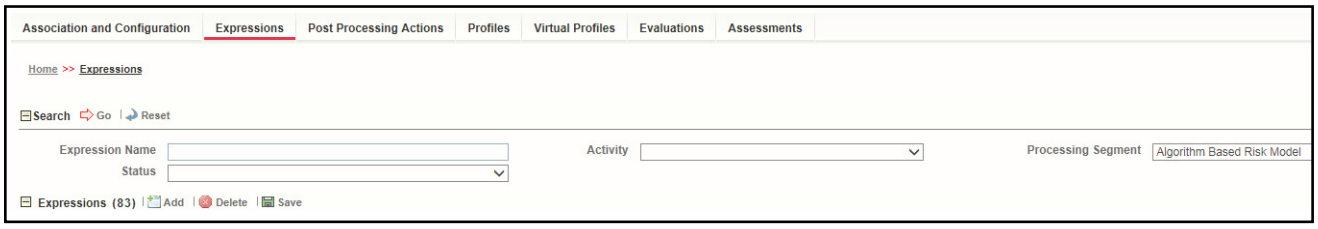


Figure 57. Expressions Menu

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

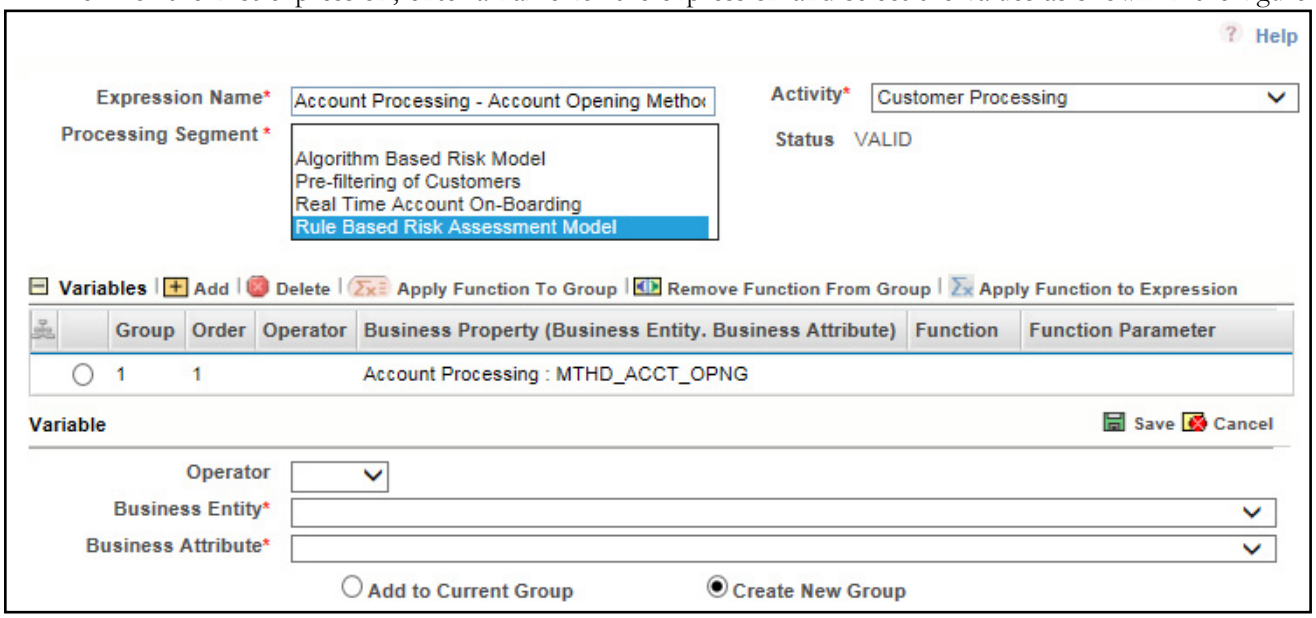


Figure 58. Adding the First Expression

d. To add a variable for the first expression, click **Add**.

e. Select the business entity and the business attribute where the value of the new parameter resides.

f. Click **Save**. The variable is displayed.

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

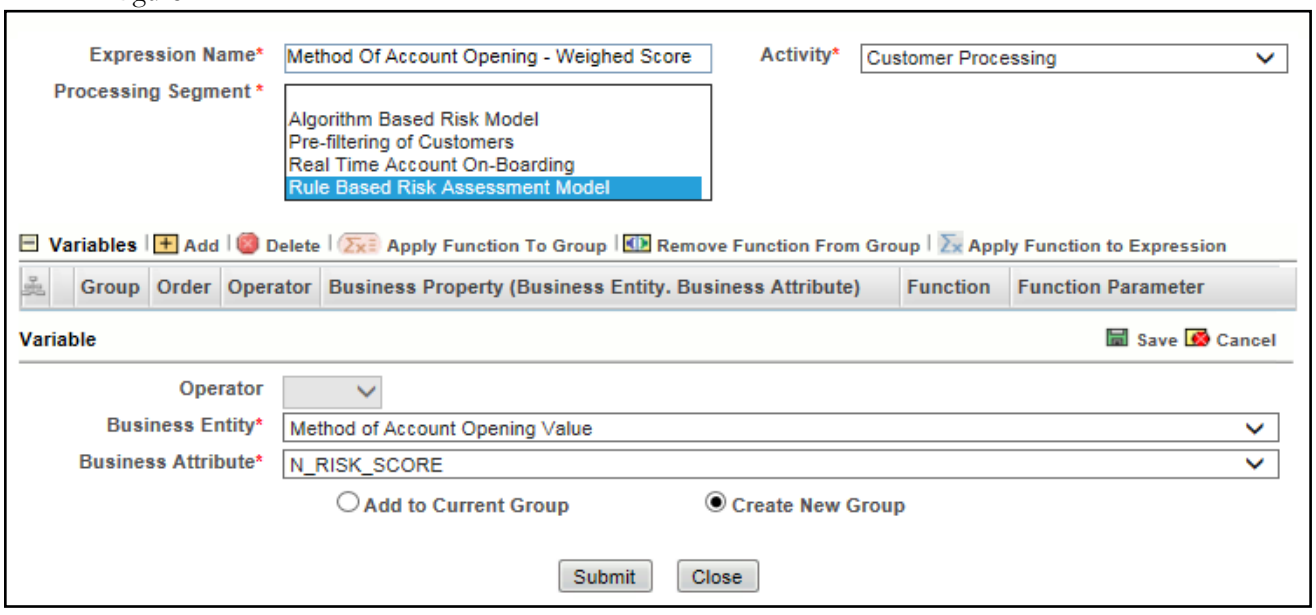


Figure 59. Adding the Second Expression

h. To add a variable for the second expression, click **Add**. For the second expression, we need to add two variables: one variable is the column which holds the risk score of the parameter, and the other variable is the column which holds the risk weight for the parameter.

i. For the first variable, select the values according to the Variable section in the above figure and click **Save**. The variable is displayed. For the second variable, select the values according to the below figure and click **Save**. The variable is displayed.

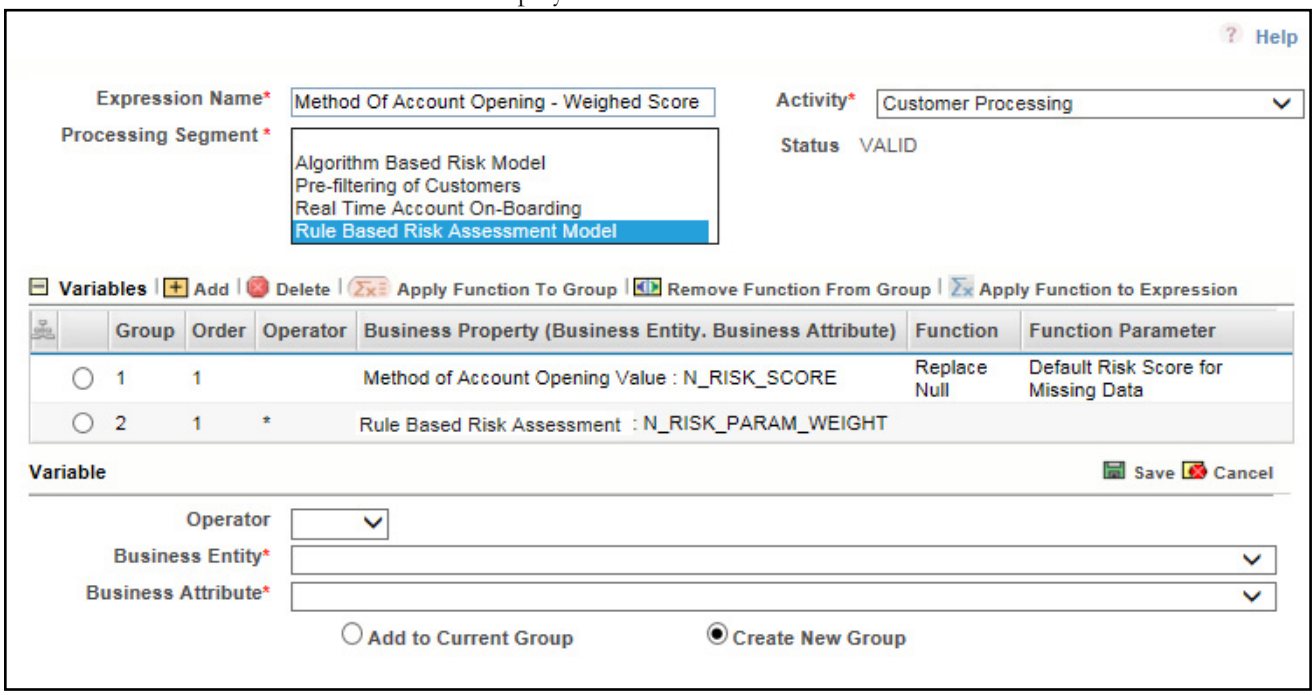


Figure 60. Adding the Second Expression - Both Variables Displayed

j. Select the Group 1 radio button.

k. Click **Apply Function To Group**.

l. In the Apply Function To Group section, select the values according to the below figure and click **Save**.

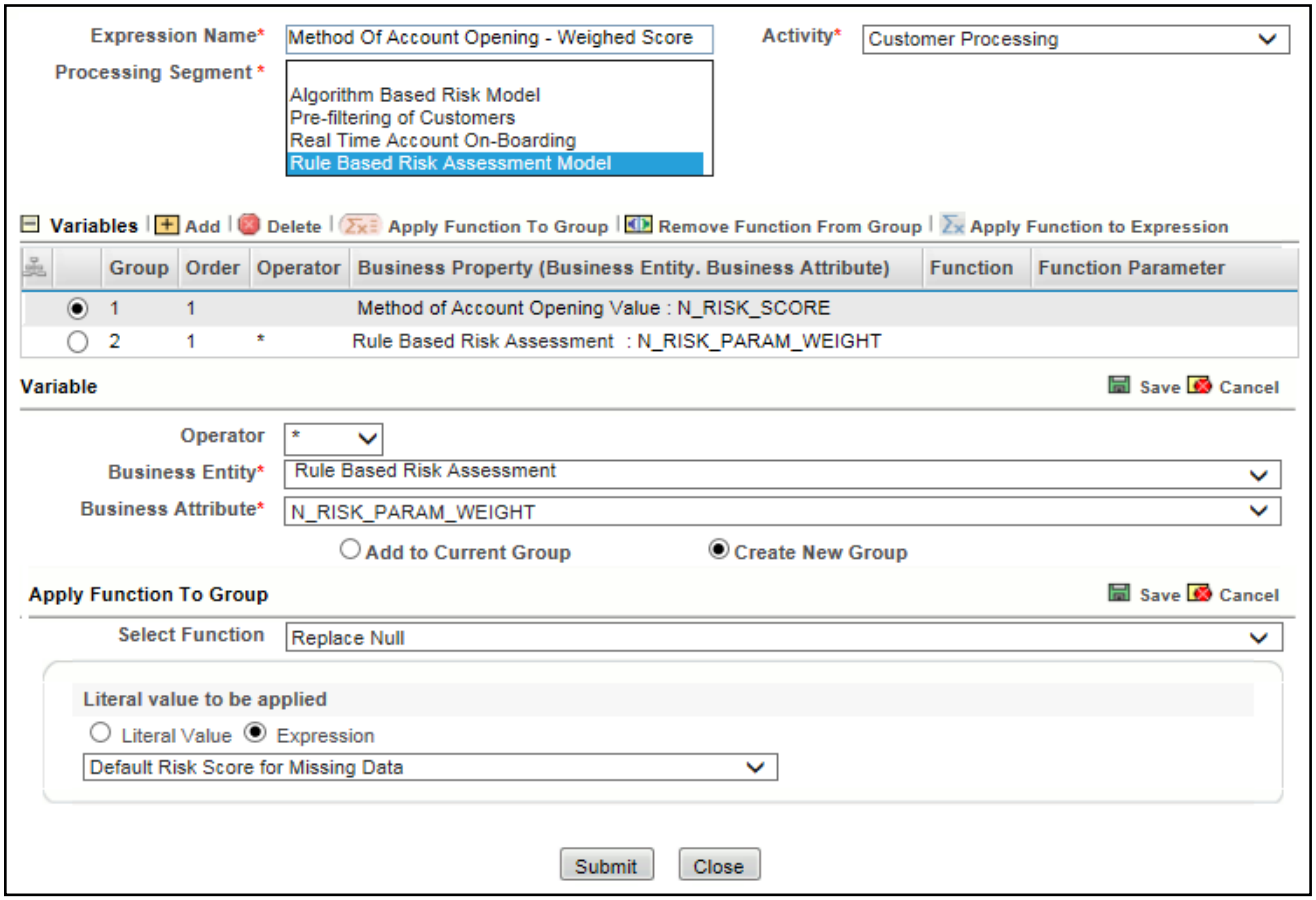


Figure 61. Adding the Second Expression - Apply Function To Group

m. Select the Group 1 radio button.

n. Click **Apply Function To Group**.

o. In the Apply Function To Group section, select the values according to the below figure and click **Save**.

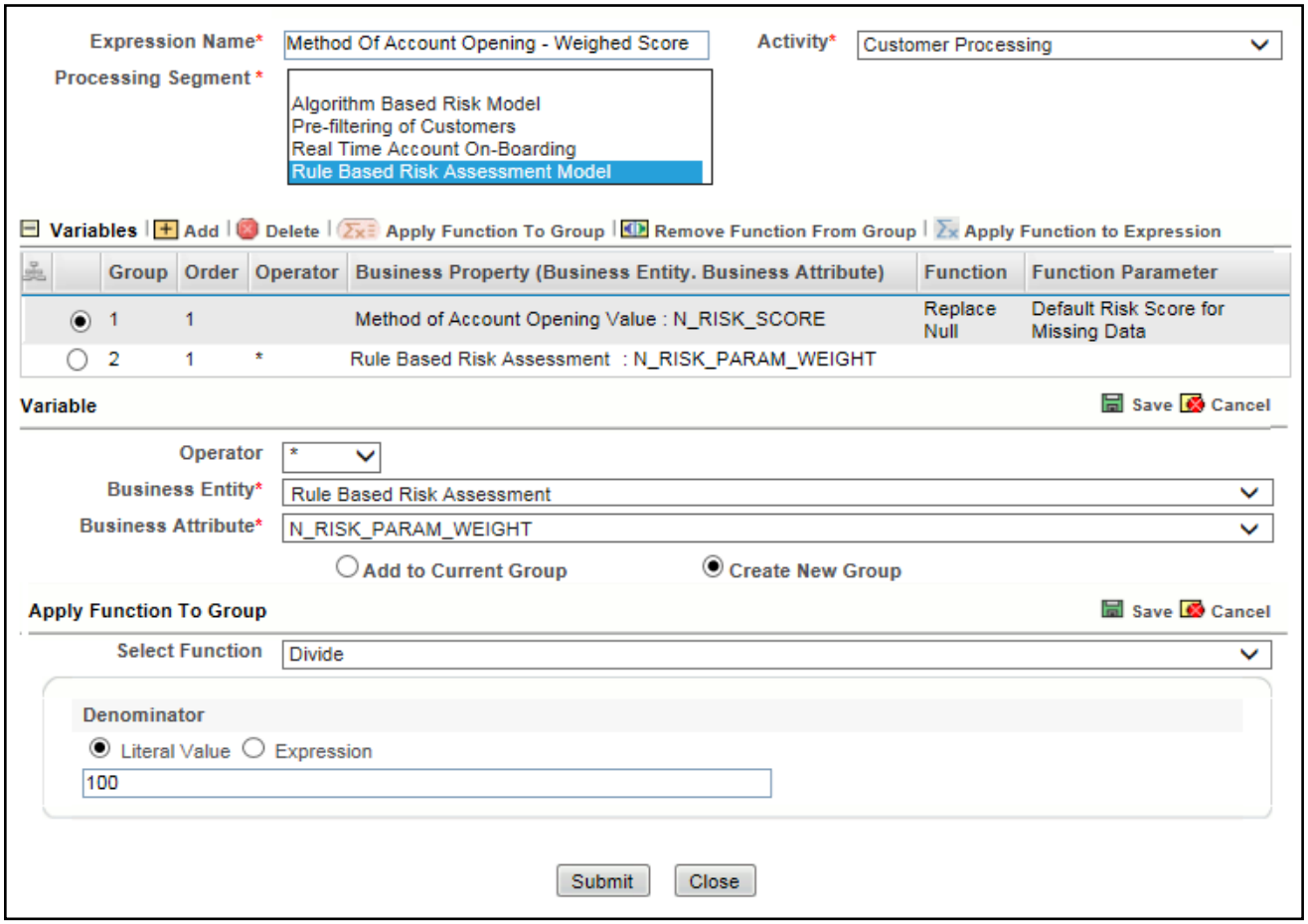


Figure 62. Adding the Second Expression - Apply Function To Group

p. Click **Submit**. The new expression is added to the list of expressions in the Expressions page.

23. Create an evaluation for the new risk parameter from the Evaluations Menu, with the same filter conditions as that of the other parameters, such as the filter details and the score type.

    To add an evaluation, follow these steps:

    a. Click the **Evaluations** menu.

    b. In the *Evaluations* page, click **Add**.

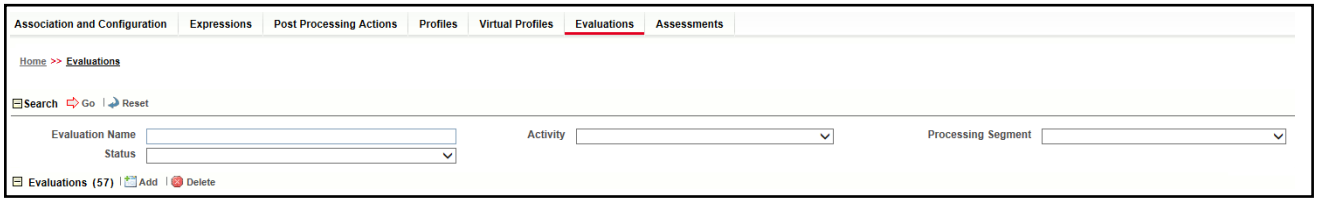


Figure 63. Evaluations Menu

c. Enter a name for the evaluation.

d. Select the Activity and Processing Segment field according to the below figure.

Note: For algorithm-based risk evaluations, the join type is always left. This allows the application to provide a default risk score.

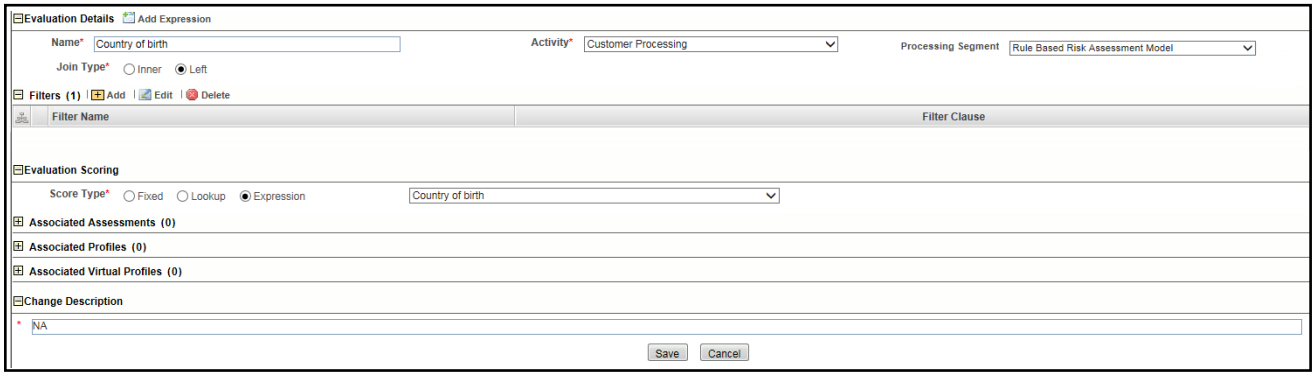


Figure 64. Adding an Evaluation

e. To add filters for the evaluation, click **Add**. You need to add two filters.

f. For the first filter, select the values according to the below figure and click **Save**:

Figure 65. Adding an Evaluation - First Filter

Note: In the Literal Value field, select the same value as provided in the F_ENABLE parameter of the APPLN_RB_PROCESSING excel sheet during upload.

g. For the second filter, select the values according to the below figure and click **Save**:

Figure 66. Adding an Evaluation - Second Filter

Note: In the Literal Value field, select the same value as provided in the V_RB_RULE_CODE parameter of the APPLN_RB_PROCESSING excel sheet during upload.

h. Select the expression that you have created for the calculation of the risk score.

i. Select the expression which holds data for the risk parameter in the Highlights section. This is required to get the actual value for every customer.

j. Click **Save**.

24. Map the evaluation to the existing assessment of the added parameter. To do this, run the following insert script:

```
insert into MAP_EVAL_RISK_ASSMNT_MODEL (N_EVAL_ID, N_EVAL_VRSN_NB, N_CNTRY_ID,
N_TABLE_BUS_ID, V_TABLE_PHY_NM, V_TABLE_BUS_NM, V_RISK_ASSMNT_MODEL, N_ASSMT_ID,
V_APP_ID, V_EVAL_NM, V_ACTV_FL, V_PARAM_RULE_CODE, V_CUST_TYPE_CD
```

The following are the expected values for the above script:

Parameter Name	Expected Value
N_EVAL_ID	<Evaluation ID>
N_EVAL_VRSN_NB	0
N_CNTRY_ID	Null
N_TABLE_BUS_ID	Null
V_TABLE_PHY_NM	Null
V_TABLE_BUS_NM	Null
V_RISK_ASSMNT_MODEL	RB
N_ASSMT_ID	6684
V_APP_ID	OFS_KYC
V_EVAL_NM	<Name of the Evaluation>
V_ACTV_FL	Null
V_PARAM_RULE_CODE	<RULE CODE from APPL_RISK_RATING_PARAMS>
V_CUST_TYPE_CD	Null

25. Click **Save**.

CHAPTER 6 Setting up Questionnaires for KYC

This chapter discusses the following topics:

About Questionnaires

As part of onboarding a customer, there is a need to assess the risk of the customer before they are on board the bank. The onboarding service does two things: gather customer data based on the anticipated behavior of the customer, and calculate the risk score of the customer. This helps in deciding whether to on board the customer or not based on their initial risk score and questionnaire responses. This happens in real time, which allows both the Rule-based and Algorithm-based models to be processed for a customer. This interactive capability allows the tellers and bank officers to gather the right information to classify the risk associated with a potential client. This also helps eliminate crucial data gaps that could impact an accurate assessment of the risk.

For more information on onboarding, see *KYC Service Guide*.

Prerequisites

- If a user needs access to a questionnaire as a part of KYC, the following roles must be mapped to the relevant group name (KYCADMNGRP):

Table 21. Questionnaire Role Mapping

Role	Group Name	Role Code
ABC Qtnr Loc Admin	KYCADMNGRP	QTNRADMNRL
ABC Qtnr Maintenance	KYCADMNGRP	QUESTMATRL
QtnrConfiguration Execute	KYCADMNGRP	QTNRCONFRL

Configuring the Questionnaire

To configure a questionnaire, you must first run insert scripts in order to populate data into the tables mentioned below. Use the sample scripts below and modify accordingly based on the attributes that you need to configure for the questionnaire:
The following insert scripts are examples for populating data into the tables mentioned above:

- DIM_COMPONENT_INFO

```
insert into DIM_COMPONENT_INFO (N_COMP_ID, N_COMP_CODE, V_COMP_NAME)
values (1, 1, 'RAOR')
```

```
/
insert into DIM_COMPONENT_INFO (N_COMP_ID, N_COMP_CODE, V_COMP_NAME)
values (2, 2, 'Compliance Investigation')
```

- DIM_COMPONENT_INFO_MLS

```
insert into DIM_COMPONENT_INFO_MLS (DESCLOCALE, V_COMP_NAME, N_COMP_ID)
values ('en_US', 'RAOR', 1)
/
insert into DIM_COMPONENT_INFO_MLS (DESCLOCALE, V_COMP_NAME, N_COMP_ID)
values ('en_US', 'Compliance Investigation', 2)
```

- APP_COMP_MAPPING

```
insert into APP_COMP_MAPPING (APP_COMP_MAP_ID, V_APP_CODE, N_COMP_ID, N_SUB_COMP_ID,
N_ENTITY_KEY)
values (1, 'OFS_KYC', 1, null, null)
/
insert into APP_COMP_MAPPING (APP_COMP_MAP_ID, V_APP_CODE, N_COMP_ID, N_SUB_COMP_ID,
N_ENTITY_KEY)
values (2, 'OFS_KYC', 2, null, null)
```

Note: For KYC, the value for `V_APP_CODE` must be `OFS_KYC`.

- QTNR_DIM_SRC

```
insert into QTNR_DIM_SRC (N_DIM_KEY, V_DIM_NAME, V_DIM_LOGICAL_NAME,
V_DIM_TAB_LOGICAL_COL_NAME, V_APP_CODE)
values (1, 'DIM_COUNTRY', 'Country', 'V_COUNTRY_NAME', 'OFS_KYC')
/
insert into QTNR_DIM_SRC (N_DIM_KEY, V_DIM_NAME, V_DIM_LOGICAL_NAME,
V_DIM_TAB_LOGICAL_COL_NAME, V_APP_CODE)
values (2, 'DIM_CURRENCY', 'Currency', 'V_ISO_CURRENCY_CD', 'OFS_KYC')
```

- QTNR_DIM_SRC_MLS

```
insert into QTNR_DIM_SRC_MLS (N_DIM_KEY, V_DIM_LOGICAL_NAME, DESCLOCALE)
values (1, 'Country', 'en_US')
/
insert into QTNR_DIM_SRC_MLS (N_DIM_KEY, V_DIM_LOGICAL_NAME, DESCLOCALE)
values (2, 'Currency', 'en_US')
```

- QTNR_HIERARCHY_SRC

```
insert into QTNR_HIERARCHY_SRC (N_HIERARCHY_KEY, V_HIERARCHY_NAME, V_APP_CODE,
V_HIERARCHY_LOGICAL_NAME)
values (1, 'HREF001', 'OFS_KYC', 'KBD 1')
/
insert into QTNR_HIERARCHY_SRC (N_HIERARCHY_KEY, V_HIERARCHY_NAME, V_APP_CODE,
V_HIERARCHY_LOGICAL_NAME)
values (2, 'HREF002', 'OFS_KYC', 'KBD 2')
```

- QTNR_HIERARCHY_SRC_MLS

```
insert into QTNR_HIERARCHY_SRC_MLS (DESCLOCALE, V_HIERARCHY_LOGICAL_NAME,
N_HIERARCHY_KEY)
values ('en_US', 'KBD 1', 1)
/
insert into QTNR_HIERARCHY_SRC_MLS (DESCLOCALE, V_HIERARCHY_LOGICAL_NAME,
N_HIERARCHY_KEY)
values ('en_US', 'KBD 2', 2)
```

- QTNR_STATIC_GRP

```
insert into QTNR_STATIC_GRP (N_GRP_KEY, V_GRP_CODE)
values (1, 'GRP001')
/
insert into QTNR_STATIC_GRP (N_GRP_KEY, V_GRP_CODE)
values (2, 'GRP002')
```

- QTNR_STATIC_GRP_MLS

```
insert into QTNR_STATIC_GRP_MLS (DESCLOCALE, V_GRP_LOGICAL_NAME, N_GRP_KEY)
values ('en_US', 'Sign Off Type', 1)
/
insert into QTNR_STATIC_GRP_MLS (DESCLOCALE, V_GRP_LOGICAL_NAME, N_GRP_KEY)
values ('en_US', 'Reassign Required', 2)
```

  Note: For KYC, the value for `DESCLOCALE` must be `en_US`.

- QTNR_STATIC_SRC

```
insert into QTNR_STATIC_SRC (N_STATIC_KEY, V_STATIC_NAME, V_APP_CODE, N_GRP_KEY)
values (1, 'Yes', 'OFS_KYC', 2)
/
insert into QTNR_STATIC_SRC (N_STATIC_KEY, V_STATIC_NAME, V_APP_CODE, N_GRP_KEY)
values (2, 'No', 'OFS_KYC', 2)
```

  Note: For KYC, the value for `V_APP_CODE` must be `OFS_KYC`.

- QTNR_STATIC_SRC_MLS

```
insert into QTNR_STATIC_SRC_MLS (DESCLOCALE, V_STATIC_LOGICAL_NAME, N_STATIC_KEY)
values ('en_US', 'No', 2)
/
insert into QTNR_STATIC_SRC_MLS (DESCLOCALE, V_STATIC_LOGICAL_NAME, N_STATIC_KEY)
values ('en_US', 'Yes', 1)
```

  Note: For KYC, the value for `DESCLOCALE` must be `en_US`.

The usage of the tables are provided below:

- APP_COMP_MAPPING: This table is used to store the information related to mapping components in the application.
- DIM_COMPONENT_INFO: This table contains information related to the components that are seeded for onboarding.

- DIM_COMPONENT_INFO_MLS: This table contains information related to the components defined in the application for multi locale support.

  Note: The three tables mentioned above are required to add the details of the component attributes as they cannot be added in the UI. If you do not load data in these tables, the components list in the UI does not display any data.

- QTNR_DIM_SRC: This table contains information related to the dimensions used as a source for the defined attributes.
- QTNR_DIM_SRC_MLS: This table contains information related to the dimensions used as a source for the defined attributes for multi locale support.
- QTNR_HIERARCHY_SRC: This table contains information about the questionnaire's hierarchy data source such as KeyBusinessDimension.
- QTNR_HIERARCHY_SRC_MLS: This table contains information about the questionnaire's hierarchy data source for multi locale support.
- QTNR_STATIC_GRP: This table groups the static data mentioned in the QTNR_STATIC_SRC table.
- QTNR_STATIC_GRP_MLS: This table groups the static data for multi locale support.
- QTNR_STATIC_SRC: This table contains information related to the static data that is grouped in the QTNR_STATIC_GRP table.
- QTNR_STATIC_SRC_MLS: This table contains information related to the static data for multi locale support.
- AAI_ABC_DIM_QTN_CATEGORY: This table stores information about the different categories the questions belong to.
- AAI_ABC_DIM_QTN_CATEGORY_MLS: This table stores information about the different categories the questions belong to for multi locale support.

  Note: The MLS tables must be populated with the same values as that of the main table. For example, the same values must be available in the DIM_COMPONENT_INFO and DIM_COMPONENT_INFO_MLS tables.

Categorizing the Questions in the Questionnaire

To categorize the questions, run the following script:

```
select * from AAI_ABC_DIM_QTN_CATEGORY
```

For more information on questionnaires, see *Chapter 8, OFS Analytical Applications Infrastructure User Guide 8.0.4.0.0*.

APPENDIX A Parameter Details

This appendix covers the following topics:

Parameters for Accelerated Re-review Assessments

The following table describes the parameter details for accelerated re-review assessments:

Evaluation Name	Profile Name	Filter	Data Set	Path	Expression
Account Country Change	Sum Of Account Country Change Count	• Account Change Log Summary - Account Country Change Count • Rereview Params - Rule Identifier	• Customer - Investigation, Customer - Cust-Acc, Cust-Acc-Account • Account - Account Change Log Summary, • Customer - Account, • Customer - Application Re-review Parameters	• Sum Of Account Country Change Count	• Account Change Log Summary - Change Date • Catch Up Lookback for Account Country Change
Account State Change	Sum Of Account State Change Count	• Account Change Log Summary - Account State Change Count • Rereview Params - Rule Identifier	• Customer - Investigation, (same as the above) • Account - Account Change Log Summary, • Customer - Account, • Customer - Application Re-review Parameters	• Customer - Application Re-review Parameters same as above	• Account Change Log Summary - Change Date • Catch Up Lookback for Account State Change

Evaluation Name	Profile Name	Filter	Data Set	Path	Expression
Change in Customer's Citizenship	Sum Of Change in Customer's Citizenship Count	• Customer Change Log Summary - CitizenshipCountry 1 Change Count • Rereview Params - Rule Identifier	• Customer - Customer Change Log Summary, • Customer - Investigation, • Account - Account Change Log Summary, • Customer - Account, • Customer - Application Re-review Parameters	• Customer - Customer Change Log Summary • Customer - Application Re-review Parameters	• Account Change Log Summary - Change Date
Customer Country Change	Sum Of Customer Country Change Count	• Sum of Customer Country Change Count • Rereview Params - Rule Identifier	• Customer - Customer Change Log Summary • Customer - Investigation • Customer - Account • Customer - Application Re-review Parameters	• Customer - Customer Change Log Summary • Customer - Application Re-review Parameters	• Catch up Lookback for Country Change • Customer Change Log Summary - Change Date
Customer State Change	Sum Of State Change Count	• Sum Of State Change Count • Rereview Params - Rule Identifier	• Customer - Customer Change Log Summary • Customer - Investigation, Customer - Account • Customer - Application Re-review Parameters	• Customer - Customer Change Log Summary • Customer - Application Re-review Parameters	• Catch Up Lookback for Customer State Change • Customer Change Log Summary - Change Date

Evaluation Name	Profile Name	Filter	Data Set	Path	Expression
Frequent Account Alert	Count of Frequent Account Alert	• Rule Identifier • Count of Frequent Account Alert	• Customer - Cust-Acc • Customer-Account - Investigation • Investigation - Entity Type • Customer - Account • Customer - Application Re-review Parameters	• Customer - Application Re-review Parameters • Customer - Entity Type_Account • Customer - Investigation-Account	• Application Rereview Params - Rule Identifier, • Application Rereview Params - Enable Flag, • Catch Up Lookback for Frequent Account Alert, • Entity Type Account, • Investigation_ Account - Closing class code, • Investigation_ Account - Created Date
Frequent Customer Alert	Count of Frequent Customer Alert	• Rule Identifier • Count of Frequent Customer Alert	• Customer - Investigation • Customer - Account • Customer - Application Re-review Parameters • Investigation - Entity Type	• Customer - Application Re-review Parameters • Customer - Entity Type, Customer - Investigation	• Application Rereview Params - Rule Identifier, • Application Rereview Params - Enable Flag, • Catch Up Lookback for Frequent Customer Alert, • Entity Type - Centricity Type code, • Investigation - Created Date, • Investigation_ Account - Closing class code

Evaluation Name	Profile Name	Filter	Data Set	Path	Expression
High Score Account Alert	Count of High Score Account Alert	• Count of High Score Account Alert, • Rule Identifier	• Customer _Account - Investigation • Customer - Account, Investigation - Entity Type • Cust-Cust-Account	• Customer - Application Re-review Parameters • Customer - Entity Type_Account, • Customer - Investigation-Account	• Application Rereview Params - Rule Identifier, • Application Rereview Params - Enable Flag, • Application Rereview Params - Threshold of Alert Score, • Entity Type Account, • Investigation_ Account - Created Date, • Investigation_ Account - Investigation Score

Evaluation Name	Profile Name	Filter	Data Set	Path	Expression
High Score Customer Alert	Count of High Score Customer Alert	• Count of High Score Customer Alert, • Rule Identifier	• Customer _Account - Investigation • Customer - Account, Investigation - Entity Type	• Customer - Application Re-review Parameters • Customer - Entity Type • Customer - Investigation (same as above)	• Application Rereview Params - Rule Identifier, • Application Rereview Params - Enable Flag, • Application Rereview Params - Threshold of Alert Score, • Entity Type - Centricity Type code, • Entity Type - Centricity Type code,Investigation - Created Date, • Investigation_ Account - Investigation Score
Increase in Customer Authority on Account	Count Of Increase in Customer Authority on Account	• Count of Increase in Customer Authority on Account	• Customer - Customer to Account Change Log Summary • Customer - Investigation, Customer - Account • Customer - Application Re-review Parameters	• Customer - Customer to Account Change Log Summary • Customer - Application Re-review Parameters	• Application Rereview Params - Rule Identifier, • Application Rereview Params - Enable Flag, • Customer to Account Change Log Summary - Change Date, Investigation_Account - Investigation Score

Evaluation Name	Profile Name	Filter	Data Set	Path	Expression
Regulatory Report action/son a Customer Alert	Sum Of Account Country Change Count	• Rereview Params - Rule Identifier • Entity Type - Centricity Type • Rule Identifier • Rule Enable Flag • Look Back Period • Investigation - Created Date • Regulatory Report Actions in • Param Identifier	• Customer - Investigation • Customer - ApplicationParameters • Customer - ApplicationRereviewParameters	• Customer - EntityType • Customer - Application Parameters • Customer - Application RereviewParameters	• Account Change Log Summary - Change Date • Catch Up Lookback for Account Country Change
Suspicious Account Alert	Count Of Suspicious Account Alert	• Count of Suspicious Account Alert • Rule Identifier	• Customer - Investigation • Customer - Application Re-review Parameters • Customer - Account (same as high score account alert)	• Customer - Application Re-review Parameters • Customer - Entity Type_Account • Customer - Investigation-Account	• Entity Type Account, • Investigation - Closing Classification, • Investigation_Account - Created Date, • Investigation_Account - Investigation Score
Suspicious Customer Alert	Count Of Suspicious Customer Alert	• Count Of Investigation • Rule Identifier	• Customer - Investigation • Customer - Application Re-review Parameters • Customer - Account, (same as high score customer alert) • Investigation - Entity Type	• Customer - Application Re-review Parameters • Customer - Entity Type • Customer - Investigation	• Entity Type - Centricity Type code, • Investigation - Closing Classification, • Investigation - Created Date, • Investigation Score, • Investigation_Account - Investigation Score

Parameters for Algorithm-based Risk Assessments

The following table describes the parameter details for algorithm-based assessments:

Evaluation Name	Filter	Data Set	Path
Risk Associated with Industry	• Enable Flag • Rule Code • Customer Type	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Risk associated to Public Company	• Enable Flag • Rule Code • Customer Type	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Operational Risk - Markets Served by the Bank	• Enable Flag • Rule Code • Customer Type • Service Effective Date • Service Expiration Date	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Geo Risk - Country of Residence	• Enable Flag • Rule Code • Customer Type	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Geo Risk - Country of Citizenship	• Customer Type • Enable Flag • Rule Code	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk for Primary Citizenship • Customer Processing: Param Risk for Primary Citizenship	• Customer Processing - Param Risk Score Jrsdn Primary Ctzsp
Geo Risk - Country of Operations	• Enable Flag • Non Individual Customers • Rule Code	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Geo Risk - Country of Head Quarters	• Enable Flag • Country of HQ • Non Individual • Business Address type	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA

Evaluation Name	Filter	Data Set	Path
Geo Risk - Country of Taxation	• Enable Flag • Rule Code • Individual Customer Type	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Risk Associated with Occupation	• Enable Flag • Rule Code • Individual Customer Type	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Risk Associated with Length of Relationship	• Length of relationship min value check • Length of Relationship Max value check • Enable Flag • Length of Relationship rule cod • Customer Type	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Risk Associated with Legal Structure Ownership	• Enable Flag • Legal Structure • FIRM Customer Type	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Operational Risk - Products Offered by the Bank	• Enable Flag • Product Rule Code • Corporate Customers	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Risk Associated with Source of Wealth	• Enable Flag • Source of wealth rule code • Individual Customer Type	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA

Evaluation Name	Filter	Data Set	Path
Risk Associated with Method Of Account Opening	• Enable Flag • Rule Code	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA
Risk Associated with Account Type	• Enable Flag • Rule Code	• Customer Processing: Appln Risk Rating Params • Appln Risk Rating Params: Param Risk Score Jrsdn MBA	• Customer Processing - Param Risk Score Jrsdn MBA

Parameters for New Accounts Opened by Customers Assessments

The following table describes the parameter details for new account assessments:

Evaluation Name	Filter	Data Set	Path
New Accounts Opened by Customers	• Account Status Code • Customer Status Code • Parameter Identifier • Parameter Value • Parameter Category • Look Back Start Range • Look Back End Range • Customer To Account - Account • Customer to Account - Investigation_Account • Investigation - Entity Type • Investigation_Account - Entity Type_Account	• Account - Account Change Log Summary • Customer - Account • Customer - Application Re-review Parameters • Customer - Application parameters • Customer - Customer Change Log Summary • Customer - Customer to Account Change Log Summary • Customer - Investigation • Customer To Account - Account • Customer to Account - Investigation_Account • Investigation - Entity Type • Investigation_Account - Entity Type_Account	• Customer - Account • Customer - Account Change Log Summary • Customer - Application Parameters • Customer - Application Re-review Parameters • Customer - Customer Change Log Summary • Customer - Customer to Account Change Log Summary • Customer - Entity Type • Customer - Entity Type_Account • Customer - Investigation • Customer - Investigation-Account

Parameters for Periodic Re-review of Customers Assessments

The following table describes the parameter details for periodic assessments:

Evaluation Name	Filter	Data Set	Path
Periodic Re-review of Customers	• Parameter Identifier • Parameter Value • Parameter Category • Next Review Start Date • Next review End Date	• Customer - Customer Review Details • Customer - Application parameters	• Customer - Customer Review Details • Customer - Application parameters

Parameters for Rule-Based Risk Assessments

The following table describes the parameter details for rule-based assessments:

Evaluation Name	Filter	Data Set	Path
Geo Risk - Country of Primary Citizenship	• Rule Code • Enable Flag • Primary Citizenship	• Customer Processing - Rule Based Processing • Rule Based Processing - Param Risk Score Jrsdn	• Customer Processing - Rule Based Processing • Customer Processing to Risk Score Jurisdiction Param • Customer Processing - Rule Based Processing
Geo Risk - Country of Secondary Citizenship	• Rule Code • Enable Flag • Secondary Citizenship	• Customer Processing - Rule Based Processing • Rule Based Processing - Param Risk Score Jrsdn	• Customer Processing - Rule Based Processing • Customer Processing to Risk Score Jurisdiction Param
Geo Risk - Country of Head Quarters	• Enable Flag • Rule Code • Address Code • Address Usage Code	• Customer Processing - Rule Based Processing • Rule Based Processing - Param Risk Score Jrsdn	• Customer Processing - Rule Based Processing • Customer Processing to Risk Score Jurisdiction Param

Evaluation Name	Filter	Data Set	Path
Geo Risk - Country of Operations	• Customer Processing - Customer Country Processing • Customer Processing - Rule Based Processing • Customer Processing to Risk Score Jurisdiction Param	• Customer Processing - Customer Address Processing • Customer Processing - Rule Based Processing • Customer Processing -Customer Country Processing • Rule Based Processing - Param Risk Score Jrsdn	• Customer Processing - Customer Country Processing • Customer Processing - Rule Based Processing • Customer Processing to Risk Score Jurisdiction Param
Geo Risk - Country of Residence	• Enable Flag • Rule Code • Residence Country Code	• Customer Processing - Rule Based Processing • Rule Based Processing - Param Risk Score Jrsdn	• Customer Processing - Rule Based Processing • Customer Processing to Risk Score Jurisdiction Param
Risk Associated with Occupation	• Rule Code • Enable Flag • Occupation Code	• Customer Processing - Rule Based Processing • Rule Based Processing - Param Risk Score Jrsdn	• Customer Processing - Rule Based Processing • Customer Processing to Risk Score Jurisdiction Param
Risk Associated with Legal Structure And Ownership	• Rule Code • Enable Flag • Legal Structure Code • Public or Private	• Customer Processing - Rule Based Processing • Rule Based Processing - Param Risk Score Jrsdn	• Customer Processing - Rule Based Processing • Customer Processing to Risk Score Jurisdiction Param
Risk Associated with Industr	• Rule Code • Enable Flag • Industry Code	• Customer Processing - Rule Based Processing • Rule Based Processing - Param Risk Score Jrsdn	• Customer Processing - Rule Based Processing • Customer Processing to Risk Score Jurisdiction Param

Parameters for On Boarding Algorithm-Based Assessments

The following table describes the parameter details for onboarding algorithm-based assessments:

Evaluation Name	Filter	Data Set	Path
On Boarding - Risk Associated with Source of Wealth	• Enable Flag • Param Code • Customer Type	• Algorithm Based Risk Scoring - Risk Score of Source of Wealth Value(s) • Appln Risk Rating Params - Param Risk Score Jrsdn DEF • Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Soruce of Wealth Value(s)	• Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer-Default Risk Score for Missing Data • Onboarding Customer - Param Risk Score Jrsdn SRCWLTH
On Boarding -Risk Associated with Account Type	• Rule Code • Enable Flag • Occupation	• Alogrithm Based Risk Scoring - Risk Score of Account Type Value(s) • Appln Risk Rating Params - Param Risk Score Jrsdn DEF • Onboarding Account - Risk Score of Account Type Value(s) • Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Onboarding Account	• Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Account Type Value(s) • Onboarding Customer-Default Risk Score for Missing Data

Evaluation Name	Filter	Data Set	Path
On Boarding Geo Risk - Country of Citizenship	• Enable Flag • Param Code • Individual Customer Type	• Alogrithm Based Risk Scoring - Risk Score of Citizenship Value(s) • Appln Risk Rating Params - Param Risk Score Jrsdn DEF • Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Citizenship Value(s)	• Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Citizenship Value(s) • Onboarding Customer-Default Risk Score for Missing Data
On Boarding Geo Risk - Country of Residence	• Enable Flag • Rule Code • Primary Citizenship	• Alogrithm Based Risk Scoring - Risk Score of Country of Residence Value(s) • Appln Risk Rating Params - Param Risk Score Jrsdn DEF • Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Country of Residence Value(s)	• Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Country of Residence Value(s) • Onboarding Customer-Default Risk Score for Missing Data
On Boarding Geo Risk - Country of Taxation	• Enable Flag • Param Code • Customer Type	• Alogrithm Based Risk Scoring - Risk Score of Country of Tax Value(s) • Appln Risk Rating Params - Param Risk Score Jrsdn DEF • Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Country of Taxation Value(s)	• Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Country of Taxation Value(s) • Onboarding Customer-Default Risk Score for Missing Data

Evaluation Name	Filter	Data Set	Path
On Boarding Geo Risk-Country of Operations	• Enable Flag • Non Individual Customer Type • Param Code	• Alogrithm Based Risk Scoring - Risk Score of Country of Operations Value(s) • Appln Risk Rating Params - Param Risk Score Jrsdn DEF • On Boarding Customer Country - Risk Score of Country of Operations Value(s) • Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - On Boarding Customer Country	• Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Country of Operation Value(s) • Onboarding Customer-Default Risk Score for Missing Data

Evaluation Name	Filter	Data Set	Path
On Boarding - Risk Associated with Method of Account Opening	• Enable Flag • Param Code	• Algorithm Based Risk Scoring - Risk Score of Method of Account Opening Value(s) • Appln Risk Rating Params - Param Risk Score Jrsdn DEF • Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Onboarding Account	• Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Method of Account Opening Value(s) • Onboarding Customer-Default Risk Score for Missing Data
On Boarding - Risk Associated with Occupation	• Rule Code • Enable Flag • Occupation	• Algorithm Based Risk Scoring- Risk Score of Occupation Value(s) • Appln Risk Rating Params - Param Risk Score Jrsdn DEF • Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Occupation Value(s) • Onboarding Customer - Rule Based Risk Assessment • Rule Based Processing - Param Risk Score Jurisdiction	• Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score for Parameter/ Rule Value • Onboarding Customer - Risk Score of Occupation Value(s) • Onboarding Customer - Rule Based Risk Assessment • Onboarding Customer-Default Risk Score for Missing Data

Parameters for On Boarding Rule-Based Assessments

The following table describes the parameter details for onboarding rule-based assessments:

Evaluation Name	Filter	Data Set	Path
On Boarding - Risk Associated with Occupation	• Rule Code • Enable Flag • Occupation	• Algorithm Based Risk Scoring- Risk Score of Occupation Value(s) • Appln Risk Rating Params - Param Risk Score Jrsdn DEF • Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score of Occupation Value(s) • Onboarding Customer - Rule Based Risk Assessment • Rule Based Processing - Param Risk Score Jurisdiction	• Onboarding Customer - Alogrithm Based Risk Scoring • Onboarding Customer - Risk Score for Parameter/ Rule Value • Onboarding Customer - Risk Score of Occupation Value(s) • Onboarding Customer - Rule Based Risk Assessment • Onboarding Customer-Default Risk Score for Missing Data
On Boarding Geo Risk - Country of Primary Citizenship	• Enable Flag • Rule Code • Primary Citizenship	• Onboarding Customer - Rule Based Risk Assessment • Rule Based Processing - Param Risk Score Jurisdiction	• Onboarding Customer - Risk Score for Parameter/ Rule Value • Onboarding Customer - Rule Based Risk Assessment

APPENDIX B KYC Batches

This appendix covers the KYC Batch and the tasks within the batches. This chapter discusses the following topics:

- Regular Processing
- Deployment Initiation Processing
- End of Day Processing

Regular Processing

The following table provides details about regular processing:

NOTE: To process watch list data, run the following data maps:

- runjob $MANTAS_HOME/bdf/scripts/execute.sh WLMProcessingLock
- runjob $MANTAS_HOME/bdf/scripts/execute.sh WatchListEntry_WatchListEntryCurrDayInsert
- runjob $MANTAS_HOME/bdf/scripts/execute.sh WatchListAudit_StatusUpd
- runjob $MANTAS_HOME/bdf/scripts/execute.sh WatchList_WatchListSourceAuditInsert
- runjob $MANTAS_HOME/bdf/scripts/execute.sh WatchList_WatchListSourceAuditUpd
- runjob $MANTAS_HOME/bdf/scripts/execute.sh WatchList_WatchListSourceUpd
- runjob $MANTAS_HOME/bdf/scripts/execute.sh WatchListEntry_WatchListAuditUpd
- runjob $MANTAS_HOME/bdf/scripts/execute.sh WatchListEntryAudit_WatchListEntryUpdate
- runjob $MANTAS_HOME/bdf/scripts/execute.sh WatchListStagingTable_WatchList
- runjob $MANTAS_HOME/bdf/scripts/execute.sh WLMProcessingUnlock

Table 22: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task1	Customer	This is an IPE prefiltering task that is used to run the Accelerated Rereview, New Accounts and Periodic Rereview Assessments and to find the eligible customers for risk Assessment.	INLINE PROCESSING	
Task2	BD_POPULATE_LAST_RUN_BATCH	This is a task that populates the `kdd_extrl_batch_last_run` table and is used to keep track of the current batch that is being run.	TRANSFORM DATA	Task1
Task3	Populate_Customer_Reasn_Prcsng	This is a task that populates customer data into the `Cust` tables when run.	LOAD DATA	Task2

Table 22: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task4	Populate_Cust_Prcsng	This is a task that populates the prefiltered Customer Data into the `Cust_Prcsng` table when run.	LOAD DATA	Task3
Task5	Populate_Cust_Addr_Prcsng	This is a task that populates the prefiltered Customer Data into the `Cust_Addr_Prcsng` table when run.	LOAD DATA	Task4
Task6	Populate_Cust_Cntry_Prcsng	This is a task that populates the prefiltered Customer Data into the `Cust_Cntry_Prcsng` table when run.	LOAD DATA	Task5
Task7	Populate_Cust_Id_Doc_Prcsng	This is a task that populates the prefiltered Customer Data into the `Cust_Id_Doc_Prcsng` table when run.	LOAD DATA	Task6
Task8	Populate_Cust_Mkt_Served_Prcsng	This is a task that populate the prefiltered Customer Data into the `Cust_Mkt_Served_Prcsng` table when run.	LOAD DATA	Task7
Task9	Populate_Cust_Phon_Prcsng	This is a task that populates the prefiltered Customer Data into the `Cust_Phon_Prcsng` table when run.	LOAD DATA	Task8
Task10	Populate_Cust_Prod_Prcsng	This is a task that populates the prefiltered Customer Data into the `Cust_Product_Prcsng` table when run.	LOAD DATA	Task9
Task11	Populate_Cust_to_Cust_Prcsng	This is a task that populates the prefiltered Customer Data into the `Cust_Cust_Prcsng` table when run.	LOAD DATA	Task10
Task12	Populate_Cust_Acct_Prcsng	This is a task that populates the prefiltered Customer Data into the `Cust_Acct_Prcsng` table when run.	LOAD DATA	Task11
Task13	Populate_Acct_Prcsng	This is a task that populates the prefiltered Customer Data into the `Acct_Prcsng` table when run.	LOAD DATA	Task12

Table 22: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task14	t2t_FCT_CUST_REVIEW_REASONS	This is a task that populates the accelereated rereview reasons for the prefiltered Customers when run.	LOAD DATA	Task10, Task11, Task12, Task13, Task14, Task2, Task3, Task4, Task5, Task6, Task7, Task8, Task9
Task15	POPULATE_IP_KYC	This is a task that populates the Intrested Party Customers and Accounts when run.	LOAD DATA	Task14
Task16	t2t_FCT_TP_WLS_REQUESTS_PRCNG	This is a task that populates Requests into the Watchlist Processing table for the prefiltered Customers when run.	LOAD DATA	Task15
Task17	Watchlist_Fuzzy Match	This is a task that calls the Watchlist Fuzzy Match to calculate the watchlist Score when run.	TRANSFORM DATA	Task16
Task18	t2t_FCT_TP_WLS_RESULTS_PRCNG	This is a task that populates the Watchlist Score in the `FCT_TP_WLS_RESULTS_PRCNG` table when run.	LOAD DATA	Task15, Task16, Task17, Task18
Task19	UPDATE_WLS_STATUS	This is a task that updates the Status of the Watchlist Request to Closed when run.	TRANSFORM DATA	Task18
Task20	Customer Processing	This is a task that is used to run the IPE assessment for Rule-based Rules and generate the scores when run.	INLINE PROCESSING	Task19
Task21	Customer Processing	This is a task that is used to run the IPE assessment for Model-based Rules and generate the scores when run.	INLINE PROCESSING	Task20
Task22	t2t_POPULATE_FCT_RA	This is a task that generates the Risk Assessment IDs for each Customer and populates the `FCT_RA` table when run.	LOAD DATA	Task21
Task23	t2t_POPULATE_FCT_RA_RISK_SUMMARY	This is a task that populates the `FCT_RA_RISK_SUMMARY` table with the final MB and RB scores for each Customer when run.	LOAD DATA	Task20, Task21, Task22, Task23

Table 22: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task24	t2t_POPULATE_FCT_RA_RISK_REASONS	This is a task that populates the FCT_RA_RISK_REASONS table with the scores of each Parameter for every Customer when run.	LOAD DATA	Task23
Task25	t2t_FCT_RA_RISK_DETAILS	This is a task that populates the FCT_RA_RISK_DETAILS table with the actual values of each Parameter for every Customer when run.	LOAD DATA	Task24
Task26	t2t_FCT_CUST_RA_HISTRY	This is a task that populates the FCT_CUST_RA_HISTRY table with the names of the prefiltered customers when run.	LOAD DATA	Task25
Task27	F_CLOSURE_UPDATES	This is a task that updates the RA once they are closed.	TRANSFORM DATA	Task26
Task28	F_RA_TO_CASE	This is a task that creates Cases for the eligible Customers when run.	TRANSFORM DATA	Task27
Task29	t2t_FCT_CUST_RVWDTLS	This is a task that populates the FCT_CUST_RVWDTLS table when run.	LOAD DATA	Task28
Task30	Auto_Case_Assignment	This is a task that assigns cases to the appropriate user when run.	TRANSFORM DATA	Task29
Task31	F_POST_CASE_ASSIGNMENT	This is a task that updates the tables after a case has been assigned.	TRANSFORM DATA	Task30
Task32	t2t_FCT_TP_WLS_REQUESTS	This is a task that populates the FCT_TP_WLS_REQUESTS table when run.	LOAD DATA	Task31
Task33	t2t_FCT_TP_WLS_RESULTS	This is a task that populates the FCT_TP_WLS_RESULTS table when run.	LOAD DATA	Task32
Task34	t2t_FCT_RA_RISK_RATING_HISTORY	This is a task that populates the FCT_RA_RISK_RATING_HISTORY table when run.	LOAD DATA	Task33
Task35	KYC_PURGE_LAST_RUN_TAB	This is a task that purges or truncates the kdd_extrl_batch_last_run table when run.	TRANSFORM DATA	Task34
Task36	t2f_GenCustDetails_ED	This is a task that generates the Customer details flat file.	LOAD DATA	Task35
Task37	t2f_GenWLSFeedback_ED	This is a task that generates the Watchlist feedback details flat file.	LOAD DATA	Task36

Table 22: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task38	t2f_GenCBSFeedback_ED	This is a task that generates the GenCBSFeedback details flat file.	LOAD DATA	Task37
Task39	KYC_File_Rename	This is a task that allows you to rename the three flat files mentioned above so that they can be fed as an input to the Mantas application.	TRANSFORM DATA	Task38

Deployment Initiation Processing

The following table provides details about deployment initiation processing:

Table 23: Deployment Initiation Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task1	FN_IPE_LAST_BATCH_RUN_KY	This is a task that captures the current batch ID when run.	TRANSFORM DATA	
Task2	Populate_Cust_Prcsng_DI	This is a task that populates the prefiltered Customer Data into the Cust_Prcsng table when run.	LOAD DATA	Task1
Task3	GathrStats_CUST_PRCSNG	This is a task that is used to gather statistics for the CUST_PRCSNG table.	LOAD DATA	Task2
Task4	Populate_Cust_Addr_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Addr_Prcsng table when run.	LOAD DATA	Task3
Task5	Populate_Cust_Cntry_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Cntry_Prcsng table when run.	TRANSFORM DATA	Task4
Task6	Populate_Cust_Id_Doc_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Id_Doc_Prcsng table when run.	TRANSFORM DATA	Task5
Task7	Populate_Cust_Mkt_Served_Prcsng	This is a task that populate the prefiltered Customer Data into the Cust_Mkt_Served_Prcsng table when run.	TRANSFORM DATA	Task6
Task8	Populate_Cust_Phon_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Phon_Prcsng table when run.	TRANSFORM DATA	Task7

Table 23: Deployment Initiation Processing

Task9	Populate_Cust_Prod_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Product_Prcsng table when run.	LOAD DATA	Task 8
Task10	Populate_Cust_to_Cust_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Cust_Prcsng table when run.	LOAD DATA	Task 9
Task11	Populate_Cust_Acct_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Acct_Prcsng table when run.	LOAD DATA	Task 10
Task12	GathrStats_CUST_ACCT_PRC	This is a task that is used to gather statistics for the CUST_ACCT_PRC table.	TRANSFORM DATA	Task11
Task13	Populate_Acct_Prcsng	This is a task that populates the prefiltered Customer Data into the Acct_Prcsng table when run.	LOAD DATA	Task 12
Task14	POPULATE_IP_KYC	This is a task that populates the Intrested Party Customers and Accounts when run.	TRANSFORM DATA	Task1,Task10,Task11, Task12, Task13,Task2,Task3,Task4, Task5,Task6, Task7,Task8, Task9
Task15	GathrStats_IP	This is a task that is used to gather statistics for the FCT_CUST_iINTERESTED_PARTY table.	TRANSFORM DATA	Task 14
Task16	t2t_FCT_TP_WLS_REQUESTS_PRCNG	This is a task that populates Requests into the Watchlist Processing table for the prefiltered Customers when run.	LOAD DATA	Task 14, Task 15
Task17	GathrStats_WLSREQUESTS_P	This is a task that is used to gather statistics for the FCT_TP_WLS_REQUESTS and FCT_TP_WLS_REQUESTS_PRCNG tables.	TRANSFORM DATA	Task 16
Task18	Watchlist_FuzzyMatch	This is a task that calls the Watchlist Fuzzy Match to calculate the watchlist Score when run.	TRANSFORM DATA	Task 17
Task19	GathrStats_WLSRESULT_STG	This is a task that is used to gather statistics for the FCT_TP_WLS_RESULTS and FCT_TP_WLS_RESULTS_PRCNG tables.	TRANSFORM DATA	Task 18
Task20	t2t_FCT_TP_WLS_RESULTS_PRCNG	This is a task that populates the Watchlist Score in the FCT_TP_WLS_RESULTS_PRCNG table when run.	LOAD DATA	Task 19

Table 23: Deployment Initiation Processing

Task21	UPDATE_WLS_STATUS	This is a task that updates the Status of the Watchlist Request to Closed when run.	TRANSFORM DATA	Task 20
Task22	GathrStats_KYCPRCSNG_TAB	This is a task that is used to gather statistics for all the KYC processing tables.	TRANSFORM DATA	Task 21
Task23	Customer Processing	This is a task which generates rule or model-based scores when run.	INLINE PROCESSING	Task16, Task17, Task18, Task19, Task20, Task21, Task22
Task24	Customer Processing	This is a task which generates rule or model-based scores when run.	INLINE PROCESSING	Task 23
Task25	t2t_FCT_RA_DI	This is a task that is used to populate the FCT_RA_DI table.	LOAD DATA	Task 24
Task26	GathrStats_FCT_RA	This is a task that is used to gather statistics for the FCT_RA table for Regular Processing.	TRANSFORM DATA	Task 25
Task27	t2t_POPULATE_FCT_RA_RISK_SUMMARY	This is a task that populates the FCT_RA_RISK_SUMMARY table with the final MB and RB scores for each Customer when run.	LOAD DATA	Task 26
Task28	t2t_POPULATE_FCT_RA_RISK_REASONS	This is a task that populates the FCT_RA_RISK_REASONS table with the scores of each Parameter for every Customer when run.	LOAD DATA	Task 27
Task29	t2t_FCT_RA_RISK_DETAILS	This is a task that populates the FCT_RA_RISK_DETAILS table with the actual values of each Parameter for every Customer when run.	LOAD DATA	Task 28
Task30	t2t_FCT_CUST_RVWDTLS_AUTO_CLOSED_DI	This is a task that stores the details of the assessments that are auto-closed.	LOAD DATA	Task 29
Task31	t2t_FCT_CUST_RVWDTLS_PTC_DI	This is a task that stores the details of the assessments that are promoted to a case through the batch.	LOAD DATA	Task 30
Task32	t2t_FCT_TP_WLS_REQUESTS	This is a task that populates the FCT_TP_WLS_REQUESTS table when run.	LOAD DATA	Task 31
Task33	t2t_FCT_TP_WLS_RESULTS	This is a task that populates the FCT_TP_WLS_RESULTS table when run.	LOAD DATA	Task 32
Task34	t2t_FCT_RA_RISK_RATING_HISTORY	This is a task that populates the FCT_RA_RISK_RATING_HISTORY table when run.	LOAD DATA	Task 33

Table 23: Deployment Initiation Processing

Task35	t2t_FCT_CUST_RA_HISTRY	This is a task that populates the FCT_CUST_RA_HISTRY table with the names of the prefiltered customers when run.	LOAD DATA	Task 34
Task36	F_RA_TO_CASE	This is a task that creates Cases for the eligible Customers when run.	TRANSFORM DATA	Task25, Task26, Task27, Task28, Task29, Task30, Task31, Task32, Task33, Task34, Task35
Task37	Auto_Case_Assignment	This is a task that assigns cases to the appropriate user when run.	TRANSFORM DATA	Task 36
Task38	GathrStats_KYCCase_Tabs	This is a task that is used to gather statistics for all case tables when run.	TRANSFORM DATA	Task 37
Task39	F_POST_CASE_ASSIGNMENT	This is a task that updates the tables after a case has been assigned.	TRANSFORM DATA	Task 38
Task40	KYC_PURGE_LAST_RUN_TAB	This is a task that purges or truncates the kdd_extrl_batch_last_run table when run.	TRANSFORM DATA	Task36, Task37, Task38, Task39

End of Day Processing

The following table provides details about end of day processing:

Table 24: End of Day Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task1	GenCustDetails_ED	Extract the customer feedback details	EXTRACT DATA	
Task2	GenWLSFeedback_ED	Extract the Watchlist scanning feedback details	EXTRACT DATA	Task1
Task3	GenCBSFeedback_ED	Extract customer details for CBS	EXTRACT DATA	Task2
Task4	FN_INCPRCDATEBYONE	Incrementing the KYC processing date by 1 day	TRANSFORM DATA	Task3
Task5	KYC_File_Rename	Renaming of the extracted files according to the AML needs	TRANSFORM DATA	Task4

Table 24: End of Day Processing

Task6	FN_RA_PURGE	Purging of the Autoclosed or UI closed risk assessments	TRANSFORM DATA	Task5
Task7	FN_PARTITION_MAINTENANCE	Droping the partition on the FCT_CUST_RA_HISTRY table	TRANSFORM DATA	Task6
Task8	FN_REREVIEW_DATE_DI	Spliting of the customers processed through the DI processing back for periodic re-review	TRANSFORM DATA	Task7

APPENDIX C Creating Highlights

This appendix provides the steps to create highlights for Risk and Algorithm-based assessments in KYC.

The ready-to-use product displays highlights as a display code for parameters. Performing the following steps display the highlights as the actual value of the code. For example, the code for India is IND. Initially, this is displayed in the UI corresponding to a Risk parameter like Country of Residence. After performing the steps shown below, the actual value, that is, India, is displayed.

To create a highlight, follow these steps:

1. Import `KDD_CODE_SET_TRNLN` table selecting type as Reference.
2. Add a virtual table for every risk factor in which the description of risk factors is required.

   To add a Business Entity, navigate to the Association and Configuration menu in the Inline Processing page and click **Business Entities**.

   In the below example, a Business Entity called Residence is created.

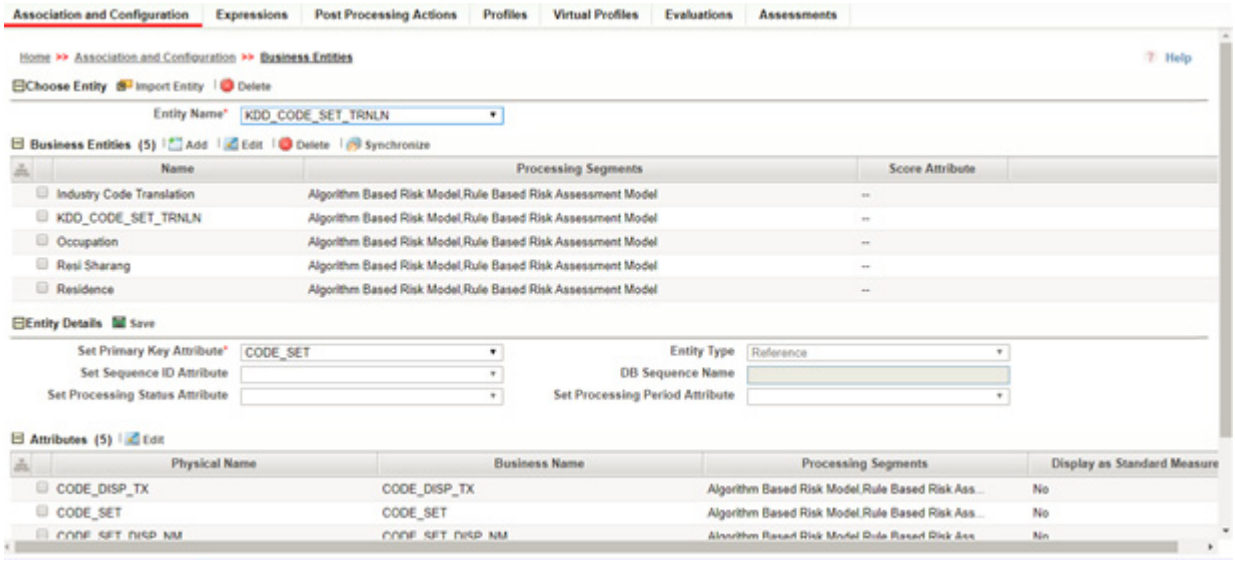


Figure 67. Business Entities

3. Add two Inline Datasets, one for the start table and one for the end table.

   To add an Inline Dataset, navigate to the Association and Configuration menu in the Inline Processing page and click **Inline Datasets**.

   In the below example, Inline Datasets are created for Country of Residence Value as the start table and Residence as the end table.

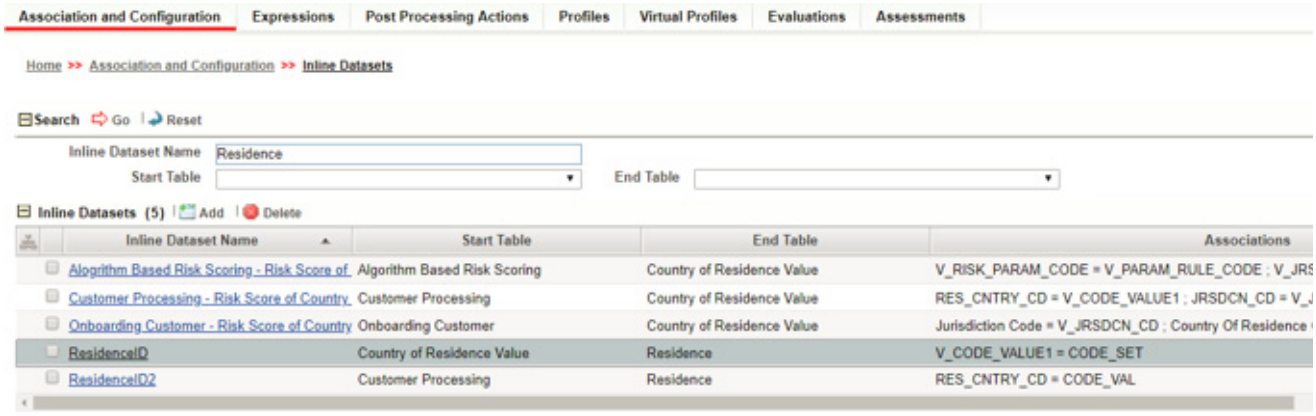


Figure 68. Inline Datasets

4. Add a Traversal Path for each join defined in Inline Datasets.

   To add a Traversal Path, navigate to the Association and Configuration menu in the Inline Processing page and click **Traversal Paths**.

   In the below example, a Traversal path is created from the Customer Processing table to the Residence table.

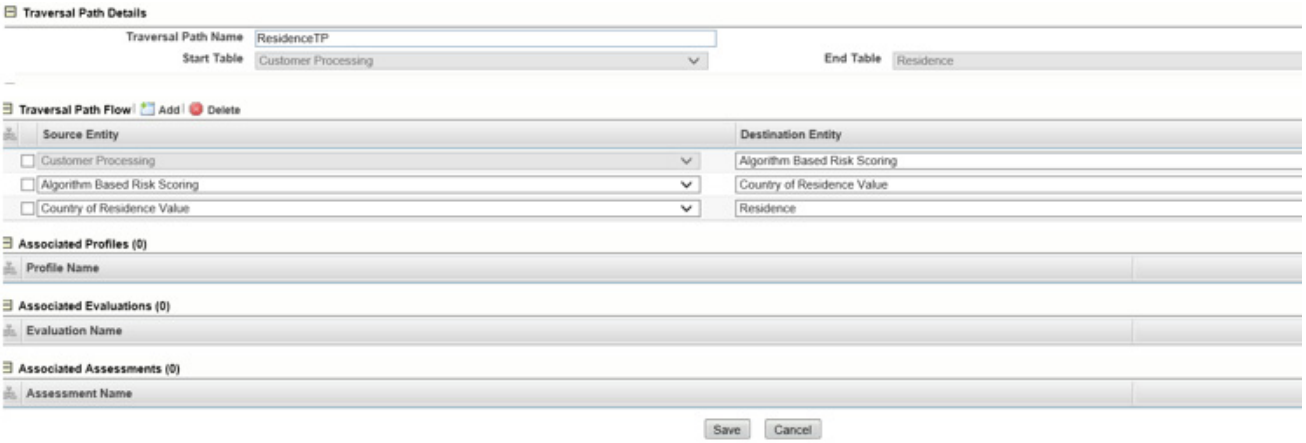


Figure 69. Traversal Paths

5. Add an expression on the risk score column of the Business Entity which is to be scored as a risk parameter.

   To add an Expression, navigate to the Expressions menu in the Inline Processing page.

In the below example, an Expression called ResidenceEPR is created for the Residence Business Entity..

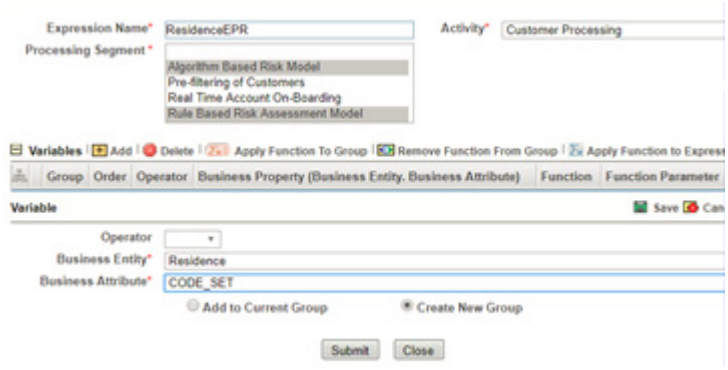


Figure 70. Expressions

6. Map an expression to the existing evaluation of the added parameter.

   To map an expression, navigate to the Evaluations menu in the Inline Processing page.

   In the below example, an Evaluation is created for the Rule Based Risk Assessment.

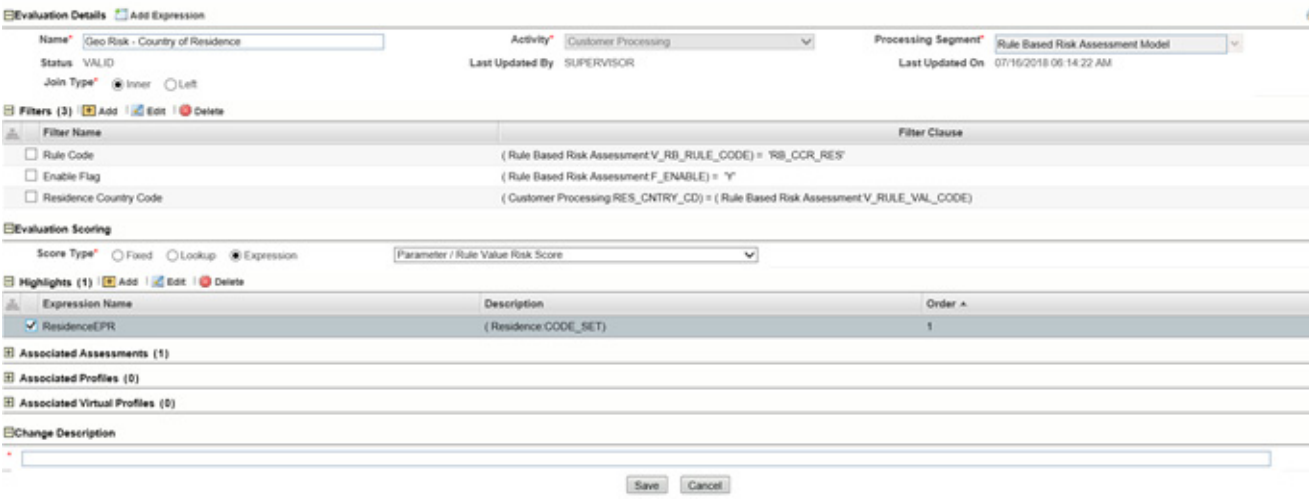


Figure 71. Evaluations

7. Resave the invalid Assessment.This is needed because when a change is made to an evaluation, the assessment becomes invalid, and needs to be saved.

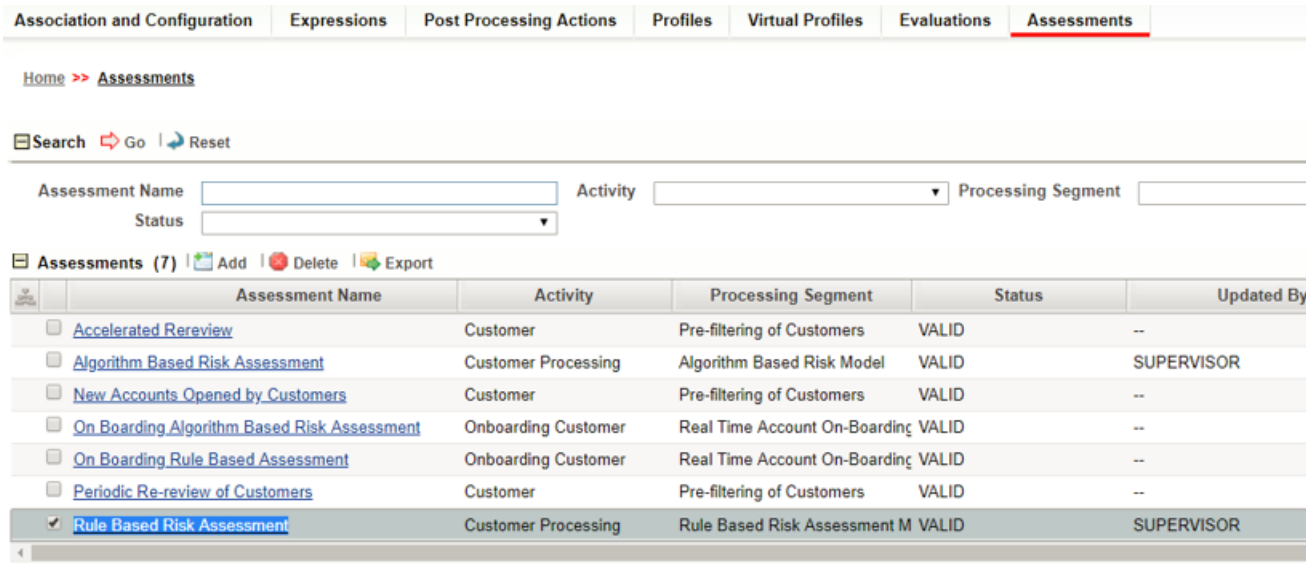


Figure 72. Assessments

Index

A

B

J

L

M

O

R

U

W