Oracle Financial Services
Know Your Customer
Administration Guide

Release 8.0.7.0.0
December 2020

ORACLE®
FINANCIAL SERVICES

ORACLE®

Oracle Financial Services
Know Your Customer
Administration Guide

Release 8.0.7.0.0
December 2020

Part Number: F17838-01

Revision History

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

Date	Edition	Description
August 2021	8.0.7.1.7	● Added the FCC_OB_RSKPRMS_JRSDCUST_MAP_ST.xls Excel type in the *Excel Upload of Data* section.
March 2021	8.0.7.0.133	● Added the run scripts for the EDQ and CS servers in the *Switching between CS and EDQ Servers for Screening* appendix.
December 2020	Third Edition of 8.0.7	● Added a section for configuring the relationship type for primary customers in the *KYC Onboarding* section.
March 2019	Third Edition of 8.0.7	● Updated the Regular Processing and Deployment Initiation Processing tasks in *Appendix A, KYC Batches*.
March 2019	8.0.7.0.2	● Added an appendix which mentions how to run daily and deployment initiation batches and how to map watch list assessments for accelerated rereviews for screening delta customers.
Jan 2019	Second edition of 8.0.7	● Updated the *Enterprise Case Management integration* section in *Chapter 4, Maintenance Activities and Configuring Setup Parameters (KYC Batch)*. ● Removed the *Customer Screening integration* section in *Chapter 4, Maintenance Activities and Configuring Setup Parameters (KYC Batch)*. ● Updated the chapter for KYC Onboarding. ● Updated *Appendix D, BDF Datamaps*.
Dec 2018	First edition of 8.0.7	● Removed all instances of negative news. ● Added a chapter for KYC Onboarding. ● Removed the *Setting up KYC Onboarding* section in *Chapter 4, Maintenance Activities and Configuring Setup Parameters (KYC Batch)*. ● Removed the *Real-time Account Onboarding Risk Assessment* section in *Chapter 4, Maintenance Activities and Configuring Setup Parameters (KYC Batch)*. ● Removed the *Questionnaire* chapter. ● Removed the *Setting up KYC Onboarding Service* chapter.

Contents

List of Tables

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

- Scope of this Guide

- How this Guide is Organized

- Where to Find More Information

- Conventions Used in this Guide

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 KYC 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.

- *Getting Started* provides step-by-step instruction to login to the Know Your Customer (KYC) application and different features of the Oracle Financial Services Analytical Applications (OFSAA) Application page.

- *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 (KYC Batch)* describes how to configure the KYC application.

- *Managing KYC Batches* provides information on how to manage the different KYC batches.

- *KYC Onboarding* provides information on the different processes involved in Know Your Customer (KYC) Onboarding.

- *Adding Risk Parameters and Rules (KYC Batch)* describes how to add risk parameters for algorithm and rule based assessments and accelerated rereview parameters.

- *Parameter Details* provides information on the parameters for KYC.

- *KYC Batches* provides information on the KYC batches.

- *Creating Highlights* provides information on how to create highlights in KYC.

- *BDF Datamaps* provides information on the BDF datamaps used in KYC.

- 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*

- *KYC API Data Elements Guide*

- *KYC Utilities Guide*

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*

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
BD	Behavior Detection
CS	Customer Screening
KYC	Know Your Customer
EDQ	Enterprise Data Quality

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 discusses the following topics:

- KYC Overview
- KYC Workflow

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:

- Onboarding
- Deployment Initiation
- Real Time Account on Boarding
- Account on Boarding or Default Review
- Rereviewx

  The Oracle KYC risk assessment application is built using the OFS AAI framework. The application functions are divided in to 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:
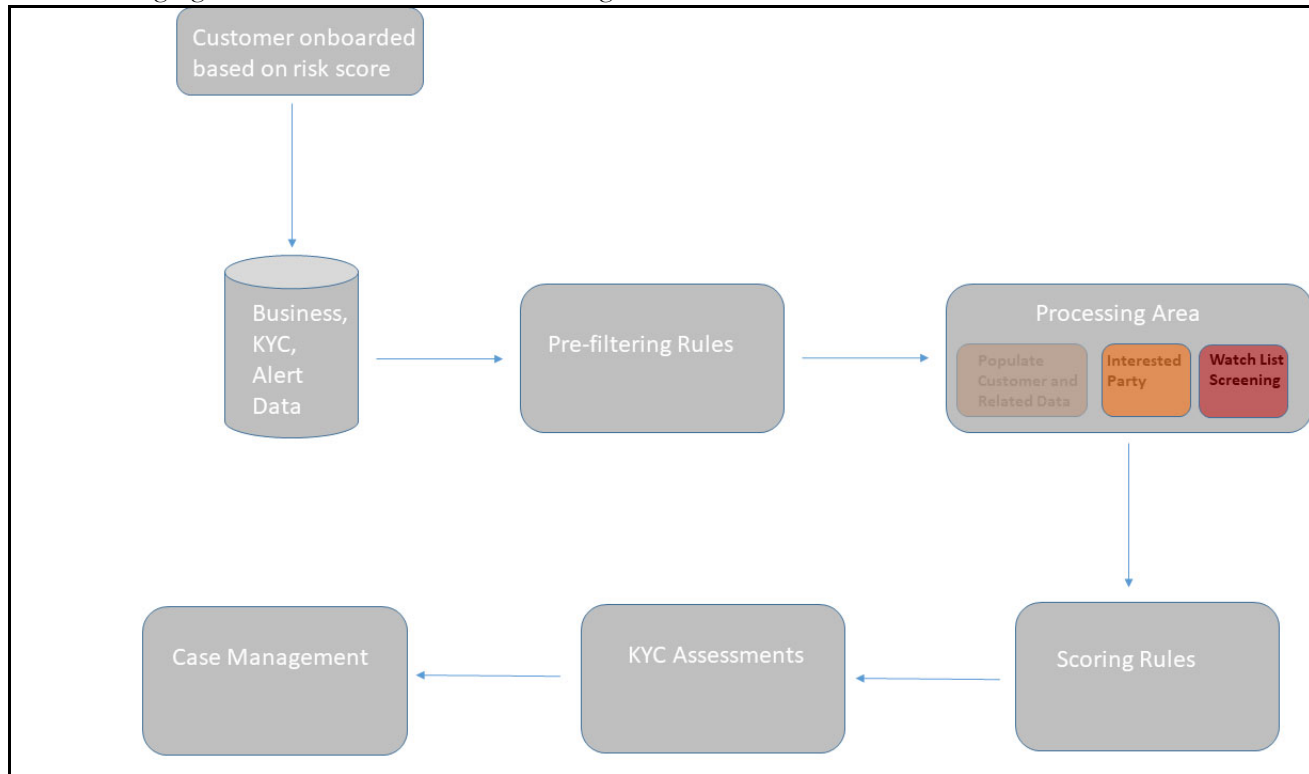
Figure 1. KYC Process Flow for Existing Customers

The following section describes the process flow:

1. Customer is onboarded based on the risk score. For more information on the Onboarding process, see *KYC Onboarding*.

2. 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.

3. 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. The prefiltering rules identify a set of customer who are due for reivew depending on these rules.

4. The processing area contains the data of all customers for whom the prefiltering rules apply and for whom risk scoring needs to be done.

5. 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.

6. 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.

7. A risk assessment is considered for a promotion 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.

Note: If the effective risk score of a customer is 0 or 0.5, a risk assessment is not created.

The cases are investigated in Enterprise Case management (ECM). The KYC system moves the risk assessments which meet the above criteria as Events to the ECM layer along with the risk scoring data, the interested party identified for the customer, and the rules met by the customer with the details of the customer and account which is used for risk scoring.

CHAPTER 2

Getting Started

This chapter provides step-by-step instruction to login to the Know Your Customer (KYC) application and different features of the Oracle Financial Services Analytical Applications (OFSAA) Application page.

This chapter discusses the following topics:

- Accessing OFSAA Applications
- Managing OFSAA Application Page
- Troubleshooting Your Display

Accessing OFSAA Applications

Access to the Oracle Financial Services KYC application depends on the Internet or Intranet environment. The system administrator provides the intranet address Uniform Resource Locator (URL), User ID, and Password. Login to the application through the Login page. You will be prompted to change your password on your first login. You can change your password whenever required by logging in. For more information, see the *Troubleshooting Your Display* section.

To access the Oracle Financial Services Analytical Application, follow these steps:

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

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

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

   The OFSAA Login page is displayed.
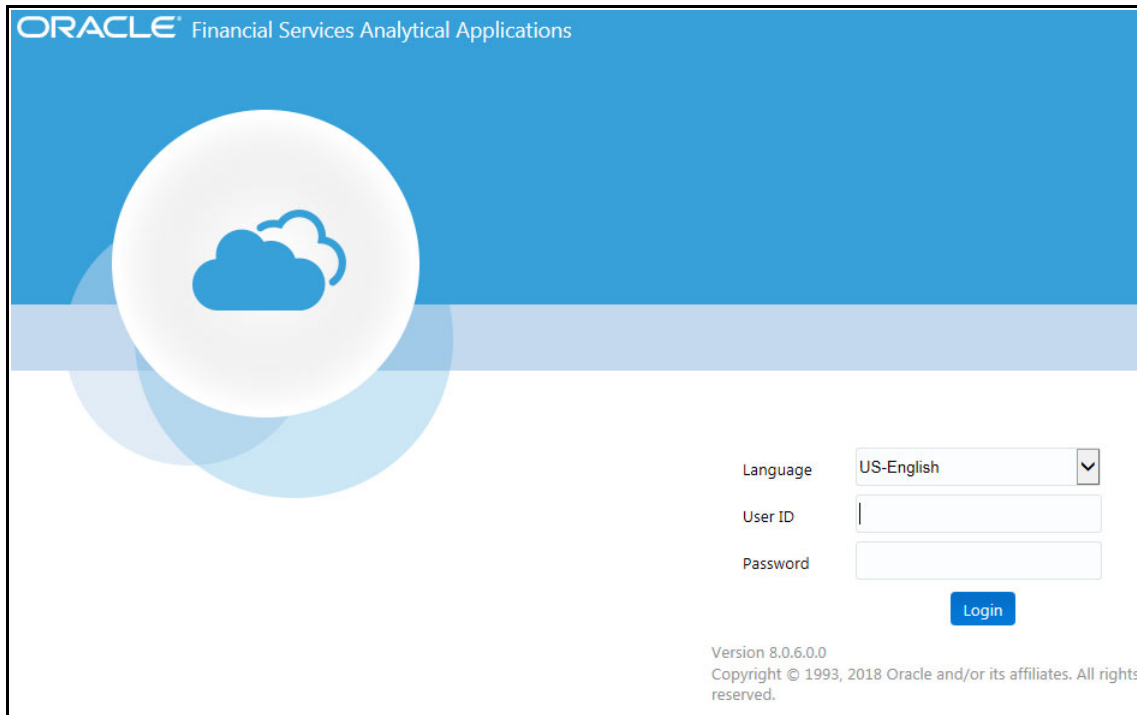
2. Select the Language from the Language drop-down list. This allows you to use the application in the language of your selection.

3. Enter your User ID and Password in the respective fields.

4. Click **Login**. The Oracle Financial Services Analytical Applications page is displayed.

Managing OFSAA Application Page

This section describes the options available for system configuration in the OFSAA Application page.

The OFSAA Application page has the following tabs:

- Behavior Detection - KYC Tab
- Common Tasks Tab

Behavior Detection - KYC Tab

The Behavior Detection - KYC tab allows the KYC administrator to do security administration for users, configure KYC application and risk assessment parameters, and configure questionnaires.

To do this, follow these steps:

1. Click the [icon] icon.
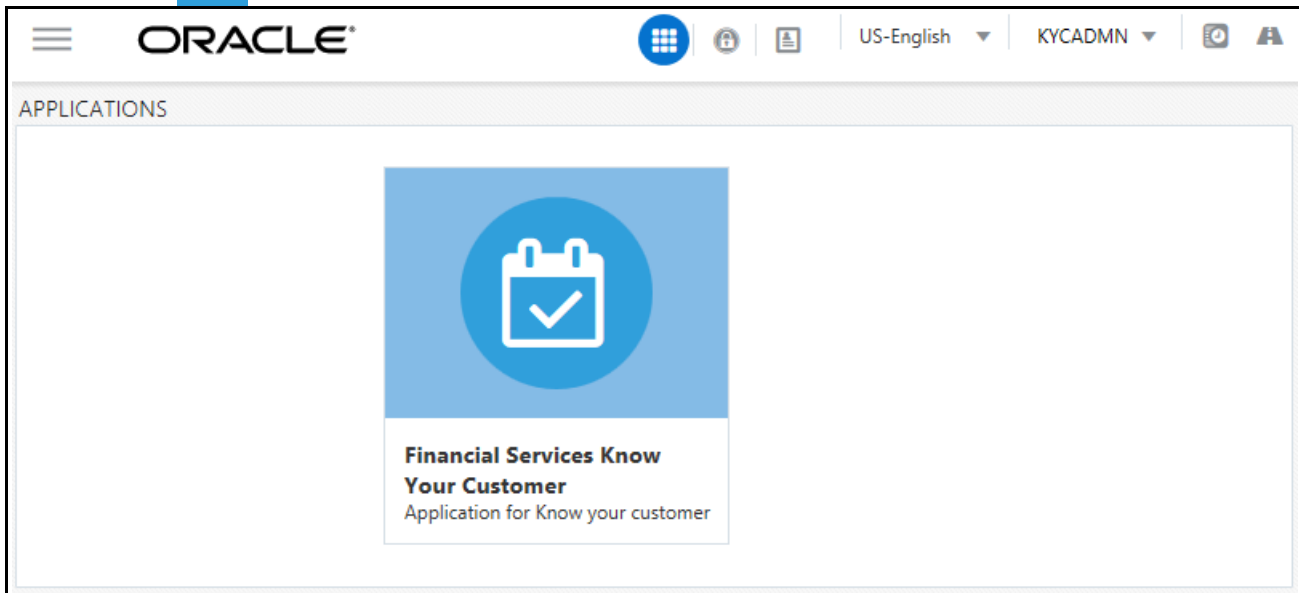
2. Click **Behavior Detection - KYC**.
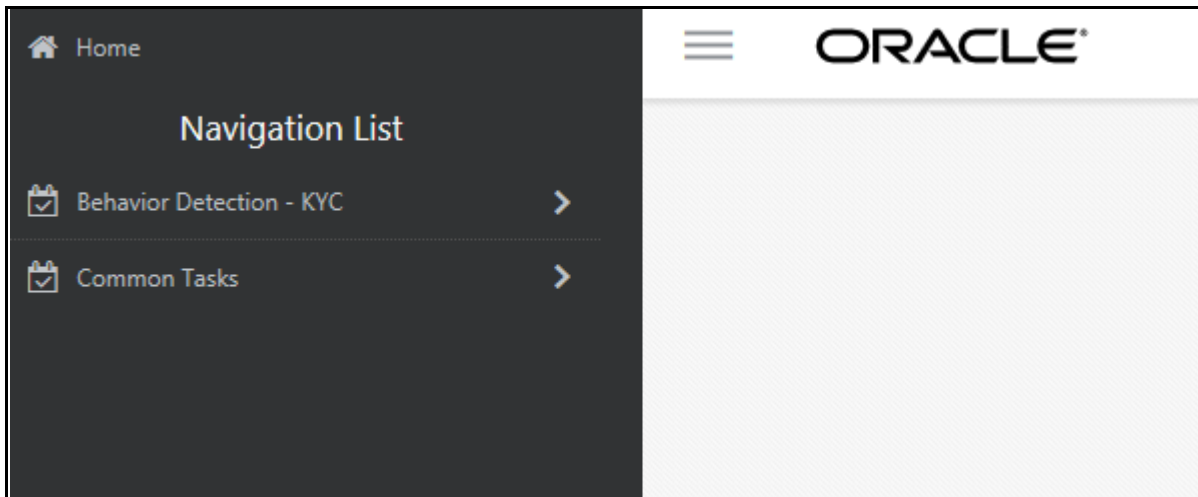
Common Tasks Tab

The Common Tasks tab allows the system administrator to configure the KYC metadata, Rule Run Framework, and KYC batches.

To do this, follow these steps:

1. Click the [icon] icon.
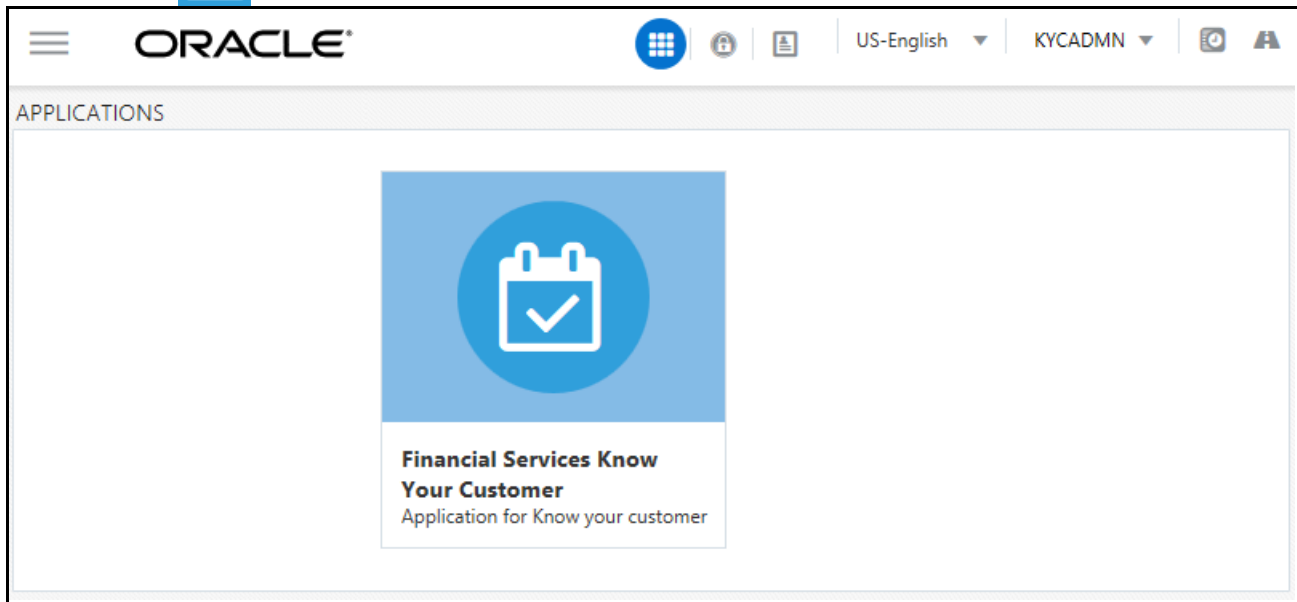
2. Click **Common Tasks**.
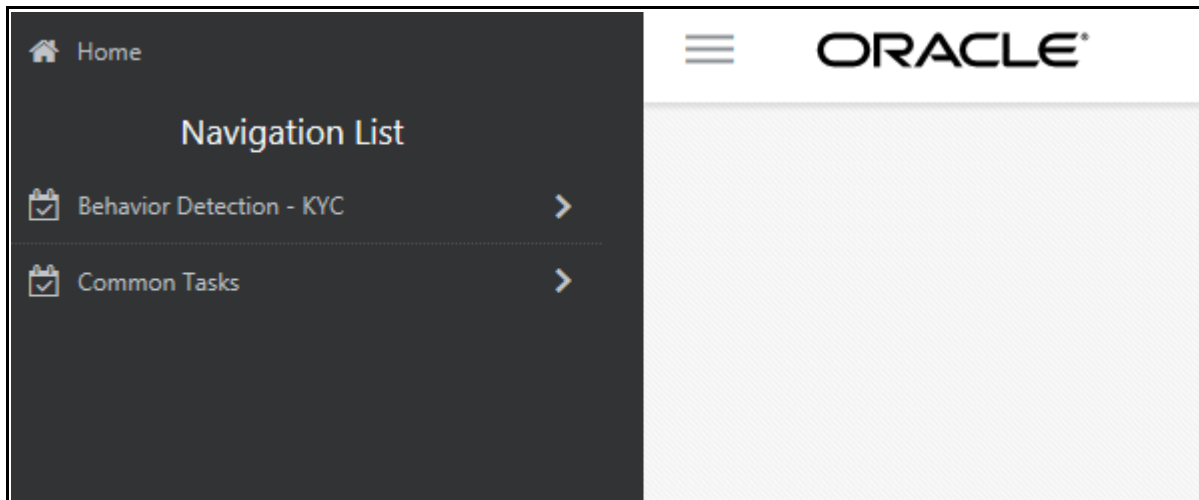
Troubleshooting Your Display

If you experience problems logging into Oracle Financial Services Transaction Filtering or with your display, the browser settings may be incompatible with running OFSAA applications. The following sections provide instructions for setting your Web display options for OFSAA applications within IE.

Note: The following procedures apply to all versions of IE listed in section. A separate procedures are listed for each version where differences exist in the locations of settings and options.

This section covers the following topics:

- Enabling JavaScript

- Enabling Cookies
- Enabling Temporary Internet Files
- Enabling File Downloads
- Setting Printing Options
- Enabling Pop-Up Blocker
- Setting Preferences

Enabling JavaScript

This section describes how to enable JavaScript.

To enable JavaScript, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.
2. Click the **Security** tab and click the **Local Intranet** icon as your Web content zone.
3. Click **Custom Level**. The Security Settings dialog box displays.
4. In the Settings list and under the Scripting setting, enable all options.
5. Click **OK,** then click **OK** again to exit the Internet Options dialog box.

Enabling Cookies

Cookies must be enabled. If you have problems troubleshooting your display, contact your System Administrator.

Enabling Temporary Internet Files

Temporary Internet files are pages that you view on the Internet and store in a folder for quick viewing later. You must adjust this setting to always check for new versions of a stored page.

To adjust your Temporary Internet File settings, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.
2. On the General tab, click **Settings**. The Settings dialog box displays.
3. Click the **Every visit to the page** option.
4. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Enabling File Downloads

This section describes how to enable file downloads.

To enable file downloads, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.
2. Click the **Security** tab and then click the **Local Intranet** icon as your Web content zone.
3. Click **Custom Level**. The Security Settings dialog box displays.

4. Under the Downloads section, ensure that **Enable** is selected for all options.

5. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Setting Printing Options

This section explains the how to enable printing background colors and images must be enabled.

To enable this option, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.

2. Click the **Advanced** tab. In the Settings list, under the Printing setting, click **Print background colors and images**.

3. Click **OK** to exit the Internet Options dialog box.

Tip: For best display results, use the default font settings in your browser.

Enabling Pop-Up Blocker

You may experience difficulty running the Oracle Financial Services Transaction Filtering application when the IE Pop-up Blocker is enabled. It is recommended to add the URL of the application to the *Allowed Sites* in the Pop-up Blocker Settings in the IE Internet Options.

To enable Pop-up Blocker, follow these steps:

1. Navigate to Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.

2. Click the **Privacy** tab. In the Pop-up Blocker setting, select the **Turn on Pop-up Blocker** option**.** The **Settings** enable.

3. Click **Settings** to open the Pop-up Blocker Settings dialog box.

4. In the Pop-up Blocker Settings dialog box, enter the URL of the application in the text area.

5. Click **Add**. The URL appears in the Allowed site list.

6. Click **Close**, then click **Apply** to save the settings.

7. Click **OK** to exit the Internet Options dialog box.

Setting Preferences

The Preferences section enables you to set your OFSAA Home Page.

To access this section, follow these steps:

1. Click **Preferences** from the drop-down list in the top right corner, where the user name is displayed. The Preferences page is displayed.
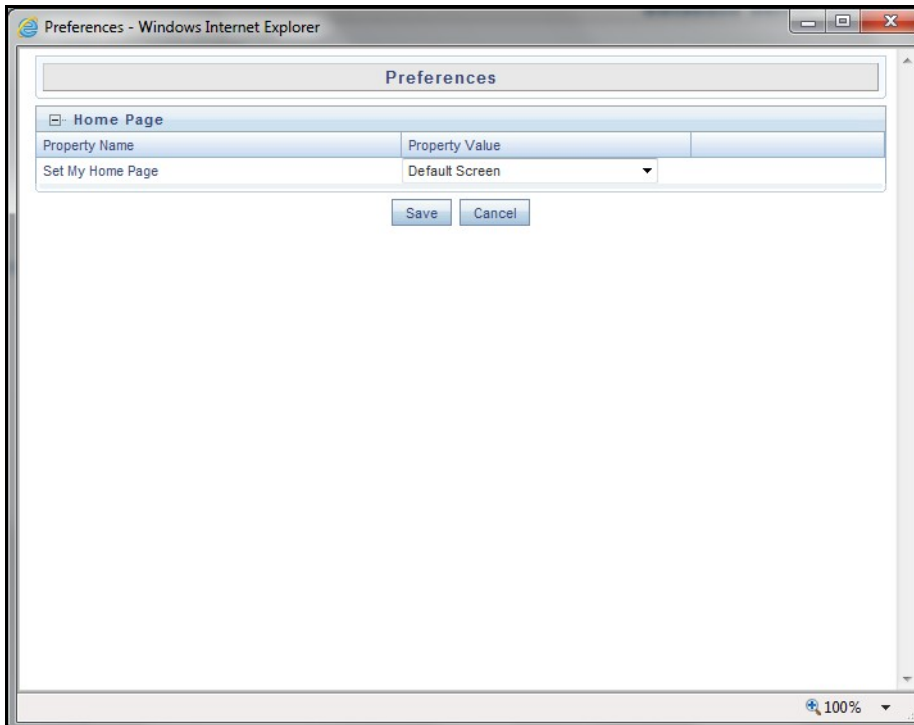
2. In the Property Value drop-down list, select the application which you want to set as the Home Page.

   Note: Whenever new application is installed, the related value for that application is found in the drop-down list.

3. Click **Save** to save your preference.

CHAPTER 3 _Managing User Administration and Security Configuration_

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

This chapter discusses the following topics:

- About User Administration
- User Provisioning Process Flow
- Managing User Administration
- Adding Security Attributes
- Mapping Security Attributes to Users

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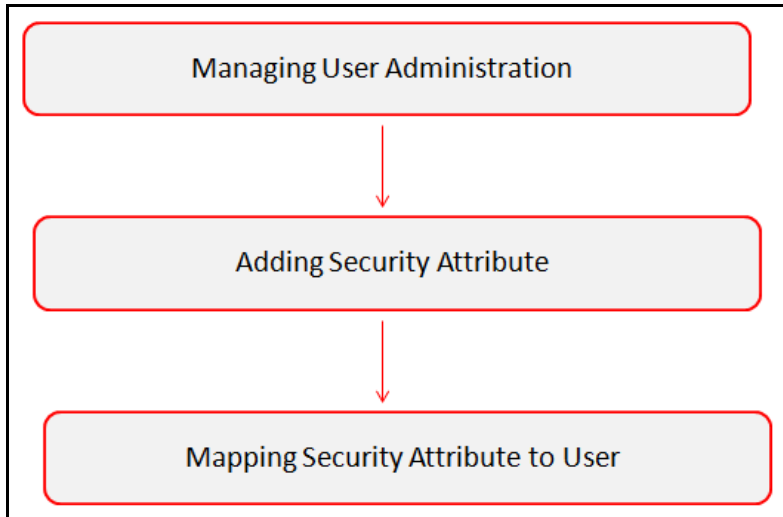
The following table lists the various actions and associated descriptions of the user administration process flow:

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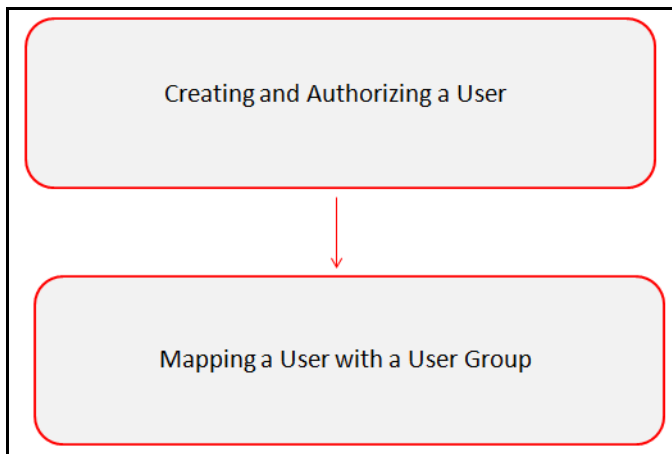
The following table lists the various actions and associated descriptions of the user administration process flow:

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	User Group
KYC Administrator User	● KYC Administrator User Group ● OB KYC Administrator Group ● IPEADMN
KYC Investigator User	● KYC Investigator User Group ● OB KYC Investigator Group

Table 5 describes the predefined KYC User Groups and the corresponding user activities.

Table 6. KYC User Groups and User Activities

User Group	User Activities
KYC Administrator User Group	The users belonging to this group will be able to perform all the KYC batch related configurations.
OB KYC Administrator Group	The users belonging to this group will be able to perform all the KYC real-time onboarding related configurations.
IPEADMN	The users belonging to this group will be able to perform all the IPE related configurations.
KYC Investigator User Group	The users belonging to this group will be able to investigate all the KYC batch risk assessments.
OB KYC Investigator Group	The users belonging to this group will be able to investigate all the KYC onboarding 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.

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.

The following security attribute is applicable for KYC:

- **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.

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).

Table 7. `KDD_JRSDCN` Table Attributes (Continued)

Column Name	Description
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')
```

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, you must 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');
```

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;
```

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') ;
```

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 must reference 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 must reference 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
```

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 must be available in the appropriate database tables and the user must be created.

- To view the Onboarding users, map the Onboarding role to the OB KYC Administrator group.

inistration >> User Administration >> Security Attribute Administration

Choose User Type: | User ⌄ | Choose User: | ⌄ |

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.

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 application 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 must be fulfilled. The user must be 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 4 — *Maintenance Activities and Configuring Setup Parameters (KYC Batch)*

This chapter provides information on the maintenance and configuration activities to be done for the KYC system.

This chapter discusses the following topics:

- Prerequisite
- Maintenance and Configuration Activities
- Integration with Enterprise Case Management

Prerequisite

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

Maintenance and Configuration Activities

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

- Initial or One time Activities
- Daily Activities

Initial or One time Activities

These are maintenance activities that need to be done only once.

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 Rule Details
- Configuring Algorithm Based Risk Parameters
- Configuring Scores for Values in KYC Risk Assessment

- Populating Data in the KDD_CODE_SET_TRNLN Table

- 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

Excel upload helps you to upload all ready-to-use metadata for multiple jurisdictions across different rules or risk parameters. If there is data for one jurisdiction from the UI, you can copy data from one jurisdiction to the other.

You can upload the following Excel sheets in the UI:

- 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 is 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.

  Note: The value in the `N_RISK_CATEGORY_KEY` column must be a unique value across jurisdictions and customer type codes.

- DIM_RA_PRIORITY: Ensure that the minimum range of consecutive rows is 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.

- APPLN_PARAMS

- APPLN_RB_PROCESSING

- DIM_WLS_FEEDBACK

  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.

You can also add a new rule, rule value, or risk parameter through the UI. For more information see *Adding Risk Parameters and Rules (KYC Batch)*.

Moving Country Data in KDD_CODE_SET_TRNLN table

KYC has multiple risk parameters which are country-based values. KYC uses the code set translation table for all code sets and their values. The country data is already available in the Geography table. The same data must also be available in the kdd_code_set_trnln table. To do this, 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;
```

Configuring Application Parameters

The parameter values 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 *Adding Risk Parameters and Rules (KYC Batch)*.

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 *Adding Risk Parameters and Rules (KYC Batch)*.

Configuring Rule Based Risk Values

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 *Adding Risk Parameters and Rules (KYC Batch)*.

Defining the Rereview Rule Details

The OFS KYC comes with pre-packaged rules based on which the Accelerated Rereview is triggered. These rules are available in the Application Rereview Parameters Table (`Appln_ReReview_Params`). . Each record contains a rule number with which it is associated in the Rereview 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 *Adding Risk Parameters and Rules (KYC Batch)*.

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 *Adding Risk Parameters and Rules (KYC Batch)*.

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. 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.

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 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 must 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`.

Note: Depending on whether KYC and ECM are installed in the same infodom or different infodom and the same machine or a different machine, synonyms for database links must be created. The list of Synonyms for database links are available in an SQL file post installation. Depending on the setup, the appropriate link muts be executed.

Scheduling KYC Batches

After the installation is complete, the user must 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 must be 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 or account and alert information available for Risk Assessment reference. All the processing batches are EOD processing. The default review execution must be 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 regular processing batch is complete. **Note:** After the KYC batch ends, the files are generated at EOD. These files can then be used by the AML system when the AML batch runs. 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. The multiple slots are to be decided only if the system requirements are unable to meet the volume of data.

Note: Slicing of data is not recommended. If it is required, you can add batch or hierarchy filters.

Partitioning IPE Tables

Partitioning of IPE tables are done in order to prevent the IPE batch from continuously running and thus help with performance. Since IPE tables add up data quickly, the batches run continuously.

To partition IPE tables, follow these steps:

1. Execute the following 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, 2) ,
V_EVAL_FLAG         VARCHAR2(100 CHAR ),
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, 2) ,
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)

)

);

To Create and Drop partition tasks as part of Regular Processing Batch, follow these steps:

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

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

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

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

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

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

To Create and Drop partition tasks as part of Deployment Initiation Batch, follow these steps:

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

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

3. Select the KYC_IPE_TABLE_CREATE_PARTITION component meta data in the RHS and Move it up to make it the first task.

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

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

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

Daily Activities

These are maintenance activities that must be done on a daily basis.

This section covers the following topics:

- Regular Processing - Account Opening Review

- Regular Processing- Accelerated Review
- Regular Processing - Rereview or Periodic
- Feedback or Application EOD Processing

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

An Accelerated Review is used to identify the customers who must be assessed. This 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 - Rereview or Periodic

After every review (Account Opening Review, Deployment Initiation, or Accelerated Rereview), 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.

Rereview Processing checks whether the Next Rereview 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.

Integration with Enterprise Case Management

KYC is integrated with ECM in order to:

- Investigate KYC events
- Promote KYC events to cases

- Close the cases

- Edit the KYC risk scores

- Execute the batches

- View the customer dashboard

Configurations in the ECM UI:

You must make the following configurations in the ECM UI. For more information, see Enterprise Case Management Administrator Guide.

- Updating the URL for the KYC Close Service

- Updating the KYC Get Overridden Risk Details URL

- Updating the BD Application URL for the KYC Customer Dashboard

- Updating the User Name and Password for the Common Gateway Service

- Updating the User Name and Password for the Create JSON Service

- Updating the User Name and Password for the KYC Risk Score UI Service

- Updating the User Name and Password for the JSON To Table Service

Updating the URL for the KYC Close Service

To update the user name and password, follow these steps:

1. Login as the ECM Administrator.

2. Navigate to **Case Management Configuration** > **Manage Common Parameters**.

3. In the Parameter Category field, select **Deployment Based**.

4. In the Parameter Name field, select **KYC Deployment**.

5. Replace 'KYC Rest Service URL' with the BD Application URL till the context name in the Attribute 1 Value field. For example: `<PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>/restapi/kycrest/AutoCloseService`

6. Click **Save** to update the details in the database.

Updating the KYC Get Overridden Risk Details URL

To update the user name and password, follow these steps:

1. Login as the ECM Administrator.

2. Navigate to **Case Management Configuration** > **Manage Common Parameters**.

3. In the Parameter Category field, select **Deployment Based**.

4. In the Parameter Name field, select **KYC Deployment**.

5. Replace the ##BD_APPLICATION_URL## placeholder with the BD Application URL till the context name in the Attribute 3 Value field. For example: `<PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>`

6. Click **Save** to update the details in the database.

Updating the BD Application URL for the KYC Customer Dashboard

To update the user name and password, follow these steps:

1. Login as the ECM Administrator.

2. Navigate to **Case Management Configuration** > **Manage Common Parameters**.

3. In the Parameter Category field, select **Deployment Based**.

4. In the Parameter Name field, select **KYC Deployment**.

5. Enter the BD Application URL till the context name in the Attribute 4 Value field. For example:
   `<PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>`

6. Click **Save** to update the details in the database.

Note:

■ To know how to manually promote KYC risk assessments to cases, see *Know Your Customer Risk Assessment Guide.*

■ To view the KYC OBI reports, see *FCCM Analytics Guide.*

■ During case closure, you can do the following in the ECM system:

   ◆ View information about the users who close the cases

   ◆ Edit the risk scores which are displayed on the case closure dates

   ◆ Override the risk expiration dates

   ◆ Update the next re-review dates

   For information on the above, see *Know Your Customer Risk Assessment Guide.*

Updating the User Name and Password for the Common Gateway Service

To update the user name and password, follow these steps:

1. Login as the ECM Administrator.

2. Navigate to **Case Management Configuration** > **Manage Common Parameters**.

3. In the Parameter Category field, select **Deployment Based**.

4. In the Parameter Name field, select **Common Gateway Deployment**.

   The Attribute 1 Value field is pre-populated with the Common Gateway Service URL during the installation process with content from the `InstallConfig.xml` file. In cases where the deployment URL is not mentioned during the installation process or if the deployment URL has changed after installation, you will need to provide the new service URL.

5. Enter the KYC Administrator user name in the Attribute 2 Value field.

6. Click **Save** to update the details in the database.

7. To update the password, navigate to the **Configuration of Web Service** screen and enter the password for the above entered KYC Administrator user in the Enter Password for Common Gateway Service field.

8. Click **Encrypt** to save the password in the database.

Updating the User Name and Password for the Create JSON Service

To update the user name and password, follow these steps:

1. Login as the ECM Administrator.

2. Navigate to **Case Management Configuration** > **Manage Common Parameters**.

3. In the Parameter Category field, select **Deployment Based**.

4. In the Parameter Name field, select **T2J Deployment**.

   The Attribute 1 Value field is pre-populated with the Create JSON Service URL during the installation process with content from the `InstallConfig.xml` file. In cases where the deployment URL is not mentioned during the installation process or if the deployment URL has changed after installation, you will need to provide the new service URL.

   The Attribute 2 Value field is pre-populated. This value must not be updated.

5. Enter the ECM Administrator user name in the Attribute 3 Value field.

6. Click **Save** to update the details in the database.

7. To update the password, navigate to the **Configuration of Web Service** screen and enter the password for the above entered ECM Administrator user in the Enter Password for Create JSON Service field.

8. Click **Encrypt** to save the password in the database.

To update the user name and password in ECM, follow these steps:

1. Login to the ECM config schema.

2. Update the placeholder in the below script and execute the same in the config schema.

```
update aai_wf_application_api_b  SET V_PARAM_1 =
'##BASE64ENCODED_ECMADMINUSERNAME:ECMADMINPASSWORD##' where V_APP_API_ID ='1543401257828';
/
commit
/
```

Updating the User Name and Password for the KYC Risk Score UI Service

To update the user name and password, follow these steps:

1. Login as the ECM Administrator.

2. Navigate to **Case Management Configuration** > **Manage Common Parameters**.

3. In the Parameter Category field, select **Deployment Based**.

4. In the Parameter Name field, select **KYC Deployment**.

   The Attribute 5 Value field is pre-populated with the KYC Service URL during the installation process with content from the `InstallConfig.xml` file. In cases where the deployment URL is not mentioned during the installation process or if the deployment URL has changed after installation, you will need to provide the new service URL.

5. Enter the KYC Administrator user name in the Attribute 6 Value field.

6. Click **Save** to update the details in the database.

7. To update the password, navigate to the **Configuration of Web Service** screen and enter the password for the above entered KYC Administrator user in the Enter Password for KYC Onboarding Risk Score Service URL field.

8. Click **Encrypt** to save the password in the database.

Updating the User Name and Password for the JSON To Table Service

To update the user name and password in PMF, follow these steps:

1. Login to the ECM config schema.

2. Update the placeholder in the below script and execute the same in the config schema.

```
update aai_wf_application_api_b  SET V_PARAM_1 =
'##BASE64ENCODED_KYCADMINUSERNAME:KYCADMINPASSWORD##' where V_APP_API_ID ='1543401605699';
/
commit
/
```

Managing KYC Batches

This chapter provides information on how to manage the different KYC batches.

This chapter discusses the following topics:

- About KYC Batches
- Deployment Initiation Processing
- End of Day Processing
- Regular Processing
- Running KYC Batches
- Running a Single Task Using a Batch
- Scheduling a Batch
- KYC Batch Execution Logs

Note: Before you Create a batch, ensure that all the necessary batch uploads mentioned in Adding Risk Parameters and Rules (KYC Batch) 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.

Adding the Beneficial Owner Process to the Deployment Initiation Processing Batch

The `KYC_PopulateBeneficialOwner` process is not available in the ready-to-use Deployment Initiation Processing Batch. To add the process:

1. Login to the KYC Application.
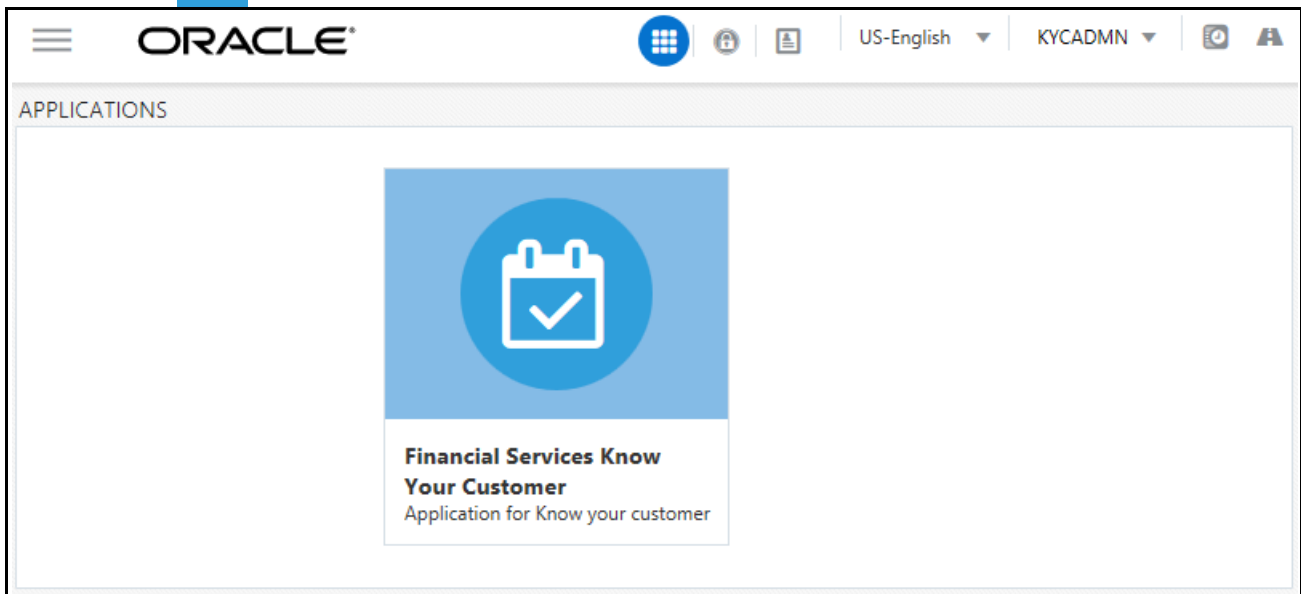
2. Click the icon.

3. Click **Common Tasks** > **Rule Run Framework** > **Run**.
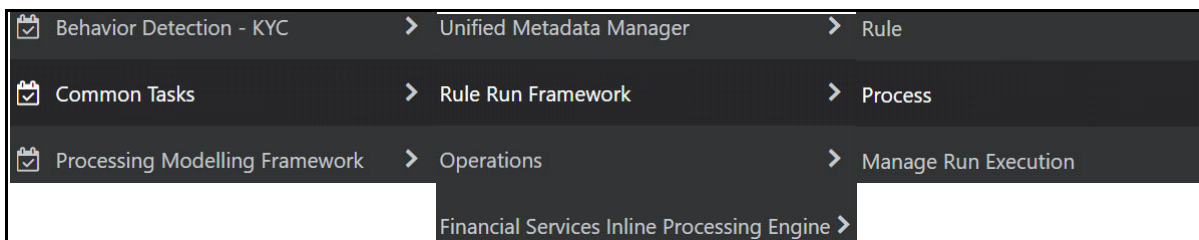
4. In the Run screen, select the **IPEKYCRunDI** code and click **Edit**.

5. Click **Selector** > **Job**.

6. In the List section, expand Processes > FCCMSEGMNT and double-click the `KYC_PopulateBeneficialOwner` task.

    The task moves to the Tasks section.

7. Move the `KYC_PopulateBeneficialOwner` process to below the `KYC_DI_Interested_Party:SD` process and above the `KYC_DI_Watchlist_Scan` process.

8. Click **Ok.**

9. Resave the run and trigger a fresh run. This ensures that the changes are saved and displayed.

Setting the Interested Party Level

This parameter allows the user to set the customer's level of relationship with the interested parties. By default, it is 1.

●   If the interested party relationship is not required for the customer, the user can set the value to 0.
There are two ways to set the interested party level.

1. To set the interested party level using the database, update the value of the following parameter.

    Parameter Name: LVL_IDF_IP

    Table Name: APPLN_INSTALL_PARAMS

2. To set the interested party level using UI, follow these steps.

    a. Login to the KYC application as KYC Administrator.

    b. Click **Behavior Detection - KYC.** Select **Manage KYC Configuration** and click **Manage KYC Installation Parameters**.

    c. On the **Manage KYC Installation Parameters** page, Select **KYC** as **Parameter Category** and **Manage KYC Installation Parameters** as **Parameter Name**.

    d. Update the Attribute 1 Value and provide your comments.

Figure 2. Setting the Interested Party Level

| Attribute 1 Name: | LVL_IDF_IP | Attribute 1 Description: | Level of Identification : Default and allowed value is 2 | Attribute 1 Value: | 1 | Comments: | |

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

    This action updates the Interested Party Level.

End of Day Processing

This topic covers the following sections:

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

●   Customer - Risk Assessment Details

●   Customer - Risk Assessment History

- Renaming and Transferring Feedback files

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.

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 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 predefined 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 Rules 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 **DIM_RISK_CATEGORY** table. The values in the **F_USR_REVIEW_REQ_FLAG** and **F_HIGH_RISK_WATCH_LIST_FLAG** parameter must always be set to N; if you set the **F_HIGH_RISK_WATCH_LIST_FLAG** parameter to Y, then a case is generated irrespective of the risk score. For more information on the columns, see Appendix B in the *KYC Risk Assessment Guide.*

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

Whenever risk assessments are promoted to cases based on certain criteria, there may be a few risk assessments which are not promoted due to 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. Click **Common Tasks**.

3. Click **Rule Run Framework**.

4. Click **Run**. The Run page is displayed.

   Click ▤ to expand the page.

5. Select the particular batch that you want to run and click **Fire Run**. The Fire Run page is displayed.

		Code		Name	Type	Folder	Version	Active
	☐	IPEKYCEODDI		IPEKYCEODDI	Base Run	FCCMSEGMNT	0	Yes
	☐	IPEKYCRun		IPEKYCRun	Base Run	FCCMSEGMNT	0	Yes
	☐	IPEKYCRunDI		IPEKYCRunDI:SD	Base Run	FCCMSEGMNT	0	Yes

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

7. 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. Click **Common Tasks**.

3. Click **Operations**.

4. Click **Batch Execution**. The Batch Execution page is displayed.

5. From the Batch Details section, select the particular batch that you want to execute.

6. From the Task Details section, click ⊡. The Task Mapping window is displayed.
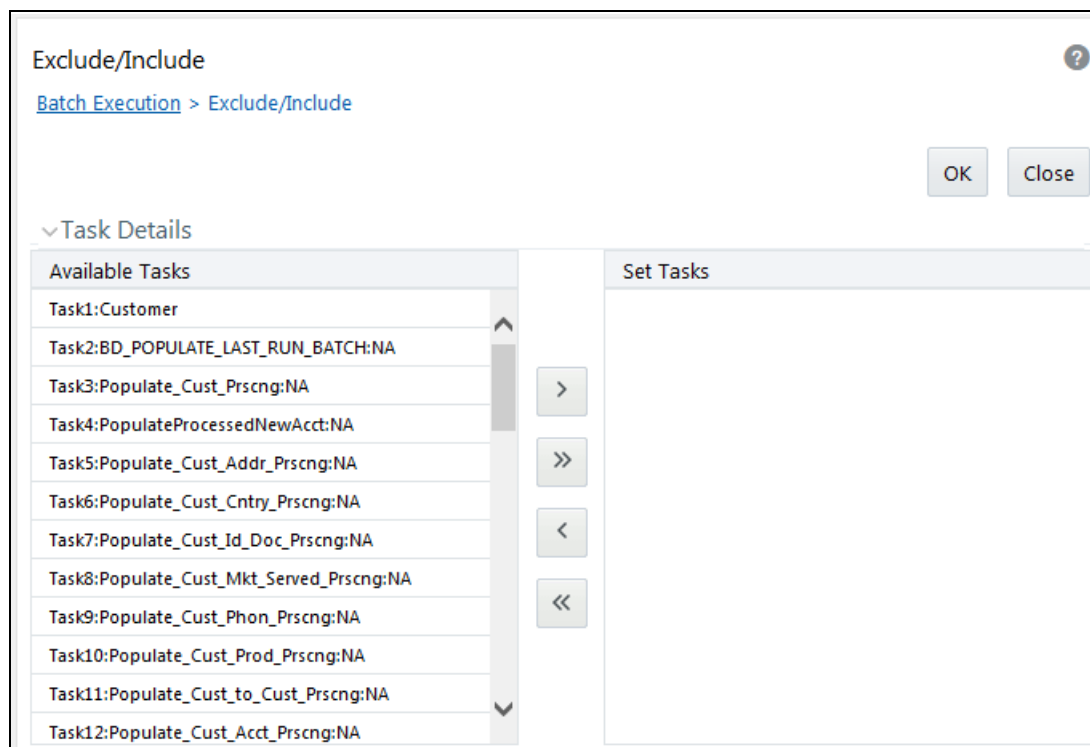
7. Retain the tasks that you want to execute under the Available Tasks section and move the rest to the Set Tasks section.

8. 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)?*

9. Click **OK**.

10. 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. Click **Common Tasks**.
3. Click **Operations**.
4. Click **Batch Scheduler**. The Batch Scheduler page is displayed.

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

9. 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. Click **Common Tasks**.

3. Click **Operations**.

4. Click **Batch Scheduler**. The Batch Scheduler page is displayed.

5. Select a batch that you want to schedule from the list of available batches. The Batch Scheduler section is expanded and displays additional options.

6. Click **New Schedule**.

7. Set the frequency of the new schedule as **Daily**.

8. Enter the schedule time of the batch by specifying the **Dates**, **Run Time**, and **Every** information.

9. 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. Click **Common Tasks**.

3. Click **Operations**.

4. Click **Batch Scheduler**. The Batch Scheduler page is displayed.

5. Select a batch that you want to schedule from the list of available batches. The Batch Scheduler section is expanded and displays additional options.

6. Click **New Schedule**.

7. Set the frequency of the new schedule as **Weekly**.

8. Enter the schedule time of the batch by specifying the **Dates**, **Run Time**, **Every, Working days of the Week** information.

9. 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. Click **Common Tasks**.

3. Click **Operations**.

4. Click **Batch Scheduler**. The Batch Scheduler page is displayed.

5. Select a batch that you want to schedule from the list of available batches. The Batch Scheduler section is expanded and displays additional options.

6. Click **New Schedule**.

7. Set the frequency of the new schedule as **Monthly**.

8. Enter the schedule time of the batch by specifying the **Dates**, **Run Time**, and **Occurrence** information.

9. Click **Save**.

Scheduling an Adhoc Batch

To schedule an adhoc batch, follow these steps:

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

2. Click **Common Tasks**.

3. Click **Operations**.

4. Click **Batch Scheduler**. The Batch Scheduler page is displayed.

5. Select a batch that you want to schedule from the list of available batches. The Batch Scheduler section is expanded and displays additional options.

6. Click **New Schedule**.

7. Set the frequency of the new schedule as **Adhoc**.

8. Click [+]. A new row is added in the Schedule Time section.

9. Provide the information date, run date, and run time.

10. 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:

`<FIC_HOME>/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.

- `<FIC_HOME>/ficdb/log/date/DT_KYC12DOM_1221824179931_20121123_1_Task23.log`

- `<FIC_HOME>/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:

`<FIC_HOME>/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 `<FIC_HOME>/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.

KYC Onboarding

This chapter provides information on the different processes involved in Know Your Customer (KYC) Onboarding.

This chapter discusses the following topics:

- Moving Country Data in KDD_CODE_SET_TRNLN table
- Configuring the Service Parameters through the User Interface
- Performing Assessments on Related Customers
- Excel Upload of Data
- Adding Rule Values for Rule-based Risk Assessments
- Modifying the Algorithm-based Risk Assessments
- Modifying the Risk Scores and Viewing the Risk Categories
- Mapping KYC Rules to Customer Evaluation Names
- Modifying Risk Scores for KYC Risk Models
- Modifying and Adding the Mapping Codes within KYC

Moving Country Data in KDD_CODE_SET_TRNLN table

Note: Ignore this step if this is already performed for Chapter 4.

KYC has multiple risk parameters which are country-based values. KYC uses the code set translation table for all code sets and their values. The country data is already available in the `Geography` table. The same data must also be available in the `kdd_code_set_trnln` table. To do this, 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;
```

Configuring the Service Parameters through the User Interface

The following UIs are used for configuring the service parameters of the KYC Onboarding services. This is done so that the Onboarding system knows the service parameter values which need to be hit during the Onboarding process.

- Configuring the Onboarding Service Parameters
- Configuring the Common Gateway Service Parameters

Configuring the Onboarding Service Parameters

Use the Configure Service Parameters UI to configure the service URL, service user name, and service password for all services.

The service URLs are pre-populated during the installation process with content from the `InstallConfig.xml` file. In cases where the deployment URL is not mentioned during installation, or if the deployment URL has changed after installation, you will need to provide the new service URL.

The service user name and password must be updated for all services except the AAI Authorization Service and the Initiate OB URL.

Note:

- Ensure that all service user names and service passwords provided are of valid OFSAA KYC Administrator users.

- For the ECM Case Creation URL service, the service user name and service password provided must be of a valid OFSAA ECM Administrator user.

To view the UI:

1. Log in to the KYC application as a KYC Administrator. For more information, see *Getting Started*.

2. Click **Behavior Detection - KYC > Manage KYC OB Configuration > Configure Service Parameters**.
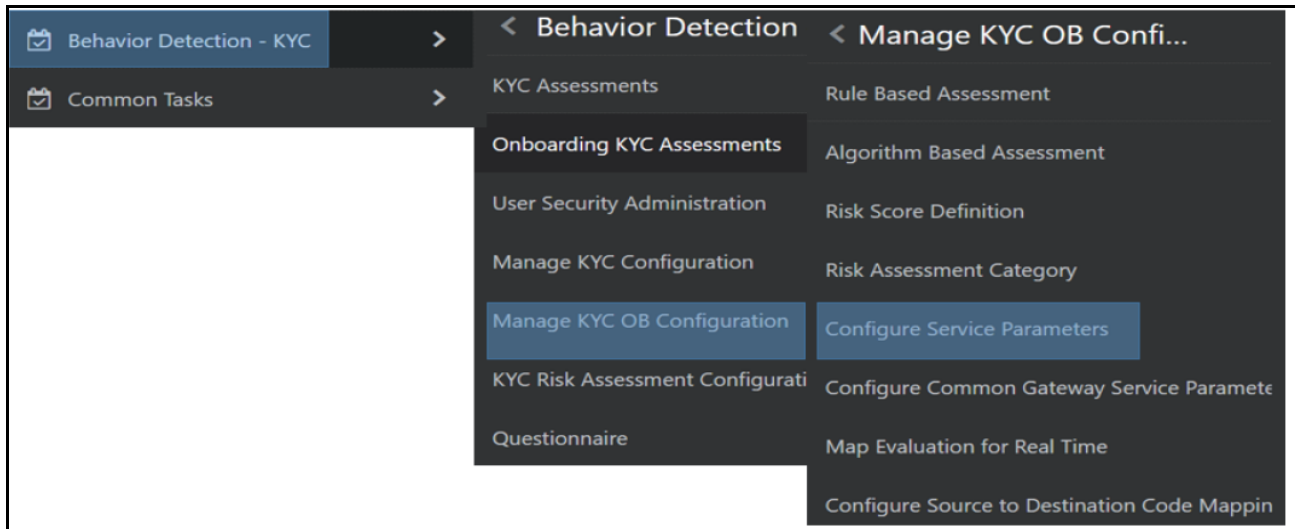
The Configure Service Parameters UI appears. You can select one of the following services:

- **AAI Authorization Service**

- **Initiate OB URL**

- **Process Modeling Framework Service**

- **Table to JSON Mapping Utility**

- **ECM Case Creation URL**

- **Generate Case Input URL**

- **Common Gateway Service URL**

Modifying the Web Service Parameter Details

The fields shown in the image are displayed when you select *Initiate OB URL* as the Service Name.

- In the **Service Name** field, select the web service for which you want to edit the service parameters.

- In the **Service URL** field, update the service URL if the deployment URL is not mentioned during installation, or if the deployment URL has changed after installation.

- For any service apart from the *Initiate OB URL* or *AAI Authorization Service* services, update the service user name in the **Service User Name** field with a valid KYC Administrator user name.

- For any service apart from the *Initiate OB URL* or *AAI Authorization Service* services, update the service password in the **Service Password** field with a valid KYC Administrator password.

- Click **Save** to save the details.

The Edit Service Parameters section is applicable only for the Process Modeling Framework service.

The three applicable parameters and their corresponding values are shown:

- PMF_PROCESS: KYC_ONBOARDING

- INFODOM: Installation Specific

- LOCALE: en_US

All the three parameters are pre-populated and should be changed only if there is a change in these values post Installation.

Configuring the Common Gateway Service Parameters

Use the Common Gateway Service Parameters UI to edit the service parameters related to the common gateway service.

To view the UI:

1. Log in to the KYC application as a KYC Administrator. For more information, see *Getting Started*.

2. Click **Behavior Detection - KYC > Manage KYC OB Configuration > Configure Common Gateway Service Parameters**.
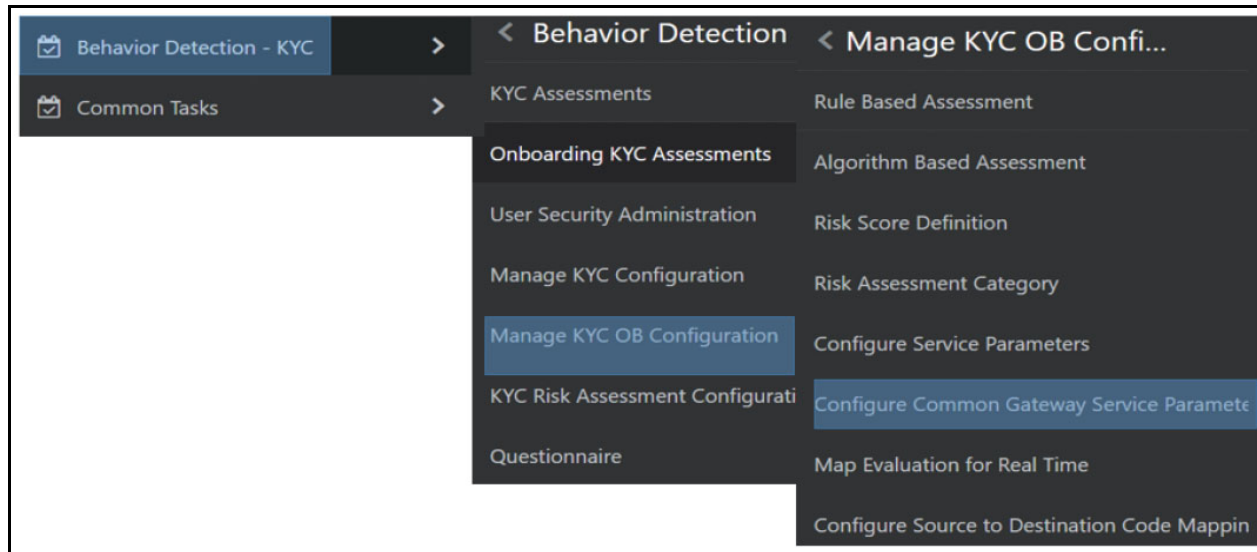
The Configure Common Gateway Service Parameters UI appears. You can select one of the following services:

- **AAI Authorization Service**

- **Internal Watch List Service**

- **Process Modeling Framework**

Modifying the Web Service Parameter Details

The fields shown in the image are displayed when you select *AAI Authorization Service* as the Service Name.

- In the **Service Name** field, select the web service for which you want to edit the service parameters.

- In the **Service URL** field, update the service URL if the deployment URL is not mentioned during installation, or if the deployment URL has changed after installation.

- For any service apart from the *AAI Authorization Service* service, update the service user name in the **Service User Name** field with a valid KYC Administrator user name.

- For any service apart from the *AAI Authorization Service* service, update the service password in the **Service Password** field with a valid KYC Administrator password.

- Click **Save** to save the details.

Note: Once you have made the above changes, you must restart the web server.

Performing Assessments on Related Customers

Note: Ensure that you perform the following configuration for all relationship types before running batch and onboarding jobs.

Full KYC is performed on primary customers. Both Full or Partial KYC can be performed on related customers. For example, a primary customer, Mark, has two related customers, one with the Authorized Signatory (AUS) and relationship type, and the other as a Parent relationship type. Full KYC is performed on Mark and the related customer who is the Parent, while only name and address matching is performed on the related customer who is the Authorized Signatory. A case is generated on the customer who has the highest score.

For related customers, you can choose which related customer must be scored using the **RelationshipCode** field. When the request JSON is sent to the KYC system, full KYC or partial KYC is done on related customers based on the values in the columns. For example, a full KYC is done on customers for whom the jurisdiction code is AMEA and relationship code is DIR, and a partial KYC (name and address verification) is done on customers for whom the jurisdiction code is AMEA and relationship code is CEO.

Use the **Relationship Type Definition** UI to choose the mode of assessment based on the Relationship Type and for a specific jurisdiction.

To view the UI:

1. Log in to the KYC application as a KYC Administrator. For more information, see *Getting Started*.

2. Click **Behavior Detection - KYC** > **Manage KYC OB Configuration** > **Relationship Type Definition**.
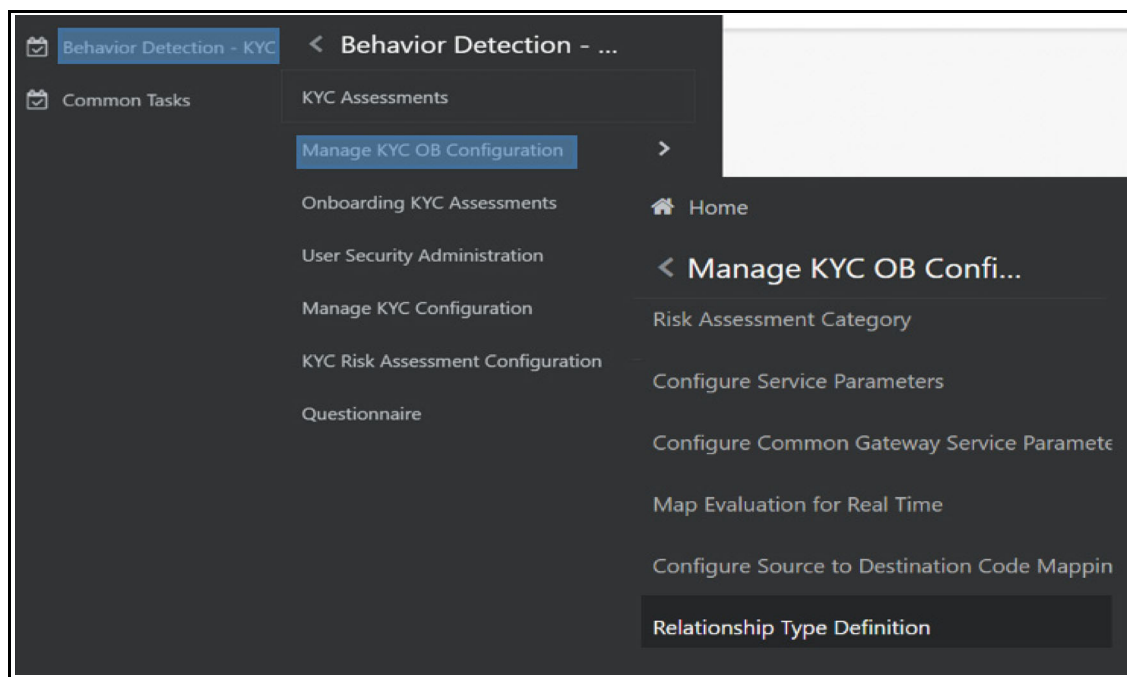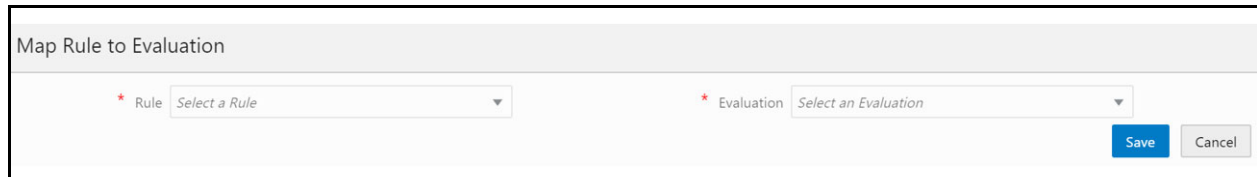
The **Relationship Type Definition** UI is displayed. In the **Search** section, select the jurisdiction of the primary customer. Based on the jurisdiction selected, the relationship type of the related party and the type of KYC performed on the related party are displayed.

If a new related customer, Beneficiary Owner, is added to the primary customer, you can click **Add** to add a new relationship type. Provide the relationship type and assessment mode and click **Save**.

To change the assessment mode of the related customer who is the Authorized Signatory from name and address screening to full KYC screening, click **Edit** to change the assessment mode. Provide the new assessment mode and click **Save**.

To remove on the related customers, click **Delete** and click **Yes** in the dialog box which appears.

Excel Upload of Data

Excel upload is a process where in the data for a particular table is uploaded in to the system as the base data according to the configurations. Once the data is uploaded, the data can be modified using the user interface.

- **FCC_OB_RISK_CATEGORY.xls**: This Excel has the configurations for risk category and case creation for a range of scores for the customer type and Jurisdiction. Once the data is uploaded into the system the data can be modified using the user interface.

- **FCC_OB_RSK_PRMS_JRSD_CUST_MAP.xls**: This Excel has the Risk Parameter configurations applicable to Customer Type and Jurisdiction. Once the data is uploaded into the system the data can be modified using the user interface.

- **FCC_OB_RSKPRMS_JRSDCUST_MAP_ST.xls**: This Excel has the Risk Parameter configurations applicable to Customer Type and Jurisdiction along with config_id to track changes made to risk parameters. Whenever data is uploaded using the FCC_OB_RSK_PRMS_JRSD_CUST_MAP.xls, the same data has to be uploaded in this excel along with a new column config_id. If the

"FCC_OB_RSKPRMS_JRSDCUST_MAP_ST" table has data, then update the column config_id with the max(config_id)+1. If there is no data in the "FCC_OB_RSKPRMS_JRSDCUST_MAP_ST" table, update the column 'config_id' as 1.

- **FCC_OB_RISK_PARAMS.xls**: This Excel allows the user to add new rules or parameters. The application is pre-packaged with ready-to-use rules and parameters which are available once you install the KYC application. This excel can be used only to add any new rules or parameters if required for the specific installation.

Note: Any new parameter id must begin with '*500..*

To view the Excel sheet, go to `FIC_HOME/ftpshare/STAGE/ExcelUpload/TEMPLATE`.

To upload the Excel sheet:

1. Log in to the KYC application. For more information, see *Getting Started*.

2. Click **Common Tasks > Unified Metadata Manager > Data Entry Forms and Queries > Bulk Upload > Excel Upload (Atomic)**.
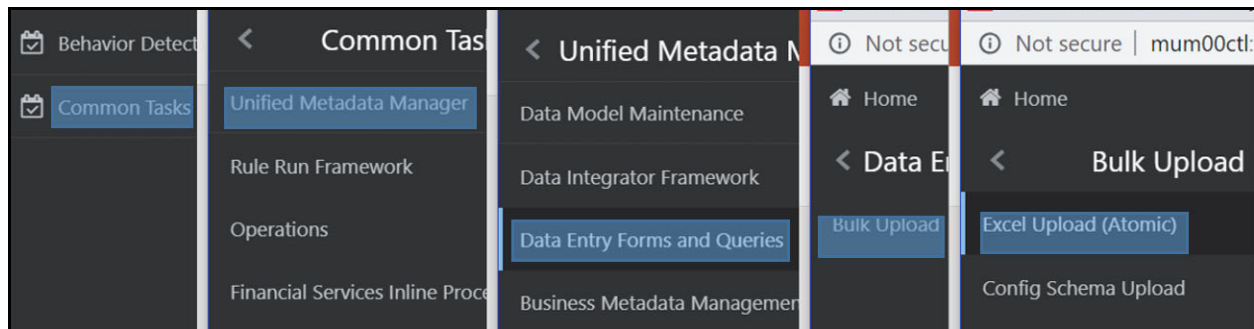
3. Click **Excel Upload** to select the Excel sheet that you want to upload.

4. In the **Excel File to Upload** section, click **Choose File** to select the file that you want to upload.

Note: During the upload, the name of the Excel must be the same as the name provided in the template. If there is any discrepancy, the upload will fail.

5. In the **Excel-Entity Mappings** section, click the arrow and select the file that you want to upload. A few of the fields are displayed as a preview.

6. Click **Upload.**

The selected Excel sheet is now uploaded. To view the Excel upload logs, click **View Log**.

Adding Rule Values for Rule-based Risk Assessments

Use the Rule-based risk assessment UI to add a rule value and to enable or disable the risk parameter during the risk assessment.

To view the UI:

1. Log in to the KYC application. For more information, see *Getting Started*.

2. Click **Behavior Detection - KYC > Manage KYC OB Configuration > Rule Based Assessment**.
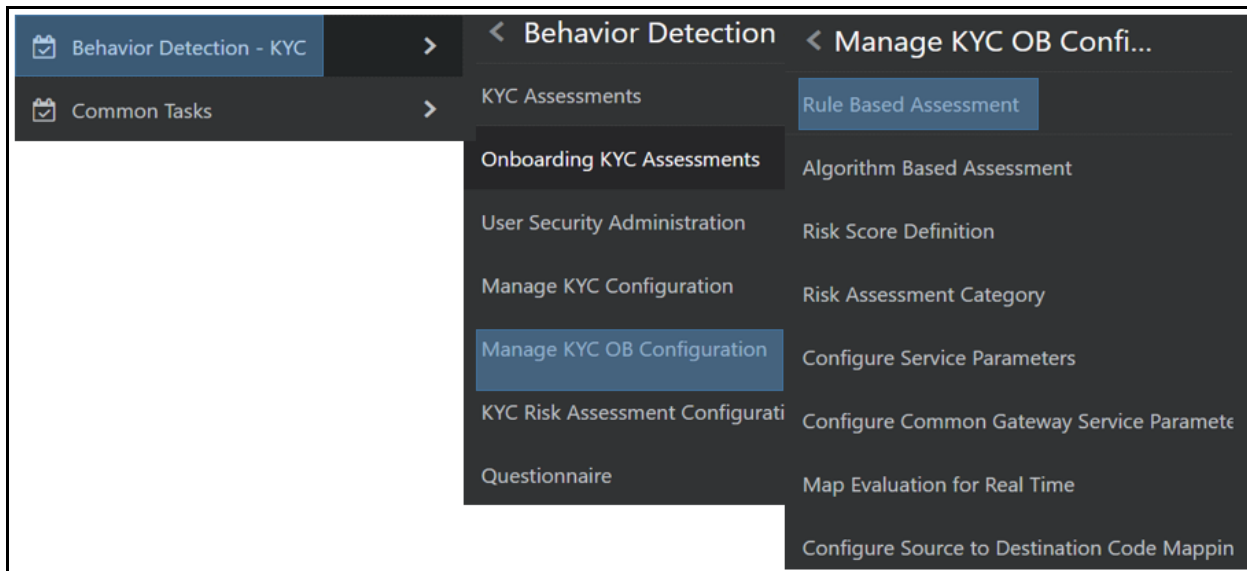
The Rule-based risk assessment UI appears with the **Search** section displayed.
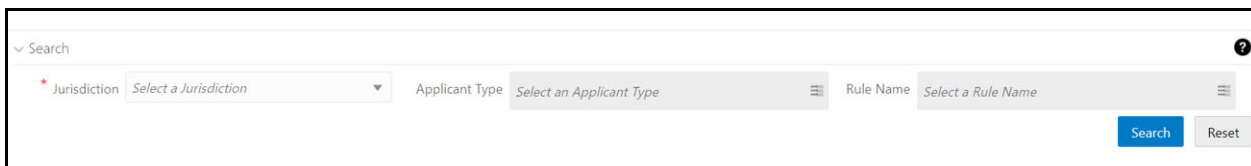
In the **Jurisdiction** field, select the jurisdiction applicable to the risk assessment. All rules defined for the selected jurisdiction appear. You can further filter your search based on an applicant type or rule name.

Adding a Rule

To add a rule:

1. Click the rule name for which the rule value must be modified.

2. Click **Add Rule Value**.

3. Provide a new rule value for the rule.

4. Click **Save**.

To view the rule values for all rules, click **View Rule Value List**.

Enabling or Disabling the Risk Parameter during Risk Assessments

To enable or disable the risk parameter:

1. Click inside the **Active** field and click the **drop-down arrow**.

2. Select **N** to disable the risk parameter during the risk assessment. Select **Y** to enable the risk parameter during the risk assessment.

Note: By default, the value is set to **Y**.

3. Click **Save**.

Modifying the Algorithm-based Risk Assessments

In the Algorithm-based risk assessment UI, you can modify the weight assigned to a risk parameter and enable or disable the risk parameter during the risk assessment.

To view the UI:

1. Log in to the KYC application. For more information, see *Getting Started*.

2. Click **Behavior Detection - KYC > Manage KYC OB Configuration > Algorithm Based Assessment**.

The Algorithm-based risk assessment UI appears with the **Search** section displayed.

Select the **jurisdiction** and **applicant type** of the risk assessment.

Modifying the Weight of the Risk Parameter

To modify the weight:

1. Double-click the **weight value** and provide the new weight value.

2. Click **Save**.

Note: The weights of all parameters, when added, must equal 100.

Enabling or Disabling the Risk Parameter during Risk Assessments

To enable or disable the risk parameter:

1. Click inside the **Active** field and click the **drop-down arrow**.

2. Select **N** to disable the risk parameter during the risk assessment. Select **Y** to enable the risk parameter during the risk assessment.

Note: By default, the value is set to Y.

3. Click **Save**.

Modifying the Risk Scores and Viewing the Risk Categories

Use the Risk Assessment Category UI to modify the risk scores and view the risk category assigned for a jurisdiction and applicant type.

To view the UI:

1. Log in to the KYC application. For more information, see *Getting Started*.

2. Click **Behavior Detection - KYC > Manage KYC OB Configuration > Risk Assessment Category**.

The Risk Assessment Category UI appears with the **Search** section displayed.

Select the **jurisdiction** and **applicant type** of the risk assessment.

The risk scores and risk category for the applicant types appear.

Modifying the Risk Scores

To modify the minimum and maximum risk scores:

1. Select the **row** for which you want to modify the risk scores using the check box.

2. Double-click the **score value** and provide the new score value.

3. Click **Save**.

Scores must be provided in such a way that the maximum score of a particular applicant type must be equal to the minimum score of the applicant type in the next row.

In the above image, the maximum score of the Financial Institution applicant type in the first row is 55 and the minimum score of the Financial Institution applicant type in the second row is also 55.

Note: The minimum score of the first row must always be equal to or more than zero. The maximum score of the last row must always be 100.

Mapping KYC Rules to Customer Evaluation Names

Use the Map Evaluation for Real Time UI to map the rule name or the parameter name from the Excel template to the evaluation name provided by the customer.

To view the UI:

1. Log in to the KYC application. For more information, see *Getting Started*.

2. Click **Behavior Detection - KYC > Manage KYC OB Configuration > Map Evaluation for Real Time**.
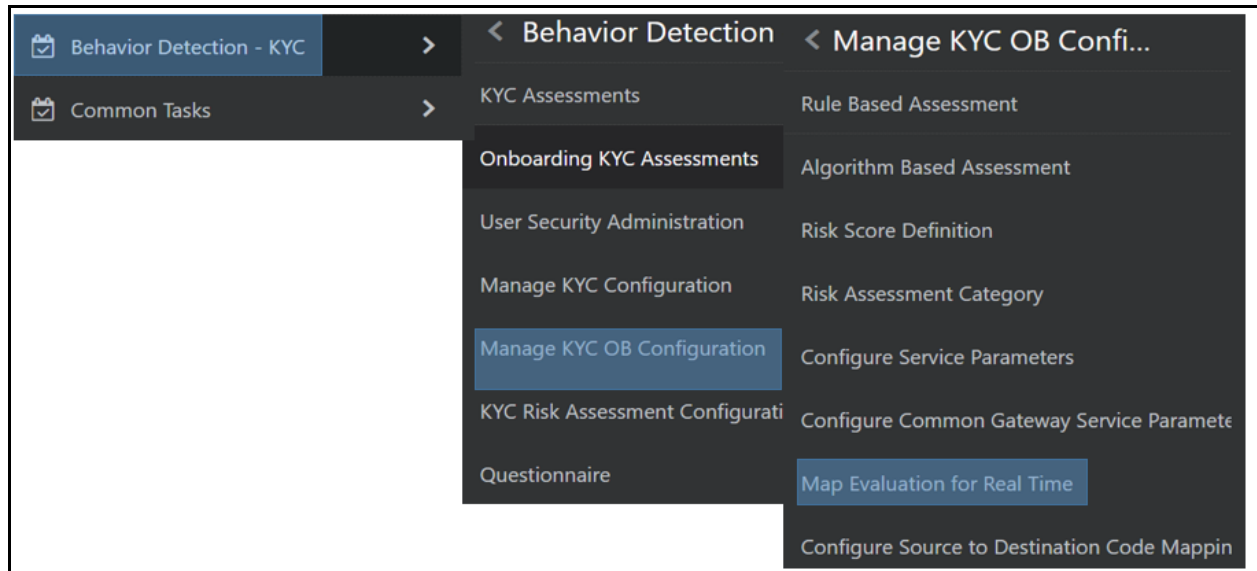
The rule names and associated evaluations for Algorithm-based and Risk-based assessments appear.

Mapping Rules to Evaluations
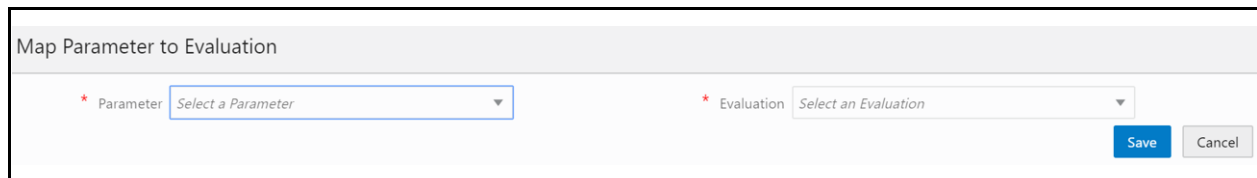
To map the rules to their respective evaluation names:

1. Click **Map Rule**.

2. Select the **rule** and the **associated evaluation name** which needs to be mapped to the rule.

3. Click **Save**.

Mapping Parameters to Evaluations

To map the parameters to their respective evaluation names:

1. Click **Map Parameter**.

2. Select the **parameter** and the **associated evaluation name** which needs to be mapped to the parameter.

3. Click **Save**.

Modifying Risk Scores for KYC Risk Models

Use the Risk Score Definition UI to provide the risk scores for the KYC risk models.

To view the UI:

1. Log in to the KYC application. For more information, see *Getting Started*.

2. Click **Behavior Detection - KYC > Manage KYC OB Configuration > Risk Score Definition**.
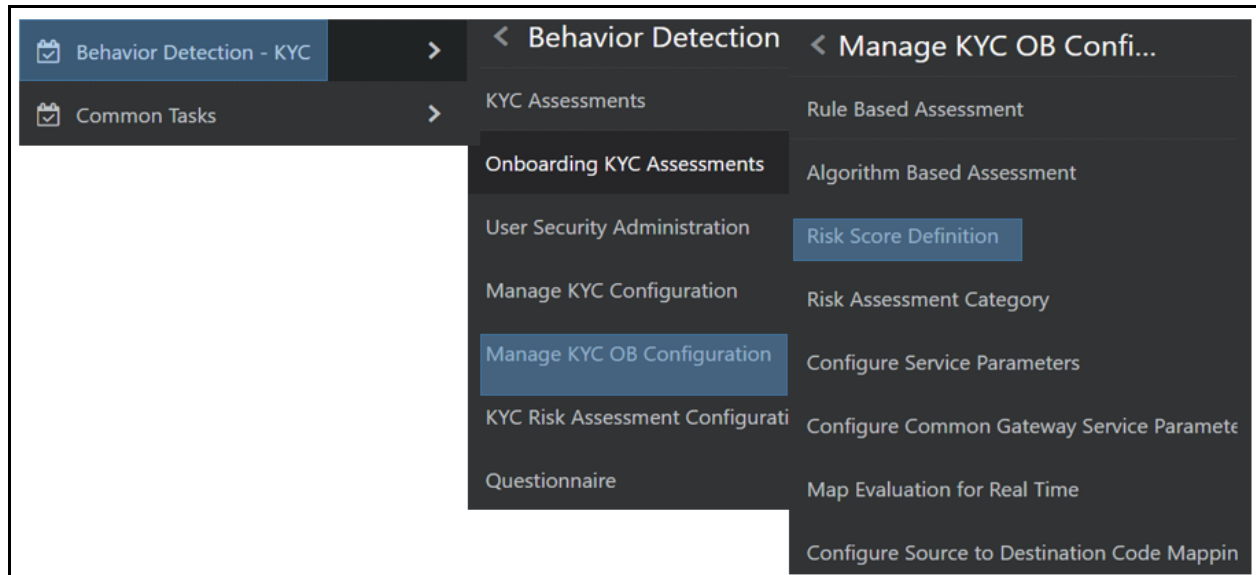
The Risk Assessment Category UI appears with the **Search** section displayed. In the **Search** section, provide the following values:

- **Jurisdiction**: The jurisdiction values are made available once you upload the KDD_JRSDCN Excel file.

- **Risk Scoring Model Type**: The model type can be Algorithm-based or Rule-based. These values are populated from the fcc_ob_rsk_prms_jrsd_cust_map table.

Note: The model types appear only after you select a **jurisdiction**.

- **Applicant Type**: The applicant type can be Individual, Financial Institution or Organization. These values are populated from the kdd_code_set_trnln table.

Note: The applicant types appear only after you select a model type.

- **Parameter/Rule Name**: The risk parameters and rules that are defined in the fcc_ob_rsk_params table appear.

Note: The parameter/rule names appear only after you select an **applicant type**.

The Applicant type, Parameter /rule name, Parameter value, and Risk score associated with the selected Jurisdiction and Model type appear in a tabular format. To modify the Risk score, double-click the value. The score is displayed up to two decimal places. The maximum value is 100 and the minimum value must be greater than or equal to 0.
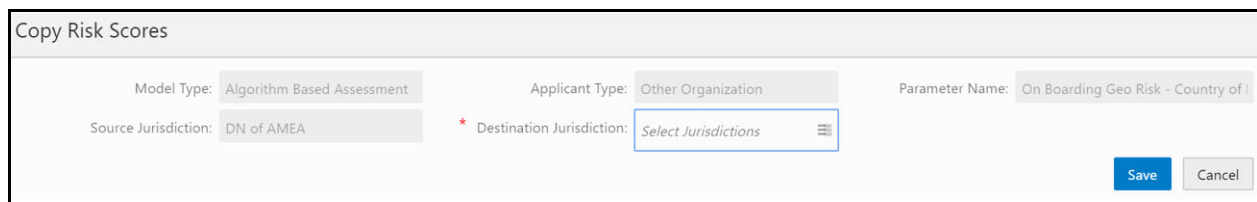
Note:

■   To populate any parameters or rules which have been added, click Auto-Populate. This button populates the new risk parameters and rules added for all jurisdictions, risk models, and applicant types.

■   In case no new rules or parameters have been added, a message is displayed when you click Auto-Populate "Auto Populate was not performed as there are no new risk parameter values."

Copying Risk Scores across Jurisdictions

You can copy risk scores only for the Algorithm-based model type. To copy risk scores from one jurisdiction to another:

1. Click **Copy**.

2. Select one or more **jurisdictions**. Only jurisdictions which have the same model type, applicant type, and parameter name as the source jurisdiction are shown.

3. Click **Save**.

Modifying and Adding the Mapping Codes within KYC

Use the Configure Source to Destination Code Mapping menu UI to view the mappings from source to destination. To view the UI:

1. Log in to the KYC application. For more information, see *Getting Started*.

2. Click **Behavior Detection - KYC > Manage KYC OB Configuration > Configure Source to Destination Code Mapping**.
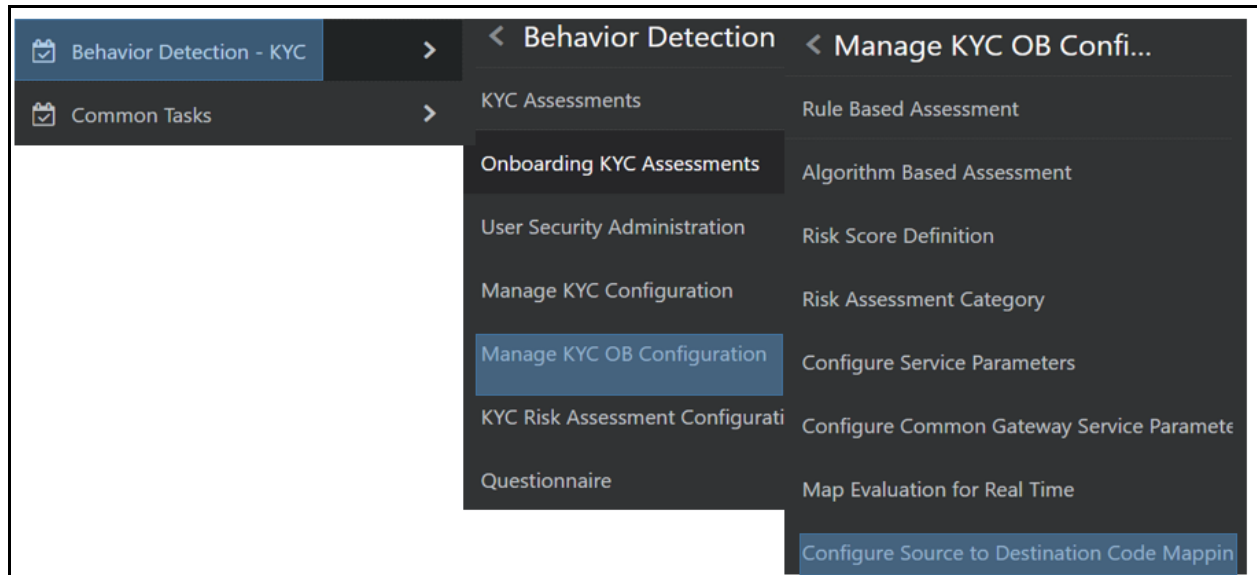
The Risk Assessment Category UI appears with the **Search** section displayed. In the **Search** section, select an option and click **Search**.
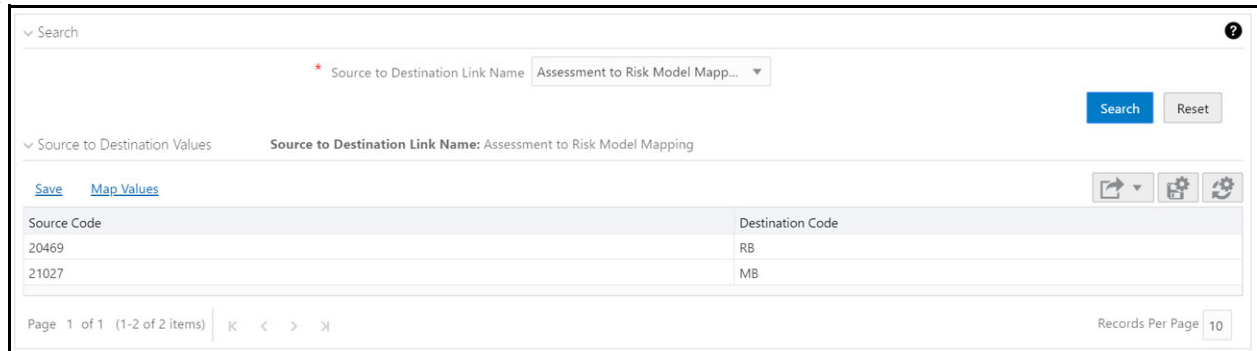
The Source Code and Destination Code values appear in a tabular format.

Downloading the Code Values

To download the code values, click . You can select between **.XLSX** or **.CSV** formats.

Modifying the Code Values

To modify the code values, follow these steps:
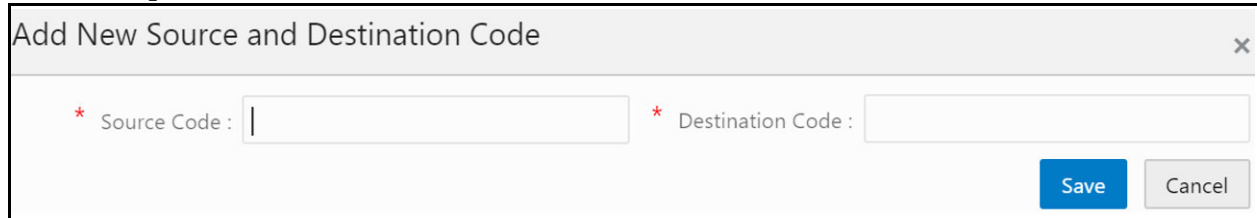
1. Double-click the **code value** and provide the new code value.

2. Click **Save**.

   To refresh the UI, click **Reset**.

Adding New Code Values

To add new code values:

1. Click **Map Values**.

2. Add a **Source code** and a **Destination code**.

3. Click **Save**.

Adding Risk Parameters and Rules (KYC Batch)

This chapter provides information on adding risk parameters, rules, risk scores, and mapping evaluations to assessments.

This chapter discusses the following topics:

- Adding Risk Parameters for Algorithm-based Risk Assessments
- Adding Rules for Rule-based Risk Assessments
- Adding Rules for Accelerated Rules
- Mapping an Evaluation to an Assessment
- Adding Risk Scores for Parameter/Rule Values

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 (KYC Batch).

2. Update the sequence ID for IPE. To do this, execute the following script in the Config schema as a post installation step:

   ```
   Begin p_set_sequence_value('TASKS','5000000','Y'); end;
   ```

   For information on the post installation activities, see Installation Guide.

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

1. Navigate to the OFSAA login page.

2. In the KYC home page, click **Behavior Detection - KYC**.

3. Click **KYC Risk Assessment Configuration**.

   Click to expand the page.

4. Click **Algorithm Based Risk Assessment**. The **Algorithm Based Risk Assessment** page appears.
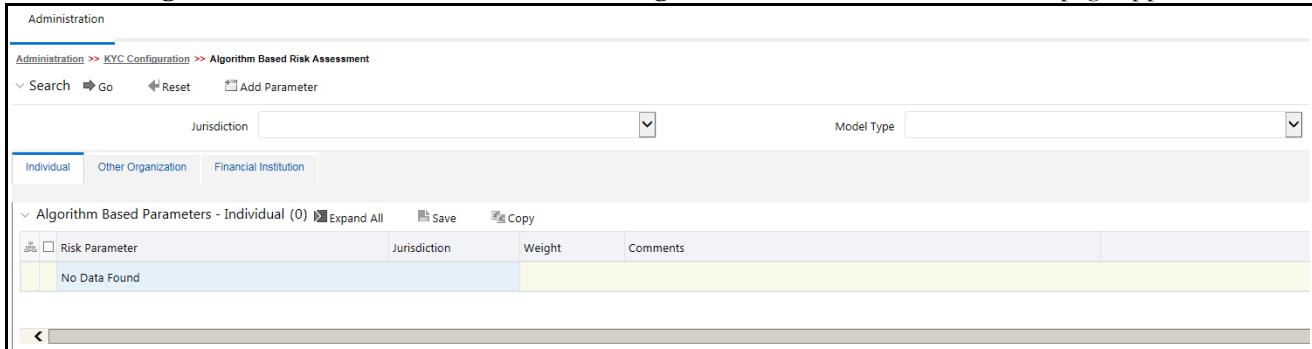
5. To add a new parameter, click **Add Parameter**. The Add New Parameter dialog box displays.

The fields are described in the following table:

Field Name	Description
Jurisdiction	Select the jurisdiction that the parameter belongs to. All the jurisdictions that are available in the `kdd_jrsdcn` table display.
Model Type	Select the model type as Algorithm-based Risk Assessment. **Note:** The Model type RAOR Risk Assessment is not supported from this user interface from 8.0.7.
Parameter Code	Enter the parameter code. This is unique for each parameter.
Parameter Name	Enter the parameter name.
Code Set	Select the code set applicable for the parameter. All the jurisdictions that are available in the `kdd_code_set_trnln` table display.
Customer Type	Select the customer type. Based on the customer type, the parameter is displayed in the Individual, Other Organization, or Financial Institution tabs.

Field Name	Description
Active Flag	Select Yes to enable the parameter for the current assessment. Select No to disable the parameter for the current assessment.
Range Flag	Select Yes to enable the parameter as range-based.
Consider For Reas-sessment	Select Yes to reasses the impacted customer. **Note:** If you select Yes, see the steps mentioned in *Adding a Risk Parameter or Rule for Reassessments*.
Re-review Rule Name	Enter the value `APPLN_REREVIEW_PARAMS`.
Comments	Enter any comments related to the parameter.

To save the parameter, click **Save**.

Note: To close the dialog box, click **Cancel**. This refreshes the screen with the new parameter.

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.

6. In the KYC home page, click **Financial Services Inline Processing Engine** in the **Common Tasks** tab.
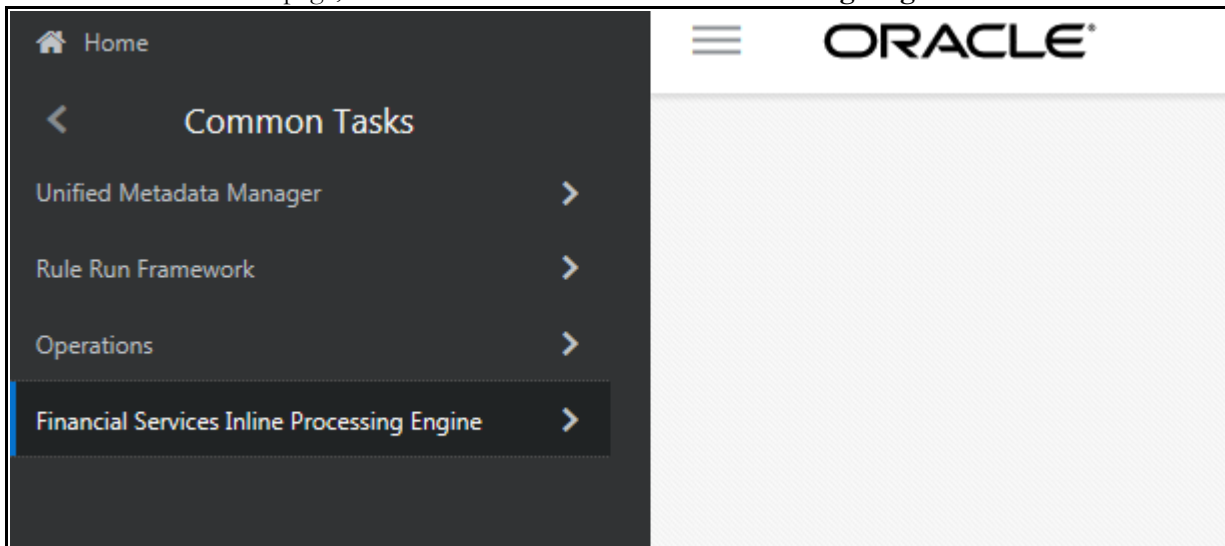
7. Click **Inline Processing**. The *Inline Processing* page is displayed.

8. 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`.

c. Click **Add**.

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

Note: For Algorithm-based parameters, select Algorithm Based Risk 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.

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

   ■ Accelerated Review Parameter to Country of Head Quarters Value: 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**.

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 Head Quarters Value**.

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.

10. 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**.

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.

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.

11. 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**.

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

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.

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 following figure and click **Save**. The variable is 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 following figure and click **Save**.

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 following figure and click **Save**.

	Group	Order	Operator	Business Property (Business Entity. Business Attribute)	Function	Function Parameter
○	1	1		Method of Account Opening Value : N_RISK_SCORE		
○	2	1	*	Algorithm Based Risk Scoring : N_RISK_PARAM_WEIGHT		

Expression Name* Country of birth

Activity* Customer Processing

Processing Segment * Algorithm Based Risk Model / Identity Verification Risk Model

Variables Add Delete Apply Function To Group Remove Function From Group Apply Function to Expression

Variable   Save   Cancel

Operator

Business Entity*

Business Attribute*

○ Add to Current Group   ● Create New Group

Apply Function to Expression   Cancel

Select Function   Divide

Denominator

● Literal Value ○ Expression

100   ✕

[Submit] [Close]

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

12. 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**.

c. Enter a name for the evaluation.

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

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

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 following figure and click **Save**:

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 following figure and click **Save**:

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 the data for the risk parameter in the Highlights section. This is required to get the actual value for every customer.

Note: To know how to add a highlight for an evaluation, see *IPE User Guide*.

j. Click **Save**.

13. 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_AP-
P_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

14. Click **Save**.
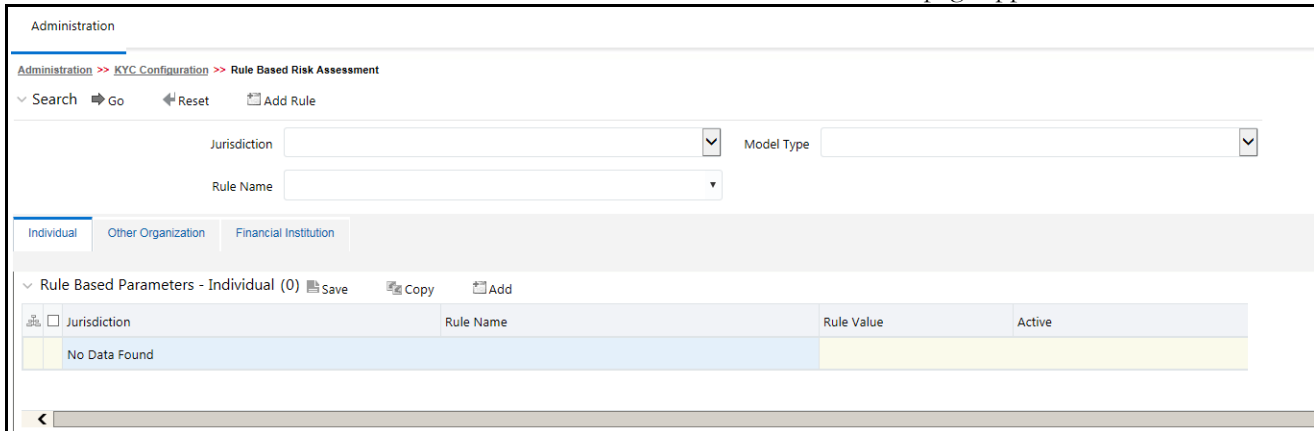
Adding Rules for Rule-based Risk Assessments

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

1. Navigate to the OFSAA login page.

2. In the KYC home page, click **Behavior Detection - KYC**.

3. Click **KYC Risk Assessment Configuration**.

   Click ☰ to expand the page.

4. Click **Rule Based Risk Assessment**. The **Rule Based Risk Assessment** page appears.
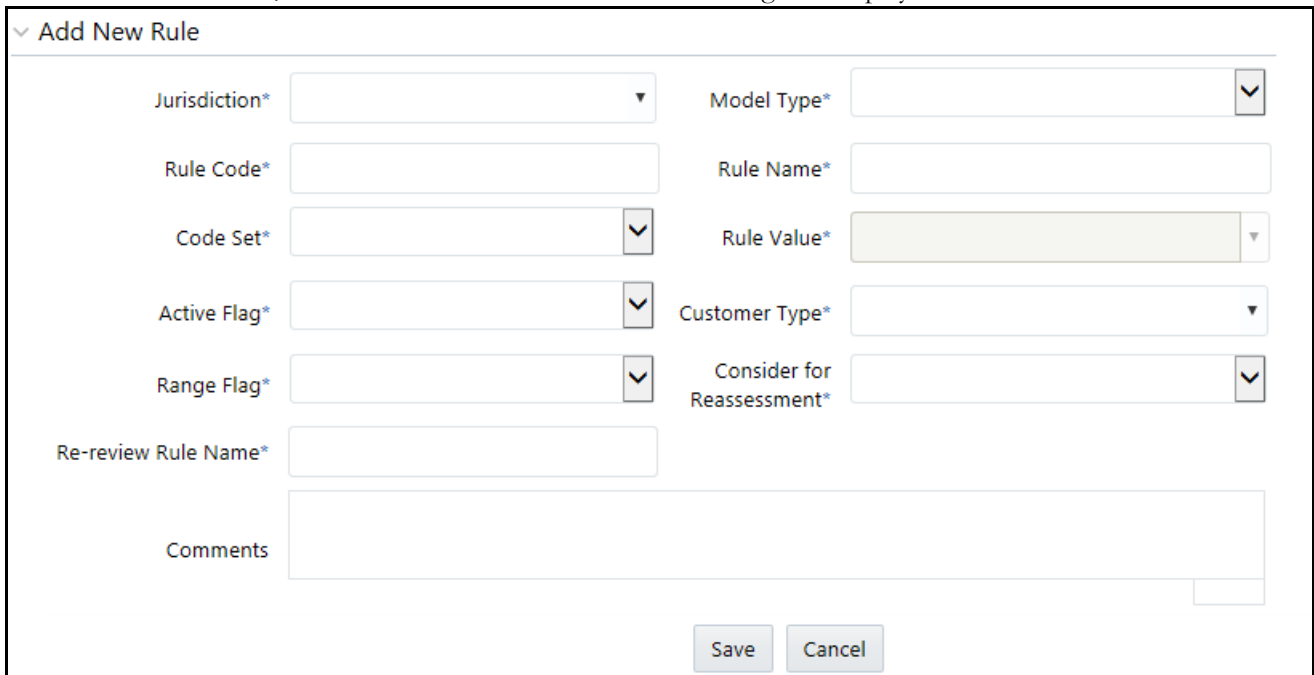
5. To add a new rule, click **Add Rule**. The Add New Rule dialog box displays.

The fields are described in the following table:

Field Name	Description
Jurisdiction	Select the jurisdiction that the parameter belongs to. All the jurisdictions that are available in the `kdd_jrsdcn` table display.
Model Type	Select the model type as Algorithm-based Risk Assessment. **Note:** The Model type RAOR Risk Assessment is not supported from this user interface from 8.0.7.
Rule Code	Enter the rule code. This is unique for each rule.
Rule Name	Enter the rule name.
Code Set	Select the code set applicable for the rule. All the jurisdictions that are available in the `kdd_code_set_trnln` table display.
Customer Type	Select the customer type. Based on the customer type, the rule is displayed in the Individual, Other Organization, or Financial Institution tabs.
Active Flag	Select Yes to enable the parameter for the current assessment. Select No to disable the parameter for the current assessment.
Range Flag	Select Yes to enable the length of relationship for the current assessment. Select No to disable the length of relationship for the current assessment.
Consider For Reassessment	Select Yes to whether the parameter is considered for reassessment or not. **Note:** If you select Yes, see the steps mentioned in *Adding a Risk Parameter or Rule for Reassessments*
Re-review Rule Name	Enter the value `APPLN_REREVIEW_PARAMS`.
Comments	Enter any comments related to the rule.

To save the rule, click **Save**.

Note: To close the dialog box, click **Cancel**. This refreshes the screen with the new rule.

6. 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.

7. In the KYC home page, click **Financial Services Inline Processing Engine** in the LHS menu.
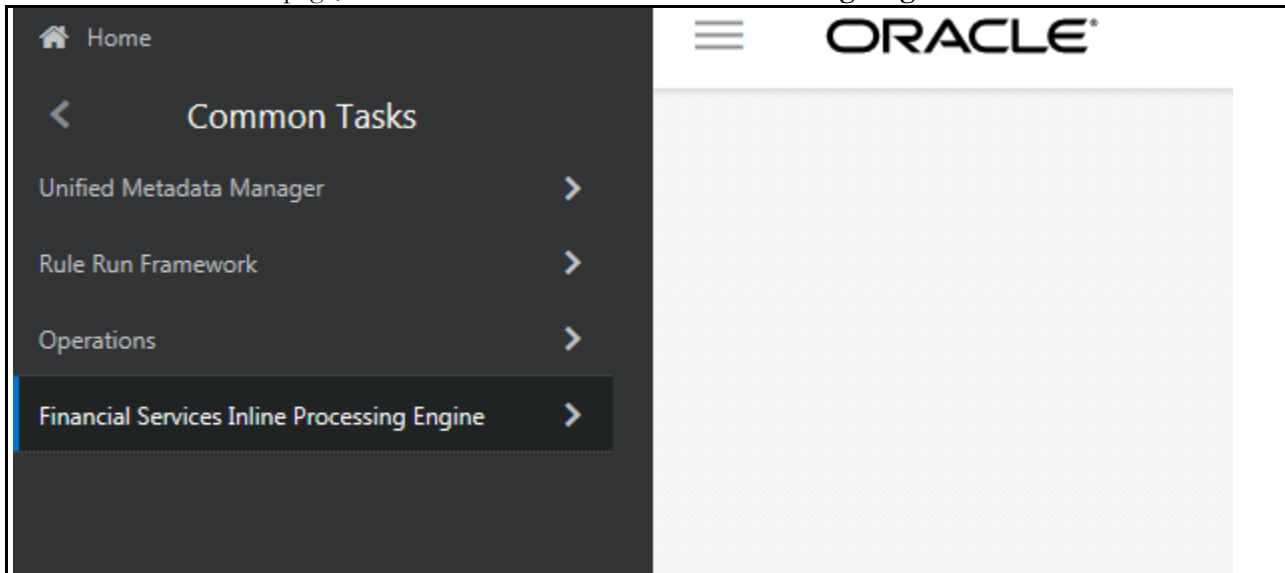
8. Click **Inline Processing** in the RHS menu. The *Inline Processing* page is displayed.
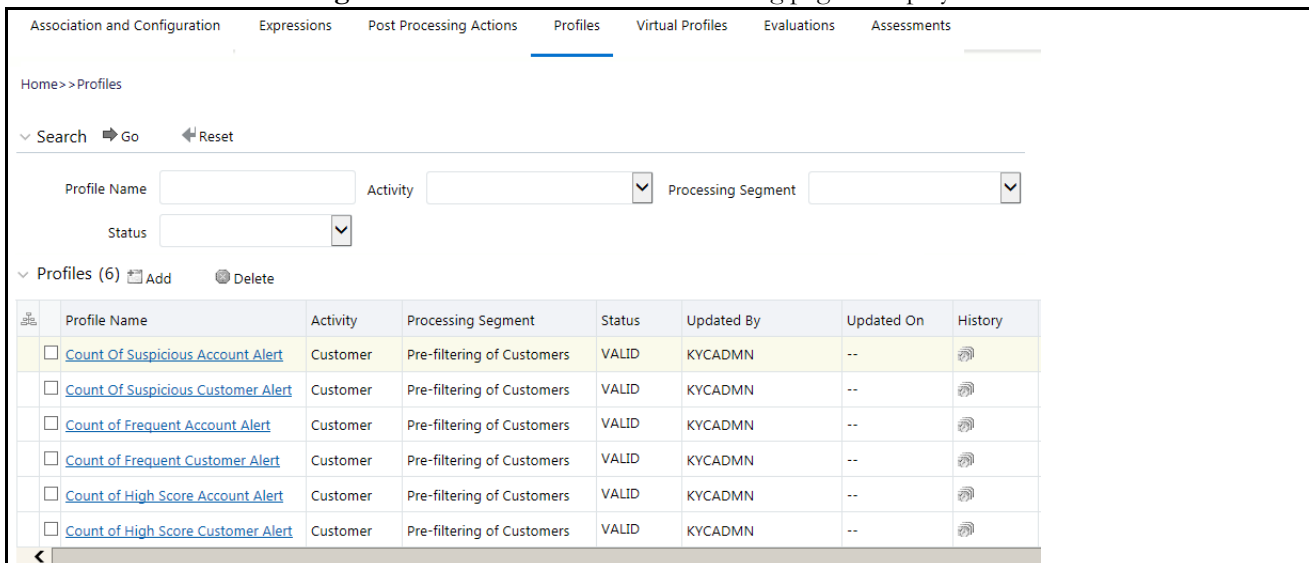
9. Add a business entity on top of the PARAM_RISK_SCORE_JRSDN table in IPE. For example, Country of Birth.

   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.

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.

10. 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**.

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.

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.

11. 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**.

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.

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*.

12. 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**.

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

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.

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 following figure and click **Save**. The variable is 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 following figure and click
    Save.

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 following figure and click
Save.

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

13. 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**.

c. Enter a name for the evaluation.

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

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

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 following figure and click **Save**:

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 following figure and click **Save**:

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 the data for the risk parameter in the Highlights section. This is required to get the actual value for every customer.

    j. Click **Save**.

14. 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_AP-
P_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

15. Click **Save**.

Adding a Risk Parameter or Rule for Reassessments

For every risk parameter or rule that you add, a corresponding evaluation is created.

Note: It is recommended that you look at the predefined values for an existing evaluation when you create a new evaluation.

The following steps are applicable if you select Consider for Reassessment as Yes:

1. Create an evaluation. While creating the evaluation, you can reuse the expressions available in the filters and provide the appropriate values for each filter.

   You need to add three filters to the evaluation:

   ■   The first filter is called Rule code. In this filter, you need to provide the risk parameter or rule code in the evaluation filter as defined for the newly added parameter.

- ■ The second filter is called Processed Flag. In this filter, you must provide the same values that are defined in the ready-to-use product.

- ■ The third filter is named according to the new risk parameter or rule which you add for the evaluation. This filter is applicable for the new risk parameter or rule which you add for the evaluation.

2. Map the new evaluation to the **Change in Risk Model** Assessment.

Adding Rules for Accelerated Rules

To add a rule which is of rule type Alert Re-review or Risk Re-assess, follow the steps mentioned. To add a rule for any other rule type, contact Oracle Support.

1. Navigate to the KYC home page.

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

3. Click **Accelerated Rules** in the RHS menu. The *Accelerated Re-review Rules* page is displayed.

4. To add a new rule, click **Add Rereview Rule**. The Add New Rule dialog box displays.

The fields are described in the following table:

Field Name	Description
Jurisdiction	Select the jurisdiction that the parameter belongs to. All the jurisdictions that are available in the `kdd_jrsdcn` table display.
Rule Type	Select the rule type. The options are Alert Rereview or Change Log.
Rule Name	Enter the rule name.
Count of Alerts	Enter the number of alerts. This indicates the number of alerts after which reassessment happens. **Note:** This field is applicable only for alert rereviews and if KYC is integrated with FCCM Alert Management (AM).

Field Name	Description
Alert Score	Enter the alert score. This indicates the alert score threshold after which reassessment happens. **Note:** This field is applicable only if KYC is integrated with FCCM Alert Management (AM). **Note:** To know how to post external alerts, see *OFS BD Administration Guide*.
Rule Score	Enter the rule score. This is the rule score for a specific parameter. **Note:** This parameter is not applicable for 805.
Active	Select Yes to enable the rule for the current assessment. Select No to disable the rule for the current assessment.
Rule Description	Enter a description for the rule.
Comments	Enter any comments related to the rule.

To save the rule, click **Save**. To close the dialog box, click **Cancel**. This refreshes the screen with the new rule.

Mapping an Evaluation to an Assessment

To map an evaluation to an assessment, follow these steps:

1. In the KYC home page, click **KYC Risk Assessment Configuration**.

2. Click **Association of Rule/Risk Parameter to Evaluation**. The *Map Evaluation* page is displayed.

3. Select the Model Type as *Accelerated Re-review Based Assessment.* and click **Go**. The Association of Rule/Risk Parameter to Evaluation grid is populated with the available evaluations.

4. Select the evaluation and click **Save**. The evaluation is now mapped to the assessment and the selected rule.

Adding Risk Scores for Parameter/Rule Values

To view the risk scores after the risk assessment of parameters or rules, follow these steps:

1. Navigate to the KYC home page.

2. Click **KYC Risk Assessment Configuration**.

3. Click **Risk Score for Parameter/Rule Value**. The *Risk Score for Parameter/Rule Value* page is displayed.

4. Select the jurisdiction, model type used for risk scoring, and the parameter or rule name and click **Go**. The risk scores are displayed on the page.

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

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

5. Click **Auto-Populate** to generate the risk scores following the risk assessment. To change the risk score, select the check box of the parameter that you want to change and enter the new risk score.

APPENDIX A   *KYC Batches*

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

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

NOTE:

- If you also have Enterprise Case Management (ECM) installed, ensure that you execute the ECM batches after running the KYC batches. This is necessary because if you do not execute the ECM batches, no assessments appear on the screen.

- Some of the tasks mentioned may be descoped in the future.

- KYC uses watch lists only for name matching. As a part of the KYC process, if you do not want to run the watch list tasks for primary customers and their interested parties, then you must unmap the watch list tasks.

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 19: 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
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	START
Task3	Populate_Cust_Prcsng	This is a task that populates the prefiltered Customer Data in to the Cust_Prcsng table when run.	LOAD DATA	Task1, Task2
Task4	Populate-Processed-NewAcct	This is a task that populates the new accounts processed in the system in to the processing table when run.	TRANSFORM DATA	Task3
Task5	Populate_Cust_Addr_Prcsng	This is a task that populates the prefiltered Customer Data in to the Cust_Addr_Prcsng table when run.	LOAD DATA	Task3
Task6	Populate_Cust_Cntry_Prcsng	This is a task that populates the prefiltered Customer Data in to the Cust_Cntry_Prcsng table when run.	LOAD DATA	Task3

Table 19: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task7	Populate_- Cust_Id_Doc _Prcsng	This is a task that populates the prefiltered Customer Data in to the Cust_Id_Doc_Prcsng table when run.	LOAD DATA	Task3
Task8	Populate_- Cust_Mkt_- Served_Prcs ng	This is a task that populate the pre- filtered Customer Data in to the Cust_Mkt_Served_Prcsng table when run.	LOAD DATA	Task3
Task9	Populate_- Cust_Phon_P rcsng	This is a task that populates the pre- filtered Customer Data in to the Cust_Phon_Prcsng table when run.	LOAD DATA	Task3
Task10	Populate_- Cust_Prod_P rcsng	This is a task that populates the pre- filtered Customer Data in to the Cust_Product_Prcsng table when run.	LOAD DATA	Task3
Task11	Populate_- Cust_to_- Cust_Prcsng	This is a task that populates the pre- filtered Customer Data in to the Cust_Cust_Prcsng table when run.	LOAD DATA	Task3
Task12	Populate_- Cust_Acct_P rcsng	This is a task that populates the pre- filtered Customer Data in to the Cust_Acct_Prcsng table when run.	LOAD DATA	Task3
Task13	Popu- late_Acct_P rcsng	This is a task that populates the pre- filtered Customer Data in to the Acct_Prcsng table when run.	LOAD DATA	Task12
Task14	POPU- LATE_IP_KYC	This is a task that populates the Intrested Party Customers and Accounts when run.	TRANSFORM DATA	Task10, Task11, Task12, Task13, Task3, Task4, Task5, Task6, Task7, Task8, Task9
Task15	t2t_PAR- TY_AD- DRESS_PRCNG _IP	This is a task that populates the party address in to the pricing table when run.	LOAD DATA	Task14
Task16	t2t_PARTY_- DETAILS_PRC NG_IP	This is a task that populates the party details in to the pricing table when run.	LOAD DATA	Task14

Table 19: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task17	t2t_PAR-TY_ID_DOC_P RCNG_IP	This is a task that populates the party doc ID in to the pricing table when run.	LOAD DATA	Task14
Task18	t2t_PAR-TY_PAR-TY_RLSHP_PR CSNG_BO	This is a task that populates the beneficial owner details in to the PARTY_PARTY_RLSH-P_PRCSNG_BO table when run.	LOAD DATA	Task14, Task15, Task16, Task17
Task19	t2t_PARTY_-DETAILS_PRC NG_BO_INT	This is a task that populates the internal beneficial owner details in to the PARTY_DE-TAILS_PRCNG_BO_INT table when run.	LOAD DATA	Task18
Task20	t2t_PARTY_-DETAILS_PRC NG_BO_EXT	This is a task that populates the external beneficial owner details in to the PARTY_DE-TAILS_PRCNG_BO_EXT table when run.	LOAD DATA	Task18
Task21	t2t_PAR-TY_AD-DRESS_PRCNG _BO_INT	This is a task that populates the internal beneficial owner details in to the PARTY_AD-DRESS_PRCNG_BO_INT table when run.	LOAD DATA	Task18
Task22	t2t_PAR-TY_AD-DRESS_PRCNG _BO_EXT	This is a task that populates the external beneficial owner details in to the PARTY_AD-DRESS_PRCNG_BO_EXT table when run.	LOAD DATA	Task18
Task23	t2t_PAR-TY_ID_DOC_P RCNG_BO_INT	This is a task that populates the internal beneficial owner details in to the PAR-TY_ID_DOC_PRCNG_BO_INT table when run.	LOAD DATA	Task18
Task24	t2t_PAR-TY_ID_DOC_P RCNG_BO_EXT	This is a task that populates the external beneficial owner details in to the PAR-TY_ID_DOC_PRCNG_BO_EXT table when run.	LOAD DATA	Task18
Task25	t2t_FCT_T-P_WLS_RE-QUESTS_PRCN G	This is a task that populates Requests in to the watch list Pro-cessing table for the prefiltered Cus-tomers when run.	LOAD DATA	Task18, Task19, Task20, Task21, Task22, Task23, Task24

Table 19: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task26	t2t_FCT_T-P_WLS_RE-SULTS_PRCNG	This is a task that populates the watch list Score in the FCT_T-P_WLS_RESULTS_PRCNG table when run.	LOAD DATA	Task27
Task27	Watchlist_-FuzzyMatch	This is a task that calls the watch list Fuzzy Match to calculate the watch list Score when run.	TRANSFORM DATA	Task25
Task28	UPDATE_WLS_STATUS	This is a task that updates the Status of the watch list Request to Closed when run.	TRANSFORM DATA	Task26
Task29	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	Task25, Task26, Task27, Task28
Task30	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	Task29
Task31	t2t_POPU-LATE_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	Task30
Task32	t2t_POPU-LATE_FCT_RA_RISK_SUM-MARY	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	Task31
Task33	t2t_POPU-LATE_FCT_RA_RISK_REA-SONS	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	Task31
Task34	t2t_FCT_RA_RISK_DE-TAILS	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	Task31
Task35	t2t_FCT_-CUST_RA_HIS-TRY	This is a task that populates the FCT_CUST_RA_HISTRY table with the names of the prefiltered customers when run.	LOAD DATA	Task36
Task36	F_CLO-SURE_UP-DATES	This is a task that updates the RA once they are closed.	TRANSFORM DATA	Task37
Task37	t2t_FCT_-CUST_RVWDTLS	This is a task that populates the FCT_CUST_RVWDTLS table when run.	LOAD DATA	Task31

Table 19: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task38	t2t_FCT_T-P_WLS_RE-QUESTS	This is a task that populates the FCT_TP_WLS_REQUESTS table when run.	LOAD DATA	Task31
Task39	t2t_FCT_T-P_WLS_RE-SULTS	This is a task that populates the FCT_TP_WLS_RESULTS table when run.	LOAD DATA	Task21
Task40	t2t_FCT_RA_RISK_RAT-ING_HISTORY	This is a task that populates the FCT_RA_RISK_RATING_HIS-TORY table when run.	LOAD DATA	Task31
Task41	t2t_FCT_-CUST_RE-VIEW_REASON S	This is a task that populates the customer review reasons in to the FCT_CUST_REVIEW_REASONS table when run.	LOAD DATA	Task31
Task42	KYC_PURGE_L AST_RUN_TAB	This is a task that purges or trun-cates the kdd_ex-trl_batch_last_run table when run.	TRANSFORM DATA	Task31, Task32, Task33, Task34, Task35, Task36, Task37, Task38, Task39, Task40, Task41
Task43	t2f_Gen-CustDe-tails_ED	This is a task that generates the Customer details flat file.	EXTRACT DATA	Task42
Task44	t2f_GenWLS-Feedback_ED	This is a task that generates the watch list feedback details flat file.	EXTRACT DATA	Task42
Task45	t2f_-GenCBSFeed-back_ED	This is a task that generates the GenCBSFeedback details flat file.	EXTRACT DATA	Task42
Task46	KYC_-File_Rename	This is a task that generates the new KYC file name.	TRANSFORM DATA	Task43, Task44, Task45

Deployment Initiation Processing

The following table provides details about deployment initiation processing:

Table 20: Deployment Initiation Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task1	`FN_IPE_LAST_BA TCH_RUN_KY`	This is a task that captures the current batch ID when run.	`TRANSFORM DATA`	`START`
Task2	`Populate_- Cust_Prcsng_DI`	This is a task that populates the prefiltered Customer Data in to 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.	`TRANSFORM DATA`	`Task2`
Task4	`Populate_- Cust_Ad- dr_Prcsng`	This is a task that populates the prefiltered Customer Data in to the `Cust_Addr_Prcsng` table when run.	`LOAD DATA`	`Task3`
Task5	`Populate_- Cust_Cn- try_Prcsng`	This is a task that populates the prefiltered Customer Data in to the `Cust_Cntry_Prcsng` table when run.	`LOAD DATA`	`Task4`
Task6	`Populate_- Cust_Id_Doc_Pr csng`	This is a task that populates the prefiltered Customer Data in to the `Cust_Id_Doc_Prcsng` table when run.	`LOAD DATA`	`Task5`
Task7	`Populate_- Cust_Mkt_- Served_Prcsng`	This is a task that populate the prefiltered Customer Data in to the `Cust_Mkt_Served_Prcsng` table when run.	`LOAD DATA`	`Task6`
Task8	`Populate_- Cust_Phon_Prcs ng`	This is a task that populates the prefiltered Customer Data in to the `Cust_Phon_Prcsng` table when run.	`LOAD DATA`	`Task7`
Task9	`Populate_- Cust_Prod_Prcs ng`	This is a task that populates the prefiltered Customer Data in to the `Cust_Product_Prcsng` table when run.	`LOAD DATA`	`Task8`
Task10	`Populate_- Cust_to_- Cust_Prcsng`	This is a task that populates the prefiltered Customer Data in to the `Cust_Cust_Prcsng` table when run.	`LOAD DATA`	`Task9`
Task11	`Populate_- Cust_Acct_Prcs ng`	This is a task that populates the prefiltered Customer Data in to the `Cust_Acct_Prcsng` table when run.	`LOAD DATA`	`Task10`
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	`Popu- late_Acct_Prcs ng`	This is a task that populates the prefiltered Customer Data in to the `Acct_Prcsng` table when run.	`LOAD DATA`	`Task12`

Table 20: Deployment Initiation Processing

Task14	POPU-LATE_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_i-INTERESTED_PARTY` table.	TRANSFORM DATA	Task14
Task16	t2t_PARTY_DE-TAILS_PRCNG_IP	This is a task that populates the party details in the `PARTY_DE-TAILS_PRCNG_IP` table when run.	LOAD DATA	Task15
Task17	t2t_PARTY_AD-DRESS_PRCNG_IP	This is a task that populates the party address in the `PARTY_AD-DRESS_PRCNG_IP` table when run.	LOAD DATA	Task15
Task18	t2t_PAR-TY_ID_DOC_PRCNG_IP	This is a task that populates the party doc ID in the `PAR-TY_ID_DOC_PRCNG_IP` table when run.	LOAD DATA	Task15
Task19	t2t_FCT_T-P_WLS_RE-QUESTS_PRCNG	This is a task that populates the watch list Score in the `FCT_T-P_WLS_REQUESTS_PRCNG` table when run.	LOAD DATA	Task14, Task15, Task16, Task17, Task18
Task20	GathrStats_WL-SREQUESTS_P	This is a task that is used to gather statistics for the `FCT_T-P_WLS_REQUESTS` and `FCT_TP_WLS_RE-QUESTS_PRCNG` tables.	TRANSFORM DATA	Task19
Task21	Watchlist_Fuz-zyMatch	This is a task that calls the watch list Fuzzy Match to calculate the watch list Score when run.	TRANSFORM DATA	Task20
Task22	GathrStats_WL-SRESULT_STG	This is a task that is used to gather statistics for the `FCT_T-P_WLS_RESULTS` and `FCT_TP_WLS_RE-SULTS_PRCNG` tables.	TRANSFORM DATA	Task21
Task23	t2t_FCT_T-P_WLS_RE-SULTS_PRCNG	This is a task that populates the watch list Score in the `FCT_T-P_WLS_RESULTS_PRCNG` table when run.	LOAD DATA	Task22

Table 20: Deployment Initiation Processing

Task24	UPDATE_WLS_STATUS	This is a task that updates the Status of the watch list Request to Closed when run.	TRANSFORM DATA	Task 23
Task25	GathrStats_KYCPRCSNG_TAB	This is a task that is used to gather statistics for all the KYC processing tables.	TRANSFORM DATA	Task 24
Task26	Customer Processing	This is a task which generates rule or model-based scores when run.	INLINE PROCESSING	Task19, Task20, Task21, Task22, Task23, Task24, Task25
Task27	Customer Processing	This is a task which generates rule or model-based scores when run.	INLINE PROCESSING	Task26
Task28	t2t_FCT_RA_DI	This is a task that is used to populate the FCT_RA_DI table.	LOAD DATA	Task27
Task29	GathrStats_FCT_RA	This is a task that is used to gather statistics for the FCT_RA table for Regular Processing.	TRANSFORM DATA	Task28
Task30	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	Task29
Task31	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	Task30
Task32	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	Task31
Task33	t2t_FCT_CUST_RVWDTLS_AUTO_CLOSED_DI	This is a task that stores the details of the assessments that are auto-closed.	LOAD DATA	Task32
Task34	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	Task33
Task35	t2t_FCT_TP_WLS_REQUESTS	This is a task that populates the watch list score in the FCT_TP_WLS_REQUESTS table when run.	LOAD DATA	Task 34
Task36	t2t_FCT_TP_WLS_RESULTS	This is a task that populates the watch list score in the FCT_TP_WLS_RESULTS table when run.	LOAD DATA	Task 35

Table 20: Deployment Initiation Processing

Task37	t2t_FCT_RA_RISK_RATING_HIS-TORY	This is a task that populates the `FCT_RA_RISK_RAT-ING_HISTORY` table when run.	LOAD DATA	Task 36
Task38	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 37
Task39	KYC_PURGE_LAST_RUN_TAB	This is a task that purges or truncates the `kdd_ex-trl_batch_last_run` table when run.	TRANSFORM DATA	Task28, Task 29, Task 30, Task 31, Task 32, Task 33, Task 34, Task 35, Task 36, Task 37, Task 38

End of Day Processing

The following table provides details about end of day processing:

Table 21: End of Day Processing

Task No	Rule Name (As configured)	Description	Component Id	Precedence
Task1	t2f_GenCustDetails_ED	Extract the customer feedback details	EXTRACT DATA	
Task2	t2f_GenWLSFeedback_ED	Extract the watch list scanning feedback details	EXTRACT DATA	
Task3	t2f_GenCBSFeedback_ED	Extract customer details for CBS	EXTRACT DATA	
Task4	KYC_File_Rename	Renaming of the extracted files according to the AML needs	TRANSFORM DATA	Task1, Task2, Task3
Task5	FN_REREVIEW_DATE_DI	Splitting of the customers processed through the DI processing back for periodic rereview	TRANSFORM DATA	Task1, Task2, Task3, Task4

APPENDIX B   *Creating Highlights*

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

To create a highlight, follow these steps:

1. 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 following example, a Business Entity called Residence is created.

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

3. 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 following example, a Traversal path is created from the Country of Processing table to the Algorithm Based Risk Scoring table.
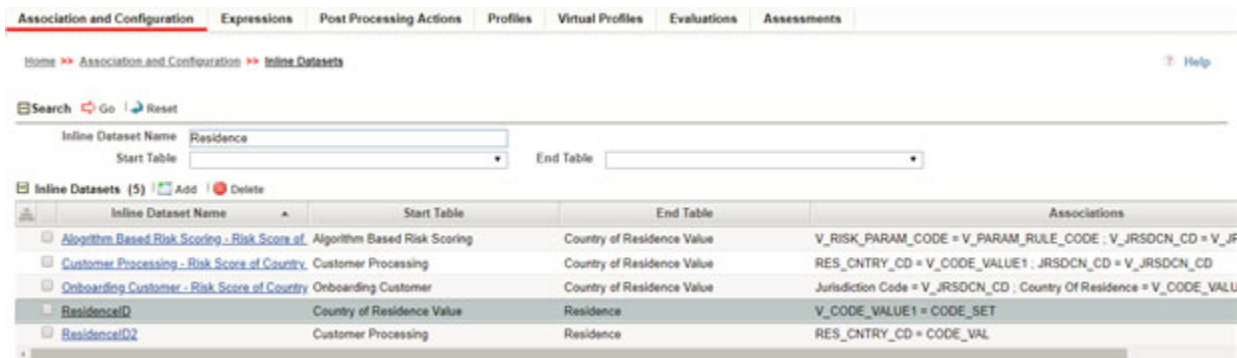
4. Add an expression on the risk score column of the Business Entity which is to be scored as a risk parameter.

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

   In the following example, an Expression called ResidenceEPR is created for the Residence Business Entity..
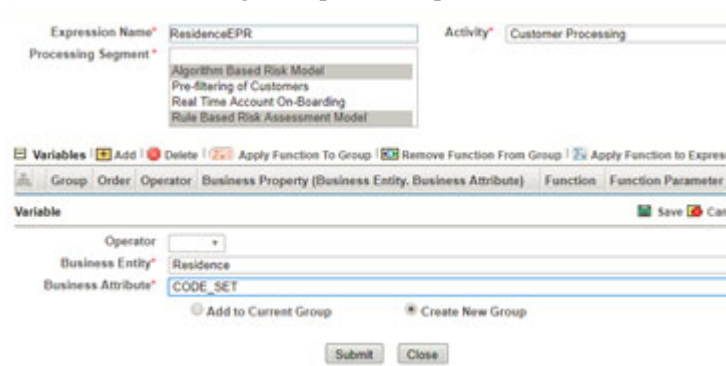
5. Map an evaluation to the existing assessment of the added parameter.

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

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

6. Add an Assessment. To add an Assessment, navigate to the Assessments menu in the Inline Processing page. In the following example, an Assessment is created for Rule Based Risk Assessment.

APPENDIX C   *Configuration Steps for Customer Screening Delta Updates*

This appendix provides the configuration steps needed to view the delta updates when customers are screened for matches against the Customer Screening Watch list. If there is a match, then an accelerated rereview is generated.

NOTE: The latest matches are picked when the `cust_watchlist_mtchs` batch is run.

This appendix discusses the following topics:

- Adding the Customer Screening Task to the KYC Daily Batch
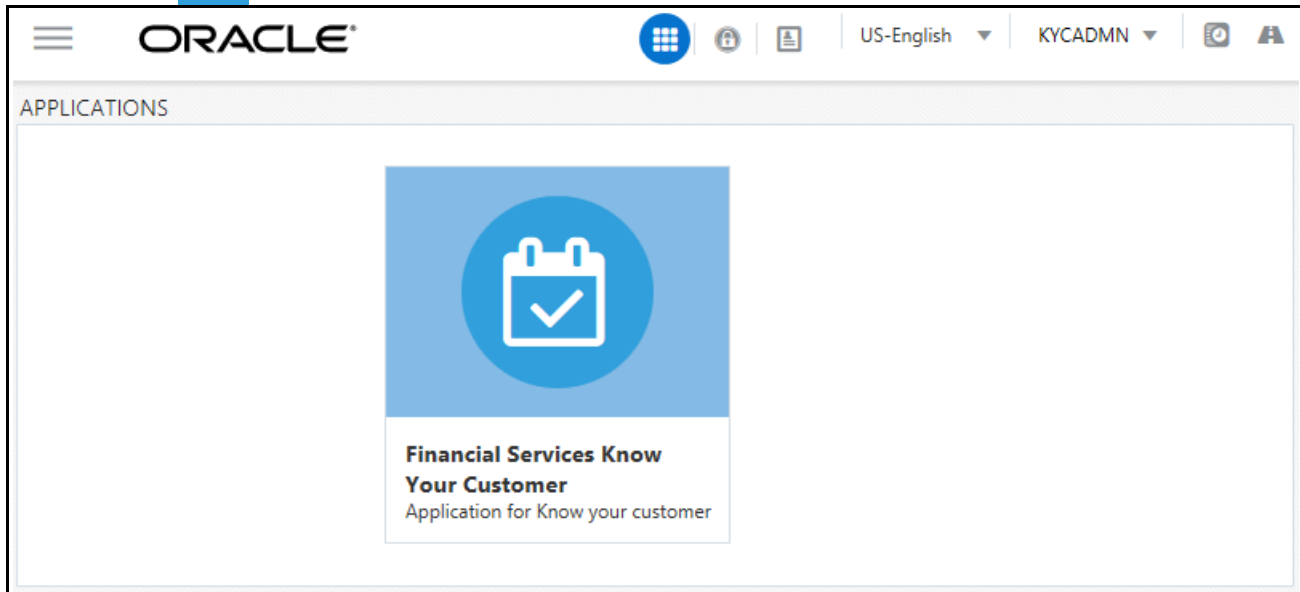- Mapping the Watch List evaluation to the Accelerated Rereview Assessment

Adding the Customer Screening Task to the KYC Daily Batch

To add the customer screening task to the KYC daily batch, follow these steps:

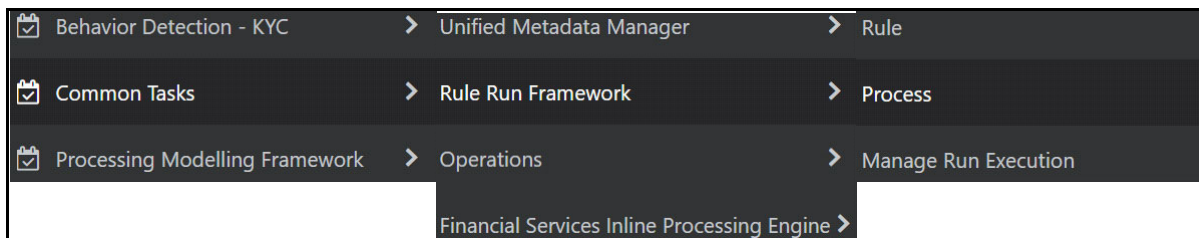**NOTE:** Before you run the batch, ensure that you have completed data ingestion in all relevant tables.

1. Login to the KYC Application.

2. Click the [icon] icon.

3. Click **Common Tasks >> Rule Run Framework >> Process**.

Running the Daily Batch

To run the Daily batch, follow these steps:

1. In the Process screen, provide the value `IPEPREProcess` in the Name field and click **Search**.

.

2. Select the `IPEPREProcess` check box and click **Edit**. The Process Definition (Edit Mode) screen appears.

3. In the Process Definition (Edit Mode) screen, click **Component**.

4. On the Component selector screen, search for the Processes node in the List window on the left.

5. Expand the Processes node, and then the FCCMSEGMNT node.

6. Search for the **Load Customer Match Data from Oracle CS** process and double-click the process. It moves to the Tasks window on the right.

7. Click **Ok**.

8. In the Process Definition (Edit Mode) screen, click **Precedence**.

9. On the Precedence Selector screen, select **Load Customer Match Data from Oracle CS** in the Available Precedence window and **BD_POPULATE_LAST_RUN_BATCH** in the Existing Precedence window.
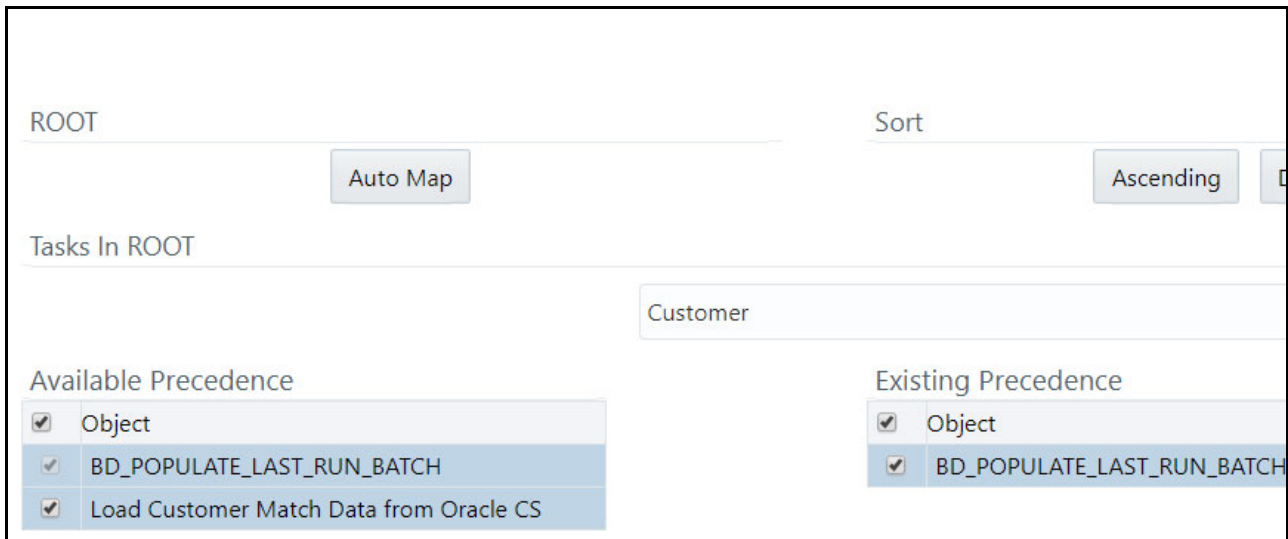
10. Click **Ok**.

11. Click **Save** to save the process.

12. Recreate the Batch corresponding to this RUN.

Running the Deployment Initiation Batch

To run the Deployment Initiation batch, follow these steps:

1. In the Process screen, provide the value `KYC_DI_Populate_Processing` in the Name field and click **Search**.

.

2. Select the `KYC_DI_Populate_Processing` check box and click **Edit**. The Process Definition (Edit Mode) screen appears.

3. In the Process Definition (Edit Mode) screen, click **Component**..

Process

Process Definition(Edit Mode)
⌄Linked to

Folder   FCCMSEGMNT

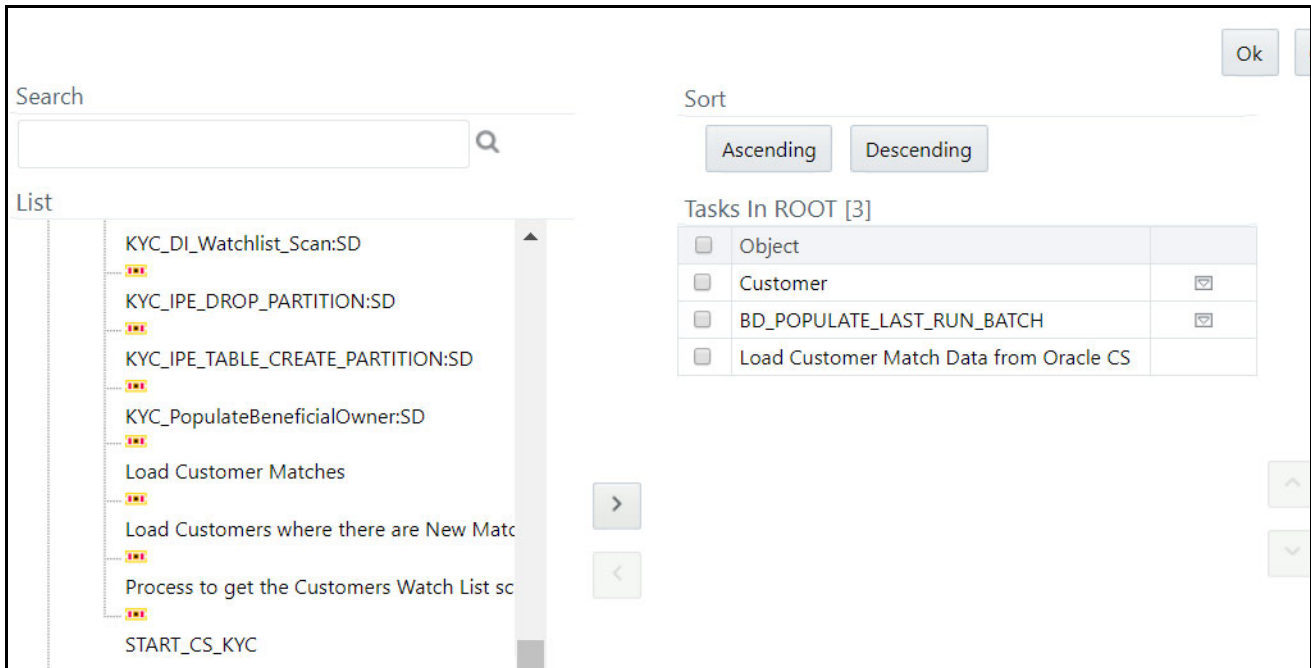⌄Master Information ☐ Properties

ID   1461724461468

Code   IPEPREProcess

Name   IPEPREProcess

Executable   ☐

⌄ ▽Subprocess ☐Component ▦ Precedence   ✎ Move 🗑 Remove ▢ Show Details 🗗 Merge Rules

⊟ Process
  ─ Customer
  ─ BD_POPULATE_LAST_RUN_BATCH
  ─ Load Customer Match Data from Oracle CS

| ☐ | Object |
☐	Customer
☐	BD_POPULATE_LAST_RUN_BATCH
☐	Load Customer Match Data from Oracle CS

4. On the Component selector screen, search for the Processes node in the List window on the left.

5. Expand the Processes node, and then the FCCMSEGMNT node.

6. Search for the **Load Customer Match Data from Oracle CS** process and double-click the process. It moves to the Tasks window on the right.

7. Click **Ok**.

8. In the Process Definition (Edit Mode) screen, click **Precedence**.

9. On the Precedence Selector screen, select **Load Customer Match Data from Oracle CS** in the Available Precedence window and **FN_IPE_LAST_BATCH_RUN_KY** in the Existing Precedence window..

10. Click **Ok**.

11. Click **Save** to save the process.

12. Recreate the Batch corresponding to this RUN.

Mapping the Watch List evaluation to the Accelerated Rereview Assessment

To map the evaluation, follow these steps:

1. Login to the KYC Application.

2. Click the icon.
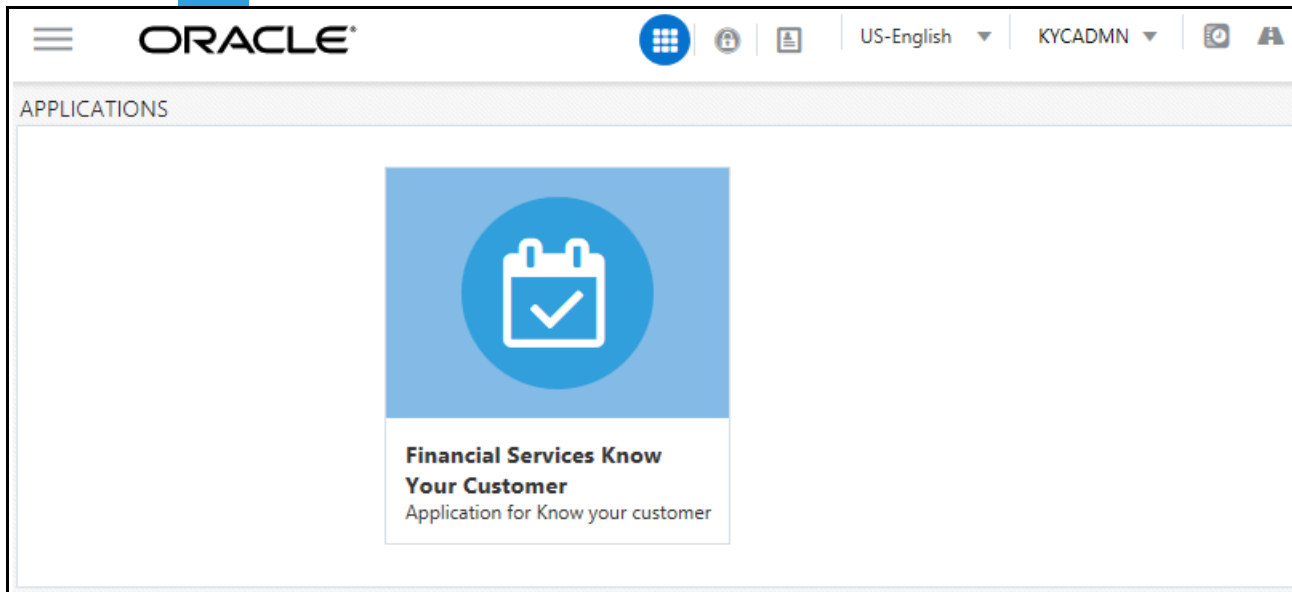
3. Click **Common Tasks >> Financial Services Inline Processing Engine >> Inline Processing >> Assessments**.

4. Click **Accelerated Rereview** and then click **MAP**.

5. In the Assessment Evaluation Mapping screen, select **New Watch List Matches** from the Available Evaluations window and move it to the Included Evaluations window.

6. Click **Save**.

7. Restart the servers.

Switching between CS and EDQ Servers for Screening

This appendix provides the run scripts you must execute if you want to use the EDQ server for the screening process. By default, the CS server is enabled. It discusses the following topics:

- Script for the EDQ Server
- Script for the CS Server

Script for the EDQ Server

To switch to the EDQ server, use the following script:

```
MERGE INTO AAI_WF_TRANSITION_B T USING (

 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1612765003317' V_TRANSITION_ID,
'Job_1569914716746' V_FROM_ACTIVITY_ID, 'Job_1612420416740' V_TO_ACTIVITY_ID,
'1533703981393' V_CONDITION_EXPR, '1' V_CONDITION_TYPE, '1' V_PRECEDENCE, 'L'
V_TRANSITION_TYPE, ' ' V_TRANSITION_STROKE FROM DUAL) S

 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID )

 WHEN MATCHED THEN UPDATE SET T.V_FROM_ACTIVITY_ID = S.V_FROM_ACTIVITY_ID,
T.V_TO_ACTIVITY_ID = S.V_TO_ACTIVITY_ID, T.V_CONDITION_EXPR = S.V_CONDITION_EXPR,
T.V_CONDITION_TYPE = S.V_CONDITION_TYPE, T.V_PRECEDENCE = S.V_PRECEDENCE,
T.V_TRANSITION_TYPE = S.V_TRANSITION_TYPE, T.V_TRANSITION_STROKE =
S.V_TRANSITION_STROKE

 WHEN NOT MATCHED THEN INSERT


(V_PROCESS_ID,V_TRANSITION_ID,V_FROM_ACTIVITY_ID,V_TO_ACTIVITY_ID,V_CONDITION_EXPR
,V_CONDITION_TYPE,V_PRECEDENCE,V_TRANSITION_TYPE,V_TRANSITION_STROKE)

 VALUES


(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_FROM_ACTIVITY_ID,S.V_TO_ACTIVITY_ID,S.V_COND
ITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_TYPE,S.V_TRANSITION_ST
ROKE)
/
MERGE INTO AAI_WF_TRANSITION_B T USING (

 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1612765856141' V_TRANSITION_ID,
'Job_1612420416740' V_FROM_ACTIVITY_ID, 'Job_1569914839756' V_TO_ACTIVITY_ID, '-1'
V_CONDITION_EXPR, '1' V_CONDITION_TYPE, '1' V_PRECEDENCE, 'L' V_TRANSITION_TYPE, '
' V_TRANSITION_STROKE FROM DUAL) S

 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID )

 WHEN MATCHED THEN UPDATE SET T.V_FROM_ACTIVITY_ID = S.V_FROM_ACTIVITY_ID,
T.V_TO_ACTIVITY_ID = S.V_TO_ACTIVITY_ID, T.V_CONDITION_EXPR = S.V_CONDITION_EXPR,
T.V_CONDITION_TYPE = S.V_CONDITION_TYPE, T.V_PRECEDENCE = S.V_PRECEDENCE,
```

```
T.V_TRANSITION_TYPE = S.V_TRANSITION_TYPE, T.V_TRANSITION_STROKE =
S.V_TRANSITION_STROKE

 WHEN NOT MATCHED THEN INSERT


(V_PROCESS_ID,V_TRANSITION_ID,V_FROM_ACTIVITY_ID,V_TO_ACTIVITY_ID,V_CONDITION_EXPR
,V_CONDITION_TYPE,V_PRECEDENCE,V_TRANSITION_TYPE,V_TRANSITION_STROKE)
 VALUES


(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_FROM_ACTIVITY_ID,S.V_TO_ACTIVITY_ID,S.V_COND
ITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_TYPE,S.V_TRANSITION_ST
ROKE)
/
MERGE INTO AAI_WF_TRANSITION_B T USING (

 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1612765986197' V_TRANSITION_ID,
'Job_1569914716746' V_FROM_ACTIVITY_ID, 'Job_1612420546036' V_TO_ACTIVITY_ID,
'1533704236345' V_CONDITION_EXPR, '1' V_CONDITION_TYPE, '1' V_PRECEDENCE, 'L'
V_TRANSITION_TYPE, ' ' V_TRANSITION_STROKE FROM DUAL) S

 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID )

 WHEN MATCHED THEN UPDATE SET T.V_FROM_ACTIVITY_ID = S.V_FROM_ACTIVITY_ID,
T.V_TO_ACTIVITY_ID = S.V_TO_ACTIVITY_ID, T.V_CONDITION_EXPR = S.V_CONDITION_EXPR,
T.V_CONDITION_TYPE = S.V_CONDITION_TYPE, T.V_PRECEDENCE = S.V_PRECEDENCE,
T.V_TRANSITION_TYPE = S.V_TRANSITION_TYPE, T.V_TRANSITION_STROKE =
S.V_TRANSITION_STROKE

 WHEN NOT MATCHED THEN INSERT


(V_PROCESS_ID,V_TRANSITION_ID,V_FROM_ACTIVITY_ID,V_TO_ACTIVITY_ID,V_CONDITION_EXPR
,V_CONDITION_TYPE,V_PRECEDENCE,V_TRANSITION_TYPE,V_TRANSITION_STROKE)
 VALUES


(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_FROM_ACTIVITY_ID,S.V_TO_ACTIVITY_ID,S.V_COND
ITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_TYPE,S.V_TRANSITION_ST
ROKE)
/
MERGE INTO AAI_WF_TRANSITION_B T USING (

 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1612766020389' V_TRANSITION_ID,
'Job_1612420546036' V_FROM_ACTIVITY_ID, 'Job_1569914839756' V_TO_ACTIVITY_ID, '-1'
V_CONDITION_EXPR, '1' V_CONDITION_TYPE, '1' V_PRECEDENCE, 'L' V_TRANSITION_TYPE, '
' V_TRANSITION_STROKE FROM DUAL) S

 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID )

 WHEN MATCHED THEN UPDATE SET T.V_FROM_ACTIVITY_ID = S.V_FROM_ACTIVITY_ID,
T.V_TO_ACTIVITY_ID = S.V_TO_ACTIVITY_ID, T.V_CONDITION_EXPR = S.V_CONDITION_EXPR,
T.V_CONDITION_TYPE = S.V_CONDITION_TYPE, T.V_PRECEDENCE = S.V_PRECEDENCE,
T.V_TRANSITION_TYPE = S.V_TRANSITION_TYPE, T.V_TRANSITION_STROKE =
S.V_TRANSITION_STROKE

 WHEN NOT MATCHED THEN INSERT
```

```
(V_PROCESS_ID,V_TRANSITION_ID,V_FROM_ACTIVITY_ID,V_TO_ACTIVITY_ID,V_CONDITION_EXPR
,V_CONDITION_TYPE,V_PRECEDENCE,V_TRANSITION_TYPE,V_TRANSITION_STROKE)
 VALUES


(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_FROM_ACTIVITY_ID,S.V_TO_ACTIVITY_ID,S.V_COND
ITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_TYPE,S.V_TRANSITION_ST
ROKE)
/


MERGE INTO AAI_WF_TRANSITION_TL T USING (
 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1612765003317' V_TRANSITION_ID,
'Transition Line to Service-Task for Individual Screening via EDQ'
V_TRANSITION_NAME, '' V_TRANSITION_DESC, 'en_US' V_LOCALE_CODE FROM DUAL) S
 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID AND
T.V_LOCALE_CODE = S.V_LOCALE_CODE )
 WHEN MATCHED THEN UPDATE SET T.V_TRANSITION_NAME = S.V_TRANSITION_NAME,
T.V_TRANSITION_DESC = S.V_TRANSITION_DESC
 WHEN NOT MATCHED THEN INSERT
 (V_PROCESS_ID,V_TRANSITION_ID,V_TRANSITION_NAME,V_TRANSITION_DESC,V_LOCALE_CODE)
 VALUES


(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_TRANSITION_NAME,S.V_TRANSITION_DESC,S.V_LOCA
LE_CODE)
/
MERGE INTO AAI_WF_TRANSITION_TL T USING (
 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1612765856141' V_TRANSITION_ID,
'Transition Line from Service-Task for Individual Screening via EDQ'
V_TRANSITION_NAME, '' V_TRANSITION_DESC, 'en_US' V_LOCALE_CODE FROM DUAL) S
 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID AND
T.V_LOCALE_CODE = S.V_LOCALE_CODE )
 WHEN MATCHED THEN UPDATE SET T.V_TRANSITION_NAME = S.V_TRANSITION_NAME,
T.V_TRANSITION_DESC = S.V_TRANSITION_DESC
 WHEN NOT MATCHED THEN INSERT
 (V_PROCESS_ID,V_TRANSITION_ID,V_TRANSITION_NAME,V_TRANSITION_DESC,V_LOCALE_CODE)
 VALUES


(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_TRANSITION_NAME,S.V_TRANSITION_DESC,S.V_LOCA
LE_CODE)
/
MERGE INTO AAI_WF_TRANSITION_TL T USING (
```

```
   SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1612765986197' V_TRANSITION_ID,
'Transition Line to Service-Task for Non-Individual Screening via EDQ'
V_TRANSITION_NAME, '' V_TRANSITION_DESC, 'en_US' V_LOCALE_CODE FROM DUAL) S
 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID AND
T.V_LOCALE_CODE = S.V_LOCALE_CODE )
 WHEN MATCHED THEN UPDATE SET T.V_TRANSITION_NAME = S.V_TRANSITION_NAME,
T.V_TRANSITION_DESC = S.V_TRANSITION_DESC
 WHEN NOT MATCHED THEN INSERT
 (V_PROCESS_ID,V_TRANSITION_ID,V_TRANSITION_NAME,V_TRANSITION_DESC,V_LOCALE_CODE)
 VALUES

(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_TRANSITION_NAME,S.V_TRANSITION_DESC,S.V_LOCA
LE_CODE)
/
MERGE INTO AAI_WF_TRANSITION_TL T USING (
 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1612766020389' V_TRANSITION_ID,
'Transition Line from Service-Task for Non-Individual Screening via EDQ'
V_TRANSITION_NAME, '' V_TRANSITION_DESC, 'en_US' V_LOCALE_CODE FROM DUAL) S
 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID AND
T.V_LOCALE_CODE = S.V_LOCALE_CODE )
 WHEN MATCHED THEN UPDATE SET T.V_TRANSITION_NAME = S.V_TRANSITION_NAME,
T.V_TRANSITION_DESC = S.V_TRANSITION_DESC
 WHEN NOT MATCHED THEN INSERT
 (V_PROCESS_ID,V_TRANSITION_ID,V_TRANSITION_NAME,V_TRANSITION_DESC,V_LOCALE_CODE)
 VALUES

(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_TRANSITION_NAME,S.V_TRANSITION_DESC,S.V_LOCA
LE_CODE)
/

delete from AAI_WF_TRANSITION_B where v_process_id='KYC_ONBOARDING' and
V_TRANSITION_ID in
('1569914778656','1569914846233','1569914782899','1569914849735');
delete from AAI_WF_TRANSITION_TL where v_process_id='KYC_ONBOARDING' and
V_TRANSITION_ID in
('1569914778656','1569914846233','1569914782899','1569914849735');

commit;
```

Script for the CS Server

```
MERGE INTO AAI_WF_TRANSITION_B T USING (
 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1569914778656' V_TRANSITION_ID,
'Job_1569914716746' V_FROM_ACTIVITY_ID, 'Job_1569914731139' V_TO_ACTIVITY_ID,
```

```
'1533703981393' V_CONDITION_EXPR, '1' V_CONDITION_TYPE, '1' V_PRECEDENCE, 'C'
V_TRANSITION_TYPE, ' ' V_TRANSITION_STROKE FROM DUAL) S

 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID )

 WHEN MATCHED THEN UPDATE SET T.V_FROM_ACTIVITY_ID = S.V_FROM_ACTIVITY_ID,
T.V_TO_ACTIVITY_ID = S.V_TO_ACTIVITY_ID, T.V_CONDITION_EXPR = S.V_CONDITION_EXPR,
T.V_CONDITION_TYPE = S.V_CONDITION_TYPE, T.V_PRECEDENCE = S.V_PRECEDENCE,
T.V_TRANSITION_TYPE = S.V_TRANSITION_TYPE, T.V_TRANSITION_STROKE =
S.V_TRANSITION_STROKE

 WHEN NOT MATCHED THEN INSERT


(V_PROCESS_ID,V_TRANSITION_ID,V_FROM_ACTIVITY_ID,V_TO_ACTIVITY_ID,V_CONDITION_EXPR
,V_CONDITION_TYPE,V_PRECEDENCE,V_TRANSITION_TYPE,V_TRANSITION_STROKE)

 VALUES


(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_FROM_ACTIVITY_ID,S.V_TO_ACTIVITY_ID,S.V_COND
ITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_TYPE,S.V_TRANSITION_ST
ROKE)
/
MERGE INTO AAI_WF_TRANSITION_B T USING (

 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1569914846233' V_TRANSITION_ID,
'Job_1569914731139' V_FROM_ACTIVITY_ID, 'Job_1569914839756' V_TO_ACTIVITY_ID, '-1'
V_CONDITION_EXPR, '1' V_CONDITION_TYPE, '1' V_PRECEDENCE, 'C' V_TRANSITION_TYPE, '
' V_TRANSITION_STROKE FROM DUAL) S

 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID )

 WHEN MATCHED THEN UPDATE SET T.V_FROM_ACTIVITY_ID = S.V_FROM_ACTIVITY_ID,
T.V_TO_ACTIVITY_ID = S.V_TO_ACTIVITY_ID, T.V_CONDITION_EXPR = S.V_CONDITION_EXPR,
T.V_CONDITION_TYPE = S.V_CONDITION_TYPE, T.V_PRECEDENCE = S.V_PRECEDENCE,
T.V_TRANSITION_TYPE = S.V_TRANSITION_TYPE, T.V_TRANSITION_STROKE =
S.V_TRANSITION_STROKE

 WHEN NOT MATCHED THEN INSERT


(V_PROCESS_ID,V_TRANSITION_ID,V_FROM_ACTIVITY_ID,V_TO_ACTIVITY_ID,V_CONDITION_EXPR
,V_CONDITION_TYPE,V_PRECEDENCE,V_TRANSITION_TYPE,V_TRANSITION_STROKE)

 VALUES


(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_FROM_ACTIVITY_ID,S.V_TO_ACTIVITY_ID,S.V_COND
ITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_TYPE,S.V_TRANSITION_ST
ROKE)
/
MERGE INTO AAI_WF_TRANSITION_B T USING (

 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1569914782899' V_TRANSITION_ID,
'Job_1569914716746' V_FROM_ACTIVITY_ID, 'Job_1569914762385' V_TO_ACTIVITY_ID,
'1533704236345' V_CONDITION_EXPR, '1' V_CONDITION_TYPE, '1' V_PRECEDENCE, 'C'
V_TRANSITION_TYPE, ' ' V_TRANSITION_STROKE FROM DUAL) S

 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID )
```

```
 WHEN MATCHED THEN UPDATE SET T.V_FROM_ACTIVITY_ID = S.V_FROM_ACTIVITY_ID,
T.V_TO_ACTIVITY_ID = S.V_TO_ACTIVITY_ID, T.V_CONDITION_EXPR = S.V_CONDITION_EXPR,
T.V_CONDITION_TYPE = S.V_CONDITION_TYPE, T.V_PRECEDENCE = S.V_PRECEDENCE,
T.V_TRANSITION_TYPE = S.V_TRANSITION_TYPE, T.V_TRANSITION_STROKE =
S.V_TRANSITION_STROKE

 WHEN NOT MATCHED THEN INSERT


(V_PROCESS_ID,V_TRANSITION_ID,V_FROM_ACTIVITY_ID,V_TO_ACTIVITY_ID,V_CONDITION_EXPR
,V_CONDITION_TYPE,V_PRECEDENCE,V_TRANSITION_TYPE,V_TRANSITION_STROKE)

 VALUES


(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_FROM_ACTIVITY_ID,S.V_TO_ACTIVITY_ID,S.V_COND
ITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_TYPE,S.V_TRANSITION_ST
ROKE)

/

MERGE INTO AAI_WF_TRANSITION_B T USING (

 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1569914849735' V_TRANSITION_ID,
'Job_1569914762385' V_FROM_ACTIVITY_ID, 'Job_1569914839756' V_TO_ACTIVITY_ID, '-1'
V_CONDITION_EXPR, '1' V_CONDITION_TYPE, '1' V_PRECEDENCE, 'C' V_TRANSITION_TYPE, '
' V_TRANSITION_STROKE FROM DUAL) S

 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID )

 WHEN MATCHED THEN UPDATE SET T.V_FROM_ACTIVITY_ID = S.V_FROM_ACTIVITY_ID,
T.V_TO_ACTIVITY_ID = S.V_TO_ACTIVITY_ID, T.V_CONDITION_EXPR = S.V_CONDITION_EXPR,
T.V_CONDITION_TYPE = S.V_CONDITION_TYPE, T.V_PRECEDENCE = S.V_PRECEDENCE,
T.V_TRANSITION_TYPE = S.V_TRANSITION_TYPE, T.V_TRANSITION_STROKE =
S.V_TRANSITION_STROKE

 WHEN NOT MATCHED THEN INSERT


(V_PROCESS_ID,V_TRANSITION_ID,V_FROM_ACTIVITY_ID,V_TO_ACTIVITY_ID,V_CONDITION_EXPR
,V_CONDITION_TYPE,V_PRECEDENCE,V_TRANSITION_TYPE,V_TRANSITION_STROKE)

 VALUES


(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_FROM_ACTIVITY_ID,S.V_TO_ACTIVITY_ID,S.V_COND
ITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_TYPE,S.V_TRANSITION_ST
ROKE)

/


MERGE INTO AAI_WF_TRANSITION_TL T USING (

 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1569914778656' V_TRANSITION_ID, 'Gateway
To CSIND' V_TRANSITION_NAME, '' V_TRANSITION_DESC, 'en_US' V_LOCALE_CODE FROM
DUAL) S

 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID AND
T.V_LOCALE_CODE = S.V_LOCALE_CODE )

 WHEN MATCHED THEN UPDATE SET T.V_TRANSITION_NAME = S.V_TRANSITION_NAME,
T.V_TRANSITION_DESC = S.V_TRANSITION_DESC
```

```
WHEN NOT MATCHED THEN INSERT
 (V_PROCESS_ID,V_TRANSITION_ID,V_TRANSITION_NAME,V_TRANSITION_DESC,V_LOCALE_CODE)
 VALUES

(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_TRANSITION_NAME,S.V_TRANSITION_DESC,S.V_LOCA
LE_CODE)
/
MERGE INTO AAI_WF_TRANSITION_TL T USING (
 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1569914846233' V_TRANSITION_ID,
'Job_1569914731139_Job_1569914839756' V_TRANSITION_NAME, '' V_TRANSITION_DESC,
'en_US' V_LOCALE_CODE FROM DUAL) S
 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID AND
T.V_LOCALE_CODE = S.V_LOCALE_CODE )
 WHEN MATCHED THEN UPDATE SET T.V_TRANSITION_NAME = S.V_TRANSITION_NAME,
T.V_TRANSITION_DESC = S.V_TRANSITION_DESC
 WHEN NOT MATCHED THEN INSERT
 (V_PROCESS_ID,V_TRANSITION_ID,V_TRANSITION_NAME,V_TRANSITION_DESC,V_LOCALE_CODE)
 VALUES

(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_TRANSITION_NAME,S.V_TRANSITION_DESC,S.V_LOCA
LE_CODE)
/
MERGE INTO AAI_WF_TRANSITION_TL T USING (
 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1569914782899' V_TRANSITION_ID, 'Gateway
To CSNONIND' V_TRANSITION_NAME, '' V_TRANSITION_DESC, 'en_US' V_LOCALE_CODE FROM
DUAL) S
 ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID AND
T.V_LOCALE_CODE = S.V_LOCALE_CODE )
 WHEN MATCHED THEN UPDATE SET T.V_TRANSITION_NAME = S.V_TRANSITION_NAME,
T.V_TRANSITION_DESC = S.V_TRANSITION_DESC
 WHEN NOT MATCHED THEN INSERT
 (V_PROCESS_ID,V_TRANSITION_ID,V_TRANSITION_NAME,V_TRANSITION_DESC,V_LOCALE_CODE)
 VALUES

(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_TRANSITION_NAME,S.V_TRANSITION_DESC,S.V_LOCA
LE_CODE)
/
MERGE INTO AAI_WF_TRANSITION_TL T USING (
 SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1569914849735' V_TRANSITION_ID,
'Job_1569914762385_Job_1569914839756' V_TRANSITION_NAME, '' V_TRANSITION_DESC,
'en_US' V_LOCALE_CODE FROM DUAL) S
```

```
ON ( T.V_PROCESS_ID = S.V_PROCESS_ID AND T.V_TRANSITION_ID = S.V_TRANSITION_ID AND
T.V_LOCALE_CODE = S.V_LOCALE_CODE )
 WHEN MATCHED THEN UPDATE SET T.V_TRANSITION_NAME = S.V_TRANSITION_NAME,
T.V_TRANSITION_DESC = S.V_TRANSITION_DESC
 WHEN NOT MATCHED THEN INSERT
 (V_PROCESS_ID,V_TRANSITION_ID,V_TRANSITION_NAME,V_TRANSITION_DESC,V_LOCALE_CODE)
 VALUES

(S.V_PROCESS_ID,S.V_TRANSITION_ID,S.V_TRANSITION_NAME,S.V_TRANSITION_DESC,S.V_LOCA
LE_CODE)
/

delete from AAI_WF_TRANSITION_B where v_process_id='KYC_ONBOARDING' and
V_TRANSITION_ID in
('1612765003317','1612765856141','1612765986197','1612766020389');

delete from AAI_WF_TRANSITION_TL where v_process_id='KYC_ONBOARDING' and
V_TRANSITION_ID in
('1612765003317','1612765856141','1612765986197','1612766020389');


commit;
```

Index