

Oracle Financial Services Know Your Customer

Administration Guide

Release 8.1.2.3.0

December 2022

F17838-04

ORACLE®

Financial Services

OFS Know Your Customer Administration Guide

Copyright © 2022 Oracle and/or its affiliates. All rights reserved.

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

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

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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

For information on third party licenses, click [here](#).

Document Control

Table 1: Document Control

Revision Number	Revision Date	Change Log
8.1.2.3.0	December 2022	<ul style="list-style-type: none">Updated the Mapping a User with a User Group section with updated user roles.Added Setting the Interested party Level, Modifying the Risk Scores and Viewing the Risk Categories and APPENDIX-D Switching between EDQ and CS sections.
8.1.2.2.0	September 2022	Added the steps to Add a Parameter/Rule value in Adding Risk Scores for Parameter/Rule Values section.
8.1.2.1.0	June 2022	A new version is created and the screenshots are updated for the KYC Onboarding and Adding Risk Parameters and Rules (KYC Batch) section as part of the UI changes.
8.1.2.0.0	March 2022	A new version has been created for the 8.1.2.0.0 release.

Table of Contents

1	About This Guide	8
1.1	Intended Audience	8
1.2	Access to Oracle Support	8
1.3	How this Guide is Organized	8
1.4	Where to Find More Information	9
1.5	Conventions Used in This Guide	9
2	About Oracle Financial Services KYC	11
2.1	KYC Overview	11
2.2	KYC Workflow	11
3	Getting Started	14
3.1	Accessing OFSAA Applications	14
3.2	Managing OFSAA Application Page	15
3.2.1	<i>Behavior Detection - KYC Tab</i>	15
3.2.2	<i>Common Tasks Tab</i>	16
3.3	Troubleshooting Your Display	16
3.3.1	<i>Enabling JavaScript</i>	17
3.3.2	<i>Enabling Cookies</i>	17
3.3.3	<i>Enabling Temporary Internet Files</i>	17
3.3.4	<i>Enabling File Downloads</i>	17
3.3.5	<i>Setting Printing Options</i>	18
3.3.6	<i>Enabling the Pop-Up Blocker</i>	18
3.3.7	<i>Setting Preferences</i>	18
4	Managing User Administration and Security Configuration	20
4.1	About User Administration	20
4.2	User Provisioning Process Flow	20
4.2.1	<i>Managing User Administration</i>	21
4.3	Adding Security Attributes	23
4.3.1	<i>About Security Attributes</i>	23
4.3.2	<i>Loading Security Attributes through SQL Scripts</i>	24
4.4	Mapping Security Attributes to Users	27

4.5	Removing Security Attributes.....	30
5	Maintenance Activities and Configuring Setup Parameters (KYC Batch).....	31
5.1	Prerequisite.....	31
5.2	Maintenance and Configuration Activities	31
5.2.1	<i>Initial or One-time Activities</i>	31
6	Integrating with ECM.....	39
6.1	Configuring in the ECM UI:.....	39
6.1.1	<i>Updating the URL for the KYC Close Service</i>	39
6.1.2	<i>Updating the KYC Get Overridden Risk Details URL</i>	39
6.1.3	<i>Updating the BD Application URL for the KYC Customer Dashboard</i>	40
6.1.4	<i>Updating the Username and Password for the Common Gateway Service</i>	40
6.1.5	<i>Updating the Username and Password for the Create JSON Service</i>	41
6.1.6	<i>Updating the Username and Password for the KYC Risk Score UI Service</i>	41
6.1.7	<i>Updating the Username and Password for the JSON To Table Service</i>	42
7	Managing KYC Batches	43
7.1	About KYC Batches.....	43
7.2	Deployment Initiation Processing.....	43
7.2.1	<i>Adding the Beneficial Owner Process to the Deployment Initiation Processing Batch</i>	44
7.2.2	<i>Setting the Interested party Level</i>	44
7.3	End of Day Processing	44
7.3.1	<i>Feedback to the OFS BD Framework or Account Opening System</i>	45
7.3.2	<i>Renaming and Transferring Feedback files</i>	47
7.4	Regular Processing	47
7.4.1	<i>Prefilter Rules</i>	47
7.4.2	<i>Risk Assessment Initiation</i>	47
7.4.3	<i>Closure Updates</i>	48
7.4.4	<i>Promote to Case</i>	49
7.5	Running KYC Batches.....	49
7.6	Running a Single Task Using a Batch	50
7.7	Scheduling a Batch	51
7.7.1	<i>Scheduling a Batch Once</i>	52

7.7.2	<i>Scheduling a Daily Batch</i>	53
7.7.3	<i>Scheduling a Weekly Batch</i>	54
7.7.4	<i>Scheduling a Monthly Batch</i>	54
7.7.5	<i>Scheduling an Adhoc Batch</i>	54
7.7.6	<i>KYC Batch Execution Logs</i>	55
8	KYC Onboarding	57
8.1	Populating Country Data in KDD_CODE_SET_TRNLN Table	57
8.2	Configuring the Service Parameters through the User Interface	57
8.2.1	<i>Configuring the Onboarding Service Parameters</i>	57
8.2.2	<i>Configuring the Common Gateway Service Parameters</i>	59
8.3	Performing Assessments on Related Applicants	61
8.4	Uploading Excel Data	62
8.5	Adding Rule Values for Rule-based Risk Assessments	63
8.5.1	<i>Adding a Rule</i>	64
8.5.2	<i>Enabling or Disabling the Risk Parameter during Risk Assessments</i>	64
8.6	Modifying the Algorithm-based Risk Assessments	64
8.6.1	<i>Modifying the Weight of the Risk Parameter</i>	65
8.6.2	<i>Enabling or Disabling the Risk Parameter during Risk Assessments</i>	65
8.7	Modifying the Risk Scores and Viewing the Risk Categories	65
8.7.1	<i>Modifying the Risk Scores</i>	66
8.7.2	<i>Mapping Rules to Evaluations</i>	67
8.7.3	<i>Mapping Parameters to Evaluations</i>	67
8.7.4	<i>Copying Risk Scores across Jurisdictions</i>	69
8.8	Modifying and Adding the Mapping Codes within KYC	70
8.8.1	<i>Downloading the Code Values</i>	70
8.8.2	<i>Adding New Code Values</i>	70
9	Adding Risk Parameters and Rules (KYC Batch)	71
9.1	Adding Risk Parameters for Algorithm-based Risk Assessments	71
9.2	Adding Rules for Rule-based Risk Assessments	82
9.2.1	<i>Adding a Risk Parameter or Rule for Reassessments</i>	92
9.3	Adding Rules for Accelerated Rules	93

9.3.1	<i>Mapping an Evaluation to an Assessment</i>	94
9.3.2	<i>Adding Risk Scores for Parameter/Rule Values</i>	95
9.3.3	<i>Disabling Accelerated Re-Review Rules</i>	97
9.4	Modifying the Risk Scores and Viewing the Risk Categories	97
9.4.1	<i>Modifying the Risk Scores</i>	97
9.4.2	<i>Copying the Risk Scores</i>	98
9.4.3	<i>Showing the History of Risk Scores</i>	98
10	APPENDIX-A	KYC Batches 99
10.1	Regular Processing	99
10.2	Deployment Initiation Processing	104
10.3	End of Day Processing	108
11	APPENDIX-B	Creating Highlights 109
12	APPENDIX-C	Configuring Steps for CS Delta Updates 112
12.1	Adding the CS Task to the KYC Daily Batch	112
12.1.1	<i>Running the Daily Batch</i>	112
12.1.2	<i>Running the Deployment Initiation Batch</i>	114
12.2	Mapping the Watch List evaluation to the Accelerated Re-review Assessment	117
13	APPENDIX-D Switching between EDQ and CS	119
14	OFSAA Support	123
15	Send Us Your Comments	124

1 About This Guide

This guide provides information about risk assessments being performed on a customer to adhere to the norms of Oracle Financial Services Know Your Customer (OFS KYC). It also covers different risk models with the parameters considered for assessing a customer's risk to a financial institution.

Topics:

- [Intended Audience](#)
- [Access to Oracle Support](#)
- [How this Guide is Organized](#)
- [Where to Find More Information](#)
- [Conventions Used in This Guide](#)

1.1 Intended Audience

The KYC Risk Assessment Guide is designed for various OFS KYC users. Their roles and responsibilities, as they operate within the OFS KYC application, include the following:

- **Business Analyst:** A user in this role analyses and disposes the risk assessments. This user understands how risk assessments are calculated and which risk score attributes contribute to the risk score. This user can also manually promote the risk assessments to a case and review the KYC Cases if KYC is integrated with Enterprise Case Management (ECM). A Business Analyst guides the Administrator to fine-tune the parameters required for risk assessments.
- **KYC Administrator:** This user is a manager for data center activities and application administration activities in a financial institution. This user has access to configuration functionalities and is responsible for configuring the required details for executing the KYC process. This user also has in-depth knowledge of all modules of KYC to perform the necessary administration and maintenance.

1.2 Access to Oracle Support

Oracle customers have access to electronic support through [My Oracle Support](#). For information, visit [Oracle Accessibility Learning and Support](#).

Or visit [Telecommunications Relay Service](#), if you are hearing-impaired.

1.3 How this Guide is Organized

The OFS KYC Administration Guide includes the following chapters:

- [About Oracle Financial Services KYC](#) provides a brief overview of the OFS KYC process and its components.
- [Getting Started](#) explains common elements on the interface, includes instructions on how to configure your system, access KYC, and exit the application.
- [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 \(KYC Batch\)](#) describe how to configure the KYC application.

- [Integrating with ECM](#) explains the configurations that must be performed in the ECM User Interface (UI).
- [Managing KYC Batches](#) provides information on how to manage the different KYC batches.
- [KYC Onboarding](#) provides information on the different processes involved in KYC Onboarding.
- [Adding Risk Parameters and Rules \(KYC Batch\)](#) describes how to add risk parameters for algorithm-based assessments, rule-based assessments, and accelerated re-review parameters.
- [APPENDIX-A KYC Batches](#) provides information on the KYC batches.
- [APPENDIX-B Creating Highlights](#) provides information on how to create highlights for risk assessments.
- [APPENDIX-C Configuring Steps for CS Delta Updates](#) provides information on the configuration steps.

1.4 Where to Find More Information

For more information about OFS KYC, see the following KYC application documents, which can be found on the [Oracle Help Center](#) page:

- KYC Risk Assessment Guide
- Data Interface Specification (DIS) Guide
- Data Model Reference (DMR) Guide
- Service Guide
- API Data Elements Guide
- Utilities Guide
- ECM User Guide

To find additional information about how OFS solves real business problems, see our website on [Oracle for Financial Services home page](#).

1.5 Conventions Used in This Guide

[Table 1](#) mentions the conventions used in this guide.

Table 1: Conventions Used

Conventions	Meaning
<i>Italics</i>	<ul style="list-style-type: none"> • Names of books as references • Emphasis • Substitute input values
Bold	<ul style="list-style-type: none"> • Menu names, field names, options, button names • Commands typed at a prompt • User input

Table 1: Conventions Used

Conventions	Meaning
Monospace	<ul style="list-style-type: none">• Directories and subdirectories• File names and extensions• Code sample, including keywords and variables within the text and as separate paragraphs, and user-defined program elements within the text
Hyperlink	Hyperlink type indicates the links to external websites and internal document links to sections.
Asterisk (*)	Mandatory fields in User Interface.
<Variable>	Substitute input value.

2 About Oracle Financial Services KYC

This chapter briefly overviews Oracle Financial Services Know Your Customer (OFS KYC) in terms of its architecture and operations.

Topics:

- [KYC Overview](#)
- [KYC Workflow](#)

2.1 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
- Re-review

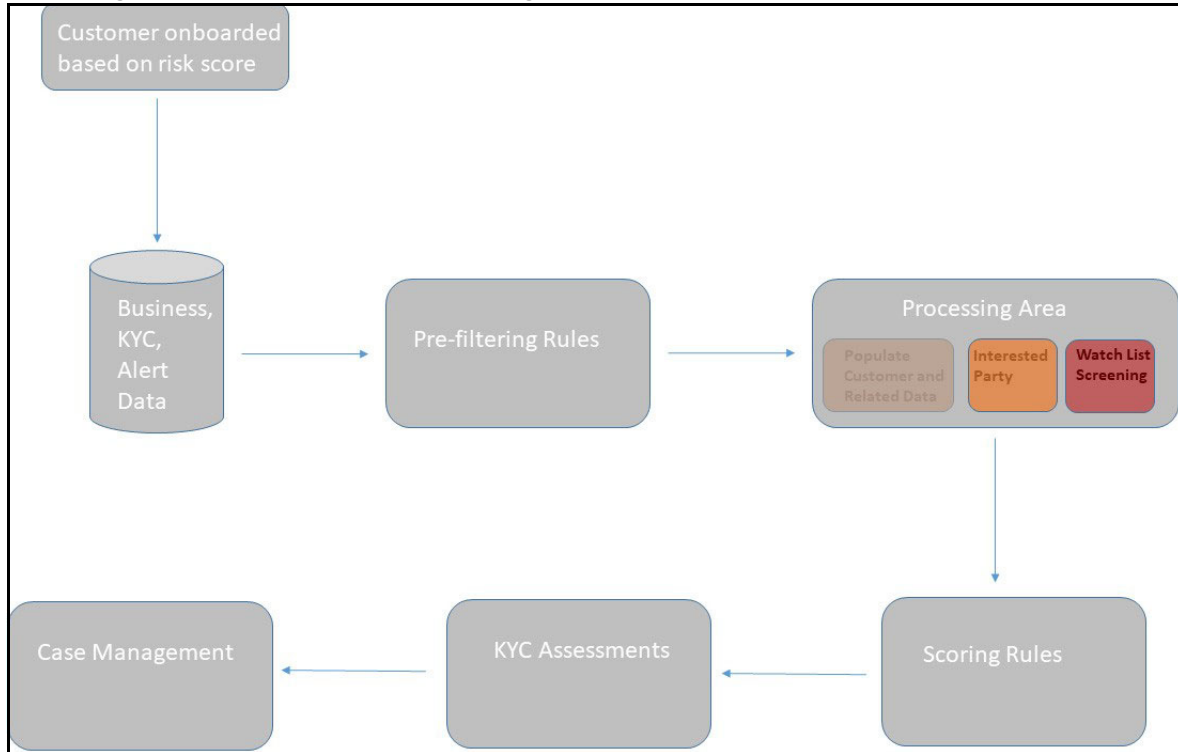
The Oracle KYC risk assessment application is built using the OFS Analytical Applications Infrastructure (AAI) framework. The application functions are divided into the following areas:

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

2.2 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. The 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.
All data is not moved to the processing area. It is moved using certain prefiltering rules, such as accelerated re-reviews, periodic reviews, and account Onboarding. The prefiltering rules identify a set of customers due for review depending on these rules.
3. The processing area contains the data of all customers for whom the prefiltering rules apply and for whom risk scoring needs to be done.
4. The prefiltered customers are scored using two risk assessments to get the risk score on the customer attributes: Algorithm-based risk assessments and Rule-based risk assessments. The risk score is the maximum of the Algorithm-based risk score and Rule-based risk score.
5. A risk assessment record is created for each customer who is scored. The risk assessment contains data such as the risk score, risk assessment history, and customer review details. Based on the risk score, the risk assessment can either be closed or promoted to a case.
6. A risk assessment is considered for a promotion to a case under the following conditions:
 - The customer's 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.

3 Getting Started

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

Topics:

- [Accessing OFSAA Applications](#)
- [Managing OFSAA Application Page](#)
- [Troubleshooting Your Display](#)

3.1 Accessing OFSAA Applications

Access to the OFS KYC application depends on the Internet or Intranet environment. The system administrator provides the intranet address uniform resource locator (URL), User ID, and Password. Log in 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 OFSAA, follow these steps:

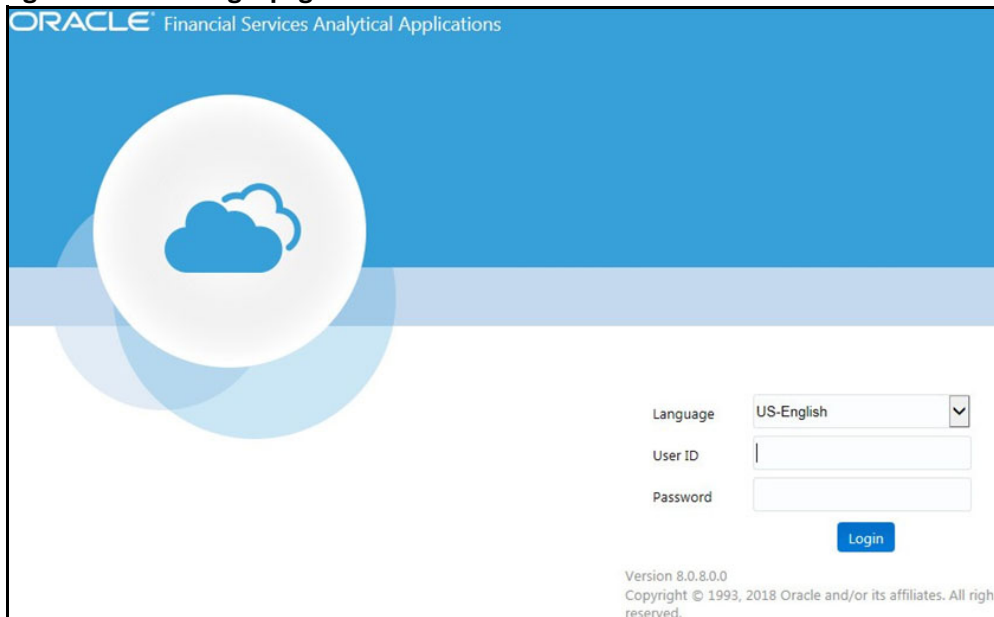
1. Enter the URL in your browser using the following format:

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

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

The OFSAA Login page is displayed.

Figure 2: OFSAA Login page



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 OFSAA page is displayed.

3.2 Managing OFSAA Application Page

This section describes the options available for system configuration on the OFSAA Application page. The OFSAA Application page has the following tabs:

- Behavior Detection - KYC Tab
- Common Tasks Tab

3.2.1 Behavior Detection - KYC Tab

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

To do this, follow these steps:


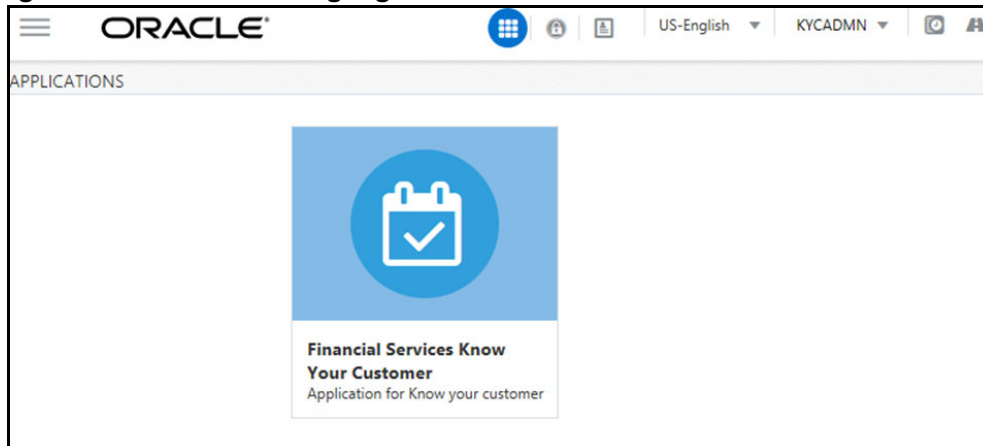
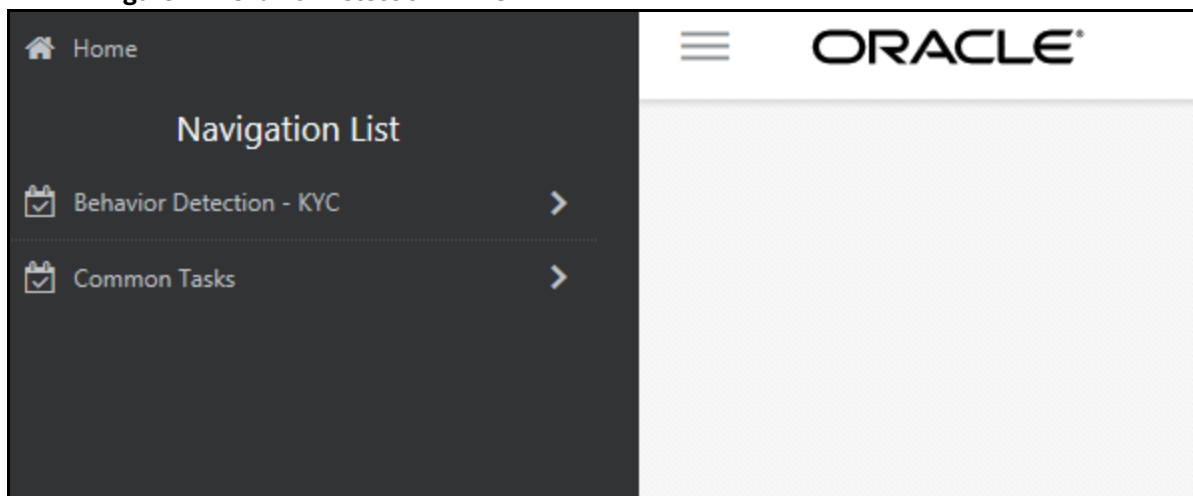
1. Click the  icon.

Figure 3: OFSAA KYC Landing Page



2. Click **Behavior Detection - KYC**. The KYC page appears.

Figure 4: Behavior Detection – KYC Link



3.2.2 Common Tasks Tab

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

To work with KYC common tasks tab, follow these steps:


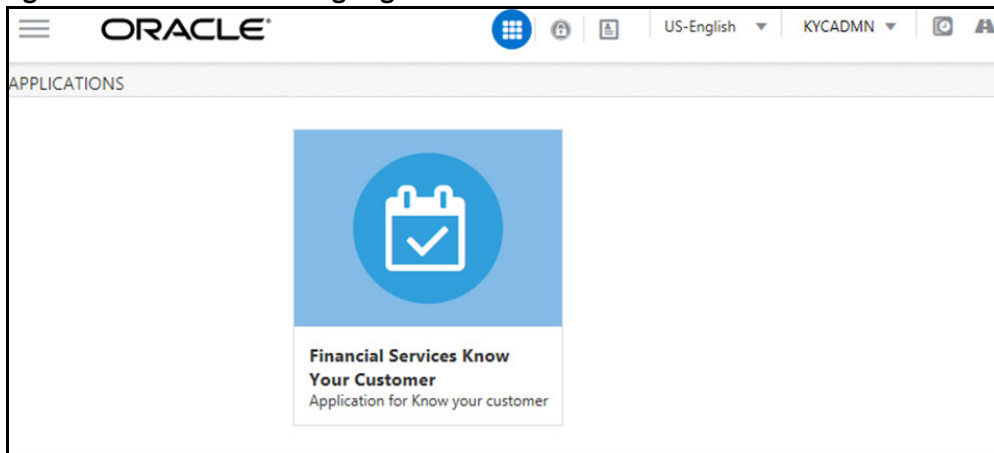
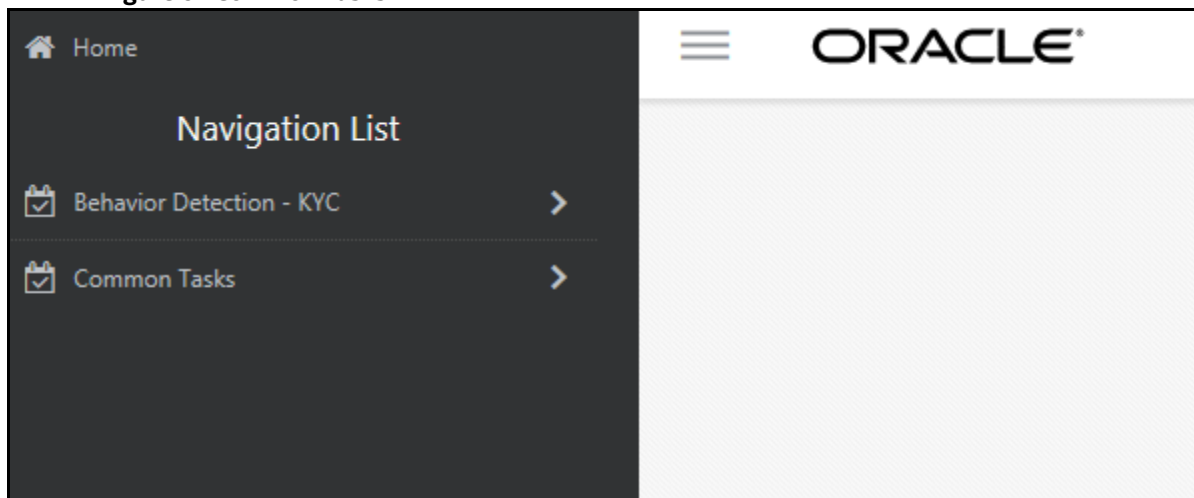
1. Click the  icon.

Figure 5: OFSAA KYC Landing Page



2. Click **Common Tasks**. The KYC page appears.

Figure 6: Common Tasks



3.3 Troubleshooting Your Display

If you experience problems logging into OFS KYC 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.

Topics:

- [Enabling JavaScript](#)
- [Enabling Cookies](#)

- [Enabling Temporary Internet Files](#)
- [Enabling File Downloads](#)
- [Setting Printing Options](#)
- [Enabling the Pop-Up Blocker](#)
- [Setting Preferences](#)

3.3.1 Enabling JavaScript

This section describes how to enable JavaScript.

To enable JavaScript, follow these steps:

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

3.3.2 Enabling Cookies

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

3.3.3 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.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. On the **General** tab, click **Settings**. The **Settings** dialog box is displayed.
4. Click **Every visit to the page**.
5. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

3.3.4 Enabling File Downloads

This section describes how to enable file downloads.

To enable file downloads, follow these steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Security** tab and then click **Local Intranet**.
4. Click **Custom Level**. The **Security Settings** dialog box is displayed.

5. Under the **Downloads** section, ensure that **Enable** is selected for all options.
6. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

3.3.5 Setting Printing Options

This section explains how to enable printing background colors and images.

To enable this option, follow these steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Advanced** tab. In the **Settings** list.
4. Under the **Printing** setting, click **Print background colors and images**.
5. Click **OK** to exit the **Internet Options** dialog box.

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

3.3.6 Enabling the Pop-Up Blocker

You may have trouble running the OFC KYC application when the Internet Explorer (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** menu.

To enable the Pop-up Blocker, follow these steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Privacy** tab. In the **Pop-up Blocker** setting, select **Turn on Pop-up Blocker**. The Settings are enabled.
4. Click **Settings** to open the **Pop-up Blocker Settings** dialog box.
5. In the **Pop-up Blocker Settings** dialog box, enter the URL of the application in the text area.
6. Click **Add**. The URL appears in the **Allowed Sites** list.
7. Click **Close**, then click **Apply** to save the settings.
8. Click **OK** to exit the **Internet Options** dialog box.

3.3.7 Setting Preferences

Use the Preferences section to enable you to set your OFSAA home page.

To access this section, follow these steps:

1. On the **Financial Services Analytical Applications Know Your Customer** landing page, select **Preferences** from the username drop-down list. The **Preferences** page is displayed.

Figure 7: Preferences Page



The screenshot shows a 'Preferences' window with a tree view on the left containing 'Home Page'. The main area is a table with two columns: 'Property Name' and 'Property Value'. The table has two rows: 'Set My Home Page' with a dropdown menu showing 'Default Screen', and 'Date Format' with a dropdown menu showing '-- Select --'. At the bottom right are 'Save' and 'Cancel' buttons.

Property Name	Property Value
Set My Home Page	Default Screen
Date Format	-- Select --

2. In the **Set My Home Page** drop-down list, select the window you want to view when you log in. When a new application is installed, the related window of the application is found in the drop-down list.
3. In the **Date Format** drop-down list, select the date format you want to see. The options available are dd/MM/yyyy or M/dd/yyyy.
4. Click **Save** to save your preferences.

4 Managing User Administration and Security Configuration

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

Topics:

- [About User Administration](#)
- [User Provisioning Process Flow](#)
- [Managing User Administration](#)
- [Mapping Security Attributes to Users](#)
- [Removing Security Attributes](#)

4.1 About User Administration

User administration involves creating and managing users and providing access rights based on their roles.

4.2 User Provisioning Process Flow

The following image shows the process flow for user provisioning:

Figure 8: User Provisioning Process Flow

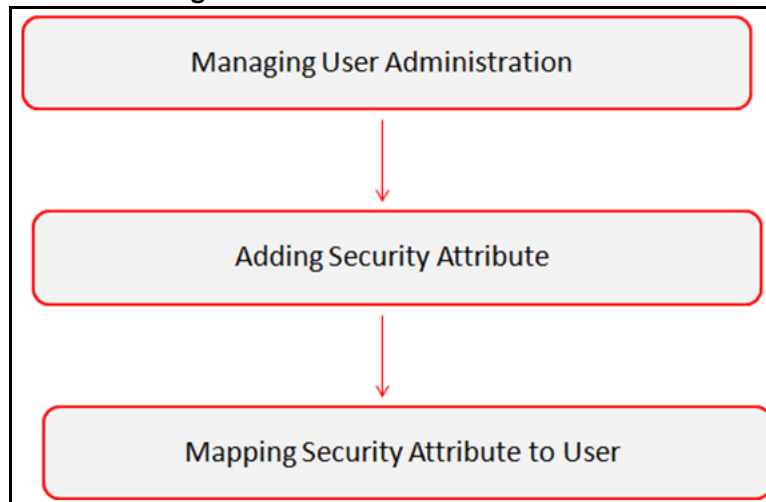


Table 2 lists the various actions and associated descriptions of the user administration process flow.

Table 2: 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.

Table 2: User Provisioning Process Flow

Action	Description
Table 4 describes the predefined KYC User Groups and the corresponding user activities.	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.

4.2.1 Managing User Administration

This section allows you to create, map, and authorize users to define a security framework restricting access to the KYC application.

4.2.1.1 Managing Identity and Authorization

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

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

Figure 9: Managing Identity and Authorization Process Flow

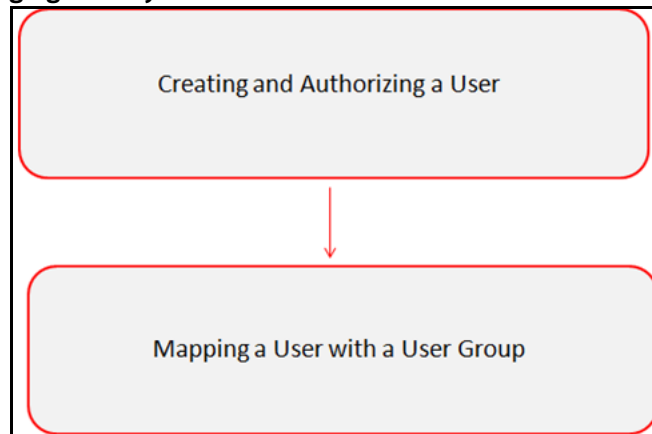


Table 3 lists the various actions and associated descriptions of the user administration process flow.

Table 3: Administration Process Flow

Action	Description
Creating and Authorizing a User	Create a user. This involves providing a username, 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.

4.2.1.1.1 Creating and Authorizing a User

The sysadm 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](#).

4.2.1.1.2 Mapping a User with a User Group

This section explains how to map Users and User Groups. With this, the user can access the privileges as per the role. The sysadm user maps a user to a user group in the KYC application.

Table 4 describes the predefined KYC User Roles and corresponding User Groups.

Table 4: KYC Roles and User Groups

Role	User Group
KYC Administrator User	<ul style="list-style-type: none"> KYC Administrator User Group OB (Onboarding) KYC Administrator Group IPEADMN
KYC Investigator User	<ul style="list-style-type: none"> KYC Investigator User Group OB KYC Investigator Group
KYC Investigator Rd Only	<ul style="list-style-type: none"> KYC Investigator Read Only Group

Table 4 describes the predefined KYC User Groups and the corresponding user activities.

Table 5: 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.
KYC Investigator Read Only Group	The users belonging to this group will only be able to view KYC batch risk assessments.

4.2.1.1.3 Privileges, Function Code & Name and their Description

This section explains KYC-related Privileges, Function Code and Name and their Description.

Table 6 describes the Privileges, Function Code & Name and their Description.

Table 6: Privileges, Function Code & Name and their Description

SL #	Privileges	V_FUNCTION_CODE	V_FUNC-TION_NAME	V_FUNCTION_DESC
1	Access KYC Batch Admin Menus	CMKYCADMN	CM KYC Administrator	CM KYC Administrator
2	Access Onboarding KYC Admin Menus	OBKYCADMN	OB KYC Administrator	OB KYC Administrator
3	Access KYC Assessments Menu - Read Only	OFSKYC	View KYC	View KYC
4	Access KYC Assessments Menu	KYCRA	KYC Assessments	KYC Assessments
5	KYC Redact Function	KYC_REDACT	Redact Function for KYC	Redact Function for KYC
6	Access Onboarding KYC Assessments Menu	OBKYCASMNT	View OB KYC Assessments	View OB KYC Assessments
7	Access KYC Tabs in case management	CMKYCACSES	CM KYC Access	CM KYC Access

4.3 Adding Security Attributes

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

4.3.1 About Security Attributes

Security attributes help an organization classify their users based on geographical location, jurisdiction, and business domain to restrict access to the data they can view.

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

The following security attributes are 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:** Data division based on geographical boundaries, such as countries and states.
 - **Organizational:** Data division based on different legal entities that compose the client's business.

- **Other:** Combination of geographic and organizational definitions. You can customize this attribute.

4.3.2 Loading Security Attributes through SQL Scripts

Topics:

- [Loading Jurisdictions](#)
- [Loading Business Domains](#)
- [Loading Scenario Groups](#)
- [Loading Scenario Group Memberships](#)
- [Loading Organizations](#)

4.3.2.1 Loading Jurisdictions

To load jurisdictions in the database, follow these steps:

1. Add the appropriate record to the `KDD_JRSDCN` database table.

[Table 7](#) shows the `KDD_JRSDCN` database table attributes.

Table 7: KDD_JRSDCN Table Attributes

Column Name	Description
JRSDCN_CD	Code (one to four characters) that represents a jurisdiction (For example, N for North, or S for South).
JRSDCN_NM	Name of the jurisdiction (For example, North or South).
JRSDCN_DSPLY_NM	Display the 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 an SQL script similar to the following sample script:

```
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.

4.3.2.2 Loading Business Domains

To load a business domain, follow these steps:

1. Add the appropriate user record to the `KDD_BUS_DMN` database table.

Table 8 shows the KDD_BUS_DMN database table attributes.

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 the name of the business domain (For example, INST or RET).
MANTAS_DMN_FL	The flag that indicates whether Oracle Financial Services Behavior Detection (OFS BD) Framework specified the business domain (Y). If a BD client specifies 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 an SQL script similar to the following sample script:

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

4.3.2.3 Loading Scenario Groups

To load a Scenario Group, follow these steps:

1. Add the appropriate user record to the KDD_SCNRO_GRP database table.

Table 9 shows the KDD_SCNRO_GRP database table attributes.

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 following sample script:

```
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;

4.3.2.4 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.

Table 10 shows the `KDD_SCNRO_GRP_MEMBERSHIP` database table attributes.

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 following sample script:

```
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') ;
```

4.3.2.5 Loading Organizations

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

1. Add the appropriate user record to the `KDD_ORG` database table.

Table 11 shows the `KDD_ORG` database table attributes.

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	The parent organization of which this organization is a child. This must reference an <code>ORG_CD</code> in the <code>KDD_ORG</code> 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. This must reference a user in the Investigation Owner table (<code>KDD_REVIEW_OWNER.OWNER_SEQ_ID</code>).
COMMENT_TX	Additional remarks added by the user.

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

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

4.4 Mapping Security Attributes to Users

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

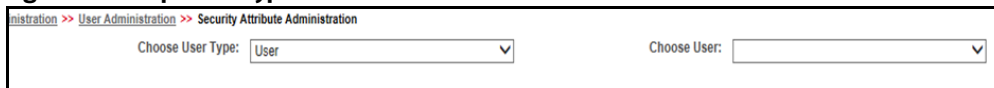
To map a Security Attribute, follow these steps:

1. Log in 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. In the **Administration** menu, select the **User Administration** sub-menu, and click **Security Attribute Administration**. The **Security Attribute Administration** page is displayed.
4. Select the user type from the **Choose User Type** drop-down list (Organization or User).

NOTE Before proceeding with providing a user access through this User Interface (UI), all necessary data must be available in the appropriate database tables and the user must be created.

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

Figure 10: Map User Types to Users



The screenshot shows the breadcrumb navigation: Administration >> User Administration >> Security Attribute Administration. Below the navigation, there are two dropdown menus. The first is labeled 'Choose User Type:' and has 'User' selected. The second is labeled 'Choose User:' and is currently empty.

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

Figure 11: Security Attribute Administration Page

Administration >> User Administration >> Security Attribute Administration

Choose User Type: Organization Choose User: RetailOrg

User/Pool: POOL

Line Organization: RetailOrg

Parent Organization: --

Own Case Flag: No

Own Alert Flag: No

Email Address: --

Jurisdiction: AMEA,DOM

Jurisdiction (2) | Remove

Jurisdiction Code	Jurisdiction Name
<input type="checkbox"/> AMEA	AMEA
<input type="checkbox"/> DOM	DOM

Business Domain: GEN,INST,RB/PC,RET,C/WS,EMP,DEFAULT

Business Domain (7) | Remove

Business Domain Code	Business Domain Name	Business Domain Description
<input type="checkbox"/> a	GEN	General
<input type="checkbox"/> b	INST	Institutional Broker Dealer
<input type="checkbox"/> c	RB/PC	Retail Brokerage/Private Client
<input type="checkbox"/> d	RET	Retail Banking
<input type="checkbox"/> e	C/WS	Corporate/Wholesale Banking

Scenario Group: TC,BEX,ML,IML,CST,MF,TRA,ET,IA,FR,AM,CR,ECTC

Scenario Group (13) | Expand All | Remove

Scenario Class Code	Scenario Class Name
<input type="checkbox"/> AM	Asset Management
<input type="checkbox"/> CR	Control Room
<input type="checkbox"/> ET	Employee Trading
<input type="checkbox"/> FR	Fraud
<input type="checkbox"/> IA	Investment Advisor

Case Type Subtype: Access/Online Fraud,Account and Product Fraud,AML Surveillance,Enhanced Due Diligence,Terrorist Financing,Patriot Act - CIP Exceptions,Employ

Case Type Subtype (11) | Expand All | Remove

Case Type Subtype Code	Case Type Subtype Name
<input type="checkbox"/> FR_ON	Access/Online Fraud
<input type="checkbox"/> FR_AC	Account and Product Fraud
<input type="checkbox"/> AML_SURV	AML Surveillance
<input type="checkbox"/> AML_DD	Enhanced Due Diligence
<input type="checkbox"/> AML_TER	Terrorist Financing

Correlation Rule:

Correlation Rule (0) | Remove

Save Cancel

NOTE

- 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 becomes inactive.

Table 12 shows the security attributes.

Table 12: Security Attributes

Column Name	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, suppose a user is mapped to Org1 and Org2. In that case, it implies that this user can access alerts and cases belonging to these two organizations, provided other security attributes also match.
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 an alert flag from the drop-down list. 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 user must be mapped to any one of the following user groups: <ul style="list-style-type: none"> • Case Supervisor • Case Analyst1 • Case Analyst2
PRNT_ORG_CD	The parent organization of which this organization is a child. 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. This must reference a user in the Investigation Owner table (KDD_REVIEW_OWNER.OWNER_SEQ_ID).
COMMENT_TX	Additional remarks added by the user.
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 one or more jurisdictions to a user or organization allow this user or organization to access cases, alerts, watch lists, and watch list members belonging to the mapped jurisdiction. The selected jurisdictions are displayed in the Jurisdictions section after you save your selection.
Business Domain	Select the business domains from the drop-down list. Mapping one or more business domains to a user or organization allow this user or organization to access cases, alerts, watch lists, and watch list members belonging to the mapped business domains. The selected jurisdictions are displayed in the Jurisdictions section after you save your selection.
Scenario Group	Select the scenario group from the drop-down list. Mapping 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 the Jurisdictions section after you save your selection.

Table 12 shows the security attributes.

Table 12: Security Attributes

Column Name	Description
Case Type	Select the case type from the drop-down list. Mapping 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 the Case Types section after you save your selection.
Correlation Rule	Select the correlation rule from the drop-down list. Mapping one or more correlation rules allows the user to view the correlations generated based on the mapped correlation. The selected jurisdictions are displayed in the correlation section after you save your selection.

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

4.5 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 record?
3. Click **OK**. The selected record is deleted from the list.
4. Click **Save**. The changes are updated.

5 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.

Topics:

- [Prerequisite](#)
- [Maintenance and Configuration Activities](#)

5.1 Prerequisite

The OFS BD application pack must be installed. For information on pack installation, see the *Obtaining Software* section in the [Oracle Financial Services Behavior Detection \(OFS BD\) Application Pack Installation Guide](#).

5.2 Maintenance and Configuration Activities

OFS Know Your Customer (KYC) activities are classified into the following types:

- [Initial or One-time Activities](#)
- [Daily Activities](#)

5.2.1 Initial or One-time Activities

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

Topics:

- [Managing Users](#)
- [Uploading Data using Excel](#)
- [Moving the Country Data in the KDD_CODE_SET_TRNLN table](#)
- [Configuring Application Parameters](#)
- [Configuring Application Installation Parameters](#)
- [Configuring Rule Based Risk Values](#)
- [Defining the Re-review Rule Details](#)
- [Configuring Algorithm Based Risk Parameters](#)
- [Configuring Scores for Values in KYC Risk Assessments](#)
- [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](#)

5.2.1.1 Managing Users

Users need to be created in KYC for KYC-related processing. For information on the users that need to be created, see [Mapping a User with a User Group](#). For information on how to create users, see [Managing User Administration and Security Configuration](#).

5.2.1.2 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 you have uploaded equals 100.
- **DIM_RISK_CATEGORY:** Ensure that the minimum range of consecutive rows equals 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_ACCT_CUST_ROLE_TYPE:** Ensure that the value in the F_CONTROLLING_ROLE column is Y 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 excel through the UI. All column values must be according to the data types and expected character length. Refer to 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 \(KYC Batch\)](#).

5.2.1.3 Moving the Country Data in the 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 perform this activity, 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;
```


5.2.1.4 **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 impact the various services invoked by the application, and the workflow 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 \(KYC Batch\)](#).

5.2.1.5 **Configuring Application Installation Parameters**

The Application Installation Parameters contain information about installation-specific parameters that do not vary with the jurisdiction. This table has only one set of parameters for an installation. You can modify the values in the UI. For more information, see [Adding Risk Parameters and Rules \(KYC Batch\)](#).

5.2.1.6 **Configuring Rule Based Risk Values**

Rule-Based Risk Assessment Parameters contain information about the pre-defined rules and the parameter values (which can vary according to the jurisdiction). It is mandatory to update rules values for all the jurisdictions for which the Rule-Based Risk Assessment is used. For more information, see [Adding Risk Parameters and Rules \(KYC Batch\)](#).

5.2.1.7 **Defining the Re-review Rule Details**

The OFS KYC comes with pre-packaged rules based on which the Accelerated Re-review is triggered. These rules are available in the Application Re-review Parameters Table (`Appln_ReReview_Params`). Each record contains a rule number associated with the Re-review Rules. Each rule can be enabled or disabled depending on the site-specific requirement. The `Appln_ReReview_Params` table specifies details such as Look Back Period, Count of Alerts, and Alert Score for the Rule. For more information, see [Adding Risk Parameters and Rules \(KYC Batch\)](#).

5.2.1.8 **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 database 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 \(KYC Batch\)](#).

5.2.1.9 **Configuring Scores for Values in KYC Risk Assessments**

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.

5.2.1.10 **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 on 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_trnltn set code_val='', code_disp_tx = '' where
code_val = '' and code_set='';
```

5.2.1.11 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 the `appln_install_params` table 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_URL:** Replace the placeholders for <PROTOCOL>, <HOST_NAME>, <PORT> and <OFSAA_DOMAIN> in the `v_attribute1_value` field with the appropriate values.
- **RAOR_URL:** 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 Enterprise Case Management (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 is available in an SQL file post-installation. Depending on the setup, the appropriate link must be executed.

5.2.1.12 Scheduling KYC Batches

After the installation is complete, the user must log in to the OFS KYC as the KYC Administrator and perform the steps mentioned in Managing KYC Batches.

NOTE

The batches are not visible on the Batch execution page 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 the OFS BD 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 Enhanced Due Diligence (EOD) processing. The default review execution must be scheduled as an EOD activity.

Table 13: Scheduling Batches

Criteria	Remarks
Sequence of Execution of KYC batches	<p>The Processing of the batch is in the following sequence:</p> <ul style="list-style-type: none"> • 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. <p>After the KYC batch ends, the files are generated at EOD. These files can then be used by the Anti Money Laundering (AML) system when the AML batch runs. The feedback processing creates feeds for the account opening system and OFS BD application.</p> <p>Ensure that the feeds are scheduled as part of the data ingestion process in the account opening system and OFS BD application.</p>

5.2.1.13 Listing Holidays in the OFS AAI Administration User Interface

Use the OFS AAI Administration UI to set up and maintain the holiday list for the financial institution. To access the holiday calendar, follow these steps.

1. From the **Administration** menu, select **Security Management**.
2. Select **System Administrator**, and then select **Holiday Maintenance**.

5.2.1.14 Deployment Initiation Processing Based on the Implementation Requirement

After installing KYC, the existing customers are 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 customer risk score.

Deployment Initiation Processing can be done in a single slot or executed in multiple slots (for example, the Number of Customers to be processed) to manage the performance due to volume. The prerequisite for triggering the process execution involves correctly setting up the KYC related parameters using the application parameter configuration UI. The multiple slots are to be decided only if the system requirements cannot meet the volume of data.

NOTE

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

5.2.1.15 Partitioning IPE Tables

Partitioning Inline processing Engine (IPE) tables is done 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_IDNUMBER(22) , N_BATCH_IDNUMBER(22) ,
N_TASK_IDVARCHAR2(100 CHAR) , N_START_TIMETIMESTAMP ,
N_ASSMNT_EVAL_RESULT_ID VARCHAR2(3800 CHAR) , N_ASSMNT_RESULT_ID
NUMBER(22) ,
```

```
N_EVAL_IDNUMBER(22) ,
N_EVAL_VERSIONNUMBER(22) DEFAULT 0 , N_EVAL_SCORENUMBER(22, 2) ,
V_EVAL_FLAGVARCHAR2(100 CHAR) , D_EVAL_TMTIMESTAMP , N_ENTITY_SEQ_ID
VARCHAR2(3500 CHAR) , N_ACTIVITY_BUS_IDNUMBER(22) , N_ASSMT_IDNUMBER(22)
,
V_THRESHOLDVARCHAR2(100 CHAR) ,
V_INFODOMVARCHAR2(100 CHAR) , V_BATCH_RUN_IDVARCHAR2(200 CHAR) ,
V_BATCH_ASSMNT_RES_IDVARCHAR2(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_IDNUMBER(22) , N_BATCH_IDNUMBER(22) ,
N_TASK_IDVARCHAR2(100 CHAR) , N_START_TIMETIMESTAMP , N_ASSMNT_RESULT_ID
NUMBER(22) ,

N_ASSMT_IDNUMBER(22) NOT NULL , N_ASSMNT_VERSIONNUMBER(22) DEFAULT 0 ,
N_ASSMNT_SCORENUMBER(22, 2) , N_ENTITY_SEQ_IDVARCHAR2(3500 CHAR) ,
D_ASSMNT_EXEC_TMTIMESTAMP , V_ERROR_CODEVARCHAR2(10 CHAR) , V_ERROR_MSG
VARCHAR2(500 CHAR) , N_ACTIVITY_BUS_IDNUMBER(22) , V_ASSMNT_EXEC_MODE
VARCHAR2(10 CHAR) , V_ASSMNT_EXEC_RESULTVARCHAR2(10 CHAR) , N_ALERT_ID
NUMBER(22) ,
V_THRESHOLDVARCHAR2(100 CHAR) ,
V_INFODOMVARCHAR2(100 CHAR) , V_BATCH_RUN_IDVARCHAR2(200 CHAR) ,
V_BATCH_ASSMNT_RES_IDVARCHAR2(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)
)
);
```

2. To create and drop partition tasks as part of the Regular Processing Batch, follow these steps:
 - a. Open the IPEKYCRun run in edit mode, click **Selector** drop-down, and select **Job**.
 - b. On the Left Hand Side (LHS) of the pop-up, look for KYC_IPE_TABLE_CREATE_PARTITION under *Processes* and move that component to Right Hand Side (RHS).
 - c. Select the KYC_IPE_TABLE_CREATE_PARTITION component check box in the RHS and move it up to make it the first task.
 - d. On the LHS of the pop-up, look for KYC_IPE_DROP_PARTITION under *Processes* and move that component to RHS.
 - e. Select the KYC_IPE_DROP_PARTITION component check box in the RHS and move it down to make it the last task.
 - f. Click **OK** to close the pop-up.
 - g. Click **Save**.
 - h. Click **Run**.
3. To Create and Drop partition tasks as part of the Deployment Initiation Batch, follow these steps:
 - a. Open the IPEKYCRunDI run in edit mode, click **Selector** drop-down, and select **Job**.
 - b. On the LHS of the pop-up, look for KYC_IPE_TABLE_CREATE_PARTITION under *Processes* and move that component to RHS.
 - c. Select the KYC_IPE_TABLE_CREATE_PARTITION component metadata in the RHS and move it up to make it the first task.
 - d. On the LHS of the pop-up, look for KYC_IPE_DROP_PARTITION under **Processes** and move that component to RHS.
 - e. Select the KYC_IPE_DROP_PARTITION component check box in the RHS and move it down to make it the last task.
 - f. Click **Ok** to close the pop-up.
 - g. Click **Save**.
 - h. Click **Run**.

5.2.1.16 Daily Activities

These are maintenance activities that must be done daily.

Topics:

- [Regular Processing - Account Opening Review](#)
- [Regular Processing- Accelerated Review](#)
- [Regular Processing - Re-review or Periodic](#)
- [Feedback or Application EOD Processing](#)

5.2.1.16.1 Regular Processing - Account Opening Review

All the accounts opened in the previous x days and are in Active status are picked for risk assessment. The accounts opened in the last seven days and activated the previous day are also selected. The lookback period is set to x days, where x is configurable. The account range for the regular processing parameter can be modified from the **Application Parameters** UI page under the **KYC Administration** option by the KYC Administrator.

5.2.1.16.2 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 as the alerts behavior. The accelerated review processing is executed, along with default or account opening review, after the alert generation is complete.

5.2.1.16.3 Regular Processing - Re-review or Periodic

After every review (account opening review, deployment initiation, or accelerated re-review), the next review date is set for the customer based on the risk assessed. Thus, customers are periodically subjected to risk assessment, which is essential as the risk associated with each customer may change over time.

After a case is closed, the customer's next review date is determined by adding the time period (specified for the current risk category of the case) to the processing date in line with the holiday list definition. Re-review processing checks whether the next re-review date falls between the processing date and the number of days specified for the attribute in the `KYC_PERIODIC_REVIEW` parameter.

NOTE

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

5.2.1.16.4 Feedback or Application EOD Processing

During the execution of the regular processing batches, the risk scores at customer levels are sent to 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 customers whose reviews have been completed.

6 Integrating with ECM

Know Your Customer (KYC) is integrated with Enterprise Case Management (ECM) to perform the following tasks:

- Investigate KYC events
- Promote KYC events to cases
- Close the cases
- Edit the KYC risk scores
- Execute the batches
- View the customer dashboard

6.1 Configuring in the ECM UI:

You must make the following configurations in the ECM User Interface (UI). For more information, see the *Managing KYC Configurations* section in the [Oracle Financial Services Enterprise Case Management \(OFS ECM\) Administration and Configuration 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 Username and Password for the Common Gateway Service](#)
- [Updating the Username and Password for the Create JSON Service](#)
- [Updating the Username and Password for the KYC Risk Score UI Service](#)
- [Updating the Username and Password for the JSON To Table Service](#)

6.1.1 Updating the URL for the KYC Close Service

To update the URL, follow these steps:

1. Log in as the ECM Administrator.
2. Navigate to **Case Management Configuration** and select **Manage Common Parameters**.
3. In the **Parameter Category** field, select **Deployment Based**.
4. In the **Parameter Name** field, select **KYC Deployment**.
5. Replace the KYC Rest Service URL with the Behavior Detection (BD) Application URL till the context name is 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.

6.1.2 Updating the KYC Get Overridden Risk Details URL

To update the URL, follow these steps:

1. Log in as the ECM Administrator.
2. Navigate to **Case Management Configuration** and select **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 is in the **Attribute 3** value field. For example: <PROTOCOL:/HOSTNAME:PORT/CONTEXT_NAME>.
6. Click **Save** to update the details in the database.

6.1.3 Updating the BD Application URL for the KYC Customer Dashboard

To update the URL, follow these steps:

1. Log in as the ECM Administrator.
2. Navigate to **Case Management Configuration** and select **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 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 the *Manual Promotion of KYC Risk Assessments to Cases* section in the [Oracle Financial Services Know Your Customer \(OFS KYC\) Risk Assessment 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.

6.1.4 Updating the Username and Password for the Common Gateway Service

To update the username and password, follow these steps:

1. Navigate to **Case Management Configuration** and select **Manage Common Parameters**.
2. In the **Parameter Category** field, select **Deployment Based**.
3. In the **Parameter Name** field, select **Common Gateway Deployment**.
4. 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 username 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** page 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.

6.1.5 Updating the Username and Password for the Create JSON Service

To update the username and password, follow these steps:

1. Log in as the ECM Administrator.
2. Navigate to **Case Management Configuration** and select **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 username 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** page 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 username and password in ECM, follow these steps:

1. Log in 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_bSET V_PARAM_1 =  
'##BASE64ENCODED_ECMADMINUSERNAME:ECMADMINPASSWORD##' where V_APP_API_ID  
='1543401257828';  
  
/ commit  
  
/
```

6.1.6 Updating the Username and Password for the KYC Risk Score UI Service

To update the username and password, follow these steps:

1. Log in as the ECM Administrator.
2. Navigate to **Case Management Configuration** and select **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 username 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** page 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.

6.1.7 Updating the Username and Password for the JSON To Table Service

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

1. Log in 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_bSET V_PARAM_1 =  
'##BASE64ENCODED_KYCADMINUSERNAME:KYCADMINPASSWORD##' where V_APP_API_ID  
='1543401605699';  
  
/ commit  
  
/
```

7 Managing KYC Batches

This chapter provides information on how to manage the different Know Your Customer (KYC) batches.

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.
- A prerequisite for KYC batches is to run ingestion first.

7.1 About KYC Batches

KYC batches are run using the following processes:

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

NOTE

With relation to version 8.0.2.0.0 KYC, the equivalent batches in version 8.0.4.0.0 KYC for deployment initiation processing, regular processing, and end of day processing are `IPEKYCRunDI`, `IPEKYCRun`, and `IPEKYCEODDI`.

7.2 Deployment Initiation Processing

This batch is to be executed only once when the KYC application goes live. All the sections listed under this batch are also part of the Re-review Processing Batch. 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 (OFS) clients can process the deployment workflow based on specific jurisdiction.

- **Customer Type:** OFS clients can also process data based on customer type.
- **Length of Relationship:** OFS clients can also process data based on the length of the customer's relationship which is configurable.

NOTE All the above criteria for processing can be done separately or by combining them. See the `KYC_DEPLOYMNT_INIT_WF` parameter under the application parameter.

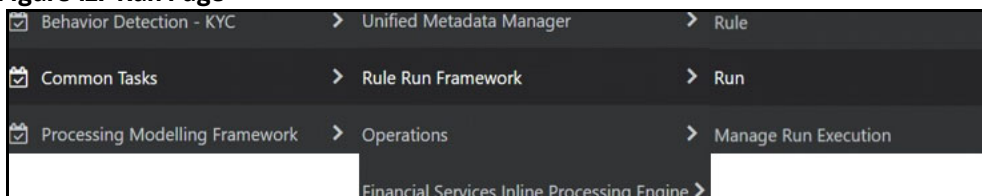
7.2.1 Adding the Beneficial Owner Process to the Deployment Initiation Processing Batch

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

To add the process, follow these steps:

1. Log in to the KYC Application.
2. Click **Common Tasks**. Select **Rule Run Framework** and select **Run**.

Figure 12: Run Page



3. In the **Run** screen, select the `IPEKYCRunDI` code and click **Edit**.
4. Click **Selector** and select **Job**.
5. In the List section, expand **Processes** and select **FCCMSEGMNT** and double-click the `KYC_PopulateBeneficialOwner` task. The task moves to the **Tasks** section.
6. Move the `KYC_PopulateBeneficialOwner` process to below the `KYC_DI_Interested_Party:SD` process and above the `KYC_DI_Watchlist_Scan` process.
7. Click **Ok** to save the changes.
8. Resave the run and trigger a fresh run. This ensures that the changes are saved and displayed.

7.2.2 Setting the Interested party Level

This parameter allows the user to set the customer's level of relationship with the interested parties. Valid values are 1 and 2. By default, it is 1. If the second level relationship is required for the customer, the user can set the value to 2.

Set the interested party level to 2 in the following.

Parameter name: `LVL_IDF_IP`

Table name: `APPLN_INSTALL_PARAMS`.

7.3 End of Day Processing

This topic covers the following sections:

- [Feedback to the OFS BD Framework or Account Opening System](#)

- [Renaming and Transferring Feedback files](#)

7.3.1 Feedback to the OFS BD 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 OFS Behavior Detection (BD) 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 OFS BD 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 as of processing day)
- 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 the Unified Metadata Data Integrator.

7.3.1.1 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](#) shows the CBS feedback.

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

7.3.1.2 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](#) shows the watch list feedback.

Table 15: Watch List Feedback

SL No.	Business Name	Data Type
1	Entity Identifier Type	String
2	Entity Identifier	String

Table 15: Watch List Feedback

SL No.	Business Name	Data Type
3	Watch List Identifier (Referred from Application parameter KYC_WLS_ENTRY_FILE_ID)	String
4	Watch List Entry Description Text	String
5	Risk Assessment Closed Date	Date
6	Next Re-review Date	Date

7.3.1.3 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 OFS BD 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 shows the risk assessment feedback.

Table 16: Risk Assessment Feedback

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

7.3.1.4 Customer - Risk Assessment History

The KYC application captures the history of all the risk assessments created on all the customers within 12 months and would retain for x period of months. Twelve months is configured by default, and the

administrator can update this parameter based on the client's 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 updated value.

7.3.2 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 OFS KYC application is also responsible for sharing Account, Customer, and Watch List feedback to the Oracle Flexcube application at the disposition of the KYC review.

The extract names are incompatible with the OFS BD Framework file naming convention. This utility completes the following activities based on the configurations set for the implementation:

- Moves the files to a different location on the same server.
- Renames the files with the extension defined.
- Maintain a copy of the extract in the history directory with its original name.

The utility covers the following extracts in KYC 2.0:

- `GenCustDetails_ED<YYYYMMDD>`
- `GenWLSFeedback_ED<YYYYMMDD>`

7.4 Regular Processing

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

Topics:

- [Prefilter Rules](#)
- [Risk Assessment Initiation](#)
- [Closure Updates](#)
- [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)

7.4.1 Prefilter Rules

These rules comprise of accelerated re-review, periodic review, and new accounts.

7.4.2 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 matches, 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](#)

7.4.2.1 Rule-based Risk Assessment

Rule-based assessment calculates a risk score based on client configurable rules. The 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 the rule-based assessment, the values for each rule are provided by the Admin user. For more information about providing values to the rule-based assessment, see [Adding Rules for Rule-based Risk Assessments](#).

A customer can fall under one or more rules during the 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 workflow 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 the *Examples of Derivation of Risk Score* appendix in the [Oracle Financial Services Know Your Customer \(OFS KYC\) Risk Assessment Guide](#).

7.4.2.2 Algorithm-based Risk Assessment

The algorithm-based assessment model calculates the risk of customers based on different parameters that 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.

7.4.3 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 current risk score and a 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_Rvwdt1s`), are 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.

7.4.4 Promote to Case

Whenever risk assessments are promoted to cases based on certain criteria, there may be a few risk assessments that are not promoted due to the non-availability of data, system issues, server problems and so on

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.

7.5 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. Log in 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.
5. Click  to expand the page.
6. Select the batch you want to run and click **Fire Run**. The **Fire Run** page is displayed.

Figure 13: Run Page

The screenshot shows a 'Run' page with a search bar at the top right containing 'Search' and 'Reset' buttons. Below the search bar are input fields for 'Code', 'Version' (set to 0), 'Name', 'Active' (set to Yes), 'Folder', and 'Type'. A toolbar below the filters includes buttons for '+ New', 'View', 'Edit', 'Copy', 'Remove', 'Authorize', 'Export', and 'Fire Run'. A table lists three runs:

<input type="checkbox"/>	Code	Name	Type	Folder	Version	Active
<input type="checkbox"/>	IPEKYCEODDI	IPEKYCEODDI	Base Run	FCCMSEGMNT	0	Yes
<input type="checkbox"/>	IPEKYCRun	IPEKYCRun	Base Run	FCCMSEGMNT	0	Yes
<input type="checkbox"/>	IPEKYCRunDI	IPEKYCRunDI:SD	Base Run	FCCMSEGMNT	0	Yes

At the bottom, it shows 'Page 1 of 1 (1-15 of 3 items)' and 'Records Per Page 3'.

7. On the **Fire Run** page, provide the required values.

Figure 14: Run Page Fields

The screenshot shows a 'Run Definition' dialog box with 'OK' and 'Close' buttons at the top right. The fields are:

- Run Definition:** Name: IPEKYCEODDI, Request Type: Single
- Execution Mode:** Batch: Create, Wait: No
- Others:** Parameters: (empty text box), Filters: (empty text box)

8. Click **OK**.

7.6 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 task.

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


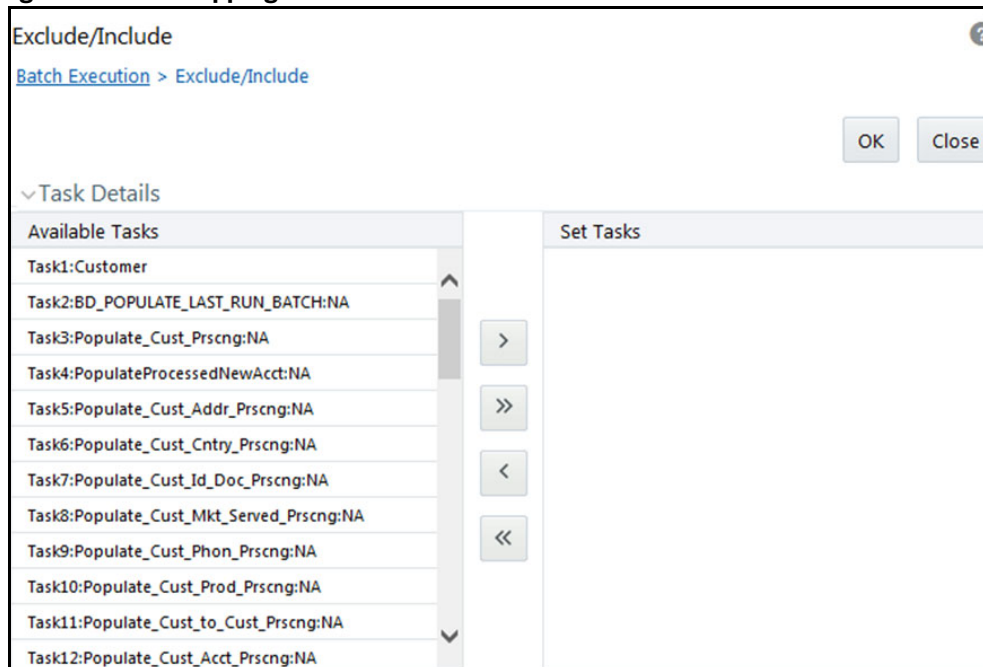
1. Log in as the KYC Administrator. The KYC application home page is displayed.
2. Click **Common Tasks**.
3. Click **Operations**.
4. Click **Batch Execution**. The **Batch Execution** page is displayed.
5. From the **Batch Details** section, select the batch you want to execute.
6. From the **Task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

Figure 15: Task Mapping Window



7. Retain the tasks 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**.

7.7 Scheduling a Batch

Topics:

- [Scheduling a Batch Once](#)
- [Scheduling a Daily Batch](#)
- [Scheduling a Weekly Batch](#)
- [Scheduling a Monthly Batch](#)
- [Scheduling an Adhoc Batch](#)

- [KYC Batch Execution Logs](#)

7.7.1 Scheduling a Batch Once

The following section shows you how to schedule a batch once.

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

1. Log in 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.

Figure 16: Batch Scheduler Page

The screenshot shows the 'Batch Scheduler' interface. At the top, there are search filters for 'Batch ID Like' (with 'INFOFCCM11_' entered), 'Batch Description Like', 'Module' (a dropdown menu), and 'Last Modification Date' (with 'Between' and two date pickers). A 'Refresh' button is on the right. Below the filters, the 'Current Server Time' is displayed as '25/04/2018 15:12:50'. Under the 'Batch Name' section, a table lists three batches with checkboxes for selection. The table has columns for 'Batch ID' and 'Batch Description'. At the bottom, there is a pagination control showing 'Page 1 of 1 (1-3 of 3 items)' and 'Records Per Page 15'. 'Save' and 'Cancel' buttons are at the bottom right.

Batch ID	Batch Description
<input type="checkbox"/> INFOFCCM11_1524479149689	AutoRun_1469444745341_Description
<input type="checkbox"/> INFOFCCM11_1524479356237	AutoRun_1469444745341_Description
<input type="checkbox"/> INFOFCCM11_1524479623424	AutoRun_1469444745341_Description

5. Select a batch 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 scheduled time of the batch by specifying the Start Date and the Run-Time.

Figure 17: Batch Scheduler Filter Fields

The screenshot shows the 'Batch Scheduler' interface. At the top, there are search and filter fields: 'Batch ID Like' (with value 'INFOFCCM11_'), 'Batch Description Like', 'Module' (dropdown), and 'Last Modification Date' (Between two date pickers). A 'Refresh' button is on the right. Below this, the 'Current Server Time' is displayed as '25/04/2018 15:12:50'. A section titled 'Batch Name' contains a table with the following data:

Batch ID	Batch Description
<input checked="" type="checkbox"/> INFOFCCM11_1524479149689	AutoRun_1469444745341_Description
<input type="checkbox"/> INFOFCCM11_1524479356237	AutoRun_1469444745341_Description
<input type="checkbox"/> INFOFCCM11_1524479623424	AutoRun_1469444745341_Description

Below the table, there are pagination controls: 'Page 1 of 1 (1-3 of 3 items)' and 'Records Per Page 15'. The 'Batch Scheduler' section is expanded, showing 'Domain: INFOFCCM11' and 'Batch: INFOFCCM11_1524479149689'. The 'Schedule' section has radio buttons for 'New Schedule' (selected) and 'Existing Schedule'. The 'New Schedule' section includes a 'Schedule Name' field and radio buttons for frequency: 'Once' (selected), 'Daily', 'Weekly', 'Monthly', and 'Adhoc'. The 'Schedule Time' section includes 'Dates' (Start Date and End Date pickers), 'Run Time' (00 Hours, 00 Minutes), and 'Lag' (0 Days). 'Save' and 'Cancel' buttons are at the bottom right.

9. Click **Save**.

7.7.2 Scheduling a Daily Batch

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

1. Log in 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 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 scheduled time of the batch by specifying the Dates, Run Time, and Every information.
9. Click **Save**.

7.7.3 Scheduling a Weekly Batch

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

1. Log in 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 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 scheduled time of the batch by specifying the Dates, Run Time, Every, Working days of the Week information.
9. Click **Save**.

7.7.4 Scheduling a Monthly Batch


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

1. Log in 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 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 scheduled time of the batch by specifying the Dates, Run Time, and Occurrence information.
9. Click **Save**.

7.7.5 Scheduling an Adhoc Batch

To schedule an adhoc batch, follow these steps:

1. Log in 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**.

7.7.6 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 rules. The following sections describe the types of tasks present in the batches.

7.7.6.1 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
```

Table 17 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 Task1 of the batch.

7.7.6.2 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` which is present in the path `<FIC_HOME>/ficdb/log/`

Table 18 shows the shell script transform data.

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.

7.7.6.3 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.

8 KYC Onboarding

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

Topics:

- [Populating Country Data in KDD_CODE_SET_TRNLN Table](#)
- [Configuring the Service Parameters through the User Interface](#)
- [Performing Assessments on Related Applicants](#)
- [Uploading Excel 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](#)

8.1 Populating Country Data in KDD_CODE_SET_TRNLN Table

NOTE Ignore this step if it is already performed during the user administration process.

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;
```

8.2 Configuring the Service Parameters through the User Interface

The following User Interfaces (UI) 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.

8.2.1 Configuring the Onboarding Service Parameters

Use the Configure Service Parameters UI to configure the service URL, service username, 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 username and password must be updated for all services except the AAI Authorization Service and the Initiate OB URL.

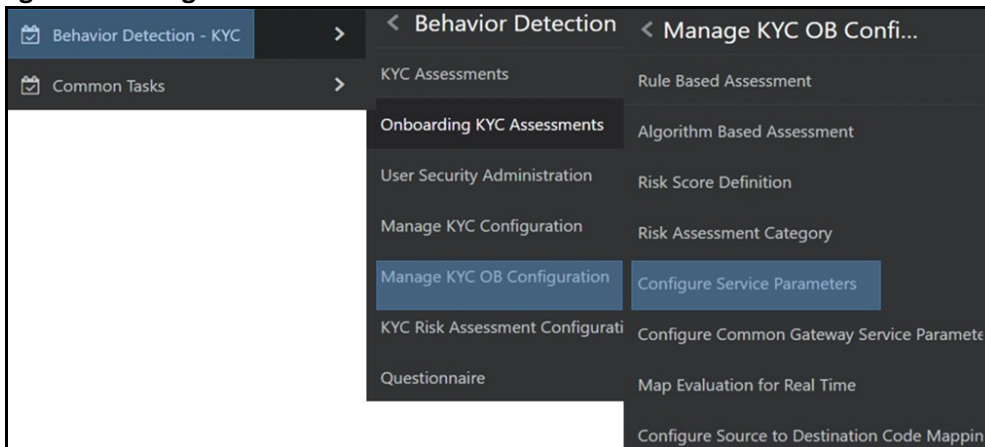
NOTE Ensure that all service usernames and service passwords provided are of valid OFSAA KYC Administrator users.

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

To view the UI, follow these steps:

1. Log in to the KYC application as a KYC Administrator. For more information, see [Getting Started](#).
2. Click **Behavior Detection - KYC**. Select **Manage KYC OB Configuration** and click **Configure Service Parameters**.

Figure 18: Configure Service Parameters Menu



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
- Questionnaire Response Service URL

8.2.1.1 Modifying the Web Service Parameter Details

To modify the parameters for a web service, follow these steps.

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

Figure 19: Web Service Parameters

1. In the **Service Name** field, select the web service for which you want to edit the service parameters.
2. 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.
3. For the **ECM Case Creation URL** and **Questionnaire Response Service URL** services, update the service username in the **Service Username** field with a valid KYC Administrator username.
4. For the **ECM Case Creation URL** and **Questionnaire Response Service URL** services, update the service password in the **Service Password** field with a valid KYC Administrator password.
5. Click **Save** to save the details.

The **Edit Service Parameters** section is applicable only for the Process Modeling Framework service. [Table 19](#) shows the three applicable parameters and their corresponding values.

Table 19: Edit Service Parameters

Parameters	Values
PMF_PROCESS	KYC_ONBOARDING
INFODOM	Installation Specific
LOCALE	en_US

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

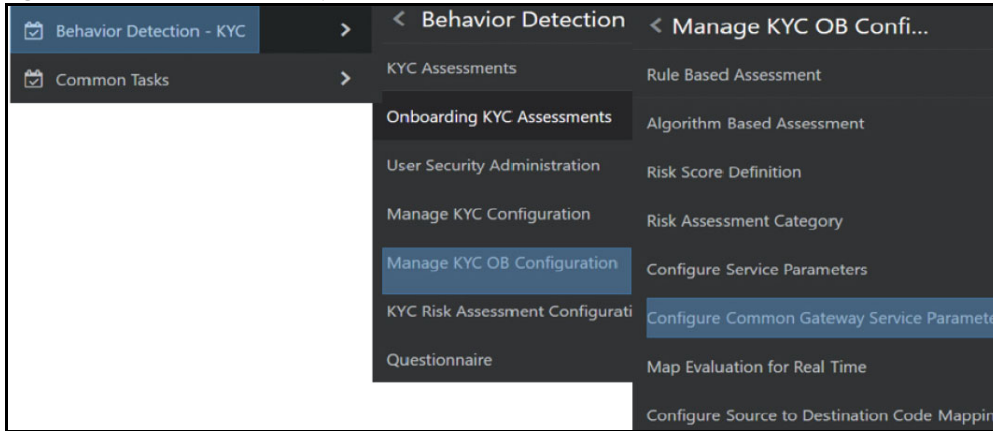
8.2.2 Configuring the Common Gateway Service Parameters

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

To view the UI, follow these steps:

1. Log in to the KYC application as a KYC Administrator. For more information, see [Getting Started](#).
2. Click **Behavior Detection - KYC**. Select **Manage KYC OB Configuration** and click **Configure Common Gateway Service Parameters**.

Figure 20: Common Gateway Service Parameters Menu



The **Configure Common Gateway Service Parameters** UI appears. You can select one of the following services:

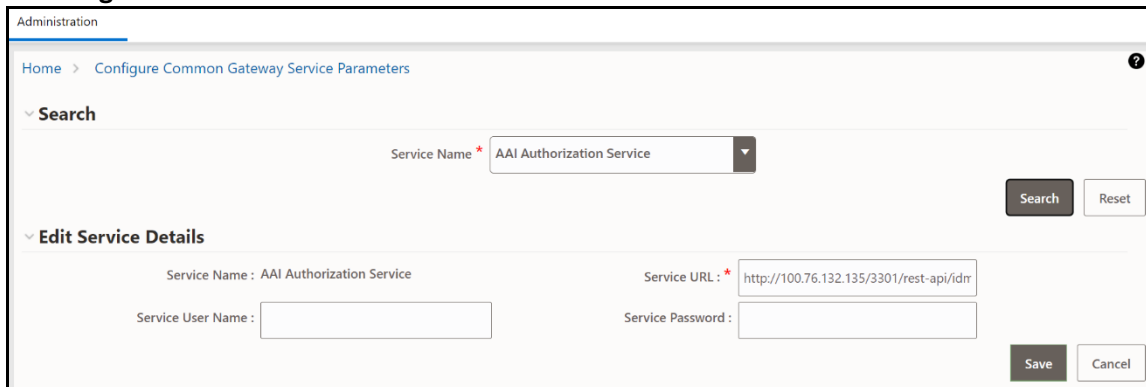
- AAI Authorization Service
- Internal Watch List Service
- Process Modeling Framework

8.2.2.1 Modifying the Web Service Parameter Details

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

To modify the Web Service Parameter Details, follow these steps:

Figure 21: Web Service Parameters



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

8.3 Performing Assessments on Related Applicants

NOTE Ensure that you perform the following configuration for all relationship types before running onboarding jobs.

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

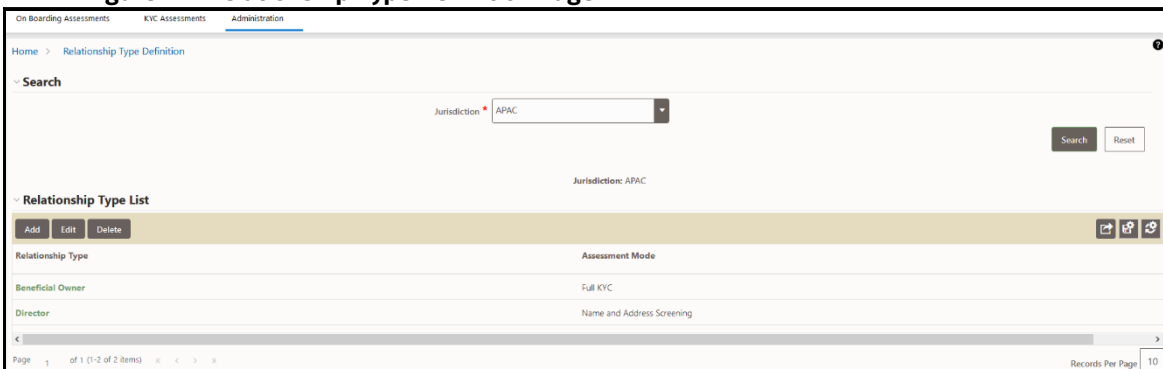
To view the UI, follow these steps:

1. Log in to the KYC application as a KYC Administrator. For more information, see [Getting Started](#).
2. Click **Behavior Detection - KYC**. Select **Manage KYC OB Configuration** and click **Relationship Type Definition**.
3. The **Relationship Type Definition** UI is displayed. In the **Search** section, select the jurisdiction.
4. Based on the jurisdiction selected, the **Relationship Type List** displays all configured relationship types and their respective assessment modes.

NOTE Assessment modes are configured in the `kdd_code_set_trnln` table, and `code_set` is the `KYCAssessmentMode`. `FULL_KYC` and `NAME_ADDR` are the code values defined for the code set.

- For Primary applicants, the default assessment mode is always `FULL_KYC`.
- For Related applicants, the default assessment mode is `NAME_ADDR` provided no configuration is defined for the relationship type in the Relationship Type Definition UI.

Figure 22: Relationship Type Definition Page



To add a new **Relationship Type**, follow these steps:

1. Click **Add** to add a new relationship type.
2. Provide the **Relationship Type** and **Assessment Mode** and click **Save**.

To change the **Assessment Mode** of a **Relationship Type**, follow these steps.

1. Click **Edit** to change the assessment mode.
2. Provide the new **Assessment Mode** and click **Save**.

To remove the **Relationship Type**, follow these steps:

1. Click **Delete** and click **Yes** in the dialog box which appears.

8.4 Uploading Excel Data

Excel upload is a process wherein the data for a particular table is uploaded into 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, follow these steps:

1. Log in to the KYC application. For more information, see [Getting Started](#).
2. Click **Common Tasks**. Select **Unified Metadata Manager**, click **Data Entry Forms and Queries**.
3. Click **Bulk Upload** and select **Excel Upload (Atomic)**.
4. Click **Excel Upload** to select the Excel sheet that you want to upload.

Figure 23: Excel Upload

5. In the **Excel File to Upload** section, click **Choose File** to select the file 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.

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

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

8.5 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.

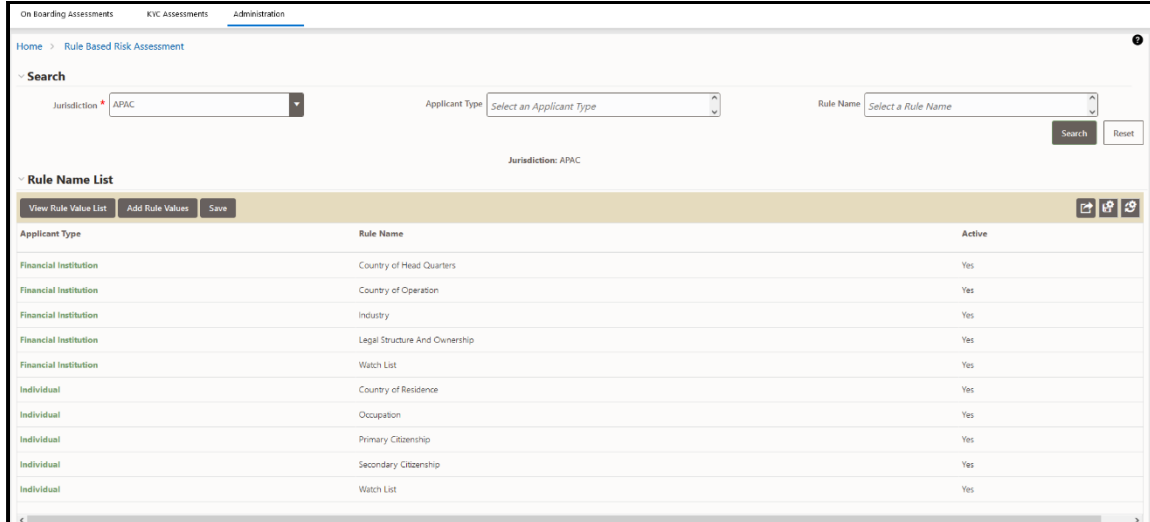
To view the UI, follow these steps:

1. Log in to the KYC application. For more information, see [Getting Started](#).
2. Click **Behavior Detection - KYC**. Select **Manage KYC OB Configuration** and click **Rule-Based Assessment**.
3. The Rule-based risk assessment UI appears with the **Search** section displayed.

Figure 24: Search Fields

4. 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.

Figure 25: Rule Name List



8.5.1 Adding a Rule

To add a rule, follow these steps:

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

8.5.2 Enabling or Disabling the Risk Parameter during Risk Assessments

To enable or disable the risk parameter, follow these steps:

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**.

8.6 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, follow these steps:

1. Log in to the KYC application. For more information, see [Getting Started](#).
2. Click **Behavior Detection - KYC**. Select **Manage KYC OB Configuration** and click **Algorithm Based Assessment**.

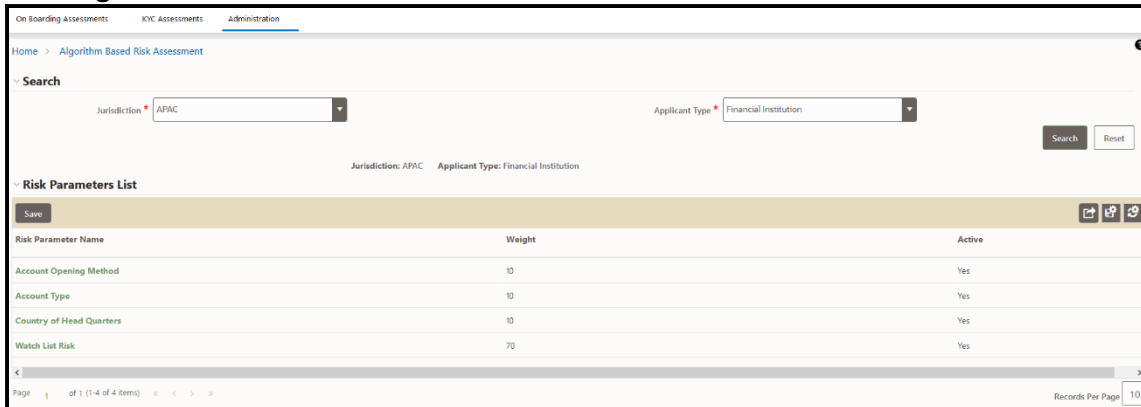
The Algorithm-based risk assessment UI appears with the Search section displayed.

Figure 26: Search Fields



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

Figure 27: Risk Parameters List



8.6.1 Modifying the Weight of the Risk Parameter

To modify the weight, follow these steps:

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.

8.6.2 Enabling or Disabling the Risk Parameter during Risk Assessments

To enable or disable the risk parameter, follows these steps:

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**.

8.7 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, follow these steps:

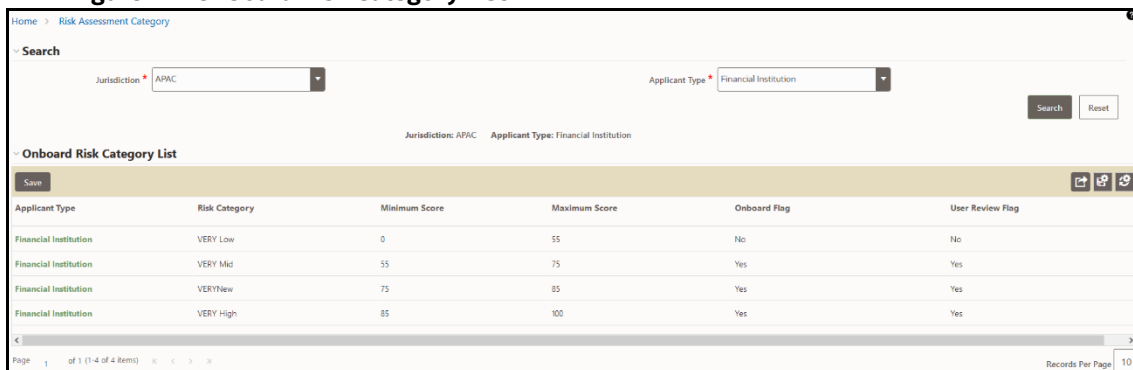
1. Log in to the KYC application. For more information, see [Getting Started](#).
2. Click **Behavior Detection - KYC**. Select **Manage KYC OB Configuration** and click **Risk Assessment Category**.
3. The Risk Assessment Category UI appears with the Search section displayed.

Figure 28: Search Fields



Select the jurisdiction and applicant type of risk assessment.

Figure 29: Onboard Risk Category List



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

8.7.1 Modifying the Risk Scores

To modify the minimum and maximum risk scores, follow these steps:

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 so 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.

8.7.1.1 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.

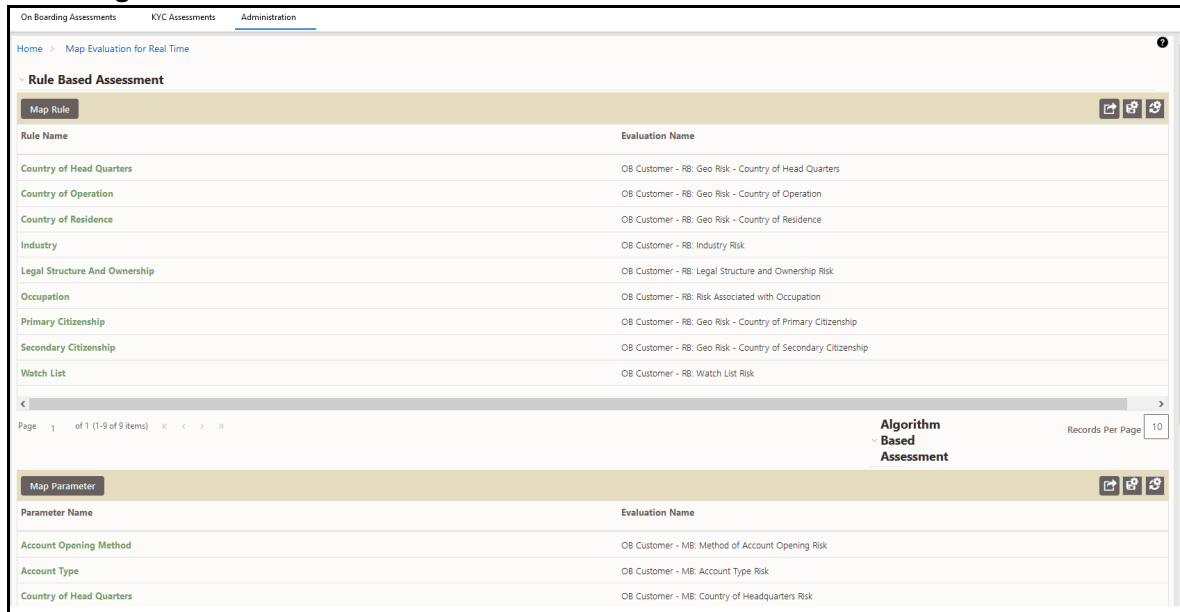
To view the UI, follow these steps:

1. Log in to the KYC application. For more information, see [Getting Started](#).

2. Click **Behavior Detection - KYC**. Select **Manage KYC OB Configuration** and click **Map Evaluation for Real Time**.

The rule names and associated evaluations for Algorithm-based and Risk-based assessments appear.

Figure 30: Rule Based Assessment Section



8.7.2 Mapping Rules to Evaluations

To map the rules to their respective evaluation names, follow these steps:

1. On the Rule Based Assessment page, click **Map Rule**. This action displays the Map Rule to Evaluation.

Figure 31: Map Rule to Evaluation

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

8.7.3 Mapping Parameters to Evaluations

To map the parameters to their respective evaluation names:

Figure 32: Map Parameter to Evaluation

1. Click **Map Parameter**.

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

8.7.3.1 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, follow these steps:

1. Log in to the KYC application. For more information, see [Getting Started](#).
2. Click **Behavior Detection - KYC**. Select **Manage KYC OB Configuration** and click **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_trnl` 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 applicant types appear only after you select a model type.
- The Parameter/Rule names appear only after you select an applicant type.

Figure 33: Search Fields

The screenshot shows a search interface for risk scores. At the top, there are four dropdown menus: Jurisdiction (APAC), Applicant Type (Individual), Risk Scoring Model Type (Algorithm Based Assessment), and Parameter/Rule Name (Account Opening Method). An 'Auto-Populate' button is on the right. Below the search fields, the current search criteria are displayed: Jurisdiction: APAC, Model Type: Algorithm Based Assessment. A table titled 'Risk Score for Parameter/Rule Value' contains the following data:

Applicant Type	Parameter/Rule Name	Parameter Value	Risk Score
Individual	Account Opening Method	In Person	0
Individual	Account Opening Method	Legal Representative	0
Individual	Account Opening Method	Online	3
Individual	Account Opening Method	Others	0
Individual	Account Opening Method	Phone	0

At the bottom, there is a pagination bar showing 'Page 1 of 1 (1-5 of 5 items)' and a 'Records Per Page' dropdown set to 10.

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 to all jurisdictions, risk models, and applicant types.
- In case no new rules or parameters have been added, the following message is displayed when you click Auto-Populate.

Auto Populate was not performed as there are no new risk parameter values

8.7.4 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, follow these steps:

1. Click **Copy**.

Figure 34: Copy Risk Scores

The screenshot shows a 'Copy Risk Scores' dialog box. It contains the following fields: Model Type (Algorithm Based Assessment), Applicant Type (Individual), Parameter Name (Account Opening Method), Source Jurisdiction (APAC), and Destination Jurisdiction (a dropdown menu with the text 'Select Jurisdictions'). There are 'Save' and 'Cancel' buttons at the bottom right.

2. Select one or more jurisdictions. Only jurisdictions with the same model type, applicant type, and parameter name as the source jurisdiction are shown.
3. Click **Save**.

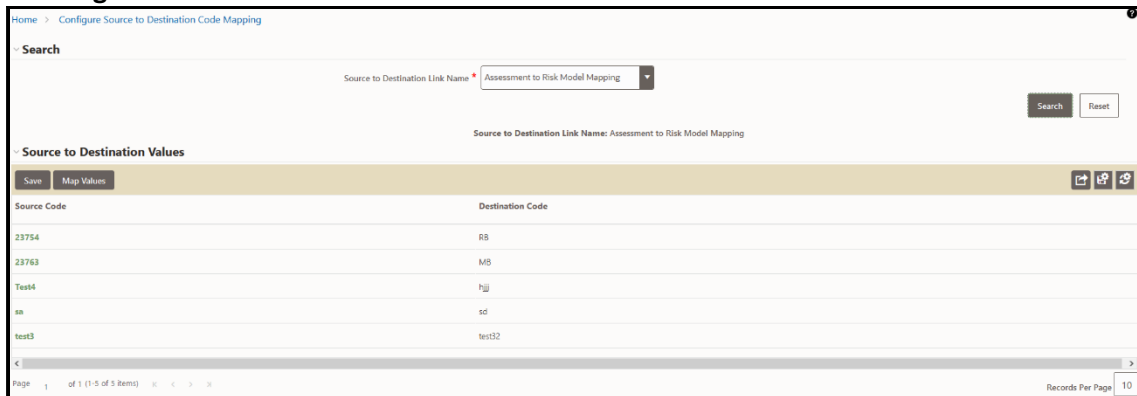
8.8 Modifying and Adding the Mapping Codes within KYC

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**. Select **Manage KYC OB Configuration** and click **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**.

Figure 35: Search Fields



The **Source Code** and **Destination Code** values appear in a tabular format.

8.8.1 Downloading the Code Values

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

8.8.1.1 Modifying the Code Values

To modify the code values, follow these steps:

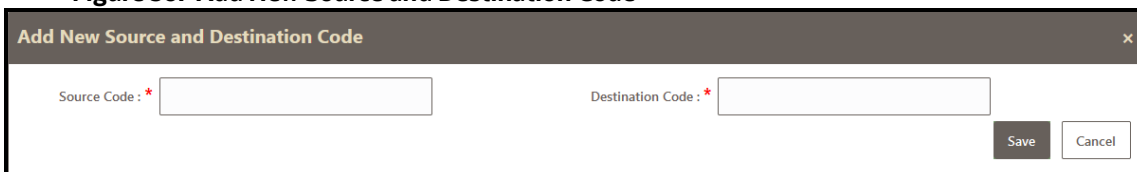
1. Double-click the code value and provide the new code value.
2. Click **Save**.
3. To refresh the UI, click **Reset**.

8.8.2 Adding New Code Values

To add new code values, follow these steps:

1. Click **Map Values**.

Figure 36: Add New Source and Destination Code



2. Add a **Source code** and a **Destination code**.
3. Click **Save**.

9 Adding Risk Parameters and Rules (KYC Batch)

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

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](#)

9.1 Adding Risk Parameters for Algorithm-based Risk Assessments

Before you add risk parameters, you must perform the following actions:

- Prepare the metadata in the application. For more information, see [Maintenance Activities and Configuring Setup Parameters \(KYC Batch\)](#).
- Update the sequence ID for Inline Processing Engine (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 the [Oracle Financial Services Behavior Detection \(OFS BD\) Installation Guide](#).

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


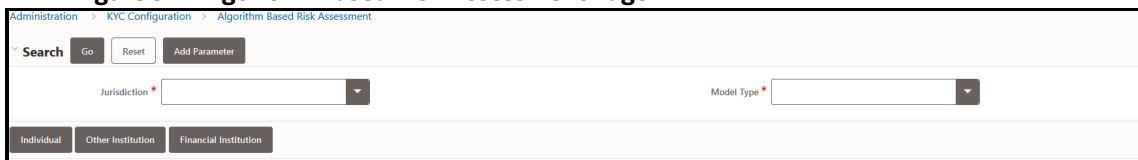
1. Navigate to the OFSAA login page.
2. On the Know Your Customer (KYC) home page, click **Behavior Detection - KYC**.
3. Click the **KYC Risk Assessment Configuration**.
4. Click  to expand the page.
5. Click **Algorithm Based Risk Assessment**. The **Algorithm Based Risk Assessment** page appears.

Figure 37: Algorithm Based Risk Assessment Page



6. To add a new parameter, click **Add Parameter**. The **Add New Parameter** dialog box displays.

Figure 38: Add New Parameter Fields

Table 20 describes the fields.

Table 20: Add New Parameter Fields

Field Name	Description
Jurisdiction	Select the jurisdiction that the parameter belongs to. All the jurisdictions that are available in the <code>kdd_jrsdcn</code> table display.
Model Type	Select the model type as Algorithm-based Risk Assessment .
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 <code>kdd_code_set_trnl</code> 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.
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 Reassessment	Select Yes to reassess 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 <code>APPLN_REREVIEW_PARAMS</code> .
Comments	Enter any comments related to the parameter.

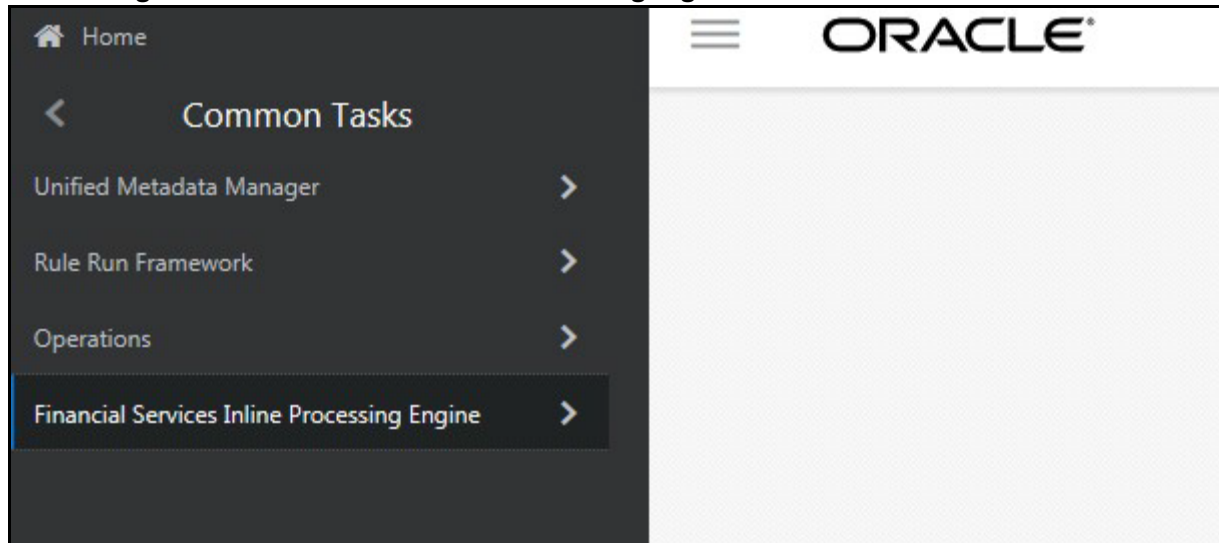
- To save the parameter, click **Save**.

NOTE

- To close the dialog box, click Cancel. This refreshes the screen with the new parameter.
- 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.

- On the KYC home page, click **Financial Services Inline Processing Engine** in the **Common Tasks** tab.

Figure 39: Financial Services Inline Processing Engine Menu



- Click **Inline Processing**. The **Inline Processing** page is displayed.

The following window shows the **Profiles** menu. Profiles are an aggregation of information. Profiles can be based on different grouping entities (For example, account and customer) and can be filtered to only look at specific types of transactions. Profiles can also be based on time (last three months) or activity counts (last 100 transactions). For more information on Profiles, see the *Managing Profiles* chapter in the [Oracle Financial Services Inline Processing Engine \(OFS IPE\) User Guide](#).

Figure 40: Inline Processing Menu

Association and Configuration Expressions Post Processing Actions Profiles Virtual Profiles Evaluations Assessments

Home >> Profiles

Search Go Reset

Profile Name Activity Processing Segment Status

Profiles (6) Add Delete

Profile Name	Activity	Processing Segment	Status	Updated By	Updated On	History
Count Of Suspicious Account Alert	Customer	Pre-filtering of Customers	VALID	KYCADMN	--	
Count Of Suspicious Customer Alert	Customer	Pre-filtering of Customers	VALID	KYCADMN	--	
Count of Frequent Account Alert	Customer	Pre-filtering of Customers	VALID	KYCADMN	--	
Count of Frequent Customer Alert	Customer	Pre-filtering of Customers	VALID	KYCADMN	--	
Count of High Score Account Alert	Customer	Pre-filtering of Customers	VALID	KYCADMN	--	
Count of High Score Customer Alert	Customer	Pre-filtering of Customers	VALID	KYCADMN	--	

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

To add a business entity, follow these steps:

- a. Click the **Business Entities** sub-menu in the **Association and Configuration** menu.
- b. Select the Entity Name as PARAM_RISK_SCORE_JRSDN.

Figure 41: Association and Configuration Menu

The screenshot shows the 'Association and Configuration' menu with the following structure:

- Navigation tabs: Association and Configuration, Expressions, Post Processing Actions, Profiles, Virtual Profiles, Evaluations, Assessments.
- Breadcrumbs: Home >> Association and Configuration >> Business Entities
- Buttons: Choose Entity, Import Entity, Delete
- Entity Name*: PARAM_RISK_SCORE_IRSDN
- Business Entities (18) buttons: Add, Edit, Delete, Synchronize
- Table with columns: Name, Processing Segments, Score Attribute

	Name	Processing Segments	Score Attribute
<input type="checkbox"/>	Account Type Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/>	Citizenship Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/>	Corporate Age Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/>	Country of Head Quarters Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/>	Country of Operations Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/>	Country of Residence Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/>	Country of Taxation Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/>	Default Risk Score	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/>	Industry Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/>	Legal Structure Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--

- 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.

Figure 42: Parameter Fields

The screenshot shows the 'Parameter Fields' form with the following fields:

- Name*: Country of Birth
- Processing Segment*: Algorithm Based Risk Model
- Set Score Attribute: N_RISK_SCORE
- Buttons: Add, Cancel

- e. Click **Add**. The new parameter is added to the list of Business Entities on the **Business Entities** page.
11. 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:

- f. On the **Inline Datasets** page, click **Add**.
- g. Enter a name for the inline dataset.
- h. In the **Start Table** field, select **Algorithm Based Risk Scoring**.
- i. In the **End Table** field, select **Country of Head Quarters Value**.

Figure 43: Inline Datasets Page

Inline Dataset Details			
Inline Dataset Name*		Rule Score - Country of Birth	
Start Table*	Algorithm Based Risk Scoring	End Table*	Country of Head Quarters Value
Inline Dataset Condition Add Delete			
Start	Operator	End	
<input type="checkbox"/> Attribute	V_RISK_PARAM_CODE	=	Attribute V_PARAM_RULE_CODE
<input type="checkbox"/> Attribute	V_JRSDCN_CD	=	Attribute V_JRSDCN_CD
		Save	Cancel

- j. Click **Add**.
- k. Select the values for the dataset condition as shown in the figure.
- l. Click **Save**. The new dataset is added to the list of Inline Datasets on the **Inline Datasets** page.

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

12. 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.
13. To add a traversal path, follow these steps:
 - a. Click the **Traversal Paths** sub-menu in the **Association and Configuration** menu.
 - b. On 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**.

Figure 44: Traversal Paths Page

Traversal Path Details			
Traversal Path Name		Customer Processing - Account Processing	
Start Table	Customer Processing	End Table	Account Processing
Traversal Path Flow Add Delete			
Source Entity	Destination Entity		Sequence ID
<input type="checkbox"/> Customer Processing	Algorithm Based Risk Scoring		1
<input type="checkbox"/> Customer Processing	Customer Account Processing		2
<input type="checkbox"/> Customer Account Processing	Account Processing		3
		Save	Cancel

- 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 on the **Traversal Paths** page. For more information on the datasets and traversal paths used in KYC, see the *Association*

and Configuration chapter in the [Oracle Financial Services Inline Processing Engine \(OFS IPE\) User Guide](#).

NOTE

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

14. 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 the Method of Account Opening.

To add an expression, follow these steps:

- a. Click the **Expressions** menu.
- b. On the **Expressions** page, click **Add**.
- c. For the first expression, enter a name for the expression and select the values as shown in the following figure.

Figure 45: Expressions Page – First Expression

The screenshot shows the 'Expressions Page' configuration for the first expression. The 'Expression Name' is 'Country of birth' and the 'Activity' is 'Customer Processing'. The 'Processing Segment' is 'Algorithm Based Risk Model'. The 'Variable' section shows the 'Operator' dropdown, 'Business Entity' set to 'Algorithm Based Risk Scoring', and 'Business Attribute' set to 'V_RISK_PARAM_CODE'. The 'Create New Group' radio button is selected.

- 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 following figure.

Figure 46: Expressions Page – Second Expression

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

Group	Order	Operator	Business Property (Business Entity, Business Attribute)	Function	Function Parameters
-------	-------	----------	---------------------------------------------------------	----------	---------------------

Variable Save Cancel

Operator

Business Entity* Method of Account Opening Value

Business Attribute* N_RISK_SCORE

Add to Current Group Create New Group

Submit Close

- 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 that holds the risk score of the parameter, and the other variable is the column that 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.

Figure 47: Expressions Page – Displayed Values

Expression Name* Method Of Account Opening - Weighed Score Activity* Customer Processing

Processing Segment*
 Algorithm Based Risk Model
 Pre-filtering of Customers
 Real Time Account On-Boarding
 Rule Based Risk Assessment Model

Status VALID

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

Group	Order	Operator	Business Property (Business Entity, Business Attribute)	Function	Function Parameter
1	1		Method of Account Opening Value : N_RISK_SCORE	Replace Null	Default Risk Score for Missing Data
2	1	*	Algorithm Based Risk Scoring : N_RISK_PARAM_WEIGHT		

Variable Save Cancel

Operator
 Business Entity*
 Business Attribute*

Add to Current Group Create New Group

- 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 on the **Expressions** page.
15. 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. On the Evaluations page, click **Add**.

Figure 48: Evaluations Page

Home >> Evaluations

Search Go

Evaluation Name Activity Processing Segment

Status

Evaluations (93)

	Evaluation Name	Score	Activity	Processing Segment	Status	Updated By	Updated On	History
<input type="checkbox"/>	Change In Risk Model - Account Type	10	Customer	Pre-filtering of Customer	VALID	KYCADMN	09/13/2017 10:27:23	
<input type="checkbox"/>	Change In Risk Model - Corporate Age	10	Customer	Pre-filtering of Customer	VALID	KYCADMN	09/13/2017 10:27:25	
<input type="checkbox"/>	Change In Risk Model - Country Of Head Quarters	10	Customer	Pre-filtering of Customer	VALID	KYCADMN	09/13/2017 10:27:25	
<input type="checkbox"/>	Change In Risk Model - Country Of Residence	10	Customer	Pre-filtering of Customer	VALID	KYCADMN	09/13/2017 10:27:25	
<input type="checkbox"/>	Change In Risk Model - Country of Operation	10	Customer	Pre-filtering of Customer	VALID	KYCADMN	09/13/2017 10:27:25	
<input type="checkbox"/>	Change In Risk Model - Legal Structure And Owns	10	Customer	Pre-filtering of Customer	VALID	KYCADMN	09/13/2017 10:27:25	
<input type="checkbox"/>	Change In Risk Model - Length Of Relationship	10	Customer	Pre-filtering of Customer	VALID	KYCADMN	09/13/2017 10:27:25	

- 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.

Figure 49: Evaluation Details

Evaluation Details

Name* Activity* Processing Segment*

Join Type* Inner Left

Filters (0)

Evaluation Scoring

Score Type* Fixed Lookup Expression

Associated Assessments (0)

Associated Profiles (0)

Associated Virtual Profiles (0)

Change Description

- 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**.

Figure 50: Filter Details – First Expression

Filter Details

Filter Name*

Source Expression* Operator*

Comparator Type* Expression Literal Value

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**.

Figure 51: Filter Details – Second Expression

The screenshot shows a 'Filter Details' window with the following fields:

- Filter Name***: Parameter Code
- Source Expression***: Algorithm Based Risk Scoring - Parameter (dropdown)
- Operator***: = (dropdown)
- Literal Value**: "MB_CCR_MAO_RSK" (text field with a clear button)
- Comparator Type***: Literal Value, Expression

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 that holds the risk parameter data in the Highlights section. This is required to get the actual value for every customer. For information on how to create a highlight, see [APPENDIX-B Creating Highlights](#).
 - j. Click **Save**.
16. Map the evaluation of the existing assessment of the added parameter. To do this, run the following insert script:

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

Table 21 shows the expected values for the above script.

Table 21: Expected Values

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

17. Click **Save**.

9.2 Adding Rules for Rule-based Risk Assessments

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


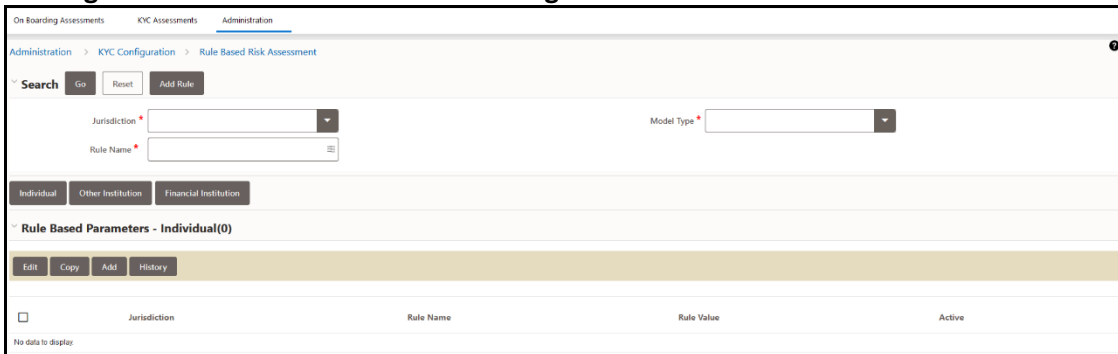
1. Navigate to the OFSAA login page.
2. On the KYC home page, click **Behavior Detection - KYC**.
3. Click **KYC Risk Assessment Configuration**.
4. Click  to expand the page.
5. Click **Rule Based Risk Assessment**. The **Rule Based Risk Assessment** page appears.

Figure 52: Rule Based Risk Assessment Page



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

Figure 53: Add a New Rule

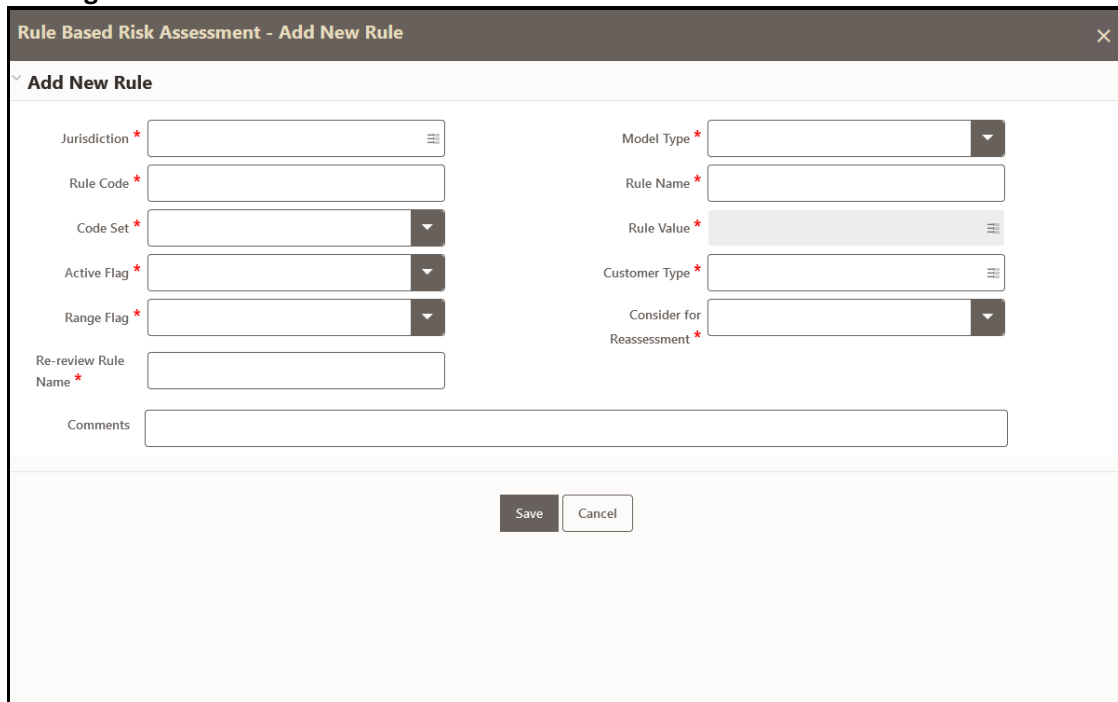


Table 22 describes the rule fields.

Table 22: Add New Rule Fields

Field Name	Description
Jurisdiction	Select the jurisdiction that the parameter belongs to. All the jurisdictions that are available in the <code>kdd_jrsdcn</code> table display.
Model Type	Select the model type as Algorithm-based Risk Assessment .
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 <code>kdd_code_set_trnl</code> 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 the relationship for the current assessment. Select No to disable the length of the 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 <code>APPLN_REREVIEW_PARAMS</code> .
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.

- 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 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.

- To define a rule, follow these steps:
 - 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:
 - Click the Business Entities sub-menu in the Association and Configuration menu.

- c. Select the Entity Name as PARAM_RISK_SCORE_JRSDN.

Figure 54: Association and Configuration Menu

The screenshot shows the 'Association and Configuration' menu with the 'Business Entities' sub-menu selected. The 'Entity Name' dropdown is set to 'PARAM_RISK_SCORE_JRSDN'. Below, a table lists various business entities with their processing segments and score attributes.

Name	Processing Segments	Score Attribute
<input type="checkbox"/> Account Type Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/> Citizenship Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/> Corporate Age Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/> Country of Head Quarters Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/> Country of Operations Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/> Country of Residence Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/> Country of Taxation Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/> Default Risk Score	Algorithm Based Risk Model,Real Time Account On-Boarding	--
<input type="checkbox"/> Industry Value	Algorithm Based Risk Model,Real Time Account On-Boarding	--

10. Click **Add**.
11. 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.

Figure 55: Filter Fields

The screenshot shows the 'Filter Fields' dialog box. The 'Name' field contains 'Country of Birth', the 'Processing Segment' dropdown is set to 'Rule Based Risk Assessment Model', and the 'Set Score Attribute' dropdown is set to 'N_RISK_SCORE'. There are 'Add' and 'Cancel' buttons at the bottom.

12. Click **Add**. The new parameter is added to the list of Business Entities on the Business Entities page.
13. 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. On 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 the Country of Birth. This is the new business entity that you have added.

Figure 56: Inline Dataset Fields

The screenshot shows the 'Inline Dataset Details' form. The 'Inline Dataset Name' field contains 'Rule Score-Country of Birth'. The 'Start Table' dropdown is set to 'Rule Based Risk Assessment' and the 'End Table' dropdown is set to 'Country of Birth'. Under the 'Inline Dataset Condition' section, there are two rows of conditions. The first row has 'Attribute' dropdown set to 'V_RISK_PARAM_CODE', an '=' operator, and another 'Attribute' dropdown set to 'V_PARAM_RULE_CODE'. The second row has 'Attribute' dropdown set to 'V_JRSDCN_CD', an '=' operator, and another 'Attribute' dropdown set to 'V_JRSDCN_CD'. At the bottom are 'Save' and 'Cancel' buttons.

- 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 on the Inline Datasets page.

NOTE To view the results of the newly added values, use **Search**.

14. 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. On the Traversal Paths page, click **Add**.

Figure 57: Traversal Paths Fields

The screenshot shows the 'Traversal Paths' page. At the top, there are navigation tabs: 'Association and Configuration', 'Expressions', 'Post Processing Actions', 'Profiles', 'Virtual Profiles', 'Evaluations', and 'Assessments'. Below the tabs, there is a search bar with 'Search', 'Go', and 'Reset' buttons. The main form has 'Traversal Path Name' and 'End Table' text boxes, and 'Start Table' and 'End Table' dropdown menus. Below the form is a table with 73 entries. The table has columns: 'Traversal Path Name', 'Start Table', 'End Table', and 'Traversal Path Flow'. The first few rows are:

Traversal Path Name	Start Table	End Table	Traversal Path Flow
Customer - Accelerated Re-review Param	Customer	Accelerated Review Parameter	Customer : Accelerated Review Parameter
Customer - Account	Customer	Account	Customer : Customer To Account , Customer To Account : Account
Customer - Application Parameters	Customer	Application Parameters	Customer : Application Parameters
Customer - Change Log	Customer	CHG_LOG	Customer : CHG_LOG
Customer - Customer Address	Customer	CUST_ADDR	Customer : CUST_ADDR

- c. Enter a name for the traversal path.
- d. In the **Start Table** field, select **Customer Processing**.
- e. In the **End Table** field, select **Rule-Based Risk Assessment**.

Figure 58: Traversal Path Details

Source Entity	Destination Entity	Sequence ID
Customer Processing	Rule Based Risk Assessment	1
Customer Processing	Customer Account Processing	2
Customer Account Processing	Account Processing	3

- 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 on the Traversal Paths page.
15. 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 the Method of Account Opening.

To add an expression, follow these steps:

- a. Click the Expressions menu.
- b. On the Expressions page, click **Add**.

Figure 59: Expressions Fields

Expression Name	Description	Status	Activity	Processing Segment
Accelerated Re review Parameter	(Accelerated Review Parameter:F_ENABLE)	VALID	Customer	Pre-filtering...
Accelerated Re review Parameter	(Accelerated Review Parameter:N_RULE_ID)	VALID	Customer	Pre-filtering...
Accelerated Re review Parameter	(Accelerated Review Parameter:N_ALERT_SCORE)	VALID	Customer	Pre-filtering...
Accelerated Rereview Params - C	(Accelerated Review Parameter:N_COUNT_OF_ALERTS)	VALID	Customer	Pre-filtering...
Account - Account Open Date	(Account:ACCT_OPEN_DT)	VALID	Customer	Pre-filtering...
Account - Account Status Code	(Account:ACCT_STAT_CD)	VALID	Customer	Pre-filtering...

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

Figure 60: Expressions Page – First Expression

- d. To add a variable for the first expression, click **Add**.
- e. Select the business entity and the business attribute where the value of the new parameter resides.
- f. Click **Save**. The variable is displayed.
- g. For the second expression, enter a name for the expression and select the values as shown in the following figure.

Figure 61: Expressions Page – Second Expression

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

Figure 62: Expressions Page – Displayed Values

The screenshot shows the 'Expressions Page' with the following configuration:

- Expression Name***: Method Of Account Opening - Weighed Score
- Activity***: Customer Processing
- Processing Segment***: A dropdown menu is open, showing options: Algorithm Based Risk Model, Pre-filtering of Customers, Real Time Account On-Boarding, and Rule Based Risk Assessment Model (highlighted).
- Status**: VALID

Below the configuration, there are buttons for **Variables**, **Add**, **Delete**, **Apply Function To Group**, **Remove Function From Group**, and **Apply Function to Expression**.

Group	Order	Operator	Business Property (Business Entity, Business Attribute)	Function	Function Parameter
<input type="radio"/> 1	1		Method of Account Opening Value : N_RISK_SCORE		
<input type="radio"/> 2	1	*	Algorithm Based Risk Scoring : N_RISK_PARAM_WEIGHT		

Below the table, there is a **Variable** section with a **Save** button and a **Cancel** button. The variable configuration includes:

- Operator**: A dropdown menu.
- Business Entity***: A dropdown menu.
- Business Attribute***: A dropdown menu.

At the bottom, there are two radio buttons: **Add to Current Group** and **Create New Group**.

- 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**.

Figure 63: Expression Function

Expression Name* Method Of Account Opening - Weighed Score Activity* Customer Processing

Processing Segment*
 Algorithm Based Risk Model
 Pre-filtering of Customers
 Real Time Account On-Boarding
 Rule Based Risk Assessment Model

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

Group	Order	Operator	Business Property (Business Entity, Business Attribute)	Function	Function Parameter
<input checked="" type="radio"/> 1	1		Method of Account Opening Value : N_RISK_SCORE	Replace Null	Default Risk Score for Missing Data
<input type="radio"/> 2	1	*	Rule Based Risk Assessment : N_RISK_PARAM_WEIGHT		

Variable

Operator *
 Business Entity* Rule Based Risk Assessment
 Business Attribute* N_RISK_PARAM_WEIGHT
 Add to Current Group Create New Group

Apply Function To Group

Select Function Replace Null

Literal value to be applied
 Literal Value Expression
 Default Risk Score for Missing Data

- 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**.

Figure 64: Literal Value Function

Expression Name* Method Of Account Opening - Weighed Score Activity* Customer Processing

Processing Segment *

- Algorithm Based Risk Model
- Pre-filtering of Customers
- Real Time Account On-Boarding
- Rule Based Risk Assessment Model**

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

Group	Order	Operator	Business Property (Business Entity, Business Attribute)	Function	Function Parameter
<input checked="" type="radio"/> 1	1		Method of Account Opening Value : N_RISK_SCORE	Replace Null	Default Risk Score for Missing Data
<input type="radio"/> 2	1	*	Rule Based Risk Assessment : N_RISK_PARAM_WEIGHT		

Variable Save Cancel

Operator * Business Entity* Rule Based Risk Assessment Business Attribute* N_RISK_PARAM_WEIGHT

Add to Current Group Create New Group

Apply Function To Group Save Cancel

Select Function Divide

Denominator

Literal Value Expression

100

Submit Close

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

16. 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:

- Click the **Evaluations** menu.
- On the Evaluations page, click **Add**.
- Enter a name for the evaluation.
- 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.

Figure 65: Evaluation Details

- 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**.

Figure 66: Filter Details – First Filter

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

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

Figure 67: Filter Details – First Filter

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

- h. Select the expression that you have created for the calculation of the risk score.
 - i. Select the expression that holds the risk parameter data in the Highlights section. This is required to get the actual value for every customer.
 - j. Click **Save**.
17. Map the evaluation to the existing assessment of the added parameter. To do this, run the following insert script:

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

Table 23 shows the expected values for the above script.

Table 23: Expected Values

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

18. Click **Save**.

9.2.1 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 creating a new one.

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.
2. Add three filters to the evaluation:
 - a. 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.
 - b. 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.
 - c. 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.
3. Map the new evaluation to the Change in Risk Model Assessment.

9.3 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. On 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.

Figure 68: Administration Menu



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

Figure 69: Add a New Rule

Table 24 describes the rule fields.

Table 24: Add a New Rule Fields

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 Re-review 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 re-reviews.
Asterisk (*)	Mandatory fields in User Interface.
<Variable>	Substitute input value.

Table 24: Add a New Rule Fields

Field Name	Description
Alert Score	Enter the alert score. This indicates the alert score threshold after which reassessment happens. 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.
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.

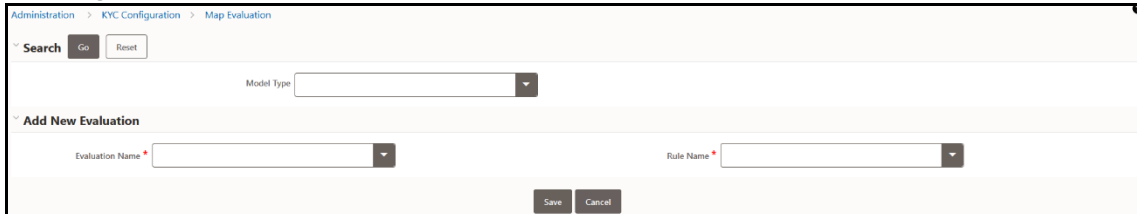
- To save the rule, click **Save**. To close the dialog box, click **Cancel**. This refreshes the screen with the new rule.

9.3.1 Mapping an Evaluation to an Assessment

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

- On the KYC home page, click **KYC Risk Assessment Configuration**.
- Click **Association of Rule/Risk Parameter to Evaluation**. The **Map Evaluation** page is displayed.

Figure 70: Administration Menu



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

Figure 71: Map Evaluation

Evaluation Name	Rule Name
<input type="checkbox"/> Customer Address Change Log	Customer Change Log
<input type="checkbox"/> Frequent Account Alert	Frequent Account Alert
<input type="checkbox"/> Customer Address Change Log	Frequent Account Alert

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

9.3.2 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.

Figure 72: Administration Menu

Jurisdiction * [dropdown]
Risk Scoring Model Type * [dropdown]
Parameter/Rule Name * [dropdown]

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

Figure 73: Risk Score for Parameter/Rule Value

NOTE

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

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

To add Parameter/Rule value follow these steps:

1. Click **Add** in the Risk Score for Parameter/Rule Value section. The following pop-up window opens.

NOTE

Add any new Parameter/Rule value to the KDD_CODE_SET_TRNLN table corresponding to the rule code. You can view the Parameter/Rule value in the drop-down once added to the table.

Figure 74: Add Parameter/Rule Value Pop-up

2. After adding values in the required fields, click **Save**.

9.3.3 Disabling Accelerated Re-Review Rules

You can disable or deactivate individual Rules or the entire Accelerated re-review Rules.

- To enable or disable an individual Rule, you must set the `F_ENABLE` flag in the `appln_rereview_params` table as `Y` or `N`.
- To disable the entire Assessment (all of its rules), follow these steps::
 - On the KYC home page, click **Financial Services Inline Processing Engine** in the **Common Tasks** tab.
 - Navigate to **Assessment** tab and click the **Accelerated Review** assessment and open it. The **Assessment** pop-up appears.
 - Under the **Schedule** section, select the **Deactivate** radio button, and click **Save**.

9.4 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 Customer Type.

To view the UI, follow these steps.

1. Log in to the KYC application.
2. Under **Behavior Detection**, click **KYC Risk Assessment Configuration** and select **Risk Assessment Category**.

This action displays the Risk Assessment Category UI with the Search section.

Figure 75: Search Fields

3. Select the **Jurisdiction** and **Customer Type** and click **Go**.

Figure 76: Risk Score Categories Based on the Search Criteria

Jurisdiction	Customer Type	Risk Score Category	Minimum Score	Maximum Score	Re-review	User Review Required
DN of AMEA	Financial Institution	Standard	0	50	24	No
DN of AMEA	Financial Institution	Elevated	51	75	24	No
DN of AMEA	Financial Institution	High	76	100	6	No

This action displays the risk scores and risk categories for the selected Jurisdiction and Customer Type.

9.4.1 Modifying the Risk Scores

NOTE The minimum and the maximum risk score values should be in sequence and the numbers should not overlap.

To modify the minimum and maximum risk scores, follow these steps.

1. Select the row for which you want to modify the risk scores.
2. Double-click the score value and provide the new score value.
3. Click **Save**.

9.4.2 Copying the Risk Scores

To Copy the Risk Scores to Destination Jurisdiction, follow these steps.

1. Select the row that you want to copy the risk scores from.
2. Click **Copy**.
3. In the pop-up, select the Destination Jurisdiction to which you want to copy the risk scores.
4. Click on **Confirm**.

This action copies the risk scores to the destination jurisdiction.

9.4.3 Showing the History of Risk Scores

To show the History of risk scores, follow these steps.

1. Select the row for which you want to view the History.
2. Click **History**.

This displays a pop-up with the History of Risk Scores that are modified previously.

10 APPENDIX-A KYC Batches

This appendix covers the Know Your Customer (KYC) Batch and the tasks within the batches.

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.

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.

10.1 Regular Processing

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 25 provides details about regular processing.

Table 25: 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 Re-review, New Accounts, and Periodic Re-review 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_extra_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 into 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 into the processing table when run.	TRANSFORM DATA	Task3
Task5	Populate_Cust_Ad- dr_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Addr_Prcsng table when run.	LOAD DATA	Task3
Task6	Populate_Cust_Cn- try_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Cntry_Prcsng table when run.	LOAD DATA	Task3
Task7	Populate_Cust_Id_Doc _Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Id_Doc_Prcsng table when run.	LOAD DATA	Task3
Task8	Populate_Cust_Mkt- Served_Prcs ng	This is a task that populates the prefiltered Customer Data into the Cust_Mkt_Served_Prcsng table when run.	LOAD DATA	Task3
Task9	Populate_Cust_Phon_P rcsng	This is a task that populates the prefiltered Customer Data into the Cust_Phon_Prcsng table when run.	LOAD DATA	Task3
Task10	Populate_Cust_Prod_P rcsng	This is a task that populates the prefiltered Customer Data into the Cust_Product_Prcsng table when run.	LOAD DATA	Task3
Task11	Populate_Cust_to- Cust_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Cust_Prcsng table when run.	LOAD DATA	Task3
Task12	Populate_Cust_Acct_P rcsng	This is a task that populates the prefiltered Customer Data into the Cust_Acct_Prcsng table when run.	LOAD DATA	Task3

Table 25: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task13	Populate_Acct_Prcsng	This is a task that populates the pre-filtered Customer Data into the Acct_Prcsng table when run.	LOAD DATA	Task12
Task14	POPULATE_IP_KYC	This is a task that populates the Interested Party Customers and Accounts when they are run.	TRANSFORM DATA	Task10, Task11, Task12, Task13, Task3, Task4, Task5, Task6, Task7, Task8, Task9
Task15	t2t_PARTY_ADDRESS_PRCNG_IP	This is a task that populates the party address into the pricing table when run.	LOAD DATA	Task14
Task16	t2t_PARTY_DETAILS_PRCNG_IP	This is a task that populates the party details into the pricing table when run.	LOAD DATA	Task14
Task17	t2t_PARTY_ID_DOC_PRCNG_IP	This is a task that populates the party doc ID into the pricing table when run.	LOAD DATA	Task14
Task18	t2t_PARTY_PARTY_RELSHIP_PRCNG_BO	This is a task that populates the beneficial owner details into the PARTY_PARTY_RELSHIP_PRCNG_BO table when run.	LOAD DATA	Task14, Task15, Task16, Task17
Task19	t2t_PARTY_DETAILS_PRCNG_BO_INT	This is a task that populates the internal beneficial owner details into the PARTY_DETAILS_PRCNG_BO_INT table when run.	LOAD DATA	Task18
Task20	t2t_PARTY_DETAILS_PRCNG_BO_EXT	This is a task that populates the external beneficial owner details into the PARTY_DETAILS_PRCNG_BO_EXT table when run.	LOAD DATA	Task18
Task21	t2t_PARTY_ADDRESS_PRCNG_BO_INT	This is a task that populates the internal beneficial owner details into the PARTY_ADDRESS_PRCNG_BO_INT table when run.	LOAD DATA	Task18

Table 25: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task22	t2t_PARTY_AD-DRESS_PRCNG_BO_EXT	This is a task that populates the external beneficial owner details into the PARTY_AD- DRESS_PRCNG_BO_EXT table when run.	LOAD DATA	Task18
Task23	t2t_PARTY_ID_DOC_PRCNG_BO_INT	This is a task that populates the internal beneficial owner details into the PARTY_ID_DOC_PRCNG_BO_INT table when run.	LOAD DATA	Task18
Task24	t2t_PARTY_ID_DOC_PRCNG_BO_EXT	This is a task that populates the external beneficial owner details into the PARTY_ID_DOC_PRCNG_BO_EXT table when run.	LOAD DATA	Task18
Task25	t2t_FCT_TP_WLS_REQUESTS_PRCNG	This is a task that populates Requests into the watch list Processing table for the prefiltered Customers when run.	LOAD DATA	Task18, Task19, Task20, Task21, Task22, Task23, Task24
Task26	t2t_FCT_TP_WLS_RESULTS_PRCNG	This is a task that populates the watch list Score in the FCT_TP_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_POPULATE_FCT_RA	This is a task that generates the Risk Assessment IDs for each Customer and populates the FCT_RA table when run.	LOAD DATA	Task30
Task32	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	Task31

Table 25: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
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_RVWDTL S	This is a task that populates the FCT_CUST_RVWDTLS table when run.	LOAD DATA	Task31
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 into 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 truncates the kdd_ex- trl_batch_last_run table when run.	TRANSFORM DATA	Task31, Task32, Task33, Task34, Task35, Task36, Task37, Task38, Task39, Task40, Task41

Table 25: Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
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

10.2 Deployment Initiation Processing

Table 26 provides details about deployment initiation processing.

Table 26: Deployment Initiation Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task1	FN_IPE_LAST_BATCH_RUN_KY	This is a task that captures the current batch ID when run.	TRANSFORM DATA	DATA
Task2	Populate_-Cust_Prcsng_DI	This is a task that populates the prefiltered Customer Data into the Cust_Prcsng table when run.	LOAD DATA	Task1
Task3	GathrStats_-CUST_PRCsNG	This is a task that is used to gather statistics for the Cust_Prcsng table.	TRANSFORM DATA	DATA
Task4	Populate_-Cust_Ad-dr_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Addr_Prcsng table when run.	LOAD DATA	Task3
Task5	Populate_-Cust_Cn-try_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Cntry_Prcsng table when run.	LOAD DATA	Task4
Task6	Populate_-Cust_Id_Doc_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Id_Doc_Prcsng table when run.	LOAD DATA	Task5
Task7	Populate_-Cust_Mkt_-Served_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Mkt_Served_Prcsng table when run.	LOAD DATA	Task6
Task8	Populate_-Cust_Phon_Prcsng	This is a task that populates the prefiltered Customer Data into the Cust_Phon_Prcsng table when run.	LOAD DATA	Task7

Table 26: Deployment Initiation Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task9	Populate_-Cust_Prod_Prcs ng	This is a task that populates the prefiltered Customer Data into 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 into 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 into 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
Task13	Populate_-Acct_Prcs ng	This is a task that populates the prefiltered Customer Data into the Acct_Prcsng table when run.	LOAD DATA	Task12
Task14	POPULATE_IP_KYC	This is a task that populates the Interested Party Customers and Accounts when they are 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_DETAILS_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_ADDRESS_PRCNG_IP	This is a task that populates the party address in the PARTY_ADDRESS_PRCNG_IP table when run.	LOAD DATA	Task15
Task18	t2t_PARTY_ID_DOC_PRCNG_IP	This is a task that populates the party doc ID in the PARTY_ID_DOC_PRCNG_IP table when run.	LOAD DATA	Task15

Table 26: Deployment Initiation Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
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_FuzzyMatch	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
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_KY-CPRCSNG_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 that generates rule or model-based scores when run.	INLINE PROCESSING	Task19, Task20, Task21, Task22, Task23, Task24, Task25
Task27	Customer Processing	This is a task that 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_POPU-LATE_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

Table 26: Deployment Initiation Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task31	t2t_POPU-LATE_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_T-P_WLS_REQUESTS	This is a task that populates the watch list score in the FCT_T- P_WLS_REQUESTS table when run.	LOAD DATA	Task 34
Task36	t2t_FCT_T-P_WLS_RESULTS	This is a task that populates the watch list score in the FCT_T- P_WLS_RESULTS table when run.	LOAD DATA	Task 35
Task37	t2t_FCT_RA_RISK_RATING_HISTORY	This is a task that populates the FCT_RA_RISK_RATING_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

10.3 End of Day Processing

Table 27 provides details about the end of day processing.

Table 27: End of Day Processing

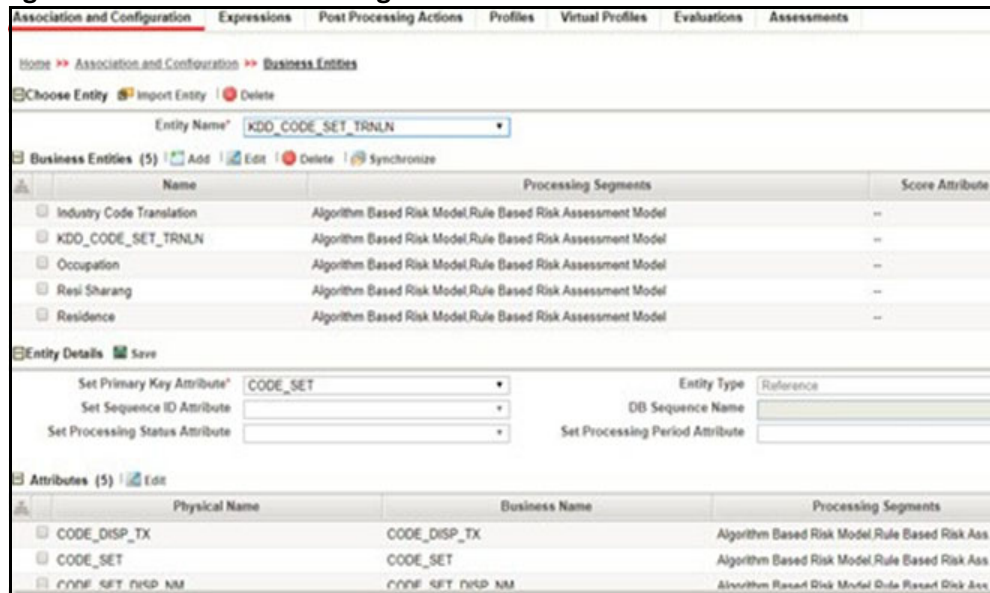
Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task1	t2f_GenCustDetails_ED	Extract the customer feedback details.	EXTRACT DATA	
Task2	t2f_GenWLSFeedba ck_ED	Extract the watch list scanning feedback details.	EXTRACT DATA	
Task3	t2f_GenCBSFeedbac k_ED	Extract customer details for CBS.	EXTRACT DATA	
Task4	KYC_File_Rename	Renaming of the extracted files according to the Anti Money Laundering (AML) needs.	TRANSFORM DATA	Task1, Task2, Task3
Task5	FN_REREVIEW_DAT E_DI	Splitting of the customers processed through the DI processing back for periodic re-review.	TRANSFORM DATA	Task1, Task2, Task3, Task4

11 APPENDIX-B Creating Highlights

This appendix provides the steps to create highlights for Risk and Algorithm-based assessments in know Your Customer (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.
2. To add a Business Entity, navigate to the **Association and Configuration** menu on the **Inline Processing** page and click **Business Entities**.

Figure 77: Association and Configuration Menu

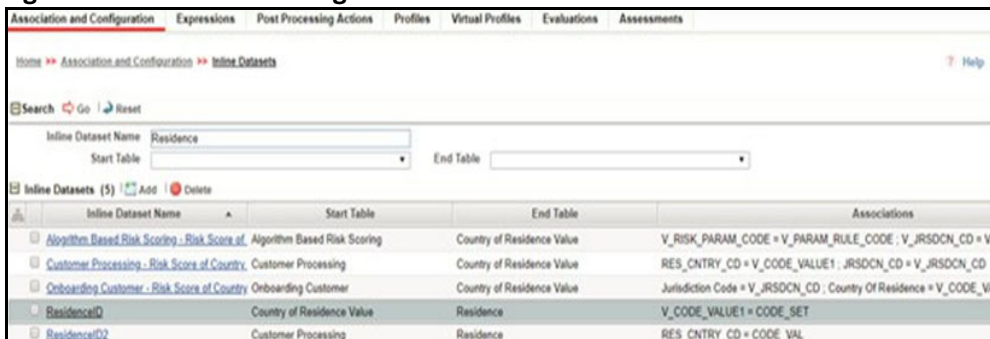


In the following example, a Business Entity called Residence is created.

3. Add two Inline Datasets, one for the start table, and one for the end table.
4. To add an Inline Dataset, navigate to the Association and Configuration menu on 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.

Figure 78: Inline Datasets Page

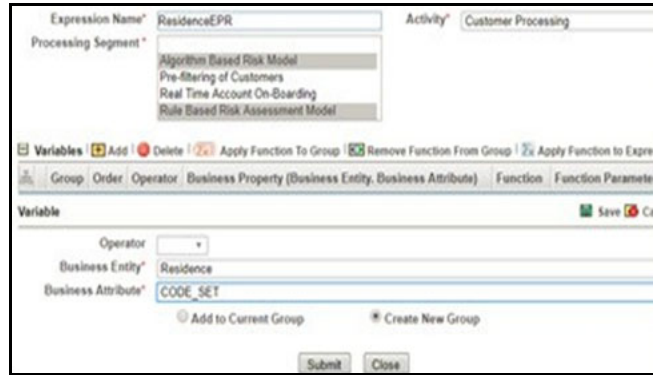


5. Add a Traversal Path for each join defined in Inline Datasets.
6. To add a Traversal Path, navigate to the Association and Configuration menu on the Inline Processing page and click Traversal Paths.

In the following example, a Traversal path is created from the Country of Processing table to the Algorithm Based Risk Scoring table.

7. 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 on the Inline Processing page.

Figure 79: Expressions Menu



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

8. Map an evaluation to the existing assessment of the added parameter.

To map an evaluation, navigate to the Evaluations menu on the Inline Processing page. In the following example, an Evaluation is created for the Rule-Based Risk Assessment.

Figure 80: Evaluations Menu

Evaluation Name	Score	Activity	Processing Segment	Status	Updated By
Account Country Change	10	Customer	Pre-filtering of Customers	VALID	06/06/2017
Account State Change	10	Customer	Pre-filtering of Customers	VALID	06/06/2017
Change in Customer's Citizenship	10	Customer	Pre-filtering of Customers	VALID	06/06/2017
Customer Country Change	10	Customer	Pre-filtering of Customers	VALID	06/06/2017
Customer State Change	10	Customer	Pre-filtering of Customers	VALID	06/06/2017
Frequent Account Alert	10	Customer	Pre-filtering of Customers	VALID	06/06/2017
Frequent Customer Alert	10	Customer	Pre-filtering of Customers	VALID	06/06/2017
Geo Risk - Country of Head Quarters	Parameter / Rule Value Risk Score	Customer Processing	Rule Based Risk Assessme	VALID	01/24/2017
Geo Risk - Country of Operations	Parameter / Rule Value Risk Score	Customer Processing	Rule Based Risk Assessme	VALID	01/24/2017
Geo Risk - Country of Primary Citizenship	Parameter / Rule Value Risk Score	Customer Processing	Rule Based Risk Assessme	VALID	01/24/2017
Geo Risk - Country of Residence	Parameter / Rule Value Risk Score	Customer Processing	Rule Based Risk Assessme	VALID	SUPERVISOR
Geo Risk - Country of Secondary Citizenship	Parameter / Rule Value Risk Score	Customer Processing	Rule Based Risk Assessme	VALID	01/24/2017
Geo Risk - Country of Taxation	Country of Taxation - Weighted Scor	Customer Processing	Algorithm Based Risk Mod	VALID	SUPERVISOR
Geo Risk - Country of Citizenship	Count of Citizenship - Weighted Soc	Customer Processing	Algorithm Based Risk Mod	VALID	01/24/2017
Geo Risk -Country of Head Quarters	Country of Head Quarters - Weighted	Customer Processing	Algorithm Based Risk Mod	VALID	01/24/2017

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

Figure 81: Assessments Menu

Association and Configuration | Expressions | Post Processing Actions | Profiles | Virtual Profiles | Evaluations | **Assessments**

Home >> Assessments

Search Go

Assessment Name Activity Processing Segment

Status

Assessments (7)

	Assessment Name	Activity	Processing Segment	Status	
<input type="checkbox"/>	Accelerated Re-review	Customer	Pre-filtering of Customers	VALID	--
<input type="checkbox"/>	Algorithm Based Risk Assessment	Customer Processing	Algorithm Based Risk Model	VALID	SUPER
<input type="checkbox"/>	New Accounts Opened by Customers	Customer	Pre-filtering of Customers	VALID	--
<input type="checkbox"/>	On Boarding Algorithm Based Risk Assessment	Onboarding Customer	Real Time Account On-Boarding	VALID	--
<input type="checkbox"/>	On Boarding Rule Based Assessment	Onboarding Customer	Real Time Account On-Boarding	VALID	--
<input type="checkbox"/>	Periodic Re-review of Customers	Customer	Pre-filtering of Customers	VALID	--
<input checked="" type="checkbox"/>	Rule Based Risk Assessment	Customer Processing	Rule Based Risk Assessment M	VALID	SUPER

12 APPENDIX-C Configuring Steps for CS Delta Updates

This appendix provides the configuration steps needed to view the delta updates when customers are screened for matches against the Customer Screening (CS) Watch list. If there is a match, then an accelerated re-review is generated. The latest matches are picked when the `cust_watchlist_mtchs` batch is run.

Topics:

- [Adding the CS Task to the KYC Daily Batch](#)
- [Mapping the Watch List evaluation to the Accelerated Re-review Assessment](#)

12.1 Adding the CS Task to the KYC Daily Batch

To add the CS task to the Know Your Customer (KYC) daily batch, follow these steps. Before you run the batch, ensure that you have completed data ingestion in all relevant tables.

1. Log in to the KYC Application.
2. Click **Common Tasks**. Select **Rule Run Framework** and click **Process**.

12.1.1 Running the Daily Batch

To run the Daily batch, follow these steps:

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

Figure 82: Process Page

PROCESS

Code

Name

Folder

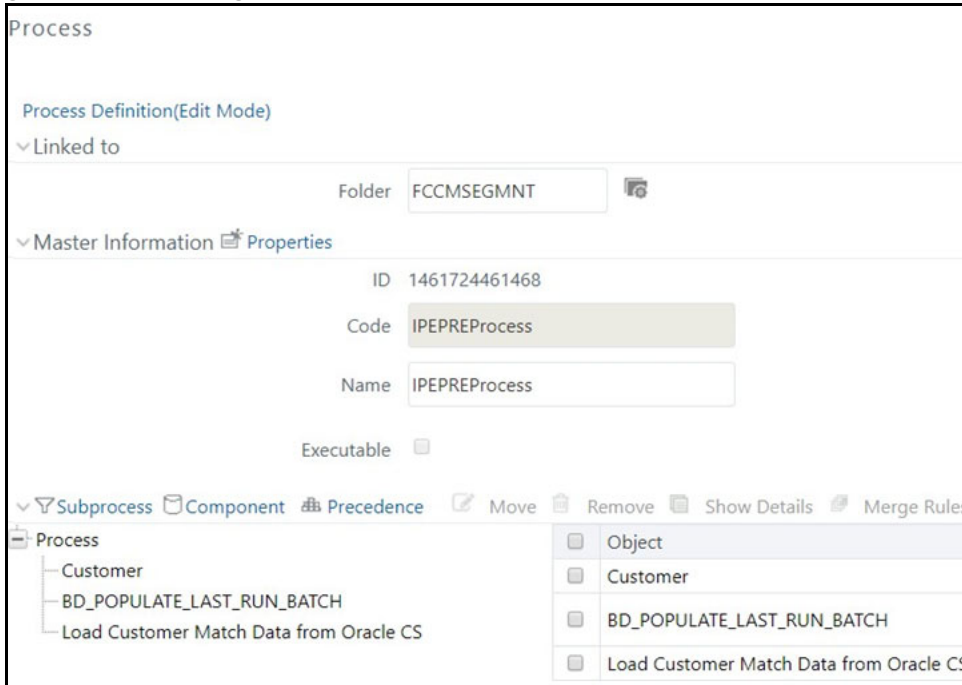
+ New View Edit Copy Remove Authorize Export Trace Definition

<input type="checkbox"/>	Code	Name
<input checked="" type="checkbox"/>	IPEPREProcess	IPEPREProcess

Page 1 of 1 (1-15 of 1 items)

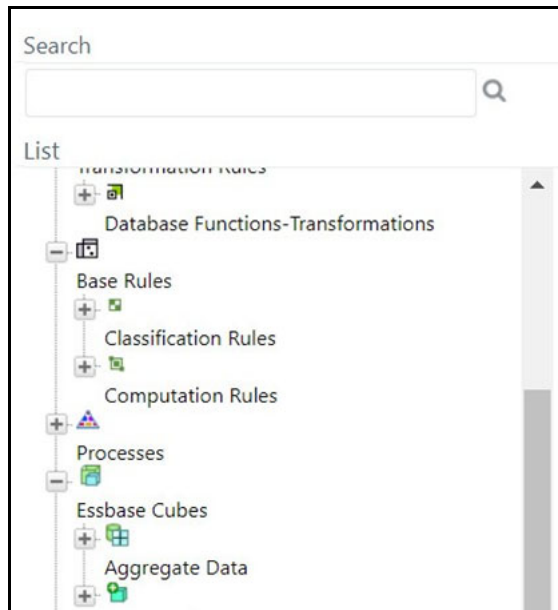
2. Select the `IPEPREProcess` check box and click **Edit**. The **Process Definition (Edit Mode)** page appears.
3. Click **Component**.

Figure 83: Process Page in Edit Mode



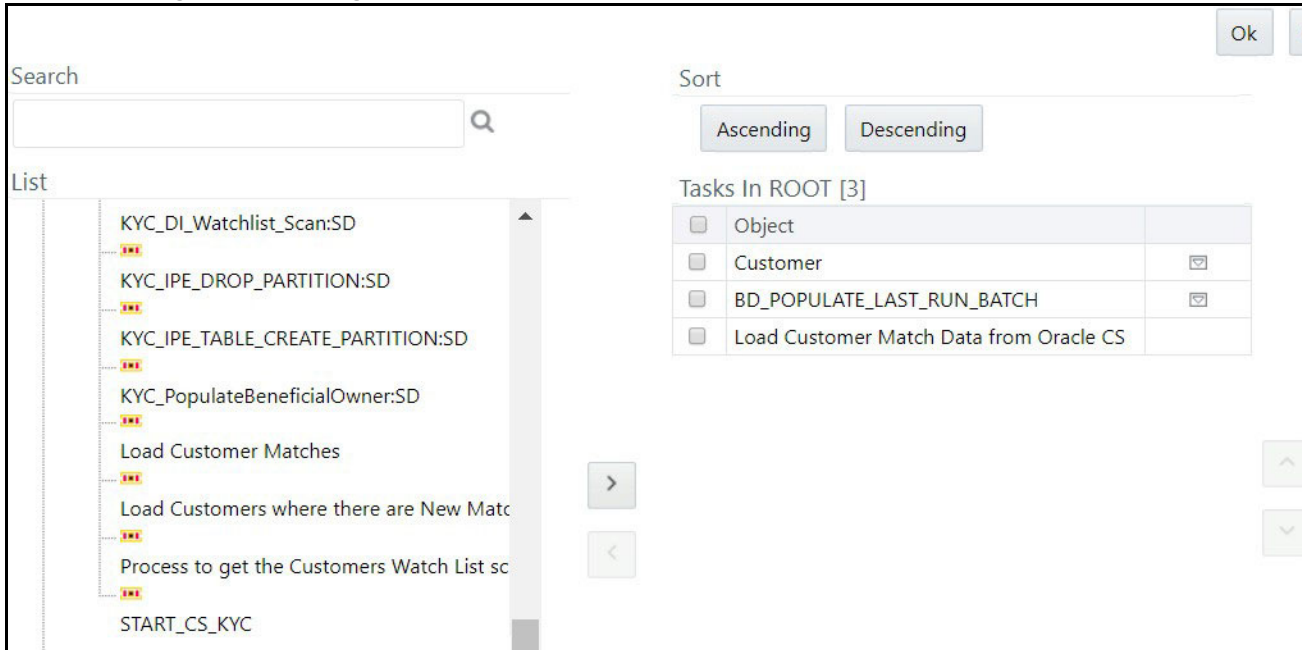
4. On the **Component Selector** screen, search for the **Processes** node in the List window on the left.

Figure 84: Component Selector



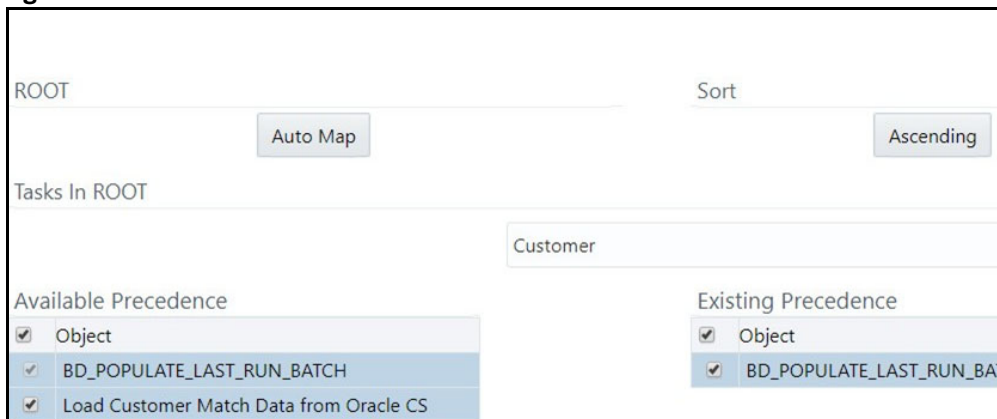
5. Expand the **Processes** node, and then the **FCCMSEGMNT** node.
6. Search for Load Customer Match Data from the Oracle CS process and double-click the process. It moves to the **Tasks** window on the right.

Figure 85: Moving Load Customer Match Data



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.

Figure 86: Precedence Selector



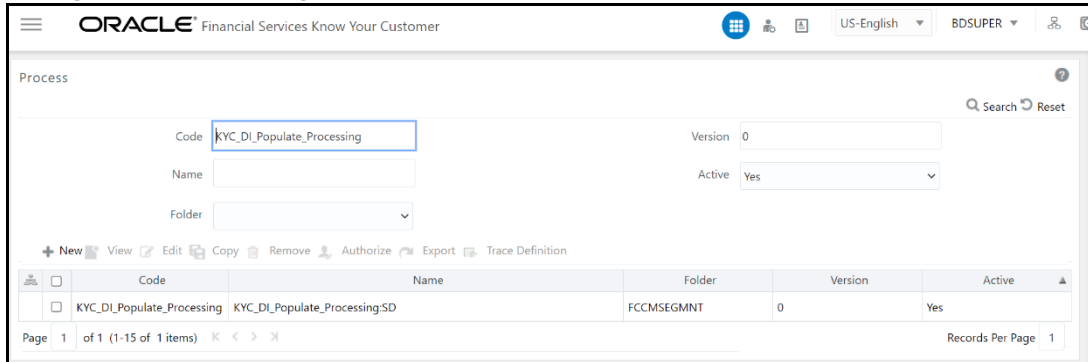
10. Click **Ok**.
11. Click **Save** to save the process.
12. Recreate the Batch corresponding to this RUN.

12.1.2 Running the Deployment Initiation Batch

To run the Deployment Initiation batch, follow these steps:

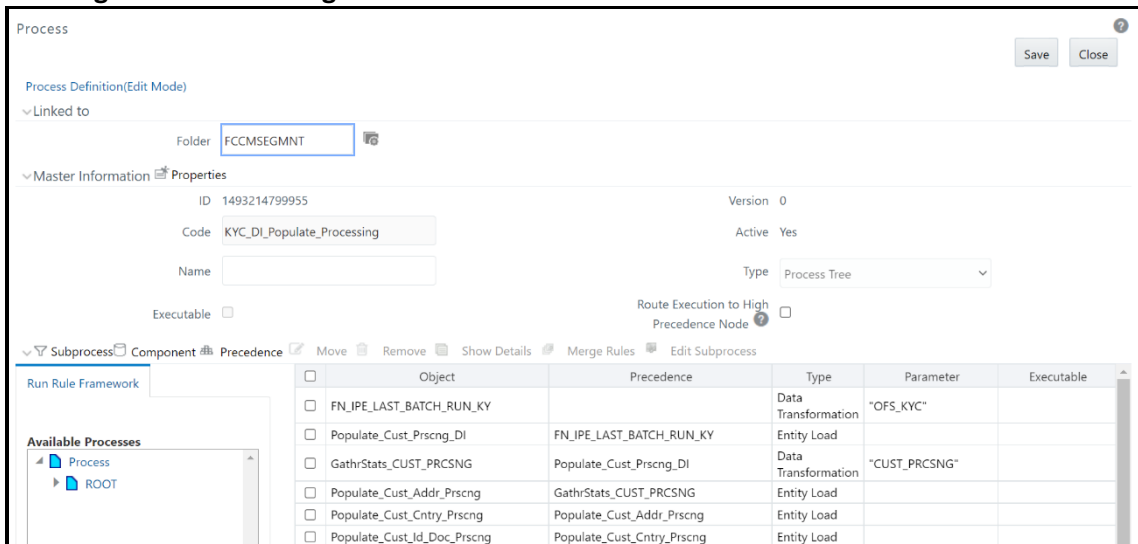
1. On the **Process** page, provide the value `KYC_DI_Populate_Processing` in the **Code** field and click **Search**.

Figure 87: Process Page



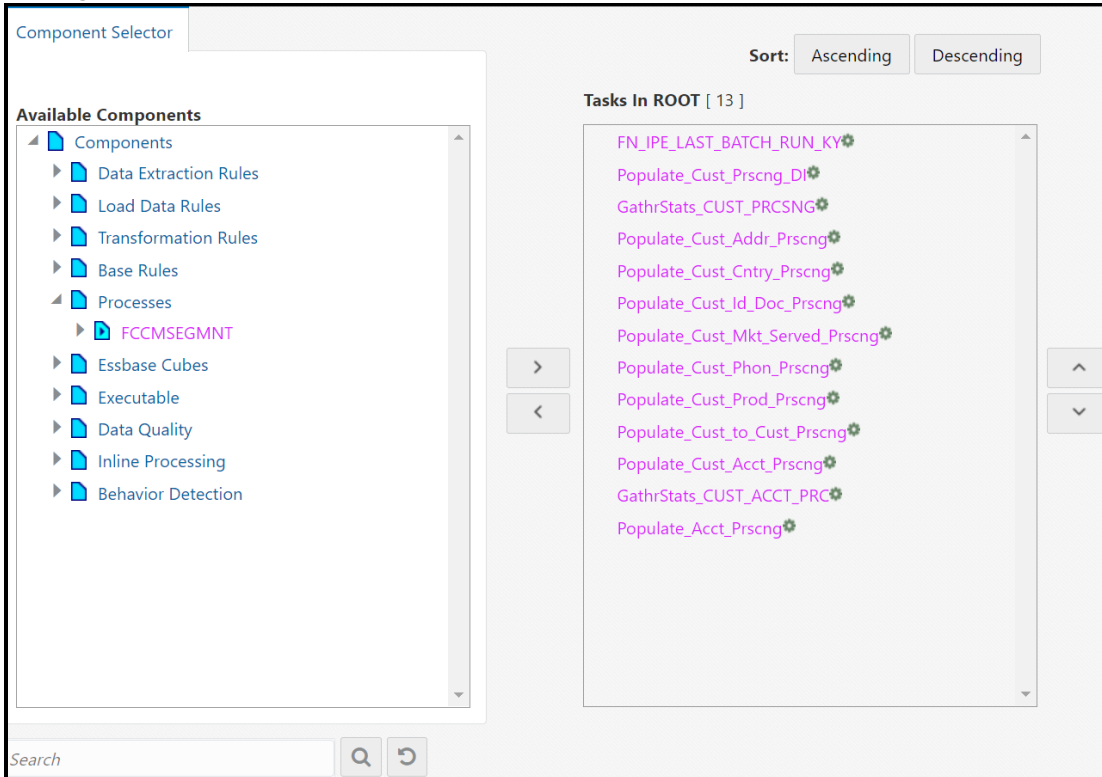
2. Select the `KYC_DI_Populate_Processing` check box and click **Edit**. The **Process Definition (Edit Mode)** page appears.
3. On the **Process Definition (Edit Mode)** screen, click **Component**.

Figure 88: Process Page in Edit Mode



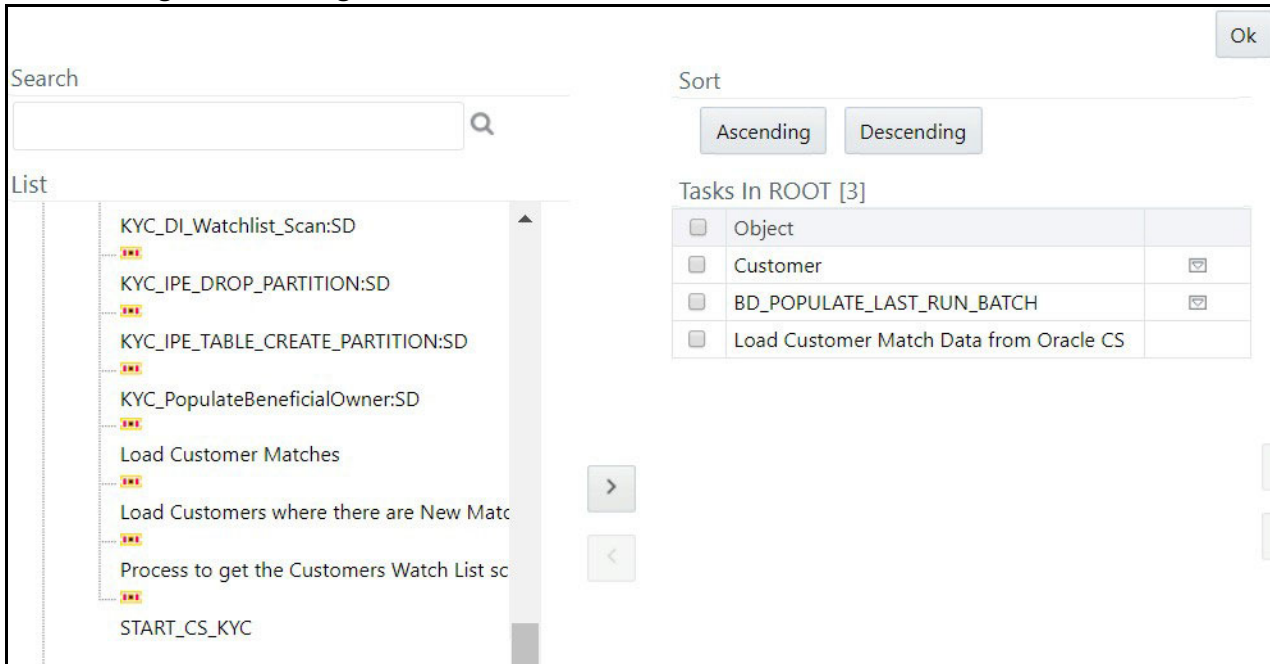
4. On the **Component Selector** screen, search for the **Processes** node in the List window on the left.

Figure 89: Component Selector



5. Expand the **Processes** node, and then the **FCCMSEGMNT** node.
6. Search for the **Load Customer Match Data from the Oracle CS** process and double-click the process. It moves to the **Tasks** window on the right.

Figure 90: Moving Load Customer Match Data



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.

Figure 91: Precedence Selector

10. Click **Ok**.
11. Click **Save** to save the process.
12. Recreate the Batch corresponding to this RUN.

12.2 Mapping the Watch List evaluation to the Accelerated Re-review Assessment

To map the evaluation, follow these steps:

1. Log in to the KYC Application.
2. Click **Common Tasks**. Select **Financial Services Inline Processing Engine** and click **Inline Processing** and select **Assessments**.

Figure 92: Precedence Selector

Assessment Name	Activity	Processing Segment	Status
Accelerated Rereview	Customer	Pre-filtering of Customers	VALID
Algorithm Based Risk Assessment	Customer Processing	Algorithm Based Risk Model	VALID
Change in Risk Model	Customer	Pre-filtering of Customers	VALID

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

Figure 93: Associated Evaluations

Assessment Details + Define KYC Attributes
 Name* Accelerated Rereview Activity* Customer
 Status VALID Execution mode Live Test
 Updated By KYCADMN Updated On 10/20/2017 07:14:10 PM

Associated Evaluations (14) [Map](#)

	Evaluation Name	Score
<input type="checkbox"/>	Customer Address Change Log	10
<input type="checkbox"/>	Customer Change Log	10
<input type="checkbox"/>	Customer Country Change Log	10
<input type="checkbox"/>	Customer Market Served Change Log	10

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

Figure 94: Moving the Evaluations

Available Evaluations

- Change In Risk Model - Occupation
- Periodic Re-review of Customers
- Change In Risk Model - Product Risk
- Change In Risk Model - Corporate Age
- Change In Risk Model - Industry Risk
- Change In Risk Model - Country Of Residence
- Change In Risk Model - Country Of Head Quar
- Change In Risk Model - Markets Risk
- New Watch List Matches
- Change In Risk Model - Secondary Citizenship

>>

<<

Included Evaluations

- Customer Country Change Log
- High Score Customer Alert
- Frequent Account Alert
- Frequent Customer Alert
- Suspicious Account Alert
- High Score Account Alert
- Customer Change Log
- Customer Market Served Change Log
- Suspicious Customer Alert
- Customer to Customer Change Log

Save Close

- Click **Save**.
- Restart the servers.

13 APPENDIX-D Switching between EDQ and CS

This chapter shows the scripts that are to be executed to switch between EDQ () and CS (Customer Screening).

- Execute the following script to switch to EDQ.

```

MERGE INTO AAI_WF_TRANSITION_B T USING (
    SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1665487085276' V_TRANSITION_ID,
    'Job_1533292500818' V_FROM_ACTIVITY_ID, 'Job_1665486756737'
    V_TO_ACTIVITY_ID, '0' 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_CON
    DITION_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_I
    D,S.V_CONDITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_T
    YPE,S.V_TRANSITION_STROKE)
/
MERGE INTO AAI_WF_TRANSITION_B T USING (
    SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1665487085277' V_TRANSITION_ID,
    'Job_1665486756737' V_FROM_ACTIVITY_ID, 'Job_1601833121763'
    V_TO_ACTIVITY_ID, '0' 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_CON
    DITION_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_CONDITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_TYPE,S.V_TRANSITION_STROKE)
```

```
/
```

```
MERGE INTO AAI_WF_TRANSITION_TL T USING (
```

```
  SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1665487085276' V_TRANSITION_ID,
 'Job_1533292500818_Job_1665486756737' 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_LOCALE_CODE)
```

```
/
```

```
MERGE INTO AAI_WF_TRANSITION_TL T USING (
```

```
  SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1665487085277' V_TRANSITION_ID,
 'Job_1665486756737_Job_1601833121763' 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_LOCALE_CODE)
```

```
/
```

- Execute the following script to switch to CS.

```
MERGE INTO AAI_WF_TRANSITION_B T USING (
```

```
  SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1665487085276' V_TRANSITION_ID,
 'Job_1533292500818' V_FROM_ACTIVITY_ID, 'Job_1665486756736'
 V_TO_ACTIVITY_ID, '0' 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_CON
DITION_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_CONDITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_T
YPE,S.V_TRANSITION_STROKE)

/

MERGE INTO AAI_WF_TRANSITION_B T USING (

  SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1665487085277' V_TRANSITION_ID,
'Job_1665486756736' V_FROM_ACTIVITY_ID, 'Job_1601833121763'
V_TO_ACTIVITY_ID, '0' 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_CON
DITION_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_CONDITION_EXPR,S.V_CONDITION_TYPE,S.V_PRECEDENCE,S.V_TRANSITION_T
YPE,S.V_TRANSITION_STROKE)

/

MERGE INTO AAI_WF_TRANSITION_TL T USING (

  SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1665487085276' V_TRANSITION_ID,
'Job_1533292500818_Job_1665486756736' 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_LOCALE_CODE)
/

MERGE INTO AAI_WF_TRANSITION_TL T USING (
    SELECT 'KYC_ONBOARDING' V_PROCESS_ID, '1665487085277' V_TRANSITION_ID,
'Job_1665486756736_Job_1601833121763' 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_LOCALE_CODE)
/
```

OFSAA Support

Raise a Service Request (SR) in [My Oracle Support \(MOS\)](#) for queries related to the OFSAA applications.

Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.

