Oracle® Financial Services Know Your Customer

Administration Guide

Release 8.1.2.10.0
G42129-01
August 2025

Oracle Financial Services Know Your Customer Administration Guide, Release 8.1.2.10.0

G42129-01

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

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

Contributors: (contributor), (contributor)

Contents

10 Simulation Capability

Document Control

Table Document Control

Revision Number	Revision Date	Change Log
8.1.2.10.0	August 2025	Updated the following sections: • Managing KYC Batches • Simulation Capability
8.1.2.9.0	February 2025	Updated the following section: • Simulation Capability
8.1.2.8.0	August 2024	Updated the following sections: • KYC Onboarding • Simulation Capability • APPENDIX-C Configuring Steps for CS Delta Updates
8.1.2.7.0	February 2024	Updated the Simulation Capability section.
8.1.2.6.2	December 2023	Introduced the following sections: • Simulation Capability • Appendix-E Configurations for the Bearer Token • Appendix-F Setting theZEPPELIN_INTERPETER_OUTPUT_LIMITin
8.1.2.6.0	October 2023	Updated the Running KYC Batches section.
8.1.2.5.0	June 2023	There are no updates to this guide in this release.
8.1.2.4.0	March 2023	Added sections User Authentication and Performing Assessments on Related Customers.
8.1.2.3.0	December 2022	• 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.

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.

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.
- Simulation Capability describes how you can tune the configurations for respective jurisdictions, analyze the results of each simulation run including comparison against production data and decide on the right champion model to be deployed back to production.
- 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.
- APPENDIX-D Switching between EDQ and CS describes the scripts that are to be executed to switch between EDQ (Enterprise Data Quality) and CS (Customer Screening).
- Appendix-E Configurations for the Bearer Token takes you through the process of generating a token and using it to get the individual or entity JSON, depending on the API request. A token is used to authorize the request.
- Appendix-F Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMIT in Python Interpreter describes how to directly execute instructions written in a programming or scripting language without requiring them previously to be compiled into a machine language program.

1.4 Where to Find More Information

For more information about OFS KYC, see the following KYC application documents on OHC:

- 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 Financial Services.

1.5 Conventions Used in This Guide

The following table mentions the conventions used in this guide.

Table 1-1 Conventions Used

Conventions	Meaning
Italics	• Names of books as references • Emphasis • Substitute input values
Bold	• Menu names, field names, options, button names • Commands typed at a prompt • User input
Monospace	• 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.

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

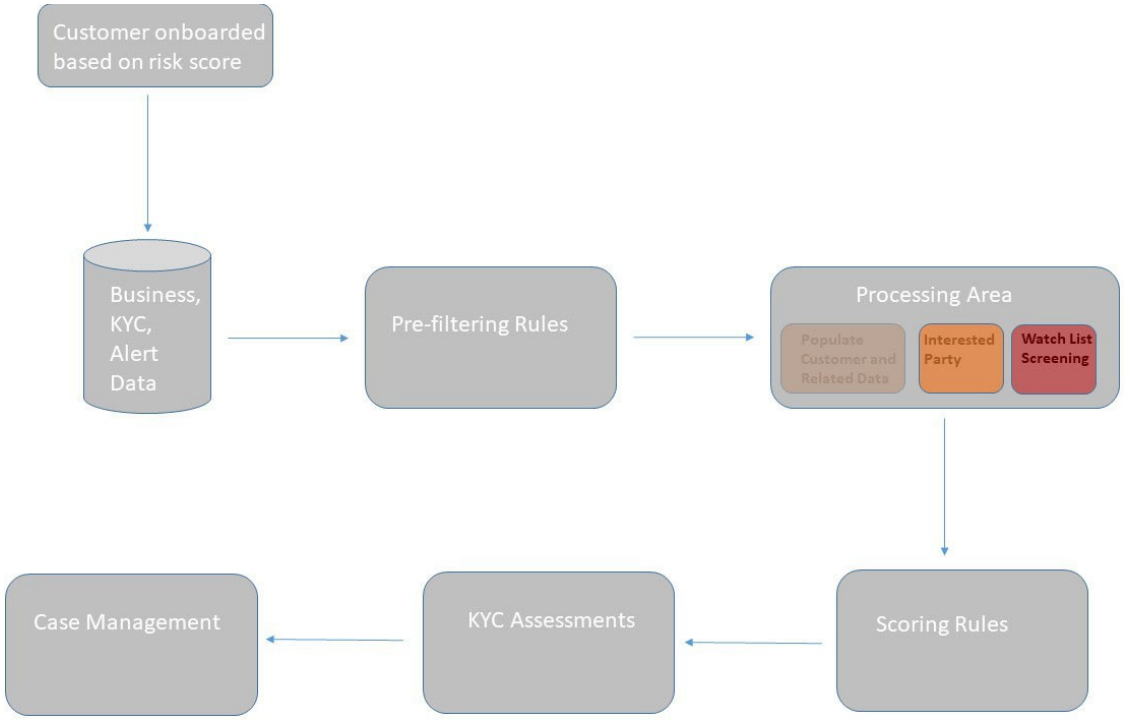
The Oracle KYC risk assessment application is built using the OFS Analytical Applications Infrastructure (AAI) framework. The application functions are divided into the following areas:

- 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 2-1 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:

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.

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/ofsaaapp/login.jsp`

   The **OFSAA Login page** is displayed.
2. Select the Language from the **Language** drop-down list.

   This allows you to use the application in the language of your selection.
3. Enter your **User ID** and **Password** in the respective fields.
4. Click **Login**.

   The 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:

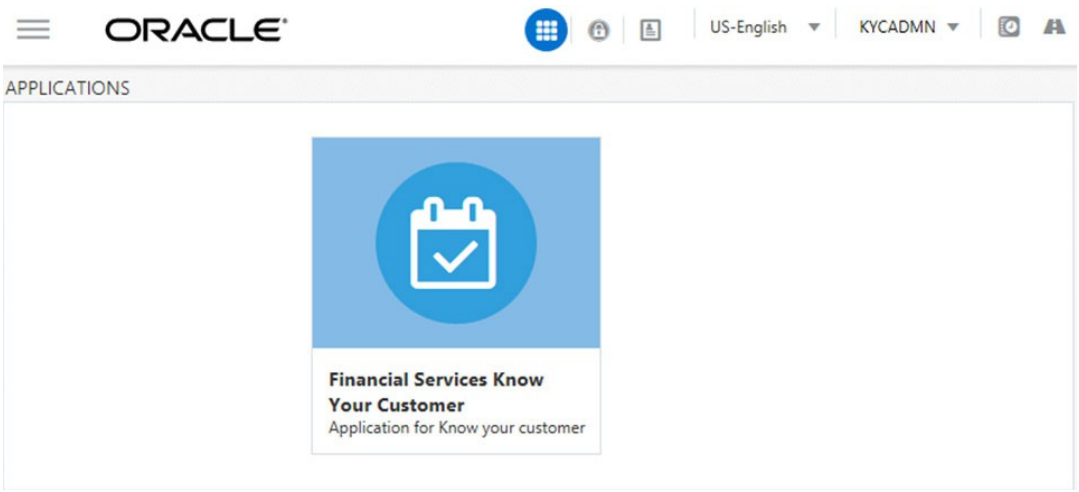
3.2.1 Behavior Detection - KYC Tab

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 **Application for Know your customer** icon.

Figure 3-1 OFSAA KYC Landing Page



2. In the **Navigation List**, click **Behavior Detection - KYC** .

   The KYC page appears.

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 **Application for Know your customer** icon.
2. In the **Navigation List**, click **Common Tasks**. The KYC page appears.

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.

- 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.
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:

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 4-1 User Provisioning Process Flow

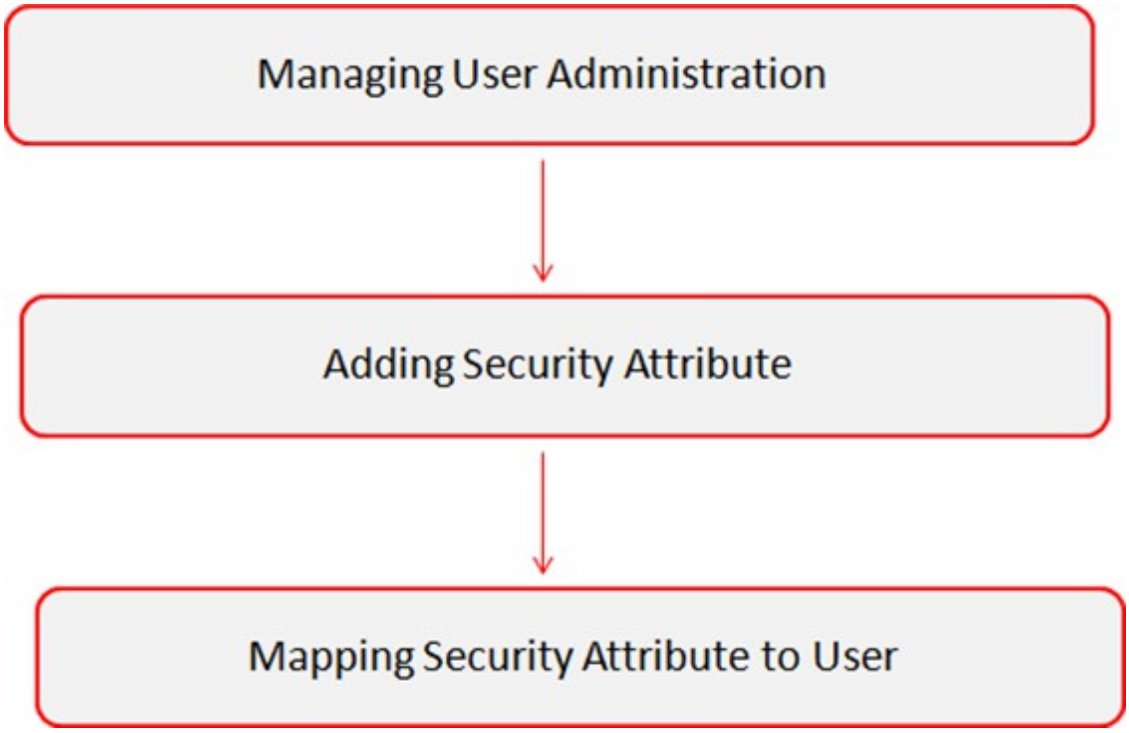


Table 4-1 User Provisioning Process Flow

Action	Description
Managing User Administration	Create users and map users to user groups. This allows Administrators to provide access, monitor, and administer users.
The KYC User Groups and User Activities table 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.

Topics:

- Managing Identity and Authorization

4.2.2 Managing Identity and Authorization

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

Topics:

- #unique_43
- Mapping a User with a User Group
- Privileges, Function Code and Name and their Description

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

Figure 4-2 Managing Identity and Authorization Process Flow

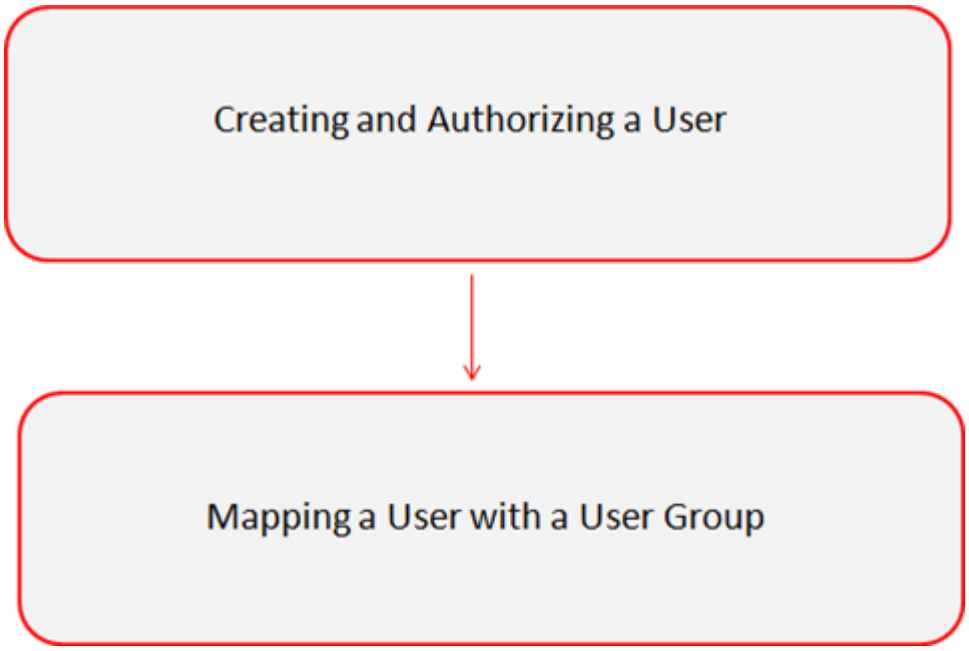


Table 4-2 Administration Process Flow

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.

4.2.2.1 Creating and Authorizing a User

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

4.2.2.2 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.

The following table describes the predefined KYC User Roles and corresponding User Groups.

Table 4-3 KYC Roles and User Groups

Role	User Group
KYC Administrator User	• KYC Administrator User Group • OB (Onboarding) KYC Administrator Group • IPEADMN
KYC Investigator User	• KYC Investigator User Group • OB KYC Investigator Group
KYC Investigator Rd Only	• KYC Investigator Read Only Group

The following table describes the predefined KYC User Groups and the corresponding user activities.

Table 4-4 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.

4.2.2.3 Privileges, Function Code and Name and their Description

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

Table 4-5 Privileges, Function Code and 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

Table 4-5 (Cont.) Privileges, Function Code and Name and their Description

SL #	Privileges	V_FUNCTION_CODE	V_FUNC-TION_NAME	V_FUNCTION_DESC
7	Access KYC Tabs in case management	CMKYCACSES	CM KYC Access	CM KYC Access

4.3 Adding Security Attributes

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

Topics:

- About Security Attributes
- Loading Security Attributes through SQL Scripts

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.

   The following table shows the KDD_JRSDCN database table attributes.

Table 4-6 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.

   The following table shows the *KDD_BUS_DMN* database table attributes.

Table 4-7 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).

Table 4-7 (Cont.) KDD_BUS_DMN Table Attributes

Column Name	Description
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. The following table shows the *KDD_SCNRO_GRP* database table attributes.

Table 4-8 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. The following table shows the *KDD_SCNRO_GRP_MEMBERSHIP* database table attributes.

Table 4-9 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. The following table shows the KDD_ORG database table attributes.

Table 4-10 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 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.

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,COM MENT_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.

> **Note**
>
> Do not combine this activity with any other Administration Configuration activities.

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.

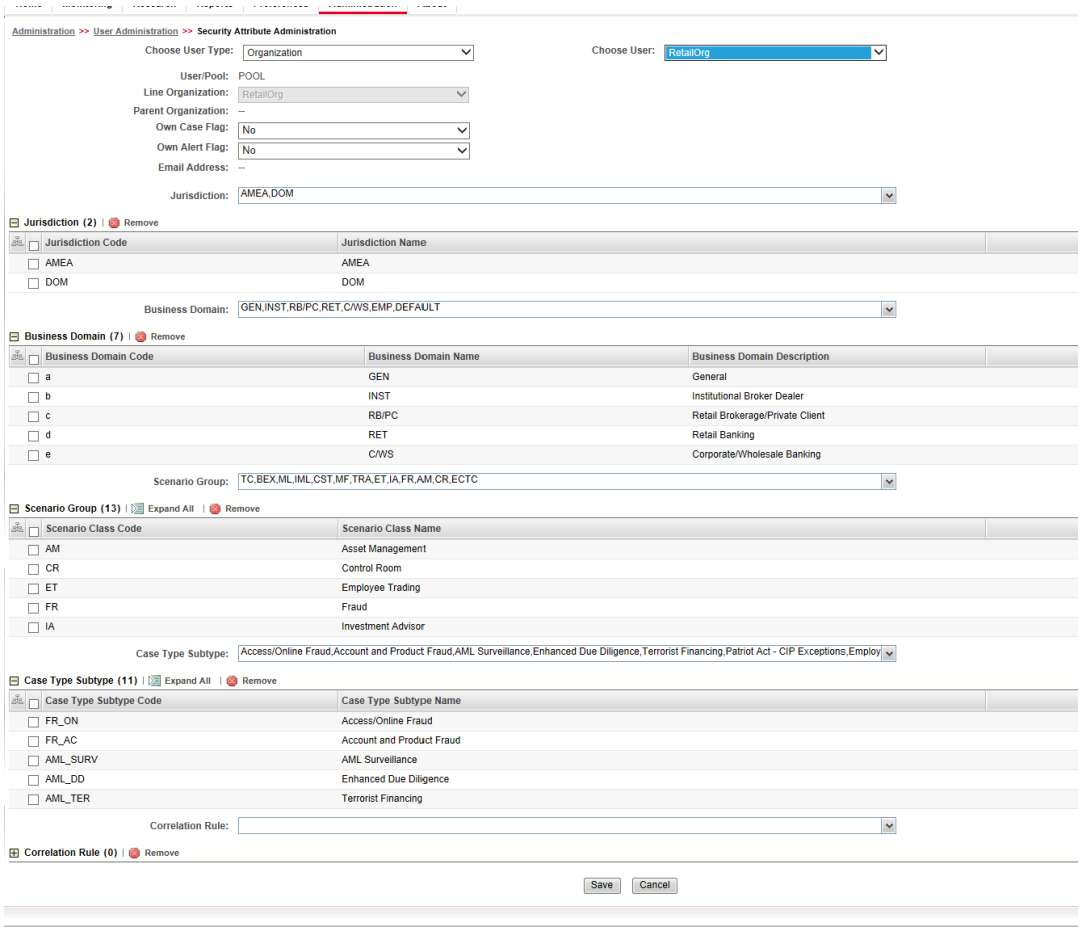
5. To view the Onboarding users, map the Onboarding role to the OB KYC Administrator group.

Figure 4-3 Map User Types to Users

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 5: Security Attribute Administration Page

Figure 4-4 Security Attribute Administration Page



> **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.

The following table shows the security attributes.

Table 4-11 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: • 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.
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**. A confirmation message is displayed.
8. Click **OK**. A confirmation message is displayed.
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.
3. Click **Remove**. A confirmation message is displayed.
4. Click **OK**. The selected record is deleted from the list.
5. 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:

5.1 Prerequisite

The OFS BD application pack must be installed. During OFS BD installation, for Simulation, install App Server and Web Server in the same user.

For information on pack installation, see the *Obtaining Software* section in the Oracle FinancialServices 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:

5.2.1 Initial or One-time Activities

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

- 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).

For more information on how to manage Application Parameters, see Manage KYC Application Parameters.

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).

For more information on how to manage Application Installation Parameters, see Manage KYC Installation Parameters.

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_trnln 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 5-1 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.
Sequence of Execution of KYC batches	The Processing of the batch is in the following sequence: • Deployment Initiation Processing - For processing the Existing customers. • Regular Processing - For daily processing. • EOD Processing (Feedback Processing) - For processing after the entire regular processing batch is complete. 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. Ensure that the feeds are scheduled as part of the data ingestion process in the account opening system and OFS BD application.

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_TAB_CRT_PARTITION_DLY* under Processes and move that component to Right Hand Side (RHS).
   c. Select the **KYC_IPE_TAB_CRT_PARTITION_DLY** 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_DLY** under **Processes** and move that component to RHS.

e. Select the **KYC_IPE_DROP_PARTITION_DLY** 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:

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 look- back 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.

5.3 Manage KYC Configuration

This section describes how to manage the KYC Application and Installation Parameters.

Topics:

5.3.1 Manage KYC Application Parameters

To display the KYC Application Parameters, follow these steps:

1. Navigate to **Behavior Detection - KYC**.
2. Click **Manage KYC Configuration** and then **Manage KYC Application Parameters**.
3. Select an option from the **Jurisdiction** , **Classification** , and **Parameter Name** drop-downs. It displays the data based on search criteria.

Click **History** to view the Application Parameters audit history.

5.3.2 Manage KYC Installation Parameters

To display the KYC Installation Parameters, follow these steps:

1. Navigate to **Behavior Detection - KYC**.
2. Click **Manage KYC Configuration** and then **Manage KYC Installation Parameters**.
3. Select **KYC** from the **Parameter Category** drop-down.
4. Select an option from the **Parameter Name** drop-down. It displays the data based on search criteria.

Click **History** to view the Installation Parameters audit history.

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.

Topics:

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/AutoCloseServic`.
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 following 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 following 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:

> **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.

Topics:

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**.
3. Select **Rule Run Framework** and select **Run**.
4. In the Run screen, select the **IPEKYCRunDI** code and click **Edit**.
5. Click **Selector** and select **Job**.
6. In the **List** section, expand Processes and select **FCCMSEGMNT** and double-click the **KYC_PopulateBeneficialOwner** task.

   The task moves to the **Tasks** section.
7. Move the *KYC_PopulateBeneficialOwner* process to below the *KYC_DI_Interested_Party:SD* process and above the *KYC_DI_Watchlist_Scan* process.
8. Click **OK** to save the changes.
9. 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. By default, it is **1**.

> **Note**
>
> If the interested party relationship is not required for the customer, the user can set the value to **0**.

There are two ways to set the interested party level.

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

   Parameter Name: LVL_IDF_IP

   Table Name: APPLN_INSTALL_PARAMS

2. To set the interested party level using UI, follow these steps.
   a. Login to the KYC application as KYC Administrator.
   b. Click **Behavior Detection - KYC**. Select **Manage KYC Configuration** and click **Manage KYC Installation Parameters** .
   c. On the **Manage KYC Installation Parameters** page, Select **KYC as Parameter Category** and **Manage KYC Installation Parameters as Parameter Name**.
   d. Update the **Attribute 1 Value** and provide your comments.
   e. Click **Save** to save the changes.
   This action updates the Interested Party Level.

7.3 End of Day Processing

Topics:

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 7-1 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 7-2 Watch List Feedback

SL No.	Business Name	Data Type
1	Entity Identifier Type	String
2	Entity Identifier	String
3	Watch List Identifier (Referred from Application parameter KYC_WLS_ENTRY_FILE_ID)	String
4	Watch List Entry Description Text	String
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. For more information, see https://docs.oracle.com/cd/E91253_01/kycguides.htm

Table 7-3 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_Rvwdtls)*, 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 Adding Tasks Based on Requirement

This section describes how to add a new task to the KYC Daily batch based on your requirement.

Adding New Task to KYC Daily Batch

To improve batch performance, you may need to add a task that removes (truncates) RTI Assessment tables.

To add a new task to the KYC Daily batch, follow these steps:

1. Log in as an Admin user.
2. Navigate to the **Common Tasks** section, select the **Rule Run Framework**, and then select **Process**.
3. Select **IPEEndBatchProcess** from the table list and click **Edit**.
4. Click **Component** in the new window.
5. Expand **Transformation Rules** from **Available Components**.
6. Click **Database Functions-Transformations** and expand it.
7. Move **F_TRUNC_RTI_ASSMNT_TABLES** to the right into Tasks in **ROOT**.
8. Click **OK** and **Save**.

7.6 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 the icon to expand the page.
6. Select the batch you want to run and click Fire Run. The Fire Run page is displayed.
7. On the Fire Run page, provide the required values. If the **IPEKYCRun** daily batch is selected, then provide the following values in **Parameters** option.

   ```
   [MODELID]=PROD,[VERSION]=0,[APP_ID]=OFS_KYC
   ```

8. Click **OK**.

7.7 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** icon. The **Task Mapping** window is displayed.
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**. A warning message is displayed.
9. Click **OK**.
10. Click **Execute Batch**.

7.8 Scheduling a Batch

This section describes how to schedule a batch.

Topics:

7.8.1 Scheduling a Batch Once

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

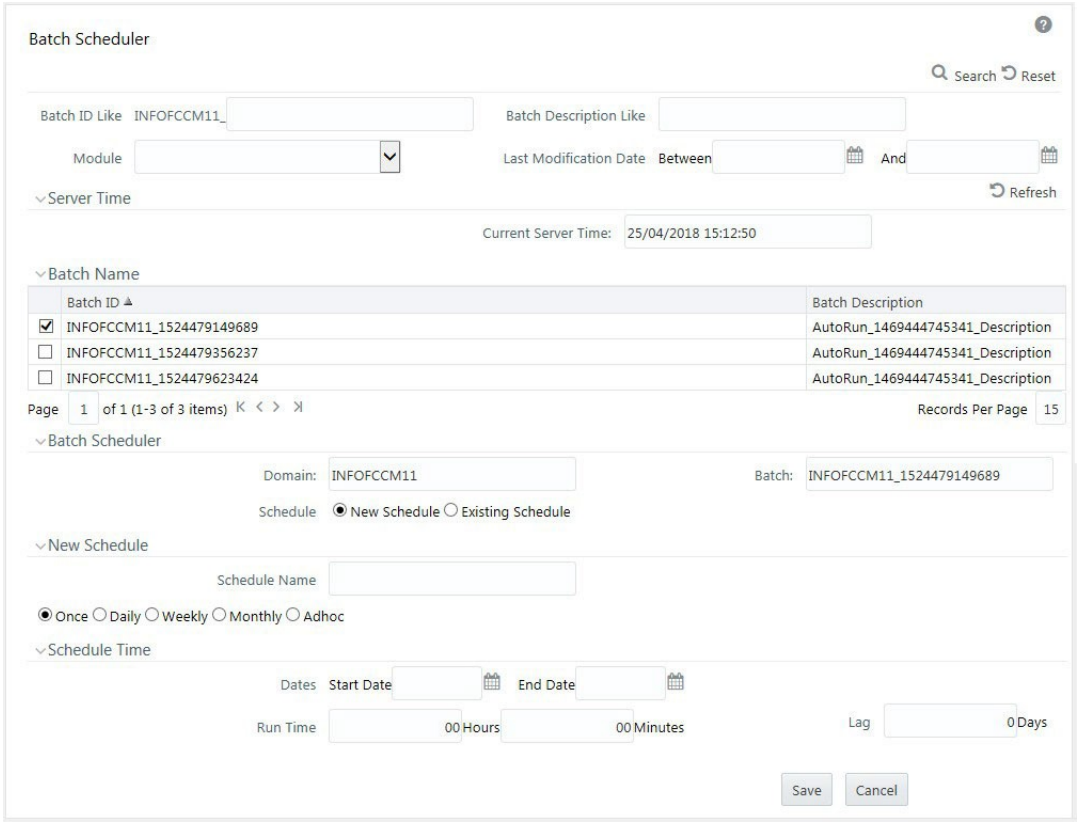
To schedule a batch that you want to run only once, follow these steps:

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.
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 6: Batch Scheduler Filter Fields

Figure 7-1 Batch Scheduler Filter Field



9. Click **Save**.

7.8.2 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**.

7.8.3 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**.

7.8.4 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** .

7.8.5 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 the **Plus** icon. A new row is added in the **Schedule Time** section.
9. Provide the information date, run date, and run time.
10. Click **Save**.

7.8.6 KYC Batch Execution Logs

Logs are created only after the batches are executed. Batch Execution Logs are based on the types of rules.

The following sections describe the types of tasks present in the batches:

- Table 2 Table (T2T)
- Transform Data (Data Transformation or DT Logs)
- Promote to Case

7.8.6.1 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 7-4 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.

7.8.6.2 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 available in the path:

```
<FIC_HOME>/ficdb/log/
```

Table 7-5 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.

7.8.6.3 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:

8.1 User Authentication

Only a valid user with the required user roles will b allowed to post a KYC Onboarding request.

To allow a user to post a KYC Onboarding request, the following authorizations are done by the system:

1. As a first check, authentication is done to check if the user ID and password is valid in the system. Authentication can be Basic Authentication or Bearer Token (Token based authentication).

   For more information on how to generate the Bearer Token, see Appendix-E: Configurations for the Bearer Token.

2. Secondly, authorization is done to check if user has **WFACCNEXE** and **WFACC** roles.

   If the user belongs to **OB KYC Administrator Group**, by default **WFACCNEXE** and **WFACC** roles are assigned.

8.2 Populating Country Data in KDD_CODE_SET_TRNLN Table

> **Note**
>
> Ignore this step if it is already performed during the use 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;
```

8.3 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.

8.3.1 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**.

   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

8.3.1.1 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 8-1 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. The following table shows the three applicable parameters and their corresponding values.

Table 8-1 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.

8.3.2 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**.

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

   - AAI Authorization Service
   - Process Modeling Framework

8.3.2.1 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:

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 any service apart from the AAI Authorization Service, update the service username in the **Service Username** field with a valid KYC Administrator Username.
4. For any service apart from the AAI Authorization Service, update the service password in the **Service Password** field with a valid KYC Administrator password.
5. Click **Save** to save the details.

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

8.4 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.

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.

8.5 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**, and 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.
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**.

8.6 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.

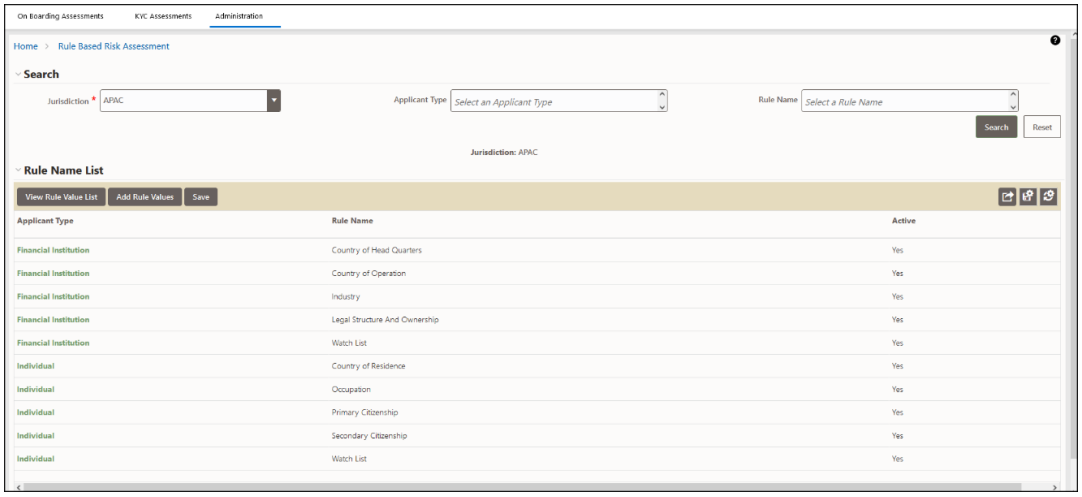
To view the UI, follow these steps:

1. Log in to the KYC application. For more information, see.
2. Click **Behavior Detection - KYC**.
3. Select **Manage KYC OB Configuration** and click **Rule-Based Assessment**.

   The **Rule-based risk assessment** UI appears with the **Search** section displayed.
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 7: Rule Name List Image16

Figure 8-2 Rule Name List



8.6.1 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**.

8.6.2 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**.

8.7 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.

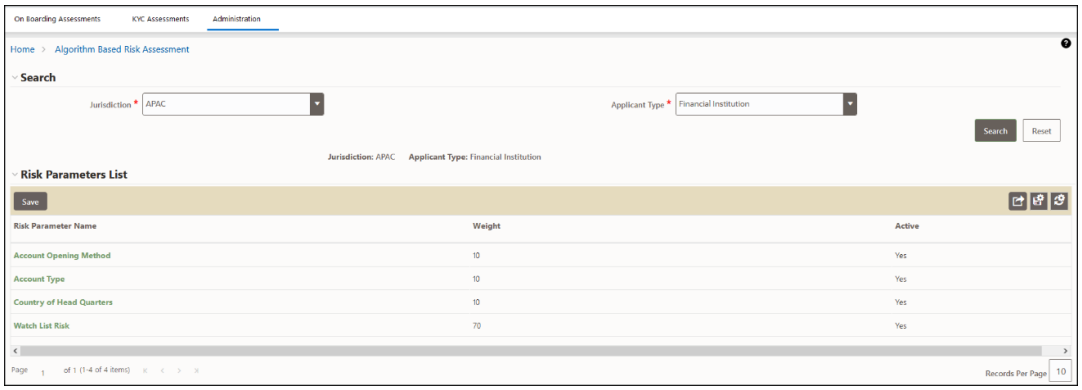
2. Click **Behavior Detection - KYC**. Select **Manage KYC OB Configuration** and click **Algorithm Based Assessment**.

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

Figure 8-3 Search Fields

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

Figure 8-4 Risk Parameters List



8.7.1 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.

8.7.2 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** .

8.8 Modifying the Risk Scores and Viewing the Risk Categories

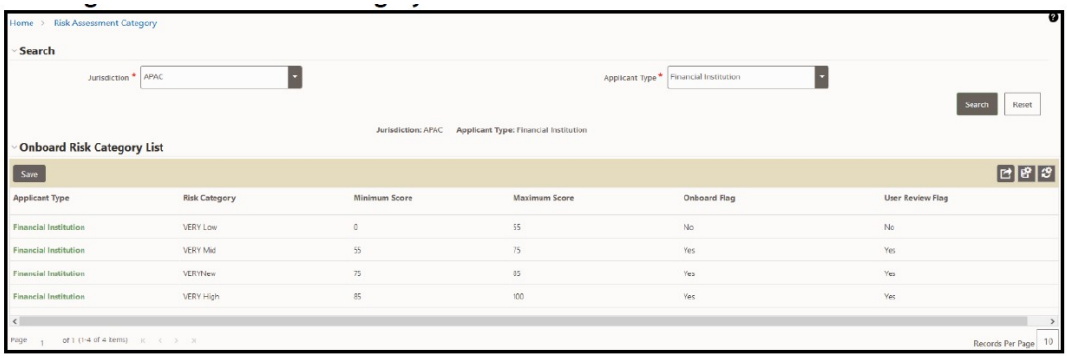
Use the Risk Assessment Category UI to modify the risk scores and view the risk category assigned for a jurisdiction and applicant type.

To view the UI, follow these steps:

1. Log in to the KYC application. For more information, see.
2. Click **Behavior Detection - KYC**.
3. Select **Manage KYC OB Configuration** and click **Risk Assessment Category**.

   The **Risk Assessment Category UI** appears with the **Search** section displayed.
4. Select the jurisdiction and applicant type of risk assessment.

Figure 8-5 Onboard Risk Category List



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

8.8.1 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 more than zero. The maximum score of the last row must always be 100.

8.8.1.1 Mapping KYC Rules to Customer Evaluation Names

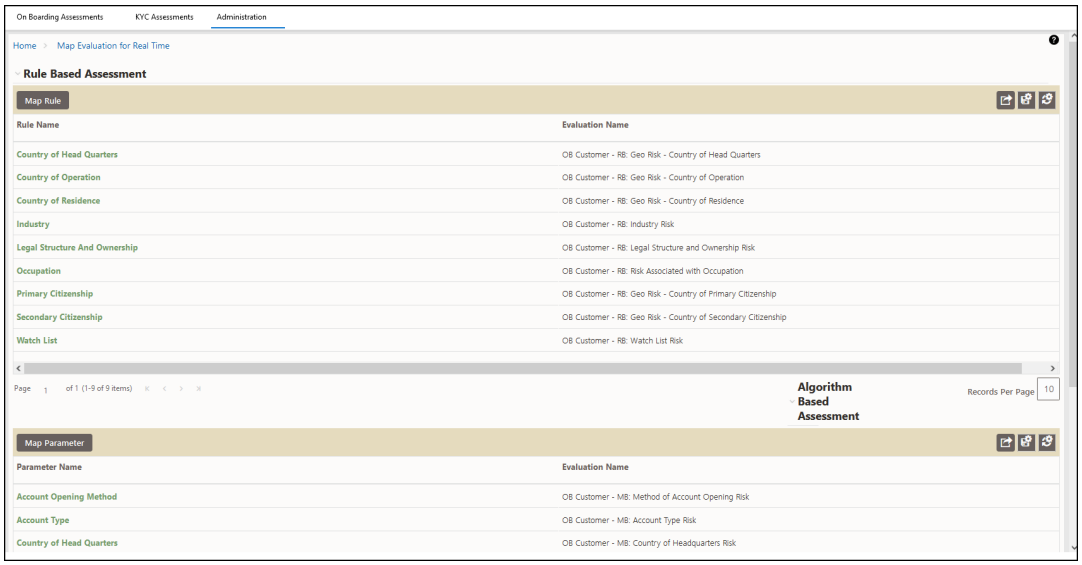
Use the Map Evaluation for Real Time UI to map the rule name or the parameter name from the Excel template to the evaluation name provided by the customer.

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 8-6 Rule Based Assessment Section



8.8.1.2 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.
2. Select the rule and the associated evaluation name which needs to be mapped to the rule.
3. Click **Save**.

8.8.1.3 Mapping Parameters to Evaluations

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

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

8.8.1.3.1 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**.
3. 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.

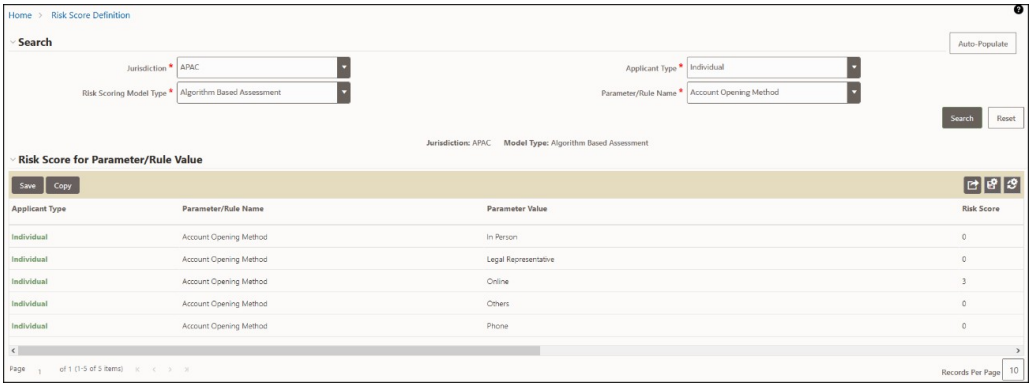
   - **Applicant Type** : The applicant type can be Individual, Financial Institution, or Organization. These values are populated from the `kdd_code_set_trnln` table.

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

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

     > **Note**
     >
     > – The applicant types appear only after you select a model type
     > – The Parameter/Rule names appear only after you select an applicant type.

Figure 8-7 Search Fields



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, a confirmation message is displayed when you click **Auto- Populate**.

8.8.1.4 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**.
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**.

8.9 Modifying and Adding the Mapping Codes within KYC

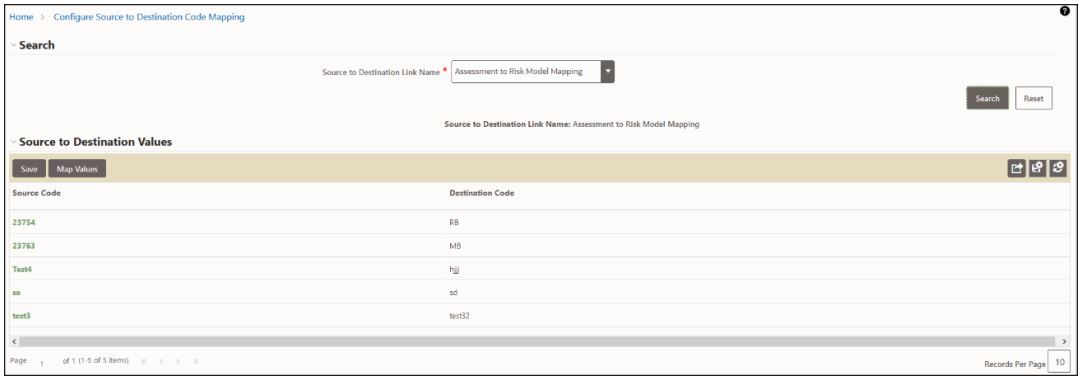
Use the Configure Source to Destination Code Mapping menu UI to view the mappings from source to destination.

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 8-8 Search Fields



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

8.9.1 Downloading the Code Values

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

8.9.1.1 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**.

8.9.2 Adding New Code Values

To add new code values, follow these steps:

1. Click **Map Values**.
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:

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.
- 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 more information, see the Inline Processing Engine (IPE) guides.

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 the icon to expand the page.
5. Click **Algorithm Based Risk Assessment**.

   The **Algorithm Based Risk Assessment** page appears.
6. To add a new parameter, click **Add Parameter**.

   The **Add New Parameter** dialog box displays.

Table 9-1 Add New Parameter 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.
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 `kdd_code_set_trnln` table display.
Customer Type	Select the customer type. Based on the customer type, the parameter is displayed in the Individual, Other Organization, or Financial Institution tabs.
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.
Re-review Rule Name	Enter the value `APPLN_REREVIEW_PARAMS`.
Comments	Enter any comments related to the parameter.

7. 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.

8. On the KYC home page, click **Financial Services Inline Processing Engine** in the **Common Tasks** tab.
9. 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 Inline Processing Engine User Guide.
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**.

c. Click **Add**.

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

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

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

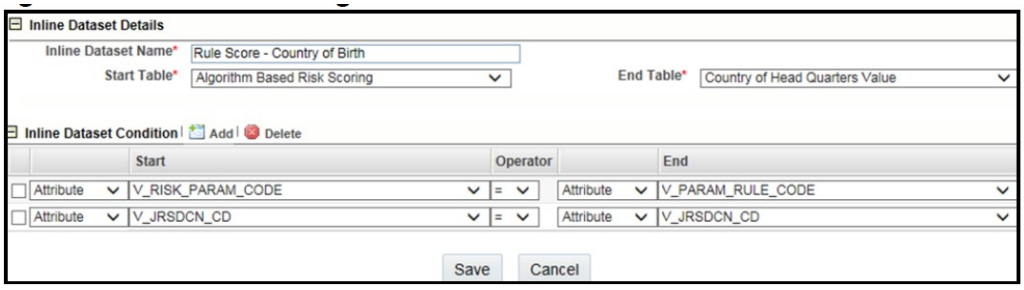
a. On the Inline Datasets page, click **Add**.

b. Enter a name for the inline dataset.

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

d. In the **End Table** field, select **Country of Head Quarters Value**.

Figure 9-1 Inline Datasets Page



e. Click **Add**.

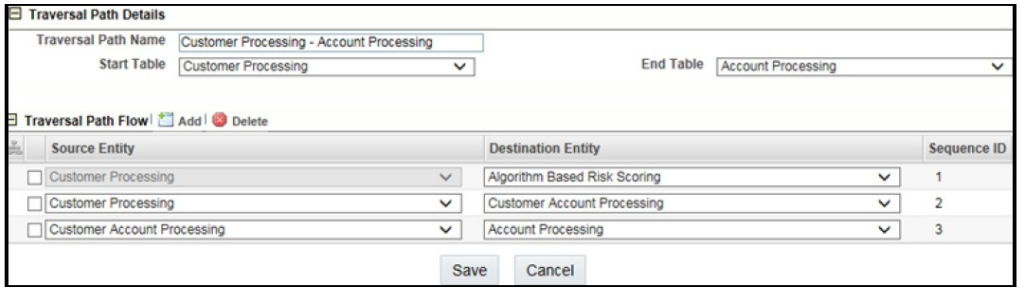
f. Select the values for the dataset condition as shown in the above figure.

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.

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 9-2 Traversal Paths Page



    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 Inline Processing Engine 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.

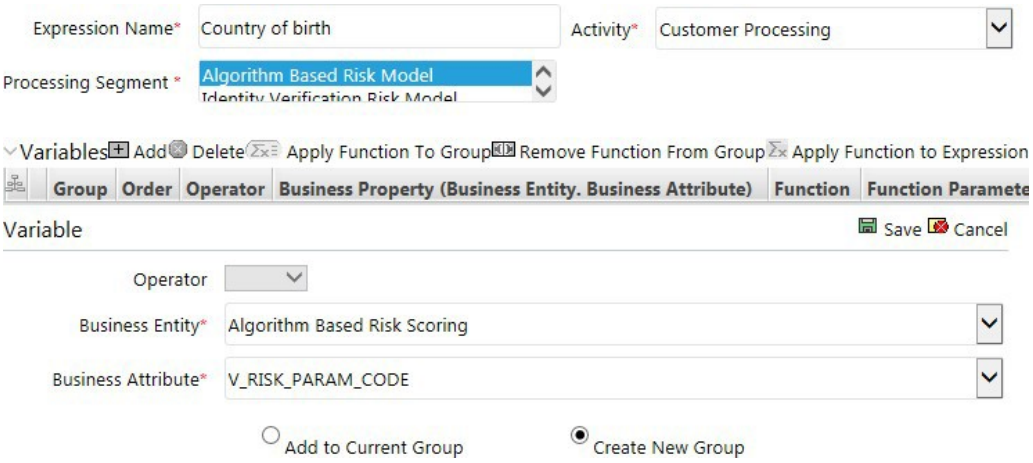
To add an expression, follow these steps:

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 9-3 Expressions Page - First Expression



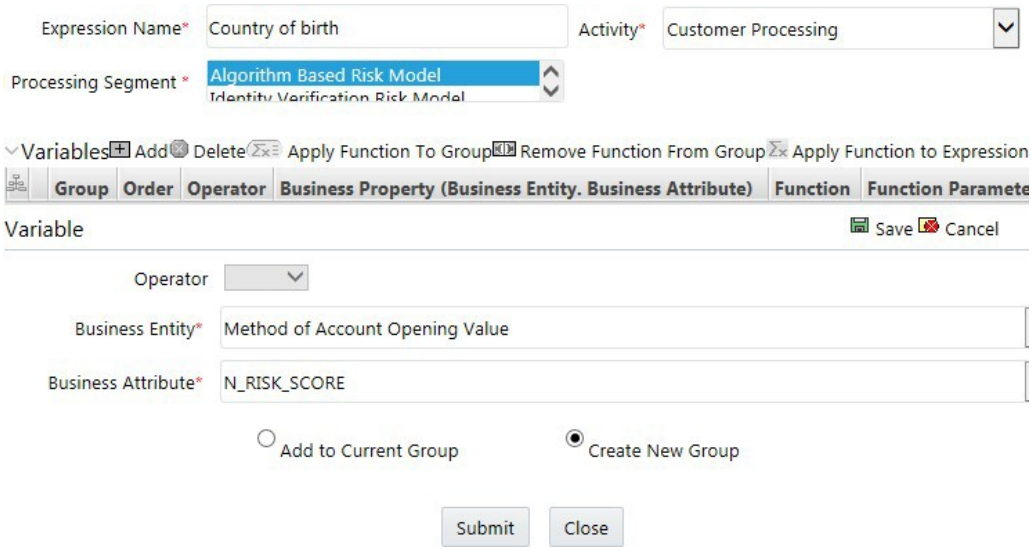
d. To add a variable for the first expression, click **Add**.

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.

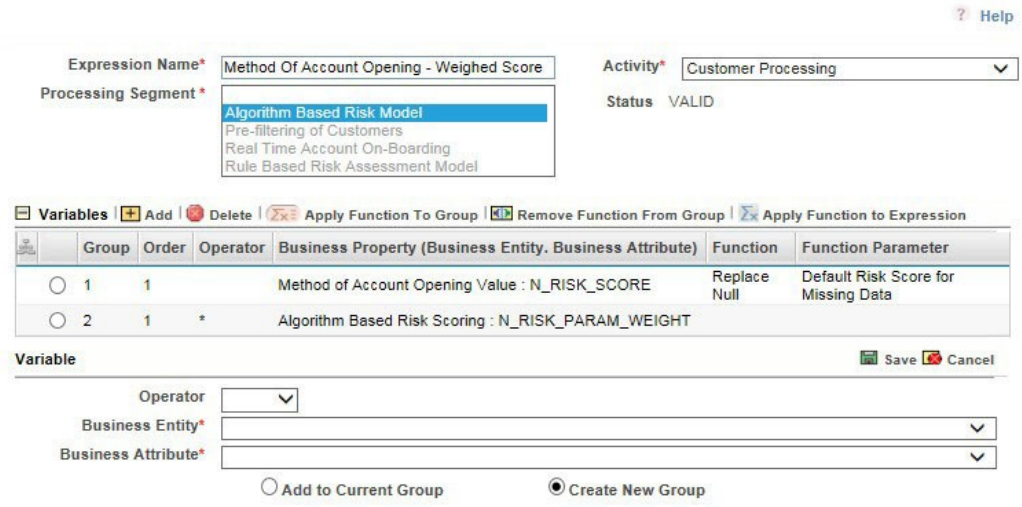
Figure 9-4 Expressions Page - Second Expression



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 9-5 Expressions Page - Displayed Values



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.

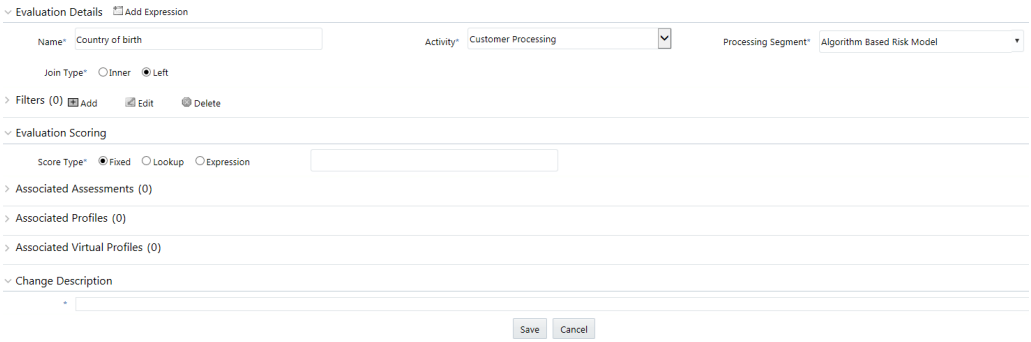
    b. On the **Evaluations** page, click **Add**.

    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.

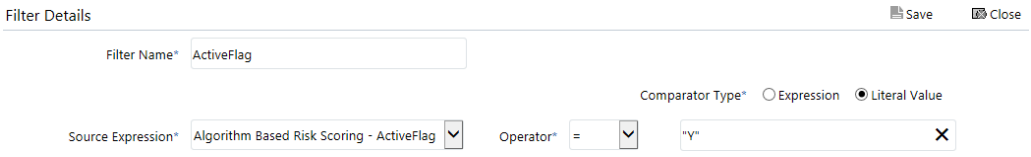
Figure 9-6 Evaluations Details



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**.

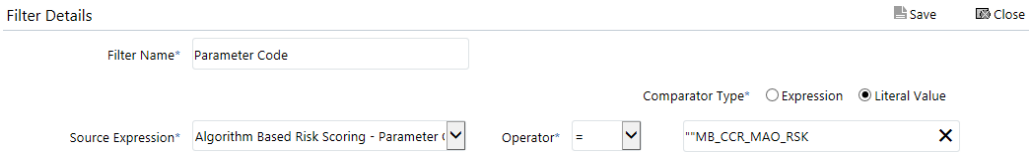
Figure 9-7 Filter Details - First Expression



> **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 9-8 Filter Details - First Filter



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

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

i. Select the expression 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.

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_AP- P_ID, V_EVAL_NM, V_ACTV_FL,
V_PARAM_RULE_CODE, V_CUST_TYPE_CD
```

Table 9-2 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**. Click **KYC Risk Assessment Configuration**.
3. Click the **Expand** icon to expand the page.
4. Click **Rule Based Risk Assessment**. The **Rule Based Risk Assessment** page appears.
5. To add a new rule, click **Add Rule**. The **Add New Rule** dialog box is displayed.

Table 9-3 Add 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.
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 `kdd_code_set_trnln` table display.

Table 9-3 (Cont.) Add New Rule Fields

Field Name	Description
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 **APPLN_REREVIEW_PARAMS**.
Comments	Enter any comments related to the rule.

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

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

7. 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.

8. To define a rule, follow these steps:
   a. 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:
   b. Click the **Business Entities** sub-menu in the Association and Configuration menu.
   c. Select the Entity Name as **PARAM_RISK_SCORE_JRSDN**.
9. Click **Add**.
10. 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 N_RISK_SCORE** as the set score attribute. Segment and **N_RISK_SCORE** as the set score attribute.

11. Click **Add**. The new parameter is added to the list of Business Entities on the **Business Entities** page.
12. 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.
    e. Click **Add**.
    f. Select the values for the dataset condition as shown in the figure.
    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.

13. 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**.
    c. Enter a name for the traversal path.
    d. In the **Start Table** field, select **Customer Processing**.
    e. In the **End Table** field, select **Rule-Based Risk Assessment**.
    f. Click **Add**.
    g. Select the values for the traversal path flow as shown in the figure.
    h. Click **Save**. The new path is added to the list of traversal paths on the Traversal Paths page.

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.

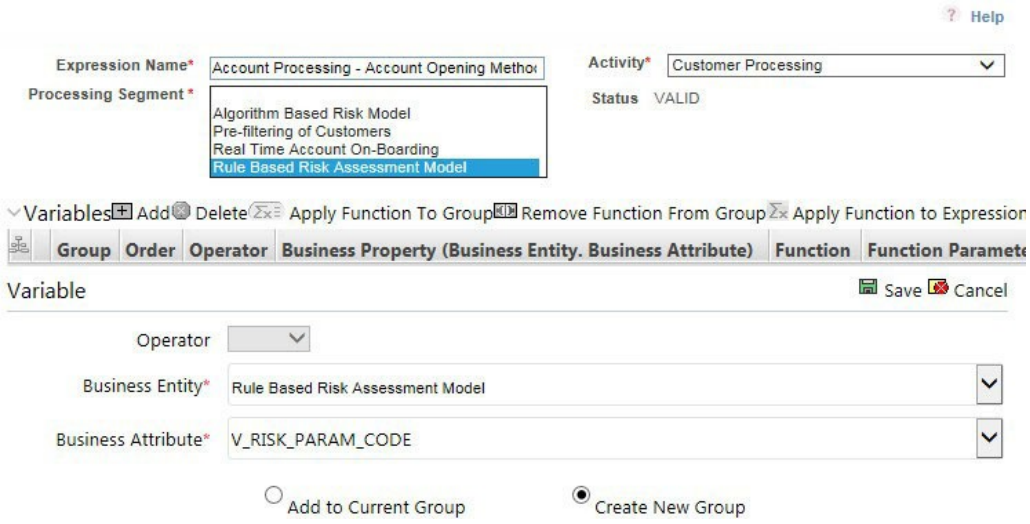
To add an expression, follow these steps:

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 9-9 Expressions Page – First Expression



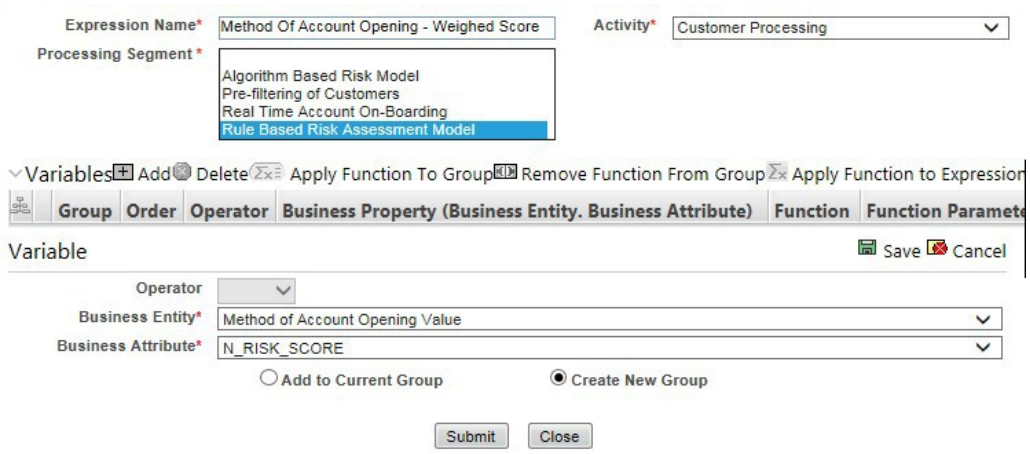
d. To add a variable for the first expression, click **Add**.

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.

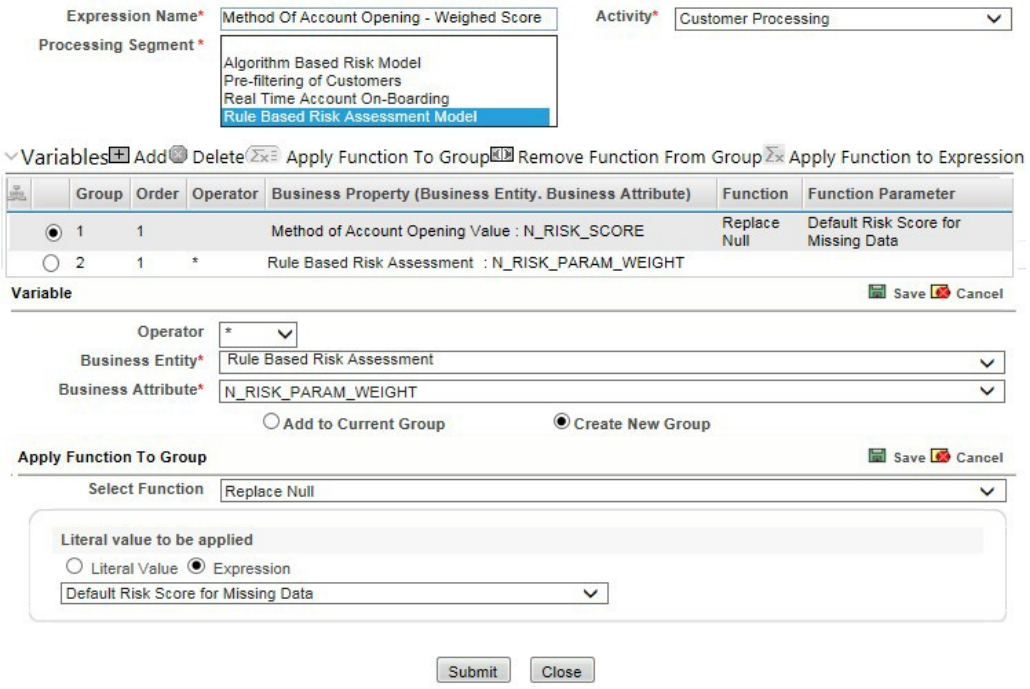
Figure 9-10 Expressions Page – Second Expression



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 9-11 Expression Function

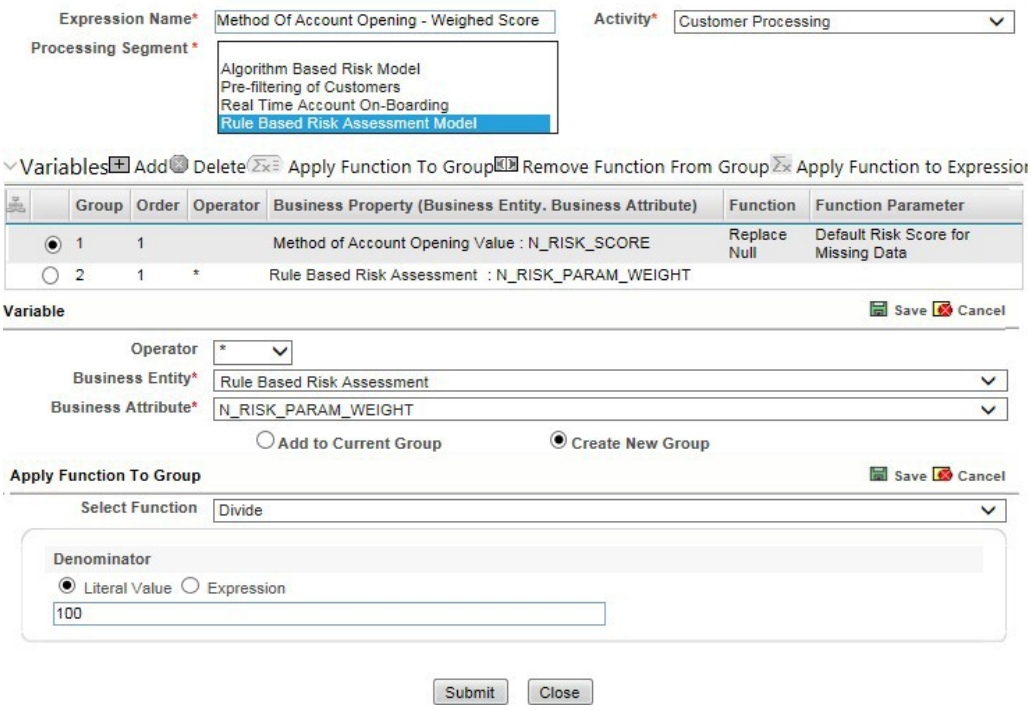


j. Select the **Group 1** radio button.

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 26: Expression Function img54

Figure 9-12 Literal Value Function

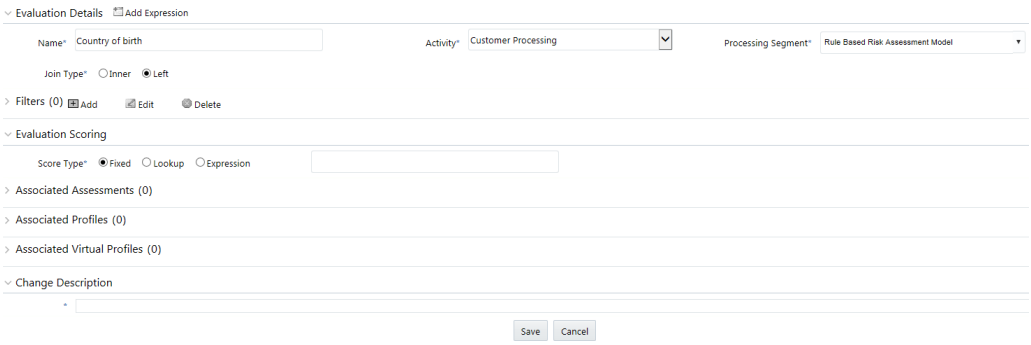


m. Select the **Group 1** radio button.

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 9-13 Evaluation Details



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**.

c. Enter a name for the evaluation.

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

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

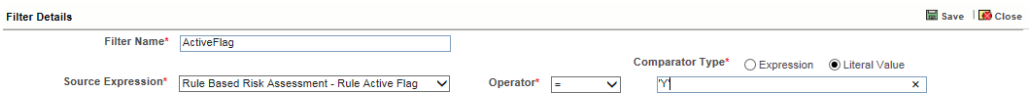
e. To add filters for the evaluation, click

> **Note**
>
> Add

. You need to add two filters.

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

Figure 9-14 Filter Details – First Filter

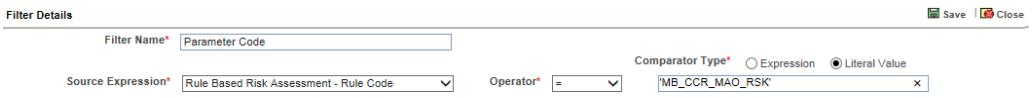


> **Note**
>
> In the Literal Value field, select the same value as provided in the `F_ENABLE` parameter of the `APPLN_RB_PROCESSING` excel sheet during upload.

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

> **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.

Figure 9-15 Filter Details – First Filter



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**.

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

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

The following table shows the expected values for the above script.

Table 9-4 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

17. 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

Topics:

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

Table 9-5 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.
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.
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.

Table 9-5 (Cont.) Add a New Rule Fields

Field Name	Description
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.

5. 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:

1. On the KYC home page, click KYC Risk Assessment Configuration.
2. Click **Association of Rule/Risk Parameter to Evaluation**. The **Map Evaluation** page is displayed.
3. Select the **Model Type** as **Accelerated Re-review Based Assessment**.
4. Click **Go**. The Association of Rule/Risk Parameter to Evaluation grid is populated with the available evaluations.
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. **Click KYC Risk Assessment Configuration.**
2. Click **Risk Score for Parameter/Rule Value**. The **Risk Score for Parameter/Rule Value** page is displayed.
3. Select the jurisdiction, model type used for risk scoring, and the parameter or rule name.
4. Click **Go**. The risk scores are displayed on the page.

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

5. Click **Auto-Populate** to generate the risk scores following the risk assessment. To change the risk score, select the check box of the parameter 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.

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

   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.

9.5 Performing Assessments on Interested Parties

> **Note**
>
> Ensure that you perform the following configuration for all relationship types before running batch 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 **KYC Risk Assessment Configuration** and click **Relationship Type Definition**. The Relationship Type Definition UI is displayed.
3. In the **Search** section, select the jurisdiction. Click **Go**.
4. In the **Default Assessment Mode** section, Select the risk assessment type that you want to perform on any interested parties and click **Save**.

> **Note**
>
> - For Interested Parties, the Default Assessment Mode is performed when a particular assessment mode for a relationship type is not explicitly configured in the Relation Type Definition UI.
> - For Primary customer, the Default Assessment Mode is always FULL_KYC.

5. Based on the jurisdiction selected, the Relationship Type List displays all configured relationship types and their respective assessment modes.

To add a new Relationship Type, follow these steps:

1. Click **Add** under the **Relationship Type List** 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 change the Assessment Mode of a Relationship Type:

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

10

Simulation Capability

The OFS KYC Simulation capability allows the user to run & test effectiveness of KYC risk assessment model(s) in a sandbox environment. User can tune the configurations (i.e. threshold weights and scores for risk parameters) for respective jurisdictions, analyze the results of each simulation run including comparison against production data and decide on the right champion model to be deployed back to production.

The KYC Simulation capability is available via integration with OFS Compliance Studio Application. This allows the user to seamlessly replicate and test the KYC risk assessment model in a dedicated sandbox environment without impacting the production set up. The Sandbox workspace allows the user to import required dataset from the production environment, perform simulation and analyze results using built in GUI and visualization tool.

Topics:

10.1 Integrating With Compliance Studio

OFS Compliance Studio is an advanced analytics application that supercharges anti-financial crime programs for better customer due diligence, transaction monitoring, and investigations by leveraging the latest innovations in artificial intelligence, open-source technologies, and data management. It combines Oracle's Parallel Graph Analytics (PGX), Machine Learning for AML, Entity Resolution, and notebook-based code development and enables Contextual Investigations in one platform with complete and robust model management and governance functionality.

For information on installation and configuration of the Compliance Studio application, see Oracle Financial Services Compliance Studio Installation Guide.

For the following information, see Oracle Financial Services Compliance Studio User Guide:

- Using the Application UI
- Mapping User Groups
- Access the Workspace Dashboard Window

- Using the OFS Compliance Studio Application
- Using Workspaces
- Managing Datasets
- Managing Model Pipelines

10.2 KYC Simulation Process Flow

The process flow for building KYC models in Compliance Studio involves the configuration, creation of Sandboxes and the creation of Models mapped to the Sandboxes. You can use these KYC models to perform model visualizations and test for the outcomes. You can then publish a model into production and make it available to users after you have determined that the models and the parameters used to construct the models meet the requirements of your business logic.

Figure 10-1 User Process Flow

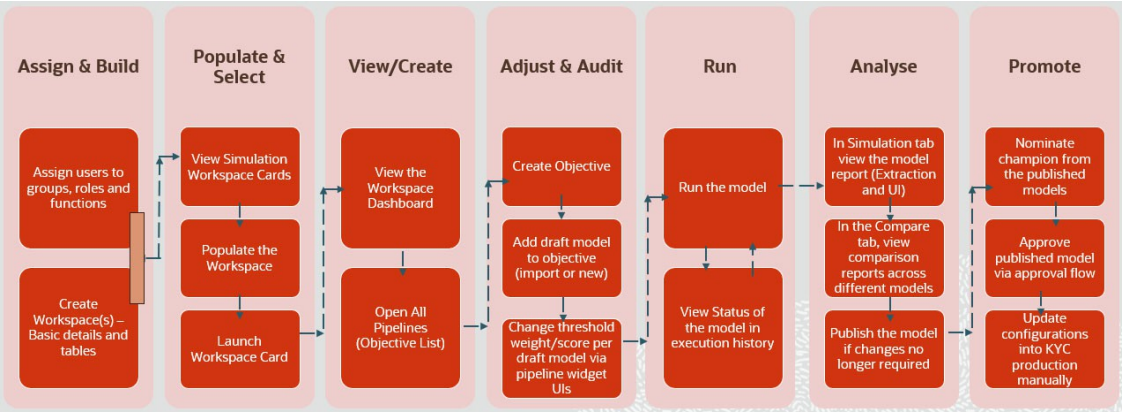
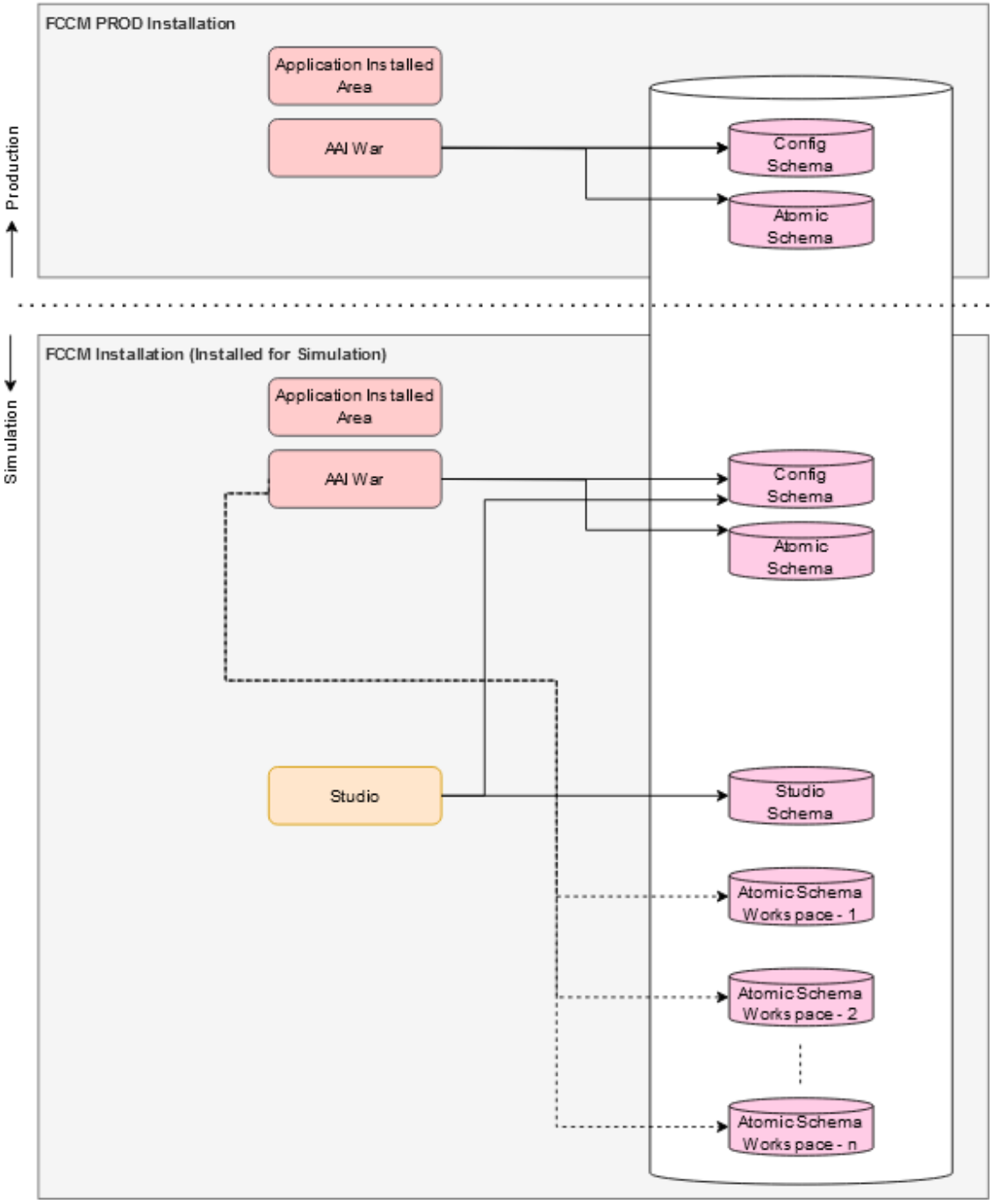


Figure 10-2 Simulation Data Process Flow



10.2.1 Configuring KYC in Compliance Studio

To configure KYC in Compliance Studio, follow these steps:

1. Execute the following script in Compliance Studio schema:

```
insert into mmg_app_menu_mapping(V_APP_ID,V_MENU_CODE) select
'KYC',V_MENU_CODE from MMG_MENU;
```

10.3 Registering the OFSAA Environment Details with Compliance Studio

This section describes how to register the OFSAA Environment details with Compliance Studio.

To Register the OFSAA Environment details with Compliance Studio, follow these steps:

1. Click the **User Icon** and select the **OFSAA Environment** from the list.
2. Click **Register Environment**. The OFSAA Environment page is displayed.
3. Click **Register Environment** to register the new KYC Environment.
4. Provide input for the following fields:
   - **Name** : Name of the environment Must be minimum 5 characters and maximum 20 characters
   - **Description** : Description for the environment
   - **Type** : Select either simulation or production
   - **Properties** : Select the key and enter the corresponding value. For information on Key and their description, see the following tables.
5. Click **Create**.

Table 10-1 OFSAA Production Environment Key and Description

Key	Description
PROD_baseUrl	BD Production URL. For example: http://<ipadress>:<portno>/<context>
PROD_app_id	BD Production Application ID. For example: OFC_KYC
PROD_infodom	BD Production Setup infodom.
PROD_ficserver_hostname	Hostname of Linux machine where the BD application is installed.
PROD_ficserver_username	Username to access the BD application. For example: ofsaaweb
PROD_ficserver_password	Password to access the BD application.
PROD_ftpshare_path	Path of FTPshare location where the BD application is installed. For example: /scratch/ofsaaweb/812FEB/ftpshare
PROD_instanceName	Name of Production Instance which is used to generate the token. For example: MMG1
PROD_instanceAccessToken	Access Token for Production Instance.

Table 10-2 OFSAA Simulation Environment Key and Description

Key	Description
SIM_ficserver_hostname	Hostname of Simulation Server where the BD application is installed.
SIM_ftpshare_path	Path of Simulation FTPshare location where the BD application is installed.
SIM_sys_admin_user	Admin Username to access the Simulation Server.

Table 10-2 (Cont.) OFSAA Simulation Environment Key and Description

Key	Description
SIM_sys_auth_user	Authorized Username to access the Simulation Server.
SIM_ficserver_username	Username to access the BD application.
SIM_ficserver_password	Password to access the BD application.
SIM_instanceName	Name of Production Instance which is used to generate the token.
SIM_instanceAccessToken	Access Token for Production Instance.
SIM_baseUrl	BD Simulation URL.
SIM_app_server	BD Simulation Application Server IP.
SIM_ficdb_path	Path of Simulation FICDB location where the BD application is installed.

10.3.1 Workspace Creation Pre-requisites

The following are the pre-requisites for creating a workspace:

1. Create User TableSpace in simulation database by executing the script as a *sysdba* user:

   ```
   CREATE TABLESPACE AIF_USER_TS DATAFILE '<DATAFILE PATH>/
   aif_user_data_tablespace.dbf' SIZE 1G REUSE AUTOEXTEND ON NEXT 500M
   MAXSIZE UNLIMITED;
   ```

   DATAFILE PATH example: `/scratch/oraofss/app/oradata`.

2. Create Instance Token for Production and Simulation in the KYC application.

   For more information on Instance Token, see Appendix-E: Configurations for the Bearer Token.

10.4 Configuring New User Schema

This section describes how to create a new user schema in the `sys user`.

To create the new user, follow these steps:

1. Run the following SQL statements in simulation as `sys user`:

   ```
   CREATE USER <New Workspace Schema> IDENTIFIED BY <password> DEFAULT
   TABLESPACE
   AIF_USER_TS TEMPORARY TABLESPACE TEMP QUOTA UNLIMITED ON AIF_USER_TS;
   grant create SESSION to <New Workspace Schema>;
   grant create PROCEDURE to <New Workspace Schema>;
   grant create SEQUENCE to <New Workspace Schema>;
   grant create TABLE to <New Workspace Schema>;
   grant create TRIGGER to <New Workspace Schema>;
   grant create VIEW to <New Workspace Schema>;
   grant create MATERIALIZED VIEW to <New Workspace Schema>;
   grant select on SYS.V_$PARAMETER to <New Workspace Schema>;
   grant create SYNONYM to <New Workspace Schema>;
   grant select on sys.v_$parameter to <New Workspace Schema>;
   grant select on sys.dba_free_space to <New Workspace Schema>;
   grant select on sys.dba_tables to <New Workspace Schema>;
   ```

```
grant select on sys.Dba_tab_columns to <New Workspace Schema>;
grant create RULE to <New Workspace Schema>;
grant create any trigger to <New Workspace Schema>;
grant drop any trigger to <New Workspace Schema>;
grant select on SYS.DBA_RECYCLEBIN to <New Workspace Schema>;
grant connect, resource, dba to <new workspace schema>;
```

2. Once the user is created, run the following SQL statements in new workspace schema user created:

   a.
   ```
   CREATE OR REPLACE EDITIONABLE SYNONYM PR2_FIRERUN_FILTER FOR
   <<config_schema>>.PR2_FIRERUN_FILTER;
   CREATE OR REPLACE EDITIONABLE SYNONYM PR2_RUN_EXECUTION_FILTER FOR
   <<config_schema>>.PR2_RUN_EXECUTION_FILTER;
   CREATE OR REPLACE EDITIONABLE SYNONYM AAI_WF_FILTER_EXEC_MAP FOR
   <<config_schema>>.AAI_WF_FILTER_EXEC_MAP;
   CREATE OR REPLACE EDITIONABLE SYNONYM CONFIGURATION FOR
   <<config_schema>>.CONFIGURATION;
   CREATE OR REPLACE EDITIONABLE SYNONYM PR2_RUN_EXECUTION_B FOR
   <<config_schema>>.PR2_RUN_EXECUTION_B;
   CREATE OR REPLACE EDITIONABLE SYNONYM METADATA_ELEMENT_MASTER FOR
   <<config_schema>>.METADATA_ELEMENT_MASTER;
   CREATE OR REPLACE EDITIONABLE SYNONYM RTI_EVALUATION FOR
   <<config_schema>>.RTI_EVALUATION;
   CREATE OR REPLACE SYNONYM checkenvfordataredaction FOR
   <<config_schema>>.checkenvfordataredaction;
   CREATE OR REPLACE SYNONYM cssms_role_mast FOR
   <<config_schema>>.cssms_role_mast;
   CREATE OR REPLACE SYNONYM cssms_group_role_map FOR
   <<config_schema>>.cssms_group_role_map;
   CREATE OR REPLACE SYNONYM cssms_usr_group_map_view FOR
   <<config_schema>>.cssms_usr_group_map_view;
   CREATE OR REPLACE SYNONYM AAI_DB_PROPERTY FOR
   <<config_schema>>.AAI_DB_PROPERTY;
   CREATE OR REPLACE SYNONYM CONFIGURATION FOR
   <<config_schema>>.CONFIGURATION;
   CREATE OR REPLACE SYNONYM AAI_DB_DETAIL FOR
   <<config_schema>>.AAI_DB_DETAIL;
   CREATE OR REPLACE SYNONYM DSNMASTER FOR <<config_schema>>.DSNMASTER;
   CREATE OR REPLACE EDITIONABLE SYNONYM CSSMS_USR_PROFILE FOR
   <<config_schema>>."CSSMS_USR_PROFILE";
   ```

   b. Execute the following from SYSDB:

   ```
   grant select on <<config_schema>>.PR2_RUN_MAP to <SCHEMA_NAME>;
   grant insert on <<config_schema>>.PR2_RUN_MAP to <SCHEMA_NAME>;
   grant insert on <<config_schema>>.PR2_RUN_OBJECT_MEMBER to
   <SCHEMA_NAME>;
   grant select on <<config_schema>>.PR2_FIRERUN_FILTER to <SCHEMA_NAME>;
   grant select on <<config_schema>>.AAI_DB_PROPERTY to <SCHEMA_NAME>;
   grant select on <<config_schema>>.CONFIGURATION to <SCHEMA_NAME>;
   grant select on <<config_schema>>.DSNMASTER to <SCHEMA_NAME>;
   grant select on <<config_schema>>.AAI_DB_DETAIL to <SCHEMA_NAME>;
   grant select on <<config_schema>>.CSSMS_HOLIDAY_LIST to <SCHEMA_NAME>;
   grant select on <<config_schema>>.rti_evaluation to <SCHEMA_NAME>;
   grant select on <<config_schema>>.pr2_run_object_member to
   ```

```
<SCHEMA_NAME>;
grant select on <<config_schema>>.pr2_run_map to <SCHEMA_NAME>;
grant select on <<config_schema>>.PR2_FILTERS to <SCHEMA_NAME>;
grant select on <<config_schema>>.pr2_run_object to <SCHEMA_NAME>;
grant select on <<config_schema>>.PR2_RUN_EXECUTION_FILTER to
<SCHEMA_NAME>;
grant select on <<config_schema>>.CONFIGURATION to <SCHEMA_NAME>;
grant select on <<config_schema>>.AAI_WF_FILTER_EXEC_MAP to
<SCHEMA_NAME>;
grant select on <<config_schema>>.PR2_RUN_EXECUTION_B to <SCHEMA_NAME>;
grant select on <<config_schema>>.metadata_element_master to
<SCHEMA_NAME>;
grant execute on <<config_schema>>.checkenvfordataredaction to
<SCHEMA_NAME>;
```

c.
```
CREATE OR REPLACE FORCE EDITIONABLE VIEW PR2_RUN_MAP ("V_RUN_ID",
"V_INFODOM_NAME", "V_TASK_REF_UNIQUE_NAME", "V_OBJECT_UNIQUE_NAME",
"V_MEMBER_UNIQUE_NAME") AS
SELECT V_RUN_ID,
V_INFODOM_NAME,
V_TASK_REF_UNIQUE_NAME,
V_OBJECT_UNIQUE_NAME,
V_MEMBER_UNIQUE_NAME
FROM <<config_schema>>.PR2_RUN_MAP PRM
WHERE PRM.V_INFODOM_NAME = '<<WORKSPACE_INFODOM>>';
```

d.
```
CREATE OR REPLACE FORCE EDITIONABLE VIEW PR2_RUN_OBJECT ("V_RUN_ID",
"V_INFODOM_NAME", "V_OBJECT_UNIQUE_NAME", "V_OBJECT_TYPE_CODE",
"V_OBJECT_LOCATION_CODE", "N_OBJECT_ORDER", "V_TASK_REF_UNIQUE_NAME",
"V_TASK_TYPE_CODE", "V_TASK_SUB_TYPE_CODE", "V_TASK_REF_1_NAME",
"V_TASK_REF_1_VALUE", "V_TASK_REF_2_NAME", "V_TASK_REF_2_VALUE",
"V_TASK_REF_3_NAME", "V_TASK_REF_3_VALUE", "V_TASK_REF_4_NAME",
"V_TASK_REF_4_VALUE") AS
SELECT V_RUN_ID,
V_INFODOM_NAME,
V_OBJECT_UNIQUE_NAME,
V_OBJECT_TYPE_CODE,
V_OBJECT_LOCATION_CODE,
N_OBJECT_ORDER,
V_TASK_REF_UNIQUE_NAME,
V_TASK_TYPE_CODE,
V_TASK_SUB_TYPE_CODE,
V_TASK_REF_1_NAME,
V_TASK_REF_1_VALUE,
V_TASK_REF_2_NAME,
V_TASK_REF_2_VALUE,
V_TASK_REF_3_NAME,
V_TASK_REF_3_VALUE,
V_TASK_REF_4_NAME,
V_TASK_REF_4_VALUE
FROM <<config_schema>>.PR2_RUN_OBJECT PRO
WHERE PRO.V_INFODOM_NAME = '<<WORKSPACE_INFODOM>>';
```

e.
```
CREATE OR REPLACE FORCE EDITIONABLE VIEW PR2_RUN_OBJECT_MEMBER
("V_RUN_ID", "V_INFODOM_NAME", "V_OBJECT_UNIQUE_NAME",
```

```
"V_MEMBER_UNIQUE_NAME", "V_MEMBER_TYPE_CODE", "N_MEMBER_ORDER") AS
SELECT V_RUN_ID,
V_INFODOM_NAME,
V_OBJECT_UNIQUE_NAME,
V_MEMBER_UNIQUE_NAME,
V_MEMBER_TYPE_CODE,
N_MEMBER_ORDER
FROM <<config_schema>>.PR2_RUN_OBJECT_MEMBER PROM
WHERE PROM.V_INFODOM_NAME = '<<WORKSPACE_INFODOM>>';
```

f.
```
CREATE OR REPLACE FORCE EDITIONABLE VIEW PR2_FILTERS ("F_IS_RRF",
"V_DSN_NAME", "V_EXECUTION_ID", "V_TASK_ID", "V_COMPONENT_CODE",
"N_RUN_SKEY", "V_RUN_CODE", "V_RULE_CODE", "V_FILTER") AS
SELECT FILTERS.F_IS_RRF,
FILTERS.V_DSN_NAME,
FILTERS.V_EXECUTION_ID,
FILTERS.V_TASK_ID,
FILTERS.V_COMPONENT_CODE,
FILTERS.N_RUN_SKEY,
FILTERS.V_RUN_CODE,
FILTERS.V_RULE_CODE,
FILTERS.V_FILTER
FROM (SELECT 'RRF' AS F_IS_RRF,
PREF.V_INFODOM_NAME AS V_DSN_NAME,
PREF.V_RUN_EXECUTION_ID AS V_EXECUTION_ID,
PREF.V_TASK_ID AS V_TASK_ID,
PREF.V_PROCESS_ID AS V_COMPONENT_CODE,
PREF.N_RUN_SKEY AS N_RUN_SKEY,
PREB.V_RUN_ID AS V_RUN_CODE,
PREF.V_RULE_ID AS V_RULE_CODE,
'(' || CASE
WHEN PREF.V_PROCESS_FILTER IS NULL THEN
'7=7'
ELSE
PREF.V_PROCESS_FILTER
END || ')' || ' AND ' || '(' || CASE
WHEN PREF.V_RUN_FILTER IS NULL THEN
'8=8'
ELSE
PREF.V_RUN_FILTER
END || ')' || ' AND ' || '(' || CASE
WHEN PFF.V_RUN_FILTER IS NULL THEN
'9=9'
ELSE
PFF.V_RUN_FILTER
END || ')' AS V_FILTER
FROM <<config_schema>>.PR2_RUN_EXECUTION_B PREB
LEFT OUTER JOIN <<config_schema>>.PR2_FIRERUN_FILTER PFF ON
PFF.V_RUN_EXECUTION_ID =
PREB.V_RUN_EXECUTION_ID
AND PFF.V_INFODOM_NAME =
PREB.V_INFODOM_NAME
JOIN <<config_schema>>.PR2_RUN_EXECUTION_FILTER PREF ON
PREF.V_RUN_EXECUTION_ID =
PREB.V_RUN_EXECUTION_ID
AND PREF.V_INFODOM_NAME =
```

```
PREB.V_INFODOM_NAME
WHERE PREB.V_INFODOM_NAME = '<<WORKSPACE_INFODOM>>'
UNION ALL
SELECT 'PR2' AS F_IS_RRF,
V_DSN_NAME,
V_EXECUTION_ID,
NULL AS V_TASK_ID,
V_COMPONENT_CODE,
N_RUN_SKEY,
V_RUN_CODE,
V_RULE_CODE,
V_FILTER
FROM <<config_schema>>.PR2_FILTERS PF
WHERE PF.V_DSN_NAME = '<<WORKSPACE_INFODOM>>') FILTERS
JOIN <<config_schema>>.CONFIGURATION ON UPPER(PARAMVALUE) =
UPPER(F_IS_RRF)
WHERE PARAMNAME = 'F_IS_RRF'
UNION ALL
SELECT AWFEM.F_IS_RRF,
AWFEM.V_DSN_NAME,
AWFEM.V_EXECUTION_ID,
AWFEM.V_TASK_ID,
AWFEM.V_COMPONENT_CODE,
AWFEM.N_RUN_SKEY,
AWFEM.V_RUN_CODE,
AWFEM.V_RULE_CODE,
AWFEM.V_FILTER
FROM <<config_schema>>.AAI_WF_FILTER_EXEC_MAP AWFEM;
```

3. Configure the new INFODOM with the new schema details in the `tnsnames.ora` file and WebLogic server. To enter the new schema details in the `tnsnames.ora` file, see the following sample template:

```
<SCHEMA_NAME> =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = <IP ADDRESS>)(PORT = <PORT>)
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = <SERVICE_NAME>)
)
)
<SIM_NEW_INFODOM> =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST =<IP ADDRESS>)(PORT = <PORT>))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = <SERVICE_NAME>)
)
)
```

4. To enter new INFODOM details in the WebLogic server and add the INFODOM in Console, follow these steps:
   a. Log into **WebLogic** console and go to **Services**.
   b. Click **Data Sources**.

c. Click **New** and add **Data Source** name as *Simulation_infodom* and JNDI Name as *JDBC/<Simulation_infodom>* for the new database schema details.

> **Note**
>
> <<*Simulation Infodom*>> must not have more than 11 characters.

5. Add the entry for new INFODOM in *web.xml* under *##Deployed Area##/##Context##/ WEB- INF:*

```
<resource-ref>
<description>DB Connection <<Infodom Name>></description>
<res-ref-name>JDBC/<<Infodom name>> </res-ref-name>
<res-type>javax.sql.DataSource</res-type>
<res-auth>Container</res-auth>
</resource-ref>
```

6. Configure the wallet with the new schema details in the Studio Setup.

   For more information, see *Setup Password Stores with Oracle Wallet* section in Compliance Studio Installation Guide.

7. Before running the batch, create the *IPE_KYC_Source* folder under`/ftpshare/<<Workspace infodom>>/logs/`.

10.5 Configuring Data Source

The Data Source allows you to manage the Data Schemas registered with the OFS Compliance Studio application. The Data Source Summary window shows the list of Data schemas registered with OFS Compliance Studio. These Data schemas can be used either for workspace or for sourcing data.

The Data Source Summary is divided into the following two sections:

- **Used Data Sources** : This shows the list of Data Sources registered with any workspace. Here, you can only view the Data Source details. The count of Used Data Sources also displayed at the top of Data Source Summary page.
- **Unused Data Sources** : This shows the list of Data Sources those are not registered with any workspace. Here, you can only view, edit, or delete the Data Source details. The count of Unused Data Sources also displayed at the top of Data Source Summary page.

To view the Data Source details, click the **Action** icon next to corresponding Workspace and select **View**.

After the per-configuration procedures you must add the new data source in the Compliance Studio application.

To add the new data source, follow these steps:

1. Click on the **User** icon.
2. Click **Data Source**. The **Data Source** page is displayed.
3. Click **Add Data Source** and enter the value for the following fields:
   - **Data Source Name** : Enter the connection URL to the database for the data schema.
   - **Description** : Enter the description of database connection.

- **Type** : Enter the type of the database connection.
- **Database Type** : Select the Database Type as Oracle.
- **Wallet Alias** : Enter the Wallet Alias. This value must be same as configured using Oracle Wallet.
- **Table Owner** : Enter the table owner value.

4. Click **Test Connection** to check the status of the connection.
5. Click **Create** to create the Data Source or click **Cancel** to skip the changes.

10.6 Creating Workspace

Topics:

The Workspace creation requires entry of the source of dataset, validation, and deployment.

To create a Workspace, follow these steps:

1. Navigate to the **Workspace Summary** page. The page displays the workspace records in a table.
2. Click **Add Workspace**. The Create Workspace page is displayed.

   The window displays a progress indicator at the left that indicates the active window where you are entering details.
3. Click **Previous** to go back a step and click **Next** to go to the next step.

   The following are the various phases from workspace creation to deployment:

   - Configuring Basic Details
   - Configuring Workspace Schema
   - Configuring Data Sourcing
   - Configuring Metadata Sourcing
   - Validating Workspace
   - Displaying Summary

10.6.1 Configuring Basic Details

This section describes how to configure the basic details.

To configure the basic details follow these steps:

1. Click **Use Template**. The Use Template popup window is displayed.

2. Select the KYC workspace template (*KYCWorkspaceTemplate.zip)* from the drop-down.

   The **Update Schema Mapping** window is displayed.

3. Enter the following target schema field details:
   - **New Data Schema** : Enter the newly created schema ID.
   - **New Data Source Name** : Enter the production data source name.
4. Click **Update** to update the basic details or click **Cancel** to exit the window.
5. Enter the value for the fields displayed in the following table.
6. Click **Next** to open the next page.

> **Note**
>
> The field drop-down values are populated based on the registration in the OFSAA Environment.

Table 10-3 Basic Details Fields and their Description

Fields	Description
Workspace Code	Enter the code of the workspace. This field is limited to 20 characters.
Purpose	Enter the purpose of the creation of the Workspace.
User group	Click on this field to display a list of User-group values. Select the required value. • Modeling Approver • Modeling Reviewer • Modeling User
Type	Select the type of Workspace as Simulation to perform simulation.
Sub Type	If you have selected Modeling, select the subtype of Workspace as Sandbox Workspace or Production Workspace.
Application Type	Select Know Your Customer.
Production	The KYC Production environment drop down value will be populated as a result of registering the OFSAA Environment Detail.
Simulation	The KYC Simulation environment drop down value will be populated as a result of registering the OFSAA Environment Details.
Simulation Infodom	Enter Infodom name.
Simulation User Group Code	Enter the User Group Code.
Simulation User ID	Enter the User ID.
Simulation User Password	Enter the User Password.
Simulation DB Server	Enter the BD application server IP address.
Simulation DB Schema name	Enter new Workspace Schema name.
Simulation DB Password	Enter new Workspace Schema password.
Simulation JDBC Connection String	Enter the connection String. For example: `jdbc:oracle:thin:@<DBServerIP>:<port>/<Servicename>`

10.6.2 Configuring Workspace Schema

Select the new schema created under *Data Schema*. Note that the schema will be selected by default if you are using template.

10.6.3 Configuring Data Sourcing

The schema type selected in the previous step requires the definition of database objects to be used for model creation. The data sourcing step of Workspace provisioning allows the select tables from Hive-based data sources from which data has to be pulled into the Oracle-based Workspace data schema. In case any of the selected tables are not present in the target schema, those tables are included in the failed objects count in the workspace provisioning summary.

As a part of using the template, all the KYC specific data sourcing objects are available by default.

To configure Data Sourcing, follow these steps:

1. Select a Data Source from the **Data Source Name** drop-down list.
2. Select **Target Data Schema**.
3. Select the object type and corresponding object names from the drop-down list.
4. Click **Next**.

Table 10-4 Data Sourcing Object Type and Names

Object Type	Object Name
Table	ACC_RVW_CUST
Synonym	KDD_CASES_ECM KDD_CASE_CUSTOMERS_ECM KDD_CASE_INVOLVED_PARTY_LINK_ECM KDD_CASE_INVOLVED_PARTY_DETAIL_ECM
Function	F_INS_ACC_RVW_CUST F_UPDT_ACC_RVW_CUST

10.6.4 Configuring Metadata Sourcing

The Metadata Sourcing is a stage during Workspace provisioning to allow seeding of metadata like KYC IPE ASSESSMENTS at the time of workspace provisioning.

To configure Metadata Sourcing, select the KYC specific schema from the Object Type drop-down list and corresponding available objects.

Table 10-5 Metadata Sourcing Object Type and Names

Object Type	Object Name
KYC IPE ASSESSMENTS	Algorithm Based Risk Assessment
	Rule Based Risk Assessment
	Accelerated Re-review
	New Customers Without Acct
	Periodic Re-review of Customers

Table 10-5 (Cont.) Metadata Sourcing Object Type and Names

Object Type	Object Name
	Watch List
	New Accounts Opened By Customers
	Change in Risk Model
KYC Batch	KYC Batch Run Definition
	KYC DMT Source Definition

10.6.5 Validating Workspace

The Validate pane displays a preview of the configuration values entered in the previous panes.

10.6.6 Displaying Summary

The Summary pane displays the status of the workspace creation.

Click **Download** to download the deployment report.

10.6.7 Importing Workspace Metadata for ML4AML for the Created Workspace

To import Workspace Metadata for ML4AML for the created workspace, follow these steps:

1. Login to Compliance Studio installed UNIX Machine.
2. Navigate to the path: `/deployed/ml4aml/bin`.
3. Execute the following UNIX command once, against the schema used in the current Sandbox workspace:

   ```
   ./importWorkspaceSQL.sh -w <wallet alias>
   ```

> **Note**
>
> The *wallet alias* must be the same as the one provided when the data store was created.

10.6.8 Security Mapping for the New User

For security mapping for the new user, follow these steps:

1. Open the BD application and navigate to **Behavior Detection - KYC**.
2. Select **User Security Administration** and then select **Security Attribute Administration**.
3. Select the **User Type** as *User* and choose User as the new user and map the Security Attributes.

10.7 Managing Workspace

The workspace displays a menu for Models and an application configuration and model creation sub- menu.

For more information on the following topics, see the *Managing Workspaces* section in Oracle Financial Services Compliance Studio User Guide:

- Launching a Workspace
- Viewing the Workspace
- Editing the Workspace
- Deleting the Workspace
- Downloading the Workspace

10.7.1 Populating Workspace

The workspace is populated with data from the datasets in External sources. When you are creating a workspace the table definitions are created. The Data movement from production to simulation occurs when you populate the screen.

To populate the Workspace, follow these steps:

1. Navigate to the **Workspace Summary** page. The page displays Workspace records in a table.
2. Click **Action** next to corresponding Workspace to launch Workspace and select Populate

   Workspace to populate the Workspace with data from a dataset data in the Populate Workspace window.
3. For using Template for Populating Workspace, follow these steps:
   a. Click Use Template. **Select KYCJurisdictionFilterTemplate.zip.**
   b. Add the required SQL filters.
   c. Click **Populate Workspace** and then select either **Create Batch** or **Create and Execute Batch**.
   The following table provides field descriptions for the Oracle Populate Workspace window.

Table 10-6 Populate Workspace

Object Type	Object Name
Workspace Code	The code of the Workspace.
Purpose	The description for the Workspace
Creation Date	The date on which the Workspace was created.
Data Source Type	The source of data. The value can be the OFSAA Data Schema or an external data source.
Data Filter - Global	Enter the data filter that needs to be applied on all the tables selected for data sourcing. For example: If MISDATE is equal to Today, then it is applied to all tables (wherever it is available) for selected Data Sources during population. If this field is not found (MISDATE) in the tables, it is not updated.

Table 10-6 (Cont.) Populate Workspace

Object Type	Object Name
Data Filter - Table level	Provide the data filters individually on the tables here. NOTE: You can provide multiple table names for the same SQL filter. For example, there are two tables called Student and Employee in the target data source, and below filters are applied: l MISDATE as Today for Student and Employee tables l ID as 1 for Student table Then, Student table will be populated with MISDATE and ID filters and Employee table will be populated with only MISDATE filter. Global Filters will not be applicable for those tables on which filters have been applied individually. If the same table name is provided in more than one rows here, then filter condition is generated as a conjunction of all the provided filters.
Fetch Size	Enter the Fetch size for data upload.
Batch Commit Size	Enter the Batch Commit size for data upload.
Write Mode	You can either overwrite the existing data (truncate and insert) or to append to the existing data. You can choose to either overwrite the data or append to the existing data.
Rejection Threshold	The following two options are available: Custom Rejection Threshold: Enter the maximum of number of inserts that may fail for any of the selected tables. You can provide the maximum number of inserts that can fail while loading data to a given table from all the sources. In case of threshold breach, all the inserts into the particular target schema will be rolled back. However, it will continue with populating the next target schema. Unlimited: Here, all the errors will be ignored during the data population.

4. Click **Populate Workspace** to start the process.

   Here, you can create the batch using Create Batch, or create and execute using the Create and Execute Batch option. On selecting either of these options, a workspace population task gets added to the batch.

   > **Note**
   >
   > You may require approval from an approver to populate the workspace.
   >
   > - When you select the Create and Execute Batch option, it allows you to create batch and triggers the batch as well.
   > - When you select the Create Batch option, it allows you to prepare the batch and then execute or schedule the batch at a later time through Scheduler Service window. The Workspace population task execution can be tracked in the Monitor Batch window.

5. Navigate to Scheduler Service and select Define Task.
6. Enter the following parameters for workspace population.
   - **Additional Parameters** : Enter the Additional Parameters in following format:

     ```
     {"fetch_size" :10, "batch_commit_size" :1000, "rejection_threshold"
     :"UNLIMITED", "write_mode" :"OVERWRITE"}
     ```

Global Filter provided input will be applied as a data filter on all the tables selected for data sourcing.

- **Table Filter** : You can provide data filters individually on the tables here. You must provide multiple table names for the same SQL filter. Global Filters will not be applicable for those tables on which filters have been applied individually. In case the same table name is provided in more than one rows here, the filter condition will be generated as a conjunction of all the provided filters. Enter the Table Filters in following the format:

```
[{"id":1,"filter":"","tables":["TABLE1", "TABLE2"]},
{"id":2,"filter":"","tables":["TABLE2"]}]
```

> **Note**
>
> You can run workspace population for a given workspace any number of times. New tables may be added to the definition. Any new table added to the definition, that is not present in the target schema will be physicalized on update of the workspace. Also, you can add new sources if required. Any table that is deselected from the data sourcing definition will not be dropped.

7. To drop and create Sequence in the Workspace Schema:
   a. DROP SEQUENCE FCC_KYC_MODEL_SIMULATION_SEQ;
   b. Get the max value N_MODEL_SIM_SKEY from table FCC_KYC_MODEL_SIMULATION SELECT MAX(N_MODEL_SIM_SKEY) FROM FCC_KYC_MODEL_SIMULATION; -- value
   c. CREATE SEQUENCE FCC_KYC_MODEL_SIMULATION_SEQ MINVALUE 1 MAXVALUE 999999999999999999999999999 INCREMENT BY 1 START WITH ##value+1## CACHE 20 NOORDER NOCYCLE NOKEEP NOSCALE GLOBAL;

10.8 Managing Model Pipelines

Model Pipeline allows you to create and publish models based on the workspaces created from datasets in the database. The published models are then deployed in production.

For more information on model pipelines, see the *Managing Model Pipelines* section in Oracle Financial Services Compliance Studio User Guide .

Prerequisites:

- Access the Workspace Dashboard Window
- Accessing the Model Pipelines
- Reviewing, Approving Model
- Import a Workspace Model Data into a New Model
- Import/Export Models
- Using View Models
- Editing Models
- Deleting Objectives and Draft Models

10.8.1 Creating a Model

Model creation and deployment undergo a workflow of Model Governance where the following types of users in the system have privileges that restrict the activities, they can do in the model creation and deployment workflow.

Topics:

10.8.1.1 Creating Objective (Folders)

Create folders called Objectives within which you can create Models. To create an Objective, follow these steps:

1. Click **Launch Workspace** next to corresponding Workspace to launch Workspace to display the Dashboard window with application configuration and model creation menu.
2. Click **Modeling** and select **Pipelines** from the drop-down to display the **Model Pipeline** window.
3. Click **Add** and select **Objective** from the list to display the **Objective Details** dialog box.
4. Enter details in **Objective Name** and **Description** fields in the **Add Objective** dialog box.
5. Click **Save**.

10.8.1.2 Creating Draft Models

Create Models that are classified as draft models. These models will be reviewed before being sent for Scoring.

To create a draft model, follow these steps:

1. Click **Launch Workspace** next to corresponding Workspace to launch Workspace to display the Dashboard window with application configuration and model creation menu.
2. Click **Objective**.
3. Click **Add** and select **Draft** from the list to display the **Add Draft** dialog box.
4. Create New Model is the default setting in the Model Details dialog box. Drag the toggle button to select Import Dump. Use **Create New Model** to start from a blank Notebook in Compliance Studio. Import Dump lets you drag and drop an existing file with model data and modify it.

   To create a new model, follow these steps:

   a. Click **Use Template**.
   b. Select the **KYC Simulation** zip file from the templates.
   c. Enter details for **Draft Name** and **Description**.
   d. Enter a tag in the **Tags** field.
   e. Click **Create**. A model pipeline will be created from the template. To create a pipeline from scratch, see

- Pipeline.

10.8.1.3 Creating Seeded Models

You can seed the models from the external sources which can be imported in the OFS Compliance Studio application.

To import the models, follow these steps:

1. Click **Launch Workspace** next to corresponding Workspace to launch Workspace to display the Dashboard window with application configuration and model creation menu.
2. Click **Objective**.
3. Click **Add** and select Seeded Models from the list to display the **Add Draft** dialog box.
4. You must add the models in the installed path location: `/scratch/kyc8126/ftpshare/KYC/ seeded/models`.
5. Select the models which you want to import and click **Import Seeded Models**. The selected models are imported and displayed in the **Model Pipelines** page.

10.8.1.4 Cloning a Model

You can pick any published model and clone the contents to a new draft in the same objective or clone the content to the current parent draft. The cloned draft can be edited and used further. The **Audit Trail** window also captures the clone information.

To clone the model details, follow these steps:

1. Open a Published Model in Pipeline Designer.
2. Select **Clone** to new Draft to re-image parent draft with current.

10.9 Pipeline Designer

The following sections are available on the Pipeline Designer window:

- Pipeline
- Dashboard
- Notebook
- Simulations
- Execution History
- Compare

10.9.1 Pipeline

Use the Pipeline canvas to create the paragraph and execute the pipeline using widgets.

Topics:

- #unique_197
- Executing the Pipeline
- Notebook
- Simulations

- Execution History
- Compare
- Report Extraction

10.9.1.1 Creating a Paragraph using Pipeline

To create a paragraph using pipeline, follow these steps:

1. Navigate to the **Pipeline Designer** page. The **Pipeline Canvas** is displayed.
2. Click the **Connector** to display the widgets. This is a dummy node with no paragraph is created/ associated on node save. During execution, this is used in to execute API, but will not get executed. It behaves like non-physicalized paragraph widget on execute. This node can be used as a dummy start node or connector node. The *START* widget is displayed by default in the canvas screen. You cannot edit this Widget but can be deleted. Whenever a new draft is created (not by importing dump files), the default paragraph created is converted into a start widget. The visibility of code/result/title in notebook of this node will be kept to invisible.
3. Select KYC from the list.
4. Select a widget from the following available KYC widgets:
   - RULE_BASED
   - MODEL_BASED
   - ACC_RULES
   - RISK_ASS_CAT
   - RISK_SCR_PARAM
   - MAP_EVALUATION
   - KYC Batch RRF

   The widget is added to the pipeline canvas.
5. From the pipeline canvas double-click on the widget to open the widget details screen on the right side.
6. On the widget screen under the Custom Parameters tab, click Copy to open the Clone Objects window
7. Select the source model ID from the Clone Objects window and select the version from which you want to clone the widget.

   > **Note**
   >
   > For the first model, select model ID as *PROD*.

8. Click **Copy** . The KYC Widget clone process begins. Once the cloning is completed, the current model ID and version will automatically be populated on the widget screen.
9. Click **Save** to save the widget.
10. Click **Add the next widget** and repeat from steps *5-8*.

> **Note**
>
> Any changes to the IPE Evaluations or KYC Batch must be processed in Production and then moved to Simulation.

10.9.1.2 Executing the Pipeline

To execute the pipeline follow these steps:

1. Click **Launch Workspace** next to corresponding Workspace to launch Workspace to display the Dashboard window with application configuration and model creation menu.
2. Click **Modeling** and select **Pipelines** from the drop-down to display the **Model Pipeline** window.
3. Select **Objective** from the list. The **Publish Canvas** is displayed.
4. Select the widget and click **Execute**. The **Execute Pipeline** window is displayed.
5. Click **Add** to add new parameters.
6. Click **Execute** to initiate the execution. The pipeline will be execute sequentially and you can see on each widget for a successful execution.
7. For individual widget execution details hover over the widget and click **View Details**.

10.9.1.3 Notebook

Navigate to the **Notebook** tab to view the paragraphs. You can run, invalidate session, edit, add, and export the notebook in the Notebook tab.

10.9.1.4 Simulations

The simulation flow allows for iterative execution along that path with input drivers (variables) that are passed through a parameter set. You can either create a new parameter set or use the existing parameter set and execute it from this tab.

10.9.1.5 Execution History

The **Execution History** tab displays the history of the executions of the current pipeline. You can view the list of executions, check the report for the corresponding simulation run, and extract the report. You can compare multiple executions by selecting multiple executions and click on the **Compare** icon.

10.9.1.6 Compare

The Compare option allows you to compare the executions with champion model.

To compare, follow these steps:

1. Navigate to the **Execution Summary** window.
2. Select the executions using the corresponding check-boxes.
3. Click **Compare**.

   The Execution Comparison window is displayed.

   The Window displays the following comparison details:

- Model Properties
- Model Input (Last Execution Details)
- Audit Log
- Model Script
- Model Output (Last Execution Outputs)

10.9.1.7 Report Extraction

You can view the output of the executions from all the tabs of the model pipeline. The Execution History tab allows you to download the execution output to the local system.

> **Note**
>
> You must open the report text file in excel or drag and drop in excel to view the output. If the execution output is truncated, update the Zeppelin interpreter output limit.

For more information, see Appendix-F: Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMIT in Python Interpreter.

10.10 Simulation Reports

Topics:

10.10.1 Report Types

The following two are the out of the box simulation reports:

- **Aggregate Comparison Reports** : These reports provide the aggregate comparison of risk assessments between production and respective simulation run.
  - Total Number of Low Risk Customers
  - Total Number of Medium Risk Customers
  - Total Number of High Risk Customers
- **Detailed Reports** : These reports provide comparison of risk assessments between production and respective simulation run at individual customer level.

10.10.2 Downloading Reports

Topics:

You can download the reports both via Execution History and Pipeline.

To download the report via Execution History, follow these steps:

1. Navigate to the **Execution History** tab.

2. Click the **Output** icon of the respective batch. The **Output Details** page is displayed.

   To download the report via Pipeline, follow these steps:

   a. Navigate to the **Pipeline** tab.

   b. Click the **Aggregate Report/Detailed Report** widget, and then click the **Green** tick mark.

   c. Click **View Results**. It displays the **Aggregate Report/Detailed Report**.

Figure 10-3 Aggregate Report Widget

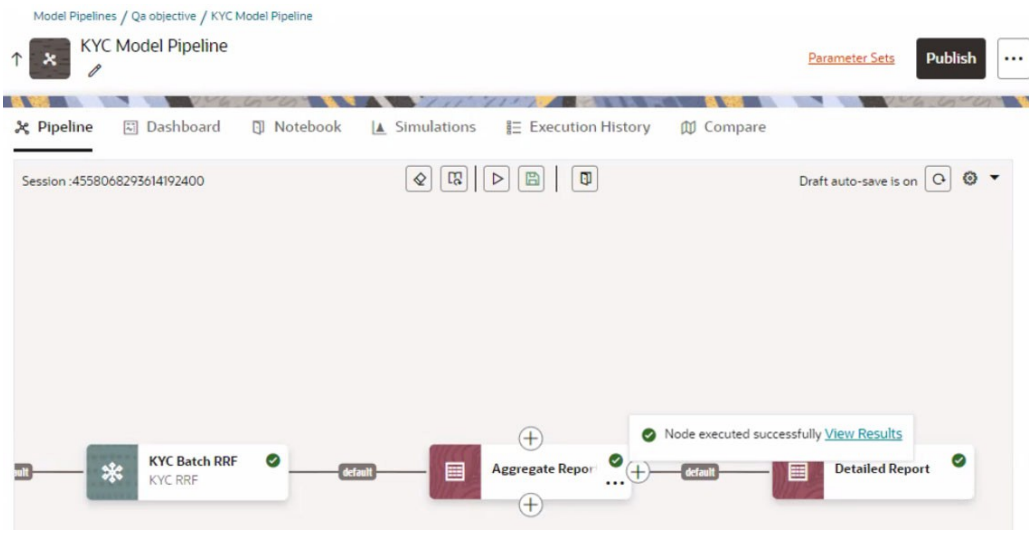
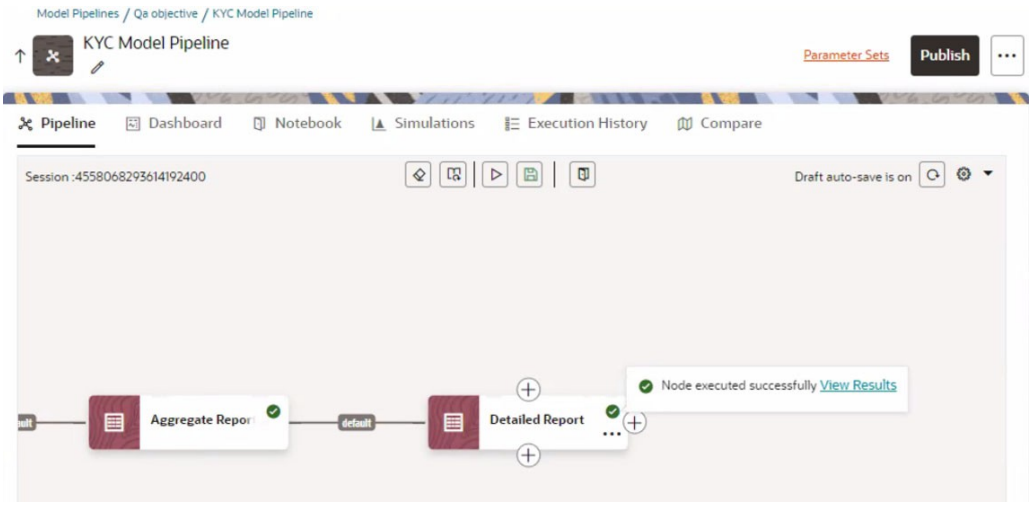


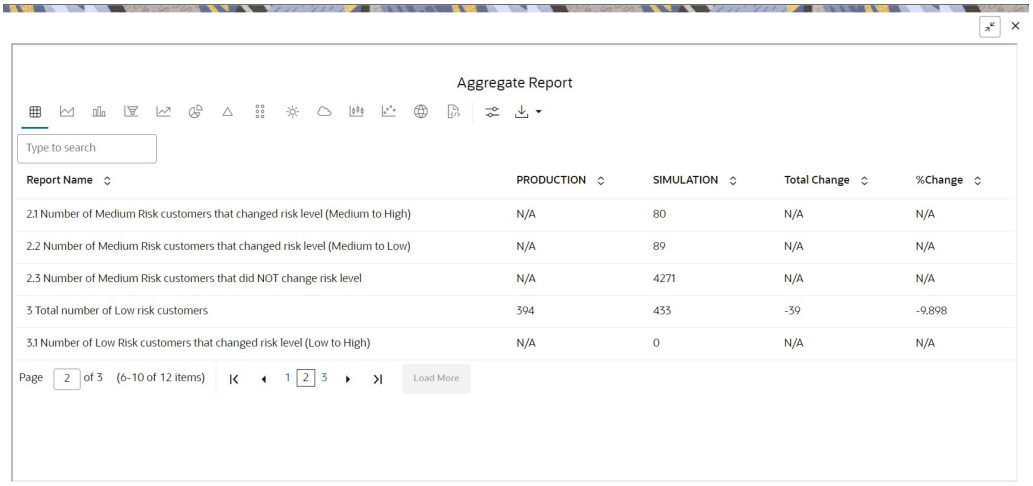
Figure 10-4 Detailed Report Widget



   d. From the **Report Widget** tile click the **Download** icon to download the report in the text file format.

> **Note**
>
> You must open the extracted report file in Excel or drag and drop the file in Excel to view the Simulation output.

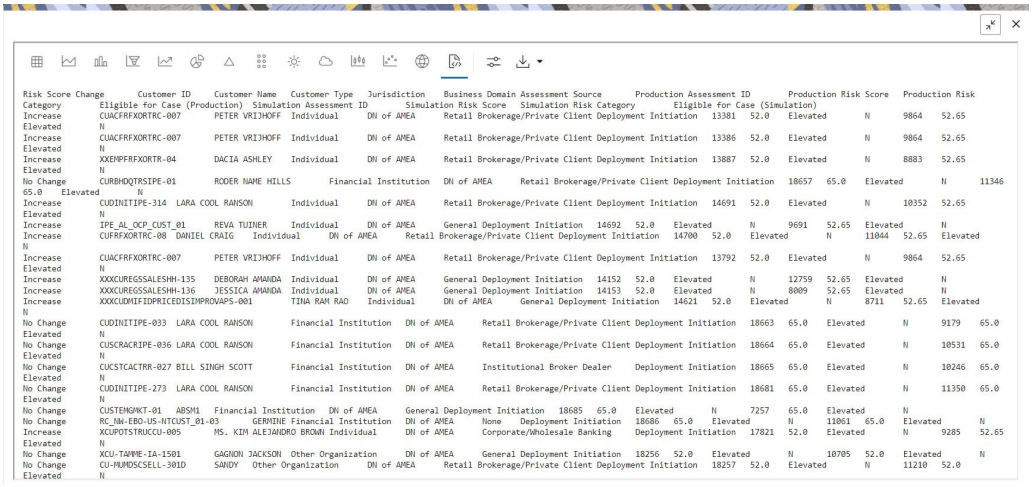
Figure 10-5 Aggregate Report



Report Name	PRODUCTION	SIMULATION	Total Change	%Change
2.1 Number of Medium Risk customers that changed risk level (Medium to High)	N/A	80	N/A	N/A
2.2 Number of Medium Risk customers that changed risk level (Medium to Low)	N/A	89	N/A	N/A
2.3 Number of Medium Risk customers that did NOT change risk level	N/A	4271	N/A	N/A
3 Total number of Low risk customers	394	433	-39	-9.898
3.1 Number of Low Risk customers that changed risk level (Low to High)	N/A	0	N/A	N/A

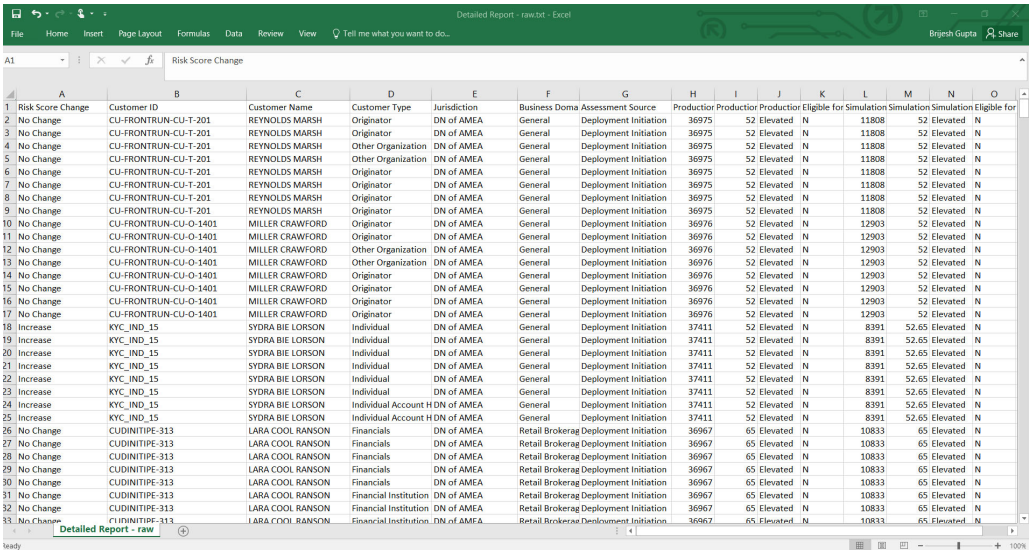
Page 2 of 3 (6-10 of 12 items) 1 2 3 Load More

Figure 10-6 Detailed Report



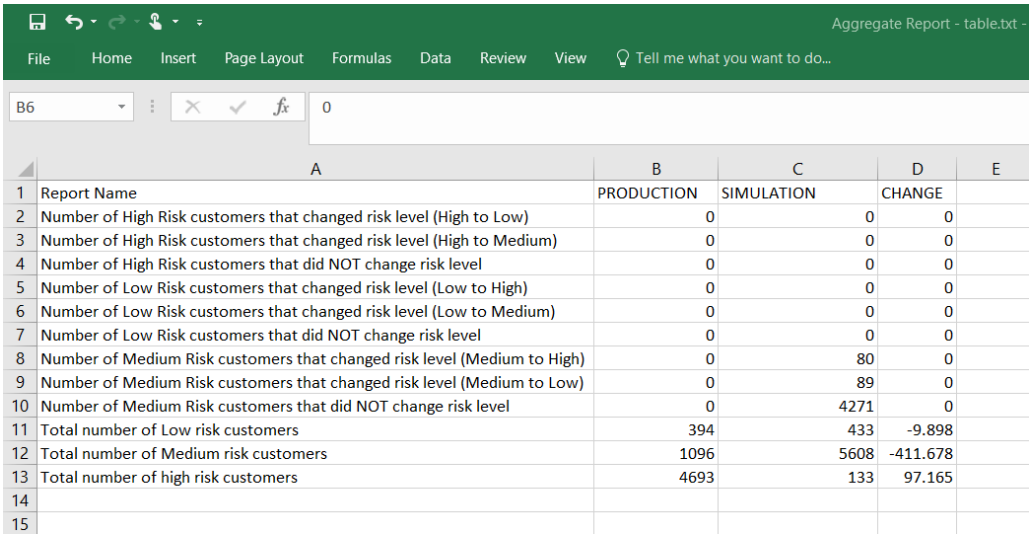
Risk Score Change Category	Customer ID	Customer Name	Customer Type	Jurisdiction	Business Domain	Assessment Source	Production Assessment ID	Production Risk Score	Production Risk Category	Eligible for Case (Production)	Simulation Assessment ID	Simulation Risk Score	Simulation Risk Category	Eligible for Case (Simulation)
Increase	CUACFRFXORTRC-007	PETER VRIJHOFF	Individual	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	13381	52.0	Elevated	N	9864	52.65	Elevated	N
Increase	CUACFRFXORTRC-007	PETER VRIJHOFF	Individual	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	13386	52.0	Elevated	N	9864	52.65	Elevated	N
Increase	XXEMPFRFXORTR-04	DACIA ASHLEY	Individual	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	13887	52.0	Elevated	N	8883	52.65	Elevated	N
No Change	CURBHDQTRSIPE-01	RODER NAME HILLS	Financial Institution	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	18657	65.0	Elevated	N	11346	65.0	Elevated	N
Increase	CUDINITIPE-314	LARA COOL RANSON	Individual	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	14691	52.0	Elevated	N	10352	52.65	Elevated	N
Increase	IPE_AL_OCP_CUST_01	REVA TUINER	Individual	DN of AMEA	General Deployment	Initiation	14692	52.0	Elevated	N	9691	52.65	Elevated	N
Increase	CUFRFXORTRC-08	DANIEL CRAIG	Individual	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	14700	52.0	Elevated	N	11044	52.65	Elevated	N
Increase	CUACFRFXORTRC-007	PETER VRIJHOFF	Individual	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	13792	52.0	Elevated	N	9864	52.65	Elevated	N
Increase	XXXCUREGSSALESHH-135	DEBORAH AMANDA	Individual	DN of AMEA	General Deployment	Initiation	14152	52.0	Elevated	N	12759	52.65	Elevated	N
Increase	XXXCUREGSSALESHH-136	JESSICA AMANDA	Individual	DN of AMEA	General Deployment	Initiation	14153	52.0	Elevated	N	8009	52.65	Elevated	N
Increase	XXXCUDMIFIDPRICEDISIMPROVAPS-001	TINA RAM RAO	Individual	DN of AMEA	General Deployment	Initiation	14621	52.0	Elevated	N	8711	52.65	Elevated	N
No Change	CUDINITIPE-033	LARA COOL RANSON	Financial Institution	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	18663	65.0	Elevated	N	9179	65.0	Elevated	N
No Change	CUSCRACRIPE-036	LARA COOL RANSON	Financial Institution	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	18664	65.0	Elevated	N	10531	65.0	Elevated	N
No Change	CUCSTCACTRR-027	BILL SINGH SCOTT	Financial Institution	DN of AMEA	Institutional Broker Dealer	Deployment Initiation	18665	65.0	Elevated	N	10246	65.0	Elevated	N
No Change	CUDINITIPE-273	LARA COOL RANSON	Financial Institution	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	18681	65.0	Elevated	N	11350	65.0	Elevated	N
No Change	CUSTEMGMKT-01	ABSM1	Financial Institution	DN of AMEA	General Deployment	Initiation	18685	65.0	Elevated	N	7257	65.0	Elevated	N
No Change	RC_NW-EBO-US-NTCUST_01-03	GERMINE	Financial Institution	DN of AMEA	None	Deployment Initiation	18686	65.0	Elevated	N	11061	65.0	Elevated	N
Increase	XCUPOTSTRUCCU-005	MS. KIM ALEJANDRO BROWN	Individual	DN of AMEA	Corporate/Wholesale Banking	Deployment Initiation	17821	52.0	Elevated	N	9285	52.65	Elevated	N
No Change	XCU-TAMME-IA-1501	GAGNON JACKSON	Other Organization	DN of AMEA	General Deployment	Initiation	18256	52.0	Elevated	N	10705	52.0	Elevated	N
No Change	CU-MUMDSCSELL-301D	SANDY	Other Organization	DN of AMEA	Retail Brokerage/Private Client	Deployment Initiation	18257	52.0	Elevated	N	11210	52.0	Elevated	N

Figure 10-7 Detailed Report in xls Format



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Risk Score Change	Customer ID	Customer Name	Customer Type	Jurisdiction	Business Doma	Assessment Source	Production	Production	Production	Eligible for	Simulation	Simulation	Simulation	Eligible for
2	No Change	CU-FRONTRUN-CU-T-201	REYNOLDS MARSH	Originator	DN of AMEA	General	Deployment Initiation	36975	52	Elevated	N	11808	52	Elevated	N
3	No Change	CU-FRONTRUN-CU-T-201	REYNOLDS MARSH	Originator	DN of AMEA	General	Deployment Initiation	36975	52	Elevated	N	11808	52	Elevated	N
4	No Change	CU-FRONTRUN-CU-T-201	REYNOLDS MARSH	Other Organization	DN of AMEA	General	Deployment Initiation	36975	52	Elevated	N	11808	52	Elevated	N
5	No Change	CU-FRONTRUN-CU-T-201	REYNOLDS MARSH	Other Organization	DN of AMEA	General	Deployment Initiation	36975	52	Elevated	N	11808	52	Elevated	N
6	No Change	CU-FRONTRUN-CU-T-201	REYNOLDS MARSH	Originator	DN of AMEA	General	Deployment Initiation	36975	52	Elevated	N	11808	52	Elevated	N
7	No Change	CU-FRONTRUN-CU-T-201	REYNOLDS MARSH	Originator	DN of AMEA	General	Deployment Initiation	36975	52	Elevated	N	11808	52	Elevated	N
8	No Change	CU-FRONTRUN-CU-T-201	REYNOLDS MARSH	Originator	DN of AMEA	General	Deployment Initiation	36975	52	Elevated	N	11808	52	Elevated	N
9	No Change	CU-FRONTRUN-CU-T-201	REYNOLDS MARSH	Originator	DN of AMEA	General	Deployment Initiation	36975	52	Elevated	N	11808	52	Elevated	N
10	No Change	CU-FRONTRUN-CU-O-1401	MILLER CRAWFORD	Originator	DN of AMEA	General	Deployment Initiation	36976	52	Elevated	N	12903	52	Elevated	N
11	No Change	CU-FRONTRUN-CU-O-1401	MILLER CRAWFORD	Originator	DN of AMEA	General	Deployment Initiation	36976	52	Elevated	N	12903	52	Elevated	N
12	No Change	CU-FRONTRUN-CU-O-1401	MILLER CRAWFORD	Other Organization	DN of AMEA	General	Deployment Initiation	36976	52	Elevated	N	12903	52	Elevated	N
13	No Change	CU-FRONTRUN-CU-O-1401	MILLER CRAWFORD	Other Organization	DN of AMEA	General	Deployment Initiation	36976	52	Elevated	N	12903	52	Elevated	N
14	No Change	CU-FRONTRUN-CU-O-1401	MILLER CRAWFORD	Originator	DN of AMEA	General	Deployment Initiation	36976	52	Elevated	N	12903	52	Elevated	N
15	No Change	CU-FRONTRUN-CU-O-1401	MILLER CRAWFORD	Originator	DN of AMEA	General	Deployment Initiation	36976	52	Elevated	N	12903	52	Elevated	N
16	No Change	CU-FRONTRUN-CU-O-1401	MILLER CRAWFORD	Originator	DN of AMEA	General	Deployment Initiation	36976	52	Elevated	N	12903	52	Elevated	N
17	No Change	CU-FRONTRUN-CU-O-1401	MILLER CRAWFORD	Originator	DN of AMEA	General	Deployment Initiation	36976	52	Elevated	N	12903	52	Elevated	N
18	Increase	KYC_IND_15	SYDRA BIE LORSON	Individual	DN of AMEA	General	Deployment Initiation	37411	52	Elevated	N	8391	52.65	Elevated	N
19	Increase	KYC_IND_15	SYDRA BIE LORSON	Individual	DN of AMEA	General	Deployment Initiation	37411	52	Elevated	N	8391	52.65	Elevated	N
20	Increase	KYC_IND_15	SYDRA BIE LORSON	Individual	DN of AMEA	General	Deployment Initiation	37411	52	Elevated	N	8391	52.65	Elevated	N
21	Increase	KYC_IND_15	SYDRA BIE LORSON	Individual	DN of AMEA	General	Deployment Initiation	37411	52	Elevated	N	8391	52.65	Elevated	N
22	Increase	KYC_IND_15	SYDRA BIE LORSON	Individual	DN of AMEA	General	Deployment Initiation	37411	52	Elevated	N	8391	52.65	Elevated	N
23	Increase	KYC_IND_15	SYDRA BIE LORSON	Individual	DN of AMEA	General	Deployment Initiation	37411	52	Elevated	N	8391	52.65	Elevated	N
24	Increase	KYC_IND_15	SYDRA BIE LORSON	Individual Account H	DN of AMEA	General	Deployment Initiation	37411	52	Elevated	N	8391	52.65	Elevated	N
25	Increase	KYC_IND_15	SYDRA BIE LORSON	Individual Account H	DN of AMEA	General	Deployment Initiation	37411	52	Elevated	N	8391	52.65	Elevated	N
26	No Change	CUDINITIPE-313	LARA COOL RANSON	Financials	DN of AMEA	Retail Brokerag	Deployment Initiation	36967	65	Elevated	N	10833	65	Elevated	N
27	No Change	CUDINITIPE-313	LARA COOL RANSON	Financials	DN of AMEA	Retail Brokerag	Deployment Initiation	36967	65	Elevated	N	10833	65	Elevated	N
28	No Change	CUDINITIPE-313	LARA COOL RANSON	Financials	DN of AMEA	Retail Brokerag	Deployment Initiation	36967	65	Elevated	N	10833	65	Elevated	N
29	No Change	CUDINITIPE-313	LARA COOL RANSON	Financials	DN of AMEA	Retail Brokerag	Deployment Initiation	36967	65	Elevated	N	10833	65	Elevated	N
30	No Change	CUDINITIPE-313	LARA COOL RANSON	Financials	DN of AMEA	Retail Brokerag	Deployment Initiation	36967	65	Elevated	N	10833	65	Elevated	N
31	No Change	CUDINITIPE-313	LARA COOL RANSON	Financial Institution	DN of AMEA	Retail Brokerag	Deployment Initiation	36967	65	Elevated	N	10833	65	Elevated	N
32	No Change	CUDINITIPE-313	LARA COOL RANSON	Financial Institution	DN of AMEA	Retail Brokerag	Deployment Initiation	36967	65	Elevated	N	10833	65	Elevated	N
33	No Change	CUDINITIPE-313	LARA COOL RANSON	Financial Institution	DN of AMEA	Retail Brokerag	Deployment Initiation	36967	65	Elevated	N	10833	65	Elevated	N

Figure 10-8 Aggregate Report in xls Format



	A	B	C	D	E
1	Report Name	PRODUCTION	SIMULATION	CHANGE	
2	Number of High Risk customers that changed risk level (High to Low)	0	0	0	
3	Number of High Risk customers that changed risk level (High to Medium)	0	0	0	
4	Number of High Risk customers that did NOT change risk level	0	0	0	
5	Number of Low Risk customers that changed risk level (Low to High)	0	0	0	
6	Number of Low Risk customers that changed risk level (Low to Medium)	0	0	0	
7	Number of Low Risk customers that did NOT change risk level	0	0	0	
8	Number of Medium Risk customers that changed risk level (Medium to High)	0	80	0	
9	Number of Medium Risk customers that changed risk level (Medium to Low)	0	89	0	
10	Number of Medium Risk customers that did NOT change risk level	0	4271	0	
11	Total number of Low risk customers	394	433	-9.898	
12	Total number of Medium risk customers	1096	5608	-411.678	
13	Total number of high risk customers	4693	133	97.165	
14					
15					

10.10.2.1 Publishing a Pipeline

If you are satisfied with the results of the execution you can publish the pipeline.

To publish the pipeline, follow these steps:

1. Click **Launch Workspace** next to corresponding Workspace to launch Workspace to display the Dashboard window with application configuration and model creation menu.
2. Click **Modeling** and select **Pipelines** from the drop-down to display the **Model Pipeline** window.
3. Select **Objective** from the list. The **Publish Canvas** is displayed.
4. Click **Publish** . The **Publish Pipeline** popup is displayed.
5. Enter the field details as described in the following table.

Table 10-7 Publish Pipeline

Field or Icon	Description
Model Name	The field displays the name of the Model. Modify the name if required.
Model Description	The field displays the description for the Model. Enter or modify the description if required.
Technique	Enter the registered technique to use.
Run Version	Select a run version.
Variable Mapping	The table displays the OFSAA variables and datasets used in the creation of the Training Model.
Script	The table displays the Paragraphs created in the Training Model. Select the Paragraphs that you want to use to create the Scoring Model. Track Output - Select this to track the output of the paragraph.

6. Select the required configuration and click **Publish** to publish the pipeline or click Cancel to go back to previous page.
7. To view the published model, follow the steps:
   a. Navigate to the **Model Pipeline** page.
   b. Click **Models in-line with the Object Name** . The published models are displayed.

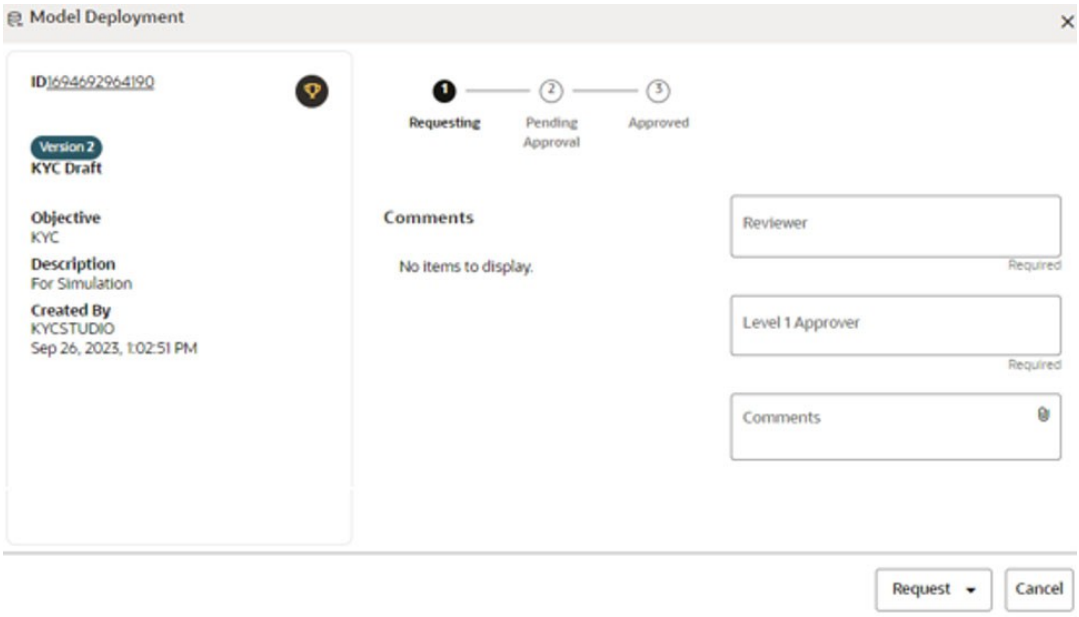
10.10.2.2 Deploying the Model

You can promote the published model to production by deploying the model.

To deploy the model follow the subsequent steps:

1. Click **Launch Workspace** next to corresponding Workspace to launch Workspace to display the Dashboard window with application configuration and model creation menu.
2. Click **Modeling** and select **Pipelines** from the drop-down to display the Model Pipeline window.
3. Select the **Objective name** from the list and then select the published Model.
4. Click the icon to view the **Model Deployment** screen.

Figure 10-9 Model Deployment Window



5. Select a value for the following fields:
   - Reviewer
   - Level 1 Approver
   - Comments
6. Click **Request** and select the **Model Acceptance** action.
7. Click **Cancel** to cancel the model Deployment.

   For more information on the following topics, see Oracle Financial Services Compliance Studio User Guide.
   - Understanding Model Governance
   - Request Model Acceptance
   - Review Models and Move to Approve or Reject
   - Approve Models and Promote to Production
   - Deploying Models in Production and Make it a Global Champion
   - Executing Models using Scheduler Service

> **Note**
>
> There can only be one champion model per workspace.

10.11 Audit Trail

You can audit the models at any time from the Audit Trail window. The Audit Trail window displays all model details. This displays information such as when the Model was created, who created the Model, the Model's workflow, such as when this Model became a champion or was deployed, and so on.

For information on how to use audit trail, see *Audit Trail* in Oracle Financial Services Compliance Studio User Guide.

10.12 Moving Champion Model (Configuration Data) from Simulation to Production

This section describes how to move configuration data for the Champion Model from Simulation to Production.

To move configuration data from Simulation to Production, follow these steps:

1. Navigate to the **Model Pipeline**.
2. Click the **Download** button to download the zip file and extract it.
3. Update the existing version of configuration in the following production tables as `V_MODEL_ID = 'PROD' and N_VERSION = '-1'`.

   For example, `UPDATE APPLN_RB_PROCESSING SET N_VERSION = -1 where V_MODEL_ID = 'PROD' and N_VERSION = 0 ;`

Table 10-8 Table and Widget Names

Table Name	Widget Name
• APPLN_RB_PROCESSING • H$APPLN_RB_PROCESSING	RULE_BASED_ASSESSMENT
• APPLN_RISK_RATING_PARAMS • H$APPLN_RISK_RATING_PARAMS	ALGORITHM_BASED_ASSESSMENT
• APPLN_REREVIEW_PARAMS • H$APPLN_REREVIEW_PARAMS	ACCELERATED_REREVIEW
• DIM_RISK_CATEGORY • H$DIM_RISK_CATEGORY	RISK_ASSESSMENT_CATEGORY
• PARAM_RISK_SCORE_JRSDN • H$PARAM_RISK_SCORE_JRSDN	RISK_SCORE_PARAM
• MAP_EVAL_RISK_ASSMNT_MODEL	MAP_EVALUATION

4. Open the required the configuration (cfg) file.
5. Take the data, form as the following Request JSON, and hit the production URL.

> **Note**
>
> Except for IPE_ASSESSMENT, the following API works for all configurations.

URL: <prod_base_url>/kyc/simulation/configuration/import

```
Headers:
infodom : <prod_infodom>,
user : <admin_user_id>,
locale : en_US
Request Body:
{
"page_code": "<ra_config_name>",
```

```
"mmg_model_id": "PROD",
"mmg_model_version": "0",
"mmg_model_name" : "PROD_MOVEMENT",
"objectdata": "<file_data>" //this <file_data> must be provided
with escape characters
}
```

6. For IPE_ASSESSMENT, file path and file name are provided in the IPE_ASSESSMENT-related configuration file. Take the file and proceed with the RTIImport.
7. Navigate to `$FIC_HOME/ficapp/common/FICServer/bin` and execute the following command:

   ```
   ./RTIImport.sh <filepath> <infodom> OFS_KYC false.
   ```

10.13 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 the icon to expand the page.
6. Select the batch you want to run and click Fire Run. The Fire Run page is displayed.
7. On the Fire Run page, provide the required values. If the **IPEKYCRun** daily batch is selected, then provide the following values in **Parameters** option.

   ```
   [MODELID]=PROD,[VERSION]=0,[APP_ID]=OFS_KYC
   ```

8. Click **OK**.

A

APPENDIX-A: KYC Batches

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

Topics:

> **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.

A.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 A-1 Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task1	Customer	This is an IPE pre filtering 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_extrl_batch_last_run table and is used to keep track of the current batch that is being run.	TRANSFORM DATA	START
Task3	Populate_Cust_Prcsng	This is a task that populates the pre-filtered 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_Addr_Prcsng	This is a task that populates the pre-filtered Customer Data into the Cust_Addr_Prcsng table when run.	LOAD DATA	Task3
Task6	Populate_Cust_Cntry_Prcsng	This is a task that populates the pre-filtered 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 pre-filtered Customer Data into the Cust_Id_Doc_Prcsng table when run.	LOAD DATA	Task3
Task8	Populate_Cust_Mkt_Served_Prcsng	This is a task that populates the pre-filtered Customer Data into the Cust_Mkt_Served_Prcsng table when run.	LOAD DATA	Task3
Task9	Populate_Cust_Phon_Prcsng	This is a task that populates the pre-filtered Customer Data into the Cust_Phon_Prcsng table when run.	LOAD DATA	Task3
Task10	Populate_Cust_Prod_Prcsng	This is a task that populates the pre-filtered 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 pre-filtered Customer Data into the Cust_Cust_Prcsng table when run.	LOAD DATA	Task3
Task12	Populate_Cust_Acct_Prcsng	This is a task that populates the pre-filtered Customer Data into the Cust_Acct_Prcsng table when run.	LOAD DATA	Task3
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

Table A-1 (Cont.) Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
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_RLSHP_PRCSNG_BO	This is a task that populates the beneficial owner details into the PARTY_PARTY_RLSHP_PRCSNG_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
Task22	t2t_PARTY_ADDRESS_PRCNG_BO_EXT	This is a task that populates the external beneficial owner details into the PARTY_ADDRESS_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

Table A-1 (Cont.) Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
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 pre-filtered 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
Task33	t2t_POPULATE_FCT_RA_RISK_REASONS	This is a task that populates the FCT_RA_RISK_REASONS table with the scores of each Parameter for every Customer when run.	LOAD DATA	Task31
Task34	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
Task35	t2t_FCT_CUST_RA_HISTRY	This is a task that populates the FCT_CUST_RA_HISTRY table with the names of the pre-filtered customers when run.	LOAD DATA	Task36

Table A-1 (Cont.) Regular Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task36	F_CLOSURE_UPDATES	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_TP_WLS_REQUESTS	This is a task that populates the FCT_TP_WLS_REQUESTS table when run.	LOAD DATA	Task31
Task39	t2t_FCT_TP_WLS_RESULTS	This is a task that populates the FCT_TP_WLS_RESULTS table when run.	LOAD DATA	Task21
Task40	t2t_FCT_RA_RISK_RATING_HISTORY	This is a task that populates the FCT_RA_RISK_RATING_HISTORY table when run.	LOAD DATA	Task31
Task41	t2t_FCT_CUST_REVIEW_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_LAST_RUN_TAB	This is a task that purges or truncates the kdd_extrl_batch_last_run table when run.	TRANSFORM DATA	Task31, Task32, Task33, Task34, Task35, Task36, Task37, Task38, Task39, Task40, Task41
Task43	t2f_GenCustDetails_ED	This is a task that generates the Customer details flat file.	EXTRACT DATA	Task42
Task44	t2f_GenWLSFeedback_ED	This is a task that generates the watch list feedback details flat file.	EXTRACT DATA	Task42
Task45	t2f_GenCBSFeedback_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

A.2 Deployment Initiation Processing

Table A-2 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

Table A-2 (Cont.) Deployment Initiation Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task2	Populate_Cust_Prcsng_DI	This is a task that populates the pre-filtered 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
Task4	Populate_Cust_Addr_Prcsng	This is a task that populates the pre-filtered Customer Data into the Cust_Addr_Prcsng table when run.	LOAD DATA	Task3
Task5	Populate_Cust_Cntry_Prcsng	This is a task that populates the pre-filtered 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 pre-filtered 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 pre-filtered 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 pre-filtered Customer Data into the Cust_Phon_Prcsng table when run.	LOAD DATA	Task7
Task9	Populate_Cust_Prod_Prcsng	This is a task that populates the pre-filtered 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 pre-filtered Customer Data into the Cust_Cust_Prcsng table when run.	LOAD DATA	Task9
Task11	Populate_Cust_Acct_Prcsng	This is a task that populates the pre-filtered 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_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	Task1, Task10, Task1 1, Task12, Task13, Task2, Task3, Task4, Task5, Task6, Task7, Task8, Task9

Table A-2 (Cont.) Deployment Initiation Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task15	GathrStats_IP	This is a task that is used to gather statistics for the FCT_CUST_iINTERESTED_PARTY table.	TRANSFORM DATA	Task14
Task16	t2t_PARTY_DETAILS_PRCNG_IP	This is a task that populates the party details in the PARTY_DETAILS_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
Task19	t2t_FCT_TP_WLS_REQUESTS_PRCNG	This is a task that populates the watch list Score in the FCT_TP_WLS_REQUESTS_PRCNG table when run.	LOAD DATA	Task14, Task15, Task16, Task17, Task18
Task20	GathrStats_WLSREQUESTS_P	This is a task that is used to gather statistics for the FCT_TP_WLS_REQUESTS and FCT_TP_WLS_REQUESTS_PRCNG tables.	TRANSFORM DATA	Task19
Task21	Watchlist_Fuzzy Match	This is a task that calls the watch list Fuzzy Match to calculate the watch list Score when run.	TRANSFORM DATA	Task20
Task22	GathrStats_WLSRESULT_STG	This is a task that is used to gather statistics for the FCT_TP_WLS_RESULTS and FCT_TP_WLS_RESULTS_PRCNG tables.	TRANSFORM DATA	Task21
Task23	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	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_KYCPRCSNG_TAB	This is a task that is used to gather statistics for all the KYC processing tables.	TRANSFORM DATA	Task 24
Task26	Customer Processing	This is a task 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

Table A-2 (Cont.) Deployment Initiation Processing

Task ID	Rule Name (As configured)	Description	Component ID	Precedence
Task28	t2t_FCT_RA_DI	This is a task that is used to populate the FCT_RA_DI table.	LOAD DATA	Task27
Task29	GathrStats_FCT_RA	This is a task that is used to gather statistics for the FCT_RA table for Regular Processing.	TRANSFORM DATA	Task28
Task30	t2t_Populate_FCT_RA_RISK_SUMMARY	This is a task that populates the FCT_RA_RISK_SUMMARY table with the final MB and RB scores for each Customer when run.	LOAD DATA	Task29
Task31	t2t_Populate_FCT_RA_RISK_REASONS	This is a task that populates the FCT_RA_RISK_REASONS table with the scores of each Parameter for every Customer when run.	LOAD DATA	Task30
Task32	t2t_FCT_RA_RISK_DETAILS	This is a task that populates the FCT_RA_RISK_DETAILS table with the actual values of each Parameter for every Customer when run.	LOAD DATA	Task31
Task33	t2t_FCT_CUST_RVWDTLS_AUTO_CLOSED_DI	This is a task that stores the details of the assessments that are auto-closed.	LOAD DATA	Task32
Task34	t2t_FCT_CUST_RVWDTLS_ PTC_DI	This is a task that stores the details of the assessments that are promoted to a case through the batch.	LOAD DATA	Task33
Task35	t2t_FCT_TP_WLS_REQUESTS	This is a task that populates the watch list score in the FCT_TP_WLS_REQUESTS table when run.	LOAD DATA	Task 34
Task36	t2t_FCT_TP_WLS_RESULTS	This is a task that populates the watch list score in the FCT_TP_WLS_RESULTS table when run.	LOAD DATA	Task 35
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 pre-filtered customers when run.	LOAD DATA	Task 37
Task39	KYC_PURGE_LAST_RUN_TAB	This is a task that purges or truncates the kdd_extrl_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

A.3 End of Day Processing

Table A-3 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_GenWLSFeedback_ED	Extract the watch list scanning feedback details.	EXTRACT DATA	
Task3	t2f_GenCBSFeedback_ED	Extract customer details for CBS.	EXTRACT DATA	
Task4	KYC_File_Rename	Renaming of the extracted files according to the Anti Money Laundering (AML) needs.	TRANSFORM DATA	Task1, Task2, Task3
Task5	FN_REREVIEW_DATE_DI	Splitting of the customers processed through the DI processing back for periodic re-review.	TRANSFORM DATA	Task1, Task2, Task3, Task4

B

APPENDIX-B: Creating Highlights

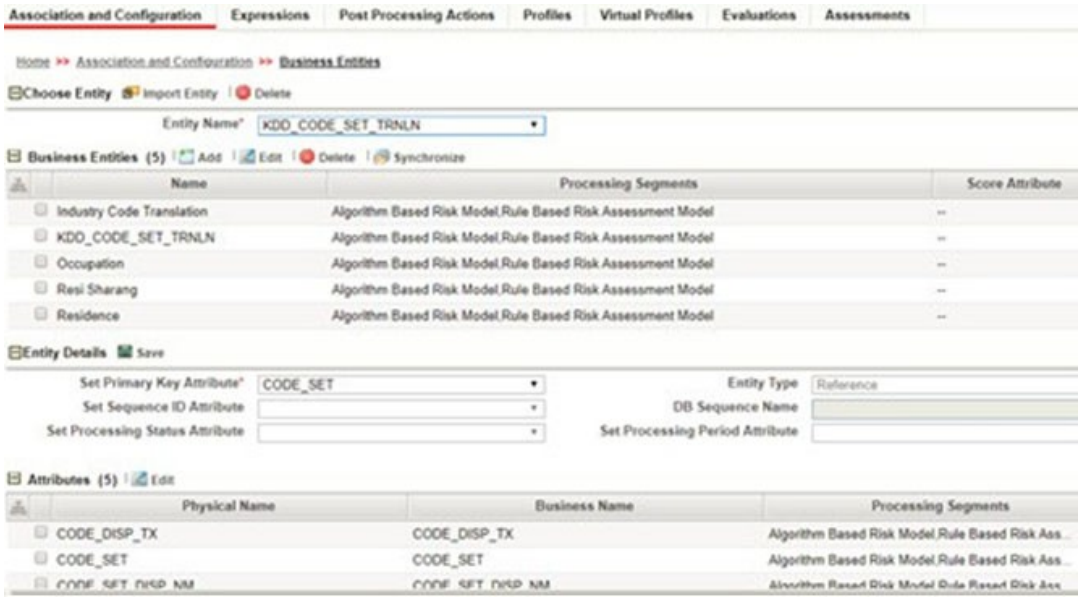
This appendix provides the steps to create highlights for Risk and Algorithm-based assessments in Know Your Customer (KYC).

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**.

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

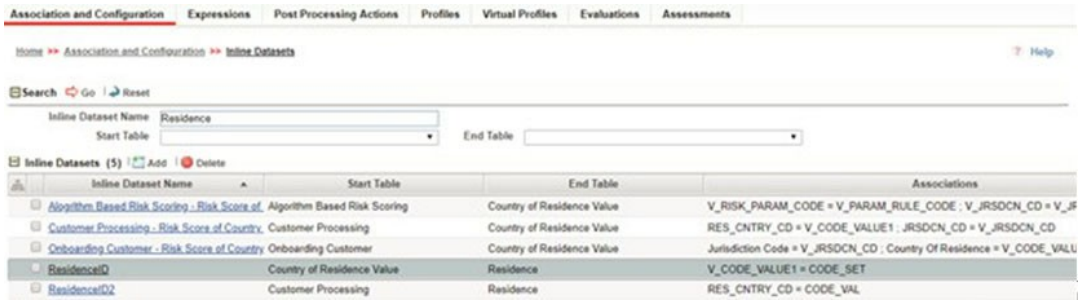
Figure B-1 Association and Configuration Menu



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 B-2 Inline Datasets Page

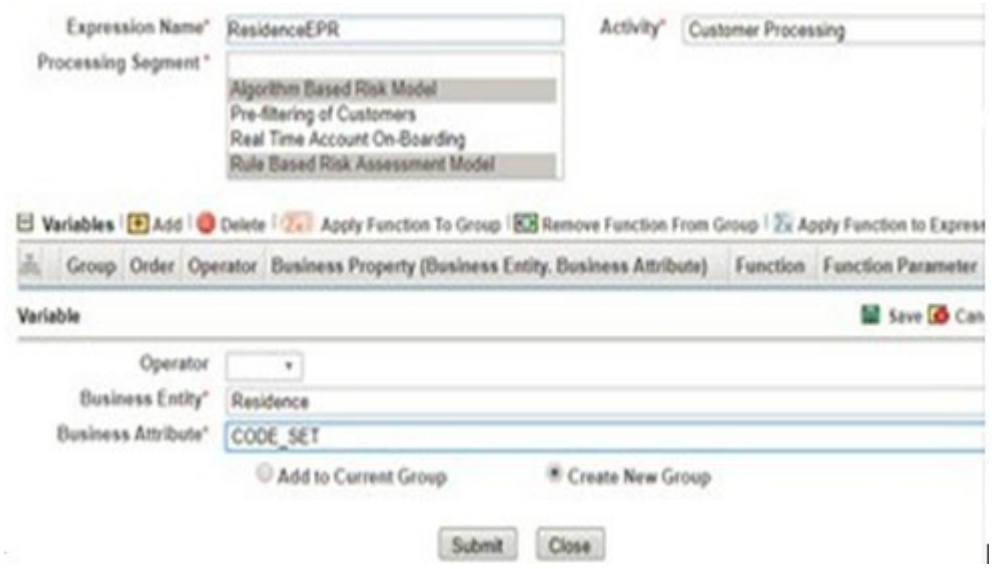


5. Add a Traversal Path for each join defined in Inline Datasets.
6. To add a Traversal Path, navigate to the **Association and Configuration** menu on the **Inline Processing** page and click **Traversal Paths**.

   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.

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

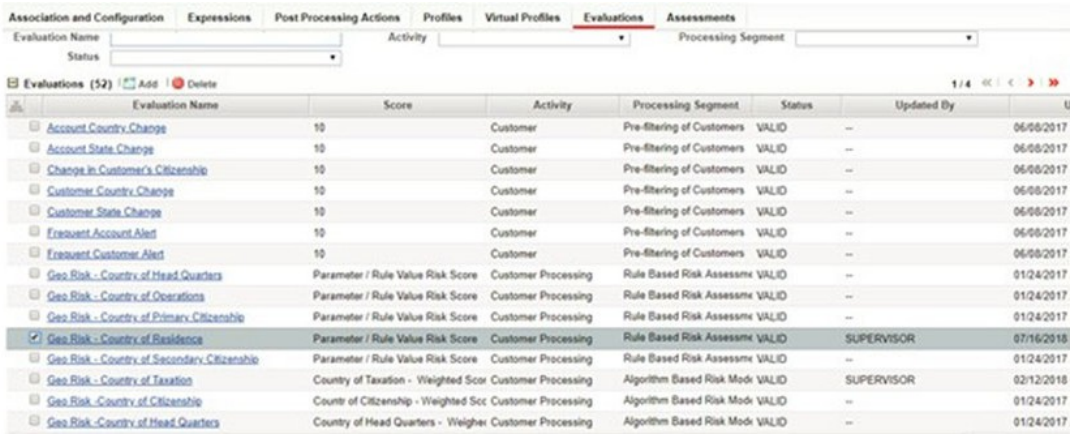
Figure B-3 Expressions Menu



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

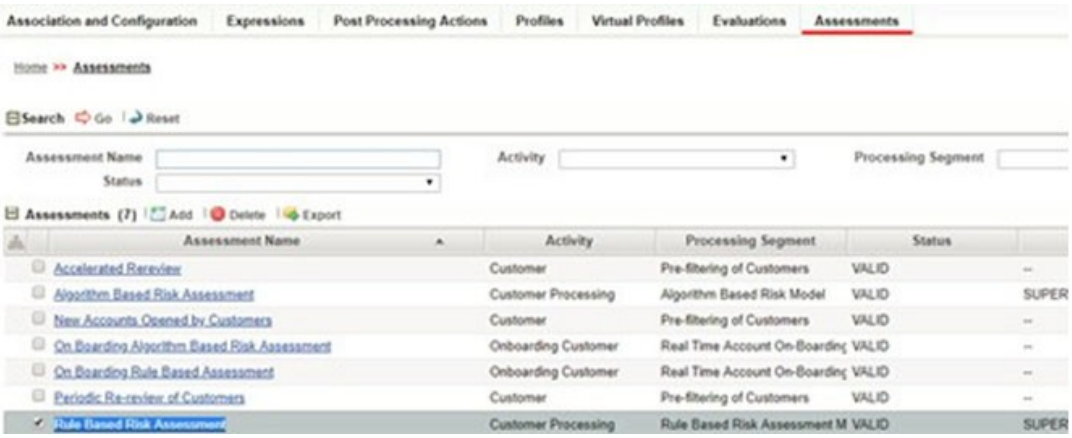
   To map an evaluation, navigate to the **Evaluations** menu on the **Inline Processing** page. In the following example, an Evaluation is created for the Rule-Based Risk Assessment.

Figure B-4 Evaluations Menu



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 B-5 Assessments Menu



C

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:

C.1 Executing the CS Task

> **Note**
>
> - If Load Customer Match Data from the Oracle CS task is already added in IPEPREProcess then remove this task and execute as a separate batch.
> - For new installation, CS task must be added as a separate batch by adding Load Customer Match Data from the Oracle CS task. Before you run the batch, ensure that you have completed data ingestion in all relevant tables. This batch must be executed before running the daily batch.

C.1.1 Running the Deployment Initiation Batch

To run the Deployment Initiation batch, follow these steps:

1. Log in to the KYC Application.
2. Click **Common Tasks**, select **Rule Run Framework**, and click **Process**.
3. On the **Process** page, provide the value **KYC_DI_Populate_Processing** in the **Code** field and click **Search**.
4. Select the **KYC_DI_Populate_Processing** check box and click **Edit**. The Process Definition (Edit Mode) page appears.
5. On the **Process Definition (Edit Mode)** screen, click **Component**.
6. On the **Component Selector** screen, search for the Processes node in the List window on the left.
7. Expand the **Processes** node, and then the **FCCMSEGMNT** node.
8. 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.
9. Click **OK**.

10. In the **Process Definition (Edit Mode)** screen, click **Precedence**.
11. 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.
12. Click **OK**.
13. Click **Save** to save the process.
14. Recreate the Batch corresponding to this RUN.

C.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**.
3. Select **Financial Services Inline Processing Engine** and click **Inline Processing** and select **Assessments**.
4. Click **Accelerated Rereview** and then click **MAP**.
5. In the **Assessment Evaluation Mapping** screen, select **New Watch List Matches from the Available Evaluations** window and move it to the **Included Evaluations** window.
6. Click **Save**.
7. Restart the servers.

D

APPENDIX-D: Switching between EDQ and CS

This chapter shows the scripts that are to be executed to switch between EDQ (Enterprise Data Quality) 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_ST
ROKE)
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_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_CONDITI
ON_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_CONDITI
ON_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_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_CONDITI
ON_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_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)
/
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_ST
ROKE) 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_ST
ROKE) 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)
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_DE
SC,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)
/
```

E

Appendix-E: Configurations for the Bearer Token

The following section takes you through the process of generating a token and using it to get the individual or entity JSON, depending on the API request. A token is used to authorize the request.

You can begin by generating a password for the user who sends the request. After the password is generated, generate a token to authorize this request. The default time for token expiration is 3600 seconds (1 hour) and can be changed. To change the validity, see Change Token Validity.

Topics:

E.1 Generate User Password

To generate a password for the user, follow these steps:

1. Log in as a system administrator.
2. Click **System Configuration** in the **Administration** page and select **Configure Instance Access Token**.

   The Configure Instance Access Token window is displayed.
3. In the **Configure Instance Access Token** section, click **Add**. A new window is displayed.
4. Enter the username in the **Instance Name** field and click **Generate Token**. The token is displayed in the Instance Access Token Details section.
5. Copy and save the text generated in the **Instance Access Token Details** section.

   > **Note**
   >
   > The **STP_ACC_NM** field displays the username. The **STP_ACC_TKN** field displays the password.
6. Click the **Close** icon and log out as the system administrator.

E.2 Change Token Validity

To generate a password for the user, follow these steps:

1. Log in as a system administrator.
2. Click **System Configuration** in the **Administration** page and select **Configure System Configuration**. The **Configuration** window is displayed.

3. In the **Configuration** window, change the token validity time in the API token validity in seconds field.
4. Click **Save**.

> **Note**
>
> You can monitor the Simulation batch by login using the newly created username and password (Username is created at time of workspace creation).

F

Appendix-F: Setting the ZEPPELIN_INTERPETER_OUTPUT_LIMIT in Python Interpreter

An interpreter is a program that directly executes instructions written in a programming or scripting language without requiring them previously to be compiled into a machine language program.

Interpreters are plug-ins that enable users to use a specific language to process data in the backend. In Compliance Studio, Interpreters are used in Notebooks to execute code in different languages. Each The interpreter has a set of adjusted and applied properties across all notebooks. For more information on Interpreter Configuration and Connectivity, see OFS Compliance Studio Administration and Configuration Guide .

Using the **zeppelin.interpreter.output.limit** field you can enter the output message limit. Any message that exceeds the limit is truncated.

Topics:

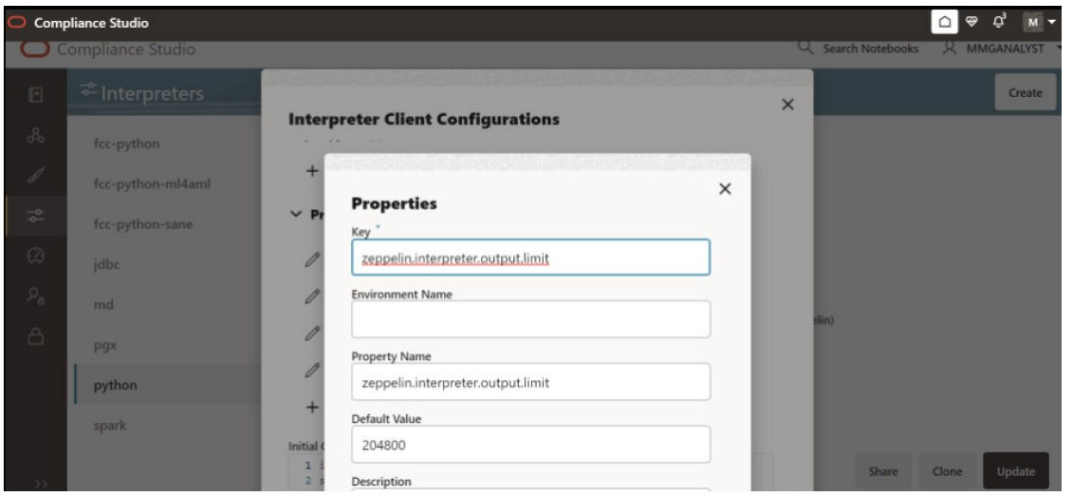
F.1 Configuring through the UI

Follow the subsequent steps to configure the `zeppelin.interpreter.output.limit` through the UI:

Using the Wizard screen:

1. Click the **User** icon right top corner.
2. Go to **Data Studio Options**.
3. Click **Interpreters**. The **Interpreters** page is displayed.
4. Select the python interpreter for which you want to configure the `zeppelin.interpreter.output.limit`.
5. Select **python** from the LHS options.
6. Click on the **Wizard** icon.
7. From the RHS side click on **oracle.datastudio.python.DsPythonInterpreter** under **Interpreter Client Configurations**. The **Interpreter Client Configuration** popup is displayed.
8. Under Properties, click **+Properties**. The **Properties** popup is displayed.
9. Fill the options as shown in the following figure . Set the default value to 870400 (for 1000 records approx.).

Figure F-1 spring-postSacalert.properties file



> **Note**
>
> - Configuration using the Wizard screen is preferable to other ways of configuration.
> - If the data is more than 1000 records, update the **zeppelin.python.maxResult** in properties to the desired value and `zeppelin.interpreter.output.limit` as 870.4 x maxResult.
> - If you cannot see the **Create** and **Cancel** buttons, click on the header label of the **Properties** window.
> - The default value for `zeppelin.interpreter.output.limit` i is 102400 (in bytes).
> - Increasing the default value from 102400 bytes to an immense value will slow down the rendering of outputs of python paragraphs.

10. 10. Click **Create**. The **Interpreter Client Configuration** popup is displayed and `zeppelin.interpreter.output.limit` is displayed under **Properties**.
11. Click **Confirm**. The **Interpreter Client Configuration** window is displayed.
12. Click **Update**.
13. Restart the **Compliance Studio** application to reflect the changes.

Configuration through JSON Screen:

1. Click the **User** icon right top corner.
2. Go to **Data Studio Options**.
3. Click **Interpreters**. The **Interpreters** page is displayed.
4. Select the python interpreter for which you want to configure the `zeppelin.interpreter.output.limit`.
5. Select python from the LHS options.
6. Click on the **JSON configuration** icon. The **JSON configuration** screen is displayed.

7. Scroll down and locate `interpreterClientConfigs` with className `oracle.datastudio.python.DsPythonInterpreter`. You can find the properties section with zeppelin configurations.
8. Add the `zeppelin.interpreter.output.limit`.

Figure F-2 JSON Screen

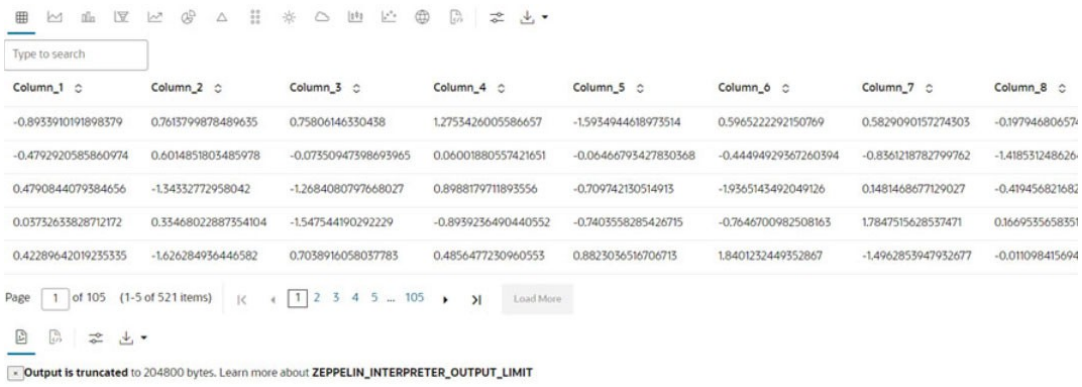
9. The update button will be enabled in the bottom right corner after the JSON modification. Click **Update**.
10. Restart the Compliance Studio application to reflect the changes.

F.2 Configuring through the Filesystem

To configure the `zeppelin.interpreter.output.limit` through the filesystem, follow these steps:

1. Go to the python interpreter option as pointed out in the Configuring through the UI section. You can see the python interpreter listed there if you have run the MMG services before. Delete it, if you run the MMG application for the first time on a fresh schema, then you don't need to do this step.
2. After deleting the python interpreter or if the start has not been done, go to the filesystem inside `mmg-home/mmg-studio/server/builtin/interpreters`, and open `python.json` in a text editor.
3. Scroll down under **interpreterClientConfigs** with className **oracle.datastudio.python.DsPythonInterpreter**, you will find the following properties section with Zeppelin configurations. After the last entry in properties, add the `zeppelin.interpreter.output.limit` using the JSON screen.
4. Save the `python.json` with the desired default value.
5. Restart the Compliance Studio application to reflect the changes.

Figure F-3 Output in Tabular View



You can see the `zeppelin.interpreter.output.limit` value as a warning if the table content is more than the set default value for `zeppelin.interpreter.output.limit`, and accordingly, you can modify the default value for the same.

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

Glossary

Index