Configuration Guide

Oracle Financial Services:

Anti-Money Laundering | Fraud | Trading Compliance | Broker Compliance | Energy and Commodity Trading Compliance | Enterprise Case Management | Know Your Customer | FATCA Management | Personal Trading Approval

Release 6.2.4
August 2014

ORACLE

Configuration Guide
Oracle Financial Services:

Anti-Money Laundering |Fraud| Trading Compliance |Broker Compliance |Energy and Commodity Trading Compliance| Enterprise Case Management| Know Your Customer| FATCA Management|Personal Trading Approval

Release 6.2.4
August 2014

Document Control Number:9MN12-62410003
Document Number: CG-14-FCCM-0003-6.2.4-01

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

Document Number: CG-14-FCCM-0003-6.2.4-01
First Edition (August 2014)

Oracle Financial Services Software, Inc.
1900 Oracle Way
Reston, VA 20190
Phone: (703) 478-9000
Fax: (703) 318-6240
Internet: www.oracle.com/financialservices

Contents

List of Figures

List of Tables

About this Guide

This guide explains the structure behind the Oracle Financial Services Behavior Detection Framework and Oracle Financial Services Enterprise Case Management user interface (UI) and provides comprehensive instructions for configuring modifiable components. This chapter focuses on the following topics:

- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information
- Conventions Used in this Guide

Who Should Use this Guide

The *Configuration Guide* is designed for use by application users and client personnel who have a working knowledge of eXtensible Markup Language (XML) and UI software components. Their roles and responsibilities, as they operate within the Oracle Financial Services Behavior Detection Framework and Oracle Financial Services Enterprise Case Management, include the following:

- **Installers:** Installs and configures the Oracle Financial Services Behavior Detection Platform and Oracle Financial Services Enterprise Case Management at a specific deployment site. The Oracle Financial Services application Installer also requires access to deployment-specific configuration information (for example, machine names and port numbers).

- **Administrators:** Configures, maintains, and adjusts the Oracle Financial Services Behavior Detection Platform and Oracle Financial Services Enterprise Case Management user interface, and is usually an employee of a specific Oracle Financial Services customer.

How this Guide is Organized

The *Configuration Guide* includes the following chapters:

- Chapter 1, *General Configuration,* provides instructions for configuring general items that are reflected throughout the UI, such as, default settings that are configurable within the UI.
- Chapter 2, *Alert Management Configuration,* provides instructions for configuring the parameters specific to alert management.
- Chapter 3, *Administration Tools Configuration,* provides instuctions for configuring the parameters specific to administration tools.
- Chapter 4, *Case Management Configuration,* provides instructions for configuring the parameters specific to case management.
- Chapter 5, *Assessment Configuration,* provides instructions for configuring the parameters specific to risk assessment.
- Chapter 6, *KYC Risk Assessment Configuration,* provides instructions on configuring the weights of the risk assessment parameters per customer type for different risk models available in KYC.
- Chapter 7, *Actions Configuration,* provides instructions for configuring the Action page of the UI.
- Chapter 8, *Web Application Configuration,* provides instructions for configuring the functional settings of the Web Application for the UI post installation.
- Chapter 9, *OBIEE Report Configuration,* provides instructions for configuring Oracle Financial Services Analytic reports and graphs.
- The *Index,* provides an alphabetized cross-reference list that helps you locate information quickly.

Where to Find More Information

For more information about Oracle Financial Services Behavior Detection Framework, refer to the following documents:

- *Administration Guide*
- *Administration Tools User Guide*
- *Scenario Manager User Guide*
- *Installation Guide - Stage 1*
- *Installation Guide - Stage 3*
- *Alert Management User Guide*
- *Enterprise Case Management User Guide*
- *KYC Risk Assessment Guide*

To learn more about Oracle Financial Services and our complete product line, refer to our Web site www.oracle.com/financialservices.

Conventions Used in this Guide

Table 1 lists the conventions used in this guide.

Table 1. Conventions Used in this Guide

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

CHAPTER 1 General Configuration

This chapter provides instructions for configuring parameters that are common for both alert and case management. This chapter includes the following topics:

- Configuring the Client Logo Image
- Configuring the Base Time Zone
- Configuring the Default Currency Code
- Configuring the Lock Time Period for Alert/Case Actions
- Configuring Notifications
- Configuring E-mail
- Configuring Organization Type
- Configuring View All Organization
- Configuring XML Export
- Configuring the Display of Value in By Field Name/ID
- Configuring the Default Due Date Calculation
- Configuring the Alert/Case Auto Assignment Web Service
- Configuring File Size
- Configuring Views

Configuring the Client Logo Image

The client logo has a default blank image included in all Mantas JSPs. You need to replace the blank image for both your Oracle Financial Services product and the Administration Tools with a `.gif` file that contains your firm's name and logo.

Logo Specification

The following lists the client logo specification:

- The logo name should be `client_logo.gif`
- Dimensions: Height: 40 pixels; Width: Constrain Proportions
- File format: GIF

Placing a new Client Logo

To place a new client logo, follow these steps:

1. Make a backup of existing `client_logo.gif` from the location: `<AAI deployed area>/images` (for example, `/OFSAAI/images/`).
2. Place the customer logo from location: `<AAI deployed area>/images` (for example, `/OFSAAI/images/`).
3. After placing the image in the web server, refresh the IE browser.
4. Refresh the Appserver's work folder.

Removing a Client Logo

To remove a custom client logo, follow these steps:

1. Replace `client_logo.gif` from the backup location.
2. After placing the image in the web server, refresh the IE browser.
3. Refresh the Appserver's work folder.

Configuring the Base Time Zone

The Base Time Zone parameter is used in the Export to XML action from Alert Management/Case Management. You can modify the default Base Time Zone through the Manage Common Parameters screen (Figure 1).

From the Menu option, go to Administration >Manage Parameters > Manage Common Parameters to access the Manage Common Parameters screen (Figure 1).

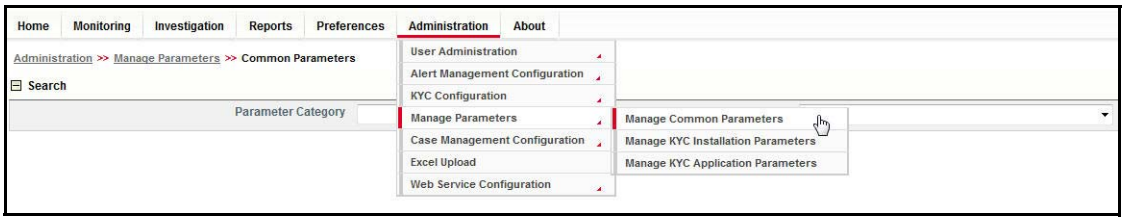

Figure 1. Manage Common Parameter Screen

To modify the base time zone, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Base Time Zone** from the Parameter Name drop-down list.

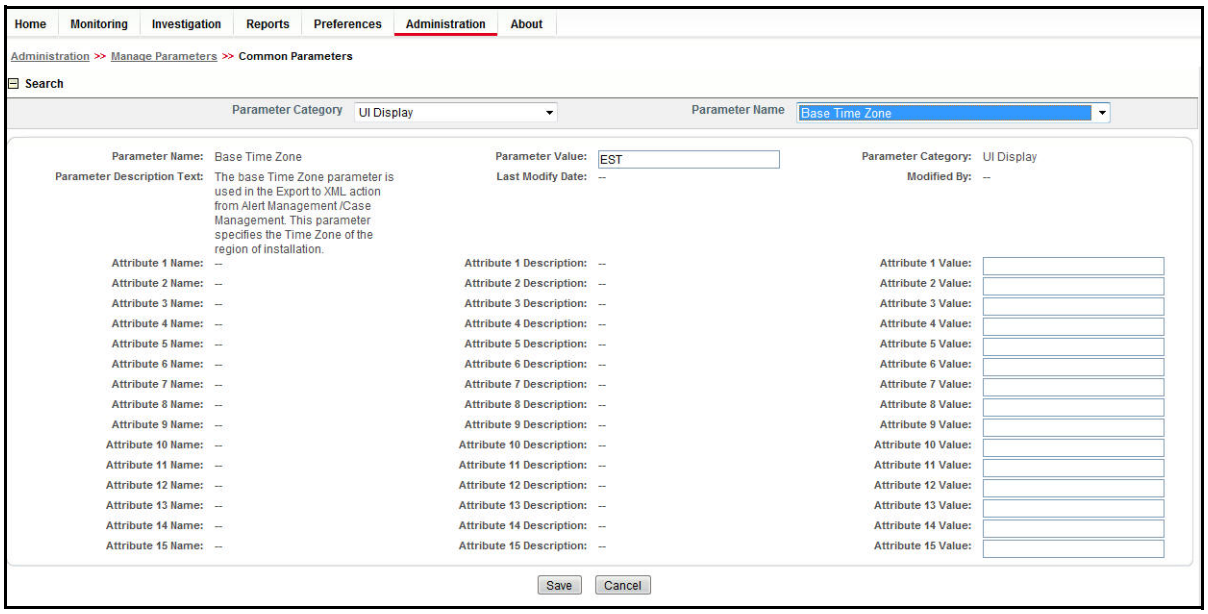

Figure 2. Configuring Base Time Zone

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring the Default Currency Code

You can modify the default currency settings that display throughout the UI. The following section provides detailed instructions to modify the currency code, which is highlighted in Figure 3.

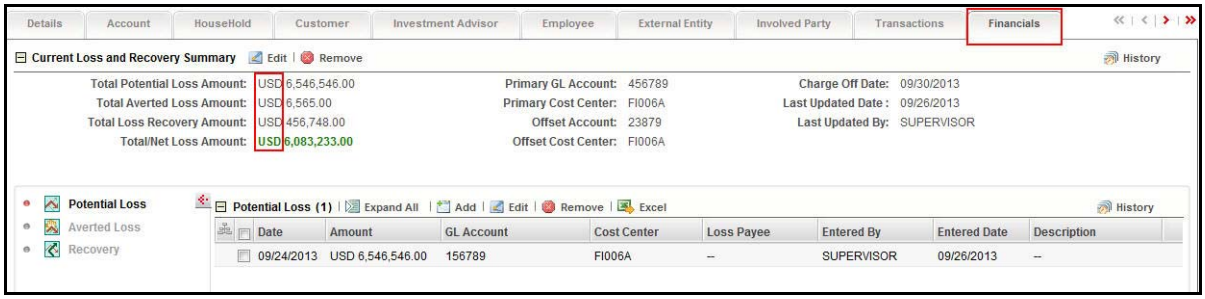

Figure 3. Financials Tab—Default Currency Format

To modify the default currency code, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Base Currency** from the Parameter Name drop-down list.
4. Edit the parameter. Figure 4 illustrates the modified currency code as EUR.

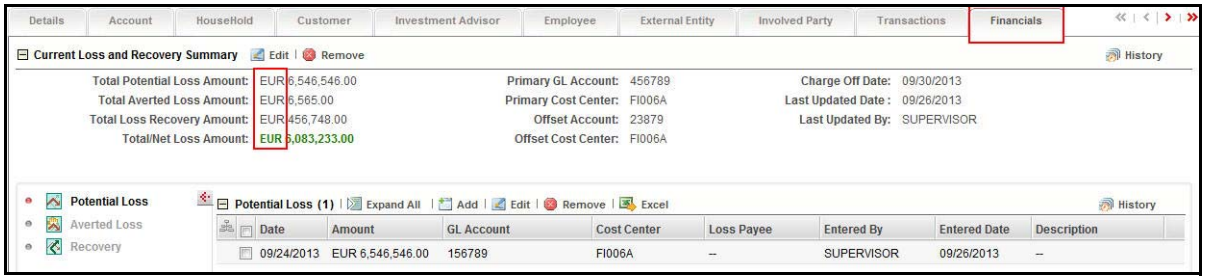

Figure 4. Financials Tab—with Modified Currency Format

To modify the default currency code, from the backend, follow these steps:

1. Locate the `CFG_Env.xml` file in the following directory:

   `<MANTAS_HOME>/alert_management/alert_mgmt/WEB-INF/classes/conf/ui_config`

2. Save a copy of the original `CFG_Env.xml` file in the custom directory that contains backup files:

   `<MANTAS_HOME>/alert_management/alert_mgmt/WEB-INF/classes/conf/ui_config/custom/backup`

3. Open the original `CFG_Env.xml` in an editor.
4. Locate thedefault currency code that you want to modify, that is similar to the following:

   ```
   <I18N lang="en" country="US" dateFormat="MM/dd/yyyy" baseTimeZone="EST" defaultCur-
   rency="USD" pdfFont="ArialUnicodeMS"/>
   ```

5. Modify the currency code.

   In the following example, the modified currency code is EUR (Euro):

```
<I18N lang="en" country="US" dateFormat="MM/dd/yyyy" baseTimeZone="EST" defaultCur-
rency="EUR" pdfFont="ArialUnicodeMS"/>
```

6. Save the file to the original directory and exit the editor.

Note: The currency for highlights is configured in the `<OFSBDP Installed Directory>/database/dbtools/mantas_cfg` directory where you run the `run_highlights.ksh` script. Refer to the *Administration Guide* for more information.

Configuring the Lock Time Period for Alert/Case Actions

Alerts and cases are locked when you are taking actions on them, however, the lock is opened when you complete the action. If you close the browser window while the lock is still active, then the lock remains active until it expires. This prevents other users from acting on the locked alert or case.

By default, the system retains the lock for 30 minutes. This parameter applies for both Alert and Case Management implementations. If you want to change the time period for this lock, then follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **UI Lockout Time** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

   Note: UI Lock Out Time should be mentioned in minutes. That is, `param_value_tx` value should be in minutes.

Configuring Notifications

This parameter specifies the list of attributes used to display Notifications. The attributes include the number of days to be used to identify near due alerts and cases, the number of days until the notification is displayed on the UI, and the number of days when the notifications will be purged.

To modify Notification parameters, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Notification** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 2 describes the attributes which need to be configured for Notification parameter.

Table 2. Configuring Notification Attributes

Attribute	Description
NEAR_DUE_DATE	This attribute specifies the number of days before the due date of an alert or a case is generated. This attribute value accepts only natural numbers.
UI_DISPLAY_DAYS	This attribute specifies the number of days when a notification is displayed on the UI. If no particular action is taken on the notification, and the number of days for the notification exceeds, the notification is no longer displayed. This attribute value accepts only natural numbers.
PURGE_NOTIFICATION	This attribute specifies the number of days until the notification is purged from the database. The `PURGE_NOTIFICATION` should be set greater than the `UI_DISPLAY_DAYS` value. This attribute value accepts only natural numbers.

Configuring E-mail

This parameter specifies the attributes for the E-mail action. The value of this parameter should be set to Y.
To modify E-mail parameters, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **E-Mail** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 3 describes the attributes which need to be configured for E-mail parameters.

Table 3. Configuring E-mail Attributes

Attribute	Description
DEF_SEND_USR	This attribute specifies whether the system should use a pre-defined E-mail address or the E-mail address of the current logged in user as the default sender address. The parameter value can have only Y or N value. Y sets the E-mail of the sender as the User ID specified in DEF_SEND_USR_ID attribute as the default. N sets the E-mail of the current logged in user as the default.
DEF_SEND_USR_ID	This attribute specifies the default user ID for the E-mail action. This parameter must have a value when the DEF_SEND_USR is set to Y. **Note:** The attribute value should reference a user in the KDD_REVIEW_OWNER table.
DEF_DOM_ENABLED	This attribute enables/disables the set of domains where E-mails can be sent. The parameter value can have only Y or N value. Y restricts the user from sending E-mails to the domains specified in the DEF_DOM attribute. When it is set to N, the UI presents the user with a selection box from which the E-mail IDs of the users identified in TO_LST_USR_ID attribute can be selected.
DEF_DOM	This attribute specifies the domains to which the E-mails can be sent. This attribute should be populated only when the DEF_DOM_ENABLED attribute is set to Y.
TO_LST_USR_ID	This attribute specifies the users to whom the E-mails can be sent. This attribute should be populated only when the DEF_DOM_ENABLED attribute is set to N. **Note:** The attribute value(s) should reference users in the KDD_REVIEW_OWNER table.
MAIL_HOST	This attribute specifies Mail SMTP host IP address/Server name. If this attribute is not populated, E-mail actions cannot be performed.
DEF_SUBJECT	This attribute specifies the default subject text that appears on E-mails when an E-mail action is taken for alerts or cases.
MAIL_FOOTER	This attribute specifies optional footer details which can be appended to the E-mail.
MAIL_ATTACH_LIMIT	This attribute specifies the attachment size limit. The value is given in MB.
DISPLAY_ACTIONS_TAKEN	This attribute specifies whether to display the 'Actions Taken' in the attached HTML or not.

Table 3. Configuring E-mail Attributes

Attribute	Description
HTML_REPORT_IN_BODY	This attribute specifies for a single alert, whether the html report should come in mail body or as attachment.
DEF_ACTION_TAKER	This attribute specifies the default action taker for the received response if the system cannot identify the Response Sender as a valid User.

Configuring Organization Type

This parameter specifies the type of organization that is used to populate the list of available cost centers wherever cost center appears as a selection or data entry criteria throughout the application. Records in the Organization table with this specified Organization Type (`ORG.ORG_TYPE_CD`) is displayed in the cost center drop-downs. The parameter value is limited to specifying only one organization type.

To modify the Organization Type, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Organization Type** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring View All Organization

This parameter, along with other access permissions defined for the user, determines the alerts and cases that can be viewed by a user in the Related Alerts and Related Cases matrices of the Relationship tab for both Alert Management and Case Management implementations. The parameter value can have only Y or N value. Y enables the current user to view alerts and cases as related alerts and related cases respectively, even if the user does not have viewing rights for the alert's or case's primary organization, which is defined based on the organization associated with the owning user. N restricts the user from viewing, as related, alerts or cases whose primary organizations the user does not have access to view.

For example, User Joe Smith may be not be allowed to see the details of alerts or cases owned by users (or a pool) who have Employee Compliance as their primary organization. However, if this parameter is set to Y, Joe Smith would be able to see alerts or cases associated with the organization of Employee Compliance in a list of related alerts/cases, as long as they have a relationship to the current alert/case being viewed. If this parameter is set to N, Joe Smith would have no ability to see the above mentioned alerts or cases, even as related.

To disable View All Organization, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **View All Organization** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring XML Export

This parameter specifies attributes related to Alert or Case Export to XML actions. The parameter should be set to Y.
To modify the XML export, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Export XML** from the Parameter Name drop-down list.

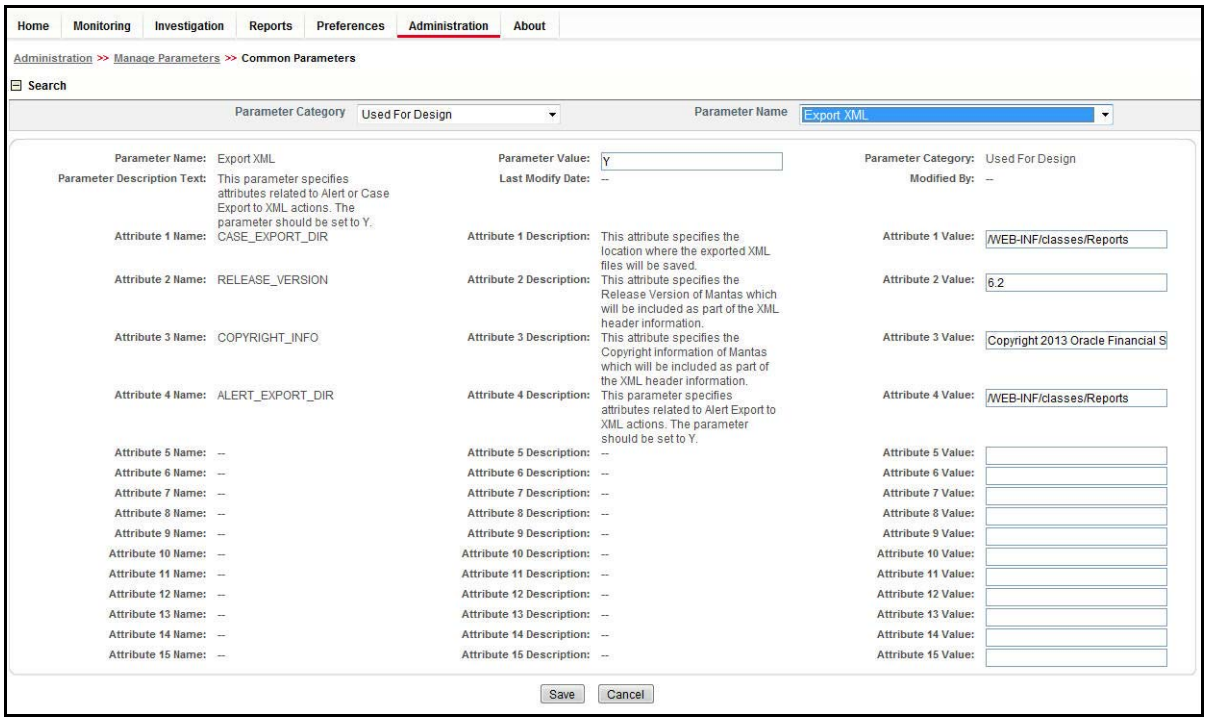

Figure 5. Configuring XML Export

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 4 describes the attributes which need to be configured for XML export.

Table 4. Configuring XML Export Attributes

Attribute	Description
CASE_EXPORT_DIR	This attribute specifies the location where the exported case XML files is saved.
ALERT_EXPORT_DIR	This attribute specifies the location where the exported alert XML files is saved.

Note: These are relative paths located within the .EAR file.

Configuring the Display of Value in By Field Name/ID

This configuration allows you to see either the ID or Name field for the User, Focus, Branch, Division and Organization in the UI. This parameter specifies the client to specify the Name or ID value in the By field.

To modify the Display of Value in the By Field Name/ID, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Display of Value in By Field Name/ID** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 5 describes the attributes which should be configured for Display of Value in By Field Name/ID.

Table 5. Configuring Display of Value in By Field Name/ID Attributes

Attribute	Description
User	ID or Name for User field.
Focus	ID or Name for Focus field.
Branch	ID or Name for Branch field.
Division	ID or Name for Division field.
Org	ID or Name for Org field.

Configuring the Default Due Date Calculation

This parameter allows the client to specify the use of Business days versus Calendar days. Here you can specify **C** for Calendar days and **B** for Business days.

Note: The default value is Calendar days (C).

To modify the Default Due Date Calculation, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Default Due Date Calculation** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring the Alert/Case Auto Assignment Web Service

This parameter specifies the attributes required to invoke the Alert/Case Auto Assignment Web Service. This parameter should have a value as *Y.*

To modify the Alert/Case Auto Assignment Web Service, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Deployment Based** from the Parameter Category drop-down list.
3. Select **Alert/Case Auto Assignment Web Service** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 6 describes the attributes which needs to be configured for `Display of Value in By field Name/ID`.

Table 6. Configuring Alert - Case Assigner Web Service Attributes

Attribute	Description
userid	This attribute specifies the user ID for the Alert/Case Assigner webservice. If this attribute has an incorrect value the webservice fails.It should be the same value set during the OFSBDF installation as web services user. For more information, refer to the *Installation Guide - Stage 1, APPENDIX B. Variables Used in the Silent Properties File,* section - *Services Variables' web_service_user.*
service_url	This attribute specifies the URL to be used by the webservice to call the Alert/Case Assigner. For Service URL, refer to the *Services Guide* section - *Post Alert Service, Service Requests.*

Note: Once user name and URL is set, set its password using Encrypt Utility.

To set password, follow these steps:

1. Login as OFSECM Administrator.
2. Navigate to Administration menu > Web Services Configuration > Common Web Services.
3. Enter password for `web_service_user` in **Enter Password for Assigner Web Service** text box.
4. Click **Ecrypt**.

Enter the same password set using `changePasswords.sh` all during OFSBDF installation. For more information, refer to the *Installation Guide - Stage 1,* section *Setting All Passwords.*

Configuring File Size

By default the size supported by attachment is 1 MB. If you want to attach files greater than 1 MB size using the Save and Attach button, follow these steps:

1. Open file `$FIC_HOME/EXEWebService/<WebSphere or Weblogic or Tomcat>/ROOT/conf/DynamicWSConfig.xml`
2. Update from:

   ```
   <PROPERTY NAME="MAXFILESIZE" VALUE="1024000"/>
   ```

   to:

   ```
   <PROPERTY NAME="MAXFILESIZE" VALUE="<desired value in bytes up to 10MB>"/>
   ```
3. Recreate the `ExeWebservices ear` file and redeploy it.
4. Restart the web application server.

The size that is allowed to be attached while performing document attachment action should be configured in Configuration table of OFSSAAI configuration schema in its `PARAMVALUE` column where `PARAMNAME` is `DOCUMENT_MAX_SIZE`.

Configuring Views

Views help you to quickly view search results based on pre-defined search queries.

Adding Views

To add views, follow these steps:

1. Make entry in the KDD_QUEUE_MASTER table.

Table 7. KDD_QUEUE_MASTER table

QUEUE_SEQ_ID	QUEUE_CD	QUEUE_DISPLAY_NM	QUEUE_TYPE	QUEUE_QUERY
Unique sequence ID	Unique Queue Code	The name of the view that will be displayed in the UI	**AL**: if the view is related to Alert **CA** : If the view is related to Cases	Corresponding Query for the view which filters the case/alert List

2. Map Queue in the KDD_QUEUE_ROLE_MAP table.

Table 8. KDD_QUEUE_ROLE_MAP table

QUEUE_SEQ_ID	ROLE_CD
Queue sequence id as given in the above table	Role code

Modifying Views

Following are the various modifications for views:

1. **Modify An Existing View Query**

   In order to modify the underlying query of a view, changes are to be done in the KDD_QUEUE_MASTER.QUEUE_QUERY column.

2. **Modifying View-Role Mapping**

   In order to make a view available for an existing role , the mapping has to be done in KDD_QUEUE_ROLE_MAP table.

3. **Modifying the Display Name of the View**

   In order to change the display name for a particular view, changes have to be done in KDD_QUEUE_MASTER.QUEUE_DISPLAY_NM column.

Removing Views

To remove a view, entries for that view must be deleted from the KDD_QUEUE_MASTER table and KDD_QUEUE_ROLE_MAP table

```
Delete KDD_QUEUE_MASTER where QUEUE_SEQ_ID = <View Sequence Id>; Delete KDD_QUEUE_ROLE_MAP
 where QUEUE_SEQ_ID = <View Sequence Id>; COMMIT;
```

Note: Incase the view that was removed is set as the default view in Preferences, then preferences must be reset. Else, Views will be displayed as blank values in the UI.

CHAPTER 2 Alert Management Configuration

This chapter provides instructions for configuring parameters specific to alert management and includes the following topics:

- Configuring a Visual Cue
- Configuring New Alert Score
- Configuring Alert Inheritance
- Configuring Four Eyes Approval
- Configuring Highlights
- Configuring Alert Highlight Status
- Configuring Default Selection of MAMC versus MASC Option
- Configuring Organization Relationships for Trade Blotter
- Configuring Search Criteria Population Options for Trade Blotter
- Configuring Trusted Pair Duration Option
- Configuring Suppression Rule Duration
- Configuring Default Alert Owner
- Manage Security Restrictions
- Manage Controlling Customer

Configuring a Visual Cue

This section describes configuring visual cue for the following:

- For Alerts Nearing Due Date
- For Alert Suppression Nearing Expiration Date
- For the Trusted Pair Nearing Expiration Date

For Alerts Nearing Due Date

You can configure a time period for alerts that signals when they are approaching their due date. When the specified time period is reached or passed, the due date column (Due) displays the dates highlighted in red.

To configure a time period that signals when an alert or case is approaching its due date, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Near Due Date** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

For Alert Suppression Nearing Expiration Date

When an alert suppression rule approaches its date of expiration, the Expiration Date column of the Managed Suppression Rule List page displays a visual indicator that the rule is nearing expiration. You can modify, how many days prior to the expiration date the UI will display that visual indicator.

For the Trusted Pair Nearing Expiration Date

When a trusted pair approaches its date of expiration,, the Expiration Date column of the Trusted Pair List page displays a visual indicator that the pair's trust period is nearing expiration. You can modify how many days prior to the expiration date the UI will display that visual indicator.

To modify the Near Due Date parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Near Due Date** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 9. Configuring Trusted pair Nearing Expiration Date

Attribute	Description
MSR_Near	This attribute specifies the number of days to be considered before the expiration of a suppression in order to color code the suppression in the UI.
MTP_Near	This attribute specifies the number of days to be considered before the expiration of a trusted pair in order to color code the trusted pair in the UI.
AL_Near	This attribute specifies the number of days to be considered before the due date of an alert in order to color code the alert as a near due alert in the UI.

Configuring New Alert Score

This parameter specifies the score to be assigned to a newly created alert from the New Alert workflow. It includes the Default, Minimum, and Maximum Score to be assigned to the alert. The parameter value accepts only natural numbers.

To modify the New Alert Score, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **New Alert Score** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

   Note: Default score for an alert can be modified by the user at the time they create the new alert.

Table 10 describes the attributes which must be configured for the Notification parameter.

Table 10. Configuring New Alert Score Attributes

Attribute	Description
MIN_SC	Minimum score that a newly created alert is allowed to hold.
MAX_SC	Maximum score that a newly created alert is allowed to hold.
DEFAULT_SC	• Specifies the default alert score which is set for a newly created alert. • DEFAULT_SC value is to be set in between the MIN_SC and MAX_SC value.

Configuring Alert Inheritance

This parameter is used for enabling and disabling Alert Inheritance. The allowed values are Y and N. If set to Y, the system automatically assigns ownership of an alert owned by pools (as long as it is not in a closed status) to the user who has selected to view the alert. If set to N, alert ownership is not inherited by a user just by viewing the alert.

Note: The default value is Y.

To modify the Alert Inheritance parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Alert Inheritance** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Four Eyes Approval

This parameter is used to enable and disable Four Eyes Approval. This parameter defines the workflow of an alert while it is being investigated. The actions available to the Analyst and Supervisor user depend upon this parameter. The parameter value can have only Y or N value. The value Y enables Four Eyes Approval which allows an Analyst to only recommend certain actions (most commonly are the actions associated with closing alerts) and requires a Supervisor to approve the action. The value N disables Four Eyes Approval, allowing analysts to take actions without requiring supervisor approval.

Note: The default value is N.

To modify the Four Eyes Approval, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Four Eyes Approval** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Highlights

This parameter specifies the default value of highlights to be pre-populated on an alert for new alert creation.

To modify the highlight, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Highlight** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

   Note: The default highlight is editable by users on the created alert.

Configuring Alert Highlight Status

This parameter specifies the list of Alert statuses to be highlighted in **bold** font when displayed in the UI. Making bold font for certain statuses ensures that alerts with the corresponding statuses are more easily identified when in a list with other alerts.

To modify the Alert Highlight Status, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Alert Highlight Status** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Default Selection of MAMC versus MASC Option

This parameter allows clients to specify which option would be selected by default when user is promoting multiple alerts to a case. The parameter value can be Multi Alert Multi Case (MAMC) or Multi Alert Single Case (MASC).

To modify the Default Selection of the MAMC versus MASC Option parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Default selection of MAMC versus MASC** option from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Organization Relationships for Trade Blotter

This parameter specifies the organization relationship code which is used in Trade Blotter.

To modify the Application Server Parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Organization Relationship** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 11 describes the attributes which should be configured for the configuring Organization Relationship option.

Table 11. Configuring Organization Relationships for Trade Blotter Attributes

Attribute	Description
Organization To Division Relationship	This attribute provides a list of values that identify which Relationship Type values from your Organizational Relationship data feed are to be considered Organization-to-Division relationships.
Division To Branch Relationship	This attribute provides a list of values that identify which Relationship Type values from your Organizational Relationship data feed are to be considered Division-to-Branch relationships.
Trading Desk	This parameter provides a list of values that identify which Organization Type values from your Organization data feed are to be considered Trading Desks.

Configuring Search Criteria Population Options for Trade Blotter

Within the Trade Blotter utility users have the ability to search for Trades based upon Trade Characteristics, Product Type and Product Subtype associated with the product being traded.

The definition of Trade Characteristics, Product Type, and Product Subtype for Trade records in the Oracle FSDM are client specified. In order to have populated values for the Trade Blotter Trade Characteristics, Product Type, and Product Subtype search filters it is necessary to add the distinct list of your firm's Trade Execution, Trade Characteristics, Product Types, and Product Subtypes to the Code Set Translation (KDD_CODE_SET_TRNLN) table.

This section covers the following topics:

- Adding Product Types to the Code Set Translation Table
- Adding Product Subtypes to the Code Set Translation Table
- Adding Trade Characteristics to the Code Set Translation Table

Adding Product Types to the Code Set Translation Table

To add product types to the Code Set Translation table, follow these steps:

1. Insert the following information into KDD_CODE_SET_TRNLN for Trade Execution Product Type:
   a. CODE_SET - populate with ProductType as the Code set name. You must use this as the name for the Product Type code set.
   b. CODE_VAL - populate with a distinct value as would appear in the FSDM for a Trade record for Product Type.
   c. CODE_DISP_TX - populate with the display value of the product type code to be shown in the UI search filter.
   d. SRC_SYS_CD - populate with 'MTS'.
2. Repeat this for all distinct Product Type codes that are present in the Trade data.

Example:
```
insert into kdd_code_set_trnln
(code_set, code_val, src_sys_cd, code_disp_tx)
values
('ProductType',
 '[Product Type Code]',
 'MTS',
 '[Display value of Product Type]')
```

Adding Product Subtypes to the Code Set Translation Table

To add product subtypes to the Code Set Translation table, follow these steps:

1. Insert the following information into KDD_CODE_SET_TRNLN for Trade Execution Product Subtype:
   a. CODE_SET - populate with ProductSubtype as the Code set name. You must use this as the name for the Product Subtype code set.
   b. CODE_VAL - populate with a distinct value as would appear in the FSDM for a Trade record for Product Subtype.
   c. CODE_DISP_TX - populate with the display value of the product subtype code to be show in the UI search filter.
   d. SRC_SYS_CD - populate with 'MTS'.
2. Repeat this for all distinct Product Subtype codes that are present in the Trade data.

Example:
```
insert into kdd_code_set_trnln
(code_set, code_val, src_sys_cd, code_disp_tx)
values
('ProductSubtype',
'[Product Sub-Type Code]',
'MTS',
'[Display value of Product Sub-Type]')
```

Adding Trade Characteristics to the Code Set Translation Table

To add Trade Characteristics to the Code Set Translation table, follow these steps:

1. Insert the following information into KDD_CODE_SET_TRNLN for Trade Execution Product Subtype:
   a. CODE_SET - populate with TradeBlotterTradeTypeCode as the Code set name. You must use this as the name for the Trade Characteristics code set.
   b. CODE_VAL - populate with a distinct value as would appear in the FSDM for a Trade record for Trade Characteristics.
   c. CODE_DISP_TX - populate with the display value of the Trade Characteristics code to be shown in the UI search filter.
   d. SRC_SYS_CD - populate with 'MTS'.
2. Repeat this for all distinct Product Subtype codes that are present in the Trade data.

Example:
```
insert into kdd_code_set_trnln
(code_set, code_val, src_sys_cd, code_disp_tx)
values
(' Trade Characteristics',
'[Trade Characteristics Code]',
'MTS',
'[Display value of Trade Characteristics]')
```

Configuring Trusted Pair Duration Option

This parameter specifies the number of months the trusted pair remains active. Trusted pairs can be configured in months. This parameter contain two parts:

- Creating the Duration for Trusted Pair
- Extending the Duration for Trusted Pair

Creating the Duration for Trusted Pair

To create the duration option, in months, that a pair of entities are considered trusted, follow these steps:

1. In the config schema, back up the `forms_control_option` table.
2. Run the following query, to display your current trusted pair settings:

   ```
   select t.* from forms_control_options t where
   t.form_code='Aml_TP_Dsgnt' and t.control_id=30
   ```

3. Run the following query to update your current trusted pair settings:

   ```
   update forms_control_options t set t.option_key=<number of
   month>,t.option_value=<Value to be display in UI>
   where t.form_code='Aml_TP_Dsgnt' and t.control_id=30 and t.option_key=<Period which
   needs to be modify>
   Example:
   update forms_control_options t set t.option_key=7
   ,t.option_value='7 month'
   where t.form_code='Aml_TP_Dsgnt' and t.control_id=30
   and t.option_key=6
   ```

4. Run the following query to insert the new period:

   ```
   insert into FORMS_CONTROL_OPTIONS (FORM_CODE, CONTROL_ID, OPTION_KEY, OPTION_VALUE,
   DSN_ID, LOCALE, ALIGN)
   values ('Aml_TP_Dsgnt', 30, '<Number of month>', '<Value to be display in UI>', '<Alert
   Management Infodom>', 'en_US', 'H')
   Example:
   insert into FORMS_CONTROL_OPTIONS (FORM_CODE, CONTROL_ID, OPTION_KEY, OPTION_VALUE,
   DSN_ID, LOCALE, ALIGN)
   values ('Aml_TP_Dsgnt', 30, '12', '12 month', 'AMINFO', 'en_US', 'H')
   ```

Extending the Duration for Trusted Pair

To extend the duration option, in months, that a pair of entities are considered trusted, follow these steps:

1. In the config schema, back up the forms_control_option table.
2. Run the following query to display your current trusted pair settings:

```
select t.* from forms_control_options t where
t.form_code='Aml_TP_Updt' and t.control_id=30
```

3. Run the following query to update your current trusted pair settings:

```
update forms_control_options t
set t.option_key=<number of month>,t.option_value=<Value to be
display in UI>
where t.form_code='Aml_TP_Updt' and t.control_id=30 and t.option_key=<Period which
needs to be modify>
Example:
update forms_control_options t set t.option_key=7
,t.option_value='7 month'
where t.form_code='Aml_TP_Updt' and t.control_id=30
and t.option_key=6
```

4. Run the following query to insert the new period:

```
insert into FORMS_CONTROL_OPTIONS (FORM_CODE, CONTROL_ID, OPTION_KEY, OPTION_VALUE,
DSN_ID, LOCALE, ALIGN)
values ('Aml_TP_Updt', 30, '<Number of month>', '<Value to be display in UI>', '<Alert
Management Infodom>', 'en_US', 'H')
Example:
insert into FORMS_CONTROL_OPTIONS (FORM_CODE, CONTROL_ID, OPTION_KEY, OPTION_VALUE,
DSN_ID, LOCALE, ALIGN)
values ('Aml_TP_Updt', 30, '12', '12 month', 'AMINFO', 'en_US', 'H')
```

Configuring Suppression Rule Duration

This parameter specifies the number of months that the suppression rule remains active. You cannot create suppression rule duration, but you can update or extend the duration by following these steps:

1. In the config schema, back up the `forms_control_option table`.
2. Run the following query to display the current suppression rule settings:

```
select t.* from forms_control_options t where t.form_code=' Aml_Sup_Updt' and
t.control_id=10
```

3. Run the following query to modify the current suppression rule settings:

```
update forms_control_options t
set t.option_key=<number of month> ,t.option_value=<Value to be display in UI>
where t.form_code=' Aml_Sup_Updt ' and t.control_id=10
```

Configuring Default Alert Owner

Allows the client to specify the user or user pool to which cases created through promotion of an alert or manual creation is assigned to. This allows for specification of Owner and Assign To users.

To modify the Alert Owner, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Alert Owner** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 12. Configuring Default Alert Owner

Attribute	Description
DEF_OWNER	This parameter specifies the owner for the Alert.

Manage Security Restrictions

The Manage Security Restriction workflow on the UI can be enabled and disabled by mapping or unmapping the function **Manage Security Restrictions** (AMSECRST) from the corresponding User Roles. This function is already mapped to required roles and pre packaged in the Installer.

Note: The application supports managing security restrictions either through the UI or through DIS files. These options are mutually exclusive.

Manage Controlling Customer

The Manage Controlling Customers workflow on the UI can be enabled and disabled by mapping or unmapping the function **Manage Controlling Customer** (AMCTRLCUST) from the corresponding User Roles. This function is already mapped to required roles and pre packaged in the Installer.

Refer to the *Oracle Financial Services Analytical Applications Infrastructure User Manual Release 7.3,* for more information about mapping/un mapping functions to roles.

Note: The application supports managing controlling customer either through the UI or through DIS files. These options are mutually exclusive.

CHAPTER 3 Administration Tools Configuration

This chapter provides instructions for configuring parameters specific to administration tools.

This chapter covers the following topics:

- Configuring Administration Tools
- Configuring Application Server

Configuring Administration Tools

This parameter specifies the web application context and URL of the admin tools application.

Follow these steps incase admin tools deployed web application context and URL were different from the default values populated by the Installer.

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Admin Tool** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 13 describes the attributes which should be configured for enabling and using the administration tools.

Table 13. Configuring Administration Tools

Attribute	Description
APPLICATION_CONTEXT	This parameter specifies the context name of admin tools application.
ADMINISTRATION_TOOLS_APPLICATION_URL	This parameter specified the URL of admin tools application.

Configuring Application Server

This parameter specifies the OFSAAI Application Server IP Address and Java Port.

Follow these steps if in case the values were different from the default values populated by the Installer.

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Application Server** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 14 describes the attributes to be configured for setting the application server.

Table 14. Configuring Application Server

Attribute	Description
Application Server IP	This parameter specifies Oracle Financial Services Analytical Applications Infrastructure Application server IP address/server name details required for admin tools.
Application Server Port	This parameter specifies Oracle Financial Services Analytical Applications Infrastructure Application server port details required for admin tools.

CHAPTER 4 Case Management Configuration

This chapter provides instructions for configuring parameters specific to Case Management. This chapter includes the following sections:

- Configuring a Visual Cue for Cases Nearing Due Date
- Configuring Case Inheritance
- Configuring Case Prefix
- Configuring Case Assignment Inheritance
- Configuring Highlights for Case Status
- Configuring Case Own Flag Consideration
- Configuring Mode of Transferring Alert Information
- Configuring Mode of Transferring Case Information
- Configuring Case Age Calculation
- Configuring Case Risk Values
- Configuring Case Correlation Owner
- Configuring Default Case Owner

Configuring a Visual Cue for Cases Nearing Due Date

You can configure a time period for cases that signals when they are approaching their due date. When the specified time period is reached or passed, the due date column (Due) displays the dates in highlighted red.

To configure a time period that signals when a case is approaching its due date, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Case Near Due Date** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 15. Configuring a Visual Cue for Cases Nearing Due Date

Attribute	Description
CM_Near	This attribute specifies the number of days to be considered before the due date of a case in order to color code the case as a near due case in the UI.

Configuring Case Inheritance

This parameter specifies the status of Case Inheritance for the installation. The parameter can have only Y or N values.

If set to Y, the case ownership changes for cases when in New or Reopened statuses based on the rules defined for case inheritance. If set to N, then ownership does not change when a user accesses the case.

If set to Y the system automatically assigns ownership of a case owned by pools (as long as not in a closed status) to the user who has selected to view the case. If set to N, case ownership is not inherited by a user just by viewing the case.

To modify the Case Inheritance parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Case Inheritance** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Case Prefix

This parameter specifies the non numeric value to be prefixed before the Case ID while displaying the Case ID in the UI.

To modify the Case Prefix parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI display** from the Parameter category drop-down list.
3. Select **Case Prefix** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Case Assignment Inheritance

This parameter specifies the status of Case Assignment Inheritance for the installation. The parameter can have only Y or N values. If set to Y and if the current Assign To user of the case is a pool (not an individual user), then the current user inherits as the Assign To user of the case. If set to N, then the Assign To user is not changed just by a user viewing the case.

Note: The default value is Y.

To modify the Case Assignment Inheritance parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Case Assignment Inheritance** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Highlights for Case Status

This parameter specifies the list of case statuses to be highlighted in **Bold** font when displayed in the UI. Making bold font for certain statuses ensures that cases with corresponding statuses are more easily identified when in a list with other cases.

To modify the Case Highlight Status for status codes, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Case Highlight Status** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Case Own Flag Consideration

This parameter specifies if a user should be checked for their case owning eligibility before they are assigned the case. The parameter should have only Y or N values. If the value is set to Y, then only those users who have access privileges to the case and are also eligible to own a case are displayed in the Assign To fields. If set to N, then all users who have access privileges to the case, regardless of their eligibility to own a case, are displayed in the Assigned to fields.

Note: The default value is Y.

To disable the Case Own Flag Consideration, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Case Own Flag Consideration** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Mode of Transferring Alert Information

This parameter specifies the mode in which business data from an alert to a case is transferred during Promote to Case or Link actions. The parameter value can have only S or A value. Synchronous (S) restricts the user from working on the alert or case until the data transfer action is complete. Asynchronous (A) allows the user to continue to work on the alert or case, while the data transfer is being carried out in the background.

Note: The default value is synchronous (S).

To modify the Mode of Transferring Alert Information, follow these steps:

1. Open the Manage Common Parameters screen.
2. Select **Used for design** from the Parameter Category drop-down list.
3. Select **Mode of Transferring Alert Information** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Mode of Transferring Case Information

This parameter specifies the mode in which case information is transferred during Merge Action and is applicable for implementations which have installed Oracle Financial Services Enterprise Case Management. The parameter value can have only S or A value. S (Synchronous) restricts the user from working on the alert or case until the data transfer action is complete. A (Asynchronous) allows the user to continue to work on the alert or case, while the data transfer is being carried out in the background.

Note: The default value is synchronous (S).

To modify the Mode of Transferring Case Information, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Mode of Transferring Case Information** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Case Age Calculation

This parameter allows the client to specify whether the calculation of the age of a case is to be done in Calendar or Business days. The param value can be either C or B.

Note: The default value is Business (B).

To modify the Case Age Calculation parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Case Age Calculation** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Case Risk Values

This parameter allows deployment level configuration of the minimum and maximum range of risk values during add and edit feature in Case related business tabs.

To modify the Case Age Calculation parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Case Risk Values** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 16. Configuring Case Risk Values

Attribute	Description
Min Risk Value	Will define the minimum value of all the types of risks; will have a default value of -2.
Max Risk Value	Will define the maximum value of all the types of risks; will have a default value of 10.

Configuring Case Correlation Owner

This parameter specifies the users or user pools who should be assigned as the *Owner* and *Assign To* users for cases created through correlation promotion. The users or user pools that need to be assigned as the *Owner* and *Assign To* users are identified from other attributes of this parameter based on the case type. Here every attribute specifies an owner for a Case Type Sub Type. Some of the Case Type Sub Type will be prepackaged.

Client can specify new case type sub type and default owner for the case type subtype. To add new case type sub type, follow these steps:

1. If the Case Correlation Owner parameter has used up to attribute 4, then use the following query:

   ```
   update kdd_install_param set kdd_install_param.attr_5_cd='<Case Type Sub Type>'
   ,kdd_install_param.attr_5_value_tx='<Owner>'
   where kdd_install_param.param_id=30 and kdd_install_param.param_nm='Case Correlation
   Owner 1'
   ```

2. If all the attributes have been filled then add one more case correlation owner Parameter. To add another Correlation parameter, follow these steps:

   a. Get maximum param ID of `kdd_install_param` table by running the following query.
   `select max (param_id) from kdd_install_param`.

   b. Insert into `kdd_install_param (param_id, param_nm, param_value_tx, param_cat_cd,param_desc_tx)` values

   `(< Max Param id > +1,'Case Correlation Owner 2','Y','Used for Design',`

This parameter specifies the users or user pools who should be assigned as the *Owner* and *Assign To* users for cases created through correlation promotion. The parameter value by default is kept as Y but can also be changed and the same is not validated. The users or userpools who need to be assigned as the Owner and Assign To users are identified from other attributes of this parameter based on the case type.

c. To add new case type sub type and owner use the query mentioned in step 1 after replacing the filter clause with the new param ID and name.

To modify the Case Correlation Owner for an existing Case Type Sub Type, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Case Correlation Owner** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 17. Configuring Case Correlation Owner

Attribute	Description
DEF_OWNER	This attribute specifies the default Case owner. **Note:** The attribute value can have only one user ID ● Should be the same as of `KDD_REVIEW_OWNER.OWNER_ID` ● Should have Case role and ● Have access to all the security attributes defined in the Security Attribute Administration User Interface, if not the alerts would not be assigned to any user.

Configuring Default Case Owner

This parameter allows the client to specify the default user or user pool to which cases created through promotion of an alert or manual creation will be assigned to. This allows for specification of default *Owner* and *Assign To* users. Some of the Case Type Sub Type will be prepackaged.

Client can specify a new case type sub type and default owner for the case type subtype. To add new case type sub type, follow these steps:

1. If the Default Case Owner parameter has used up to attribute 4 then use following query:

   ```
   update kdd_install_param set kdd_install_param.attr_5_cd='<Case Type Sub Type>'
   ,kdd_install_param.attr_5_value_tx='<Owner>'
   where kdd_install_param.param_id=33 and kdd_install_param.param_nm= 'Default Case Owner
   1'
   ```

2. If all the attributes have been filled then add one more case correlation owner Parameter. To add another Correlation parameter, follow these steps:

   a. Get the maximum param ID of `kdd_install_param` table by running the following query:

      select max`(param_id)` from `kdd_install_param`

   b. Insert into kdd_install_param (`param_id, param_nm, param_value_tx, param_cat_cd, param_desc_tx`) values

      `(< Max Param id > +1, ' Default Case Owner 2','Y', 'Used for Design',`

      This attribute specifies the default user or user pool who should be assigned as the Owner and Assigned To user for correlated cases for case types that are not mentioned in other attributes of this parameter).

   c. To add new case type sub type and owner, use the query mentioned in step 1 after replacing the filter clause with the new param ID and name.

To modify the Default Case Owner for existing Case Type Sub Type, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Default Case Owner** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Table 18. Configuring Case Owner

Attribute	Description
DEF_OWNER	This attribute specifies the default Case owner. **Note:** The attribute value can have only one user id ● Should be the same as of `KDD_REVIEW_OWNER.OWNER_ID` ● Should have Case role and ● Have access to all the security attributes defined in the Security Attribute Administration User Interface, if not the alerts would not be assigned to any user.

CHAPTER 5 Assessment Configuration

This chapter discusses the following topics.

- Configuring Assessment related Installation Parameters
- Configuring Assessment Related Application Parameters
- Configuring Assessment Related Risk Value Scores

Configuring Assessment related Installation Parameters

This section provides instructions for configuring parameters specific to Risk Assessment. This section includes the following topics:

- Configuring Callable Service Definition
- Configuring Message Logging Definition
- Configuring RAOR Service Definition
- Configuring Customer Feedback Files
- Configuring Watch List Feedback Files
- Configuring Watch List Scores for Promotion
- Configuring Encryption - Decryption Details
- Configuring Jurisdiction Specific Assessments
- Configuring Purge of Risk Assessment Repository
- Configuring Dates for Periodic Review - Deployment Initiation Customers
- Configuring Document Attachment Details
- Configuring Request XSD Location Definition
- Configuring Watch List Scanning for Batch Processing

Configuring Callable Service Definition

This parameter specifies the details of the User ID, Password, and URL for the application to invoke the Callable Service FW to enable. The parameter value must always be *Y*, which is the default and mandatory value. This value is prepackaged as a part of the application.

To modify the Callable Service Definition, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **Callable Service Definition** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 19. Configuring Callable Service Definition Attributes

Attribute	Description
USERID	This attribute specifies the login User ID for Callable Service Frame Work URL that is used by the KYC system internally. **Note:** The value provided here must be a valid OFSSAI User ID with rule execution privilege.
PASSWRD	This attribute specifies the password to access the Callable service FW URL. This field can accept only string. This password must be in-line with the password registered for the User ID in the OFSSAI SMS.
Url	This attribute specifies the URL for the OFSSAI Callable Service FW. This field can accept only a valid URL. If this URL is incorrect, the KYC Callable service will not be invoked thus failing the UI operations. **Note:** `http://localhost:9080/EXEWebServiceAXIS/EXEWebService` is the placeholder provided.
INFODOM	This attribute specifies the name of the Information Domain on which the KYC application is defined. This is required for invoking OFSSAI Callable Service FW. This field can accept only a string. If the Infodom name is incorrect, then the KYC Callable service will not be invoked and will fail the UI operations.
SEGMENT	This attribute specifies the name of the segment required for invoking OFSSAI Callable Service FW. This field can accept only a string. If the Segment is incorrect the OFSSAI Callable service will not be invoked and will fail the UI operations.

Configuring Message Logging Definition

This parameter enables the Logging of Errors. The parameter value can have only Y or N value. *Y* enables logging of errors and *N* disables logging of errors. The Pre-packaged value is *Y*.

To modify the Message Logging Definition, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **Message Logging Definition** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 20. Configuring Message Logging Definition Attributes

Attribute	Description
LOG_LEVEL	This field specifies the level of the logs to be written while processing. The field can have 1, 2, 3 as values. 1 is the default value; it can be changed to 2 or 3 for debugging purposes. • **1** indicates logging only the exceptions and warnings • **2** indicates logging of exceptions, warnings and data/information that was processed • **3** indicates number of records processed in a loop in addition to logging of exceptions, warnings, and data/information that was processed **Note:** 1 is the default value.

Configuring RAOR Service Definition

This parameter specifies details required for the Real Time Account On Boarding Risk Rating. The parameter value should be Y, which is the default and mandatory value. This value is prepackaged as a part of KYC application.

To modify the RAOR Service Definition, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **RAOR Service Definition** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 21. Configuring RAOR Service Definition Attributes

Attribute	Description
USERNAME	This attribute specifies the user name of the financial institution which will be used for invoking the RAOR service. This attribute value can accept only string values and should be configured during implementation of KYC.
PASSWORD	This attribute specifies the password required for RAOR service. This attribute value can accept only string values and should be configured during implementation of KYC. The password should be in encrypted. service by the account opening system.

Configuring Customer Feedback Files

This parameter enables the renaming of feedback file generated by the KYC application to a different naming format. The parameter value can have only Y or N value. *Y* enables renaming the feedback file, and *N* disables renaming of the file.

Note: *Y* is the default value.

To modify the Customer Risk Interface - Rename Properties, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **Customer Risk Interface - Rename Properties** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 22. Configuring Customer Risk Interface - Rename Properties Attributes

Attribute	Description
File Movement	This attribute specifies whether the renamed feedback files are to be moved to a different staging directory. The field can have only *Y* or *N* value. *Y* enables movement of files, and *N* disables movement of files. **Note:** *Y* is the default value.
History Required	This field specifies whether the history has to be maintained for the renamed files. This field can either have *Y* or *N* value. *Y* enables history and *N* disables history. **Note:** *Y* is the default value.
Destination Path	This field specifies the destination folder for storing the renamed file. This field can accept only string values. The path provided has to be valid and accessible. **Note:** /ftpshare/SaveDocument is a placeholder.
Source Path	This field specifies the source path of the renamed feedback file. This field accepts only string values. The path provided has to be valid and accessible. **Note:** /ftpshare/STAGE/KYCsource is a placeholder.
OFSAAI FileName	This attribute specifies the static part of the KYC account feedback file name. **Note:** GenCustDetails_ED is the default and the mandatory value which must not be changed.
File Context	This attribute specifies the static part of the KYC customer feedback file name. **Note:** CUST is the default and mandatory value which must not be changed.
Batch Name	This attribute specifies the batch for which this data file is being provided. The batch will be executed daily at end of day. **Note:** DLY is the default and mandatory value which must not be changed.
File Sequence	This attribute specifies the sequence number that labels each new instance of the file provided during a processing batch. The value is to be changed if there is any change in the file sequence. **Note:** 101 is the default value.
History Location	This field specifies the location for storing the history of the renamed files. History files will be created before the rename/movement of files. This field can accept only valid string value. The path provided has to be valid and accessible. **Note:** /ftpshare/TempDocument is the placeholder.
File Extension	This field specifies extension of the file generated.

Configuring Watch List Feedback Files

This parameter enables the renaming of feedback file generated by the KYC application to a different naming format. The parameter value can have only Y or N value. *Y* enables renaming the feedback file, *N* disables renaming the feedback file.

Note: *Y* is the default value.

To modify the KYC Watch List Interface - Rename Properties, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **KYC Watch List Interface - Rename Properties** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 23. Configuring KYC Watch List Feedback Files

Attribute	Description
File Movement	This attribute specifies whether the renamed feedback files have to be moved to a different staging directory. The field can have only Y or N value. *Y* enables movement of files, and *N* disables movement of files. **Note:** *Y* is the default value.
History Required	This field specifies whether the history to be maintained for the renamed files. This field can either have Y or N value. *Y* enables history and *N* disables history. **Note:** Y is the default value.
Destination Path	This field specifies the destination folder for storing the renamed file. This field can accept only string values. The path provided has to be valid and accessible. **Note:** `/ftpshare/SaveDocument` is a place holder
Source Path	This field specifies the source path of the renamed feedback file. This field accepts only string values. The path provided has to be valid and accessible. **Note:** `/ftpshare/STAGE/KYC`source is a placeholder.
OFSAAI FileName	This attribute specifies the static part of the KYC Watch List feedback file name. **Note:** `GenWLSFeedback_ED i`s the default and the mandatory value which is not supposed to be changed.file name. This value is prepackaged as a part of KYC application.
File Context	This attribute specifies the static part of the KYC Watch List feedback file name. **Note:** WLS is the default and the mandatory value which is not supposed to be changed.
Batch Name	This attribute specifies the batch for which this data file is being provided. The batch will be executed daily at EOD. **Note:** DLY is the default and mandatory value which is not supposed to be changed.
File Sequence	This attribute specifies the sequence number that labels each new instance of the file provided during a processing batch. This can be changed if there is any change in file sequence. **Note:** 101 is the default value.

Table 23. Configuring KYC Watch List Feedback Files

History Location	This field specifies the location for storing the history of the renamed files. History files will be created before the rename / movement of files. This field can accept only valid string value. The path provided has to be valid and accessible. **Note:** `/ftpshare/TempDocument` is a placeholdercan accept only valid string value. The path provided has to be valid and accessible.
File Extension	This field specifies extension of the File generated.

Configuring Watch List Scores for Promotion

This Parameter defines the Watch List Score for RA promotion to a Case if the Primary Customer or Interested Parties watch list score is greater than or equal to the score defined in the parameter value. It accepts only natural numbers.

Note: This is an exception to the requirement of RA promotion of a case based on a pre-defined score.

To modify the Watch List Scores for Promotion, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **Watch List Scores for Promotion** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Configuring Encryption - Decryption Details

This parameter specifies information about the Encryption and Decryption of Password. The parameter value should be Y, which is the default and mandatory value. This value is prepackaged as a part of KYC application.

To modify the Encryption - Decryption Details, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **Encryption - Decryption Details** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 24. Configuring Encryption - Decryption Details Attributes

Attribute	Description
ENCRYPT KEY LOCATION	This field specifies the location in which encryption key is kept. This field accepts only string values. The location (Path) provided here should be valid and accessible. **Note:** `/home/gsh/ftpshare/KYC/key.des` is a placeholder.

Configuring Jurisdiction Specific Assessments

This parameter defines the need for risk processing based on Jurisdictions. The value for this parameter can be either Y or N.

If the value is *Y* then there needs to be an attribute value. The risk processing would be done for the customers belonging to the jurisdiction value provided.

If the value is *N* then the risk processing would be carried over for all the jurisdictions.

To modify the Specific Jurisdiction Processing, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **Specific Jurisdiction Processing** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 25. Configuring Jurisdiction Specific Assessments

Attribute	Description
JRSDN_PRCNG	This attribute specifies the jurisdiction key value for which the risk processing has to be processed. **Note**: The values provided here has to match with Jurisdiction Codes available in `KDD_JRSDN`. If jurisidction specifc processing is not required then *All* has to be updated in the value which is the default value.

Configuring Purge of Risk Assessment Repository

This parameter defines the number of months the risk assessment repository table data needs to be purged.

To modify the Purge of Risk Assessment Repository, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **Purge of Risk Assessment Repository** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 26. Configuring Purge of Risk Assessment Repository Attributes

Attribute	Description
TOTAL_PART_NUMBERS	This attribute specifies the number of months after which the data of risk assessment repository to be purged. **Note:** 12 is the default value.

Configuring Dates for Periodic Review - Deployment Initiation Customers

This parameter defines the periodic review date for Deployment Initiation customers by splitting the customer base into equal slices per day starting from the number of days defined in the attribute.

Note: *Y* is the default and mandatory value.

To modify the Dates for Periodic Review - Deployment Initiation Customers, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **Dates for Periodic Review - Deployment Initiation Customers** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 27. Configuring Dates for Periodic Review - Deployment Initiation Customers Attributes

Attribute	Description
NXTREVCNT	This attribute specifies the number of days from when the customers have to be identified for next periodic re-review date. If the value provided is x days, the system would start picking up the customers after x number of days from closure of the risk assessments. **Note:** 730 is the default value.
NUM_OF_CUST	This attribute specifies the number of deployment initiation customers to be risk assessed for periodic review per day. **Note:** 6000 is the default value.

Deployment Initiation Customers Periodic Review depends on the value provided for the attributes of Setting Dates for Periodic Review - Deployment Initiation Customer parameter in Application Installation parameter table.

For Example: The bank can decide to perform the periodic review of the customers based on the number of days and the number of customers to be considered per day.

Configuring Document Attachment Details

This parameter specifies the directory path for uploading the documents submitted by the customer during default review process for the newly opened accounts in KYC application. *Y* is the default and mandatory value which is prepackaged as a part of KYC application.

To modify the Document Attachment Details, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **Document Attachment Details** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 28. Configuring Document Attachment Details Attributes

Attribute	Description
Doc Path	This attribute specifies the Directory path to upload the documents. This field can accept only string values. The path provided has to be valid and accessible. **Note:** `/home/gsh/ftpshare/Temp/` is a placeholder.
Temp Directory	This attribute specifies the temporary directory in the server in which the documents to be loaded before uploading to the permanent directory. This field can accept only string values. The path provided has to be valid and accessible. **Note:** `/home/gsh/ftpshare/TempDocument` is a placeholder.
Save Directory	This attribute specifies the actual directory in the server where the documents will be uploaded permanently. This field can accept only string values. The path provided has to be valid and accessible. **Note:** `/home/gsh/ftpshare/upload` is a place holder.
Web Server IP	This attribute specifies the Web Server IP address. The server IP provided has to be valid and accessible. **Note:** 127.0.0.1 is a placeholder.
Uploading User	This attribute specifies the User ID of the default user who is uploading the document. The User ID has to be a valid user which is defined in KYC processing.
Fic Home	This attribute specifies the path of application directory. The path should be valid and accessible. **Note:** `/home/gsh/OFSAAI73/` is a placeholder

Configuring Request XSD Location Definition

This is an application internal parameter and specifies the location in which the xsds for the KYC application are placed. The parameter value must be Y, which is the default and mandatory value. This value is prepackaged as a part of KYC application.

To modify the Request XSD Location Definition, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select **Request XSD Location Definition** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 29. Configuring Request XSD Location Definition Attributes

Attribute	Description
LOCATION	This field specifies the location in which the xsds are placed. This field accepts only string values. The path should be valid and accessible. **Note:** `/home/gsh/ftpshare/KYC/RAOR.xsd` is a place holder.

Configuring Watch List Scanning for Batch Processing

This parameter enables to call the Watch list service during the KYC Batch processing for a Single or Multi tier environment. The parameter value can have Y or N value.

Note: As of now KYC uses Watch list service of Oracle Financial Services Behavior Detection Framework. *Y* is the default value.

To modify the Watch List Scanning for Batch Processing Definition, follow these steps:

1. Open the Manage KYC Installation Parameters screen (Figure 1).
2. Select **KYC** from the Parameter Category drop-down list.
3. Select Watch List Scanning for Batch Processing from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
6. Click **OK**. The KYC Installation Parameters page is displayed.

Table 30. Watch List Scanning for Batch Processing

Attribute	Description
IS_SFTP_ENABLED	This attribute implies whether sftp or ftp is enabled in installed Unix Machines of KYC and Oracle Behavior Detection Framework. The attribute can have 1 or 0 as a value, 1 implies sftp enabled and 0 implies ftp enabled. **Note:** In case both are enabled priority should be given to sftp.
Mantas_Inst_Arch	This attribute implies whether KYC and Oracle Behavior Detection Framework systems are installed on the same machine or on different machines. The attribute can have 0 or 1 as a value where 0 implies both are installed on the same machine and 1 implies both are installed on different machine.
Mnts_Unix_Acct_Uid	This attribute hold the encrypted information about the Unix account User ID on which Watch List Component has been installed.
Mnts_Unix_Acct_Psswd	This attribute hold the encrypted information about the Unix account password on which Watch List Component has been installed.
Mantas_Host_IP	This attribute hold the IP Address/Hostname information of the system on which Watch List Component has been installed.
kycUnixUId	This attribute hold the encrypted information about the Unix account User ID on which KYC has been installed.

Table 30. Watch List Scanning for Batch Processing

kycUnixPsswd	This attribute hold the encrypted information about the Unix account password on which KYC has been installed.
KYC_Host_IP	This attribute hold the IP Address/Hostname information of the system on where KYC has been installed.

Configuring Assessment Related Application Parameters

This section provides instructions for configuring parameters specific to jurisdiction for Risk Assessment. This chapter includes the following sections:

- Configuring Risk Assessment Periodicity
- Configuring Watch List Process
- Configuring Risk Tolerance
- Configuring Risk Assessment Creation - Joint Account Holders
- Configuring Risk Assessment Creation - Guardian
- Configuring Deployment Initiation
- Configuring Document Verification
- Configuring IDV Default Score
- Configuring Identity Verification - Batch Mode
- Configuring Identity Verification
- Configuring Negative News Search
- Configuring Feedback - Watch List
- Configuring Regulatory Report Actions
- Configuring Registration Period
- Configuring Periodic Review
- Configuring Processing Date
- Configuring Purge Archive
- Configuring Risk Assessment Actions
- Configuring Rule Based
- Configuring Account Range for Regular Processing
- Configuring User Definition for System Actions

Configuring Risk Assessment Periodicity

This parameter specifies the time interval for Risk Assessment creation and helps the financial institution to create the optimal number of risk assessments to review the risk. In case if periodicity is one, two or more risk assessments will not be created for a customer on a processing day. The parameter value can have only a natural number value.

Note: 1 is the default value.

To modify the Risk Assessment Periodicity, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Case Periodicity** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Watch List Process

A Financial Institution can enable and disable third party WLS process.

Note: Y is the default and mandatory value which is prepackaged as part of KYC application.

To modify the Watch List Process, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Watch List Process** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Risk Tolerance

This parameter is an exception to the auto-closure functionality, if enabled. This parameter specifies the effective risk change tolerance in percentage for the financial institution. If the difference between the calculated customer effective risk score and the prior score is above the tolerance limit, the risk assessment will not be auto closed even if it satisfies the auto closure definition. This field accepts only values between and 100.

Note: 15 is the default value.

To modify the Risk Tolerance, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Risk Tolerance** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Risk Assessment Creation - Joint Account Holders

This parameter enables the creation of risk assessment for all the joint account holders of the new account, on account opening default review, deployment initiation, and re- review workflow. The parameter value can have only Y or N value.

Y enables risk assessment creation for the joint account holders, and *N* disables the risk assessment creation for the joint account holders.

Note: *Y* is the default value.

To modify the Risk Assessment Creation - Joint Account Holders, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Case Creation - Joint Account Holders** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Risk Assessment Creation - Guardian

This parameter enables the creation of risk assessment for the guardian if the primary holder of the new account opened is a Minor. The parameter value can have only Y or N value.

Y enables creation of risk assessment and *N* disables creation of a risk assessment for the guardian.

Note: *Y* is the default value.

To modify the Risk Assessment Creation - Guardian, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Case Creation - Guardian** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Deployment Initiation

Deployment Initiation is required to perform KYC review of the financial institutions' existing customer base once before going live with the KYC application (which will enable KYC review periodically).

This parameter enables and specifies the attributes which can be used as a filter for performing the bulk reviews in groups (either range of relationship or customer type).

Note: *Y* is the default value, the parameters needs to be fine-tuned, if deployment Initiation is planned to be scheduled for the financial organization.

To modify the Deployment Initiation, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Deployment Initiation** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Table 31. Configuring Deployment Initiation Attributes

Attribute	Description
REL_START_RANGE	This attribute specifies the starting range of Customer relationship period (in days) with the bank which can be used as a filter for deployment initiation workflow. This field is compared with the customer add date and processing date and the calculation is done backwards. This field accepts only natural numbers. **Note:** 0 is the default value.
REL_END_RANGE	This attribute specifies the end range of Customer relationship period (in days) to be considered as a filter for deployment initiation workflow. This field is compared with the customer add date and the processing date and the calculation is done backwards. Both start and end range values are to be provided if this is the mode of doing bulk review. This field accepts only natural numbers. **Note:** 1000 is the default value.
IND_CUST	This attribute specifies whether individual customer type should be used as a filter for executing the batch for deployment workflow. **Note:**This filed can accept only the valid individual code available/defined in the `Dim_Customer_type`.
LEG_CUST	This attribute specifies whether legal entity customer type should be used as a filter for executing the batch for deployment workflow. **Note**: This filed can accept only the valid legal entity code available/defined in the in the `Dim_Customer_type`.
CB_CUST	This attribute specifies whether correspondent bank customer type should be used as a filter for executing the batch for deployment workflow. **Note**: This filed can accept only the valid correspondent bank code available/defined in the `Dim_Customer_type`.

If the volume of data of customers is very large for a bank or financial institution, the execution of risk assessments can be performed based on the value defined in the Deployment Initiation parameter in the jurisdiction-specific Application Parameters table. This allows the bank or financial institution to run discrete batches of risk assessments rather than attempting to process all customers at once.

For example, if a bank has 1 million customers, the bank can decide to perform the risk assessments based on the relationship period of a customer or based on the customer type. The Deployment Initiation parameter has attributes, such as start and end range. If the value provided is 0 and 60 in start and end range, then the system will assess all customers whose relationship with the bank is between 0 to 60 months. This is compared with the customer add date. The value of start and end range has to be modified till the time the complete set of customers are risk assessed. The bank can also assess the customers based on the customer type for a batch. The bank has to update different customer types for each batch execution.

Note: Sysdate will be the starting date for slicing.

Configuring Document Verification

Automatic document verification functionality is enabled using this parameter as part of default review. This parameter describes about the number of different levels of documents to be provided by the customer for document verification to pass during default review.

Y enables the document verification as a part of default review, and *N* disables document verification.

Note: Y is the default value.

To modify the Document Verification, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Document Verification** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Table 32. Configuring Document Verification Attributes

Attribute	Description
lvl1	This attribute specifies the minimum number of Level 1 documents to be verified so that the document verification is successful. This field can accept only natural numbers. **Note:** 5 is the default value.
lvl2	This attribute specifies the number of Level 2 documents to be verified so that the document verification is successful. This field can accept only natural numbers. **Note:** 2 is the default value.
lvl3	This attribute specifies the number of Level 3 documents to be verified so that the document verification is successful. This field can accept only natural numbers. **Note:** 3is the default value.

Configuring IDV Default Score

Financial Institutions can enable and disable third party identify verification process. In the event of not having third party identity verification (IDV) result, the default identify verification score is used for risk calculation. This parameter enables the organization to set the default IDV score.

Note: *Y* is the default and mandatory value which is prepackaged as part of KYC application.

To modify the IDV Default Score, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **IDV Default Score** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Table 33. Configuring IDV Default Score Attributes

Attribute	Description
IDV_DFLT_SCORE	This attribute specifies the Default Score for Identity Verification to be used for the calculation of CIP during Risk rating. This field can accept only natural numbers between 0 and 100. **Note:** 20 is the default IDV score.

Configuring Identity Verification - Batch Mode

This parameter enables and disables third party Identity verification through a batch mode as a part of KYC review. This parameter can have only Y or N value.

Y enables this parameter and *N* disables the parameter.

Note: Y is the default value.

To modify the Identity Verification - Batch Mode, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Internal** in Classification.
4. Select **Identity Verification - Batch Mode** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Table 34. Configuring Identity Verification - Batch Mode Attributes

Attribute	Description
FTPIP	This attribute specifies the IP Address. This field can accept only a valid IP address of the third party service providing the IDV. **Note:** 127.0.0.1 is the placeholder for IP address.
USR_ID	This attribute specifies the User ID of EFunds. This can accept only a valid user ID in string format.
PASSWD	This attribute specifies the E-funds Password. This can accept only a valid user ID in string format.
Port	This attribute specifies the FTP Port. This field can accept only valid port number of the third party service providing the IDV.
Indv Directory	This attribute specifies the Individual Directory where the xml files of individual type customer has to be placed. This directory is placed in the ftp share of the third party service server. This field can accept only a valid string. **Note:** Individual is the default and mandatory value.
Buss Directory	This attribute specifies the Business Directory where the xml files of Correspondent Bank and Legal Entity customer type has to be placed. This directory is placed in the ftp share of the third party service server. This field can accept only a valid string. **Note**: Business is the default and mandatory value.

Table 34. Configuring Identity Verification - Batch Mode Attributes

Waiting Time	This attribute specifies waiting time in minutes to receive the response/poll for the response from the server of third party service provider. Based on the waiting time provided in this field the results are checked by the internal process. For example, If the waiting is 5 minutes the process checks the results for every 5 minutes. Once the result is received from the third party service the process does not check the results. This field can accept only a natural number. **Note:** 5 is the default value.
PHYSICAL_DOC _PATH	This attribute specifies the Directory for placing the temporary files. The path provided has to be valid and accessible. This field can accept only a valid string. **Note:** `D:\\ftpshare\\STAGE\\TPServices\\IDV\\` is the defined path for location of the documents.

Configuring Identity Verification

This parameter enables and disables third party Identity verification as a part of KYC review. The parameter can have only Y or N value.

Y enables this parameter and *N* disables the parameter.

Note: Y is the default value

To modify the Identity Verification, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Identity Verification** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Table 35. Configuring Identity Verification - Batch Mode Attributes

Attribute	Description
INDURL	This attribute specifies the Individual Identity Verification URL. This can accept only a valid URL.. **Note:** `https://penleyincqa.penleyinc.com/penleysoap3/services/chexsystems` is a placeholder for URL..
USR_ID	This attribute specifies the User ID of EFunds. This can accept only a valid user ID in string format.
PASSWD	This attribute specifies the E-funds Password. This can accept only a valid user ID in string format.
ACQR_ID	This attribute specifies the Acquirer ID. This can accept only a string value.

Table 35. Configuring Identity Verification - Batch Mode Attributes

EFUNDS_CUST_ID	This attribute specifies the EFunds Customer ID. This has to be a valid string entry.
CHEXSYS_VERSION	The Check System Version attribute is not used in KYC application at present.
QUALIFILE_VERSION	The Qualifile Version attribute is not used in KYC application at present.
LOC_ID	This attribute specifies the Unique identifier of the person requesting for the service that is, the Employee ID / Employee User ID etc. This helps the third party service to identify the requestor. **Note**: System is the default and mandatory value.
CHEXSYSTEMS_REPORT	The Check System Report attribute is not used in KYC application at present.
QUALIFILE_REPORT	The Qaliifle Report attribute is not used in KYC application at present.
ID_VERF_REPORT	This attribute specifies whether ID Verification Report is required. This field can accept only one of the values, either true or false.
OFAC_REPORT	This attribute specifies whether the OFAC Report is required. This field can accept one of the values, either true or false.
STAGING _CALL	This attribute specifies whether the staging call is required. This field can accept only one of the values, either true or false.
BUSURL	This attribute specifies the EFunds Business URL. This field can accept only a valid URL. **Note:** `https://penleyincqa.penleyinc.com/penleysoap3/services/business` is the placeholder for URL.
IDV_SYS	This attribute specifies the Name of the IDV Verification System. This field can accept only a string format. **Note:** EFD is the default and mandatory value.

Configuring Negative News Search

This parameter enables and disables third party negative news search as a part of KYC review. The parameter can have only Y or N value.

Y enables this parameter and *N* disables the parameter.

Note: Y is the default value

To modify the Negative News Search, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Negative News Search** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Table 36. Configuring Negative News Search Attributes

Attribute	Description
URL	This attribute specifies the Factiva NNS URL. This field can accept only a valid URL provided by the third party.
USR_ID	This attribute specifies the Factiva Login User ID. This can accept only a valid user ID in string format.
PASSWD	This attribute specifies the Factiva Login Password. This can accept password in encrypted format.
NAMESPACES	This attribute specifies the Factiva Namespace. This field can accept either a valid string or a natural number.
LOGO URL	This attribute specifies the URL from where the service provider's logo will be displayed. **Note:** `http://logos.factiva.com/fac1Logo.gif` is the placeholder.
NEGATIVE STRING	This attribute specifies the negative string. This field can accept only a valid string.
SEARCH LANGUAGE	This attribute specifies the search language code. This has to be a valid language code as understood by third party. **Note:** en is the default code for english.
SEARCH ORDER	This attribute specifies the order in which the search has to be performed. This attribute accepts only the following values: ● PublicationDateChronological ● PublicationDateReverseChronological ● Relevance **Note**: The default value is Relevance.
SEARCH CATEGORY	This attribute specifies the search category in which the third party performs its search. This attribute accepts only the following values: ● Websites ● Publications ● Pictures. Pictures are not been used as a search category for KYC application. **Note**: Websites and Publications are the default and mandatory value.
NUMBER OF SEARCH	This attribute specifies the maximum number of search results that the service should provide. This field can accept only a natural number. **Note:** 10 is the default value.
DATE FORMAT	This attribute specifies the date format required for NNS. This field can accept only a valid date format. This field accepts date format as understood by Factiva NNS. **Note**: MMDDCCYY is the default and mandatory value.
CONTINUE SEARCH	This attribute specifies whether continue search feature is required for the KYC application. The third party service provides two levels of searching. As of now KYC system supports only first level of searching. Continue Search is not supported. Note: *N* is the default and mandatory value .

Table 36. Configuring Negative News Search Attributes

WAIT TIME	This attribute specifies whether NNS requests initiated from the KYC application in batch mode has to wait in between each request before hitting the server for results. The wait time is in seconds. This attribute can accept only natural numbers. **Note:** 5 is the default value.
NNS_SYS	This attribute specifies the name of the Negative News Search System. This field can accept only a valid string format. **Note**: Factiva is the default and mandatory value which is prepackaged.
RETRIEVAL URL	This attribute specifies the Factiva NNS Retrieval URL. This field can accept only a valid URL.. **Note:** `http://developer.int.factiva.com/3.6/Retrieval/retrieval.asmx` is the default and mandatory value. This can be changed only if there is a change in the URL of Factiva NNS.

Configuring Feedback - Watch List

This parameter specifies the details for creating the feedback file for watch list. This parameter can accept only Y and N value.

Note: Y is the default value.

To modify the Feedback - Watch List, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application – Internal** in Classification.
4. Select **Feedback - Watch List** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Regulatory Report Actions

This parameter lists the actions on which a Risk Assessment on a Customer has to be created. When a user performs any actions on an alert which would result in creating a regulatory report for a customer, Risk Assessments would be created based on the look up period which is configurable.

Note: The actions to be added here should be picked up from `kdd_activity_type_cd.actvy_type_cd` where `actvy_cat_cd = 'RR'` . Those actions which are suffixed with R in the action code should not be added as these are Recommendations which requires approval.

To modify the Regulatory Report Actions, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application – Business** in Classification.
4. Select **Regulatory Report Actions** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Table 37. Configuring Regulatory Report Actions

Attribute	Description
REG_REP_ACT	This attribute specifies the action codes which is to be considered. **Note:** The actions to be added here needs to be picked up from `kdd_activity_type_cd.actvy_type_cd` where `actvy_cat_cd = 'RR'` . The actions updated should be based on the regulatory report type being installed. Those actions which are suffixed with R in the action code should not be added as these are recommendations which requires approval.

Configuring Registration Period

This parameter enables the financial institution to define the minimum period required for using the snapshot information for risk calculations. If the customer information's last modified date is beyond this definition, risk assessments are put on hold till the revised information is received/the existing information is confirmed as the latest by the relationship manager. This parameter is not considered for Account On Boarding Workflow as the system assumes that the information provided for the customers both new and existing is latest.

Note: *Y* is the default and mandatory value.

To modify the Registration Period, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Registration Period** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Table 38. Configuring Registration Period Attributes

Attribute	Description
PRD_IN_MNTHS	This attribute specifies the Period in months for triggering the registration check for the risk assessments. This can accept only a natural number value. **Note:** 6 is the default value.

Configuring Periodic Review

This parameter enables the creation of risk assessments for periodic review for the Customer for the financial institution.

Note: *Y* is the default and mandatory value which is prepackaged as a part of the KYC application.

730 is the default value for the number of days after which the customers will be considered for periodic re-review.

6000 is the default value for the number of customers picked up for periodic re-review in a day.

To modify the Periodic Review, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Periodic Review** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Processing Date

This parameter specifies the processing date for the KYC application. The information processing date is automatically incremented as part of the KYC workflow on a daily basis. This information needs to be defined once at the start of implementation. The parameter value can have only a date value in the format dd/mm/YYYY.

To modify the Processing Date, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application – Internal** in Classification.
4. Select **Processing Date** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Purge Archive

This parameter provides the flexibility to provide the Customer Effective Risk score ranges for purge activity for both auto closed and UI closed Risk Assessments.

The parameter can have Y or N as a value.

Note: Y is the default value.

To modify the Purge Archive, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Purging Risk Assessment** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Table 39. Configuring Purge Archive Attributes

Attribute	Description
ACLBP	This attribute specifies the Look Back Period in days for the purging of the Risk Assessments which are auto closed based on the closed date. **Note:** 1 is the default value.
CLLBP	This attribute specifies the Look Back Period in days for the purging of the Risk Assessments which are promoted to cases based on the case closure date. **Note:** 30 is the default value.
CERLB	This attribute specifies the Lower range of the CER score of the Risk Assessments which needs to be purged and archived. **Note:** The score provided here has to match with scores defined in Risk Category table for auto closure and Risk Assessment Promotion to Risk Assessments. 0 is the default and mandatory value.
CERUB	This attribute specifies the Upper range of the CER score of the Risk Assessments which needs to be purged and Archived. **Note:** The score provided here has to match with scores defined in Risk Category table for auto closure and Risk Assessment Promotion to Risk Assessments. 100 is the default and mandatory value.

Note: The purging of the risk assessments which are promoted to cases and are closed by the user must be purged only when the associated cases are purged, else there would be issues when the business user tries to look at the risk information or tries to reopen and initiate third party services.

Configuring Risk Assessment Actions

This parameter enables the creation of log for every single action on a Risk Assessment. Risk Assessment Actions are available for view in the UI. The parameter value can have only Y or N value.

Y enables the creation of Risk Assessment action logs and *N* disables the risk assessment action log creation.

Note: *Y* is the default value

To modify the Risk Assessment Actions, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application – Internal** in Classification.
4. Select **Case Action Log** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Rule Based

This parameter provides the flexibility of enabling and disabling the Rule Based Risk Rating Model for risk processing. The parameter can have Y or N as a value.

Note: *Y* is the default value which is prepackaged as a part of KYC.

To modify the Rule Based, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application – Business** in Classification.
4. Select **Rule Based** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Account Range for Regular Processing

This parameter provides the financial institutions' the flexibility of providing the date range based on their operational updates of the new customers opening accounts to the Core Banking System.

Note: The default value is *Y*.

To modify the Account Range for Regular Processing , follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application - Business** in Classification.
4. Select **Account Range for Regular Processing** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Table 40. Configuring Account Range for Regular Processing Attributes

Attribute	Description
ACCT_DT_START_RANGE	This attribute defines the start range to be considered for picking up the accounts newly opened. **Note:** 0 is the default value.
ACCT_DT_END_RANGE	This attribute defines the end range to be considered for picking up the accounts newly opened by the customer. This date is compared with the risk processing date. **Note:** 7 is the default value.

Configuring User Definition for System Actions

This parameter specifies the name tag that can be used for defining all system actions. The parameter value can have only a string value.

Note: System is the default and mandatory value which is prepackaged as a part of the KYC application.

To modify the System Reference, follow these steps:

1. Open the Manage KYC Application Parameters screen (Figure 1).
2. Select the required Jurisdiction.
3. Select **Application – Internal** in Classification.
4. Select **System Reference** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
6. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*
7. Click **OK**. The Manage KYC Application Parameters page is displayed.

Configuring Assessment Related Risk Value Scores

This section provides details about how to provide scores for different values of risk parameters required for risk assessments. The list with the initial risk values with the scores for default jurisdiction for is available as a part of installation. Any subsequent additions or modifications of the risk values are performed through excel upload.

The modifications to the scores to be performed using the UI which can be accessed through Administration => KYC Configuration. For any additions of the values to be performed through excel upload.

The risk values and its scores has to be made available for all the jurisdiction available for an installation. This can be performed using Copy option which would help the admin to copy all the risk values of a default jurisdiction to different jurisdictions.

Refer to the *KYC Risk Assessment Guide* to know the significance of each of these risk parameters used in different risk models.

This section includes following topics:

- Configuring Company Risk Value
- Configuring Country Risk Value
- Configuring Industry Risk Value
- Configuring Income Source Type Risk Value
- Configuring Legal Structure and Ownership Risk Value
- Configuring Markets Served Risk Value
- Configuring Products Offered Risk Value
- Configuring Relationship Period Risk Value

- Configuring Corporation Age Range Risk Value
- Configuring Negative News Range Risk Value
- Configuring Occupation Range Risk Value

Configuring Company Risk Value

The risk associated with the Ownership of the Company (Public or Private) is captured in this UI.
To modify the Company Risk Value, follow these steps:

1. Open Company Risk from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required company and click **Go**.
3. Edit/Copy the parameter.

Configuring Country Risk Value

The risk values associated with each country are listed. These values are used for Risk Rating a customer by considering the risk for country; for example, if the primary citizenship of the country should be considered for risk assessing, then the corresponding risk value for that country is picked up from here. These values are configurable according to the user requirements.
To modify the Country Risk Value, follow these steps:

1. Open Country Risk from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required country and click **Go**.
3. Edit/Copy the parameter.

Configuring Industry Risk Value

The risk associated with the Industry in which the Legal Entity operates is captured in this UI.
To modify the Industry Risk Value, follow these steps:

1. Open Industry Risk from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required Industry and click **Go**.
3. Edit/Copy the parameter.

Configuring Income Source Type Risk Value

The risk associated with the Source of Wealth for an Individual is captured in this UI
To modify the Income Source Type Risk Value, follow these steps:

1. Open Income Source Type Risk from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required Income Source and click **Go**.
3. Edit/Copy the parameter.

Configuring Legal Structure and Ownership Risk Value

The risk associated with the Legal Structure of the Entity is captured in this UI.
To modify the Legal Structure and Ownership Risk Value, follow these steps:

1. Open Legal Structure and Ownership Risk from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required Legal Structure and Ownership and click Go.
3. Edit/Copy the parameter.

Configuring Markets Served Risk Value

The risk associated with the Markets Served by the Bank is captured in this UI.
To modify the Markets Served Risk Value, follow these steps:

1. Open Markets Served Risk from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required Markets Served and click **Go**.
3. Edit/Copy the parameter.

Configuring Products Offered Risk Value

The risk associated with the Products Offered by the Bank is captured in this UI.
To modify the Products Offered Risk Value, follow these steps:

1. Open Products Offered Risk from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required Products Offered and click **Go**.
3. Edit/Copy the parameter.

Configuring Relationship Period Risk Value

The risk associated with the relationship period with the bank for each customer is captured in this UI.
To modify the Relationship Period Risk Value, follow these steps:

1. Open Relationship Period Risk from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required Relationship Period and click **Go**.
3. Select the individual, Legal Entity or Correspondent Bank tab.
4. Edit/Copy the parameter.

Configuring Corporation Age Range Risk Value

The risk values associated with the corporation age are captured in this UI.
To modify the Corporation Age Range Risk Value, follow these steps:

1. Open Corporation Age Range Risk from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required Corporation Age Range and click **Go**.
3. Select the individual, Legal Entity or Correspondent Bank tab.
4. Edit/Copy the parameter.

Configuring Negative News Range Risk Value

The risk associated with the count of Negative News of the customer is captured in this UI.
To modify the Negative News Range Risk Value, follow these steps:

1. Open Negative News Range Risk from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required Negative News Range and click **Go**.
3. Select the individual, Legal Entity or Correspondent Bank tab.
4. Edit/Copy the parameter.

Configuring Occupation Range Risk Value

The risk associated with the count of Negative News of the customer is captured in this UI.
To modify the Occupation Range Risk Value, follow these steps:

1. Open Occupation Range from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the required Occupation Range and click **Go**.
3. Select the individual, Legal Entity or Correspondent Bank tab.
4. Edit/Copy the parameter.

CHAPTER 6 KYC Risk Assessment Configuration

This chapter focuses on the details on configuring the weights of the risk assessment parameters per customer type for different risk models available in KYC. It also explains how to configure the accelerate review rules criteria.

This chapter includes following sections:

- Configuring Risk Model Weights
- Configuring Accelerated Re-review Rules
- Configuring Account Customer Role
- Configuring Risk Assessment Priority
- Configuring Risk Assessment Category
- Configuring RAOR Assessment Category

Configuring Risk Model Weights

KYC has three risk models which are used for assessing a risk a customer poses to a bank or FI. The weights of the parameter can be fine tuned for each jurisdiction based on the requirements of the FI or banks. If your firm decides not to use any one of more parameter for a jurisdiction the weights of that parameter can be defined as 0. The higher the weight the higher would be the score of that parameter for a customer. For more information, refer to *KYC Risk Assessment Guide.*

Real Time Account On-Boarding Risk Assessing Model

Real Time Account On-Boarding Risk Assessing Model is the risk assessment process at the time of the account opening. The parameters related to this process are categorized and placed in different tabs for easy categorization. Each parameter is given a configurable weight. The parameters weights are specific to the installation. Initially this is done at the time of Application installation.

To modify the Real Time Account On-Boarding Risk Assessing Model, follow these steps

1. Open Real Time Account On-Boarding Risk Assessment from Administration > KYC Configuration.
2. Select the required Jurisdiction and select click **Go**.
3. Select the individual, Legal Entity or Correspondent Bank tab based on the need.
4. Edit/Copy the weights of the parameter.

Rule Based Risk Assessment

The rule based risk assessment focuses on calculating a CER score based on client configurable rules. The rule based assessment would be executed only if it is opted by the Bank or FI for an installation. This option can be decided using the Parameter Rule Based from the jurisdiction-specific Application Parameter table.

In this UI you can perform the following:

- Add multiple values for a rule
- Edit the values entered
- Enable or disable a rule

To modify the Rule Based Risk Assessment Model, follow these steps:

1. Open Rule Based Risk Assessment from Administration > KYC Configuration.
2. Select the required Jurisdiction and select the Rule Name and click **Go**.
3. Select the individual, Legal Entity or Correspondent Bank tab as required.
4. Add/Edit/Copy the parameter.

Algorithm Based Risk Assessment

The customers who are not assessed on the Rule based shall be executed on Algorithm based risk assessment. The Algorithm based Risk Assessment shall focus on calculating the risk of the customers based on different parameters defined based on customer type. The bank can define the different weights of a risk parameter for each customer. The weight must be in the range of 0 to 100 and sum up to 100 for each customer type. If a parameter is not required for a FI or bank the weight of the same can be provided as 0.

To modify the Algorithm Based Risk Assessment Model, follow these steps:

1. Open Algorithm Based Risk Assessment from Administration > KYC Configuration.
2. Select the required Jurisdiction and click **Go**.
3. Select the individual, Legal Entity or Correspondent Bank tab as required.
4. Edit/Copy the weights of the parameter.

Configuring Accelerated Re-review Rules

Accelerated Review Rules Parameters are used in Accelerated Review processing. Accelerated Review Rules require a thresholds definition for triggering the re-review case generation. This option allows you to view the details and attributes of the Re-Review rules and redefine the threshold definition for the re-review rules. The configurable values differs based on the rule selected. During Excel Upload the admin can decide on which all rules to enable and disable for each jurisdiction and then perform excel upload.

To modify the Accelerated Re-review Rules, follow these steps:

1. Open Accelerated Rules from Administration > KYC Configuration.
2. Select the required Jurisdiction and click **Go**.
3. Select the Rule Name and modify the values applicable for that rule.
4. Edit/Copy the values of the parameter.

You can disable any of the rule for any of the jurisdiction based on the business needs.

Execute the following query to enable and disable the rules. This query must be executed in the KYC Atomic schema.

For Enabling

```
update vw_appln_rereview_params t set t.f_enable='Y' where t.n_rule_id='1' and
t.n_src_cntry_key='1';
```

Note: In the above query you can change the rule ID and the Jurisdiction key according to the business needs.

For Disabling

```
update vw_appln_rereview_params t set t.f_enable='N' where t.n_rule_id='1' and
t.n_src_cntry_key='1';
```

Note: In the above query you can change the rule ID and the Jurisdiction key according to the business needs.

Configuring Account Customer Role

This UI helps the FI or bank to enable or disable the controlling flag of an account role a customer plays on an account. If a role is not considered for risk assessment, the controlling flag can be defined as N.

To modify the Account Customer Role, follow these steps:

1. Open Account Customer Role from Administration > KYC Configuration.
2. Select the required Role Name and edit the flag of Risk Assessment Role.

Configuring Risk Assessment Priority

This UI allows the bank or FI to define the priority of cases which are promoted through risk assessments. The range of the risk score must be defined for each of the priority. For exceptions of promote to case the bank can define the priority to be either low/medium or high unlike others. The scores defined have to be in the range of 0 to 100 and the scores defined must be the same as of Risk Category table in KYC schema. The range of scores must be in sync with the scores defined in Risk Assessment Category UI.

To modify the Risk Assessment Priority, follow these steps:

1. Open Risk Assessment Priority from Administration > KYC Configuration.
2. Select the required Jurisdiction and click **Go**.
3. Edit /Copy the ranges of the priority to be defined.

Configuring Risk Assessment Category

This UI allows the bank or FI to define the ranges of the risk score to fall under different categories like Low/Elevated and High with an option to define the ranges of the score of a risk assessments to be promoted to case by selecting Y or N in the User Review column. It also allows you to configure the re-review period based on the category. It allows you to copy the values from one jurisdiction to another.

To modify the Risk Assessment Category, follow these steps:

1. Open Risk Assessment Category from Administration > KYC Configuration.
2. Select the required Jurisdiction and click **Go**.
3. Edit /Copy the ranges of the score to be defined.
4. Edit/Copy the user review flag.
5. Edit/Copy the re-review period.

Configuring RAOR Assessment Category

This UI helps the bank or FI to define the ranges of the risk score to fall under different categories like Low/Elevated and High for customers who opens an account. It allows you to copy the values from one jurisdiction to another.

To modify the RAOR Assessment Category, follow these steps:

1. Open RAOR Assessment Category from Administration > KYC Configuration.
2. Select the required Jurisdiction and click **Go**.
3. Edit /Copy the ranges of the score to be defined.

CHAPTER 7 Actions Configuration

This chapter provides procedures for configuring the list of available actions. Configuration of actions requires database privileges. Using actions pop-ups, you can document your analysis and close alerts and cases. You can take action on a selected alert or case, such as, closing it, taking a follow-up action on it, or assigning it to other users. The following sections are detailed in this chapter:

- Working with Alert Action Settings
- Working with Case Action Settings
- Configuring Mandatory Action Attributes

Working with Alert Action Settings

The following tasks describe how to work with alert action configuration settings:

- Understanding Alert Workflows
- Configuring Alert Action Data
- Configuring Standard Comment Data

Understanding Alert Workflows

In general, alert workflows consist of a series of steps and actions. The actions that are available at each step of the workflow determine the next step (or status) in the workflow. With each action, the alert can change status to advance it through the workflow.

Defining the Alert workflow consists primarily of the following steps:

1. Define activity to be used in the workflow. Refer to section *Configuring Alert Action Data*, on page 80, for more information.
2. Define standard comments that is available in the workflow. Refer to section *Configuring Standard Comment Data*, on page 81, for more information.

You can specify individual actions or groups of actions available at each step. Groups of actions are defined for either simple reuse (commonly used groups of actions), to require multiple actions to be taken to advance the alert to the next state, or to prevent incompatible actions from being taken together. In addition, you can specify standard comments or standard comment applicable for the scenario class.

Configuring Alert Action Data

You can configure alert activity as described in the following subsections.

Adding New Alert Data

To add a new alert action item, create a new action code by adding a new record in the KDD_ACTIVITY_TYPE_CD table.

While adding a new action, the set of supplemental values to be associated with the action should be decided based on the following criteria:

- ACTVY_CAT_CD: Category code that identifies the classification of an activity. You can add new actions in the existing category except Disposition Category.
- ACTVY_TYPE_CD: Defines unique identifier for actions.

  Note: You should assign new actions type code that begins with a CST prefix to indicate that they are custom actions.
- DISPL_ORDER_NB: Integer that represents the order of this activity for display purposes.
- NEXT_REVIEW_STATUS_CD: Resulting status code to be set for an alert when this activity is performed on the alert. Next Review Status Codes can be superseded by another status, if another activity is taken on the same alert at the same time where that activity has a more severe resulting status. For example, if two actions are taken where one results in a closing status, the closing status is considered the more severe status.
- REQ_REASN_FL: Indicator of whether this activity type requires reassignment of an investigation record.
- REQ_DUE_DATE_FL: Indicator of whether this activity type requires the user to enter a due date on an alert, unless superseded by another action being taken on the monitoring record that has a Closed resulting status based on the lowest order precedence established in the monitoring Status table, then the user is NOT required to enter a due-date.
- REQ_CMMNT_FL: Indicator of whether a comment, either the standard or free-text comment, is required for this activity type.

Adding New Alert Status

To add a new alert status, follow these steps:

1. Add an entry to the KDD_STATUS table, as follows:

   ```
   insert into KDD_REVIEW_STATUS (STATUS_CD, REVIEW_TYPE_CD, CAN_NHRIT_FL,
   VIEWD_BY_OWNER_ACTVY_TYPE_CD, VIEWD_RESULT_STATUS_CD, STATUS_DISPL_ORDER_NB,
   PRSDNC_ORDER_NB, CLOSED_STATUS_FL) values ('TEST', 'AL', 'N', null, null, 170, null,
   'Y');
   ```

2. Add an entry to the KDD_CODE_SET_TRNLN table, as follows:

   ```
   insert into KDD_CODE_SET_TRNLN (CODE_SET, CODE_VAL, SRC_SYS_CD, CODE_DISP_TX) values
   ('AlertStatus', 'TEST',null, 'Description¿)
   ```

3. Map the appropriate actions to the new custom status. Make entries in the

   ```
   "KDD_ACTVY_TYPE_REVIEW_STATUS" table.

   insert into KDD_ACTVY_TYPE_REVIEW_STATUS (ACTVY_TYPE_CD, STATUS_CD) values

   ('MTS719', 'TEST');
   ```

   Note: : The appropriate actions are available in the KDD_ACTIVITY_TYPE_CD table.

4. Restart the server.

Mapping the New Activity to User Role

To map the new activity to user role, create a new activity role mapping by adding a new record in the KDD_ROLE_ACTIVITY_TYPE table:

```
insert into KDD_ROLE_ACTIVITY_TYPE (ACTVY_TYPE_CD, ROLE_CD) values ('CST010', 'AMANALYST')
```

Each record in the Alert Role to Activity Map table represents the mapping between user roles and the activity that a particular user role is allowed to perform. Each Action can be mapped to multiple roles.

Mapping the New Activity to the Status

To map the new activity to the status, create a new activity status mapping by adding a new record in the KDD_ACTVY_TYPE_REVIEW_STATUS table:

```
insert into KDD_ACTVY_TYPE_REVIEW_STATUS (ACTVY_TYPE_CD ,STATUS_CD) values ('CST010','OP')
```

Each record in the Alert Status to Activity table captures the activities that are available for a alert based on the alert's current status.

Mapping the New Activity to the Scenario Class

To map the new activity to the Scenario Class, create a new activity Scenario Class mapping by adding a new record in the KDD_SCNRO_CLASS_ACTVY_TYPE table:

```
insert into KDD_SCNRO_CLASS_ACTVY_TYPE (SCNRO_CLASS_CD,ACTVY_TYPE_CD) values
('AM','CST010')
```

Records in the Scenario class to Activity table represent activities that are available for an alert, based on alert's scenario class.

Configuring Standard Comment Data

The comments are created in the KDD_CMMNT table, and the categories are in the KDD_CMMNT_CAT_CD table. To add a new standard comment, follow these steps:

1. Add an entry into the KDD_CMMNT table:

   ```
   insert into KDD_CMMNT (CMMNT_ID, EDIT_FL, CMMNT_TX,DISPL_ORDER_NB, CMMNT_CAT_CD) values
   (1000, 'N', 'Awaiting Approval', 20, 'RES')
   ```

2. Save your changes to the KDD_CMMNT table.
3. Associate the new comment with a scenario class by adding an entry in the KDD_SCNRO_CLASS_CMNT table:

   ```
   insert into KDD_SCNRO_CLASS_CMMNT (Scnro_Class_Cd, Cmmnt_Id) values ('ML', 1000)
   ```

To add a new comment category for use in the alert workflow, add an entry to the KDD_CMMNT_CAT_CD table:

```
insert into KDD_CMMNT_CAT_CD (CMMNT_CAT_CD, DISPL_NM,DISPL_ORDER_NB, MANTAS_CMMNT_CAT_FL)
values ('NCC','New comment category', 20, 'N')
```

Working with Case Action Settings

Case Management uses the Action pop-ups differently than Alert Management. Some configuration tasks are identical (creating standard comments and creating standard comment categories), however, the association of actions to how they are used in the workflow is entirely different.

The following sections defines how to configure case workflows:

- Understanding Case Workflows
- Adding New Case Statuses
- Configuring Case Action Data
- Configuring Standard Comment Data

Understanding Case Workflows

In general, Case workflows consist of a series of steps and actions. The actions that are available at each step of the workflow determine the next step (or status) in the workflow. With each action, the case can change its status to advance through the workflow.

Defining a Case workflow consists primarily of the following tasks:

1. Create case types and subtypes. Refer to the *Administration Guide*, for more information.
2. Define case statuses that represent steps in the workflow. Refer to section *Adding New Case Statuses,* on page 82 for more information.
3. Define actions to be used in the workflow. Refer to section *Configuring Case Action Data,* on page 83 for more information.
4. Define standard comments that is available in the workflow. Refer to section *Configuring Standard Comment Data,* on page 85 for more information.

Note: When defining workflows, you specify individual actions or comments available at each step.

Adding New Case Statuses

You can add a new case status by following these steps:

1. Add an entry to the `KDD_STATUS` table, as follows:

   ```
   insert into KDD_STATUS (STATUS_CD,CAN_NHRIT_FL,VIEWD_BY_OWNER_ACTVY_TYPE_CD,
   VIEWD_RESULT_STATUS_CD,CLOSED_STATUS_FL,STATUS_NM) values
   ('CZZZ','N',null,null,'Y','Closed - Loss Recovered')
   ```

2. Add an entry to the `KDD_CODE_SET_TRNLN` table, as follows:

   ```
   insert into KDD_CODE_SET_TRNLN (CODE_SET, CODE_VAL, SRC_SYS_CD, CODE_DISP_TX) values
   ('CaseStatus', 'CZZZ',null, 'Closed - Loss Recovered')
   ```

Configuring Case Action Data

You can configure case actions as described in the following subsections:

Adding a New Action Category

To add a new case action item, follow these steps:

1. Create a new action category by adding a new record in the KDD_ACTION_CAT_CD as follows:

```
insert into KDD_ACTION_CAT_CD (ACTION_CAT_CD,DISPL_NM,DISPL_ORDER_NB,
MANTAS_ACTVY_CAT_FL) values ('REV','Research & Review',40, 'Y')
```

Adding a New Action

To add a new record code, follow these steps:

1. Create a new action code by adding a new record in the KDD_ACTION table as follows:

```
insert into KDD_ACTION (ACTION_ID, ACTION_CATEGORY_CODE, ACTION_NM, ACTION_CD,
ACTION_DESC, LAST_UPDATED_DT, LAST_UPDATED_BY, COMMENTS, ACTION_ORDER, REQ_CMMNT_FL,
DFLT_DUE_DT_LM, REQ_REASN_FL, REQ_DUE_DATE_FL, NEXT_REVIEW_STATUS_CD, REG_TYPE_CD,
REQ_REASN_OWNER_FL, LAST_ASSIGN_REQ, RESOLUTION_ACTION_FL, EXPORT_DIR_REF) values (73,
'REV', 'Reviewed with Account Manager', 'CA73A', 'Reviewed with Account Manager', null,
null, null, 90, 'Y', null, 'N', 'N', 'INV', null, 'N', 'N', null, , null)
```

While adding a new action, the set of supplemental values to be associated with the action should be decided based on the following criteria:

a. ACTION_CATEGORY_CODE - Category code that identifies the classification of an action. If you want to change the category of an action, you need to change this column accordingly.

b. ACTION_ORDER - Integer that represents the order in which action is performed in the scenario of multiple action take together.

c. NEXT_REVIEW_STATUS_CD - Resulting status code to be set when this action type is performed on an investigation record.

d. REQ_REASN_FL - Indicator of whether this action type requires reassignment of an investigation record.

e. REQ_DUE_DATE_FL - Indicator of whether this action type requires the user to enter a due date on a case.

Note: Unless superseded by another action being taken on the investigation record that has a Closed status as the resulting status based on the lowest order precedence established in the Investigation Status table the provided due date will be applied on the investigation record.

f. REQ_CMMNT_FL - Indicator of whether a comment, either the standard or free-text comment, is required for this action type.

g. REQ_REASN_OWNER_FL Indicator of whether this action type requires reassignment of ownership of a case investigation record.

h. LAST_ASSIGN_REQ - Used by the system to determine the last user who performed this action in the situation where the this recommendation or escalation action is rejected and the case would need to be reassigned back to the last user who took the action. "Y" means that when this action appears on a

case previous to a rejection action by another user the user who took this action would become the owner. "N" means this is not a recommend for approval or escalation type action or is not an action that would be used by the system to determine reassignment.

i.RESOLUTION_ACTION_FL - Indicator of whether this action is a resolution action.

Mapping New Action to User Role

Create a new action Role mapping by adding a new record in the KDD_ROLE_ACTION_MAP table as follows: where the CASE_ROLE_ACTION_MAP_SEQ represents the next sequential number for a record in this table:

```
insert into KDD_ROLE_ACTION_MAP (CASE_ROLE_ACTION_MAP_SEQ, ROLE_CD, ACTION_CD) values (22, 'CMANALYST1', 'CA73A')
```

Each record in the Case Role to Action Map table represents the mapping between user roles and the actions that a particular user role is allowed to perform. Each Action can be mapped to multiple roles.

Note: You can find the highest CASE_ROLE_ACTION_MAP_SEQ used in the table and add 1 to that number while inserting a new record to this table. You can find highest CASE_ROLE_ACTION_MAP_SEQ by running the following query:

```
select max(t. CASE_ROLE_ACTION_MAP_SEQ) from KDD_ROLE_ACTION_MAP t
```

Mapping the New Action to Status

Create a new action Role mapping by adding a new record in the KDD_STATUS_ACTION_MAP table as follows: where the CASE_STATUS_ACTION_MAP_SEQ represents the next sequential number for a record in this table:

```
insert into KDD_STATUS_ACTION_MAP (CASE_STATUS_ACTION_MAP_SEQ, STATUS_CD, ACTION_CD) values (26, 'RO', 'CA73A')
```

Each record in the Case Status to Action table captures the actions that will be available for a case based on the case's current status.

Note: You can find the highest CASE_STATUS_ACTION_MAP_SEQ used in the table and add 1 to that number while inserting a new record to this table. We can find highest CASE_STATUS_ACTION_MAP_SEQ by running the below mentioned Query.

```
select max(t. CASE_STATUS_ACTION_MAP_SEQ) from KDD_STATUS_ACTION_MAP t
```

Map the New Action to the Case Type/Sub Type

Create a new Case Type/Subtype Action mapping by adding a new record in the KDD_CASETYPE_ACTION_MAP table as follows, where the CASE_CASETYPE_ACTION_MAP_SEQ represents the next sequential number for a record in this table:

```
insert into KDD_CASETYPE_ACTION_MAP (CASE_CASETYPE_ACTION_MAP_SEQ, ACTION_CD, CASE_TYPE_SUBTYPE_CD) values (80, 'CA73S', 'AML_SURV')
```

Note: You can find the highest CASE_CASETYPE_ACTION_MAP_SEQ used in the table and add (1) to that number while inserting a new record to this table. We can find highest CASE_CASETYPE_ACTION_MAP_SEQ by running the query:

```
select max(t. CASE_CASETYPE_ACTION_MAP_SEQ) from KDD_CASETYPE_ACTION_MAP t
```

Records in the Case Type to Action table represent actions that are available for a case based on the case type/subtype combination of the case.

Configuring Standard Comment Data

Configuring standard comments and standard comment categories is similar to configuring them for the Case Actions pop-up. The comments are created in the KDD_CMMNT table, and the categories are in the KDD_CMMNT_CAT_CD table. Refer to section *Configuring Standard Comment Data,* on page 81 for more information.

Mapping of Standard Comment and case type is made by entering a record in the KDD_CASE_TYPE_CMMNT table in the alert management schema.

For adding a new record in the KDD_CASE_TYPE_CMMNT table, follow the script:

```
insert into KDD_CASE_TYPE_CMMNT (CASE_TYPE_CD, CMMNT_ID) values ('AML_SURV', 8090)
```

Configuring Mandatory Action Attributes

You can configure whether or not alert or case actions require a comment, a reassignment, or a due-date. These requirements are configured by setting column values in the KDD_ACTIVITY_TYPE_CD or KDD_ACTION table in the Case Management schema.

Making Comments Mandatory

To specify comments that are mandatory for an alert action type, follow these steps:

1. Set the REQ_CMMNT_FL to Y (Yes) in the KDD_ACTIVITY_TYPE_CD table for an alert action type.

   For example, if you want to make comments mandatory for a particular alert action type 'MTSPTCAC', the SQL code should be similar to the following:

   ```
   update KDD_ACTIVITY_TYPE_CD set REQ_CMMNT_FL = 'Y' where ACTVY_TYPE_CD = 'MTSPTCAC'
   ```

2. Save your changes to the KDD_ACTIVITY_TYPE_CD table.

To specify comments that are mandatory for a case action type, follow these steps:

1. Set the REQ_CMMNT_FL to Y (Yes) in the KDD_ACTION table for a case action type.

   For example, if you want to make comments mandatory for a particular case action type, the SQL code should be similar to the following:

   ```
   update KDD_ACTION set REQ_CMMNT_FL = 'Y' where ACTION_ID= 72
   ```

2. Save your changes to the KDD_ACTION table.

Making Reassignment Mandatory

To specify that a reassignment is mandatory for an alert or case action type, follow these steps:

Alert Reassignment

1. Set the REQ_REASN_FL to Y (Yes) in the KDD_ACTIVITY_TYPE_CD table for an alert action type.

   For example, if you want to make reassignment mandatory for a particular alert action type 'MTSPTCAC', the SQL code should look similar to the following:

   ```
   update KDD_ACTIVITY_TYPE_CD set REQ_REASN_FL = 'Y' where ACTVY_TYPE_CD = 'MTSPTCAC'
   ```

2. Save your changes to the KDD_ACTIVITY_TYPE_CD table.

Case Reassignment

1. Set the REQ_REASN_FL to Y (Yes) in the KDD_ACTION table case action type.

   For example, if you want to make reassignment mandatory for a particular case action type, the SQL code should be similar to the following:

   ```
   update KDD_ACTION set REQ_REASN_FL = 'Y' where ACTION_ID= 72
   ```

2. Save your changes to the KDD_ACTION table.

Making a Due-Date for an Action Mandatory

To specify that a due-date is mandatory for an alert or case action type, follow these steps:

Alert Due-Date

1. Set the REQ_DUE_DATE_FL to Y (Yes) in the KDD_ACTIVITY_TYPE_CD table for an alert action type.

   For example, if you want to make a due date mandatory for a particular alert action type (MTSPTCAC), the SQL code should look similar to the following:

   ```
   update KDD_ACTIVITY_TYPE_CD set REQ_DUE_DATE_FL = 'Y' where ACTVY_TYPE_CD = 'MTSPTCAC'
   ```

2. Save your changes to the KDD_ACTIVITY_TYPE_CD table.

Case Due-Date

1. Set the REQ_DUE_DATE_FL to Y (Yes) in the KDD_ACTION table for a case action type.

   For example, if you want to make a due date mandatory for a particular case action type the SQL code should be similar to the following:

   ```
   update KDD_ACTION set REQ_DUE_DATE_FL = 'Y' where ACTION_ID = 72
   ```

2. Save your changes to the KDD_ACTION table.

   For Alert Action:

   ```
   update KDD_ACTIVITY_TYPE_CD set DFLT_DUE_DT_LM = 7 where ACTVY_TYPE_CD = 'MTSPTCAC'
   ```

   For Case Action:

   ```
   update KDD_ACTION set DFLT_DUE_DT_LM = 7 where ACTION_ID = 72
   ```

   Note: For specifying a default due date for any action, the DFLT_DUE_DT_LM column of KDD_ACTIVITY_TYPE_CD and KDD_ACTION can be updated with corresponding values respectively for alert and case actions. The value defined represents the number of days which will get added to the current date and set as the due date when the corresponding action is taken.

CHAPTER 8 Web Application Configuration

As an Oracle Financial Services Administrator you can customize features in the Web Application UI. This chapter contains information about configuring session time out.

Configuring the Session Timeout Setting

This section describes the following topics:

- Configuring the Session Timeout Setting for Alert Management and Case Management
- Configuring the Session Timeout Setting for Admin Tools

Configuring the Session Timeout Setting for Alert Management and Case Management

As an Oracle Financial Services Administrator, you can set the inactive web application users to automatically log off by setting the number of minutes that a user can remain inactive. This results in automatic user log-off that terminates the user's session.

Refer to the *Oracle Financial Services Analytical Applications Infrastructure User Manual Release 7.3* for more information on how to set the duration before logout for inactive sessions.

Configuring the Session Timeout Setting for Admin Tools

As Oracle Financial Services Administrator, you can optionally log off inactive Web Application users by establishing a set number of minutes that a user can remain inactive. This results in automatic user log-off that terminates the user's session.

To modify the idle session timeout for idle or inactive users, follow these steps:

1. Open the web.xml file associated with the WebLogic or WebSphere application.

   You can find this file in the WEB-INF directory under each Web application in the Oracle Financial Services installation.

2. Modify the XML code within the file that contains `<session-config>` in its `<session-descriptor>` entry.

   Do this by setting the `<session-timeout>` part of the entry so that the number of minutes equals the current quantity of minutes of inactivity that result in a logoff.

3. Save the changes.

   After setting the parameter to 30 minutes, the edited XML code should look similar to the following:

   ```
   <session-config>
   <session-timeout>30</session-timeout>
   </session-config>
   ```

CHAPTER 9 OBIEE Report Configuration

If your site has the Oracle Business Intelligence Enterprise Edition (OBIEE 11g) application installed, as an OFSBDF Administrator, you can customize several OBIEE features that affect the presentation of information in the Web Application's UI.

This chapter focuses on the following topics:

- Changing the Color Code of the Scatter Reports
- Changing the Color Code of the Statistical Reports
- Configuring the Quality Rating of Matches in the Threshold Analyzer Scatter Graph

Changing the Color Code of the Scatter Reports

You can change the color code of the Scatter reports in the Threshold Analyzer utility under the following conditions:

- If you have a description other than Productive, Non Productive, and Indeterminate for Quality Rating Code.

  Note: Quality Rating Code is like a Closing Classification Code. For example, CL01, CL02, and CL03.
- If you have more than three Quality Rating Codes. Make a backup of all the Threshold Analyzer reports.

To change the color code of the scatter reports, follow these steps:

1. After logging into the OBIEEAnalytics URL, click the **Catalog** link (Figure 6).

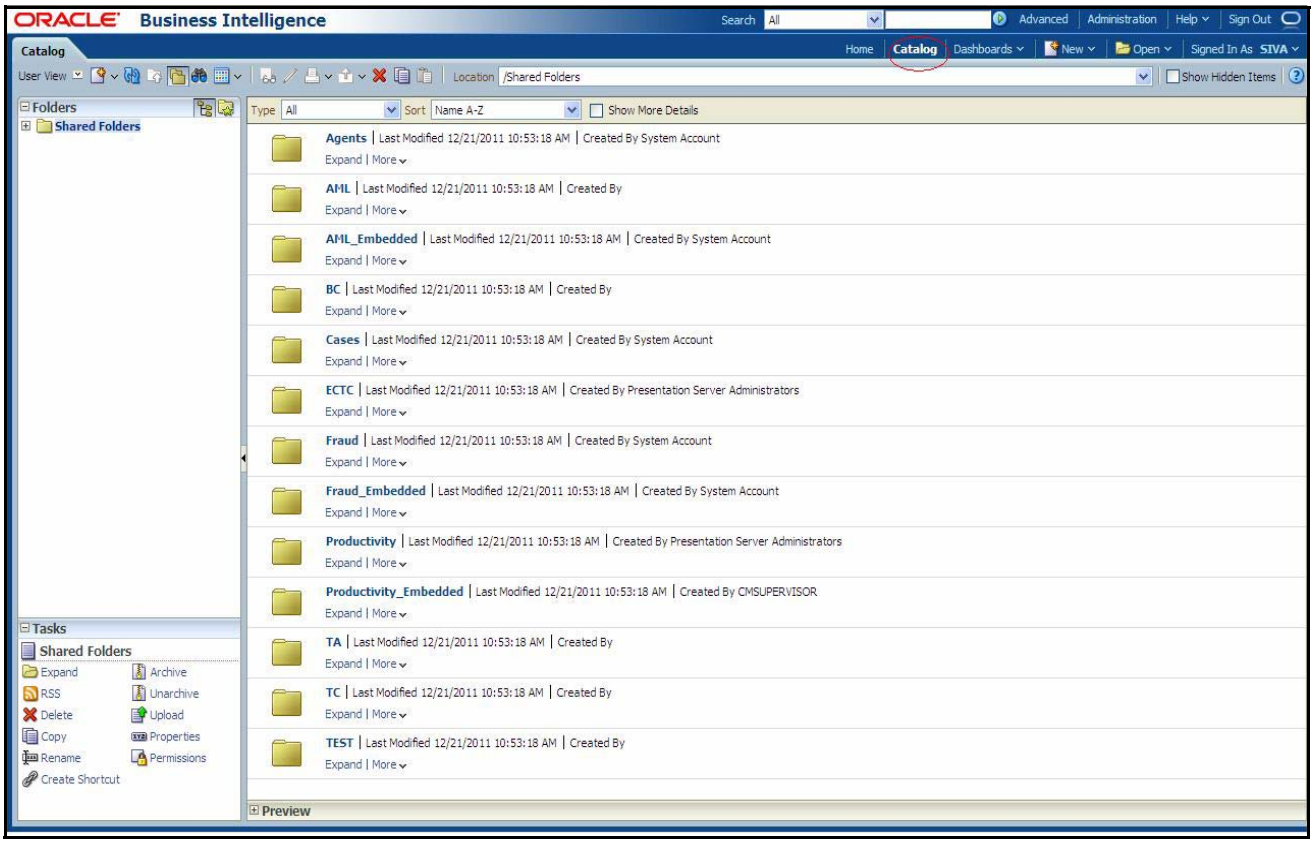

Figure 6. Shared Folder

2. Select the `AML_Scattered_Plot` report from the navigation tree: `Shared Folders/TA/TA_AML/AML_Scattered_Plot`.

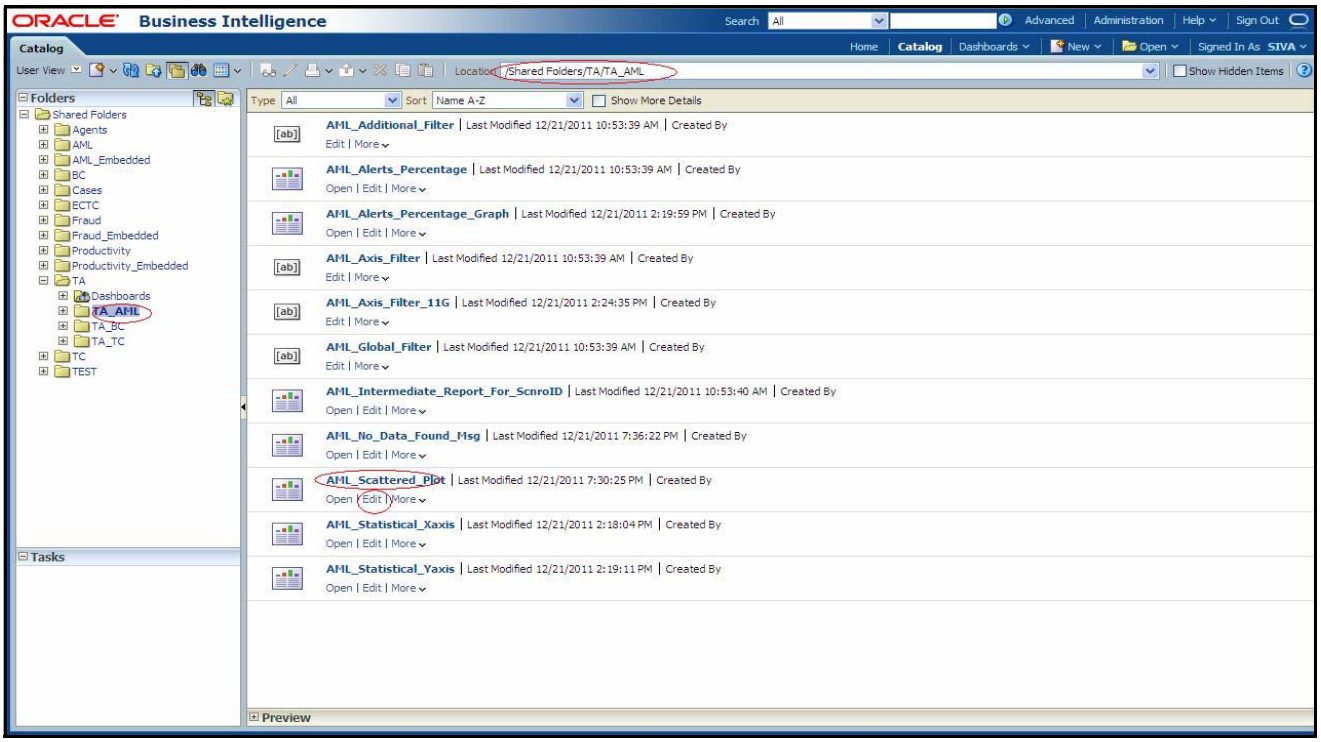

Figure 7. AML_Scattered_Plot Edit

3. Click **Edit**.
4. Click **Graph** view and select **Edit** view(Figure 8).

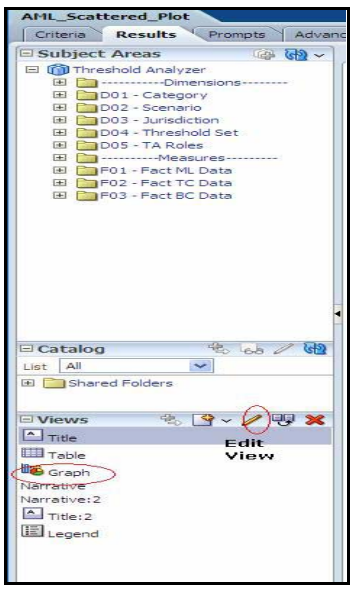

Figure 8. Answers Page - Criteria

5. Click Chart View properties ->Style ->Style and Conditional Formatting (Figure 9).

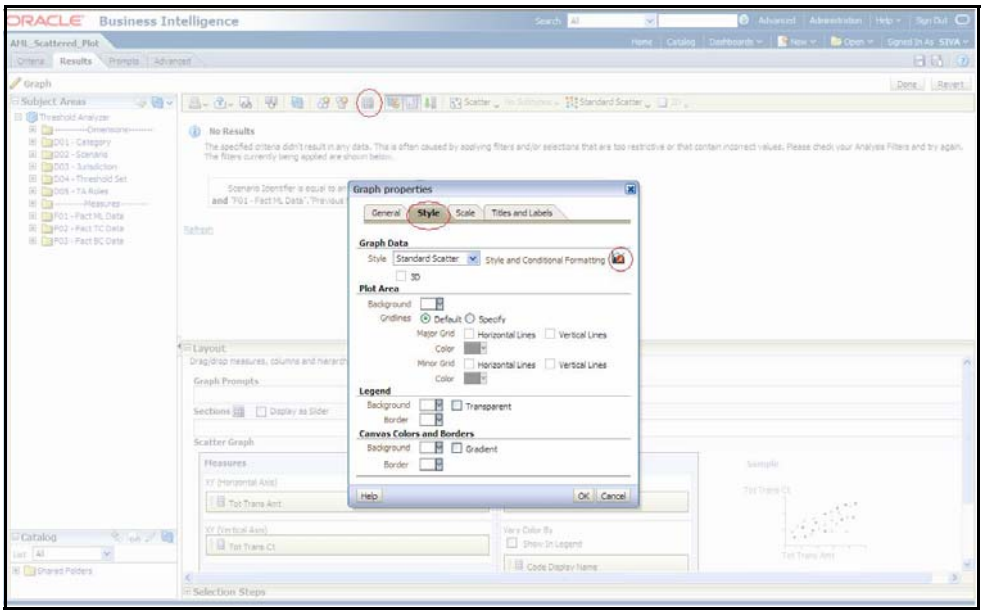

Figure 9. Chart View Properties

6. Select **Conditional Formatting**. You can see the color codes of existing code display names. (Figure 10).

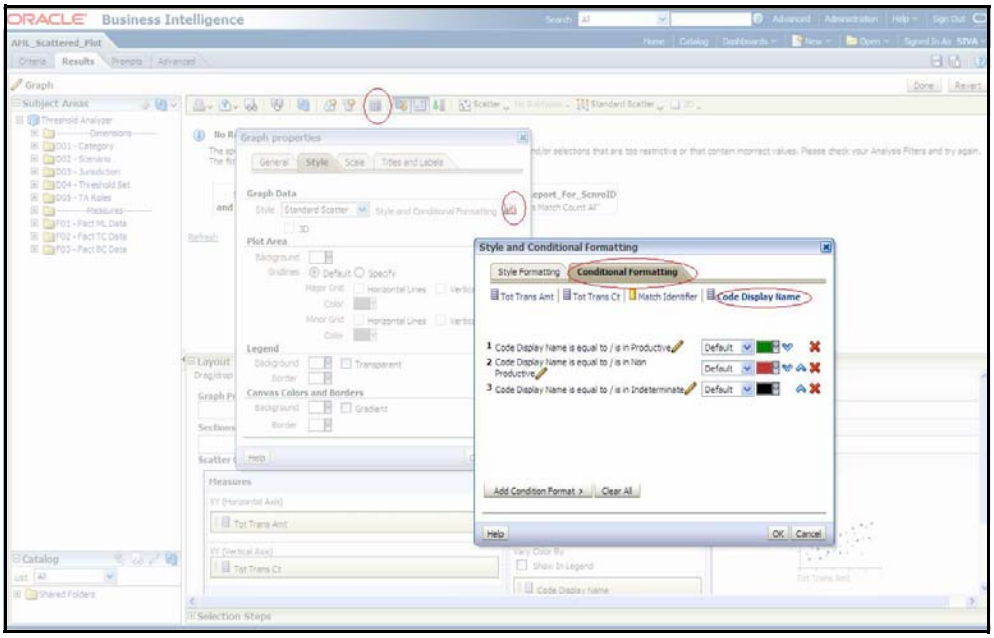

Figure 10. Conditional Formatting

7. To add conditional format, select **Code Display Name** from the Add Conditional Format tab.

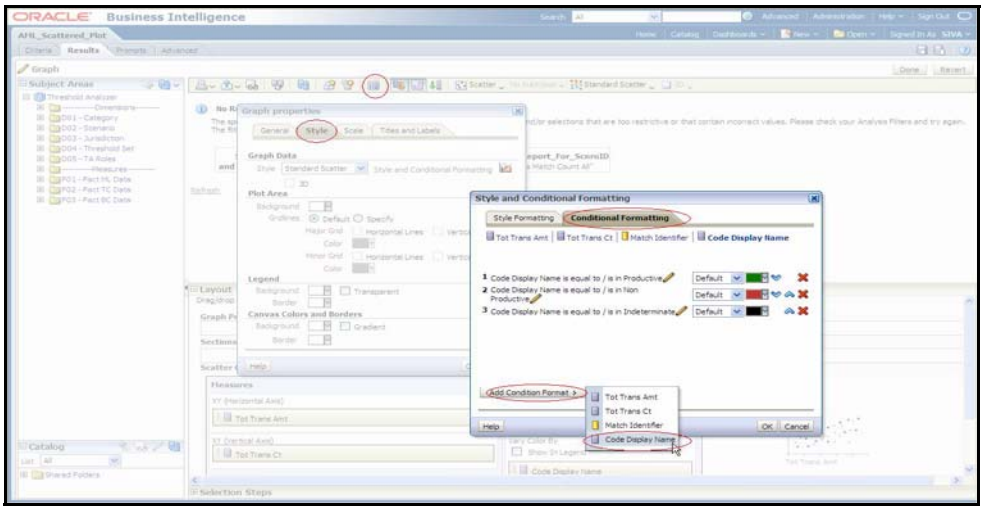

Figure 11. Add Conditional Format

8. In the Create/Edit Filter window, click the **All Choices** link. The Quality Rating description options display (for example, Productive, Non Productive, and Indeterminate).
9. Choose one option at a time from the available options and click **OK** (Figure 12).

   Note: When you click the **All Choices** link and it does not display all the Quality Code descriptions, then manually write the description in the value field. Do this for each description. In addition, ensure that you have given all the descriptions that are present in the `KDD_CODE_TRANS_TRLN` table where `CODE_SET ='A'`.

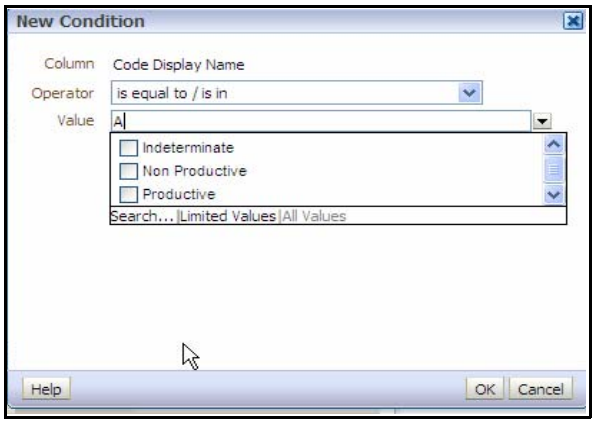

Figure 12. Create/Edit Filter Page

10. On selecting the choices, a new window displays (Figure 13). Under the **Type** drop-down list, select the **Round** option for each Quality Code description.

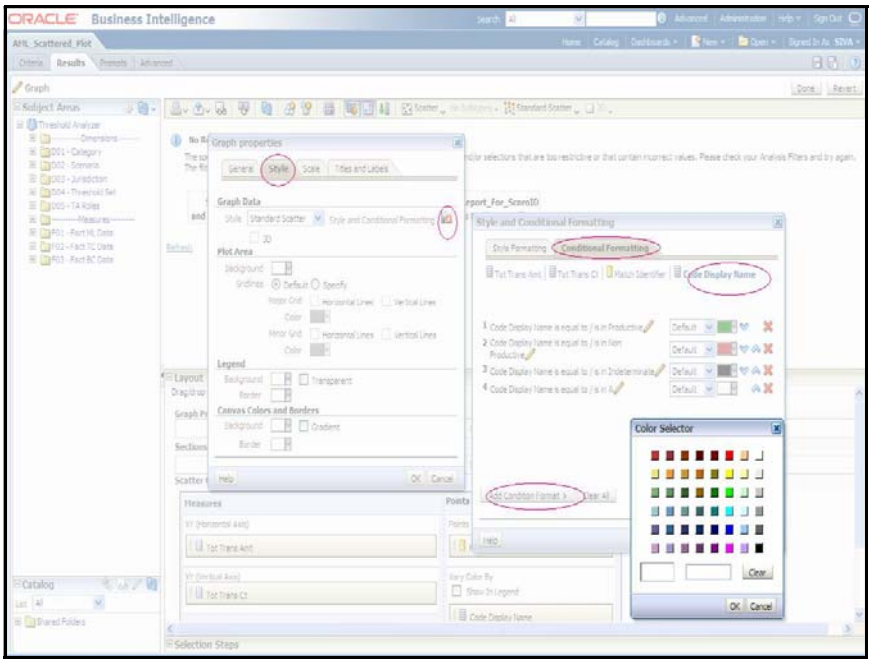

Figure 13. Format Chart Data - Type and Color Column

11. Click a blank box under the **Color** option of the Format Chart Data.

    A Color Selector window displays (Figure 14).

12. Select a color for each Quality Code description and click **OK**.

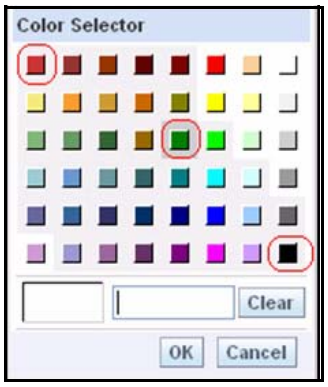

Figure 14. Color Selector Toolbox

13. Click **Save Request**.

Table 41 lists the prepackaged color coding schemes.

Table 41. Prepackaged Color Coding

Quality Code Description	Color	Color Code
Productive	Green	#008000
Indeterminate	Black	#000000
Non Productive	Red	#CC3333

The prepackaged color coding rule is as follows:

- The most prioritized alerts display in Green (that is, Productive or Actionable dependents on Customer requirement).
- The average prioritized alerts display in Black (that is, Indeterminate).
- The least prioritized alerts display in Red (that is, Non Productive or Non Actionable depending on user requirements).

If the user has the same code and some other description, then the color coding should be changed as per the above rules.

If the user has some extra quality rating code in addition to the existing code, then the color of additional description should be based on customer requirements.

Note: Follow the same steps to change the color codes of TA_BC and TA_TC pages.

Changing the Color Code of the Statistical Reports

To change the color coding of the Statistical reports in the Threshold Analyzer utility, follow these steps:

1. After logging into the OBIEEAnalytics URL, Click **Catalog** link (Figure 6).
2. Select the `AML_Statistical_Xaxis` report from the navigation tree:`Shared Folders/TA/TA_AML/AML_Statistical_Xaxis.`
3. Follow steps 3 to 10, 12, and 13 from the section *Changing the Color Code of the Scatter Reports,* on page 89.
4. Click **Save Request**.

   Note: Follow the same steps to change the color code of TA_BC and TA_TC pages.

Configuring the Quality Rating of Matches in the Threshold Analyzer Scatter Graph

The Threshold Analyzer utility generates reports based upon data in the KDD_TA_DATA table. The KDD_TA_DATA table is populated using an run_insert_ta_utility.sh and run_update_ta_utility.sh scripts, which brings data from multiple sources within the Alert Management schema into one table. These scripts contain an Insert component and an Update component. The Update component is the procedure that updates the Alert Quality Code (KDD_TA_DATA.QLTY_RTG_CD). The default logic for determining the Alert Quality Code is to utilize the closing classification code associated with an alert that has been closed. In order to modify the logic for determining the Alert Quality Code, it is necessary to update the run_update_ta_utility.sh scripts update procedure. For assistance in doing that, it is recommended that you contact Oracle Support.

CHAPTER 10 Personal Trading Approval Configuration

This chapter provides instructions for configuring parameters for the Personal Trading Approval application specific to the Account Approval (AA), Pre-Trade Approval (PTA), and Attestation (AT) functionality.

It includes the following sections:

- Configuring AA Default Owner
- Configuring PTA Default Owner
- Configuring AT Default Owner
- Configuring AA/PTA/AT Default Access Right
- Configuring AA/PTA Four Eyes Approval
- Configuring AA/PTA View Attachment and Comment
- Configuring AA/PTA/AT E-mail Notification
- Configuring Attestation Reporting Period
- Configuring AA Request Exception Action Limit
- Configuring PTA Holding Period
- Configuring PTA Request Auto Approve STR
- Configuring PTA Request Auto Reject STR
- Configuring PTA Request Auto Approve ETR
- Configuring PTA Request Auto Reject ETR
- Configuring Account Approval Confirmation Text
- Configuring Pre-Trade Approval Confirmation Text
- Configuring Attestation Confirmation Text
- Configuring Security Product Type for PTA
- Working with AA/PTA/AT Action Settings
- Loading AA Data through Excel Upload
- Loading PTA Request Data through Excel Upload

Configuring AA Default Owner

This parameter allows the client to specify the default user group (pool) to which AA requests will be assigned to. Requests from specific employees, such as the President of the Oracle client, may need to be handled by a separate group of users. The default pool is specified in Attribute 1 and the remaining attributes specify specific pool assignment rules based on the Job Title of an employee. This allows for specification of the default *Assign To* users of the requests.

To modify the AA Default Owner, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used for Design** in Parameter category.
3. Select **CR Account Approval Default Assignee** from Parameter Name drop-down.
4. Edit the Parameter.

Table 42 describes the attributes which need to be configured for Configuring AA Default Owner.

Table 42. Configuring AA Default Owner Attributes

Attribute Number	Attribute	Description
1	DEF_OWNER	This attribute specifies the default user group or pool assigned to a account approval request.
2-15	<Employee Job Title, e.g. CEO>	This attribute specifies the user group or pool assigned to a specific employee based on the employee's job title. The attribute value must match the value present in the `TITL_NM` field in the EMP table of an employee of interest.

Configuring PTA Default Owner

This parameter allows the client to specify the default user group (pool) to which PTA requests will be assigned to. Requests from specific employees, such as the President of the Oracle client, may need to be handled by a separate group of users. The default pool is specified in Attribute 1 and the remaining attributes specify specific pool assignment rules based on the Job Title of an employee. This allows for specification of the default *Assign To* users of the requests.

To modify the PTA Default Owner, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used for Design** in Parameter category.
3. Select **CR Pre-Trade Default Assignee** from Parameter Name drop-down.
4. Edit the Parameter.

Table 43 describes the attributes which need to be configured for Configuring PTA Default Owner.

Table 43. Configuring PTA Default Owner Attributes

Attribute Number	Attribute	Description
1	DEF_OWNER	This attribute specifies the default user group or pool assigned to a pre-trade approval request.
2-15	<Employee Job Title, e.g. CEO>	This attribute specifies the user group or pool assigned to a specific employee based on the employee's job title. The attribute value must match the value present in the TITL_NM field in the EMP table of an employee of interest.

Configuring AT Default Owner

This parameter allows the client to specify the default user group (pool) to which an attestation will be assigned to. An attestation from specific employees, such as the President of the Oracle client, may need to be handled by a separate group of users. The default pool is specified in Attribute 1 and the remaining attributes specify specific pool assignment rules based on the Job Title of an employee. This allows for specification of the default *Owner* users of the requests.

To modify the AT Default Owner, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used for Design** in Parameter category.
3. Select **CR Attestation Default Assignee** from Parameter Name drop-down.
4. Edit the Parameter.

Table 44 describes the attributes which need to be configured for Configuring AT Default Owner.

Table 44. Configuring AT Default Owner Attributes

Attribute Number	Attribute	Description
1	DEF_OWNER	This attribute specifies the default user group or pool assigned to a Attestation.
2-15	<Employee Job Title, e.g. CEO>	This attribute specifies the user group or pool assigned to a specific employee based on the employee's job title. The attribute value must match the value present in the TITL_NM field in the EMP table of an employee of interest.

Configuring AA/PTA/AT Default Access Right

This parameter defines the default business domain and jurisdiction for the external investment account, AA/PTA request and attestation (AT). This parameter can have values Y or N.

If the parameter value is set to Y, then business domain and jurisdiction set in the parameter is assigned to the external investment account, AA/PTA request, and attestation.

If the parameter value is set to N, then the business domain and jurisdiction of the employee submitting the AA/PTA request or attestation is inherited. In the event the business domain and jurisdiction of the employee is not provided, then the parameter value set for business domain and jurisdiction is assigned to the external investment account, the AA/PTA request and attestation.

To modify AA/PTA/AT Default Access Right, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used for Design** in Parameter category.
3. Select **CR Default Access Right** from Parameter Name drop-down.
4. Edit the Parameter.

Table 45 describes the attributes which need to be configured for Configuring AA/PTA/AT Default Access Right.

Table 45. Configuring AA/PTA Default Access Right Attributes

Attribute	Description	Attribute Sample Value
Business Domain	This attribute defines the default business domain for the external account and AA/PTA/AT requests.	a
Jurisdiction	This attribute defines the default jurisdiction for the external account and AA/PTA/AT requests.	AMEA

Configuring AA/PTA Four Eyes Approval

This parameter allows the client to specify whether an AA/PTA request requires four eyes approval from an employee with either an Investment Policy (IP) Manager or IP Manager Supervisor role, which can be set to either Y (Yes) or N (No). To enable Four Eyes Approval, the following conditions must be true:

- This parameter must be set to Y.
- Employee of the submitted request has access to sensitive information, where the Information Sensitive Indicator field in the Employee file is set to Y.
- An Investment Policy Manager in the Employee file is designated to the employee of the submitted request.

Enabling Four Eyes Approval will give the user with CR Analyst/Supervisor role the action to only recommend a request for approval and, subsequently, a user with IP Manager/IP Manager Supervisor role has the action to approve or reject the same request.

If all three conditions above are not met for an employee submitting the request, then Four Eyes Approval is not required on the request. This gives the user with CR Analyst/Supervisor role the action to approve the request and not the IP Manager/IP Manager Supervisor user.

To modify the AA/PTA Four Eyes Approval, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used for Design** in Parameter category.
3. Select **CR Four Eyes Approval** from Parameter Name drop-down.
4. Edit the Parameter.

Table 46 describes the attributes which need to be configured for Configuring AA/PTA Four Eyes Approval.

Table 46. Configuring AA/PTA Four Eyes Approval Attributes

Attribute	Description	Attribute Sample Value
AA	The parameter can have only Y or N value. Y enables Four Eye Approval which allows a CR Analyst/Supervisor user to only recommend approval of a request and an IP Manager/IP Manager Supervisor user to approve the same request. N disables Four Eye Approval which requires only the CR Analyst/Supervisor user to approve a request. This is for Account Approval application.	Y
PTA	The parameter can have only Y or N value. Y enables Four Eye Approval which allows a CR Analyst/Supervisor user to only recommend approval of a request and an IP Manager/IP Manager Supervisor user to approve the same. N disables Four Eye Approval which requires only the CR Analyst/Supervisor user to approve a request. This is for Pre-Trade Approval application.	Y

Configuring AA/PTA View Attachment and Comment

This parameter defines whether a user with an IP Manager or IP Manager Supervisor role can view comments and attachments submitted by a user with a Control Room (CR) Analyst/Supervisor role by setting this parameter to Y; otherwise when set to N, the user with the IP Manager/IP Manager Supervisor role cannot see any comments or attachments submitted by a user with CR Analyst/Supervisor role.

To modify the AA/PTA View Attachment and Comment, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **UI Display** in Parameter category.
3. Select **CR View Attachment and Comment** from Parameter Name drop-down.
4. Edit the Parameter.

Configuring AA/PTA/AT E-mail Notification

This parameter defines the attributes required for e-mail notification in Account Approval/Pre-Trade Approval/Attestation. This parameter can have Y value.

To modify the AA/PTA/AT e-mail notification, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used For design** in Parameter category.
3. Select **CR E-mail Notification** from Parameter Name drop-down.
4. Edit the Parameter.

Table 47 describes the attributes which need to be configured for configuring AA/PTA/AT e-mail notification.

Table 47. Configuring AA/PTA/AT E-mail Notification Attributes

Attribute	Description	Attribute Sample Value
From Address	This attribute specifies the e-mail address identifying where the e-mail notification is coming from.	compliance@org.com
CC Address for Account Approval	CC Email address when performing Email Notification for Account Approval. Multiple e-mail addresses must be separated by a semi-colon (;).	compliance@org.com
BCC Address for Account Approval	BCC Email address when performing Email Notification for Account Approval. Multiple e-mail addresses must be separated by a semi-colon (;).	compliance@org.com
CC Address for Pre-Trade Approval	CC Email address when performing Email Notification for Pre-Trade Approval. Multiple e-mail addresses must be separated by a semi-colon (;).	compliance@org.com
BCC Address for Pre-Trade Approval	BCC Email address when performing Email Notification for Pre-Trade Approval. Multiple e-mail addresses must be separated by a semi-colon (;).	compliance@org.com
CC Address for Attestation	CC Email address when performing Email Notification for Attestation. Multiple e-mail addresses must be separated by a semi-colon (;).	compliance@org.com
BCC Address for Attestation	BCC Email address when performing Email Notification for Attestation. Multiple e-mail addresses must be separated by a semi-colon (;).	compliance@org.com
Account Approval Workflow Subject	The subject that need to be present in the Email Notification for Account Approval Workflow.	Account Approval Workflow Notification:Request $AARrequestID$ for $BrokerDealer$ $AccountID$ status updated to $AARstatus$
Pre-Trade Approval Workflow Subject	The subject that need to be present in the Email Notification for Pre-Trade Approval Workflow.	Pre-Trade Approval Workflow Notification:Request $PTArequestID$ status updated to $PTAstatus$

Table 47. Configuring AA/PTA/AT E-mail Notification Attributes

Attestation Workflow Subject	The subject that need to be present in the Email Notification for Attestation Workflow.	Attestation Workflow Notification: Attestation $AttestationID$ status updated to $ATstatus$
MAIL_FOOTER	This attribute specifies footer details which can be appended to the e-mail.	Please do not reply to this system generated e-mail.

The e-mail notification subject for Account Approval, Pre-Trade Approval, and Attestation Workflow can be customized using the following tokens.

Table 48. AA/PTA/AT E-mail Notification Message Tokens

E-mail Subject Token	Description	Workflow
$AAaction$	Action taken on the Account Approval Request	Account Approval
$AAactionBy$	Name of person who took action on an Account Approval Request	Account Approval
$AAcommentToEmp$	Comment entered by Control Room directed to the submitter of the Account Approval Request; otherwise “(No comment provided)” is displayed	Account Approval
$AARrequestID$	ID assigned to the Account Approval request	Account Approval
$AARstatus$	Status of the Account Approval Request	Account Approval
$Account$	Investment account held with a broker/dealer as submitted in the Account Approval Request	Account Approval
$AssignedToID$	Full name of the employee currently assigned to the AA request	Account Approval
$BrokerDealer$	Name of the broker/dealer where the Investment account as submitted in the Account Approval Request	Account Approval
$PTAaction$	Action taken on the Pre-trade Approval Request	Pre-Trade Approval
$PTAactionBy$	Name of person who took action on an Pre-trade Approval Request	Pre-Trade Approval
$PTAcommentToEmp$	Comment entered by Control Room directed to the submitter of the Pre-trade Approval Request; otherwise “(No comment provided)” is displayed	Pre-Trade Approval
$PTArequestID$	ID assigned to the Pre-trade Approval Request	Pre-Trade Approval
$PTAstatus$	Status of the Pre-trade Approval Request	Pre-Trade Approval
$ATaction$	Action taken on an Attestation	Attestation
$ATactionBy$	Name of person who took action on an Attestation	Attestation
$ATcommentToEmp$	Comment entered by Control Room directed to the submitter of the Attestation; otherwise “(No comment provided)” is displayed.	Attestation
$ATstatus$	Status of the Attestation	Attestation
$AttestationID$	ID assigned to the Attestation	Attestation
$Employee$	Name of employee who submitted the Account Approval Request, Pre-trade Approval Request, or Attestation	Account Approval Pre-Trade Approval Attestation

Configuring Attestation Reporting Period

This parameter defines the attestation reporting period. The start date attribute defines the start date of the attestation period, the end date attribute defines the end date of the attestation period, Date Format Define Format of start date and end date and Date validation operator define comparison operator for start date and end date .

To modify the Attestation Reporting Period, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used for Design** in Parameter category.
3. Select **CR Attestation Reporting Period** from Parameter Name drop-down.
4. Edit the Parameter.

Table 49 describes the attributes which need to be configured for Configuring AA Account Attestation Reporting Period.

Table 49. Configuring Attestation Reporting Attributes

Attribute	Description	Attribute Sample Value
Start Date	Defines the attestation period start date. The date format should be based on the specified value in the Date Format attribute.	01/01/2012
End Date	Defines the attestation period end date. Attestation end date should be greater than attestation start date. The date format should be based on the specified value in the Date Format attribute.	01/03/2013
Date Format	Date format the value of the date attribute needs to be provided.	MM/DD/YYYY
Date Validation Operator	Validation operator to compare the Start Date attribute against the End Date attribute. Valid values are <, <=, or =.	<=

Configuring AA Request Exception Action Limit

This parameter defines the number of times an employee can perform a Request Exception Action on a rejected AA request with Pending Closure/Removal status in the account approval process.

To modify the AA Request Exception Action Limit, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used for Design** in Parameter category.
3. Select **CR Request Exception Action Limit** from Parameter Name drop-down.
4. Edit the Parameter.

Configuring PTA Holding Period

This parameter defines the specific number of days prior to the submission date of the PTA request to identify what specific External Investment Account Position data is to be displayed in the Pre-Trade Approval Request Details page for users with CR Analyst, CR Supervisor, IP Manager, or IP Manager Supervisor role. The different holding period for Equity (EQT), Preferred (PRE), Option (OPT), and Fixed Income (FI) trades are captured in Attribute 1, Attribute 2, Attribute 3, and Attribute 4 values, respectively.

To modify the PTA Holding Period Parameter, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **UI Display** in Parameter category.
3. Select **CR Holding Period Parameter** from Parameter Name drop-down.
4. Edit the Parameter.

Table 50 describes the attributes which need to be configured for configuring PTA Holding Period Parameter.

Table 50. Configuring PTA Holding Period Attributes

Attribute	Description	Attribute Sample Value
EQT	Configurable holding period parameter to specific number of days from the submission date of the EQT request to identify what specific External Investment Account Position to display.	30
PRE	Configurable holding period parameter to specific number of days from the submission date of the PRE request to identify what specific External Investment Account Position to display.	30
OPT	Configurable holding period parameter to specific number of days from the submission date of the OPT request to identify what specific External Investment Account Position to display.	30
FI	Configurable holding period parameter to specific number of days from the submission date of the FI request to identify what specific External Investment Account Position to display.	30

Configuring PTA Request Auto Approve STR

This parameter defines whether a PTA Request is automatically approved as long as the attributes of the request is not on an effective security trading restriction (STR) list. This parameter can be set to Y or N.

- If the parameter value is set to Y, it indicates that Auto Approval is enabled.
- If the parameter value is set to N, it indicates that Auto Approval is disabled.

To modify the PTA Request Auto Approve Parameter, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used For Design** in Parameter category.
3. Select **CR Pre-Trade Auto Approve STR** from Parameter Name drop-down.
4. Edit the Parameter.

Table 51. Configuring PTA Request Auto Approve STR

Attribute	Description	Attribute Sample Value
Restriction List	The Restriction List to be considered for Auto Approve should be provided in Attribute 11 value as comma separated values. The values listed in the Restriction List attribute must also be present in the Restriction List Identifier of the Security Trading Restriction file. For more information on the Security Trading Restriction file, refer to the *Oracle Financial Services Behavior Detection Platform Data Interface Specification Guide.*	RL

Configuring PTA Request Auto Reject STR

This parameter defines whether PTA Request is automatically rejected if the attributes of the request is found on an effective security trading restriction (STR) list. This parameter can have values Y or N.

- If the parameter value is set to Y, it indicates that Auto Reject is enabled.
- If the parameter value is set to N, it indicates that Auto Reject is disabled.

To modify the PTA Request Auto Reject Parameter, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used For Design** in Parameter category.
3. Select **CR Pre-Trade Auto Reject** STR from Parameter Name drop-down.
4. Edit the Parameter.

Table 52. Configuring PTA Request Auto Reject STR

Attribute	Description	Attribute Sample Value
Restriction List	The Restriction List to be considered for Auto Reject should be provided in Attribute 11 value as comma separated values. The values listed in the Restriction List attribute must also be present in the Restriction List Identifier of the Security Trading Restriction file. For more information on the Security Trading Restriction file, refer to the *Oracle Financial Services Behavior Detection Platform Data Interface Specification Guide.*	RL

Configuring PTA Request Auto Approve ETR

This parameter defines whether a PTA Request is automatically approved as long as the attributes of the request is not on an effective employee trading restriction (ETR) list. This parameter can be set to Y or N.

- If the parameter value is set to Y, it indicates that Auto Approval is enabled.
- If the parameter value is set to N, it indicates that Auto Approval is disabled.

To modify the PTA Request Auto Approve Parameter, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used For Design** in Parameter category.
3. Select **CR Pre-Trade Auto Approve ETR** from Parameter Name drop-down.
4. Edit the Parameter.

Table 53. Configuring PTA Request Auto Approve ETR

Attribute	Description	Attribute Sample Value
Restriction List	The Restriction List to be considered for Auto Approve should be provided in Attribute 11 value as comma separated values. The values listed in the Restriction List attribute must also be present in the Restriction List Identifier of the Security Trading Restriction file. For more information on the Security Trading Restriction file, refer to the *Oracle Financial Services Behavior Detection Platform Data Interface Specification Guide.*	RL

Configuring PTA Request Auto Reject ETR

This parameter defines whether PTA Request is automatically rejected if the attributes of the request is found on an effective employee trading restriction (ETR) list. This parameter can have values Y or N.

- If the parameter value is set to Y, it indicates that Auto Reject is enabled.
- If the parameter value is set to N, it indicates that Auto Reject is disabled.

To modify the PTA Request Auto Reject Parameter, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used For Design** in Parameter category.
3. Select **CR Pre-Trade Auto Reject** ETR from Parameter Name drop-down.
4. Edit the Parameter.

Table 54. Configuring PTA Request Auto Reject ETR

Attribute	Description	Attribute Sample Value
Restriction List	The Restriction List to be considered for Auto Reject should be provided in Attribute 11 value as comma separated values. The values listed in the Restriction List attribute must also be present in the Restriction List Identifier of the Security Trading Restriction file. For more information on the Security Trading Restriction file, refer to the *Oracle Financial Services Behavior Detection Platform Data Interface Specification Guide.*	RL

Configuring Account Approval Confirmation Text

This parameter defines the confirmation text to be displayed to the employee upon submission of an Account Approval request that has been newly submitted (Attribute 1 = New) and cleared account that has been modified (Attribute 2 = Modify Cleared).To modify AA/PTA Default Access Right, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used for Design** in Parameter category.
3. Select **CR Account Approval Confirmation Text** from Parameter Name drop-down.
4. Edit the Parameter.

Table 55 describes the attributes which need to be configured for Configuring AA/PTA Default Access Right.

Table 55. Configuring Account Approval Confirmation Text

Attribute	Description	Attribute Sample Value

Table 55. Configuring Account Approval Confirmation Text

New	Defines the confirmation text to be displayed to the employee upon submission of an Account Approval request	By clicking the Submit or Submit & Attach button, you confirm the account information provided is accurate and true and to be submitted for approval; otherwise click Cancel to make the necessary modifications.
Modify Cleared	Defines the confirmation text to be displayed to the employee upon modification of an Account Approval request with a Cleared status	By clicking the Submit or Submit and Attach button, you confirm the modified information on the cleared account is accurate and true and to be submitted for approval; otherwise click Cancel to make the necessary modifications.

Configuring Pre-Trade Approval Confirmation Text

This parameter defines the confirmation text to be displayed to the employee upon submission of an Pre-Trade Approval request that has been newly submitted (Attribute 1 = New). To modify AA/PTA Default Access Right, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used for Design** in Parameter category.
3. Select **CR Pre-Trade Approval Confirmation Text** from Parameter Name drop-down.
4. Edit the Parameter.

Table 56 describes the attributes which need to be configured for Configuring AA/PTA Default Access Right.

Table 56. Configuring Pre-Trade Approval Confirmation Text

Attribute	Description	Attribute Sample Value
New	Defines the confirmation text to be displayed to the employee upon submission of an Pre-Trade Approval request	I agree the trade request information I am submitting is complete and accurate.

Configuring Attestation Confirmation Text

This parameter defines the text to be displayed to the employee in the Attestation form in different sections of the form. Attribute 1 contains the text for the confirmation section of the Employee Details. Attribute 2 contains the text for the confirmation section of the Approved Account Details. Attribute 3 contains the text for the confirmation section after employee clicks the Submit button and before the attestation is submitted into the system.

To modify AA/PTA Default Access Right, follow these steps:

1. Open Manage Installation Parameter Screen (Figure 1).
2. Select **Used for Design** in Parameter category.
3. Select **CR Attestation Confirmation Text** from Parameter Name drop-down.
4. Edit the Parameter.

Table 57 describes the attributes which need to be configured for Configuring AA/PTA Default Access Right.

Table 57. Configuring Attestation Confirmation Text

Attribute	Description	Attribute Sample Value
Employee	Confirmation text to be displayed to the employee in the Employee Details section of the Attestation form	My employee details are complete and accurate.
Account	Confirmation text to be displayed to the employee in the Approved Investment Accounts section of the Attestation form	My investment account details are correct and accurate.
New	Overall attestation confirmation text to be displayed to the employee at the bottom of the Attestation form	By clicking the Submit or Submit & Attach button, you confirm this attestation is accurate and true and to be submitted for review; otherwise click Cancel to make the necessary modifications.
Outside Business Activity	Confirmation text to be displayed to the employee in the Outside Business Activity section of the Attestation form	My outside business activity details are correct and accurate.
Private Security Transaction	Confirmation text to be displayed to the employee in the Private Security Transaction section of the Attestation form	My private security transaction details are correct and accurate.

Configuring Security Product Type for PTA

In the PTA application, the Oracle client can define a list of security product types, categorized by product category, applicable when an employee is submitting a new PTA request. This information must be provided in the Reference Table Detail file where the Codeset Identifier, 'ProductType', is reserved for this purpose. For further details on how to populate the Reference Table Detail file, refer to the *Oracle Financial Services Data Interface Specification (DIS) Guide.*

The following fields in the Reference Table Detail must be populated as follows:

Table 58. Configuring Product Type in Reference Table Detail Table

Field	Instruction	Sample value
Codeset Identifier	Populate this field with ‘ProductType'	'ProductType'
Code1	Oracle client specified product type code within the product category for the security.	'CORP'
Code2	Mapping of the product type to the product category for the security. Allowable values are EQT, PRE, OPT, and FI. Refer to the Standard Code Values for Product Category in the Security file as defined in the DIS.	'FI'
Code Description	Description of the Oracle client specified product type code in Code1 field.	'Corporate Bond'
Code Additional Information	Description of the product type mapping.	'Fixed Income (FI) Product Category to Product Type Mapping'

Working with AA/PTA/AT Action Settings

Modifying AA/PTA/AT Status Descriptions

You can modify the existing status descriptions displayed on the AA/PTA/AT application in the KDD_CNTRL_ROOM_STATUS table for AA , PTA and AT using the following query:

```
update KDD_CNTRL_ROOM_STATUS set STATUS_DESC_TX = '(New Status)' where CNTRL_RM_STATUS_CD = '(Status Code to be Changed)'
```

For example, to change the status from "Cleared" to "Approved", the query is as follows:

```
update KDD_CNTRL_ROOM_STATUS set STATUS_DESC_TX = 'Approved' where CNTRL_RM_STATUS_CD = 'AA_CLEAR'
```

For AA, refer to statuses where KDD_CNTRL_ROOM_STATUS.ACTN_TYPE_WKFLW_TYPE_CD = 'AA'.

For PTA, refer to statuses where KDD_CNTRL_ROOM_STATUS.ACTN_TYPE_WKFLW_TYPE_CD = 'PA'.

For AT, refer to statuses where KDD_CNTRL_ROOM_STATUS.ACTN_TYPE_WKFLW_TYPE_CD = 'AT'.

Configuring Standard Comment Data

The standard comments are created in the KDD_CMMNT table, and the categories are in the KDD_CMMNT_CAT_CD table. To add a new standard comment for selection in AA/PTA/AT, follow these steps:

1. Add an entry into KDD_CMMNT table:

   ```
   insert into KDD_CMMNT (CMMNT_ID, EDIT_FL,CMMNT_TX,DISPL_ORDER_NB, CMMNT_CAT_CD)
   values (1000, 'N','Awaiting Approval', 20, 'CR')
   ```

   Make sure CMMNT_CAT_CD = 'CR' which is reserved for AA/PTA/AT standard comments.

2. Save your changes to the KDD_CMMNT table.

Configuring Standard Comments to AA/PTA/AT Actions Data

You can configure the standard comments available for selection to the user based on the chosen action in the Actions dialog box in the AA/PTA/AT application. The mappings from AA/PTA/AT actions to standard comments are configured by setting column values in the KDD_CNTRL_ROOM_ACTN_CMMNT table:

```
insert into KDD_CNTRL_ROOM_ACTN_CMMNT  (CNTRL_RM_ACTN_TYPE_CD, CMMNT_ID) values ('AA080', 8067)
```

Details of the AA/PTA/AT actions are stored in the KDD_CNTRL_ROOM_ACTN_TYPE table and should not be modified. For AA, refer to actions where KDD_CNTRL_ROOM_ACTN_TYPE.ACTN_TYPE_WKFLW_TYPE_CD = 'AA'. For PTA, refer to actions where KDD_CNTRL_ROOM_ACTN_TYPE.ACTN_TYPE_WKFLW_TYPE_CD = 'PA'. For AT, refer to actions where KDD_CNTRL_ROOM_ACTN_TYPE.ACTN_TYPE_WKFLW_TYPE_CD = 'AT'. The following actions are reserved and **cannot** be mapped to standard comments due to the nature of how the action is taken in the AA/PTA/AT application:

- AA: AA010, AA040, AA240, AA220a, AA220b, AA160
- PTA: PA010, PA020, PA030, PA180a, PA180b

- AT: AT010, AT020, AT100a, AT100b

Configuring E-mail Notifications by AA/PTA/AT Actions Data

In the AA/PTA, e-mail notification messages may be sent to the submitter of the request, the user assigned to the request, and the current review owner of the request each time an action is taken on a request. For AA/PTA, you can configure the e-mail notification messages sent to the submitter (`SBMTR_NTFCTN_EMAIL_MSG_TX`), assignee (`ASSIGNED_NTFCTN_EMAIL_MSG_TX`), and the current review owner (`OWNER_NTFCTN_EMAIL_MSG_TX`) of the AA/PTA request mapped to an action by updating the column values in the `KDD_CNTRL_ROOM_ACTN_EMAIL` table.

In the AT application, e-mail notification messages may be sent to the submitter of the request and the current review owner of the request each time an action is taken on a request. You can configure the e-mail notification messages sent to the submitter (`SBMTR_NTFCTN_EMAIL_MSG_TX`) and the current review owner (`OWNER_NTFCTN_EMAIL_MSG_TX`) of the request mapped to an action by updating the column values in the `KDD_CNTRL_ROOM_ACTN_EMAIL` table.

Here is an example of updating the e-mail notification messages for Approve (Level 2) action in PTA:

```
update KDD_CNTRL_ROOM_ACTN_EMAIL set
SBMTR_NTFCTN_EMAIL_MSG_TX = 'This pre-trade approval request has been approved by Control Room for trading.',
ASSIGNED_NTFCTN_EMAIL_MSG_TX = 'This pre-trade approval request has been approved.',
OWNER_NTFCTN_EMAIL_MSG_TX = 'This pre-trade approval request has been approved by the IP Manager.'
where CNTRL_RM_ACTN_TYPE_CD = 'PA100'
```

Note: If the request has the same user ID for the assignee and current owner and both the `ASSIGNED_NTFCTN_EMAIL_MSG_TX` and `OWNER_NTFCTN_EMAIL_MSG_TX` contains an e-mail notification message for a specific action taken, then the e-mail notification message for the current owner will only be sent.

The e-mail notification messages for Account Approval, Pre-Trade Approval, and Attestation Workflow can be customized using the following tokens:

Table 59. E-mail Notification Tokens for AA/PTA/AT

E-mail Notification Token	Description	Workflow
$AAaction$	Action taken on the Account Approval Request	Account Approval
$AAactionBy$	Name of person who took action on an Account Approval Request	Account Approval
$AAcommentToEmp$	Comment entered by Control Room directed to the submitter of the Account Approval Request; otherwise “(No comment provided)” is displayed	Account Approval
$AARrequestID$	ID assigned to the Account Approval request	Account Approval
$AARstatus$	Status of the Account Approval Request	Account Approval
$Account$	Investment account held with a broker/dealer as submitted in the Account Approval Request	Account Approval

Table 59. E-mail Notification Tokens for AA/PTA/AT

$AssignedToID$	Full name of the employee currently assigned to the AA request	Account Approval
$BrokerDealer$	Name of the broker/dealer where the Investment account as submitted in the Account Approval Request	Account Approval
$PTAaction$	Action taken on the Pre-trade Approval Request	Pre-Trade Approval
$PTAactionBy$	Name of person who took action on an Pre-trade Approval Request	Pre-Trade Approval
$PTAcommentToEmp$	Comment entered by Control Room directed to the submitter of the Pre-trade Approval Request; otherwise "(No comment provided)" is displayed	Pre-Trade Approval
$PTArequestID$	ID assigned to the Pre-trade Approval Request	Pre-Trade Approval
$PTAstatus$	Status of the Pre-trade Approval Request	Pre-Trade Approval
$ATaction$	Action taken on an Attestation	Attestation
$ATactionBy$	Name of person who took action on an Attestation	Attestation
$ATcommentToEmp$	Comment entered by Control Room directed to the submitter of the Attestation; otherwise "(No comment provided)" is displayed.	Attestation
$ATstatus$	Status of the Attestation	Attestation
$AttestationID$	ID assigned to the Attestation	Attestation
$Employee$	Name of employee who submitted the Account Approval Request, Pre-trade Approval Request, or Attestation	Account Approval Pre-Trade Approval Attestation

For example, the AA Reassign action, AA135, will send the following e-mail notification message to the current owner of the AA request - *This account has been re-assigned to IP Manager $AssignedToID$ for account approval.*

Loading AA Data through Excel Upload

Steps for Excel Upload

The Excel upload process inserts the data into the appropriate database tables based on the pre-configured Excel upload definitions installed as part of the application installation. Data already existing should not be loaded again, as this would result in failure of upload. When uploading additional records, only the incremental records should be maintained in the Excel template with the correct unique identifier key.

1. All template Excel files for Excel upload are available in `ftpshare/STAGE/Excelupload/AMCMLookup`Files.
2. All date values should be provided in MM/DD/YYYY format in the Excel worksheet.
3. Whenever a record is deleted from Excel, the complete row should be deleted. In other words, no blank active record should exist in the Excel.
4. After selecting the Excel template, preview it before uploading.

The Excel Upload screen can be accessed by logging in as Admin user.

The following AA tables can be populated using Excel Upload:

Table 60. Account Approval Excel Upload

Database Table	Excel Template	Description
External Investment Account Type	EXTRL_NVSMT_ACCT_TYPE.xls	Reference table to allow the Oracle Financial Services client to define specific account types applicable for the external investment accounts submitted in the AA application.
External Broker/Dealer Firm	EXTRL_BROKER_DEALER_FIRM .xls	Reference table to allow the Oracle Financial Services client to define approved or designated external broker/dealers applicable for the external investment accounts submitted in the AA application.
External Investment Account	EXTRL_NVSMT_ACCT.xls	Before using the Account Approval application, use this template to initialize this table with accounts that have already been approved and/or rejected from the legacy system of the Oracle Financial Services client. To successfully load the data in this table, the External Investment Account Type and External Broker/Dealer Firm tables must first be populated.

Loading PTA Request Data through Excel Upload

Refer to Loading AA Data through Excel Upload , to perform the Excel Upload for Pre-Trade Approval Request.

Table 61. Pre-Trade Approval Excel Upload

Database Table	Excel Template	Description
Pre-Trade Approval Request	PRETRADE_APRVL_RQST.xls	Before using the Pre-Trade Approval application, use this template to initialize this table with pre-trade approval requests that have already been approved and/or rejected from the legacy system of the Oracle Financial Services client. To successfully load the data in this table, data for the Account Approval application must first be populated.

Index