

# Configuration Guide

## Oracle Financial Services:

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

*Release 8.0.6.0.0*

*May 2018*





# **Configuration Guide**

## **Oracle Financial Services:**

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

*Release 8.0.6.0.0*

*May 2018*

Part Number: E90767-01

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

Part Number: E90767-01  
First Edition (May 2018)

**Copyright 2018, Oracle and/or its affiliates. All rights reserved.**

Printed in U.S.A. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission.

**Trademarks**

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

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

# Contents

**List of Figures ..... ix**

**List of Tables ..... xi**

**About this Guide ..... xiii**

Who Should Use this Guide ..... xiii

How this Guide is Organized ..... xiv

Where to Find More Information ..... xv

Conventions Used in this Guide ..... xv

Configuring the Client Logo Image ..... 2

    Logo Specification ..... 2

    Placing a new Client Logo ..... 2

    Removing a Client Logo ..... 2

Configuring the Base Time Zone ..... 3

Configuring the Default Currency Code ..... 4

Configuring the Lock Time Period for Alert Actions ..... 5

Configuring Notifications ..... 6

Configuring E-mail ..... 7

Configuring Organization Type ..... 8

Configuring View All Organization ..... 9

Configuring XML Export ..... 10

Configuring the Display of Value in By Field Name/ID ..... 11

Configuring the Default Due Date Calculation ..... 12

Configuring File Size ..... 12

Configuring Views ..... 13

    Adding Views ..... 13

    Modifying Views ..... 13

    Removing Views ..... 13

Managing Additional Configurations ..... 14

    Changing Passwords for System Accounts ..... 14

    Configuring File Type Extensions ..... 15

    Configuring File Size ..... 15

    Configuring Status To User Role Table ..... 15

    Mapping Status to Role in the Database through Scripts ..... 15

Enabling and Disabling Alert Management ..... 17

Configuring a Visual Cue ..... 18

    For Alerts Nearing Due Date ..... 18

    For Alert Suppression Nearing Expiration Date ..... 18

    For the Trusted Pair Nearing Expiration Date ..... 18

Configuring New Alert Score .....	19
Configuring Alert Inheritance.....	20
Configuring Four Eyes Approval.....	20
Configuring Highlights .....	21
Configuring Alert Highlight Status .....	21
Configuring Organization Relationships for Trade Blotter .....	21
Configuring Search Criteria Population Options for Trade Blotter .....	22
Adding Product Types to the Code Set Translation Table .....	22
Adding Product Subtypes to the Code Set Translation Table .....	23
Adding Trade Characteristics to the Code Set Translation Table .....	23
Configuring Trusted Pair Duration Option .....	24
Creating the Duration for Trusted Pair .....	24
Extending the Duration for Trusted Pair.....	25
Configuring Suppression Rule Duration.....	25
Configuring Default Alert Owner.....	26
Managing Security Restrictions.....	26
Managing Controlling Customer.....	26
Configuring Administration Tools.....	27
Configuring Application Server.....	28
Working with Alert Action Settings.....	29
Understanding Alert Workflows.....	29
Configuring Alert Action Data .....	30
<i>Adding New Alert Data</i> .....	30
<i>Adding New Alert Status</i> .....	30
<i>Mapping the New Activity to User Role</i> .....	31
<i>Mapping the New Activity to the Status</i> .....	31
<i>Mapping the New Activity to the Scenario Class</i> .....	31
Configuring Standard Comment Data .....	31
Configuring Mandatory Action Attributes .....	32
Making Comments Mandatory .....	32
Making Reassignment Mandatory .....	32
<i>Alert Reassignment</i> .....	32
<i>Case Reassignment</i> .....	32
Making a Due-Date for an Action Mandatory .....	33
<i>Alert Due-Date</i> .....	33
<i>Case Due-Date</i> .....	33
Configuring the Session Timeout Setting .....	35
Configuring the Session Timeout Setting for Alert Management and Case Management .....	35
Configuring the Session Timeout Setting for Admin Tools .....	35
Changing the Color Code of the Scatter Reports.....	37
Changing the Color Code of the Statistical Reports .....	43
Configuring the Quality Rating of Matches in the Threshold Analyzer Scatter Graph .....	44
Configuring AA Default Owner .....	46
Configuring PTA Default Owner .....	46

Configuring AT Default Owner.....	47
Configuring AA/PTA/AT Default Access Right.....	48
Configuring AA/PTA Four Eyes Approval.....	48
Configuring AA/PTA View Attachment and Comment.....	49
Configuring AA/PTA/AT E-mail Notification.....	50
Configuring Attestation Reporting Period .....	52
Configuring AA Request Exception Action Limit.....	53
Configuring PTA Holding Period .....	53
Configuring PTA Request Auto Approve STR.....	54
Configuring PTA Request Auto Reject STR.....	54
Configuring PTA Request Auto Approve ETR.....	55
Configuring PTA Request Auto Reject ETR.....	56
Configuring Account Approval Confirmation Text .....	56
Configuring Pre-Trade Approval Confirmation Text .....	57
Configuring Attestation Confirmation Text .....	57
Configuring Security Product Type for PTA .....	58
Working with AA/PTA/AT Action Settings .....	59
Modifying AA/PTA/AT Status Descriptions.....	59
Configuring Standard Comment Data.....	59
Configuring Standard Comments to AA/PTA/AT Actions Data .....	59
Configuring E-mail Notifications by AA/PTA/AT Actions Data.....	60
Loading AA Data through Excel Upload .....	61
Steps for Excel Upload .....	61
Loading PTA Request Data through Excel Upload .....	62
Assign Employee Users to Personal Trading Approval Attestation Questionnaire .....	63
.....	63
<b>Index.....</b>	<b>65</b>





# List of Figures

Figure 1. Manage Common Parameter Screen .....	3
Figure 2. Configuring Base Time Zone .....	3
Figure 3. Financials Tab—Default Currency Format .....	4
Figure 4. Financials Tab—with Modified Currency Format.....	4
Figure 5. Configuring XML Export .....	10
Figure 6. Sample SQL Script for Loading KDD_STATUS_ROLE .....	16
Figure 7. Shared Folder .....	38
Figure 8. AML_Scattered_Plot Edit .....	39
Figure 9. Answers Page - Criteria .....	39
Figure 10. Chart View Properties .....	40
Figure 11. Conditional Formatting.....	40
Figure 12. Add Conditional Format.....	41
Figure 13. Create/Edit Filter Page .....	41
Figure 14. Format Chart Data - Type and Color Column.....	42
Figure 15. Color Selector Toolbox.....	42



## List of Tables

Table 1. Conventions Used in this Guide.....	xv
Table 2. Configuring Notification Attributes.....	6
Table 3. Configuring E-mail Attributes.....	7
Table 4. Configuring XML Export Attributes.....	11
Table 5. Configuring Display of Value in By Field Name/ID Attributes.....	11
Table 6. KDD_QUEUE_MASTER table.....	13
Table 7. KDD_QUEUE_ROLE_MAP table.....	13
Table 8. System Account Passwords.....	14
Table 9. KDD_STATUS_ROLE Table Attributes.....	16
Table 10. KDD_STATUS_ROLE.....	16
Table 11. Configuring Trusted pair Nearing Expiration Date.....	19
Table 12. Configuring New Alert Score Attributes.....	19
Table 13. Configuring Organization Relationships for Trade Blotter Attributes.....	22
Table 14. Configuring Default Alert Owner.....	26
Table 15. Configuring Administration Tools.....	27
Table 16. Configuring Application Server.....	28
Table 17. Prepackaged Color Coding.....	43
Table 18. Configuring AA Default Owner Attributes.....	46
Table 19. Configuring PTA Default Owner Attributes.....	47
Table 20. Configuring AT Default Owner Attributes.....	47
Table 21. Configuring AA/PTA Default Access Right Attributes.....	48
Table 22. Configuring AA/PTA Four Eyes Approval Attributes.....	49
Table 23. Configuring AA/PTA/AT E-mail Notification Attributes.....	50
Table 24. AA/PTA/AT E-mail Notification Message Tokens.....	51
Table 25. Configuring Attestation Reporting Attributes.....	53
Table 26. Configuring PTA Holding Period Attributes.....	54
Table 27. Configuring PTA Request Auto Approve STR.....	54
Table 28. Configuring PTA Request Auto Reject STR.....	55
Table 29. Configuring PTA Request Auto Approve ETR.....	55
Table 30. Configuring PTA Request Auto Reject ETR.....	56
Table 31. Configuring Account Approval Confirmation Text.....	56
Table 32. Configuring Pre-Trade Approval Confirmation Text.....	57
Table 33. Configuring Attestation Confirmation Text.....	58
Table 34. Configuring Product Type in Reference Table Detail Table.....	58
Table 35. E-mail Notification Tokens for AA/PTA/AT.....	60
Table 36. Account Approval Excel Upload.....	62
Table 37. Pre-Trade Approval Excel Upload.....	62
Table 38. Personal Trading Approval Attestation Questionnaire Employee Assignment.....	63



---

# About this Guide

This guide explains the structure behind the Oracle Financial Services Behavior Detection Framework 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, include the following:

- **Installers:** Installs and configures the Oracle Financial Services Behavior Detection Platform 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 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 instructions for configuring the parameters specific to administration tools.
- *Chapter 4, Actions Configuration*, provides instructions for configuring the Action page of the UI.
- *Chapter 5, Web Application Configuration*, provides instructions for configuring the functional settings of the Web Application for the UI post installation.
- *Chapter 6, 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*
- *Alert Management User Guide**KYC Risk Assessment Guide*
- *KYC Administration Guide*

These documents can be found at the following link:

[http://docs.oracle.com/cd/E60570\\_01/homepage.htm](http://docs.oracle.com/cd/E60570_01/homepage.htm)

To learn more about Oracle Financial Services and our complete product line, refer to our Web site [www.oracle.com/financialservices](http://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 . . .
<i>Italics</i>	<ul style="list-style-type: none"> <li>● Names of books, chapters, and sections as references</li> <li>● Emphasis</li> </ul>
<b>Bold</b>	<ul style="list-style-type: none"> <li>● Object of an action (menu names, field names, options, button names) in a step-by-step procedure</li> <li>● Commands typed at a prompt</li> <li>● User input</li> </ul>
Monospace	<ul style="list-style-type: none"> <li>● Directories and subdirectories</li> <li>● File names and extensions</li> <li>● Process names</li> <li>● Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text</li> </ul>
<Variable>	<ul style="list-style-type: none"> <li>● Substitute input value</li> </ul>





This chapter provides instructions for configuring parameters that are common for alert 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 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 Views](#)
- [Managing Additional Configurations](#)

## ***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. 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).

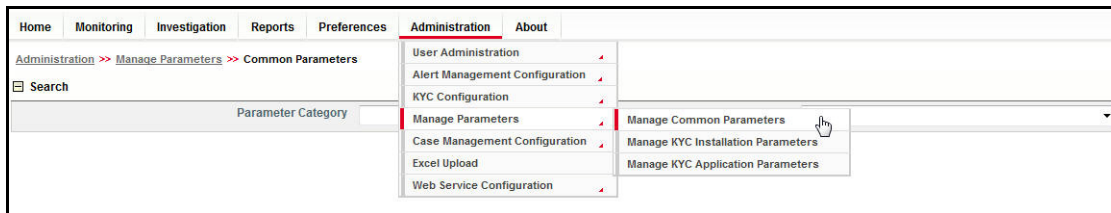


Figure 1. Manage Common Parameter Screen

To modify the base time zone, follow these steps:

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

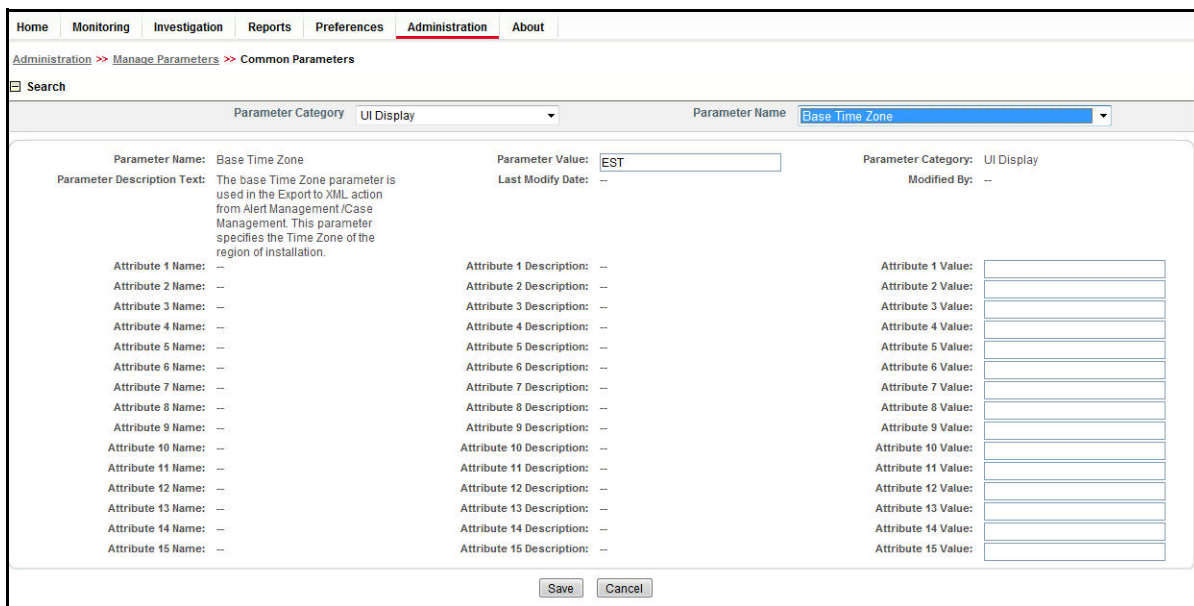


Figure 2. Configuring Base Time Zone

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.

Details	Account	Household	Customer	Investment Advisor	Employee	External Entity	Involved Party	Transactions	Financials
<b>Current Loss and Recovery Summary</b> Edit Remove History									
Total Potential Loss Amount:	USD	6,546,546.00	Primary GL Account:	456789	Charge Off Date:	09/30/2013			
Total Averted Loss Amount:	USD	6,565.00	Primary Cost Center:	FI006A	Last Updated Date:	09/26/2013			
Total Loss Recovery Amount:	USD	456,748.00	Offset Account:	23879	Last Updated By:	SUPERVISOR			
Total/Net Loss Amount:	USD	6,083,233.00	Offset Cost Center:	FI006A					
<b>Potential Loss (1)</b> Expand All Add Edit Remove Excel History									
Date	Amount	GL Account	Cost Center	Loss Payee	Entered By	Entered Date	Description		
09/24/2013	USD 6,546,546.00	156789	FI006A	--	SUPERVISOR	09/26/2013	--		

Figure 3. Financials Tab—Default Currency Format

To modify the default currency code, follow these steps:

1. Open the Manage Common Parameters screen.
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.

Details	Account	Household	Customer	Investment Advisor	Employee	External Entity	Involved Party	Transactions	Financials
<b>Current Loss and Recovery Summary</b> Edit Remove History									
Total Potential Loss Amount:	EUR	6,546,546.00	Primary GL Account:	456789	Charge Off Date:	09/30/2013			
Total Averted Loss Amount:	EUR	6,565.00	Primary Cost Center:	FI006A	Last Updated Date:	09/26/2013			
Total Loss Recovery Amount:	EUR	456,748.00	Offset Account:	23879	Last Updated By:	SUPERVISOR			
Total/Net Loss Amount:	EUR	6,083,233.00	Offset Cost Center:	FI006A					
<b>Potential Loss (1)</b> Expand All Add Edit Remove Excel History									
Date	Amount	GL Account	Cost Center	Loss Payee	Entered By	Entered Date	Description		
09/24/2013	EUR 6,546,546.00	156789	FI006A	--	SUPERVISOR	09/26/2013	--		

Figure 4. Financials Tab—with Modified Currency Format

To modify the default currency code, from the back end, 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 the default currency code that you want to modify, that is similar to the following:  
`<I18N lang="en" country="US" dateFormat="MM/dd/yyyy" baseTimeZone="EST" defaultCurrency="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 `<OFSBD 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 Actions

Alerts 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 Alert Management implementation. If you want to change the time period for this lock, then follow these steps:

1. Open the Manage Common Parameters screen.
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 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.
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 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.
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. <b>Note:</b> 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. <b>Note:</b> The attribute values 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.
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.
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 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 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.
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.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Export XML** from the Parameter Name drop-down list.

The screenshot shows the 'Manage Common Parameters' interface. The breadcrumb trail is 'Administration >> Manage Parameters >> Common Parameters'. The 'Parameter Category' is set to 'Used For Design' and the 'Parameter Name' is 'Export XML'. The parameter value is 'Y'. The parameter description is: 'This parameter specifies attributes related to Alert or Case Export to XML actions. The parameter should be set to Y.' The parameter is modified by 'Used For Design'.

Attribute Name	Attribute Description	Attribute Value
Attribute 1 Name: CASE_EXPORT_DIR	Attribute 1 Description: This attribute specifies the location where the exported XML files will be saved.	Attribute 1 Value: /WEB-INF/classes/Reports
Attribute 2 Name: RELEASE_VERSION	Attribute 2 Description: This attribute specifies the Release Version of Mantas which will be included as part of the XML header information.	Attribute 2 Value: 6.2
Attribute 3 Name: COPYRIGHT_INFO	Attribute 3 Description: This attribute specifies the Copyright information of Mantas which will be included as part of the XML header information.	Attribute 3 Value: Copyright 2013 Oracle Financial S
Attribute 4 Name: ALERT_EXPORT_DIR	Attribute 4 Description: This parameter specifies attributes related to Alert Export to XML actions. The parameter should be set to Y.	Attribute 4 Value: /WEB-INF/classes/Reports
Attribute 5 Name: --	Attribute 5 Description: --	Attribute 5 Value: --
Attribute 6 Name: --	Attribute 6 Description: --	Attribute 6 Value: --
Attribute 7 Name: --	Attribute 7 Description: --	Attribute 7 Value: --
Attribute 8 Name: --	Attribute 8 Description: --	Attribute 8 Value: --
Attribute 9 Name: --	Attribute 9 Description: --	Attribute 9 Value: --
Attribute 10 Name: --	Attribute 10 Description: --	Attribute 10 Value: --
Attribute 11 Name: --	Attribute 11 Description: --	Attribute 11 Value: --
Attribute 12 Name: --	Attribute 12 Description: --	Attribute 12 Value: --
Attribute 13 Name: --	Attribute 13 Description: --	Attribute 13 Value: --
Attribute 14 Name: --	Attribute 14 Description: --	Attribute 14 Value: --
Attribute 15 Name: --	Attribute 15 Description: --	Attribute 15 Value: --

Buttons: Save, Cancel

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. Navigate to **Applications** and click **Manage Configuration**.
2. Open the Manage Common Parameters screen.
3. Select **UI Display** from the Parameter Category drop-down list.
4. Select **Display of Value in By Field Name/ID** from the Parameter Name drop-down list.
5. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
6. Click **OK**. A confirmation dialog box appears with the message: *Update Operation Successful*.
7. 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.
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 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 6. 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	<b>AL</b> : if the view is related to Alert <b>CA</b> : 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 7. 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:** In case 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.

## ***Managing Additional Configurations***

The section describes the additional configurations that need to be carried out by the system administrator.

This section covers the following topics:

- Changing Passwords for System Accounts
- Configuring File Type Extensions
- Configuring File Size
- Configuring Status To User Role Table
- Mapping Status to Role in the Database through Scripts

### **Changing Passwords for System Accounts**

Throughout the OFSBD application there are several system accounts that may require changing the password for security purposes.

The following table summarizes the different system account passwords used by OFSBD, the subsystems that use those passwords, and instructions on how to change the passwords.

**Table 8. System Account Passwords (Continued)**

<b>System Account</b>	<b>Subsystem</b>	<b>Instructions</b>
Data Ingest User (INGEST_USER)	Data Ingestion	<ol style="list-style-type: none"><li>1. Change the password in the database server.</li><li>2. Use the Password Manager Utility to change the password in OFSBD to the new password.</li></ol>
Algorithm User (KDD_ALG)	Behavior Detection Services	<ol style="list-style-type: none"><li>1. Change the password in the database server.</li><li>2. Use the Password Manager Utility to change the password in OFSBD to the new password.</li></ol>
Data Miner User (KDD_MNR)	Alert and Case Management Data Ingestion	<ol style="list-style-type: none"><li>1. Change the password in the database server.</li><li>2. Use the Password Manager Utility to change the password in OFSBD to the new password.</li></ol>
Web Application User (KDD_WEB)	Alert and Case Management Services	<ol style="list-style-type: none"><li>1. Change the password in the database server.</li><li>2. Use the Password Manager Utility to change the password in OFSBD to the new password.</li></ol>

System Account	Subsystem	Instructions
Behavior Detection Framework	BD	<ol style="list-style-type: none"> <li>1. Execute <code>&lt;OFSBD Installed Directory&gt;/BD/scripts/changePasswords.sh</code> to generate an encrypted version of the password. where?</li> <li>2. Find the <code>&lt;OFSBD Installed Directory&gt;/BD/config/custom/BD.xml</code> with the encrypted password. how and where</li> </ol> <p>For more information, see the <a href="#">Installation Guide</a>. <b>Note:</b>OFSBD does not use Password Management utility.</p>
Reports User (KDD_REPORT)	OBIEE Reports	<p>Open the <code>&lt;ORACLEBI_HOME&gt;/server/Repository</code> and expand the Physical Layer. Open the Connection Pool and change the Password parameter to set a new value of the <code>KDD_REPORT</code> schema password. <b>Note:</b> OBIEE is an optional application.</p>

## Configuring File Type Extensions

The list of file type extensions that are allowed to be attached while performing document attachment action should be configured as comma separated values in the CONFIGURATION table of the OFSSAAI configuration schema in its PARAMVALUE column where PARAMNAME is DOCUMENT\_ALLOWED\_EXTENSION.

## 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 & Attach button, follow these steps:

Configure the size that is allowed to be attached through the document attachment action in the CONFIGURATION table of the OFSSAAI configuration schema. You can configure this in the PARAMVALUE column where the PARAMNAME is DOCUMENT\_MAX\_SIZE.

## Configuring Status To User Role Table

Within Watch List Management, each watch list and watch list entry (referred to as a *Watch List Member* on the Watch List Management UI) is assigned a status. In addition to the rules defined earlier for accessing Watch List Management, OFSFCCM uses this status to limit user access to watch lists and watch list entries within the Watch List Management. For example, a WLM Supervisor user role can view *Active* watch lists and watch list entries only if the user role WLM Supervisor is mapped to status *Active*. These mappings reside in the Status To User Role table and are applicable only to the Watch List Management. Each mapping of status to user role applies to both watch lists and watch list entries.

## Mapping Status to Role in the Database through Scripts

You can create a Status to User Role mapping in the database.

To map status to user role in database, follow these steps:

1. Add the appropriate record to the KDD\_STATUS\_ROLE database table as mentioned in the following table.

**Table 9. KDD\_STATUS\_ROLE Table Attributes**

Business Field	Column Name	Date Type	Definition	Null
Status Code	STATUS_CD	CHAR(3)	Status that can be accessed by the user role on this record.	Yes
User Role	USER_ROLE_CD	CHAR(50)	User role that is being assigned access to this status.	Yes

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

```
insert into kdd_status_role (status_cd,user_role_cd) values ('ACT','WLSUPVISR')  
insert into kdd_status_role (status_cd,user_role_cd) values ('REJ','WLSUPVISR')
```

**Figure 6. Sample SQL Script for Loading KDD\_STATUS\_ROLE**

**Note:** The KDD\_STATUS\_ROLE table is pre-populated after system initialization with the following records:

**Table 10. KDD\_STATUS\_ROLE**

STATUS_CD	USER_ROLE_CD
ACT	AMEXAUDITR
ACT	AMEXECUTIVE
ACT	AMINAUDITR
ACT	WLSUPVISR
DAC	WLSUPVISR



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

- [Enabling and Disabling Alert Management](#)
- [Configuring a Visual Cue](#)
- [Configuring New Alert Score](#)
- [Configuring Alert Inheritance](#)
- [Configuring Four Eyes Approval](#)
- [Configuring Highlights](#)
- [Configuring Alert Highlight Status](#)
- [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](#)
- [Managing Security Restrictions](#)
- [Managing Controlling Customer](#)

## ***Enabling and Disabling Alert Management***

This parameter allows the system to identify whether Alert Management Actions and Fields are to be displayed based on the deployment installation. The values to be provided for this parameter are Yes (Y) or No (N).

By default, the parameter is set to Y.

To modify this parameter, follow these steps:

1. Navigate to the Alerts Home page, for more information on how to navigate to the Alerts Home page, see Alert Management User Guide.
2. Hover over **Administration** Menu and select the **Manage Parameters**.
3. Click **Common Parameters**.
4. Select **Deployment Based** in the Parameter category.
5. Select **Alert Management** from the Parameter Name drop-down list.
6. Edit the parameter value.

7. Click **Save**. The following confirmation message is displayed: *Would you like to Save the changes?*
8. Click **OK**. The following confirmation message is displayed: *Update operation successful.*

## **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 11. 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 12 describes the attributes which must be configured for the Notification parameter.

**Table 12. 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	<ul style="list-style-type: none"> <li>● Specifies the default alert score which is set for a newly created alert.</li> <li>● DEFAULT_SC value is to be set in between the MIN_SC and MAX_SC value.</li> </ul>

## 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 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 13 describes the attributes which should be configured for the configuring Organization Relationship option.

**Table 13. 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_trnlm
(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_trnlm
```

```
(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 Infodomain>', '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 Infodomain>', '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 is used only in the Manage Suppression Rules UI. It defines values to be displayed in the **Extend Suppression By** drop-down list. This control allows a user to extend an already defined suppression rule by a set period of time. Pre-packaged options include to extend by 1 month, 3 months, 6 months or 12 months. Update this parameter to modify these options or create new ones. Please note, these durations are only used to impact the extension of an already specified suppression rule.

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.con-  
trol_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 14. Configuring Default Alert Owner**

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

## Managing 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.

## Managing 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 Guide*, 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.

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

**Table 15. 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 16 describes the attributes to be configured for setting the application server.

**Table 16. 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.

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](#)
- [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 30, for more information.
2. Define standard comments that is available in the workflow. Refer to section *Configuring Standard Comment Data*, on page 31, 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 an 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_CMNT (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')
```

## **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.



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 Guide*, 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>
```



If your site has the Oracle Business Intelligence Enterprise Edition (OBIEE 11g) application installed, as an OFSBD 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

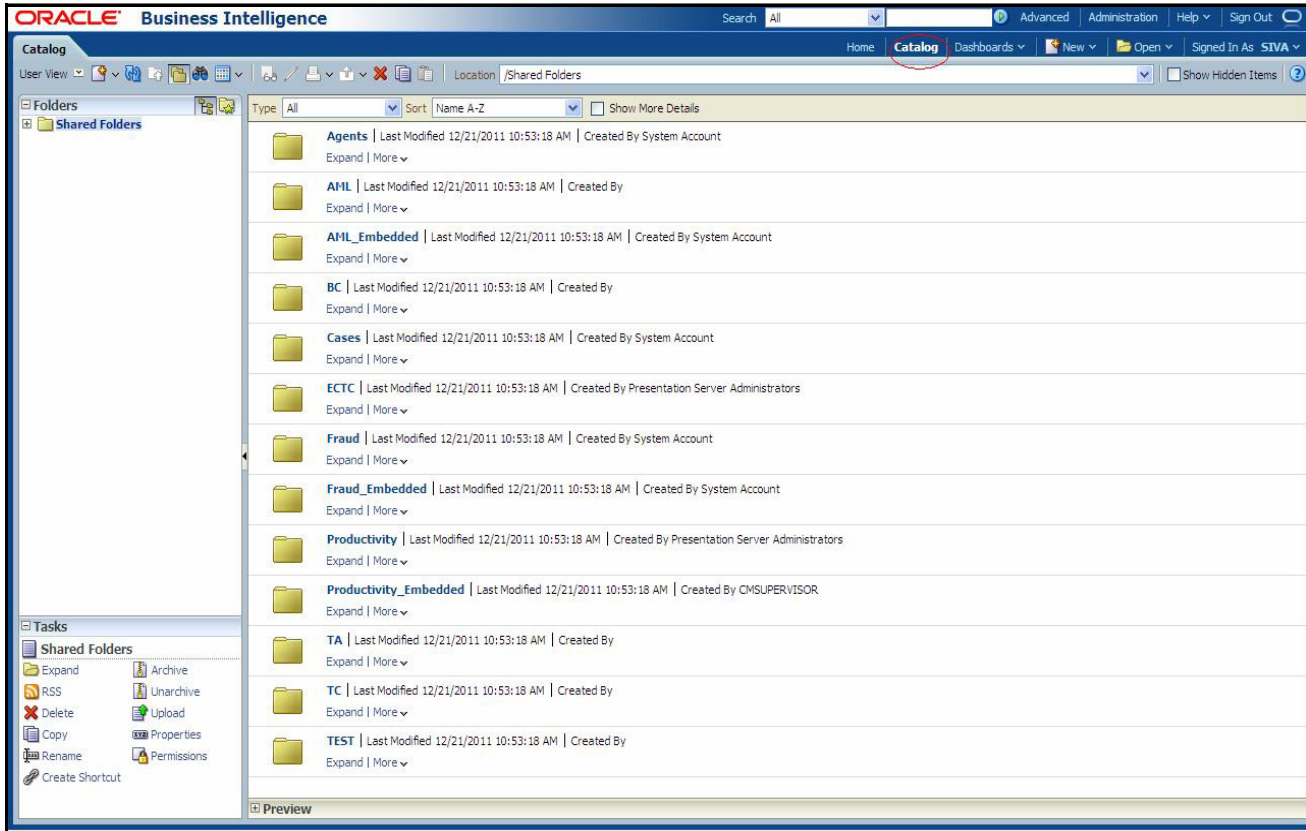
## ***Changing the Color Code of the Scatter Reports***

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 OBIEE Analytics URL, click the **Catalog** link (Figure 7).



**Figure 7. Shared Folder**

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

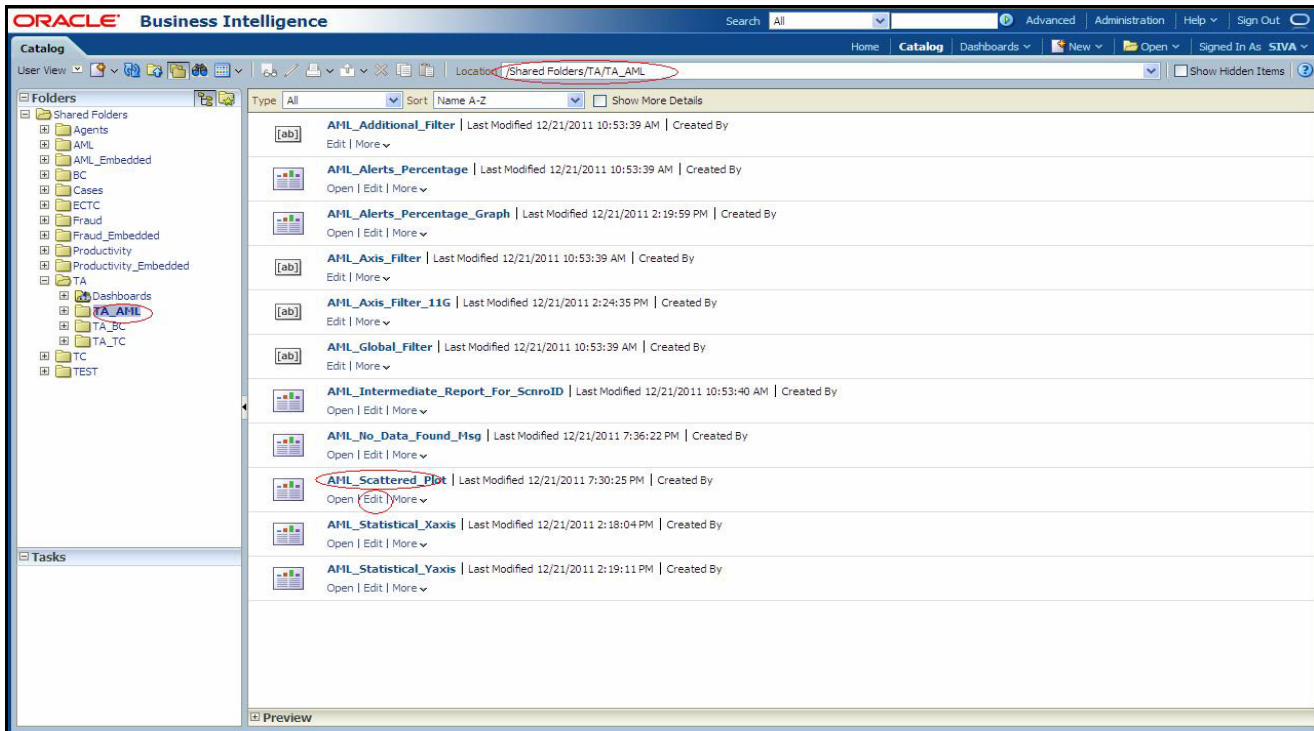


Figure 8. AML\_Scattered\_Plot Edit

3. Click **Edit**.
4. Click **Graph** view and select **Edit** view(Figure 9).

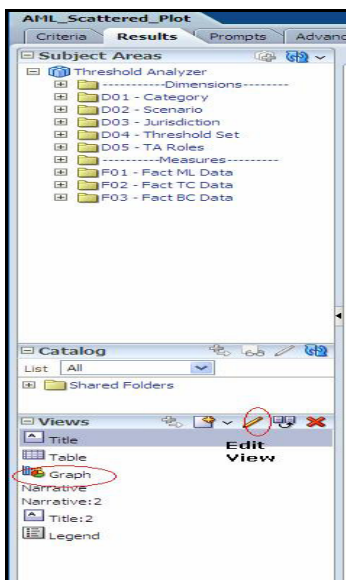


Figure 9. Answers Page - Criteria

5. Click Chart View properties ->Style ->Style and Conditional Formatting (Figure 10).

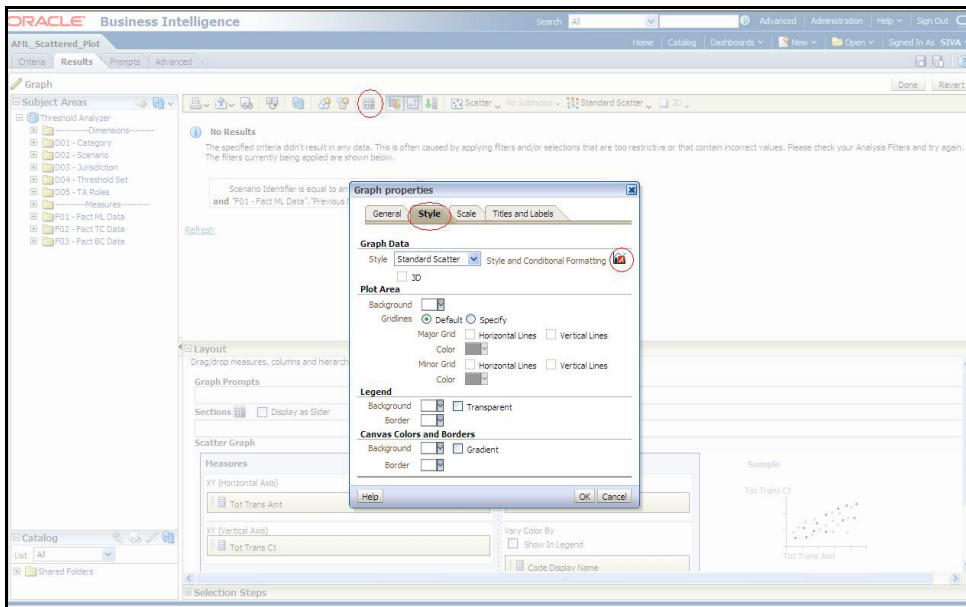


Figure 10. Chart View Properties

6. Select **Conditional Formatting**. You can see the color codes of existing code display names. (Figure 11).

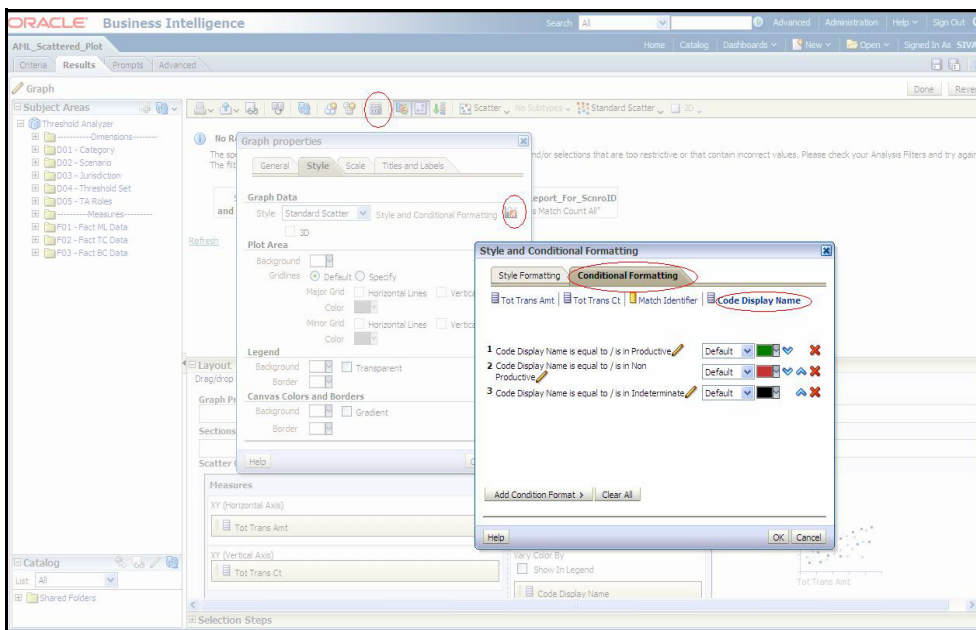


Figure 11. Conditional Formatting

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



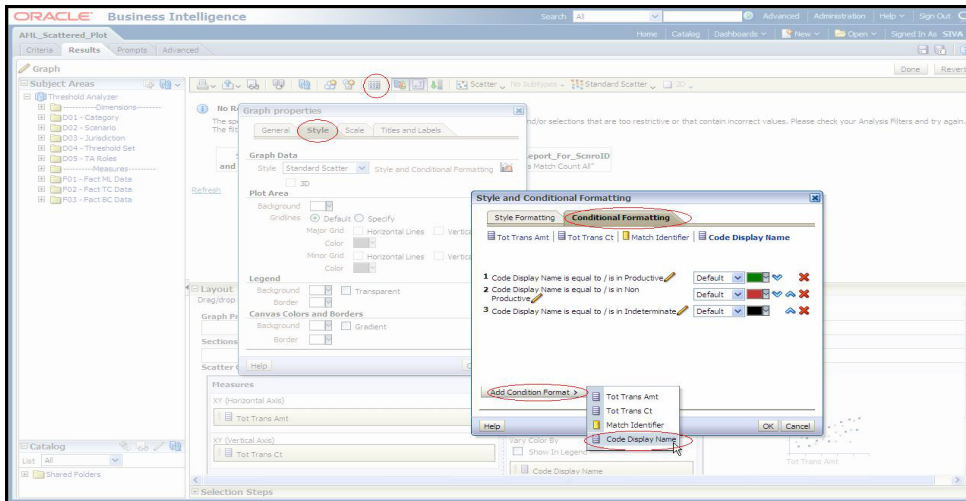


Figure 12. Add Conditional Format

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 13).

**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'.

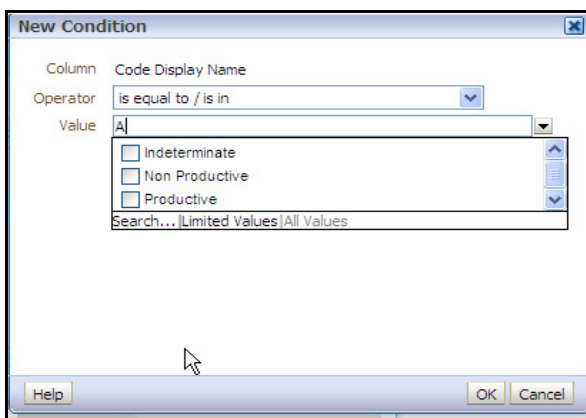


Figure 13. Create/Edit Filter Page

10. On selecting the choices, a new window displays (Figure 14). Under the **Type** drop-down list, select the **Round** option for each Quality Code description.

## Changing the Color Code of the Scatter Reports Chapter 6—OBIEE Report Configuration

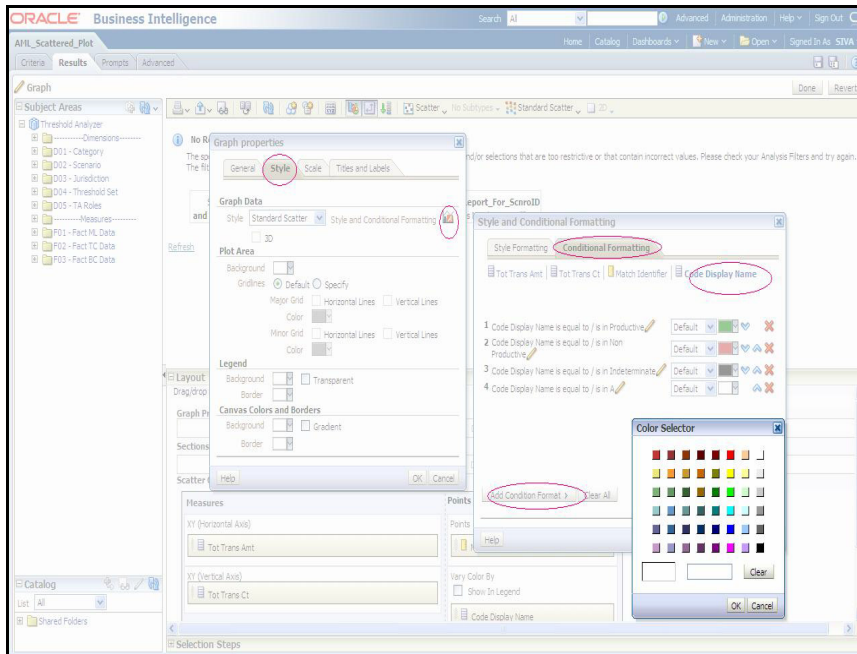


Figure 14. Format Chart Data - Type and Color Column

11. Click a blank box under the **Color** option of the Format Chart Data.  
A Color Selector window displays (Figure 15).
12. Select a color for each Quality Code description and click **OK**.

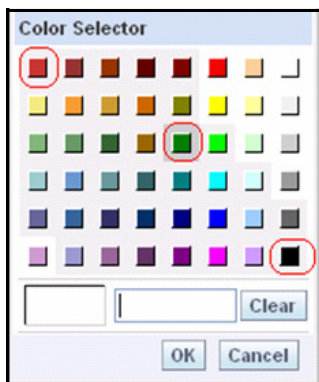


Figure 15. Color Selector Toolbox

13. Click **Save Request**.

Table 17 lists the prepackaged color coding schemes.

**Table 17. 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 depends 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 OBIEE Analytics URL, Click **Catalog** link (Figure 7).
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 37.
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.

# *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 18 describes the attributes which need to be configured for Configuring AA Default Owner.

**Table 18. 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 <code>TITL_NM</code> 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 19 describes the attributes which need to be configured for Configuring PTA Default Owner.

**Table 19. 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 <code>TITL_NM</code> 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 20 describes the attributes which need to be configured for Configuring AT Default Owner.

**Table 20. 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 <code>TITL_NM</code> 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 21 describes the attributes which need to be configured for Configuring AA/PTA/AT Default Access Right.

**Table 21. 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 22 describes the attributes which need to be configured for Configuring AA/PTA Four Eyes Approval.

**Table 22. 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 23 describes the attributes which need to be configured for configuring AA/PTA/AT e-mail notification.

**Table 23. Configuring AA/PTA/AT E-mail Notification Attributes**

<b>Attribute</b>	<b>Description</b>	<b>Attribute Sample Value</b>
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 23. 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 24. AA/PTA/AT E-mail Notification Message Tokens**

<b>E-mail Subject Token</b>	<b>Description</b>	<b>Workflow</b>
\$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 25 describes the attributes which need to be configured for Configuring AA Account Attestation Reporting Period.

**Table 25. Configuring Attestation Reporting Attributes**

<b>Attribute</b>	<b>Description</b>	<b>Attribute Sample Value</b>
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 26 describes the attributes which need to be configured for configuring PTA Holding Period Parameter.

**Table 26. Configuring PTA Holding Period Attributes**

<b>Attribute</b>	<b>Description</b>	<b>Attribute Sample Value</b>
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 27. Configuring PTA Request Auto Approve STR**

<b>Attribute</b>	<b>Description</b>	<b>Attribute Sample Value</b>
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 <i>Oracle Financial Services Behavior Detection Platform Data Interface Specification Guide</i> .	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 28. 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 <i>Oracle Financial Services Behavior Detection Platform Data Interface Specification Guide</i> .	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 29. 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 <i>Oracle Financial Services Behavior Detection Platform Data Interface Specification Guide</i> .	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 30. 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 <i>Oracle Financial Services Behavior Detection Platform Data Interface Specification Guide</i> .	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 31 describes the attributes which need to be configured for Configuring AA/PTA Default Access Right.

**Table 31. Configuring Account Approval Confirmation Text**

Attribute	Description	Attribute Sample Value
-----------	-------------	------------------------



**Table 31. 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 32 describes the attributes which need to be configured for Configuring AA/PTA Default Access Right.

**Table 32. Configuring Pre-Trade Approval Confirmation Text**

<b>Attribute</b>	<b>Description</b>	<b>Attribute Sample Value</b>
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 33 describes the attributes which need to be configured for Configuring AA/PTA Default Access Right.

**Table 33. 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 34. 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 35. 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 35. 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/AMCMLookupFiles.
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 36. Account Approval Excel Upload**

Database Table	Excel Template	Description
External Investment Account Type	EXTRL_NVSM_T_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_NVSM_T_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 37. 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.

## Assign Employee Users to Personal Trading Approval Attestation Questionnaire

Within the Attestation functionality of the Personal Trading Approval application, various questionnaires can be created by the Oracle client. The attributes of an employee, such as Job Title, determines what type of questionnaire an employee views and must attest to. Due to the high number of employees within the Oracle client that must be assigned to a specific questionnaire, the following script captures the employees and assigns each employee to the appropriate questionnaire depending on the employee attributes defined for each questionnaire:

**Table 38. Personal Trading Approval Attestation Questionnaire Employee Assignment**

Task	Script	Database Procedure / Description
Questionnaire Employee Assignment	<pre>run_pta_emp_quest_map .sh</pre>	<p>P_PTA_BA_EMP_QUEST_MAP</p> <p>Once a questionnaire is created, assignment logic can be defined to create user groups of employees. Assignment logic is defined for each questionnaire using the functionality of the generic questionnaire module. The results of the assignment logic ARE used in a scheduled batch program to populate the Employee to Attestation Questionnaire Group table. The system will check this table to determine which questionnaire to display for an employee.</p>





# Index

## A

administrator, Oracle Financial Services, xiii  
alert  
    actions, 29  
analytical reports, 37  
    Scatter reports, 37  
    Statistical reports, 43  
audience of guide, xiii

## C

client logo, 2  
client.gif, 2  
configuration, general, 1  
conventions  
    bold, xv  
    italics, xv  
    monospace, xv  
    variable, xv  
conventions, notational, xv  
currency format, modifying, 4

## D

date format  
    modifying, 3  
documentation, related, xv

## G

general configuration, 1  
    modifying default currency format, 4  
    modifying default date format, 3  
    modifying the base time zone, 3  
    modifying the client logo, 2

## I

installer, Oracle Financial Services, xiii

## K

KDD\_ACTVY\_TYPE\_REVIEW\_STATUS table, 32

## L

logo, client, 2

## O

Oracle Financial Services  
    administrator, xiii  
    installer, xiii  
    Platform documentation, xv  
    UI configuration, 1

## S

Scatter reports  
    changing color code, 37  
session timeout, 35  
settings  
    session timeout, 35  
Statistical reports  
    changing color code, 43

## W

Web Application  
    configuration, 35  
    modifying session timeout, 35





