

Administration and Configuration Guide

Oracle Financial Services

Anti-Money Laundering Event Scoring (AMLES)

Release 8.0.5.0.0

January 2018



Administration and Configuration Guide

Oracle Financial Services

Anti-Money Laundering Event Scoring

Release 8.0.5.0.0

January 2018

Part Number: E92600-01

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

Part Number: E92600-01
First Edition (January 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

Contents

About this Guide	3
Who Should Use this Guide	3
How this Guide is Organized	3
Where to Find More Information.....	4
Conventions Used in This Guide.....	4
CHAPTER 1 <i>About Oracle Financial Services Anti-Money Laundering Event Scoring</i>	1
Introduction.....	1
Administration and Configuration Activities	1
Managing User Administration.....	1
Configuring the Application.....	1
CHAPTER 2 <i>Getting Started</i>.....	3
System Requirements	3
Accessing OFSAA Applications	4
Selecting Applications.....	5
Managing OFSAA Application Page.....	6
Applications Tab	6
Object Administration Tab.....	6
System Configuration and Identity Management Tab.....	7
Change Password	8
Copyright Information	8
Troubleshooting Your Display.....	9
Enabling JavaScript.....	9
Enabling Cookies	9
Enabling Temporary Internet Files	9
Enabling File Downloads	10
Setting Printing Options	10
Enabling Pop-up Blocker.....	10
Setting Preferences.....	11
CHAPTER 3 <i>Managing User Administration</i>.....	13
About User Administration	13
Administrator User Privileges.....	13
User Provisioning Process Flow	13
Requirements to Access AMLES Application	14
Managing User Administration	14

Managing Identity and Authorization.....	14
<i>Managing Identity and Authorization Process Flow.....</i>	<i>14</i>
<i>Creating and Authorizing a User.....</i>	<i>15</i>
<i>Load User Configuration Data into CSSMS_ATTRIB_MAST table Using Excel Upload.....</i>	<i>15</i>
<i>Creating or Editing User.....</i>	<i>16</i>
<i>Understanding User Roles in OFS Anti Money Laundering Event Scoring</i>	<i>16</i>
<i>Mapping a User with a User Group.....</i>	<i>16</i>
CHAPTER 4 Configuring the Application.....	19
Starting a Batch Run and Loading Batch Execution Data.....	19
Running Batch Execution	21
CHAPTER 5 Configuring Administration Tools.....	25
Configuring Administration Tools.....	25
Configuring Application Server.....	26
CHAPTER 6 Configuring Web Application	27
Configuring the Session Timeout Setting	27
Configuring the Session Timeout Setting.....	27
Configuring the Session Timeout Setting for Admin Tools.....	27

About this Guide

This guide explains the concepts behind the Oracle Financial Services Anti-Money Laundering Event Scoring (OFS AMLES) application, and provides comprehensive instructions for system administration, daily operations, and maintenance.

This section 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

This *Administration and Configuration Guide* is designed for use by Administrators. The administrator user configures and maintains the system. The Administrator is usually an employee of a specific Oracle customer, who maintains user accounts and roles, configures and executes batch jobs, and so on.

How this Guide is Organized

This *Administration and Configuration Guide*, includes the following chapters:

- [Chapter 1, About Oracle Financial Services Anti-Money Laundering Event Scoring](#), provides a brief overview of the Oracle Financial Services Anti-Money Laundering Event Scoring application architecture, and its components.
- [Chapter 2, Getting Started](#), provides the required day-to-day operations and maintenance of Anti-Money Laundering Event Scoring application users, groups, and organizational units.
- [Chapter 3, Managing User Administration](#), provides instructions to set up and configure the Security Management System (SMS) to support AMLES application, user authentication, and authorization.
- [Chapter 4, Configuring the Application](#), provides the administration processes required to configure the application.
- [Chapter 5, Configuring Administration Tools](#), provides instructions to configure parameters specific to administration tools.
- [Chapter 6, Configuring Web Application](#), provides customization features available in the Web Application UI. This chapter contains information to configure session time out.

Where to Find More Information

For more information about Oracle Financial Services Anti-Money Laundering Event Scoring application, see the following documents in the [Oracle Help Center \(OHC\)](#):

- *Oracle Financial Services Anti-Money Laundering Event Scoring Application Pack Release Note and Readme*
- *Oracle Financial Services Anti-Money Laundering Event Scoring Application Pack Installation Guide*
- *Oracle Financial Services Anti-Money Laundering Event Scoring Application Pack User Guide*

Additionally, you can find specific information for OFSAAI documentation in the [Oracle Help Center \(OHC\)](#):

- *Oracle Financial Services Analytical Applications Infrastructure User Guide*
- *Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration Guide*
- *Oracle Financial Services Analytical Applications Infrastructure Administration Guide*

Conventions Used in This Guide

This table lists the conventions used in this guide.

Table 1. Conventions Used in This Guide

Convention	Description
<i>Italics</i>	<ul style="list-style-type: none">● Names of books, chapters, and sections as references● Emphasis
Bold	<ul style="list-style-type: none">● Object of an action (menu names, field names, options, button names) in a step-by-step procedure● Commands typed at a prompt● User input
Monospace	<ul style="list-style-type: none">● Directories and subdirectories● File names and extensions● Process names● Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text
<Variable>	<ul style="list-style-type: none">● Substitute input value

About Oracle Financial Services Anti-Money Laundering Event Scoring

This chapter provides a brief overview of the Oracle Financial Services Anti-Money Laundering Event Scoring (OFS AMLES) application.

The following sections are covered in this chapter:

- [Introduction](#)
- [Administration and Configuration Activities](#)

Introduction

Oracle Financial Services Anti Money Laundering Event Scoring application provides a mechanism to score and categorize the alerts generated by different AML engines thus reducing the manual effort of investigators. The application uses historical alert transaction to train and validate machine learning models, and apply them to score new alert data and prioritize alerts for investigation.

Administration and Configuration Activities

This section covers the following topics:

- [Managing User Administration](#)
- [Managing User Administration](#)

Managing User Administration

The system administrators provide users access and authorization to the application. For more information, see the section *Managing User Administration* on page 13

Configuring the Application

The batch execution run performs the process of loading data and preparing the system for users. For more information, see the section *Configuring the Application* on page 19.

This chapter provides step-by-step instruction to login to the AMLES application and manage the different features of the Oracle Financial Services Analytical Applications (OFSAA) application page.

The following sections are covered in this chapter:

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

System Requirements

The following applications are required to run the AMLES application:

- Microsoft Internet Explorer (IE) version 9 or later.
Earlier versions and other browsers are not supported and can produce errors, inaccurate data and display failures. For users of IE version 8.0, the browser should be run in compatibility mode.
- Adobe Acrobat Reader version 9.0, or later.
You can download a free copy of the latest version of the Acrobat Reader at www.adobe.com.
- Java should be installed. JDK 1.8 (version 8) or above.
- The screen resolution of the system should be set to 1280 × 1024 or higher for proper display of the user interface (UI).

For more information, see the *OFS Anti-Money Laundering Event Scoring Installation Guide*.

Accessing OFSAA Applications

Access to the Oracle Financial Services Anti-Money Laundering Event Scoring application depends on the Internet or Intranet environment. Oracle Financial Services Anti-Money Laundering Event Scoring is accessed through Microsoft Internet Explorer (IE). Your system administrator provides the intranet address uniform resource locator (URL).

Your system administrator provides you with a User ID and Password. Login to the application through the OFSAA login page. You will be prompted to change your password on your first login. You can change your password whenever required after logging in. For more information, see *Change Password* section.

Note: Based on your firm's configuration, you can login with Single Sign-On (SSO).

To access OFSAA Applications, follow these steps:

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

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

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

The OFSAA login page is displayed.

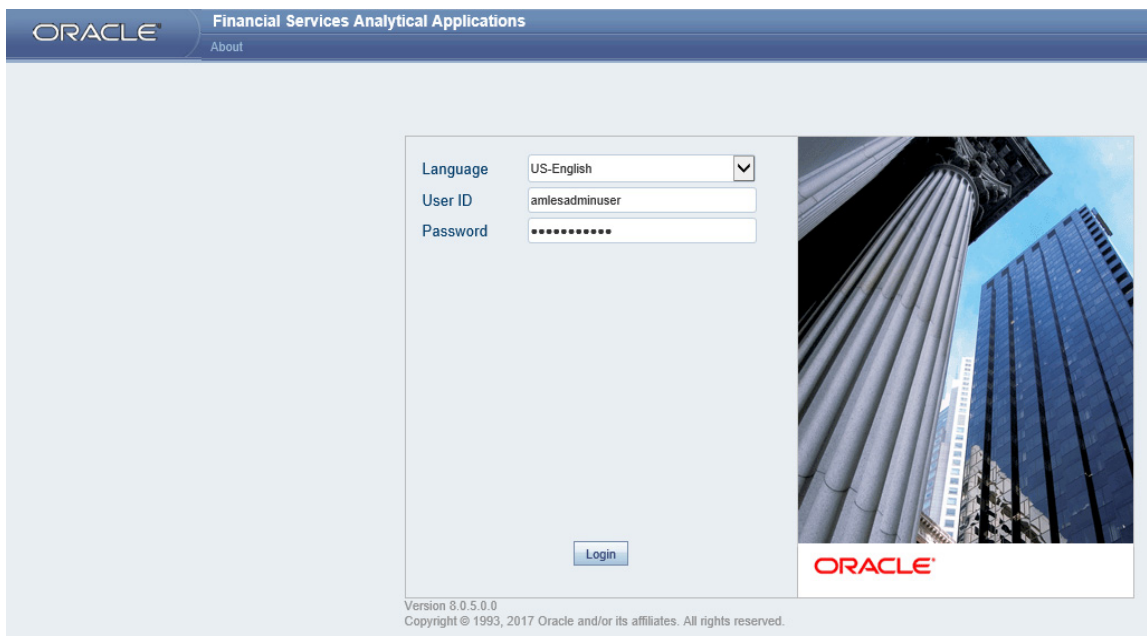


Figure 1. OFSAA Login Page

2. Select the Language from the Language drop-down list.
3. Enter your User ID and Password.
4. Click **Login**. The OFSAA Application page is displayed.

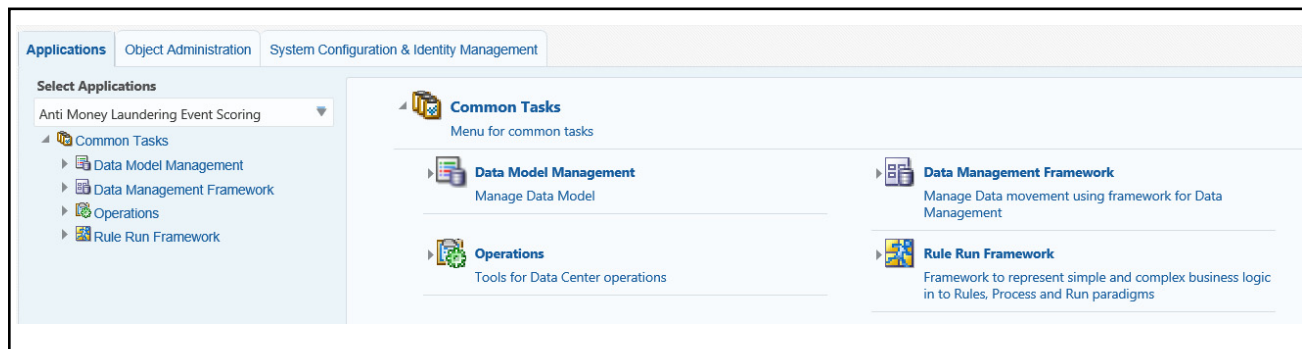


Figure 2. OFSAA Application Page

The OFSAA Application page is a common landing page for all users until a preferred application page is set. For more information about how to set your preferred application page, see [Setting Preferences](#). You can use the OFSAA Application page to access the Oracle Financial Services applications in your environment.

Selecting Applications

This section explains how to access required applications.

The OFSAA Applications page has multiple tabs and each tab has specific links to OFSAA Infrastructure and Application modules. The modules which you can access depend on your user role and the OFSAA Application you select. The relevant tabs and links are displayed.

This page is divided into two panes:

- **Left Pane:** Displays menus and links to modules in a tree format based on the application selected in the Select Applications drop-down list.
- **Right Pane:** Displays menus and links to modules in a navigational panel format based on the selection of the menu in the Left pane. It also provides a brief description of each menu or link.

To access AMLES applications, follow these steps:

1. Navigate to OFSAA Applications page.
2. Select **Anti-Money Laundering Event Scoring**. The Anti-Money Laundering Event Scoring page is displayed.

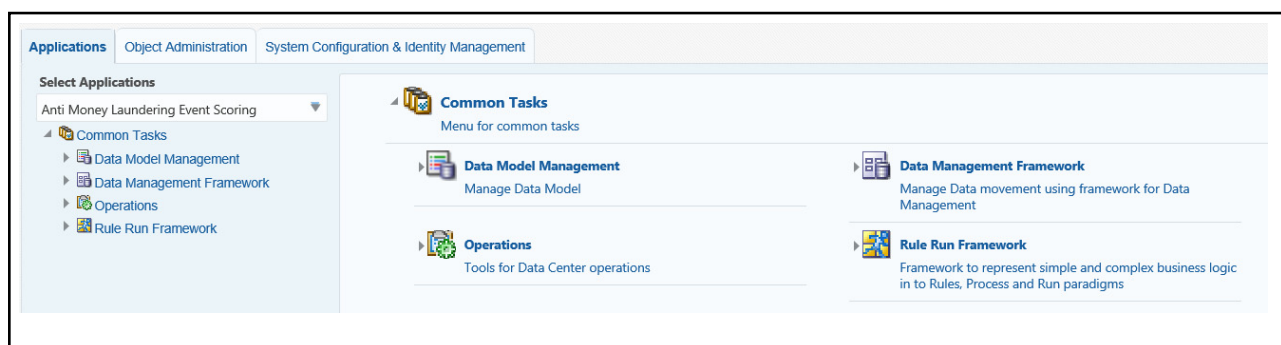


Figure 3. Anti-Money Laundering Event Scoring Page

Managing OFSAA Application Page

This section describes the different panes and tabs in the OFSAA Application page.

The OFSAA Application page has the following tabs:

- [Applications Tab](#)
- [Object Administration Tab](#)
- [System Configuration and Identity Management Tab](#)
- [Change Password](#)
- [Copyright Information](#)

Applications Tab

The Applications tab lists the OFSAA Applications that are installed in the OFSAA setup based on the logged in user and mapped OFSAA Application User Groups.

To access the OFSAA Applications, select the required Application from Select Applications drop-down list. For Anti-Money Laundering Event Scoring, select **Anti-Money Laundering Event Scoring**. Based on your selection, the page refreshes the menus and links across the panes.

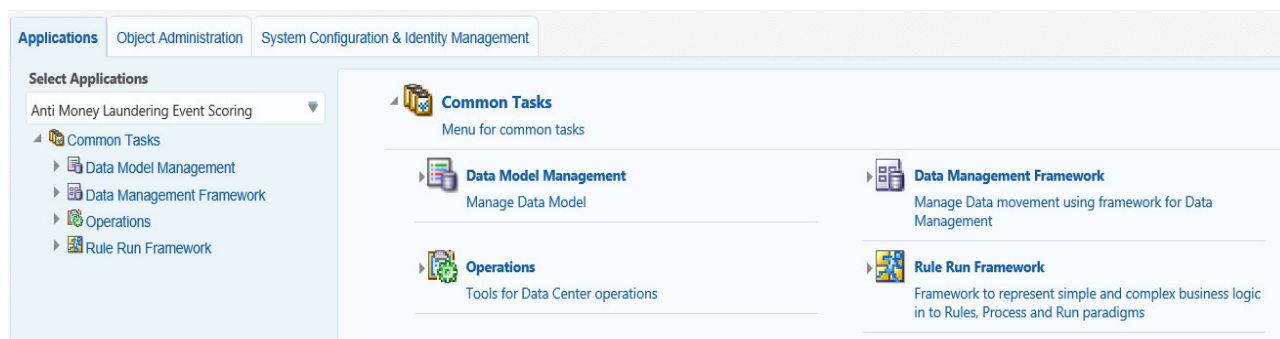


Figure 4. Applications Tab

Object Administration Tab

Object Administration is an integral part of the Infrastructure system and allows system administrators to define the security framework with the capacity to restrict access to the data and metadata in the warehouse, based on a flexible, fine-grained access control mechanism. These activities are mainly done at the initial stage, and then as required. This tab includes information related to the workflow of the Infrastructure Administration process with related procedures to assist, configure, and manage administrative tasks.

The Object Administration tab lists the OFSAA Information Domains created in the OFSAA setup based on the logged in user and mapped OFSAA Application User Groups.

To define or maintain access for an Information Domain, select the required Information Domain from the Select Information Domain drop-down list. Based on your selection, the page refreshes the menus and links across the panes.

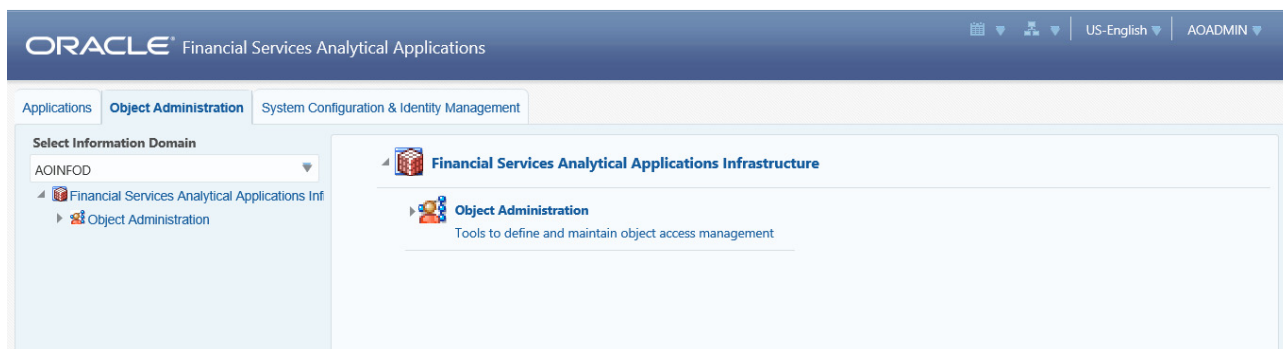


Figure 5. Object Administration Tab

System Configuration and Identity Management Tab

System Configuration and Identity Management is an integral part of the Infrastructure administration process. This tab helps System Administrators to provide security and operational framework required for the Infrastructure.

System Administrators can configure Server, Database, OLAP, and Information Domains, along with other configuration processes such as segment and metadata mapping, segments to securities mapping, and rules setup. The System Configuration is a one-time activity, which helps the System Administrator make the Infrastructure system operational.

The System Configuration and Identity Management tab lists the OFSAA Infrastructure System Configuration and Identity Management modules. These modules work across Applications and Information Domains, so there is no Application or Information Domain drop-down list in this tab.

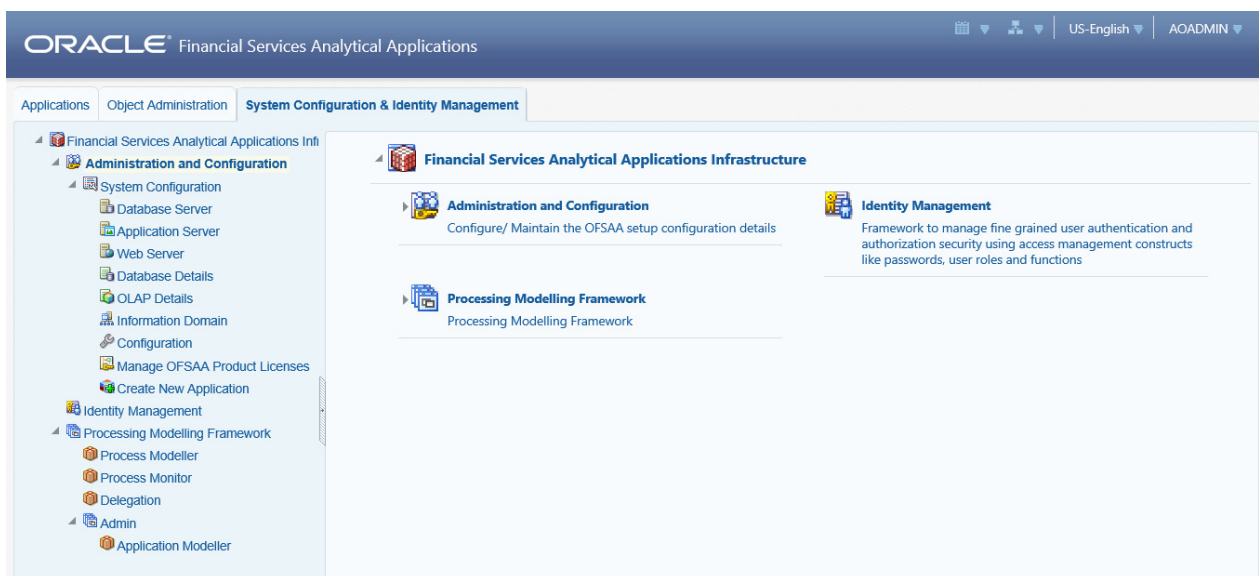


Figure 6. System Configuration and Identity Management Tab

Selecting Identity Management allows System Administrators to manage Users, User Groups, and the functions each User or User Group can access. For more information about managing Users and User Groups, see the *OFSAAI Administration Guide*.

Change Password

For security purpose, you can change the password. This section explains how to change password.

To change the password, follow these steps:

1. Navigate to OFSAA Applications page.

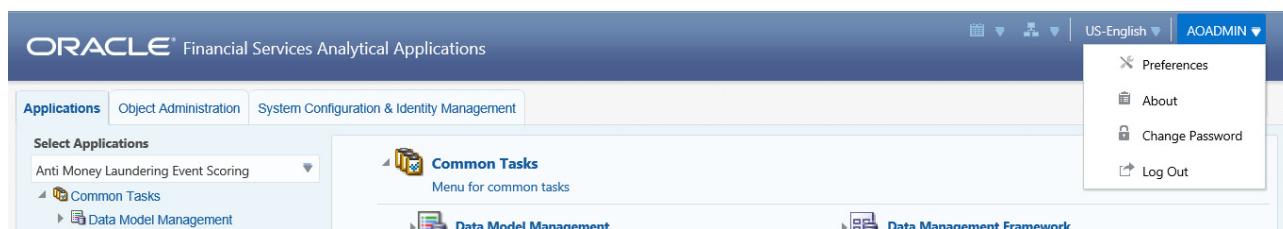


Figure 7. Change Password

2. Click the User drop-down list and select **Change Password**. The Change Password page is displayed.

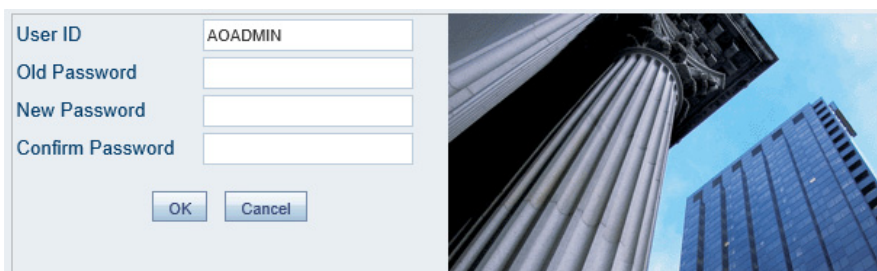


Figure 8. Change Password

3. Enter your old and new password in the respective fields.
4. Click **OK**. Your password is changed successfully. The application navigates back to the Login page where you can login with the new password.

Note: Your password is case-sensitive. If you have problems with the password, verify that the **Caps Lock** key is off. If the problem persists, contact your system administrator.

Copyright Information

To access copyright information, click the User drop-down list and select **About** in OFSAA login page.

The Copyright text displays in a new window.

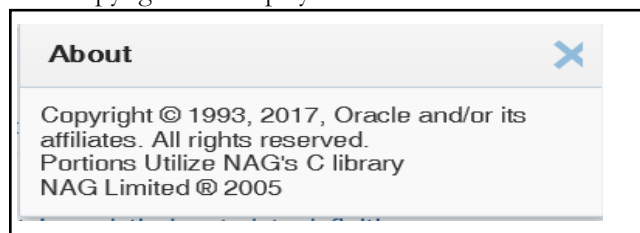


Figure 9. Copyright Information

Troubleshooting Your Display

If you experience problems logging into Oracle Financial Services AMLES or with your display, the browser settings may be incompatible with running OFSAA applications. The following sections provide instructions to set the Web display options for OFSAA applications within Internet Explorer (IE).

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

This section covers following topics:

- [Enabling JavaScript](#)
- [Enabling Cookies](#)
- [Enabling Temporary Internet Files](#)
- [Enabling File Downloads](#)
- [Setting Printing Options](#)
- [Enabling Pop-up Blocker](#)
- [Setting Preferences](#)

Enabling JavaScript

JavaScript must be enabled in the browser. To enable JavaScript, follow these steps:

1. From the Tools menu, click **Internet Options**.

The Internet Options dialog box displays.

2. Click the **Security** tab.
3. Click the **Local Intranet** icon as your Web content zone.
4. Click **Custom Level**.

The Security Setting - Local Intranet Zone dialog box displays.

5. In the Settings list and under the Scripting setting, ensure that Enable is selected for all options.
6. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Enabling Cookies

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

Enabling Temporary Internet Files

Temporary Internet files are pages that you view on the Internet and store in a folder for quick viewing later. You must adjust this setting to always check for new versions of a stored page. To adjust your Temporary Internet File settings, follow these steps:

1. From the Tools menu, click **Internet Options**.

The Internet Options dialog box displays.

2. On the General tab, click **Settings**.
The Website Data Settings dialog box displays.
3. Select the **Every time I visit the webpage** option.
4. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Enabling File Downloads

File downloads must be available. To enable file downloads, follow these steps:

1. From the Tools menu, click **Internet Options**.
The Internet Options dialog box displays.
2. Click the **Security** tab.
3. Click the **Local Intranet** icon as your Web content zone.
4. Click **Custom Level**.
The Security Setting - Local Intranet Zone dialog box displays.
5. Under the Downloads section, ensure that **Enable** is selected for all options.
6. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Setting Printing Options

Printing background colors and images must be enabled. To enable this option, follow these steps:

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

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

Enabling Pop-up Blocker

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

To enable Pop-up Blocker, follow these steps:

1. From the Tools menu, click **Internet Options**.
The Internet Options dialog box displays.
2. Click the **Privacy** tab.
3. In the Pop-up Blocker setting, select the **Turn on Pop-up Blocker** option.

The **Settings** is enabled.

4. Click **Settings** to open the Pop-up Blocker Settings dialog box.
5. In the Pop-up Blocker Settings dialog box, enter the URL of the application in Address of website to allow.
6. Click **Add**.

The URL appears in the Allowed sites list.

7. Click **Close**, then click **Apply** to save the settings.
8. Click **OK** to exit the Internet Options dialog box.

Setting Preferences

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

To access this section, follow these steps:

1. Click **Preferences** from the drop-down list in the top right corner, where the user name is displayed.
The Preferences screen is displayed.

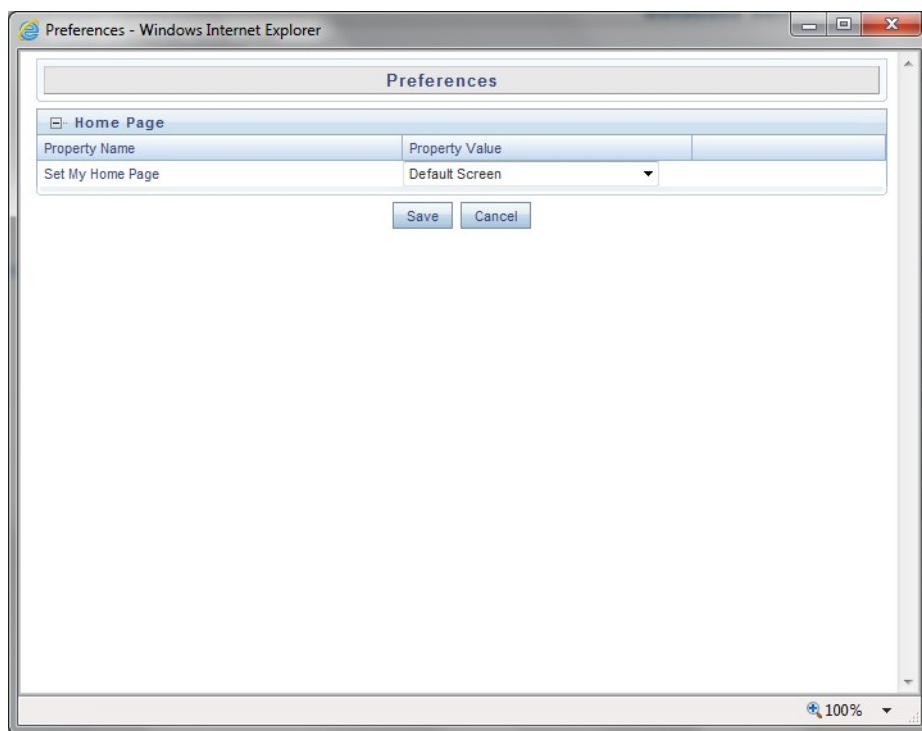


Figure 10. Preference screen.

2. In the Property Value drop-down list, select the application which you want to set as the Home Page.
Note: Whenever new application is installed, the related value for that application is found in the drop-down list.
3. Click **Save** to save your preference.

This chapter provides instructions to set up and configure the Security Management System (SMS) to support AMLES application's user authentication and authorization functions.

The following sections are covered in this chapter:

- [About User Administration](#)
- [Administrator User Privileges](#)
- [User Provisioning Process Flow](#)
- [Managing User Administration](#)

About User Administration

User administration involves creating and managing users and providing access based on their roles. This chapter discusses the following:

- Administrator permissions
- Creating and mapping users and user groups
- Loading and mapping security attributes

Administrator User Privileges

Table 2 lists the access permissions of the AMLES administrator.

Table 2. Access Permissions for Administrators

Privileges	AMLES Administrator
User Security Administration	✓
Excel Upload	✓
Web Service Configuration	✓
Common Web Service	✓
Preferences	✓
User Administration	✓

User Provisioning Process Flow

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

Table 3. User Provisioning Process Flow

Action	Description
Managing User Administration	Create users and map users to User Groups. The Administrator can provide access, monitor, and administer users.

Requirements to Access AMLES Application

A user gains access to the AMLES application based on the authentication of a unique user ID and password.

To access the AMLES application, you must fulfill the following conditions:

Table 4. Requirements

Applications	Conditions
Anti-Money Laundering Event Scoring	<ul style="list-style-type: none"> ● Set of policies that associate functional roles with access to specific system functions ● Access to one or more business domains
Administration Tools	Set of policies that associate the admin functional role with access to specific system functions

Managing User Administration

This section allows you to create, map, and authorize users and define restricted access to the AMLES application.

Managing Identity and Authorization

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

This section covers the following topics:

- [Managing Identity and Authorization Process Flow](#)
- [Creating and Authorizing a User](#)
- OFS Anti Money Laundering Event Scoring application uses four-eyes functionality to provide two levels of maker and checker to create and approve execution runs. The two levels of users are defined as creators and approvers. For example, if your user profile is mapped to a Creator role, you can create an execution run and request for deployment, which has to be approved by a user with Approver role.

Managing Identity and Authorization Process Flow

Figure 11 shows the process flow of identity management and authorization.

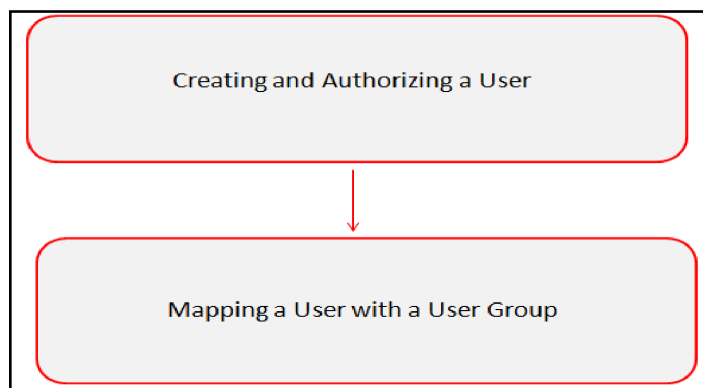


Figure 11. Managing Identity and Authorization Process Flow

Table 5 lists the various actions and associated descriptions of the user administration process flow:

Table 5. Administration Process Flow

Action	Description
Creating and Authorizing a User	Create a user. This involves providing a user name, user designation, and dates between which the user is active in the system.
OFS Anti Money Laundering Event Scoring application uses four-eyes functionality to provide two levels of maker and checker to create and	Map a user to a user group. This enables the user to have certain privileges of the mapped user group.

Creating and Authorizing a User

The SYSADMN and SYSAUTH roles can be provided to users in the AMLES application. User and role associations are established using the Security Management System (SMS) and are stored in the Config Schema. User security attribute associations are defined using Security Attribute Administration.

For more information on creating and authorizing a user, see *Chapter 9*, in *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

Load User Configuration Data into CSSMS_ATTRIB_MAST table Using Excel Upload

To load user configuration data, follow these steps:

1. Navigate to Anti-Money Laundering Event Scoring, go to Common Tasks.
2. Select **Unified Metadata Manager**. Click **Data Entry Forms and Queries**.
3. Click **Upload**. Select **Config Schema Upload**.
4. Select the CSSMS_ATTRIB_MAST table in the **Select the table** drop-down list.
5. In **Select the File to Upload** field, click **Browse**. In **Choose File to Upload** window, specify the path of the data file (Microsoft Excel 2003/2007) which you want to upload. The CSSMS_ATTRIB_MAST.xlsx will be available in the /STAGE/ExcelUpload/TEMPLATE path inside the ftpshare folder.
6. Click **Select the Sheet** button, the Sheet Selector pop-up window is displayed. Select the required sheet from the drop-down list and click OK. If the excel contains multiple sheets, select the sheet from which data is to be uploaded. Else, by default the first sheet data is selected for upload.
7. In the Upload Type options, select one of the following:
 - **Incremental**: In this type of upload, the data in Excel sheet is inserted / appended to the target database object. The upload operation is successful only when all the data in the selected Excel Sheet is uploaded. In case of an error, the uploaded data will be rolled back.
 - **Complete**: In this type of upload, the data present in the selected database object is overwritten with the data selected Excel sheet. In case of an error, data in the selected database object will be reverted back to its original state.
8. Select Upload. If you have selected Complete upload type, you must need confirm to overwrite data in the confirmation dialog.

Creating or Editing User

To create or edit user, follow these steps:

1. Create or Edit the user for which you must map the Security Attributes. For more information on creating and authorizing a user, see *Chapter 9*, in *Oracle Financial Services Analytical Applications Infrastructure User Guide*.
2. After updating the fields, click **Save**.

Figure 12. User Maintenance

Understanding User Roles in OFS Anti Money Laundering Event Scoring

OFS Anti Money Laundering Event Scoring application uses four-eyes functionality to provide two levels of maker and checker to create and approve execution runs. The two levels of users are defined as creators and approvers. For example, if your user profile is mapped to a Creator role, you can create an execution run and request for deployment, which has to be approved by a user with Approver role.

Mapping a User with a User Group

This section explains how to map Users and User Groups. With this, the user will have access to the privileges as per the role. The SYSADMN user maps a user to a user group in the AMLES application.

Table 6 describes the Anti-Money Laundering Event Scoring User Roles and corresponding User Groups.

Table 6. Anti-Money Laundering Event Scoring Roles and User Groups

Role	Group Name	User Group Code
AO Administrator	AO Admin Group	AOADMNGRP
AO Approver	AO Approver Group	AOAPPROVERGRP

Table 6. Anti-Money Laundering Event Scoring Roles and User Groups (Continued)

Role	Group Name	User Group Code
AO Authorizer	AO Authorizer Group	AOAUTHGRP
AO Creator	AO Creator Group	AOCREATORGRP

This chapter provides the details of AMLES batch run. It involves loading batch execution data from the Rule Run Framework and executing the batch from Operations for the application to be ready for users.

This chapter includes the following sections:

- Starting a Batch Run and Loading Batch Execution Data
- Running Batch Execution

Starting a Batch Run and Loading Batch Execution Data

Start a batch run and load the batch execution data to prepare the historical data for users.

Note: To execute a batch, do not start two batches simultaneously for the same processing group.

To start the batch run and load batch execution data, follow these steps:

1. Log in to the OFSAA Application with your credentials to view the Applications window.
2. Click **Anti Money Laundering Event Scoring** from the Applications window. Alternatively, you can click the link in the left menu.
3. Click **Common Tasks** displayed on the left menu to display *Rule Run Framework*.
4. Click **Rule Run Framework** to display the various menu items.
5. Click **Run**. The Run window is displayed with the available Processes.

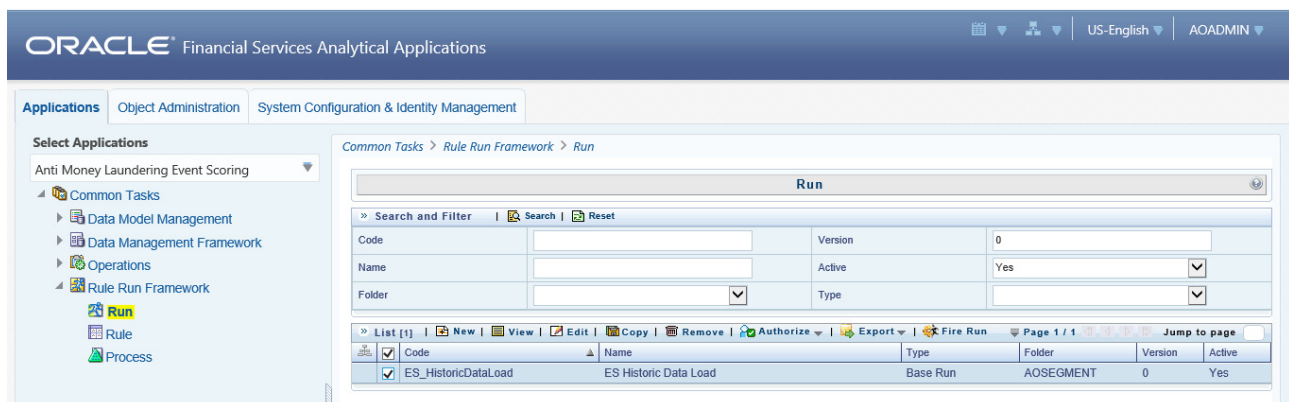


Figure 13. Application List

6. Go to the List section. Select a run, for example (ES_HistoricDataLoad).

4-Configuring the Application

7. Click **Fire Run** to load the batch execution data. The Fire Run window is displayed.

Figure 14. Fire Run Window

8. Enter the following details:

Table 7. Adding Fire Run Details

Fields	Description
Request Type	Select Request Type based on the following options: <ul style="list-style-type: none"> ● Single: If the batch must be executed once. ● Multiple: If the batch must be executed multiple times at different intervals.
Batch	Select Batch. It has the following options: <ul style="list-style-type: none"> ● Create ● Create & Execute From these options, select Create & Execute
Wait	Select Wait. It has the following options: <ul style="list-style-type: none"> ● Yes: This executes the batch after a certain duration. Enter the duration as required. ● No: This executes the batch immediately.
Filters	Enter the filter details. Note: \$MISDATE option can be used to execute the run for that particular day. The format for it to enter in the filter details is: to_date(<ACTIVITY_TABLE_NAME>.<ACTIVITY_DT_COL>)=\$MISDATE Note: For \$MISDATE option: <ul style="list-style-type: none"> ● For either Date or Timestamp datatypes, to_date is mandatory for the filter. ● Activity Table Name and Activity Column Name should be in uppercase.

9. Click **OK** to run the batch. The following message is displayed: *Batch Execution is in progress.*

Note: If batch execution fails, then see the batch details in Batch Monitor. For more information on Batch Monitor, see the *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

10. Once the batch is triggered, check for completion and perform the steps described in the next section.

Running Batch Execution

Run the Batch Execution to load the data for users.

Note: It is mandatory to name the folders where the data is stored in the format YYYYMMDD (for example, 20180115 for 15 January, 2018). Naming the folders in other formats will not generate the data for the Batch Execution Run.

To run the batch execution process, follow these steps:

1. Log in to the OFSAA Application with your credentials to view the Applications window.
2. Click **Anti Money Laundering Event Scoring** from the Applications window. Alternatively, you can click the link in the left menu.
3. Click **Common Tasks** displayed on the left menu to display *Operations*.
4. Click **Operations** to display the various menu items for administration operations.
5. Click **Batch Execution** to view the *Batch Execution* window. On this window, select the **Batch ID** AOINFO_xxx (where xxx is a multi-digit identifier).
6. Click the date-picker and select the date for the batch execution data from the **Information Date** section.
7. Click **Execute Batch** to execute the batch runs for Batch ID.

The screenshot displays the Oracle Financial Services Analytical Applications interface. The top navigation bar shows 'ORACLE Financial Services Analytical Applications' and user information 'US-English' and 'AOADMIN'. The left sidebar contains a 'Select Applications' menu with 'Anti Money Laundering Event Scoring' expanded to show 'Common Tasks', 'Operations', and 'Rule Run Framework'. Under 'Operations', 'Batch Execution' is highlighted. The main content area shows the 'Batch Execution' configuration window. It includes a breadcrumb trail 'Common Tasks > Operations > Batch Execution' and a search bar for 'Last Modification Date'. The 'Batch Details' section shows a table with one row: Batch ID 'AOINFO_1515047392273' and Batch Description 'AutoRun_1510308816297_Description'. The 'Task Details' section shows a table with 10 rows of tasks, including Task1 through Task10, with columns for Task ID, Task Description, Metadata Value, Component ID, Precedence, and Task Status. The 'Information Date' section shows a date picker set to '01/09/2018'. An 'Execute Batch' button is located at the bottom right of the configuration area.

Task ID	Task Description	Metadata Value	Component ID	Precedence	Task Status
Task1	AlertOp_Batchid	AlertOp_Batchid	TRANSFORM DATA		N
Task2	DELETE_DIM_TABLES	DELETE_DIM_TABLES	TRANSFORM DATA	Task1	N
Task3	F2T_DIM_ES_ENTITY_TYPE	F2T_DIM_ES_ENTITY_TYPE	LOAD DATA	Task2	N
Task4	F2T_DIM_ES_ENTITY_TYPE_MLS	F2T_DIM_ES_ENTITY_TYPE_MLS	LOAD DATA	Task3	N
Task5	DELETE_DIM_TABLES	DELETE_DIM_TABLES	TRANSFORM DATA	Task1	N
Task6	F2T_DIM_ES_MEASURE_NAME	F2T_DIM_ES_MEASURE_NAME	LOAD DATA	Task5	N
Task7	F2T_DIM_ES_MEASURE_NAME_MLS	F2T_DIM_ES_MEASURE_NAME_MLS	LOAD DATA	Task6	N
Task8	DELETE_DIM_TABLES	DELETE_DIM_TABLES	TRANSFORM DATA	Task1	N
Task9	F2T_DIM_ES_SCENARIO	F2T_DIM_ES_SCENARIO	LOAD DATA	Task8	N
Task10	F2T_DIM_ES_SCENARIO_MLS	F2T_DIM_ES_SCENARIO_MLS	LOAD DATA	Task9	N

4-Configuring the Application

The following table provides details for the batch execution load into the application database:

Table 8. Batch Execution Data Load and Format Details

File Name	Table Name	Description
F2T_DIM_ES_ENTITY_TYPE	DIM_ES_ENTITY_TYPE	Load data from .dat file to DIM_ES_ENTITY_TYPE table.
F2T_DIM_ES_ENTITY_TYPE_MLS	DIM_ES_ENTITY_TYPE_MLS	Load data from .dat file to DIM_ES_ENTITY_TYPE_MLS table.
F2T_DIM_ES_MEASURE_NAME	DIM_ES_MEASURE_NAME	Load data from .dat file to DIM_ES_MEASURE_NAME table.
F2T_DIM_ES_MEASURE_NAME_MLS	DIM_ES_MEASURE_NAME_MLS	Load data from .dat file to DIM_ES_MEASURE_NAME_MLS table.
F2T_DIM_ES_SCENARIO	DIM_ES_SCENARIO	Load data from .dat file to DIM_ES_SCENARIO table.
F2T_DIM_ES_SCENARIO_MLS	DIM_ES_SCENARIO_MLS	Load data from .dat file to DIM_ES_SCENARIO_MLS table.
F2T_DIM_ES_SEGMENT	DIM_ES_SEGMENT	Load data from .dat file to DIM_ES_SEGMENT table.
F2T_DIM_ES_SEGMENT_MLS	DIM_ES_SEGMENT_MLS	Load data from .dat file to DIM_ES_SEGMENT_MLS table.
F2T_DIM_ES_EVENT_WF_STATUS	DIM_ES_EVENT_WF_STATUS	Load data from .dat file to DIM_ES_EVENT_WF_STATUS table.
F2T_DIM_ES_EVENT_WF_STATUS_MLS	DIM_ES_EVENT_WF_STATUS_MLS	Load data from .dat file to DIM_ES_EVENT_WF_STATUS_MLS table.
F2T_FSI_ES_EVENT_INPUT_STG	FSI_ES_EVENT_INPUT_STG	Load data from .dat file to FSI_ES_EVENT_INPUT_STG table.
T2T_FSI_ES_EVENT_INPUT	FSI_ES_EVENT_INPUT	Data is loaded from F2T_FSI_ES_EVENT_INPUT_STG file to F2T_FSI_ES_EVENT_INPUT_STG table. After a successful DQ check the data from F2T_FSI_ES_EVENT_INPUT_STG is loaded to F2T_FSI_ES_EVENT_INPUT table by a T2T.

The following table provides details for the data format for the flat files that load batch execution data into the application database:

Note: The character ~ denotes a space in the Data Format.

Table 9. Batch Execution Data File Format

File Name	Data Format
F2T_DIM_ES_ENTITY_TYPE	D_RECORD_END_DATE (dd-mm-yyyy)~D_RECORD_START_DATE (dd-mm-yyyy)~F_AUTHFLAG~F_LATEST_RECORD_INDICATOR~~~V_ENTITY_TYPE~V_ENTITY_TYPE_CODE~~~
F2T_DIM_ES_ENTITY_TYPE_MLS	DESCLOCALE~V_ENTITY_TYPE~V_ENTITY_TYPE_CODE
F2T_DIM_ES_MEASURE_NAME	D_RECORD_END_DATE (dd-mm-yyyy)~D_RECORD_START_DATE (dd-mm-yyyy)~~F_LATEST_RECORD_INDICATOR~~~~~V_MEASURE_CODE~V_MEASURE_DESC~V_MEASURE_NAME~V_DATATYPE
F2T_DIM_ES_MEASURE_NAME_MLS	DESCLOCALE~V_MEASURE_CODE~V_MEASURE_DESC~V_MEASURE_NAME
F2T_DIM_ES_SCENARIO	D_RECORD_END_DATE (dd-mm-yyyy)~D_RECORD_START_DATE (dd-mm-yyyy)~~F_LATEST_RECORD_INDICATOR~~~~~V_SCENARIO_CODE~V_SCENARIO_DESC~V_SCENARIO_NAME
F2T_DIM_ES_SCENARIO_MLS	DESCLOCALE~V_SCENARIO_CODE~V_SCENARIO_DESC~V_SCENARIO_NAME
F2T_DIM_ES_SEGMENT	D_RECORD_END_DATE (dd-mm-yyyy)~D_RECORD_START_DATE (dd-mm-yyyy)~~F_LATEST_RECORD_INDICATOR~~~~~V_SEGMENT_CODE~V_SEGMENT_DESC~V_SEGMENT_NAME
F2T_DIM_ES_SEGMENT_MLS	DESCLOCALE~V_SEGMENT_CODE~V_SEGMENT_DESC~V_SEGMENT_NAME
F2T_DIM_ES_EVENT_WF_STATUS	D_RECORD_END_DATE (dd-mm-yyyy)~D_RECORD_START_DATE (dd-mm-yyyy)~~F_AUTHFLAG~~~~~V_WF_STATUS_CODE~V_WF_STATUS_DESC~V_WF_STATUS_NAME
F2T_DIM_ES_EVENT_WF_STATUS_MLS	DESCLOCALE~V_WF_STATUS_CODE~V_WF_STATUS_DESC~V_WF_STATUS_NAME
F2T_FSI_ES_EVENT_INPUT_STG	D_EVENT_GENERATION_DATE (dd-mm-yyyy)~N_EVENT_ID~V_ENTITY_TYPE_NAME~V_MEASURE_NAME~V_MEASURE_VALUE~V_SCENARIO_NAME~V_SEGMENT_NAME~V_WF_STATUS_NAME
T2T_FSI_ES_EVENT_INPUT	Not Applicable

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

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

Table 10. 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.
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 11 describes the attributes to be configured for setting the application server.

Table 11. 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.

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](#)
- [Configuring the Session Timeout Setting for Admin Tools](#)

Configuring the Session Timeout Setting

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.

For more information on how to set the duration before logout for inactive sessions, see the *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

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>
```