Oracle® E-Business Suite

Mobile Apps Administrator's Guide

Release 12.1 and 12.2

Part No. E64384-02

October 2015

ORACLE®

Oracle E-Business Suite Mobile Apps Administrator's Guide, Release 12.1 and 12.2

Part No. E64384-02

Primary Author: Melody Yang

Contributing Author: Tushar Abedin, Tahir Ahmad, Hadi Alatasi, Sugathan Aravindan, Max Arderius, John Brazier, Prasanna Athota, Erik Graversen, Hubert Ferst, Sri Ramya Inturi, Clara Jaeckel, Anupam Johri, Jeanne Lowell, Chidananda Pati, Balakrishna Pulivarthi, Arun Purushothaman, Esteban Rodriguez, Dilbagh Singh, Vijayakumar Shanmugam, Ryoji Suzuki, Sukanya Tadepalli, Venkatakalpanarani Thota, Arvin Tjen, Erik Wu, Bill Wyza

Contents

Send Us Your Comments

Preface

1 Introduction to Oracle E-Business Suite Mobile Apps

2 Setting Up the Mobile Apps

3 Working with Mobile Application Archives for Enterprise Distribution

4 Customization Support for Corporate Branding

5 Mobile Application Management (MAM) Support with Oracle Mobile Security Suite

6 Advanced Configurations

7 Diagnostics and Troubleshooting

A Mobile App Access Roles

B Mobile App Module Names

C Application Definition Metadata

D Setting Up and Using the Supported Languages

E Associated Products in My Oracle Support

Send Us Your Comments

Oracle E-Business Suite Mobile Apps Administrator's Guide, Release 12.1 and 12.2

Part No. E64384-02

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document. Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

Note: Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the new Oracle E-Business Suite Release Online Documentation CD available on My Oracle Support and www.oracle.com. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: appsdoc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at www.oracle.com.

Preface

Intended Audience

Welcome to Release 12.1 and 12.2 of the *Oracle E-Business Suite Mobile Apps Administrator's Guide.*

This guide assumes you have a working knowledge of the following:

- The principles and customary practices of your business area.
- Computer desktop application usage and terminology.
- Oracle E-Business Suite applications.

This documentation assumes familiarity with Oracle E-Business Suite. It is written for the technical consultants, implementers and system integration consultants who oversee the functional requirements of these applications and deploy the functionality to their users.

If you have never used Oracle E-Business Suite, we suggest you attend one or more of the Oracle E-Business Suite training classes available through Oracle University.

See Related Information Sources on page x for more Oracle E-Business Suite product information.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Structure

Related Information Sources

This book is included in the Oracle E-Business Suite Documentation Library. If this guide refers you to other Oracle E-Business Suite documentation, use only the latest Release 12.2 versions of those guides.

Online Documentation

All Oracle E-Business Suite documentation is available online (HTML or PDF).

- **Online Help** - Online help patches (HTML) are available on My Oracle Support.

- **Oracle E-Business Suite Documentation Library** - This library, which is included in the Oracle E-Business Suite software distribution, provides PDF documentation as of the time of each release.

- **Oracle E-Business Suite Documentation Web Library** - This library, available on the Oracle Technology Network, provides the latest updates to Oracle E-Business Suite documentation. See http://docs.oracle.com/cd/E26401_01/index.htm for the latest Release 12.2 documentation or http://docs.oracle.com/cd/E18727_01/index.htm for the latest Release 12.1 documentation. Most documents are available in PDF and HTML formats.

- **Release Notes** - For information about changes in this release, including new features, known issues, and other details, see the release notes for the relevant product, available on My Oracle Support.

- **Oracle Electronic Technical Reference Manual -** The Oracle Electronic Technical Reference Manual (eTRM) contains database diagrams and a detailed description of database tables, forms, reports, and programs for each Oracle E-Business Suite product. This information helps you convert data from your existing applications and integrate Oracle E-Business Suite data with non-Oracle applications, and write custom reports for Oracle E-Business Suite products. The Oracle eTRM is available on My Oracle Support.

Related Guides

You should have the following related books on hand. Depending on the requirements of your particular installation, you may also need additional manuals or guides.

Oracle Alert User's Guide

This guide explains how to define periodic and event alerts to monitor the status of your Oracle E-Business Suite data.

Oracle Diagnostics Framework User's Guide

This manual contains information on implementing and administering diagnostics tests for Oracle E-Business Suite using the Oracle Diagnostics Framework.

Oracle E-Business Suite Concepts

This book is intended for all those planning to deploy Oracle E-Business Suite Release 12.2, or contemplating significant changes to a configuration. After describing the Oracle E-Business Suite architecture and technology stack, it focuses on strategic topics, giving a broad outline of the actions needed to achieve a particular goal, plus the installation and configuration choices that may be available.

Oracle E-Business Suite CRM System Administrator's Guide

This manual describes how to implement the CRM Technology Foundation (JTT) and use its System Administrator Console.

Oracle E-Business Suite Developer's Guide

This guide contains the coding standards followed by the Oracle E-Business Suite development staff. It describes the Oracle Application Object Library components needed to implement the Oracle E-Business Suite user interface described in the *Oracle E-Business Suite User Interface Standards for Forms-Based Products*. It provides information to help you build your custom Oracle Forms Developer forms so that they integrate with Oracle E-Business Suite. In addition, this guide has information for customizations in features such as concurrent programs, flexfields, messages, and logging.

Oracle E-Business Suite Maintenance Guide

This guide explains how to patch an Oracle E-Business Suite system, describing the adop patching utility and providing guidelines and tips for performing typical patching operations. It also describes maintenance strategies and tools that can help keep a system running smoothly.

Oracle E-Business Suite Security Guide

This guide contains information on a comprehensive range of security-related topics, including access control, user management, function security, data security, and auditing. It also describes how Oracle E-Business Suite can be integrated into a single sign-on environment.

Oracle E-Business Suite Setup Guide

This guide contains information on system configuration tasks that are carried out either after installation or whenever there is a significant change to the system. The activities described include defining concurrent programs and managers, enabling Oracle Applications Manager features, and setting up printers and online help.

Oracle E-Business Suite User's Guide

This guide explains how to navigate, enter and query data, and run concurrent requests using the user interface (UI) of Oracle E-Business Suite. This guide also includes information on setting user profiles and customizing the UI.

Oracle E-Business Suite User Interface Standards for Forms-Based Products

This guide contains the user interface (UI) standards followed by the Oracle E-Business Suite development staff. It describes the UI for the Oracle E-Business Suite products and how to apply this UI to the design of an application built by using Oracle Forms.

Oracle Workflow Administrator's Guide

This guide explains how to complete the setup steps necessary for any product that includes workflow-enabled processes. It also describes how to manage workflow processes and business events using Oracle Applications Manager, how to monitor the progress of runtime workflow processes, and how to administer notifications sent to workflow users.

Oracle Workflow Developer's Guide

This guide explains how to define new workflow business processes and customize existing Oracle E-Business Suite-embedded workflow processes. It also describes how to define and customize business events and event subscriptions.

Oracle Workflow User's Guide

This guide describes how users can view and respond to workflow notifications and monitor the progress of their workflow processes.

Do Not Use Database Tools to Modify Oracle E-Business Suite Data

Oracle STRONGLY RECOMMENDS that you never use SQL*Plus, Oracle Data Browser, database triggers, or any other tool to modify Oracle E-Business Suite data unless otherwise instructed.

Oracle provides powerful tools you can use to create, store, change, retrieve, and maintain information in an Oracle database. But if you use Oracle tools such as SQL*Plus to modify Oracle E-Business Suite data, you risk destroying the integrity of your data and you lose the ability to audit changes to your data.

Because Oracle E-Business Suite tables are interrelated, any change you make using an

Oracle E-Business Suite form can update many tables at once. But when you modify Oracle E-Business Suite data using anything other than Oracle E-Business Suite, you may change a row in one table without making corresponding changes in related tables. If your tables get out of synchronization with each other, you risk retrieving erroneous information and you risk unpredictable results throughout Oracle E-Business Suite.

When you use Oracle E-Business Suite to modify your data, Oracle E-Business Suite automatically checks that your changes are valid. Oracle E-Business Suite also keeps track of who changes information. If you enter information into database tables using database tools, you may store invalid information. You also lose the ability to track who has changed your information because SQL*Plus and other database tools do not keep a record of changes.

1

Introduction to Oracle E-Business Suite Mobile Apps

Overview

Oracle E-Business Suite mobile apps enable users to perform needed tasks or take action on Oracle E-Business Suite transactions from mobile devices including iOS and Android smartphones. For example, users can handle approval requests through the mobile app for approvals or perform time entry on the mobile app for timecards. Users can download these apps from the Apple App Store and Google Play. To use the apps, users must be licensed for the base products, with mobile services configured on the Oracle E-Business Suite server. To find Oracle E-Business Suite mobile apps, search for the keywords "Oracle America EBS" in the Apple App Store and Google Play.

This guide describes how to set up an Oracle E-Business Suite instance to support connections from these mobile apps. It also describes common administrative tasks for configuring Oracle E-Business Suite mobile apps, as well as the setup tasks for working with Mobile Application Archives (MAA) to enable enterprise-distributed apps.

> **Note:** This guide does not apply to Oracle Fusion Expenses and Oracle Mobile Field Service apps. For information about Oracle Fusion Expenses, see My Oracle Support Knowledge Document 1625446.1; for information about Oracle Mobile Field Service, see My Oracle Support Knowledge Document 1564644.1.

- For known issues for Oracle E-Business Suite mobile apps, see the *Oracle E-Business Suite Mobile Foundation Release Notes*, My Oracle Support Knowledge Document 1642431.1.

- For the list of available Oracle E-Business Suite mobile apps, see the *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*, My Oracle Support Knowledge Document 1641772.1.

- For frequently asked questions, refer to My Oracle Support Knowledge Document 2064887.1, *Oracle E-Business Suite Mobile Apps Frequently Asked Questions (FAQ)*.

- To share ideas with Oracle related to mobile apps, see My Oracle Support Knowledge Document 1641772.1, *Oracle E-Business Suite Product Enhancement Request to My Oracle Support Community FAQ*.

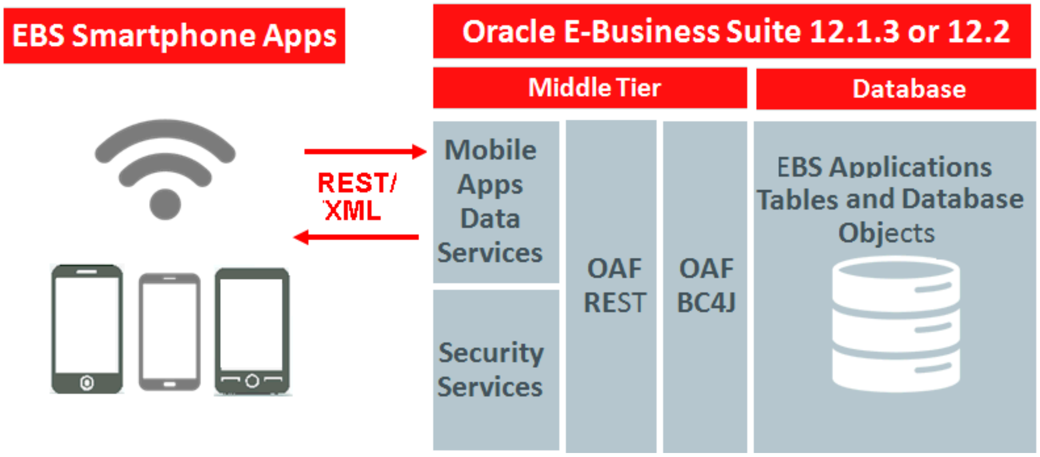
The initial releases of our mobile apps were distributed in English only. In the mobile app version 1.3.0 or the version 1.0.x for Person Directory and Learning apps, with Oracle E-Business Suite Mobile Foundation Release 4.0, the apps are available in the following languages: Brazilian Portuguese, Canadian French, Dutch, English, French, German, Italian, Japanese, Latin American Spanish, Simplified Chinese, and Spanish.

For information on using these languages, see Setting Up and Using Supported Languages, page D-1.

Technical Overview

Oracle E-Business Suite mobile apps interact with the middle tier through REST-based data services and security services. When a mobile user launches the app, the security services are invoked to authenticate the user based on user credentials and initialize the security context to authorize the user with access privileges. Once the login is validated successfully, the user can access the app and the underlying Oracle E-Business Suite REST services.

The following diagram illustrates the high level technical architecture for Oracle E-Business Suite mobile apps:


EBS Smartphone Apps
Oracle E-Business Suite 12.1.3 or 12.2
Middle Tier
Database
REST/
XML
Mobile Apps Data Services
Security Services
OAF REST
OAF BC4J
EBS Applications Tables and Database Objects

Oracle E-Business Suite mobile apps are compatible with both Release 12.1.3 and Release 12.2.3 and onwards, as well as iOS 7.0 or higher and Android 4.1 or higher.

Users can run the mobile apps on any devices that are capable of running iOS 7.0 or higher. Oracle E-Business Suite primarily tests its iOS mobile apps with iPhones, iPod Touches, and iPads.

In general, users can run Android mobile apps on any devices that are capable of running Android 4.1 or higher. Android device manufacturers often customize their Android distributions. Due to the degree of Android fragmentation, Oracle E-Business Suite cannot perform comprehensive device-specific certifications for this platform. Oracle strongly encourages all customers to test candidate mobile devices with their mission-critical Oracle E-Business Suite product flows before deploying those devices broadly to their end users. Oracle E-Business Suite primarily tests its Android mobile apps with Samsung Galaxy and Google Nexus devices. Reported issues that cannot be reproduced on Samsung or Google devices will be analyzed on a on-on-one basis and may need additional assistance from the device vendors first.

Oracle E-Business Suite mobile apps are developed using Oracle Mobile Application Framework (Oracle MAF), as well as additional components specific to Oracle E-Business Suite provided through the Oracle E-Business Suite Mobile Foundation. Different versions of the mobile apps may require different configuration steps on the Oracle E-Business Suite server. Before you begin configuring the mobile apps, Oracle recommends that you review the mobile app version requirements in this document and perform the configuration steps for the appropriate app version. See Oracle E-Business Suite Mobile Foundation Release Update History section, My Oracle Support Knowledge Document 1642431.1, *Oracle E-Business Suite Mobile Foundation Release Notes*.

As shown in the earlier diagram, there is no new technology required on the Oracle E-Business Suite server for the mobile apps. To use the Oracle E-Business Suite mobile apps, you only need to apply server-side patches and perform some setup tasks to configure your mobile app on the server.

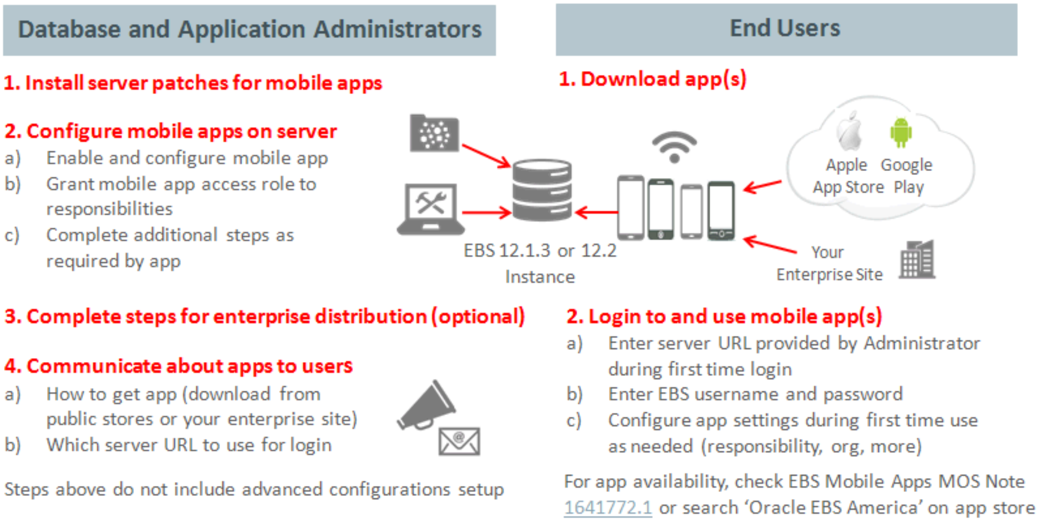
2

Setting Up the Mobile Apps

Setup Overview

Before letting the mobile users download and use an app, you need to perform administrative tasks on the Oracle E-Business Suite server for your app. These tasks include installing server patches, configuring the mobile app, granting the app access role to responsibilities, completing additional setup tasks such as device integration if required for your app, and validating the server URL before communicating the information to the users.

The following diagram illustrates these high level setup tasks for the administrators to perform on the server. Once the server-side setup is complete, the mobile users can start to download and use the app on the go.



Database and Application Administrators

1. Install server patches for mobile apps

2. Configure mobile apps on server
a) Enable and configure mobile app
b) Grant mobile app access role to responsibilities
c) Complete additional steps as required by app

3. Complete steps for enterprise distribution (optional)

4. Communicate about apps to users
a) How to get app (download from public stores or your enterprise site)
b) Which server URL to use for login

Steps above do not include advanced configurations setup

End Users

1. Download app(s)

2. Login to and use mobile app(s)
a) Enter server URL provided by Administrator during first time login
b) Enter EBS username and password
c) Configure app settings during first time use as needed (responsibility, org, more)

For app availability, check EBS Mobile Apps MOS Note 1641772.1 or search 'Oracle EBS America' on app store

This chapter describes the following administrative tasks:

1. Applying Prerequisite Patches on the Oracle E-Business Suite Server, page 2-2

2. Configuring the Mobile Apps on the Oracle E-Business Suite Server, page 2-11

3. Setting Up Mobile App Access to Responsibilities, page 2-35

4. Additional Setup for Device Integration, page 2-37

5. Additional App-Specific Setup, page 2-54

6. Communicating Mobile App Information to Users, page 2-54

Applying Prerequisite Patches on the Oracle E-Business Suite Server

For each Oracle E-Business Suite mobile app, apply the corresponding consolidated product family patch and conditionally required patches if needed.

> **Note:** Ensure that you run AutoConfig after applying the consolidated product family patch for Oracle E-Business Suite Release 12.1. In Oracle E-Business Suite Release 12.2, when you apply patches using the adop (AD Online Patching) utility, adop runs AutoConfig by default.

The following table lists the product family and the corresponding product family consolidated patches for each app:

> **Note:** If you previously configured Oracle Mobile Approvals for Oracle E-Business Suite (Approvals) or Oracle Mobile Timecards for Oracle E-Business Suite (Timecards) version 1.0.x, with Oracle E-Business Suite Mobile Foundation Release 1.0 on your Oracle E-Business Suite server, then the first time you apply these product family consolidated patches for Oracle E-Business Suite Mobile Foundation Release 2.1 or later, the app status is changed to "Not Configured" due to technical changes in the required configuration parameters. After applying the patches, you must re-enable and reconfigure these apps according to the instructions in Configuring the Mobile Apps on the Oracle E-Business Suite Server, page 2-11.

To support the "Web SSO" authentication in Oracle E-Business Suite Mobile Foundation Release 4.0, you must also apply required patches and perform additional setup tasks to enable the feature. See: Additional Setup Tasks to Enable Web SSO Authentication Security, page 2-25.

> **Important:** The Oracle E-Business Suite 12.2 server-side patches listed in this table are already included in the respective product family patches in Oracle E-Business Suite Release 12.2.5. If you have installed Oracle E-Business Suite Release 12.2.5, simply apply the Oracle

E-Business Suite Mobile Foundation Release 4.0 post-install patches described in Conditional Post-Install Patches, page 2-7.

Oracle E-Business Suite Server-Side Product Family Patches for Oracle E-Business Suite Mobile Foundation Release 4.0

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle E-Business Suite Applications Technology (atg_pf)	• Oracle Mobile Approvals for Oracle E-Business Suite	Apply the product family patches for the approval types you want to use, as shown in subsequent rows in this table.	Apply the product family patches for the approval types you want to use, as shown in subsequent rows in this table.
Oracle Financials (fin_pf)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Expense approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Supplier Invoices approvals)	Patch 20518386:R12.FIN_PF.B: FIN - 12.1.3 Consolidated Patch For Mobile Applications Foundation V4	Merge and apply the following patches using the command: • Patch 20843806:R12.FND.C • 20518468:R12.FIN_PF.C: FIN - 12.2 Consolidated Patch For Mobile Applications Foundation V4 `adop phase=apply patches=20843806,20518468 merge=yes`

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Human Resources (hr_pf)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Recruitment approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Timecard approvals) • Oracle Mobile Timecards for Oracle E-Business Suite • Oracle Mobile Learning for Oracle E-Business Suite • Oracle Mobile Person Directory for Oracle E-Business Suite	Patch 20518387:R12.HR_PF.B: HR - 12.1.3 Consolidated Patch For Mobile Applications Foundation V4	Merge and apply the following patches using the command: • Patch 20843806:R12.FND.C • 20518464:R12.HR_PF.C: HR - 12.2 Consolidated Patch For Mobile Applications Foundation V4 `adop phase=apply patches=20843806,20518464 merge=yes`

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Procurement (prc_pf)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Purchase Order approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Requisition approvals) • Oracle Mobile iProcurement for Oracle E-Business Suite • Oracle Mobile Procurement for Oracle E-Business Suite	Patch 20518405:R12.PRC_PF.B: PRC - 12.1.3 Consolidated Patch For Mobile Applications Foundation V4	Merge and apply the following patches using the command: • Patch 20843806:R12.FND.C • 20518485:R12.PRC_PF.C: PRC - 12.2 Consolidated Patch For Mobile Applications Foundation V4 `adop phase=apply patches=20843806,20518485 merge=yes`
Oracle Projects (pj_pf)	• Oracle Mobile Project Manager for Oracle E-Business Suite	Patch 20518354:R12.PJ_PF.B: PJ - 12.1.3 Consolidated Patch For Mobile Applications Foundation V4	Merge and apply the following patches using the command: • Patch 20843806:R12.FND.C • 20518456:R12.PJ_PF.C: PJ - 12.2 Consolidated Patch For Mobile Applications Foundation V4 `adop phase=apply patches=20843806,20518456 merge=yes`

Product Family	**Mobile App Name**	**Patch for Oracle E-Business Suite 12.1.3**	**Patch for Oracle E-Business Suite 12.2**
Oracle Supply Chain Management (scm_pf)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Item Changes approvals) • Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite • Oracle Mobile Inventory for Oracle E-Business Suite • Oracle Mobile Maintenance for Oracle E-Business Suite • Oracle Mobile Process Production Supervisor for Oracle E-Business Suite • Oracle Mobile Product Information for Oracle E-Business Suite • Oracle Mobile Project Manufacturing for Oracle E-Business Suite	Patch 20518353:R12.SCM_PF.B: SCM -12.1.3 Consolidated Patch For Mobile Applications Foundation V4	Merge and apply the following patches using the command: • Patch 20843806:R12.FND.C • 20518445:R12.SCM_PF.C: SCM -12.2 Consolidated Patch For Mobile Applications Foundation V4 `adop phase=apply patches=20843806,20518445 merge=yes`

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
	- Oracle Mobile Sales Orders for Oracle E-Business Suite		

Conditional Post-Install Patches

For Mobile Apps with Oracle E-Business Suite Mobile Foundation Release 4.0

Apply any additional conditionally required post-install patches from the following list for your apps, with Oracle E-Business Suite Mobile Foundation Release 4.0:

Conditional Post-Install Patches for Mobile Apps with Oracle E-Business Suite Mobile Foundation Release 4.0

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Mobile Foundation Release 4.0 Online Help	Required for all Oracle E-Business Suite mobile apps, with Oracle E-Business Suite Mobile Foundation Release 4.0, connect to Oracle E-Business Suite 12.1.3 or 12.2	Patch 21275035
Oracle E-Business Suite 12.1.3	Required if your app connects to Oracle E-Business Suite 12.1.3	Patch 21881376:R12.FND.B
Oracle E-Business Suite 12.1.3 - Oracle Mobile Approvals for Oracle E-Business Suite (Supplier Invoices approvals only)	Required if you use Oracle Mobile Approvals for Oracle E-Business Suite (Supplier Invoices approvals only) for Oracle E-Business Suite 12.1.3	Patch 21671565:R12.AP.B
Oracle E-Business Suite 12.2	Required if your app connects to Oracle E-Business Suite 12.2	Patch 21881376:R12.FND.C

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite 12.2 • Oracle Mobile Approvals for Oracle E-Business Suite (Item Changes approvals only)	Required if you use Oracle Mobile Approvals for Oracle E-Business Suite (Item Changes approvals only) for Oracle E-Business Suite 12.2	Patch 21566332:R12.ENG.D
Oracle E-Business Suite 12.2 • Oracle Mobile Approvals for Oracle E-Business Suite (Supplier Invoices approvals only)	Required if you use Oracle Mobile Approvals for Oracle E-Business Suite (Supplier Invoices approvals only) for Oracle E-Business Suite 12.2	Patch 21671565:R12.AP.C

For Mobile Apps with Oracle E-Business Suite Mobile Foundation Release 3.0

- If you have installed Oracle E-Business Suite Release 12.2.5, then you have implicitly applied the product family patches for Oracle E-Business Suite Mobile Foundation Release 4.0. In this situation, apply the post-install patches listed earlier for Oracle E-Business Suite Mobile Foundation Release 4.0 instead for the completeness of patch installation.

  Please note that the post-install patches for Oracle E-Business Suite Mobile Foundation Release 3.0 are a subset of the post-install patches for Oracle E-Business Suite Mobile Foundation Release 4.0. Once you have applied the post-install patches for Oracle E-Business Suite Mobile Foundation Release 4.0, you have implicitly applied the patches for Oracle E-Business Suite Mobile Foundation Release 3.0.

- If your app version is 1.2.x, with Oracle E-Business Suite Mobile Foundation Release 3.0, here is the reference of the server-side product family patches that you might have applied:

Oracle E-Business Suite Server-Side Product Family Patches for Oracle E-Business Suite Mobile Foundation Release 3.0

Product Family	Oracle E-Business Suite 12.1.3	Oracle E-Business Suite 12.2
Oracle Financials (fin_pf)	Patch 20049351:R12.FIN_PF.B: FIN - 12.1.3 Consolidated Patch For Mobile Applications Foundation V3	Patch 20049474:R12.FIN_PF.C: FIN - 12.2 Consolidated Patch For Mobile Applications Foundation V3
Oracle Human Resources (hr_pf)	• Release 12.1 HRMS RUP6 (R12.HR_PF.B.Delta.6) For detailed instructions, see the Oracle Human Resources Management Systems Readme, HRMS Release Update Pack 6 for Release 12.1, My Oracle Support Knowledge Document 1549442.1. • Patch 20049349:R12.HR_PF.B: HR - 12.1.3 Consolidated Patch For Mobile Applications Foundation V3	Patch 20049475:R12.HR_PF.C: HR - 12.2 Consolidated Patch For Mobile Applications Foundation V3

Product Family	Oracle E-Business Suite 12.1.3	Oracle E-Business Suite 12.2
Oracle Procurement (prc_pf)	Patch 20049346:R12.PRC_PF.B: PRC - 12.1.3 Consolidated Patch For Mobile Applications Foundation V3	Patch 20049473:R12.PRC_PF.C: PRC - 12.2 Consolidated Patch For Mobile Applications Foundation V3
Oracle Projects (pj_pf)	Patch 20049352:R12.PJ_PF.B: PJ - 12.1.3 Consolidated Patch For Mobile Applications Foundation V3	Patch 20049476:R12.PJ_PF.C: PJ - 12.2 Consolidated Patch For Mobile Applications Foundation V3
Oracle Supply Chain Management (scm_pf)	Patch 20049353:R12.SCM_PF.B: SCM -12.1.3 Consolidated Patch For Mobile Applications Foundation V3	Patch 20049477:R12.SCM_PF.C: SCM -12.2 Consolidated Patch For Mobile Applications Foundation V3

Apply the additional conditionally required post-install patches from the following list for your apps:

Conditional Post-Install Patches for Mobile Apps with Oracle E-Business Suite Mobile Foundation Release 3.0

Oracle E-Business Suite Release	Requirement	Patch Information
Oracle E-Business Suite 12.1.3	Required if your app connects to Oracle E-Business Suite 12.1.3	Patch 21643419:R12.FND.B
Oracle E-Business Suite 12.2	Required if your app connects to Oracle E-Business Suite 12.2	Patch 22046560:R12.FND.C

Configuring the Mobile Apps on the Oracle E-Business Suite Server

Before letting the mobile users download and use the app, you must first enable the mobile app that you want to configure, and then specify configuration parameter values for the app. Oracle E-Business Suite provides default values for the configuration parameters, which you can optionally override as needed.

Oracle E-Business Suite mobile apps use the configuration service to download the configuration file from the server to the mobile apps. The apps then use the parameters specified in the configuration files to connect securely from the mobile client to the Oracle E-Business Suite instance. You must validate the configuration service URL to ensure the mobile app is ready for the users.

This section includes the following topics:

- Enabling a Mobile App Individually and Specifying the Configuration through the UI, page 2-11
- Enabling and Setting Up Multiple Mobile Apps Using a Script, page 2-29
- Validating the Configuration, page 2-32

> **Note:** This setup is a one-time process for each app. You can enable and set up each app individually through the Mobile Applications Manager UI pages or set up multiple apps simultaneously using a script.
>
> After the initial setup, you can update the configuration parameters if necessary. However, if the configuration is changed after the initial setup is complete and loaded to a user's app, the updated parameters will not be automatically reloaded to the app unless the user initiates the updates from the server. See Directing Users to Obtain Connection Details and Initiate Server Updates, page 7-6.

If your mobile users need to access the Oracle E-Business Suite mobile apps over the Internet, see Demilitarized Zone (DMZ), page 6-1 for additional information on performing this configuration. Otherwise, users must access the Oracle E-Business Suite mobile apps through an intranet connection, such as a virtual private network (VPN).

Enabling a Mobile App Individually and Specifying the Configuration through the UI

Accessing the Mobile Applications Manager UI Page through Roles

To access Oracle E-Business Suite Mobile Applications Manager UI page, log in to Oracle E-Business Suite as a user who has the **Mobile Applications Manager** responsibility.

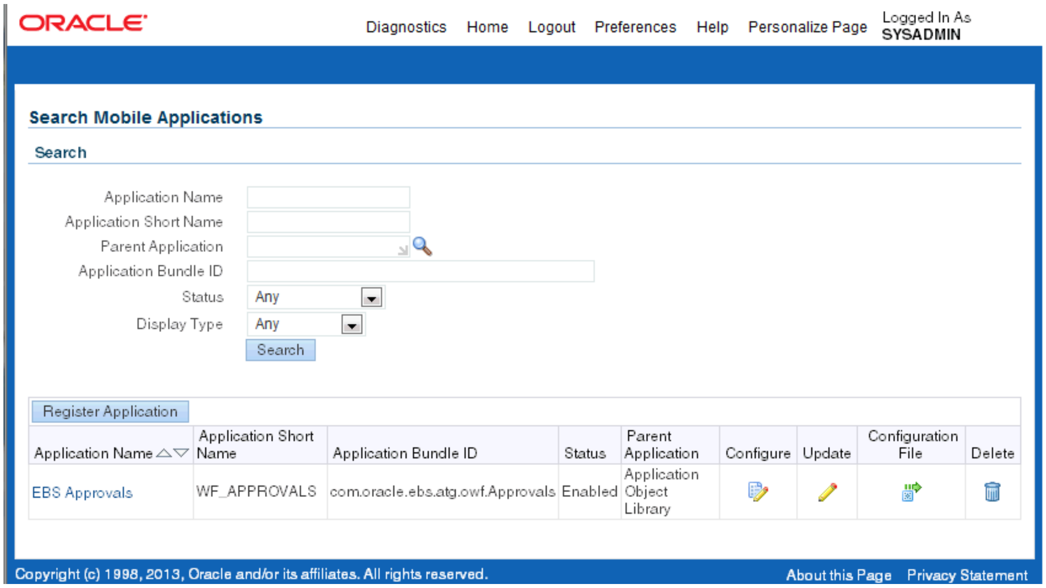
Note: The Mobile Applications Manager responsibility is assigned to the Mobile Applications Administrator role (UMX|FND_MBL_ROLE_ADMIN) and the Mobile Applications Developer role (UMX|FND_MBL_ROLE_DEV). A system administrator assigns these roles to users through Oracle User Management. See: Assigning Roles to or Revoking Roles from Users, *Oracle E-Business Suite Security Guide*.

Users granted different roles can perform various tasks as described in the following table:

Privileges	Mobile Applications Administrator	Mobile Applications Developer
Configure mobile apps	Yes	No
Register enterprise apps	Yes	Yes
Update application definitions	Yes	Yes
Delete application definitions	Yes	Yes

To configure mobile apps, users can obtain the responsibility through the Mobile Applications Administrator role. The SYSADMIN user is granted the Mobile Applications Administrator role by default.

Select the **Mobile Applications Manager** responsibility and choose the **Applications** link from the navigator. The Search Mobile Applications page appears.



Search Mobile Applications

Search

Application Name	
Application Short Name	
Parent Application	
Application Bundle ID	
Status	Any
Display Type	Any

Application Name	Application Short Name	Application Bundle ID	Status	Parent Application	Configure	Update	Configuration File	Delete
EBS Approvals	WF_APPROVALS	com.oracle.ebs.atg.owf.Approvals	Enabled	Application Object Library		✎		

Copyright (c) 1998, 2013, Oracle and/or its affiliates. All rights reserved.
About this Page
Privacy Statement

This Search Mobile Applications page is the entry point to access the application definition details for each Oracle E-Business Suite mobile app. After performing a search, a user who has the Mobile Applications Administrator role can perform the following tasks from the search result table:

> **Note:** If you plan to modify an Oracle E-Business Suite mobile app for enterprise distribution (that is, distribute the app to your users through an enterprise's own site rather than through a public app store), after the modification a user who has the Mobile Applications Developer role can perform the following tasks from the search result table:
>
> - Register the enterprise app by clicking the **Register Application** button.
> - Update the application definition metadata by clicking the **Update** icon.
> - Delete an existing application metadata by clicking the **Delete** icon.
>
> > **Warning:** Updating and Deleting applications starting with `com.oracle.ebs*` is strictly prohibited. These application definitions belong to Oracle E-Business Suite mobile apps and you should not modify any definition metadata of these mobile apps.
>
> For information on these tasks, see Registering and Updating Your Enterprise App Definition Metadata, page 3-4.

- Enable and configure an app by clicking the **Configure** icon.

  See: Enabling and Configuring a Mobile App Individually, page 2-14.

- View and validate the configuration for an app by clicking the **Configuration File** icon

  See: Viewing and Validating Your Mobile App Configuration, page 2-24.

- View overall application definition details displayed in read-only mode by clicking a desired app's Application Name link.

  See: Reviewing Your Mobile App Details, page 2-25.

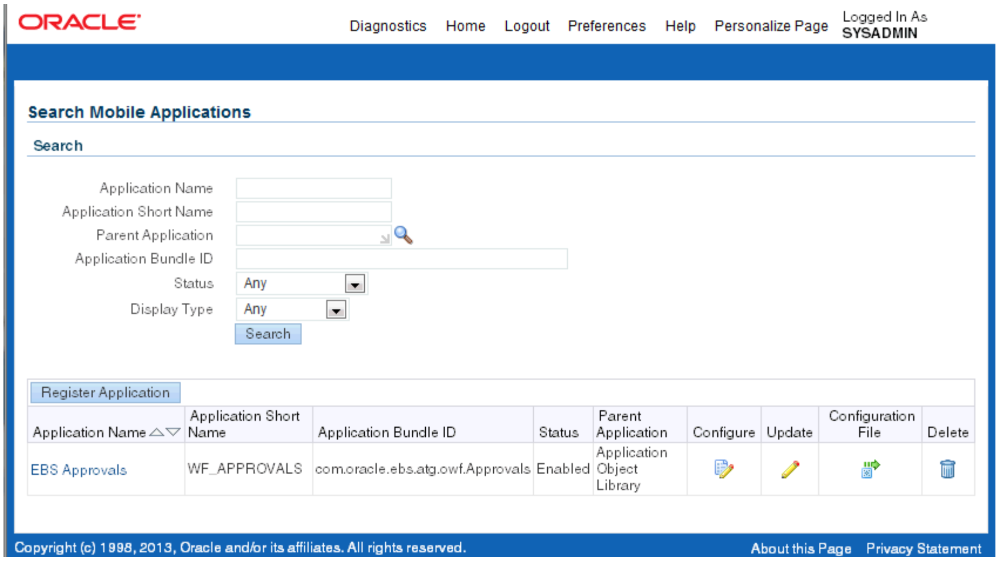
Enabling and Configuring a Mobile App Individually

Perform the following steps to configure your mobile app on the Oracle E-Business Suite server:

1. Log in to Oracle E-Business Suite as a user who has the Mobile Applications Administrator role. For example, log in as `SYSADMIN`.

2. Select the Mobile Applications Manager responsibility and choose the **Applications** link from the navigator.

3. In the Search Mobile Applications page, enter desired search criteria and click the **Search** button. The page displays the mobile apps that match the search criteria in the search result table.



Search Mobile Applications

Search

Application Name	
Application Short Name	
Parent Application	
Application Bundle ID	
Status	Any
Display Type	Any

Application Name	Application Short Name	Application Bundle ID	Status	Parent Application	Configure	Update	Configuration File	Delete
EBS Approvals	WF_APPROVALS	com.oracle.ebs.atg.owf.Approvals	Enabled	Application Object Library	✎	✎	⇨	🗑

Copyright (c) 1998, 2013, Oracle and/or its affiliates. All rights reserved.
About this Page
Privacy Statement

For metadata information that you can enter in the search criteria to locate your desired app, see Appendix C: Application Definition Metadata, page C-1.

4. Click the **Configure** icon for the mobile app that you want to configure from the search result table.

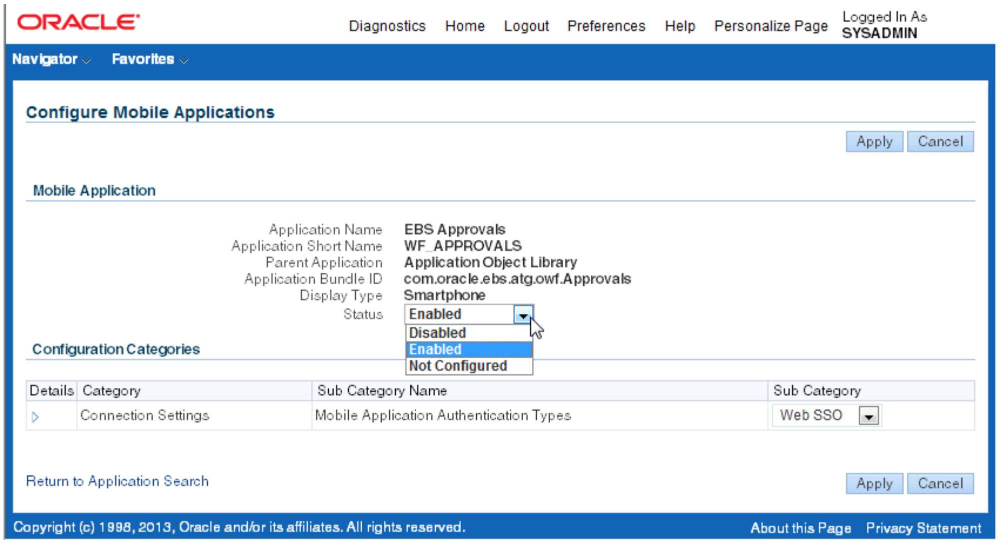
5. Review the app details in the Configure Mobile Applications page. If the selected app is not configured, change the status to "Enabled".

   - Enabled: This allows you to configure the app against Oracle E-Business Suite.

   - Disabled: The app was configured previously but is currently disabled. This prevents any further configuration on the app against Oracle E-Business Suite. If an app was configured successfully prior to setting its status to "Disabled", the app will continue to work.

   - Not Configured (default): The app's definition was just installed on the server and it is not configured yet.

     Note that after an app is configured, although it is possible to change its status to "Not Configured", it is recommended that you change it to "Disabled" only.



Configure Mobile Applications

Mobile Application

Application Name	EBS Approvals
Application Short Name	WF_APPROVALS
Parent Application	Application Object Library
Application Bundle ID	com.oracle.ebs.atg.owf.Approvals
Display Type	Smartphone
Status	Enabled

Configuration Categories

Details	Category	Sub Category Name	Sub Category
▷	Connection Settings	Mobile Application Authentication Types	Web SSO

6. In the Configuration Categories region, the authentication type value ("HTTP Basic" or "Web SSO") for the selected app is displayed in the Sub Category field. This value is predefined or selected during the app registration.

Supporting HTTP Basic and Web SSO Authentication Types in Oracle E-Business Suite Mobile Foundation Release 4.0

Oracle E-Business Suite mobile apps support the following authentication types:

- **HTTP Basic (default)**

  HTTP Basic is the default type for a mobile app to authenticate mobile users. When this type is selected for a mobile app, the users are authenticated against the Oracle E-Business Suite server. If your Oracle E-Business Suite is integrated with Oracle Directory Services, a LDAP directory, then those users are authenticated against Oracle Directory Services as well.

  The authentication type value determines the configuration parameters required to set for your mobile app. For example, when "HTTP Basic" is selected as the type, three associated parameters, that is, Session Timeout, Idle Timeout, and Service Endpoint, are displayed in the Configuration Parameters region.

  For information on setting configuration parameters for the HTTP Basic authentication type, see Configuring Parameters for the HTTP Basic Authentication Type, page 2-18, as described in step 8.

  You can override the default HTTP Basic type by selecting a desired authentication type, such as "Web SSO", from the Sub Category drop-down list when needed. After the change, the parameters corresponding to the selected authentication type will be loaded and displayed in the Configuration Parameters region.

- **Web SSO**

  When the "Web SSO" type is selected for a mobile app, the mobile users are authenticated against an external Oracle Access Manager (OAM) server.

  Use this authentication type if you want to delegate authentication to Oracle Access Manager based on a protected Login URL.

  If you want to use single sign-on across Oracle E-Business Suite mobile apps through the use of Oracle Mobile Security Suite, you must select "Web SSO" as a prerequisite when configuring your mobile apps. See: Mobile Application Management (MAM) Support with Oracle Mobile Security Suite, page 5-1.

  To use "Web SSO" as the authentication type,

  - Your Oracle E-Business Suite instance must be integrated with Oracle Access Manager.

    Refer to My Oracle Support Knowledge Document 1388152.1, *Overview of Single Sign-On Integration Options for Oracle E-Business Suite*.

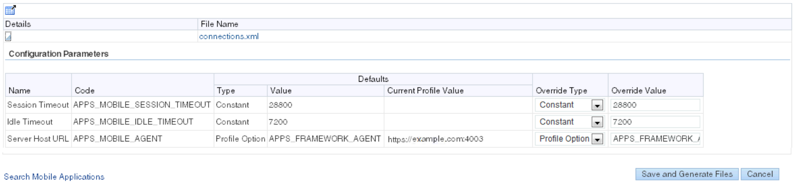
  - You must apply required patches and perform additional setup tasks to enable this feature.

    See: Additional Setup Tasks to Enable Web SSO Authentication Security, page 2-25.

  For information about single sign-on, see Single Sign-On (SSO), page 6-6.

  For information on setting configuration parameters for the Web SSO authentication type, see Configuring Parameters for the Web SSO Authentication Type, page 2-20, as described in step 8.

  > **Note:** The Sub Category field for mobile app authentication type is available in Oracle E-Business Suite Mobile Foundation Release 4.0. In releases earlier than Oracle E-Business Suite Mobile Foundation Release 4.0, the Sub Category field is not shown and "HTTP Basic" is the only supported authentication type for Oracle E-Business Suite mobile apps.



Details	File Name
	connections.xml

Configuration Parameters

		Defaults				
Name	Code	Type	Value	Current Profile Value	Override Type	Override Value
Session Timeout	APPS_MOBILE_SESSION_TIMEOUT	Constant	28800		Constant	28800
Idle Timeout	APPS_MOBILE_IDLE_TIMEOUT	Constant	7200		Constant	7200
Server Host URL	APPS_MOBILE_AGENT	Profile Option	APPS_FRAMEWORK_AGENT	https://example.com:4003	Profile Option	APPS_FRAMEWORK_

7. In the Configuration Categories region, optionally choose the **Show** link next to the Connection Settings category to display the parameters corresponding to the

selected authentication type. You can modify these parameter values for the configuration. If you want to proceed with the default parameter values, skip the next step 8, and go to step 9.

8. Update the configuration parameter values in the Configuration Parameters region to appropriate values for your Oracle E-Business Suite instance, if the configuration parameter settings for your instance are different from the default settings. For example, if the location of a web entry point specific to a mobile app is stored in a custom profile option, then update the Service Endpoint (APPS_MOBILE_AGENT) parameter as explained later in this step with the custom profile option name.

   When the configuration file is loaded to a mobile app, the app uses these parameters to connect to the intended instance.

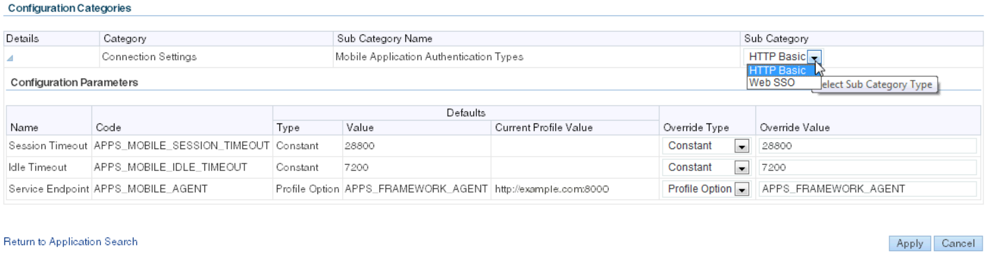
   > **Note:** The service version for the app is also included as a parameter in the configuration file in Oracle E-Business Suite Mobile Foundation Release 2.1 and onwards, but the parameter value is set by Oracle and it cannot be modified. Therefore, it is not listed in the Configuration Parameters region.

   In Oracle E-Business Suite Mobile Foundation Release 4.0, what configuration parameters are required to be included in the configuration file for the app depends on the selected authentication type in the Sub Category field.

   Configuring Parameters for the HTTP Basic Authentication Type

   If the default "HTTP Basic" type is used as the authentication type, update the following parameter values:

Configuration Parameters for the HTTP Basic Authentication Type



Configuration Categories

Details	Category	Sub Category Name	Sub Category
◢	Connection Settings	Mobile Application Authentication Types	HTTP Basic ▾

Configuration Parameters

		Defaults				
Name	Code	Type	Value	Current Profile Value	Override Type	Override Value
Session Timeout	APPS_MOBILE_SESSION_TIMEOUT	Constant	28800		Constant ▾	28800
Idle Timeout	APPS_MOBILE_IDLE_TIMEOUT	Constant	7200		Constant ▾	7200
Service Endpoint	APPS_MOBILE_AGENT	Profile Option	APPS_FRAMEWORK_AGENT	http://example.com:8000	Profile Option ▾	APPS_FRAMEWORK_AGENT

- **Session Timeout (APPS_MOBILE_SESSION_TIMEOUT):** The number of seconds that a user can remain logged in to an app.

  This parameter is specified in seconds, and the minimum value is 300 seconds. The default value is 28800 seconds. After the session expires, the user will be prompted with the standard login page if the idle timeout period has not expired.

> **Note:** Always set the Session Timeout parameter to a value greater than the Idle Timeout value.

- **Idle Timeout (APPS_MOBILE_IDLE_TIMEOUT):** The number of seconds that an app can remain idle after the system no longer detects the activation of the app.

  Similar to session timeout, the minimum value of this parameter is 300 seconds. The default value is 7200 seconds. After the Idle Timeout period expires, the user is timed out of all the app features that are secured by the login connection. In this situation, the user will be prompted with the standard login page.

  > **Note:** The Session Timeout and Idle Timeout parameter values can be set independently of the ICX_SESSION_TIMEOUT profile option on the server. If the Oracle E-Business Suite server session timed out based on the ICX_SESSION_TIMEOUT profile value, when a REST request is made from a mobile app, the request fails authentication and thus triggers the mobile app to display the standard login page.

- **Service Endpoint (APPS_MOBILE_AGENT):** This is the web entry point that the app uses to invoke Oracle E-Business Suite web services. This parameter is known as Server Host URL in Oracle E-Business Suite Mobile Foundation releases earlier than Release 2.1. If your Oracle E-Business Suite environment is configured with multiple web entry points, you can assign a dedicated web entry point for a specific mobile app to connect to the instance.

  Please note that this parameter value may be different from the server URL entered by the app users to configure the app for the first time. Compared to the service endpoint, the server URL is a common web entry point to configure the app, whereas the service endpoint URL may not be known by the mobile users. These users would simply use the usual Oracle E-Business Suite web applications URL as the server URL in the configuration flow. The app-specific configuration settings including the service endpoint parameter value are downloaded from the server through this server URL. Downloaded parameter values are configured into the app and stored in the local database of the mobile device. The app then connects to the dedicated server defined by the service endpoint to invoke Oracle E-Business Suite web services.

  This parameter value can be obtained in the following ways:

  - The default value for this parameter is the current value of the APPS_FRAMEWORK_AGENT profile option, as shown in the parameter table.

- You can optionally override the default value by selecting an override type and entering a corresponding override value.
  - **Constant:** Enter a constant URL for your Oracle E-Business Suite instance in the Override Value field.
  - **Profile Option:** If you are storing the URL for your Oracle E-Business Suite instance in a profile option, then you can enter the internal name of that profile option in the Override Value field. In this case the current value of the specified profile option will be used as the server host URL.

    > **Note:** To allow access from mobile apps to Oracle E-Business Suite over the Internet, you must set the service endpoint to the external web entry point of your DMZ configuration.
    >
    > Additionally, if you are accessing the Configure Mobile Applications page from your intranet, then the current value of the APPS_FRAMEWORK_AGENT profile option, which is the default value for the service endpoint, will be your internal web entry point. In this case, to allow access over the Internet, you must manually specify an override value for the parameter to set it to the external web entry point.
    >
    > Consequently, ensure that the Server URL entered by users to configure the app during the initial login matches the Oracle E-Business Suite web entry URL. Otherwise, Oracle E-Business Suite server might reject the REST requests from the mobile app which will result in redirecting the user to the login screen.

Configuring Parameters for the Web SSO Authentication Type

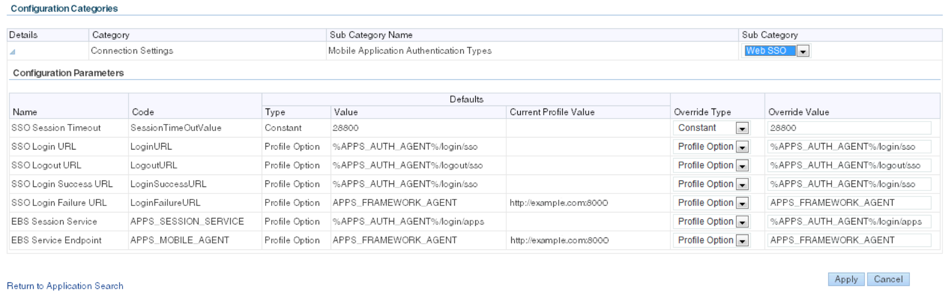
If "Web SSO" is selected as the authentication type, update the following parameter values:

- Select "Web SSO" as the authentication type if you want to delegate authentication to Oracle Access Manager based on a protected Login URL.
- Select "Web SSO" as the authentication type when the mobile app is containerized using Oracle Mobile Security Suite.

- You must apply required patches and perform additional setup tasks to enable this feature.

  See: Additional Setup Tasks to Enable Web SSO Authentication Security, page 2-25.

Configuration Parameters for the Web SSO Authentication Type



Configuration Categories

Details	Category	Sub Category Name	Sub Category
◢	Connection Settings	Mobile Application Authentication Types	Web SSO ▾

Configuration Parameters

		Defaults				
Name	Code	Type	Value	Current Profile Value	Override Type	Override Value
SSO Session Timeout	SessionTimeOutValue	Constant	28800		Constant ▾	28800
SSO Login URL	LoginURL	Profile Option	%APPS_AUTH_AGENT%/login/sso		Profile Option ▾	%APPS_AUTH_AGENT%/login/sso
SSO Logout URL	LogoutURL	Profile Option	%APPS_AUTH_AGENT%/logout/sso		Profile Option ▾	%APPS_AUTH_AGENT%/logout/sso
SSO Login Success URL	LoginSuccessURL	Profile Option	%APPS_AUTH_AGENT%/login/sso		Profile Option ▾	%APPS_AUTH_AGENT%/login/sso
SSO Login Failure URL	LoginFailureURL	Profile Option	APPS_FRAMEWORK_AGENT	http://example.com:8000	Profile Option ▾	APPS_FRAMEWORK_AGENT
EBS Session Service	APPS_SESSION_SERVICE	Profile Option	%APPS_AUTH_AGENT%/login/apps		Profile Option ▾	%APPS_AUTH_AGENT%/login/apps
EBS Service Endpoint	APPS_MOBILE_AGENT	Profile Option	APPS_FRAMEWORK_AGENT	http://example.com:8000	Profile Option ▾	APPS_FRAMEWORK_AGENT

- **SSO Session Timeout (SessionTimeOutValue):** The number of seconds that a user can remain logged in to an app.

  This parameter is specified in seconds, and the minimum value is 300 seconds. The default value is 28800 seconds. After the SSO session expires, the user will be prompted with the SSO login page.

  It is recommended that you set this parameter to a value that is less than the Oracle E-Business Suite session timeout value set in the ICX_SESSION_TIMEOUT profile option. This setting helps avoid issues with REST call failures after the ICX session timeout.

  For example, if the ICX_SESSION_TIMEOUT value is set to 30 minutes, you can set the SSO Session Timeout value to 1740 seconds (29 minutes). After the SSO session expires, the user will be prompted with the SSO login page.

- **SSO Login URL (LoginURL):** This is the login server URL that challenges the user to authenticate with Oracle Access Manager (OAM).

  If the URL is valid, a mobile app displays the login screen where a user enters the credentials for user validation through Oracle Access Manager (OAM).

  This parameter value can be obtained in the following ways:

  - The default value for this parameter is the current value of "%APPS_AUTH_AGENT%/login/sso".

    > **Note:** The convention `%<string>%` is used specifically for parameter values of type "Profile Option" and the value of

which contains content that is in addition to the profile value. For example, the run time value of this SSO Login URL parameter would be "`<profile-value-of-the-APPS_AUTH_AGENT>/login/sso`", where "`/login/sso`" is a constant.

- You can optionally override the default value by selecting an override type and entering a corresponding override value.
  - **Constant:** Enter a constant URL for your Oracle E-Business Suite instance in the Override Value field.
  - **Profile Option:** If you are storing the URL for your Oracle E-Business Suite instance in a profile option, then you can enter the internal name of that profile option in the Override Value field. In this case the current value of the specified profile option will be used as the SSO Login URL.

- **SSO Logout URL (LogoutURL):** This is the server-side URL that logs out a mobile user by terminating the server session from Oracle Access Manager.

  The default value for this parameter is the current value of "%APPS_AUTH_AGENT%/logout/sso". You can optionally override the default value by selecting an override type, Constant or Profile Option, and entering a corresponding override value.

- **SSO Login Success URL (LoginSuccessURL):** This is the URL to redirect a user to a login success page after the user is successfully authenticated from the login page.

  Please note that this URL can be the same as the SSO Login URL. In this release, the same URL is used for this SSO Login Success parameter and the SSO Login URL parameter, and it is the current value of "%APPS_AUTH_AGENT%/login/sso".

- **SSO Login Failure URL (LoginFailureURL):** This is the URL to redirect a user to a login failure page after the authentication fails from the login page. This parameter is reserved for future use.

- **EBS Session Service (APPS_SESSION_SERVICE):** This is the URL to create a session in Oracle E-Business Suite after the mobile user is successfully authenticated against the OAM server.

  The default value for this parameter is the current value of "%APPS_AUTH_AGENT%/login/apps", which is "`<profile-value-of-the-APPS_AUTH_AGENT>/login/apps`", where "

`/login/apps`" is a constant.

You can optionally override the default value by selecting an override type, Constant or Profile Option, and entering a corresponding override value.

- **EBS Service Endpoint (APPS_MOBILE_AGENT):** This is the web entry point that the app uses to invoke Oracle E-Business Suite web services.

  The usage of this parameter is the same as the Service Endpoint parameter described earlier for the HTTP Basic authentication type. See: Service Endpoint (APPS_MOBILE_AGENT), page 2-19.

9. Click the **Apply** button (or the **Save and Generate Files** button in Oracle E-Business Suite Mobile Foundation releases earlier than Release 3.0). This action saves the authentication type and configuration parameters you specified to the database to be used to generate the configuration file `ebs-mobile-config.xml` during the initial launch of the app. When an app is launched for the first time, the selected authentication type along with the configuration parameters will be loaded to the app to connect to an Oracle E-Business Suite instance, invoke configuration service to download configuration data, and invoke Oracle E-Business Suite services with the selected authentication type.

   > **Note:** For Oracle E-Business Suite Mobile Foundation releases earlier than Release 3.0:
   >
   > To generate the configuration file, click the **Save and Generate Files** button instead. This action generates the configuration file based on the configuration template and includes the updated parameter values you entered.
   >
   > If you are updating an existing configuration file, then the **Save and Regenerate Files** button appears instead. Clicking the button regenerates the file based on the updated parameter values for your app.

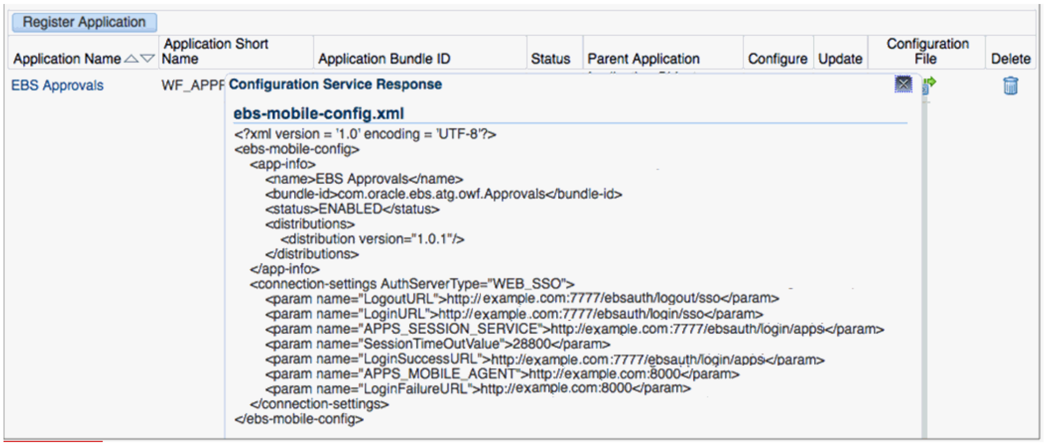
To validate the configuration, click the **Configuration File** icon from the search result table. See: Viewing and Validating Your Mobile App Configuration, page 2-24.

On the client side, once the configuration file is downloaded from the server to the mobile app during the initial login, it will be parsed to retrieve the configuration parameters. The app user can view the downloaded parameters and connection details from the mobile app in the device. Additionally, the user can check if any new updates from the server are required in the app. For example, an administrator changes the timeout values or the service endpoint for an app, or an app's server-side patch provides additional features that require the user to check for updates as described in the patch readme. In these situations, the administrator can direct users to initiate the server updates for the app from their mobile devices. See Directing Users to Obtain Connection Details and Initiate Server Updates, page 7-6.

Viewing and Validating Your Mobile App Configuration

After configuring a mobile app and applying the changes, you can view and validate the updated configuration file `ebs-mobile-config.xml` for the app.

To validate the configuration, click the **Configuration File** icon from the search result table in the Search Mobile Applications page. This displays the content of the configuration file in the Configuration Service Response pop-up window.



Register Application

Application Name	Application Short Name	Application Bundle ID	Status	Parent Application	Configure	Update	Configuration File	Delete
EBS Approvals	WF_APPF							

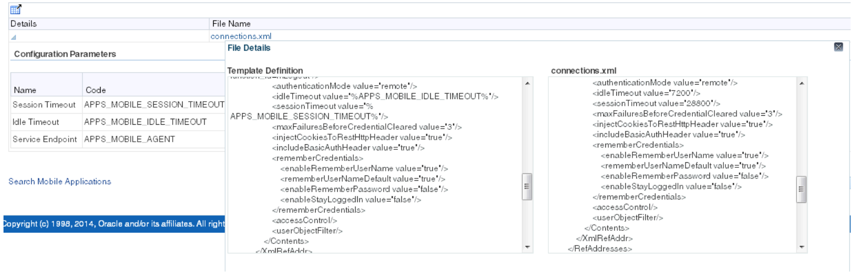
Configuration Service Response

ebs-mobile-config.xml

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<ebs-mobile-config>
   <app-info>
      <name>EBS Approvals</name>
      <bundle-id>com.oracle.ebs.atg.owf.Approvals</bundle-id>
      <status>ENABLED</status>
      <distributions>
         <distribution version="1.0.1"/>
      </distributions>
   </app-info>
   <connection-settings AuthServerType="WEB_SSO">
      <param name="LogoutURL">http://example.com:7777/ebsauth/logout/sso</param>
      <param name="LoginURL">http://example.com:7777/ebsauth/login/sso</param>
      <param name="APPS_SESSION_SERVICE">http://example.com:7777/ebsauth/login/apps</param>
      <param name="SessionTimeOutValue">28800</param>
      <param name="LoginSuccessURL">http://example.com:7777/ebsauth/login/apps</param>
      <param name="APPS_MOBILE_AGENT">http://example.com:8000</param>
      <param name="LoginFailureURL">http://example.com:8000</param>
   </connection-settings>
</ebs-mobile-config>
```

Additionally, you can validate the configuration by accessing the configuration service URL through a web browser. See Validating the Configuration, page 2-32.

> **Note:** The **Configuration File** icon is only available in Oracle E-Business Suite Mobile Foundation Release 3.0 and onwards.
>
> For Oracle E-Business Suite Mobile Foundation releases earlier than Release 3.0, to view the generated file, select the `connections.xml` link from the Configuration Files region to display the configuration file details.



Details	File Name
	connections.xml

Configuration Parameters

Name	Code
Session Timeout	APPS_MOBILE_SESSION_TIMEOUT
Idle Timeout	APPS_MOBILE_IDLE_TIMEOUT
Service Endpoint	APPS_MOBILE_AGENT

Search Mobile Applications

Copyright (c) 1998, 2014, Oracle and/or its affiliates. All right

File Details

Template Definition

```
            <authenticationMode value='remote'/>
            <idleTimeout value='%APPS_MOBILE_IDLE_TIMEOUT%'/>
            <sessionTimeout value='%
APPS_MOBILE_SESSION_TIMEOUT%'/>
            <maxFailuresBeforeCredentialCleared value='3'/>
            <injectCookiesToRestHttpHeader value='true'/>
            <includeBasicAuthHeader value='true'/>
            <rememberCredentials>
               <enableRememberUserName value='true'/>
               <rememberUserNameDefault value='true'/>
               <enableRememberPassword value='false'/>
               <enableStayLoggedIn value='false'/>
            </rememberCredentials>
            <accessControl/>
            <userObjectFilter/>
         </Contents>
      </XmlRefAddr>
```

connections.xml

```
            <authenticationMode value='remote'/>
            <idleTimeout value='7200'/>
            <sessionTimeout value='28800'/>
            <maxFailuresBeforeCredentialCleared value='3'/>
            <injectCookiesToRestHttpHeader value='true'/>
            <includeBasicAuthHeader value='true'/>
            <rememberCredentials>
               <enableRememberUserName value='true'/>
               <rememberUserNameDefault value='true'/>
               <enableRememberPassword value='false'/>
               <enableStayLoggedIn value='false'/>
            </rememberCredentials>
            <accessControl/>
            <userObjectFilter/>
         </Contents>
      </XmlRefAddr>
   </RefAddresses>
```

> To validate the configuration for your app in releases earlier than Oracle E-Business Suite Mobile Foundation Release 3.0, you must follow the validation instructions by accessing the configuration service URL as described in Validating the Configuration, page 2-32.

Reviewing Your Mobile App Details

You can review existing application definition metadata and configuration details for your app if needed before or after configuring your app.

To view the app details, click a desired mobile app's Application Name link from the search result table. The Application Details page displays the existing definition information in read-only mode for your selected app.

For example, click the "EBS Approvals" link to view the Application, Distributions, and Configuration regions in the Application Details page for Oracle Mobile Approvals for Oracle E-Business Suite.

- **Application Region**

  This region includes the selected app status, and application metadata information, such as application short name, application name, application type, parent application name, application bundle Id, and display type.

  The Status field indicates the current app condition whether if it is enabled, disabled, or not configured. Note that by default "Not Configured" is selected. To enable the app, you must update the status from "Not Configured" to "Enabled" and configure your app. For information on configuring your app, see Enabling and Configuring a Mobile App Individually, page 2-14.

- **Distributions Region**

  This region describes the information about service version and distribution platform such as Android, iOS, or both, for the selected app.

- **Configuration Region**

  If the selected mobile app is enabled and configured, this region displays the configuration details for the selected app. It includes the desired authentication type and the associated configuration parameters for the app.

To update the selected mobile app details, click the **Update** button. See: Updating a Mobile App Definition, page 3-13.

Additional Setup Tasks to Enable Web SSO Authentication Security

To support the "Web SSO" authentication type in Oracle E-Business Suite Mobile Foundation Release 4.0, in addition to integrating Oracle E-Business Suite with Oracle Access Manager for single sign-on, you must perform additional setup tasks to enable the feature.

For Oracle E-Business Suite Release 12.1.3

1. Download patch 21522495 to uptake the latest Oracle E-Business Suite AccessGate application.

2. Deploy the Oracle E-Business Suite AccessGate application by following the setup and configuration instructions in My Oracle Support Knowledge Document 1484024.1, *Integrating Oracle E-Business Suite Release 12 with Oracle Access Manager 11gR2 (11.1.2) using Oracle E-Business Suite AccessGate*.

3. After the Oracle E-Business Suite AccessGate application is successfully deployed, perform the following steps to define a public policy to make the `/accessgate/logout/sso` service to be publicly invokable:

   1. Log in to the Oracle Access Manager Console (`http://<hostname>:<port>/oamconsole`).

   2. Under the Launch Pad tab, navigate to **Access Manager** and then select **Application Domain**. In the Search Application Domains page, search and locate the identifier for your WebGate.

   3. Select the identifier for your WebGate from the application domain search result table.

   4. Click the Resources tab.

   5. Click the **New Resource** button in the Resources tab.

   6. Enter the following information in the Create Resources region to define a resource in an application domain:

      - Type: HTTP

      - Description: Logout service for mobile

      - Host Identifier: Enter the identifier for your WebGate

      - Resource URL: Enter the URL in the following format:

        `/{CONTEXT_ROOT}/logout/sso`

      - Protection Level: Unprotected

      - Authentication Policy: Public Resource Policy

      - Authorization Policy: Protected Resource Policy

   7. Click **Apply**.

      You should be able to access the newly-created public resource and verify the functionality.

4. **Enabling the feature on an SSL-based Oracle E-Business Suite environment**

If your Oracle E-Business Suite instance is SSL enabled, import the root-CA certificates from the Oracle HTTP Server (OHS) wallet and Oracle SSL CA certificates into the truststore of the managed server where the Oracle E-Business Suite AccessGate application is deployed.

For information on obtaining private keys, digital certificates, and trusted certificate authority (CA) certificates, see Configuring Identity and Trust, *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

For Oracle E-Business Suite Release 12.2

1. Uptake the latest version of Oracle E-Business Suite AccessGate application (rehosted on Oracle E-Business Suite through patch 21523147:R12.TXK.C).

2. Deploy the Oracle E-Business Suite AccessGate application by following the setup and configuration instructions in My Oracle Support Knowledge Document 1576425.1, *Integrating Oracle E-Business Suite Release 12.2 with Oracle Access Manager 11gR2 (11.1.2) using Oracle E-Business Suite AccessGate*.

   If you have already deployed an earlier version of the Oracle E-Business Suite AccessGate application, refer to section 8.2 Oracle E-Business Suite AccessGate Upgrade, My Oracle Support Knowledge Document 1576425.1.

3. After the Oracle E-Business Suite AccessGate application is successfully deployed, define a public policy to make the `/accessgate/logout/sso` service to be publicly invokable.

   Please note that the new resource `/accessgate/logout/sso` has been added to the public resources defined in the AutoConfig template `ebs_oam_uri_conf.tmp` , and will be automatically configured when you register Oracle E-Business Suite with Oracle Access Manager.

   If you have already registered Oracle E-Business Suite with Oracle Access Manager for single sign-on prior to setting up Oracle E-Business Suite Mobile Foundation Release 4.0, then you need to re-register Oracle E-Business Suite, and include an additional parameter `-policyUpdate=yes`. This adds the newly-defined public resource `/accessgate/logout/sso` to your configuration.

   To achieve this, follow the registration instructions as documented in section 4.2 Register Oracle E-Business Suite with Oracle Access Manager, My Oracle Support Knowledge Document 1576425.1, but add an additional command line parameter `-policyUpdate=yes` as shown in the following example:

   ```
   txkrun.pl -script=SetOAMReg -registeroam=yes -policyUpdate=yes \
   -oamHost=http://myoam.example.com:7001 \
   -oamUserName=weblogic \
   -ldapUrl=ldap://myoid.example.com:3060 \
   -oidUserName=cn=orcladmin \
   -skipConfirm=yes \
   -ldapSearchBase=cn=Users,dc=example,dc=com \
   -ldapGroupSearchBase=cn=Groups,dc=example,dc=com
   ```

4. **Enabling the feature on an SSL-based Oracle E-Business Suite environment**

   If your Oracle E-Business Suite instance is SSL enabled, perform the following tasks:

   1. Import the root-CA certificates from the OHS wallet into the truststore of the OAEA managed server where the Oracle E-Business Suite AccessGate application is deployed, if the root-CA certificates have not already been imported.

      > **Note:** When the OAEA managed server is isolated from the oacore server, it is required to import the certificate into the truststore of the OAEA server.

      The default truststore or keystore for the managed server is at: `<s_fmw_jdkto>/jre/lib/security/cacerts`

      For information on importing the certificates into the truststore, see Section 3.9 Update the JDK Cacerts File, My Oracle Support Knowledge Document 1367293.1, *Enabling SSL or TLS in Oracle E-Business Suite Release 12.2*.

   2. If your Oracle Fusion Middleware version is earlier than 11.1.1.9, then you must enable JSSE SSL in the Oracle E-Business Suite context file. This step is required for the Oracle Workflow Status Monitor to be displayed. Use Oracle Applications Manager to update the Oracle E-Business Suite context file.

      Prerequisites: Review My Oracle Support Knowledge Document 1617461.1, *Applying the Latest AD and TXK Release Update Packs to Oracle E-Business Suite Release 12.2*, and follow the instructions to apply the required codelevel of AD and TXK for your system.

      1. Log in to Oracle E-Business Suite as a system administrator.

      2. Navigate to System Administration. Select **Oracle Applications Manager**, and then **AutoConfig**.

      3. Select the application tier context file, and choose Edit Parameters.

      4. Search for the `s_enable_jsse` variable by selecting OA_VAR in the search list of values and entering `s_enable_jsse` in the search text box. Choose the **Go** button.

      5. By default, the `s_enable_jsse` variable is set to false. Change this value to true to enable JSSE SSL. Refer to the description of the context variable for more information.

      6. Choose the **Save** button.

      7. Enter a reason for the update, such as Enabling JSSE SSL. Then choose the

OK button.

8. Execute AutoConfig and restart all application tier services. For more information about AutoConfig, see: Technical Configuration, *Oracle E-Business Suite Setup Guide*.

Enabling and Setting Up Multiple Mobile Apps Using a Script

Instead of enabling and specifying the configuration information for each app one at a time through the Mobile Applications Manager UI pages, you can complete the setup tasks for multiple apps simultaneously by using an ant script called `EBSMblConfigApps.xml`. For example, use the script to easily copy the configuration details for your apps on different Oracle E-Business Suite instances, or use the script to reconfigure the mobile apps on the target environment after cloning.

Perform the following steps to configure multiple apps at the same time by using the script:

1. Copy the template file `Applications.xml` from the `$JAVA_TOP/oracle/apps/fnd/mobile/ant/` directory to a temporary directory in the Oracle E-Business Suite instance. Working with a copy helps you avoid changes to the seeded template file `Applications.xml`.

   The template file `Applications.xml` contains metadata for all the Oracle E-Business Suite mobile apps. The following example shows a sample template `Applications.xml` file:

   > **Note:** In Oracle E-Business Suite Mobile Foundation Release 4.0, the script supports the selection of the Sub Category (`<sub-category>`) attribute for a desired authentication type for a mobile app.

```
<applications configureAll="N">
  <application configure="N">
   <app-info>
    <name>EBS Approvals</name>
    <app-short-name>WF_APPROVALS</app-short-name>
    <bundle-id>com.oracle.ebs.atg.owf.Approvals</bundle-id>
    <status>NOT_CONFIGURED</status>
   </app-info>
   <connection-settings>
    <sub-category name="HTTP_BASIC" select="Y">
     <param name="APPS_MOBILE_IDLE_TIMEOUT" type="SERVER_DEFAULT"/>
     <param name="APPS_MOBILE_SESSION_TIMEOUT"
type="SERVER_DEFAULT"/>
     <param name="APPS_MOBILE_AGENT" type="SERVER_DEFAULT"/>
    </sub-category>
    <sub-category name="WEB_SSO" select="N">
     <param name="APPS_MOBILE_AGENT" type="SERVER_DEFAULT"/>
     <param name="APPS_SESSION_SERVICE" type="SERVER_DEFAULT"/>
     <param name="LoginFailureURL" type="SERVER_DEFAULT"/>
     <param name="LoginSuccessURL" type="SERVER_DEFAULT"/>
     <param name="LoginURL" type="SERVER_DEFAULT"/>
     <param name="LogoutURL" type="SERVER_DEFAULT"/>
     <param name="SessionTimeOutValue" type="SERVER_DEFAULT"/>
    </sub-category>
   </connection-settings>
    </application>
  ...
 </applications>
```

2. To configure all the Oracle E-Business Suite mobile apps at the same time, set the attribute `ConfigureAll` in the `Applications.xml` file to `Y` at the root element (applications) level. Otherwise, leave the `ConfigureAll` attribute to `N` and set the `Configure` attribute to `Y` at the applications level for each particular app that you want to configure.

   - If you set the `ConfigureAll` attribute to `Y`, and set the "Configure" attribute to `N` for an app at the application level, the `ConfigureAll` attribute set to `Y` at the root element will override the value set at the `Configure` attribute and will configure all the Oracle E-Business Suite mobile apps.

     Note that the `ConfigureAll` attribute with its value set to `Y` at the root element level only configures all the apps whose definitions exist in the instance. If the definition of an app, (for example, the Timecards app) does not exist in that instance, even thought you set the `ConfigureAll` attribute to `Y`, only those apps that are defined in the instance will be configured, and the Timecards app will not be configured. An appropriate message would be shown as the output of the script indicating the result.

   - If the `ConfigureAll` attribute is set to `N`, then the attribute of each individual app determines if the app will be configured or not depending on whether you set the `Configure` attribute to `Y` or `N` for each app at the application level. In this situation, only the specified apps will be configured.

3. For each app you want to configure, change the status from the default

"NOT_CONFIGURED" to "ENABLED".

4. For each app you want to configure, set the `select` attribute for the desired authentication type. By default, the `select` attribute for the "HTTP_BASIC" type is set to `Y`.

   > **Note:** If the `select` attribute for the "WEB_SSO" type is set to `Y`, you must set the `select` attribute for the "HTTP_BASIC" type to `N`. If both types are set to `Y`, then the following errors may occur:
   >
   > ```
   > [java] There are two Authentication types selected for
   > the Application, <name> (such as EBS Approvals).
   > [java] There can be only one type of authentication
   > selected while configuring <name>.
   > ```

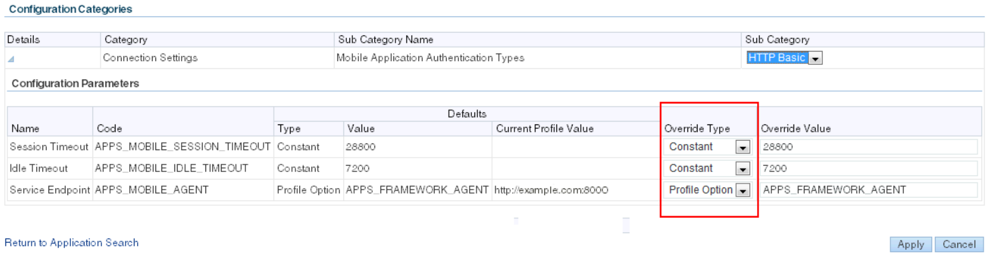
5. Set each parameter `type` attribute to one of the following values only.

   - **SERVER_DEFAULT:** The default value of the parameter is used to configure the app. For example, 28800 is the server default for Session Timeout parameter.

   - **CONSTANT:** A constant override value is used to replace the default value for the parameter. In this situation, provide a value for that parameter, such as a constant URL for your Oracle E-Business Suite instance as a constant value for the APPS_MOBILE_AGENT parameter.

   - **PROFILE_OPTION:** A profile option is used to override the default value for the parameter. For example, provide the internal name of a profile option for the APPS_MOBILE_AGENT parameter.

   The options listed above are the same as those are shown in the Configuration Parameters region if you configure the app from the Mobile Applications Manager UI pages.



Configuration Categories

Details	Category	Sub Category Name	Sub Category
	Connection Settings	Mobile Application Authentication Types	HTTP Basic ▾

Configuration Parameters

		Defaults				
Name	Code	Type	Value	Current Profile Value	Override Type	Override Value
Session Timeout	APPS_MOBILE_SESSION_TIMEOUT	Constant	28800		Constant ▾	28800
Idle Timeout	APPS_MOBILE_IDLE_TIMEOUT	Constant	7200		Constant ▾	7200
Service Endpoint	APPS_MOBILE_AGENT	Profile Option	APPS_FRAMEWORK_AGENT	http://example.com:8000	Profile Option ▾	APPS_FRAMEWORK_AGENT

   The following example shows a sample custom template `Applications.xml` file after setting the parameters with the HTTP Basic authentication type:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<applications configureAll="N">
  <application configure="Y">
   <app-info>
    <name>EBS Approvals</name>
    <app-short-name>WF_APPROVALS</app-short-name>
    <bundle-id>com.oracle.ebs.atg.owf.Approvals</bundle-id>
    <status>ENABLED</status>
   </app-info>
   <connection-settings>
    <sub-category name="HTTP_BASIC" select="Y">
     <param type="SERVER_DEFAULT" name="APPS_MOBILE_IDLE_TIMEOUT"/>
     <param type="CONSTANT"
name="APPS_MOBILE_SESSION_TIMEOUT">28800</param>
     <param type="PROFILE_OPTION"
name="APPS_MOBILE_AGENT">APPS_FRAMEWORK_AGENT</param>
    </sub-category>
   </connection-settings>
    </application>
```

6. After completing the changes in the template file `Applications.xml`, execute the following command from the folder where the template file is placed to initiate the configuration process.

   ```
   ant -f EBSMblConfigApps.xml
   ```

   If any validation error occurs during the configuration process, the error information will be reported in the command line. Additionally, an error log file `EBSMblConfigError.log` is created in the same directory to capture other types of errors. You can use the generated log file to trace and troubleshoot the errors if needed.

   When the process is completed successfully, you can verify the configuration details as described in Validating the Configuration, page 2-32 or validate the configuration from the Mobile Applications Manager UI pages.

Validating the Configuration

Once the app-specific configuration parameters are specified, these values are stored on the server and the associated configuration file of the app is not generated at this time. When a user logs in to the app for the first time, the configuration file `ebs-mobile-config.xml` is then generated when requested and downloaded to the mobile app using the configuration service.

To validate the configuration for your app, construct the configuration service URL and verify if the URL is accessible through a web browser.

> **Note:** In Oracle E-Business Suite Mobile Foundation Release 3.0 and onwards, you can also validate the configuration through the Search Mobile Applications UI pages by clicking the **Configuration File** icon from the search result table, as described in Enabling a Mobile App Individually and Specifying the Configuration through the UI, page 2-

11.

For releases earlier than Oracle E-Business Suite Mobile Foundation Release 3.0, the validation is performed only through the configuration service URL in a browser window.

1. Verify if the configuration service URL is accessible through a web browser by performing the following steps:

   1. Construct the configuration service URL in the following format:
      ```
      http(s)://<hostname>:<port>/OA_HTML/RF.jsp?function_id=mCo
      nfig&bundleId=<application bundle
      id>&file=ebs-mobile-config.xml
      ```

      Please note that this step is only for you to validate the configuration service URL for the app, and you should not provide this URL information to the mobile app users.

      For the Application Bundle Id for each app, see Appendix C: Application Definition Metadata, page C-1.

      > **Note:** In Oracle E-Business Suite Mobile Foundation releases earlier than Release 2.1, construct the configuration service URL in the following format instead:
      > ```
      > http(s)://<hostname>:<port>/OA_HTML/config/<ap
      > plication bundle id>/connections.xml
      > ```

   2. Copy the configuration service URL you just constructed and paste it into a browser window. The configuration file is uploaded and displayed in the browser window.

      Please note that in Oracle E-Business Suite Mobile Foundation releases earlier than Release 4.0, after you paste the configuration service URL into a browser window, it is required to validate the Oracle E-Business Suite user name and password before the configuration service uploads the configuration file to the browser window.

      > **Note:** In Oracle E-Business Suite Mobile Foundation releases earlier than Release 2.1, when you test the configuration service URL in the format described in step 1, the URL automatically redirects to the following format:
      > ```
      > http(s)://<hostname>:<port>/OA_HTML/RF.jsp?fun
      > ction_id=mConfig&p1=/<application bundle
      > id>/connections.xml
      > ```
      >
      > Please note that this redirection occurs because Oracle E-Business Suite HTTP server is configured to redirect to the

above RF.jsp URL to fetch the requested configuration file.

The following example shows a sample `ebs-mobile-config.xml` file returned as the response payload for the configuration service:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ebs-mobile-config>
  <app-info>
    <name>EBS Approvals</name>
    <bundle-id>com.oracle.ebs.atg.owf.Approvals</bundle-id>
    <status>ENABLED</status>
    <distributions>
     <distribution version="1.1.0" platform="IOS"/>
    </distributions>
  </app-info>
  <connection-settings>
    <param name="APPS_MOBILE_IDLE_TIMEOUT">7200</param>
    <param name="APPS_MOBILE_SESSION_TIMEOUT">28800</param>
    <param name="APPS_MOBILE_AGENT">example.com:1234</param>
  </connection-settings>
  </ebs-mobile-config>
```

In Oracle E-Business Suite Mobile Foundation Release 2.1 and onwards, a version value used to identify a given app's server level is retrieved from the app's definition metadata and is included in the `ebs-mobile-config.xml` file (as shown above), along with the configuration parameters specified either through the Mobile Applications Manager UI pages or through the script.

3. Verify the content to ensure that the configuration file for your mobile app is valid, well-formed XML, and validate that the configuration parameter values are the same values as configured from the Mobile Applications Manager UI pages or using the script.

2. Install an app on a mobile device and verify if the server URL is accessible through the configuration screen in the mobile app by performing the following configuration steps:

   1. Enter the server URL in the following format:
      `http(s)://<hostname>:<port>`

   2. Check whether the configuration on the device was successful by logging into the app and verifying that you can access the app content.

Please note the difference between the full configuration service URL used for validation in step 1 in this section and the server URL shared with the app users.

For more information about the configuration steps in earlier Oracle E-Business Suite Mobile Foundation releases, see Oracle E-Business Suite Mobile Foundation Release Update History, *Oracle E-Business Suite Mobile Foundation Release Notes*, My Oracle Support Knowledge Document 1642431.1.

Setting Up Mobile App Access to Responsibilities

Oracle E-Business Suite mobile apps use role-based access control to protect mobile app data from unauthorized access.

Most mobile apps have app-specific access roles. Only users who are assigned those app-specific roles can access the corresponding mobile apps. In order for those users to be able to access Oracle E-Business Suite data in a mobile app that invokes REST services, all REST services that the mobile app uses are grouped into a permission set that is then granted to an app-specific access role. To provide the mobile app access capability to existing Oracle E-Business Suite users, you must assign each access role to the responsibilities that you want to associate with the corresponding mobile app. Users who have the predefined mobile app access roles through those responsibilities will have access to the corresponding mobile apps.

> **Note:** Oracle Mobile Approvals for Oracle E-Business Suite does not have an app-specific access role required for users to access the app.

For Oracle E-Business Suite mobile apps, responsibility selection is based on the combination of user role and mobile app. If the mobile app access role is assigned to a single responsibility, then the responsibility is automatically set and selected for a user using that mobile app. If a user has more than one responsibility to which the mobile app access role is assigned, then those responsibilities will be displayed for selection.

Please note that it is not required to create or assign any new responsibility to users to use mobile apps. For information on the app-specific access roles, see Appendix A: Mobile App Access Roles, page A-1.

For information on creating new mobile app access roles for enterprise distribution, see Creating and Using Mobile App Access Roles, page 3-16.

Assigning Mobile App Access Roles to Responsibilities

To secure mobile app data, perform the following steps to assign predefined app-specific mobile app access roles to responsibilities:

1. Log in to Oracle E-Business Suite as a user who has the User Management responsibility. For example, log in as `SYSADMIN`.

   > **Note:** The User Management responsibility is assigned to the Security Administrator role. This seeded role is assigned to the `SYSADMIN` user by default.

2. Select the User Management responsibility and navigate to the Roles and Role Inheritance page.

3. Search for the responsibility you want.

4. In the search results table, click the "View In Hierarchy" icon for your responsibility. Note that the codes for responsibilities start with FND_RESP, while the codes for roles start with `UMX`.

5. In the Role Inheritance Hierarchy, click the **Add Node** icon for your responsibility.

   Oracle User Management displays the next role hierarchy page with a message informing you that the role you select will be inherited. In this page, either search or expand nodes until you find the app-specific access role that you want to add to the responsibility. Use the **Quick Select** icon to choose that role.

6. Oracle User Management then displays the initial page again, with a confirmation message at the top. On this page, verify that the custom UMX role appears underneath the responsibility. You may need to expand one or more nodes to display the UMX role under the responsibility. Any other inherited roles appear as well.

7. When you add the role to the responsibility, you must also update the associated grant for the app-specific access roles to reference the specific responsibility as the security context. You need a separate grant for each responsibility to which you are adding the role, so in some cases you should duplicate the shipped grant rather than updating it.

   In the row of the role that you just added, click the Update icon for your role to navigate to the Update Role page.

8. In the Grants Table at the end of the page, if this is the first responsibility to which you are adding to the role, click the Update icon for the grant you want to update. If this is the second responsibility or more to which you are adding the role, click the Duplicate icon for the grant instead of the Update icon. In the duplicate grant, you must provide a unique name for the grant.

9. Apply your changes.

If you want to use the app-specific access role with more than one responsibility, you must have a separate grant with a security context corresponding to each responsibility. You can also add grants for a given role as a separate process, rather than while you are adding the role to the responsibility. To do so, perform the following steps:

1. In the User Management responsibility, navigate to the Roles and Role Inheritance page.

2. Search for the app-specific access role you want.

3. Click the Update icon for your role to navigate to the Update Role page.

4. In the Grants Table at the end of the page, click the Duplicate icon for the grant you want to duplicate.

5. Modify the grant name of the new grant to make it unique.

6. In the Security Context region, enter the name of the additional responsibility to which you are adding the app-specific access role. Enter the name of a shipped responsibility from the table above, or, if you are using a custom responsibility, enter the name of that custom responsibility.

7. Click Next, Next, Finish, and OK to complete your grant.

For more information, see the *Oracle E-Business Suite Security Guide*.

Additional Setup for Device Integration

This section describes additional setup steps if your mobile app integrates with person contact cards or maps on the mobile devices, and provides details about barcode integration. It includes the following topics:

1. Setting Up Person Contact Cards, page 2-37

2. Setting Up Maps, page 2-50

3. Support for Barcodes, page 2-52

Setting Up Person Contact Cards

Mobile Apps Integrated with Person Contact Cards

The following Oracle E-Business Suite mobile apps integrate with person contact cards:

- Oracle Mobile Sales Orders for Oracle E-Business Suite

- Oracle Mobile iProcurement for Oracle E-Business Suite

- Oracle Mobile Procurement for Oracle E-Business Suite

- Oracle Mobile Project Manager for Oracle E-Business Suite

- Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite

- Oracle Mobile Project Manufacturing for Oracle E-Business Suite

If your mobile app integrates with person contact cards and you would like to show the contact information within the context of the app, perform the setup tasks described in this section:

1. Step 1: Setting Up a Qualifier, page 2-38

2. Step 2: Scheduling the "HR Mobile Utils Person Data Full Synch" Concurrent

Program, page 2-46

3. Step 3: Allowing Apps to Access Local Contacts, page 2-46

Step 1: Setting Up a Qualifier

Setting up a qualifier involves the following key steps:

1. Step 1.1: Creating a Qualifier, page 2-38

2. Step 1.2: Identifying the Flexfield Structure for Your Business Group, page 2-39

3. Step 1.3: Enabling the Qualifier for the Flexfield Segment, *Oracle E-Business Suite Mobile Apps Administrator's Guide*

4. Step 1.4: Adding the "HR Mobile Utils Person Data Full Synch" Concurrent Program to a Request Group, page 2-43

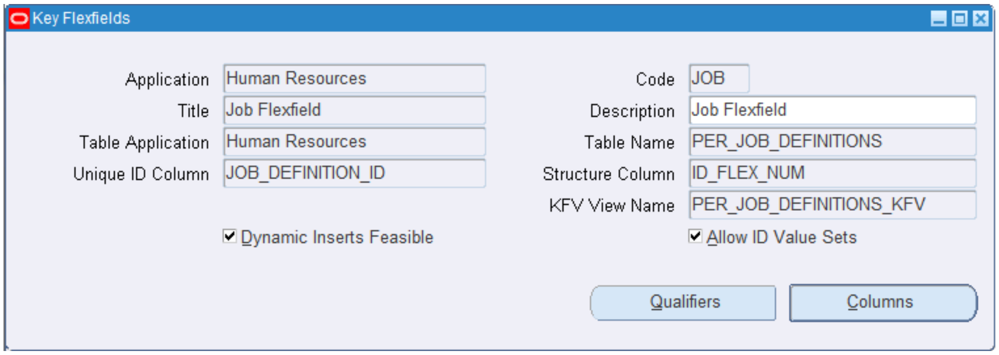
Step 1.1: Creating a Qualifier

Perform the following steps to create a qualifier for a key flexfield:

1. Log in to Oracle E-Business Suite as a user who has access to the Application Developer responsibility. For example, log in as `SYSADMIN`.

2. Select the Application Developer responsibility. Choose the **Flexfield** link, then the **Key** link, and then the **Register** link from the navigator. This displays the Key Flexfields window.

3. In the Key Flexfields window, search for the flexfield with the title "Job Flexfield" and the application name "Human Resources".



Application: Human Resources
Title: Job Flexfield
Table Application: Human Resources
Unique ID Column: JOB_DEFINITION_ID
☑ Dynamic Inserts Feasible

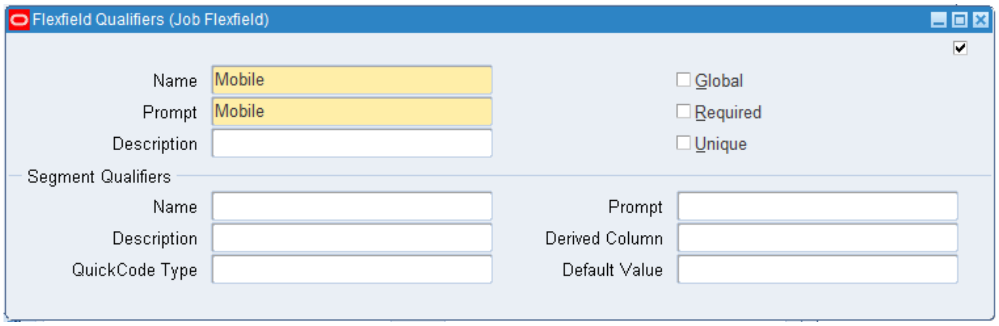
Code: JOB
Description: Job Flexfield
Table Name: PER_JOB_DEFINITIONS
Structure Column: ID_FLEX_NUM
KFV View Name: PER_JOB_DEFINITIONS_KFV
☑ Allow ID Value Sets

4. Click the **Qualifiers** button. Enter the following case sensitive information in the Flexfield Qualifiers window and then save.

   - Name: Mobile

- Prompt: Mobile

- Ensure that the Global, Required, and Unique check boxes are not selected



Flexfield Qualifiers (Job Flexfield)

Name: Mobile

Prompt: Mobile

Description:

□ Global

□ Required

□ Unique

Segment Qualifiers

Name:

Description:

QuickCode Type:

Prompt:

Derived Column:

Default Value:

Step 1.2: Identifying the Flexfield Structure for Your Business Group

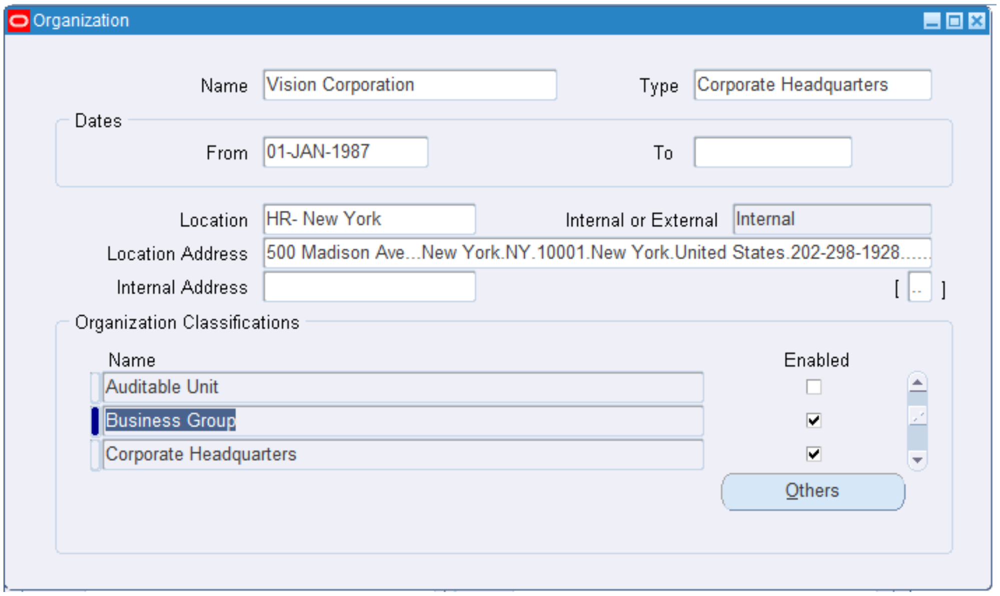
Perform the following steps to identify the flexfield structure for your business group:

1. Log in to Oracle E-Business Suite as a user who has the HRMS Manager responsibility.

2. Select the HRMS Manager responsibility. Choose the **Work Structures** link, then the **Organization** link, and then the **Description** link from the navigator.

3. In the Find Organization window, query your business group in the Name field, such as "Vision Corporation". Click the **Find** button. This displays the Organization window for the selected organization.

4. In the Organization Classifications region, select "Business Group" and click the **Others** button.



Organization

Name: Vision Corporation

Type: Corporate Headquarters

Dates

From: 01-JAN-1987

To:

Location: HR- New York

Internal or External: Internal

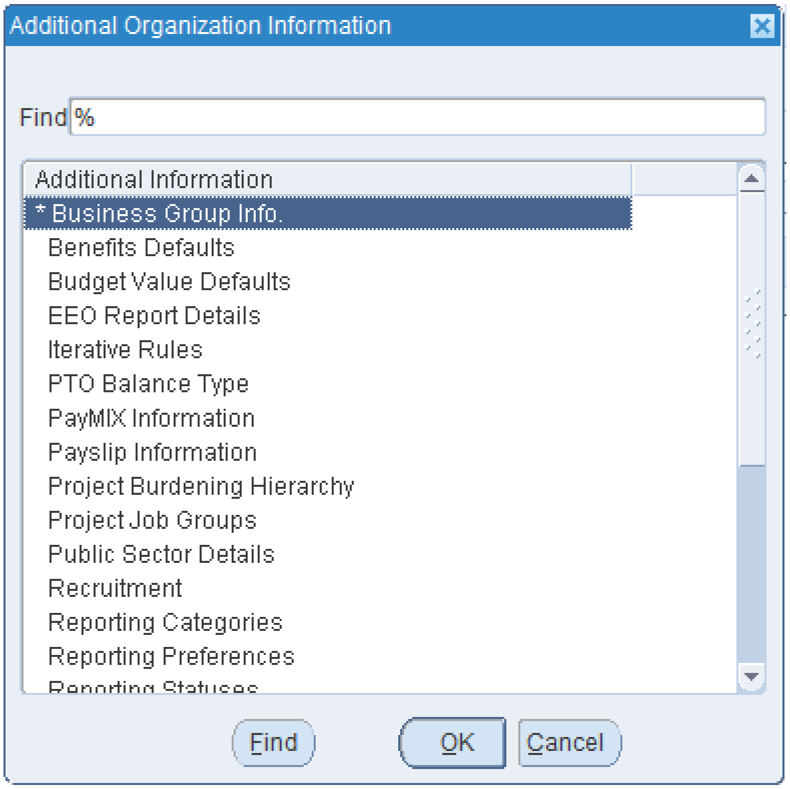
Location Address: 500 Madison Ave...New York.NY.10001.New York.United States.202-298-1928.....

Internal Address:

Organization Classifications

Name	Enabled
Auditable Unit	☐
Business Group	☑
Corporate Headquarters	☑

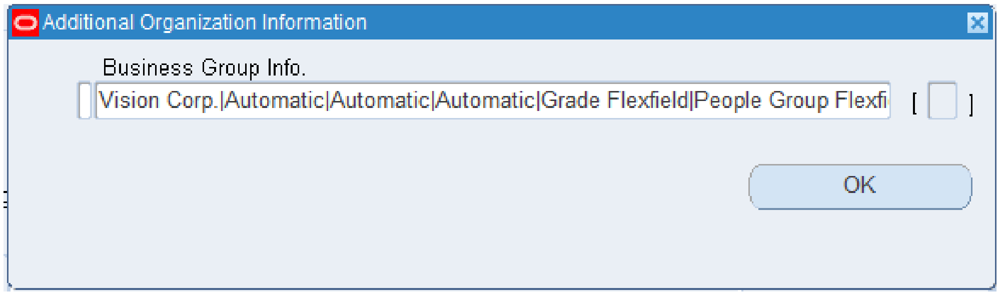
5. The Additional Organization Information window displays. Select "Business Group Info".



Additional Organization Information

Find: %

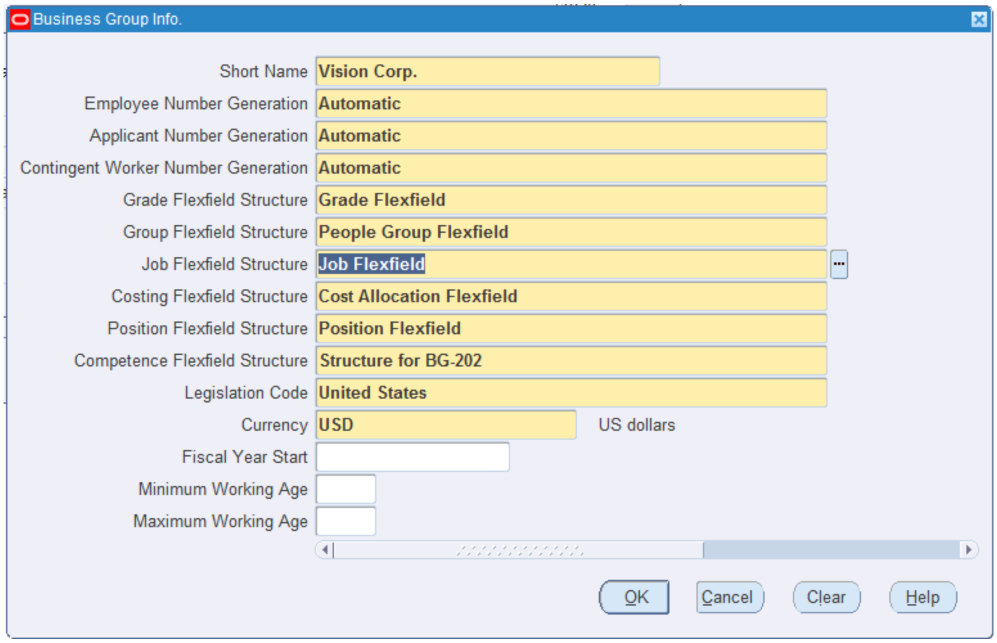
6. Place the cursor in the Business Group Info field.



Business Group Info.

Vision Corp.|Automatic|Automatic|Automatic|Grade Flexfield|People Group Flexfi [ ]

7. The complete Business Group Info window is displayed. This is the structure for the Job Flexfield for your business group. Copy the value in the Job Flexfield Structure field. This value will be used later to locate the flexfield that you want to qualify.



Short Name	Vision Corp.
Employee Number Generation	Automatic
Applicant Number Generation	Automatic
Contingent Worker Number Generation	Automatic
Grade Flexfield Structure	Grade Flexfield
Group Flexfield Structure	People Group Flexfield
Job Flexfield Structure	Job Flexfield
Costing Flexfield Structure	Cost Allocation Flexfield
Position Flexfield Structure	Position Flexfield
Competence Flexfield Structure	Structure for BG-202
Legislation Code	United States
Currency	USD US dollars
Fiscal Year Start	
Minimum Working Age	
Maximum Working Age	

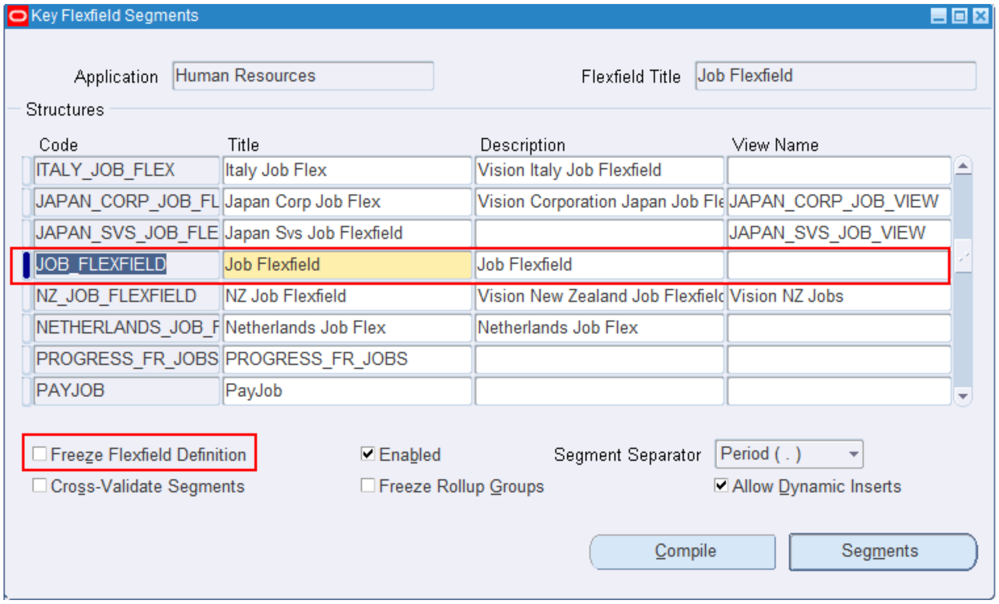
Step 1.3: Enabling the Qualifier for the Flexfield Segment

After obtaining the key flexfield structure name for your business group, perform the following steps to qualify the key flexfield segment:

1. From the navigator, select the **Flexfield** link, then the **Key** link, and then the **Segment** link.

2. In the Key Flexfield Segments window, search for the flexfield with the application name "Human Resources" and the flexfield title that you obtained from the Job Flexfield Structure field described in Step 1.2: Identifying the Flexfield Structure for Your Business Group, page 2-39, such as "Job Flexfield".

3. In the Structures region, select the Job Flexfield and then deselect the Freeze Flexfield Definition check box. This allows you to update the selected Job Flexfield definition. Click the **Segments** button. This displays the Segments Summary window for the selected Job Flexfield.



Key Flexfield Segments

Application: Human Resources

Flexfield Title: Job Flexfield

Structures

Code	Title	Description	View Name
ITALY_JOB_FLEX	Italy Job Flex	Vision Italy Job Flexfield	
JAPAN_CORP_JOB_FL	Japan Corp Job Flex	Vision Corporation Japan Job Fle	JAPAN_CORP_JOB_VIEW
JAPAN_SVS_JOB_FLE	Japan Svs Job Flexfield		JAPAN_SVS_JOB_VIEW
JOB_FLEXFIELD	Job Flexfield	Job Flexfield	
NZ_JOB_FLEXFIELD	NZ Job Flexfield	Vision New Zealand Job Flexfielc	Vision NZ Jobs
NETHERLANDS_JOB_F	Netherlands Job Flex	Netherlands Job Flex	
PROGRESS_FR_JOBS	PROGRESS_FR_JOBS		
PAYJOB	PayJob		

☐ Freeze Flexfield Definition

☑ Enabled

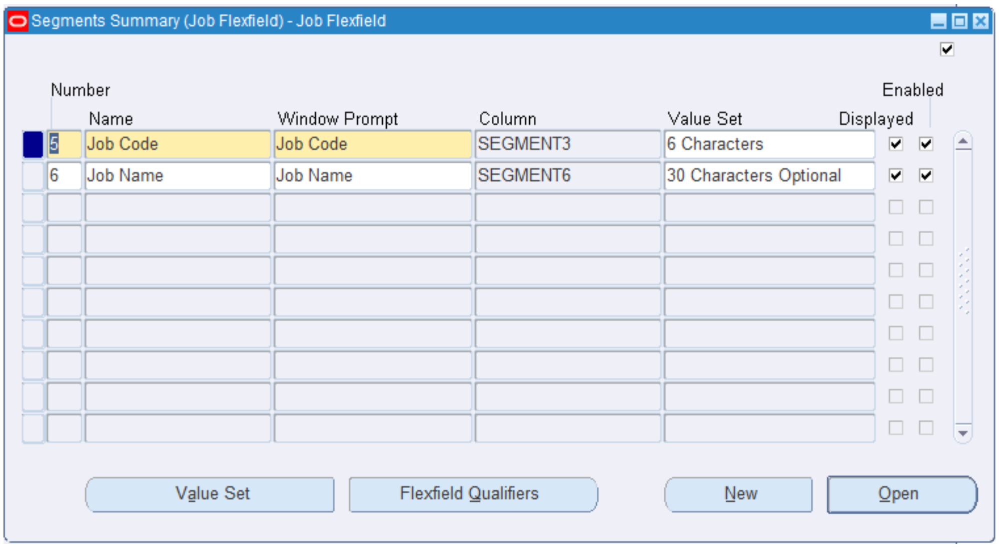
Segment Separator: Period (.)

☐ Cross-Validate Segments

☐ Freeze Rollup Groups

☑ Allow Dynamic Inserts

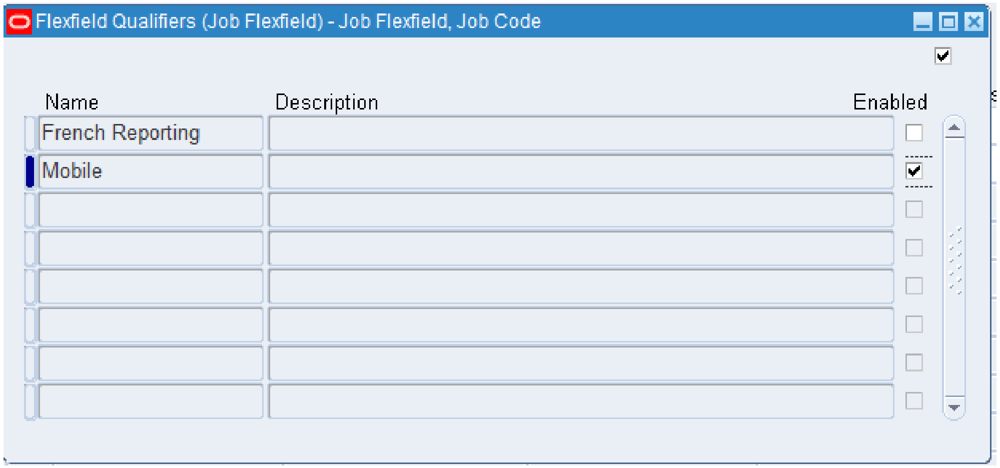
4. Select the segment you want to qualify and click the **Flexfield Qualifiers** button.



Segments Summary (Job Flexfield) - Job Flexfield

Number	Name	Window Prompt	Column	Value Set	Enabled	Displayed
5	Job Code	Job Code	SEGMENT3	6 Characters	☑	☑
6	Job Name	Job Name	SEGMENT6	30 Characters Optional	☑	☑

5. Select the qualifier "Mobile" and then select the **Enabled** check box to enable the selected qualifier for this segment. Save your work.



Flexfield Qualifiers (Job Flexfield) - Job Flexfield, Job Code

☑

Name	Description	Enabled
French Reporting		□
Mobile		☑
		□
		□
		□
		□
		□
		□

Step 1.4: Adding the "HR Mobile Utils Person Data Full Synch" Concurrent Program to a Request Group

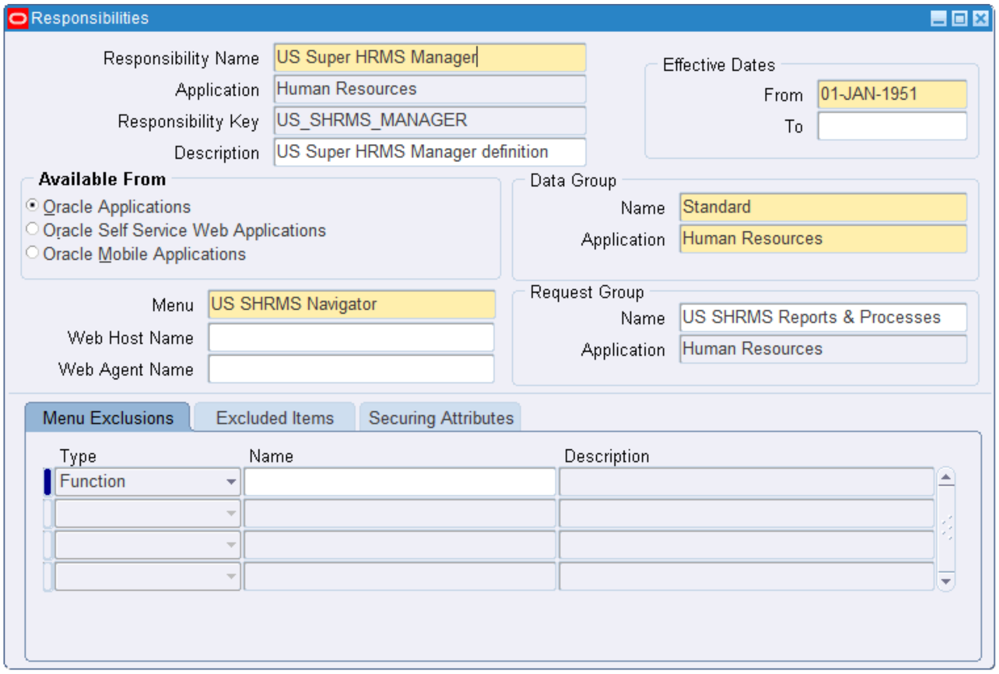
Perform the following steps to add the "HR Mobile Utils Person Data Full Synch" concurrent program to a request group, and then run the program for the first time:

> **Note:** Ensure that you have applied the patches for your app. The "HR Mobile Utils Person Data Full Synch" concurrent program should then be automatically created.
>
> For patch information for each app, see Applying Prerequisite Patches, page 2-2.

1. Log in to Oracle E-Business Suite as a user who has the System Administrator responsibility. For example, log in as `SYSADMIN`.

2. Select the System Administrator responsibility. Choose the **Security** link, then the **Responsibility** link, and then the **Define** link from the navigator. This displays the Responsibilities window.

3. In the Responsibilities window, search for the responsibility, such as "US Super HRMS Manager", that you want to run the "HR Mobile Utils Person Data Full Synch" concurrent program.



Responsibilities

Responsibility Name: US Super HRMS Manager

Application: Human Resources

Responsibility Key: US_SHRMS_MANAGER

Description: US Super HRMS Manager definition

Effective Dates

From: 01-JAN-1951

To:

Available From

● Oracle Applications
○ Oracle Self Service Web Applications
○ Oracle Mobile Applications

Data Group

Name: Standard

Application: Human Resources

Menu: US SHRMS Navigator

Web Host Name:

Web Agent Name:

Request Group

Name: US SHRMS Reports & Processes

Application: Human Resources

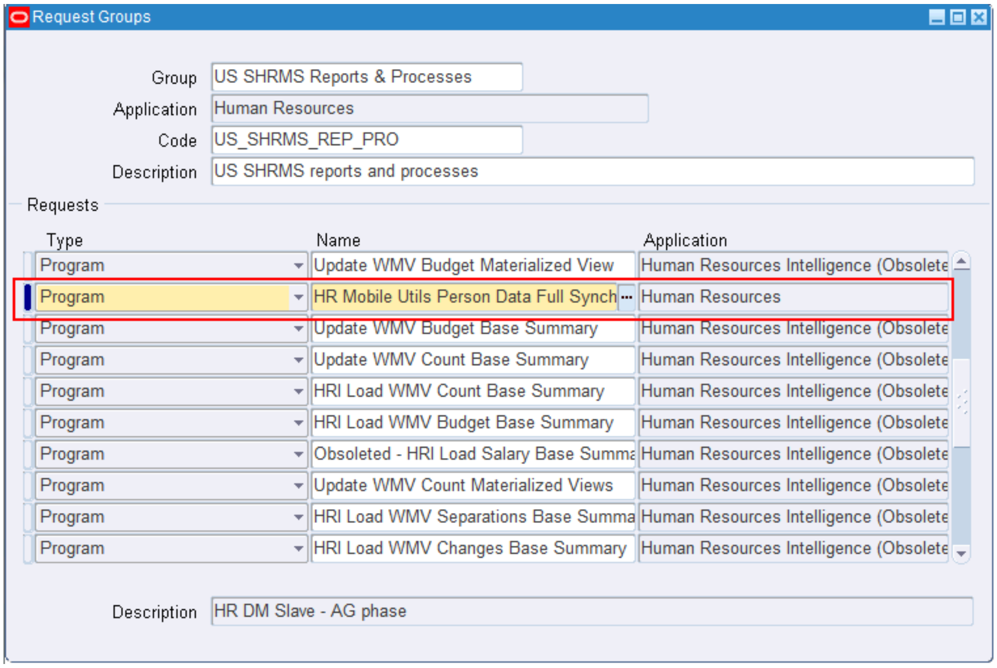
Type	Name	Description
Function		

4. In the Request Group region, record the value of the request group Name field which in this example is "US SHRMS Reports & Processes" for the "US Super HRMS Manager" responsibility. Close the window.

5. From the navigator, select the **Security** link, then the **Responsibility** link, and then the **Request** link. This displays the Request Groups window.

6. In the Request Groups window, search for the request group name "US SHRMS Reports & Processes" you recorded earlier in the Group field.

7. In the Requests region, click the **New** icon to add the "HR Mobile Utils Person Data Full Synch" concurrent program to this security group. Save your entry and close the window.



Request Groups

Group: US SHRMS Reports & Processes

Application: Human Resources

Code: US_SHRMS_REP_PRO

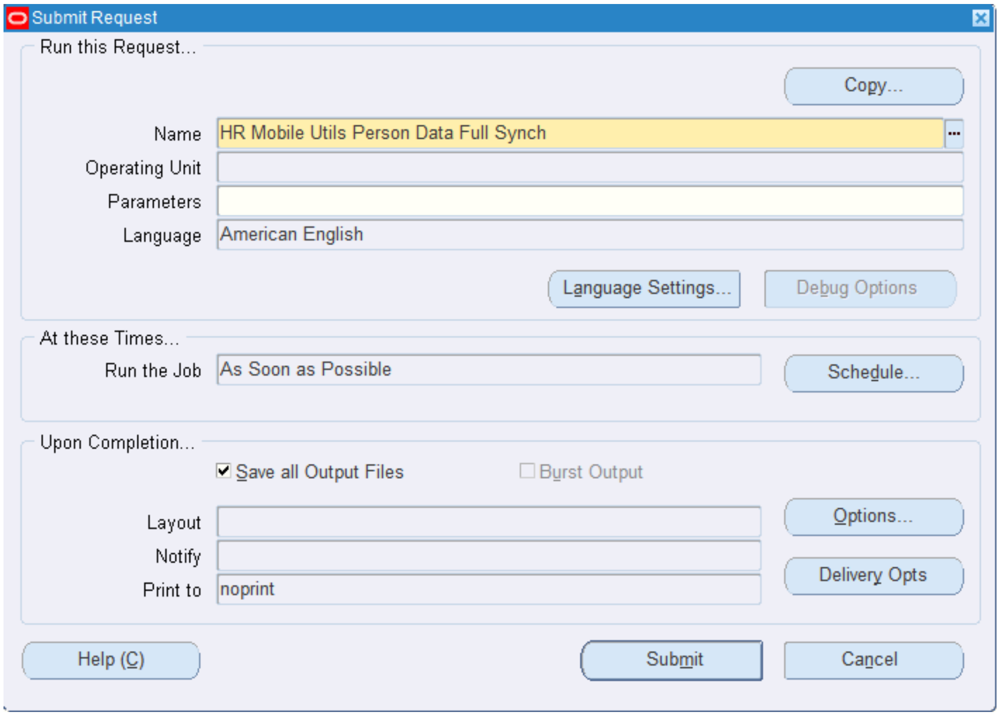
Description: US SHRMS reports and processes

Requests

Type	Name	Application
Program	Update WMV Budget Materialized View	Human Resources Intelligence (Obsolete
Program	HR Mobile Utils Person Data Full Synch	Human Resources
Program	Update WMV Budget Base Summary	Human Resources Intelligence (Obsolete
Program	Update WMV Count Base Summary	Human Resources Intelligence (Obsolete
Program	HRI Load WMV Count Base Summary	Human Resources Intelligence (Obsolete
Program	HRI Load WMV Budget Base Summary	Human Resources Intelligence (Obsolete
Program	Obsoleted - HRI Load Salary Base Summa	Human Resources Intelligence (Obsolete
Program	Update WMV Count Materialized Views	Human Resources Intelligence (Obsolete
Program	HRI Load WMV Separations Base Summa	Human Resources Intelligence (Obsolete
Program	HRI Load WMV Changes Base Summary	Human Resources Intelligence (Obsolete

Description: HR DM Slave - AG phase

8. From the navigator, select the **Requests** link and then the **Run** link. This displays the Submit Request window.



Submit Request

Run this Request...

Name: HR Mobile Utils Person Data Full Synch

Operating Unit:

Parameters:

Language: American English

At these Times...

Run the Job: As Soon as Possible

Upon Completion...

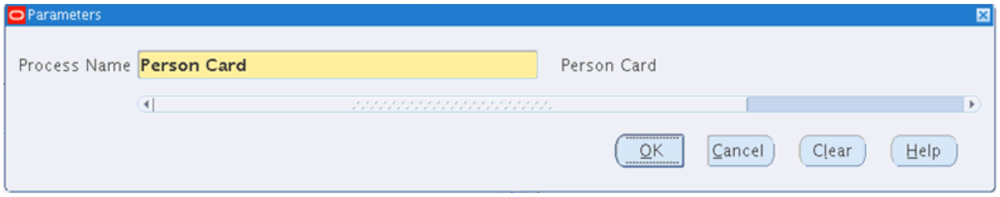
☑ Save all Output Files ☐ Burst Output

Layout:

Notify:

Print to: noprint

9. Enter the "HR Mobile Utils Person Data Full Synch" concurrent program as the request name. The Parameters window appears.



Parameters

Process Name: Person Card — Person Card

10. Select "Person Card" as the Process Name parameter. Click **OK** and **Submit** to execute the request for the first time. This concurrent request refreshes the related HR tables with the person data.

Step 2: Scheduling the "HR Mobile Utils Person Data Full Synch" Concurrent Program

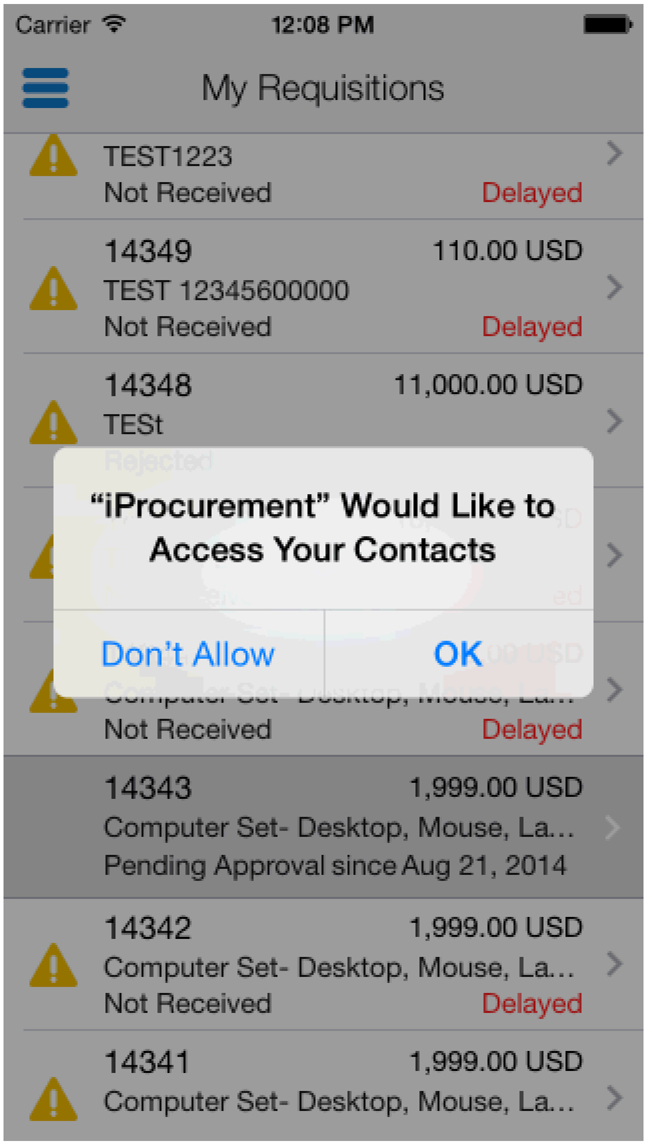
After adding the "HR Mobile Utils Person Data Full Synch" concurrent program to a request group and executing the concurrent request for the first time, you can schedule the concurrent request be run at the desired frequency to refresh the related tables with the latest person data.

Step 3: Allowing Apps to Access Local Contacts

After the setup mentioned above is complete and an iOS mobile user has installed an app that integrates with person contact cards, the first time the user accesses a page that has person contacts embedded within it, the app will request permission to access the user's local contacts on the iOS mobile device.

> **Note:** Unlike iOS mobile users, Android users do not have the option to choose whether or not to grant an app permission to access the local contacts on the devices. While installing an app from Google Play, users must grant the following permissions to the app:
>
> - From the PRIVACY section: read phone status and identity, receive text messages (SMS), modify your contacts, read your contacts, modify or delete the contents of your USB storage, read the contents of your USB storage, and find accounts on the device
> - From the Device Access section: full network access, and view network connections
>
> If a user does not grant these permissions, then the app will not be installed.
>
> After installing the app, users can review the permissions by tapping **Settings**, then **App Name**, and then **Permissions** on their Android devices.

For example, Oracle Mobile iProcurement for Oracle E-Business Suite requests the permission to access the user's local contacts on the iOS device as shown below:



TEST1223
Not Received Delayed

14349 110.00 USD
TEST 12345600000
Not Received Delayed

14348 11,000.00 USD
TESt
Rejected

"iProcurement" Would Like to Access Your Contacts

Not Received Delayed

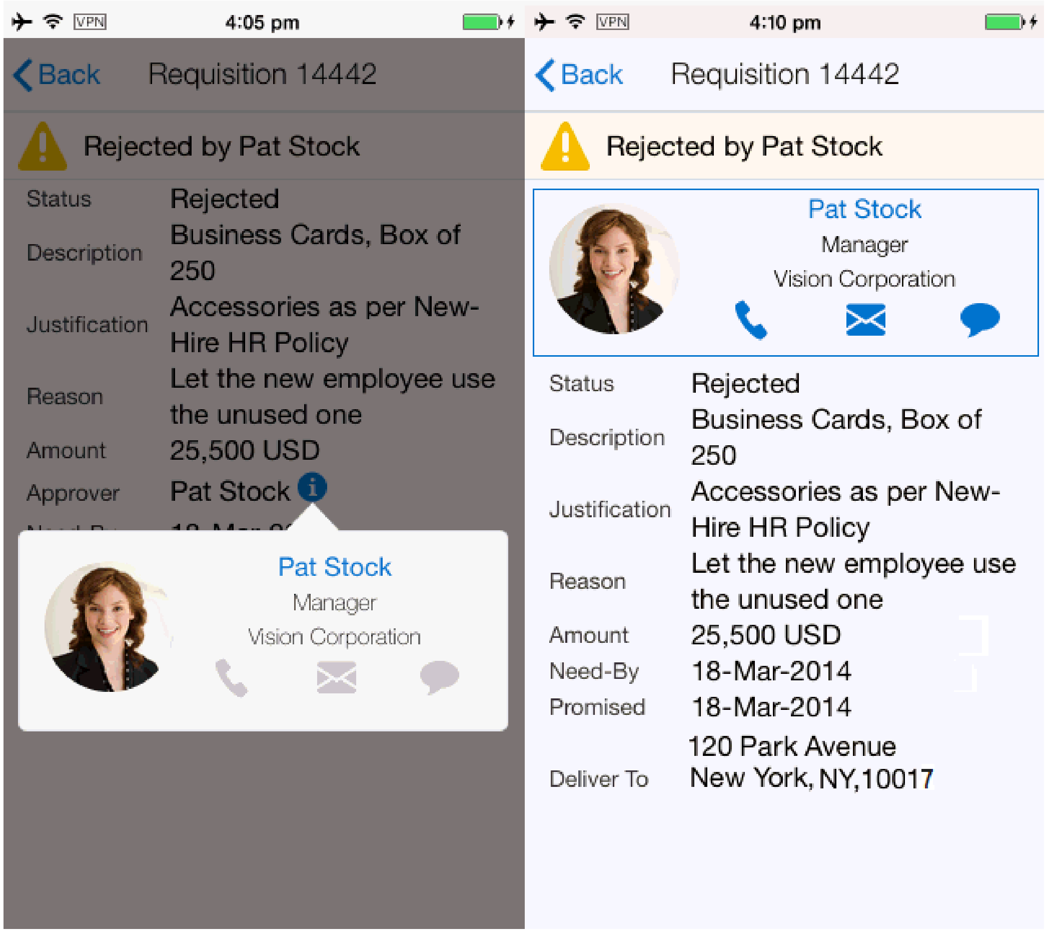
14343 1,999.00 USD
Computer Set- Desktop, Mouse, La...
Pending Approval since Aug 21, 2014

14342 1,999.00 USD
Computer Set- Desktop, Mouse, La...
Not Received Delayed

14341 1,999.00 USD
Computer Set- Desktop, Mouse, La...

> **Note:** iOS mobile users can modify the setting that determines whether the app can access local contacts at any time by tapping **Settings**, then **Privacy**, and then **Contacts** on their iOS devices.

On Android devices, and if the user gives permission on an iOS device, the app will fetch the person information from the local contacts along with the enterprise information from Oracle E-Business Suite as shown below.



4:05 pm

Back Requisition 14442

Rejected by Pat Stock

Status	Rejected
Description	Business Cards, Box of 250
Justification	Accessories as per New-Hire HR Policy
Reason	Let the new employee use the unused one
Amount	25,500 USD
Approver	Pat Stock

Pat Stock
Manager
Vision Corporation

4:10 pm

Back Requisition 14442

Rejected by Pat Stock

Pat Stock
Manager
Vision Corporation

Status	Rejected
Description	Business Cards, Box of 250
Justification	Accessories as per New-Hire HR Policy
Reason	Let the new employee use the unused one
Amount	25,500 USD
Need-By	18-Mar-2014
Promised	18-Mar-2014
Deliver To	120 Park Avenue New York, NY,10017

In this case, the user can also save enterprise contact information to add or update local contacts. If the user does not allow the app to access the local contacts on the iOS device, then the app displays only the enterprise contact information from Oracle E-Business Suite, and the user cannot save this information to the local contacts on the device.

> **Note:** Saving person contacts will not save the person's image to local contacts on the Android devices. The app on Android always displays the images for the person contacts from enterprise contacts. If the image of an enterprise contact is not present, then the app displays the person contact only without the image on the Android devices.

> **Note:** Oracle E-Business Suite mobile apps use the email address for an enterprise contact to determine whether the enterprise contact matches any existing local contact on the device.

Please note that if the setup tasks for person contact cards are not performed properly, depending on how your app is integrated with person contact cards, either the app page that includes person contact (such as the Requisition page shown above) shows a blank page with no data on it or the person contact details (such as the contact details for Pat Stock in this example) are not shown on the page.

For information on setting up person contact cards, see Setting Up Person Contact Cards, page 2-37.

Setting Up Maps

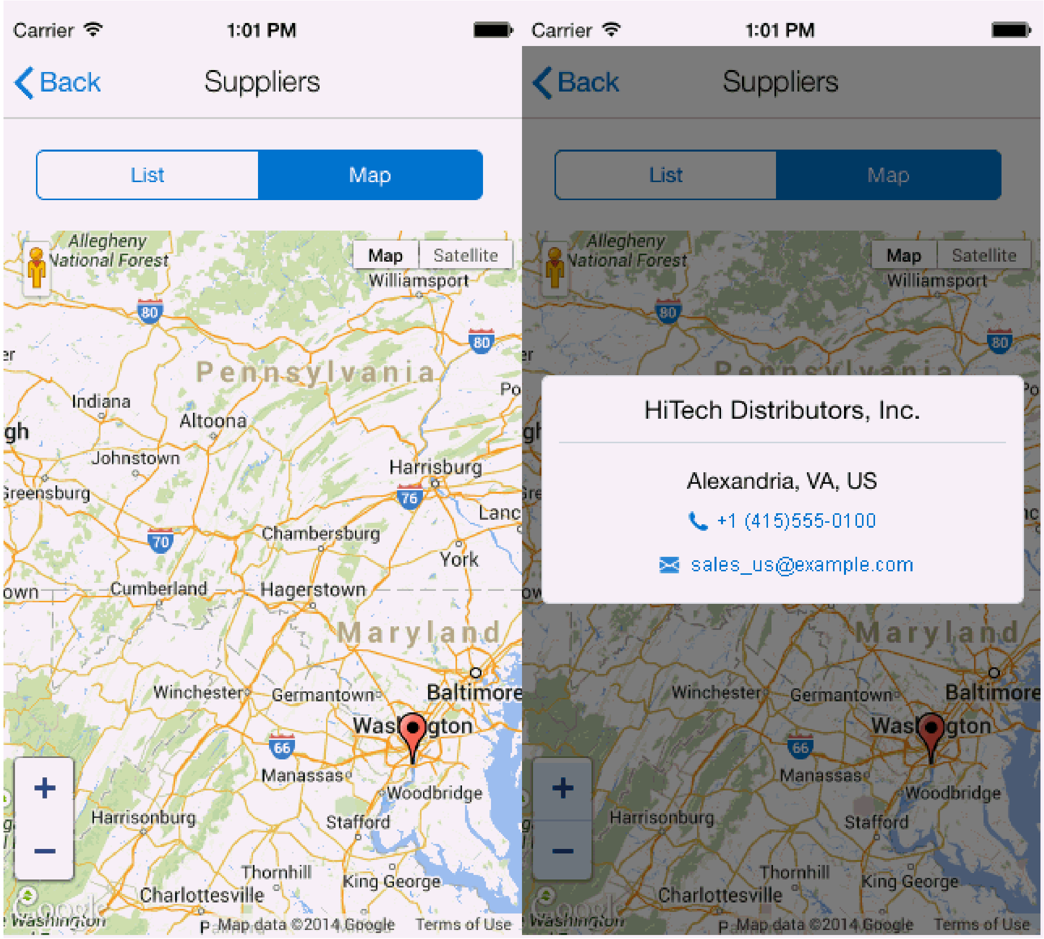
Mobile Apps Integrated with Maps

The following Oracle E-Business Suite mobile apps integrate with maps:

- Oracle Mobile Product Information for Oracle E-Business Suite (Google Maps)
- Oracle Mobile Person Directory for Oracle E-Business Suite (Google Maps)
- Oracle Mobile Maintenance for Oracle E-Business Suite (Oracle Maps)

> **Note:** The Oracle Maps feature is enabled by default; therefore, there is no additional setup required for integrating with Oracle Maps.

For example, Oracle Mobile Product Information for Oracle E-Business Suite presents the supplier information and its geographical location in a Google map as shown below.



HiTech Distributors, Inc.

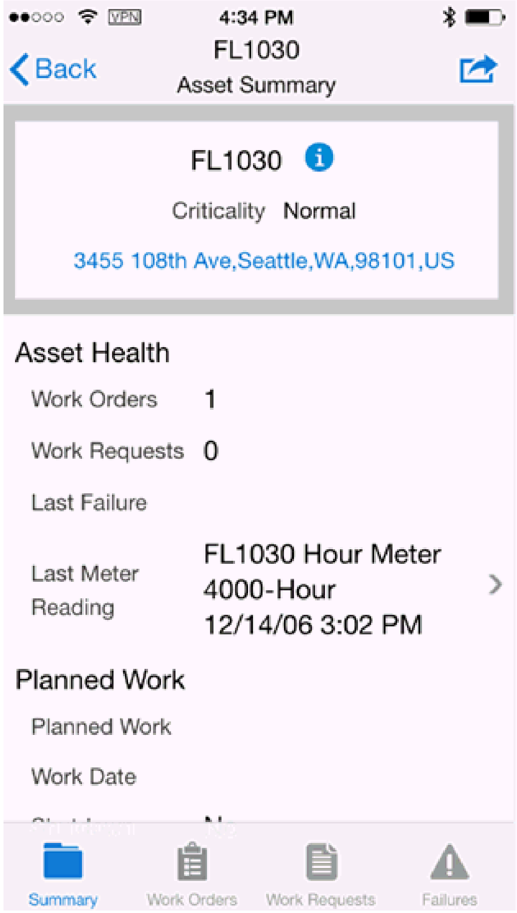
Alexandria, VA, US

☎ +1 (415)555-0100

✉ sales_us@example.com

Note: Any use of this map is subject to Google's Privacy Policy and not Oracle's Privacy Policy.

Oracle Mobile Maintenance for Oracle E-Business Suite presents the asset information and its geographical location in an Oracle map as shown below.



FL1030
Asset Summary

FL1030

Criticality Normal

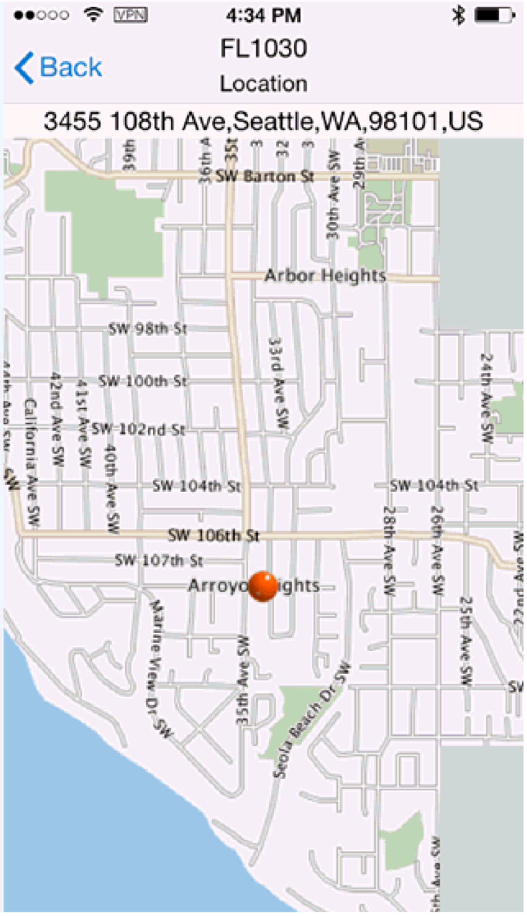
3455 108th Ave,Seattle,WA,98101,US

Asset Health

Work Orders	1
Work Requests	0
Last Failure	
Last Meter Reading	FL1030 Hour Meter 4000-Hour 12/14/06 3:02 PM

Planned Work

Planned Work	
Work Date	



FL1030
Location

3455 108th Ave,Seattle,WA,98101,US

Setting Up Google Maps

To integrate your mobile app with Google Maps, set the "CSF: Google Map Key" profile option value on the Oracle E-Business Suite instance to the Google Map JavaScript API license key. You can obtain this key by registering with Google, Inc.

If you do not provide a license key as the profile value, the map feature in Oracle E-Business Suite mobile apps will be disabled. The app users can view data (such as supplier information as shown in the screenshot) displayed in a list only. If the provided license key is not valid, even though the app displays the map option, the Google map will not be rendered when a user taps the map option. An error message also occurs indicating it is an invalid license key.

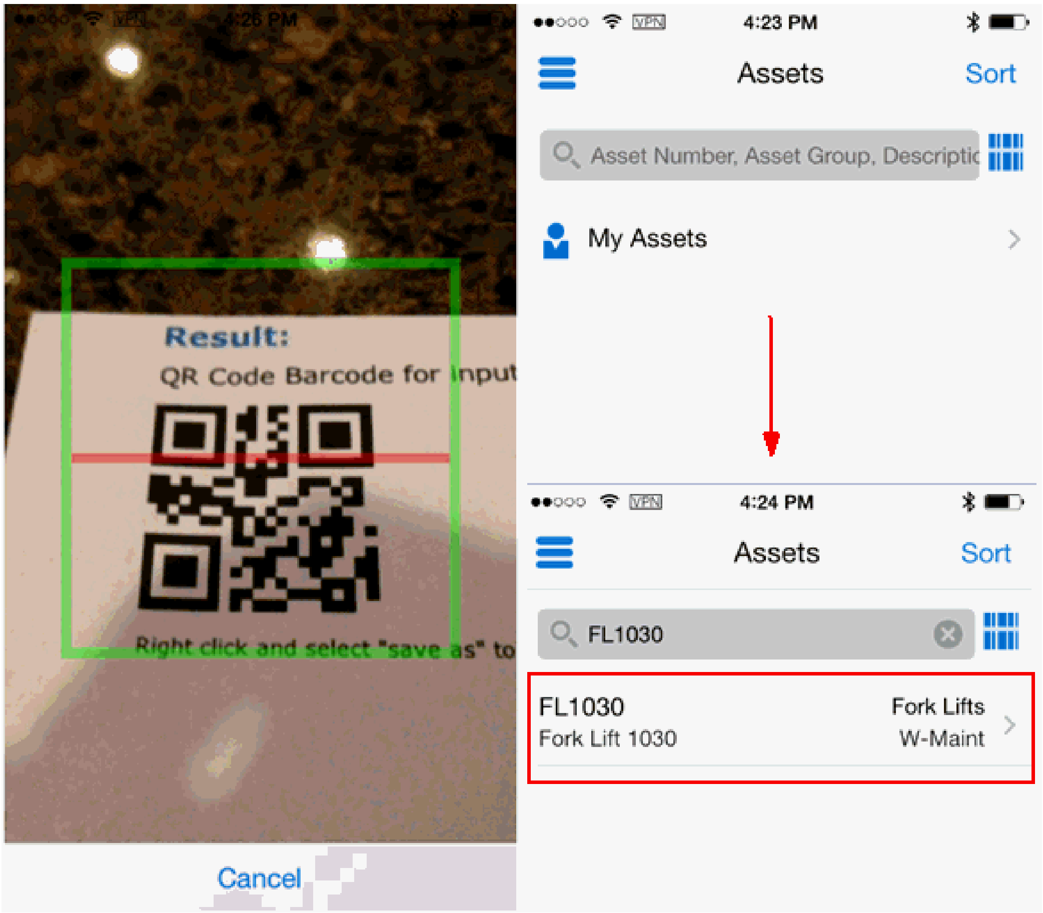
For information on how to set this profile option, see the *Oracle Field Service Implementation Guide*.

Support for Barcodes

Some Oracle E-Business Suite mobile apps provide support through the Cordova plugin for scanning barcodes to capture data or scanning an item or work order.

Note: There is no additional setup task required to integrate Oracle E-Business Suite mobile apps with barcodes.

For example, Oracle Mobile Maintenance for Oracle E-Business Suite uses barcode scanning to capture data for assets, work orders, and work requests.



Mobile Apps Integrated with Barcodes

The following Oracle E-Business Suite mobile apps integrate with barcodes:

- Oracle Mobile Process Production Supervisor for Oracle E-Business Suite
- Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite
- Oracle Mobile Product Information for Oracle E-Business Suite
- Oracle Mobile Maintenance for Oracle E-Business Suite
- Oracle Mobile Inventory for Oracle E-Business Suite

Supported Barcode Types

For mobile apps that include barcode scanning, the following barcode types are supported:

- QR Code
- Data Matrix
- UPC E
- UPC A
- EAN 8
- EAN 13
- Code 128
- Code 39

Additional App-Specific Setup

Perform any appropriate app-specific implementation steps described in each release note of the following mobile apps:

- Oracle Mobile Approvals for Oracle E-Business Suite
- Oracle Mobile Timecards for Oracle E-Business Suite
- Oracle Mobile Product Information for Oracle E-Business Suite
- Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite
- Oracle Mobile Person Directory for Oracle E-Business Suite

For the list of Oracle E-Business Suite mobile apps mentioned here, see the *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*, My Oracle Support Knowledge Document 1641772.1.

Communicating Mobile App Information to Users

After you have completed the setup tasks for your app, provide the following information required to access the app to the users who will install and use the mobile app:

- Name of the app to download

  For the name of the mobile app to download, see *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*, My Oracle Support Knowledge

Document 1641772.1.

- Where to download the app

  For the download location information for your app, see *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*, My Oracle Support Knowledge Document 1641772.1.

- Oracle E-Business Suite user name and password

  The mobile app user login information is the same user name and password used to log in to Oracle E-Business Suite.

- Oracle E-Business Suite server URL in the following format: `http(s)://<hostname>:<port>`

  Please note the difference between the server URL shared with the app users and the full configuration service URL used for validation as described in step 1, the Validating the Configuration section, page 2-32.

  > **Important:** If your Oracle E-Business Suite is deployed in a multinode and load-balanced environment, make sure that the Oracle E-Business Suite server URL represents the web entry point of your environment as specified in your $CONTEXT_FILE. By default, the web entry point is set to the hostname of the application server where Oracle E-Business Suite is installed. If a load-balancer is used, the web entry point becomes the load-balancer's hostname. Refer to *Using Load-Balancers with Oracle E-Business Suite Release 12*, My Oracle Support Knowledge Document 380489.1 for details.

If you modify the topology of your Oracle E-Business Suite server in a way that changes the server URL, then you must inform the app users of the new URL. The users must update the server URL in the device settings from the mobile home page to trigger the reconfiguration process for the app.

Note that in Oracle E-Business Suite Mobile Foundation Release 2.0, a modification entered in the iOS device settings will not trigger the reconfiguration process. To connect the mobile app to a different server, mobile users must uninstall the mobile app and then install it again. See the Oracle E-Business Suite Mobile Foundation Release Update History, *Oracle E-Business Suite Mobile Foundation Release Notes*, My Oracle Support Knowledge Document 1642431.1.

> **Note:** When the configuration service is invoked during the initial login process, it downloads the configuration details from the server with the following scenarios:

- If an app of version 1.0.X (Approvals and Timecards apps only) connects to a server that is configured for Oracle E-Business Suite Mobile Foundation Release 2.0, then the configuration is downloaded through the `connections.xml` file.

- If an app of version 1.0.X (Approvals and Timecards apps only) connects to a server that is configured for Oracle E-Business Suite Mobile Foundation Release 2.1 or later, then the configuration is downloaded through the `connections.xml` file. However, Oracle strongly recommends that you direct your users to update their apps from the Apple App Store in order to take advantage of the new features provided in Oracle E-Business Suite Mobile Foundation Release 2.1 or later releases.

- If an app of version 1.0.X (Learning and Person Directory apps only), version 1.1.0 or later connects to a server that is configured for Oracle E-Business Suite Mobile Foundation Release 2.1 or later, then the configuration is downloaded through the `ebs-mobile-config.xml` file.

- If an app of version 1.0.X (Learning and Person Directory apps only), version 1.1.0 or later connects to a server that is configured for Oracle E-Business Suite Mobile Foundation Release 1.0 or Release 2.0, then the configuration is downloaded through the `connections.xml` file.

Please note that Oracle tests the client and patch combinations with `N-1` where `N` is the latest version available. Oracle strongly recommends that you keep both the server and client versions the same in order to leverage the latest features.

If neither `ebs-mobile-config.xml` nor `connections.xml` can be found, then an error appears indicating that this mobile app is not currently configured on the server.

3

Working with Mobile Application Archives for Enterprise Distribution

Introduction

This chapter explains the concept of enterprise distribution and provides the step-by-step instructions guiding you to create enterprise-distributed apps for your enterprise needs. It includes the following topics:

- Understanding Enterprise Distribution, page 3-1
- Understanding Mobile Application Archive (MAA) Files, page 3-2
- Creating Mobile Apps through MAA files for Enterprise Distribution, page 3-3
    1. Performing Server-Side Tasks, page 3-3
    2. Performing Client-Side Tasks, page 3-20

Understanding Enterprise Distribution

What is enterprise distribution?

It is the distribution of apps to mobile users through an enterprise-controlled site rather than through a public app store, such as Apple App Store or Google Play.

Starting from Oracle E-Business Suite Mobile Foundation Release 4.0, you can distribute a mobile app to your internal users on an internal corporate location. This means that instead of downloading Oracle E-Business Suite mobile apps directly from a public app store, enterprise users can download the apps directly from an enterprise's own site.

> **Important:** This feature is only available in Oracle E-Business Suite Mobile Foundation release 4.0. Enterprise apps can only be distributed

to internal users within the enterprise, and cannot be distributed to third-party users.

This feature allows enterprises to achieve three main objectives:

- Version control

  Enterprises can control the version of the client apps that their enterprise users install on their mobile devices.

- Corporate branding

  Enterprises can have the option to replace the standard Oracle logos with their own company logos.

- Mobile app management (MAM) with Oracle Mobile Security Suite

  To secure enterprise-distributed mobile apps on mobile devices, enterprises can optionally containerize these apps by using Oracle Mobile Security Suite (OMSS). For information about containerizing enterprise-distributed Oracle E-Business Suite mobile apps, see Mobile Application Management (MAM) Support with Oracle Mobile Security Suite, page 5-1.

To accomplish these goals, Oracle E-Business Suite provides Mobile Application Archive (MAA) files for Oracle E-Business Suite mobile apps. Enterprises can use these MAA files for customization as allowed, generate their own application binaries such as iOS application bundle (.ipa) or Android application package (.apk), and deploy them to their own sites.

Understanding Mobile Application Archive (MAA) Files

A MAA file is an application archive that allows developers to use Oracle Mobile Application Framework to customize the apps and generate the enterprise version of the apps to meet enterprise needs.

Oracle delivers MAA files for Oracle E-Business Suite mobile apps to enable changes for enterprise distribution as well as mobile application management (MAM) support with Oracle Mobile Security Suite.

> **Important:** Any changes to the apps are subject to the licensing terms for Oracle Mobile Application Framework Foundation in the *Oracle E-Business Suite Licensing Information User Manual, Release 12.1 and 12.2*, and are treated as your custom code.
>
> Mobile apps created from the provided MAA files can only be distributed to internal enterprise users through an enterprise's own site. These apps cannot be redistributed to a public app store or third-party users.

> Oracle will provide technical support for issues that can be reproduced with MAA files delivered from Oracle and modified as documented in this *Oracle E-Business Suite Mobile Apps Administrator's Guide, Release 12.1 and 12.2*. When Oracle makes changes or provides fixes for the mobile apps, the updates will be delivered as new MAA files, and you will need to reapply your changes to the latest files.

To distribute the modified app to enterprise users through an enterprise's own site, a user who has the *Mobile Applications Developer role* (hereafter referred as *a mobile applications developer* or *a developer*) needs to deploy it with its own deployment profile.

Creating Mobile Apps through MAA files for Enterprise Distribution

To better understand the entire procedures to prepare your app for enterprise distribution, the following tasks are explained in this chapter:

1. Performing Server-Side Tasks, page 3-3
    1. Applying Oracle E-Business Suite Consolidated Server-Side Patches, page 3-4
    2. Setting Up Enterprise-Distributed App Definition Metadata, page 3-4
    3. Migrating Enterprise App Metadata Between Instances, page 3-19
2. Performing Client-Side Tasks, page 3-20
    1. Setting Up a Development Environment, page 3-20
    2. Creating an Oracle JDeveloper Application from a MAA File, page 3-22
    3. Customizing Mobile Apps for Corporate Branding (Optional), page 3-35
    4. Modifying an Existing Deployment Profile (Conditional), page 3-36
    5. Deploying Your Enterprise Mobile Apps, page 3-40

Performing Server-Side Tasks

To work with MAA files for enterprise distribution, perform the following tasks on the server side:

1. Applying Oracle E-Business Suite Consolidated Server-Side Patches, page 3-4
2. Setting Up Enterprise-Distributed App Definition Metadata, page 3-4
3. Migrating Enterprise App Metadata Between Instances, page 3-19

After applying the server-side patches and performing needed tasks, you need to install required software and download MAA files on the client side, as well as set up a development environment in order to create an enterprise app.

See: Performing Client-Side Tasks, page 3-20.

Applying Oracle E-Business Suite Consolidated Server-Side Patches

Oracle strongly recommends applying the latest consolidated server-side patches for your mobile apps.

For the consolidated product family patch information, see Applying Prerequisite Patches on the Oracle E-Business Suite Server, page 2-2.

Please note that the patch information is also included in the "Oracle E-Business Suite Mobile Application Archive Release 4.0" Readme that you can download from the Oracle Software Delivery Cloud. For download instructions, see: Downloading MAF Application Archives Files, page 3-22.

Setting Up Enterprise-Distributed App Definition Metadata

Perform the following tasks to ensure the enterprise app is ready before deployment:

- Registering and Updating Your Enterprise Mobile App Definition Metadata, page 3-4

  You must register the enterprise app definition metadata first before deploying and testing the app against the Oracle E-Business Suite server.

- Creating and Using Mobile App Access Roles, page 3-16

  Oracle E-Business Suite mobile apps use role-based access control to secure mobile app data. To secure the enterprise-distributed mobile apps, developers need to set up required app-specific mobile app access roles first so that administrators can assign these roles to responsibilities later. Users who have the mobile app access roles through those responsibilities will have access to the corresponding mobile apps.

- Configuring Your Enterprise App, page 3-18

  Prior to the deployment of the enterprise app, ensure that the app can work as expected. Developers need to work with administrators to configure and validate the app against an Oracle E-Business Suite environment.

Registering and Updating Your Enterprise App Definition Metadata

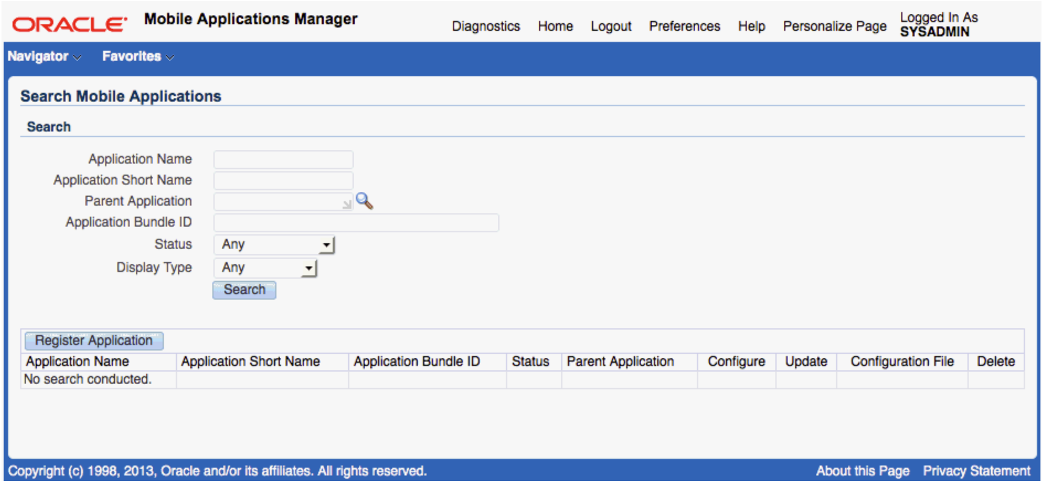
Enterprise apps are considered as new mobile apps which need to be registered on the server first before deploying and testing them. If any definition changes to the enterprise app later, a user who has the Mobile Applications Developer role can modify the application metadata if needed.

Accessing the Mobile Applications Manager UI Pages

To access the Mobile Applications Manager UI pages, log in to Oracle E-Business Suite as a user who has the Mobile Applications Manager responsibility.

> **Note:** The Mobile Applications Manager responsibility allows you to access the Mobile Applications Manager UI pages, and this responsibility is assigned through the Mobile Applications Administrator role or the Mobile Applications Developer role. For more information about these roles and their privileges, see Enabling a Mobile App Individually and Specifying the Configuration through the UI, page 2-11.

The Search Mobile Application page appears.



Search Mobile Applications

Search

Application Name

Application Short Name

Parent Application

Application Bundle ID

Status: Any

Display Type: Any

Application Name	Application Short Name	Application Bundle ID	Status	Parent Application	Configure	Update	Configuration File	Delete
No search conducted.								

Copyright (c) 1998, 2013, Oracle and/or its affiliates. All rights reserved.

This is the entry point where a developer can:

- Register an enterprise app by clicking the **Register Application** button. See: Registering an Enterprise Mobile App, page 3-6.

- Update the application definition metadata for an existing enterprise app by clicking the **Update** icon from a search result table. See: Updating an Enterprise Mobile App Definition, page 3-13.

- Delete an existing application definition metadata of an enterprise app by clicking the **Delete** icon from the search result table. See: Deleting an Enterprise Mobile App Definition, page 3-15.

For information on enabling and configuring a mobile app as well as viewing application details, see Enabling a Mobile App Individually and Specifying the Configuration through the UI, page 2-11.

Registering an Enterprise Mobile App

Once a mobile app is modified for enterprise distribution or corporate branding, a developer can register the app before the app can be deployed and tested against the Oracle E-Business Suite server.

Use the following steps to register an enterprise app on the server:

1. Log in to Oracle E-Business Suite as a user who has the Mobile Applications Developer role.

2. Select the Mobile Applications Manager responsibility and choose the **Applications** link from the navigator.

3. In the Search Mobile Applications page, click the **Register Application** button to register an enterprise app.

   The following pages are displayed in the sequence listed here as part of the registration process for an enterprise app:

   1. Application Details Page, page 3-6

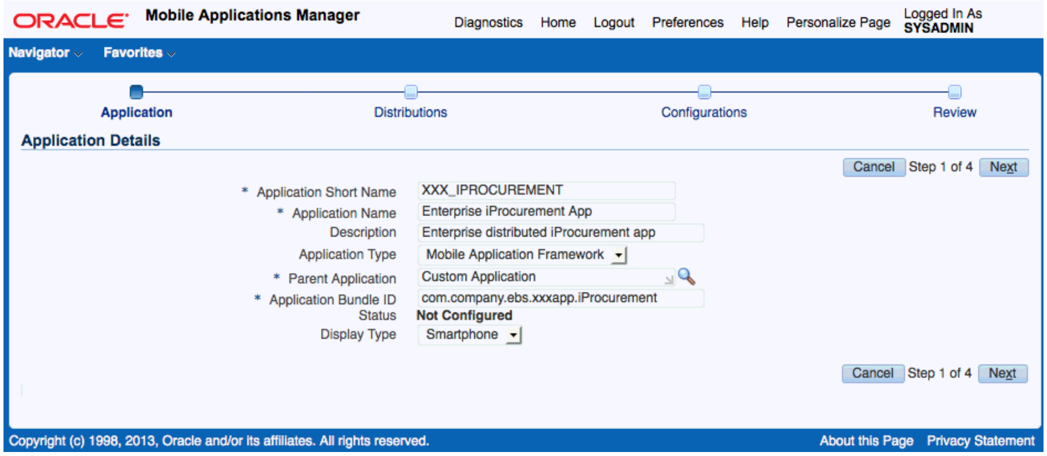
   2. Distributions Page, page 3-7

   3. Configurations Details Page, page 3-9

   4. Review Page, page 3-12

Application Details Page

After the developer clicks the **Register Application** button in the Search Mobile Applications page to register an enterprise app, the Application Details page appears.



Application Details

* Application Short Name	XXX_IPROCUREMENT
* Application Name	Enterprise iProcurement App
Description	Enterprise distributed iProcurement app
Application Type	Mobile Application Framework
* Parent Application	Custom Application
* Application Bundle ID	com.company.ebs.xxxapp.iProcurement
Status	**Not Configured**
Display Type	Smartphone

Enter the following application metadata information for your enterprise app:

- **Application Short Name:** Enter the short name for the mobile app, such as

"XXX_IPROCUREMENT".

- **Application Name:** Enter the display name for the mobile app.
- **Description:** Enter optional description information for the mobile app
- **Application Type:** "Mobile Application Framework" is selected by default.
- **Parent Application Name:** Enter the Oracle E-Business Suite application to which the mobile app belongs, such as "Custom Application".
- **Application Bundle Id:** Enter a unique bundle identifier for the mobile app, such as `com.company.ebs.xxxapp.iProcurement` for your mobile app.

  This value should be the same Id value in the `maf-application.xml` file when modifying the app in Oracle JDeveloper. See: Changing Application Bundle Id, page 3-30.
- **Display Type:** "Smartphone" is selected by default.
- **Status:** "Not Configured" is selected by default.

  Once the app is configured, set this value to "Enabled".

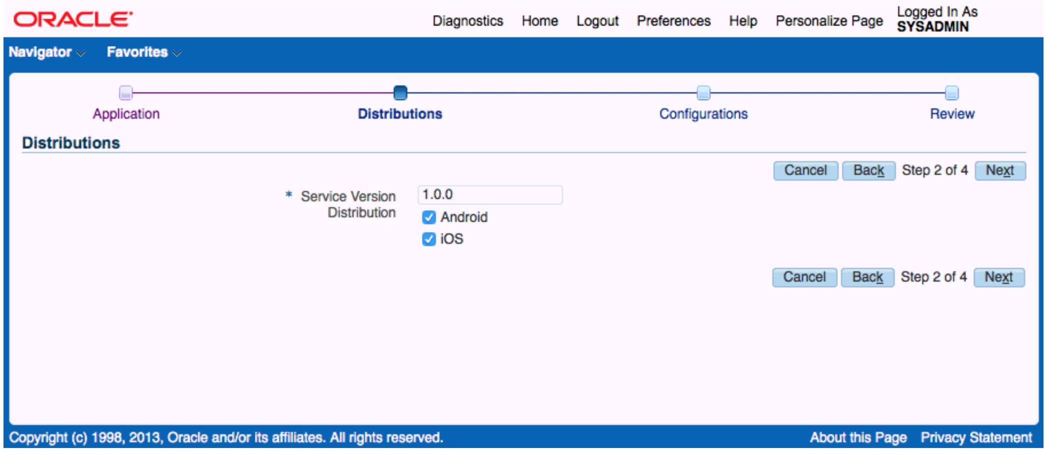
  > **Note:** Ensure that the desired information for Application Name, Application Short Name, and Application Bundle Id are correctly specified for your app. These fields are not allowed to change after the registration. See: Updating an Enterprise Mobile App Definition, page 3-13.

Click **Next** to access the Distributions page to continue the registration process. See: Distributions Page, page 3-7.

For information on registering an enterprise app, see Registering an Enterprise Mobile App, page 3-6.

Distributions Page

After the developer completes the application metadata for an enterprise app and clicks **Next**, the Distributions page appears. This is the page where the developer specifies the service version and distribution method for the app.



Distributions

* Service Version: 1.0.0

Distribution: ☑ Android ☑ iOS

Enter the following distribution information for the mobile app:

- **Service Version:** Enter the service version number corresponding to the app's REST service implementation.

  This service version number must be exactly the same as the service version of the corresponding Oracle E-Business Suite mobile app. This is because the enterprise app uses the same REST services as that of the corresponding seeded mobile app. This service version number is also important for mobile clients to access and determine the server's capability. Therefore, this service version number cannot be different from the corresponding seeded app.

  For example, the service version of the seeded Oracle Mobile iProcurement for Oracle E-Business Suite app is "1.0.0", and you must enter the same service version "1.0.0" here for the enterprise version of the iProcurement app.

  > **Note:** The service version number entered here cannot be prefixed with letter "E", such as E1.3.0, which is for the app version only.

  To obtain the service version information of the corresponding seeded app, locate the seeded app through a search first, and then click the app's Application Name link from the search result table. The service version information is displayed in the read-only Application Details page.

  Please note that if you upgrade an enterprise-distributed app to a new version of the corresponding MAA file and apply the corresponding consolidated product family patch, remember to manually check and update the Service Version number of the enterprise app to that of the value in the corresponding seeded app. For information on initiating the server updates, see Directing Users to Obtain Connection Details and Initiate Server Updates, page 7-6.

- **Distribution:** Select the desired distribution platform check boxes for your app, such as Android, iOS, or both.

Click **Next** to access the Configurations page. See: Configurations Details Page, page 3-9.

Click **Back** to modify the application metadata information if needed. See: Application Details Page, page 3-6.

For information on registering an enterprise app, see Registering an Enterprise Mobile App, page 3-6.

Configurations Details

Use the Configurations Details page to specify the desired authentication type and set the related configuration parameters for the app.

This page includes the following regions:

- **Configuration Category region**

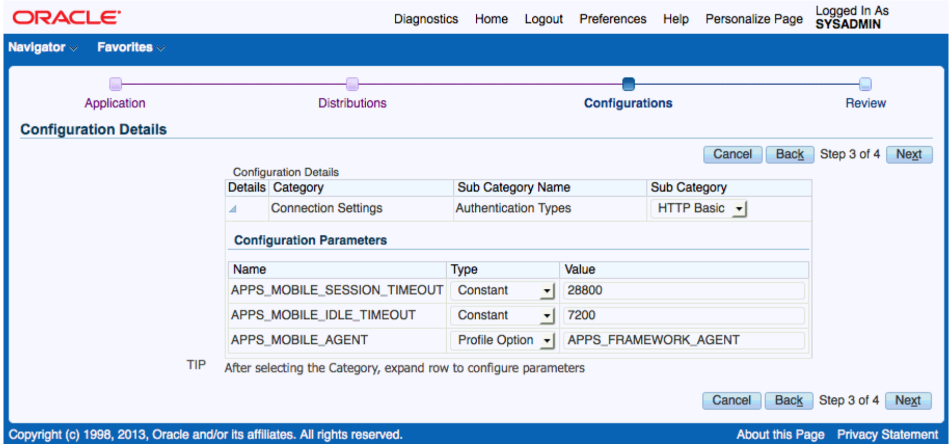
  Select either one of the authentication types as the Sub Category value from the drop-down list for the connection settings:

  > **Note:** The authentication type selected here during the app registration can be changed later when the administrator configures the app.

  - **HTTP Basic (default)**

    This is the default authentication type for the connection settings. The corresponding configuration parameters for the HTTP Basic type are:

    - APPS_MOBILE_SESSION_TIMEOUT
    - APPS_MOBILE_IDLE_TIMEOUT
    - APPS_MOBILE_AGENT



Configuration Details

Configuration Details

Details	Category	Sub Category Name	Sub Category
◢	Connection Settings	Authentication Types	HTTP Basic

Configuration Parameters

Name	Type	Value
APPS_MOBILE_SESSION_TIMEOUT	Constant	28800
APPS_MOBILE_IDLE_TIMEOUT	Constant	7200
APPS_MOBILE_AGENT	Profile Option	APPS_FRAMEWORK_AGENT

TIP After selecting the Category, expand row to configure parameters

For information on setting configuration parameters for this authentication type, see Configuring Parameters for the HTTP Basic Authentication Type, page 2-18, as described in step 8.

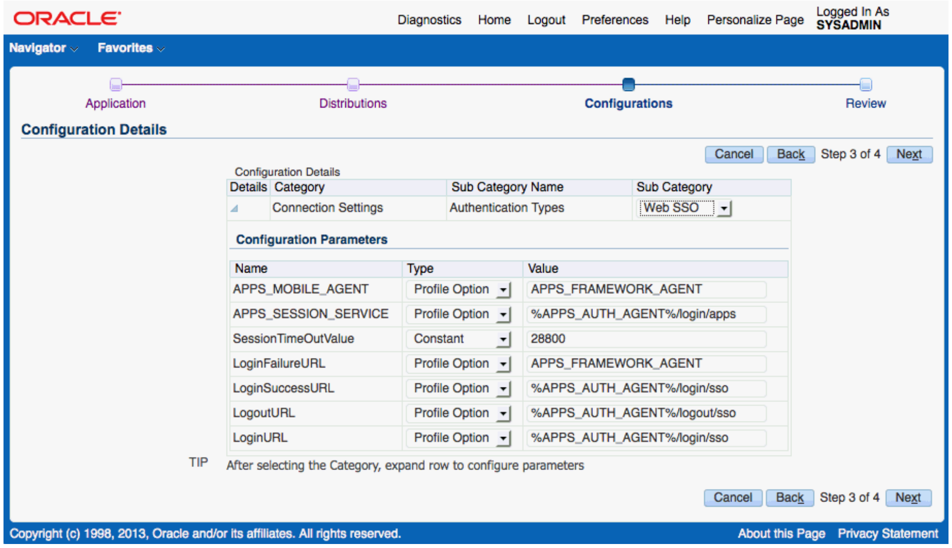
- **Web SSO**

  Use this authentication type if you want to delegate authentication to Oracle Access Manager based on a protected Login URL.

  If you want to use single sign-on across Oracle E-Business Suite mobile apps through the use of Oracle Mobile Security Suite, you must select "Web SSO" as a prerequisite when configuring your mobile apps. See: Mobile Application Management (MAM) Support with Oracle Mobile Security Suite, page 5-1.

  Additionally, before selecting this authentication type, ensure that your Oracle E-Business Suite instance is integrated with Oracle Access Manager. Refer to My Oracle Support Knowledge Document 1388152.1, *Overview of Single Sign-On Integration Options for Oracle E-Business Suite*. You must apply required patches and perform additional setup tasks to enable this feature. See: Additional Setup Tasks to Enable Web SSO Authentication Security, page 2-25.

  For more information about single sign-on, see Single Sign-On (SSO), page 6-6
  .



Configuration Details

Configuration Details

Details	Category	Sub Category Name	Sub Category
◢	Connection Settings	Authentication Types	Web SSO

Configuration Parameters

Name	Type	Value
APPS_MOBILE_AGENT	Profile Option	APPS_FRAMEWORK_AGENT
APPS_SESSION_SERVICE	Profile Option	%APPS_AUTH_AGENT%/login/apps
SessionTimeOutValue	Constant	28800
LoginFailureURL	Profile Option	APPS_FRAMEWORK_AGENT
LoginSuccessURL	Profile Option	%APPS_AUTH_AGENT%/login/sso
LogoutURL	Profile Option	%APPS_AUTH_AGENT%/logout/sso
LoginURL	Profile Option	%APPS_AUTH_AGENT%/login/sso

TIP After selecting the Category, expand row to configure parameters

Once "Web SSO" is selected as the authentication type, the following corresponding configuration parameters are automatically displayed in the Configuration Parameters region:

- APPS_MOBILE_AGENT
- APPS_SESSION_SERVICE
- SessionTimeOutValue
- LoginFailureURL
- LoginSuccessURL
- LogoutURL
- LoginURL

For information on setting configuration parameters for this authentication type, see Configuring Parameters for the Web SSO Authentication Type, page 2-20, as described in step 8.

- **Configuration Parameters region**

  The Configuration Parameters region allows the developer to predefine the configuration parameters for the app's configuration file based on the selected authentication type. To display this region, click the **Show** link next to the Connection Settings category in the Configuration Categories region.

  Specify the parameter values listed in the region to predefine the configuration settings for the app.

- **Name:** This is the configuration parameter name corresponding to the authentication type specified earlier in the Configuration Categories region.

- **Type:** This determines how the default value for a parameter is assigned. Select either one of the following values:

  - Constant - It indicates that the value for the parameter is a constant.

    For example, if "Constant" is selected, enter a constant value "28800" seconds as the default value in the Value field for the Session Timeout (APPS_MOBILE_SESSION_TIMEOUT) parameter.

  - Profile Option - It indicates a profile option is used to retrieve the value for the parameter.

    If this is selected, enter the profile option name in the Value field for the parameter. For example, enter "APPS_FRAMEWORK_AGENT" as the default profile option name in the Value field for the Service Endpoint (APPS_MOBILE_AGENT) parameter.

- **Value:** This is the default value for the parameter. This value is either a valid profile option internal name or a constant value depending on the value selected in the Type field.

  For example, the default value for the SSO Login URL (LoginURL) parameter is the current value of `%APPS_AUTH_AGENT%/login/sso`.

  Please note that the convention `%<string>%` is used specifically for parameter values of type "Profile Option" and the value of which contains content that is in addition to the profile value. For example, the runtime value of this SSO Login URL parameter would be `<profile-value-of-the-APPS_AUTH_AGENT>/login/sso`, where `/login/sso` is a constant.

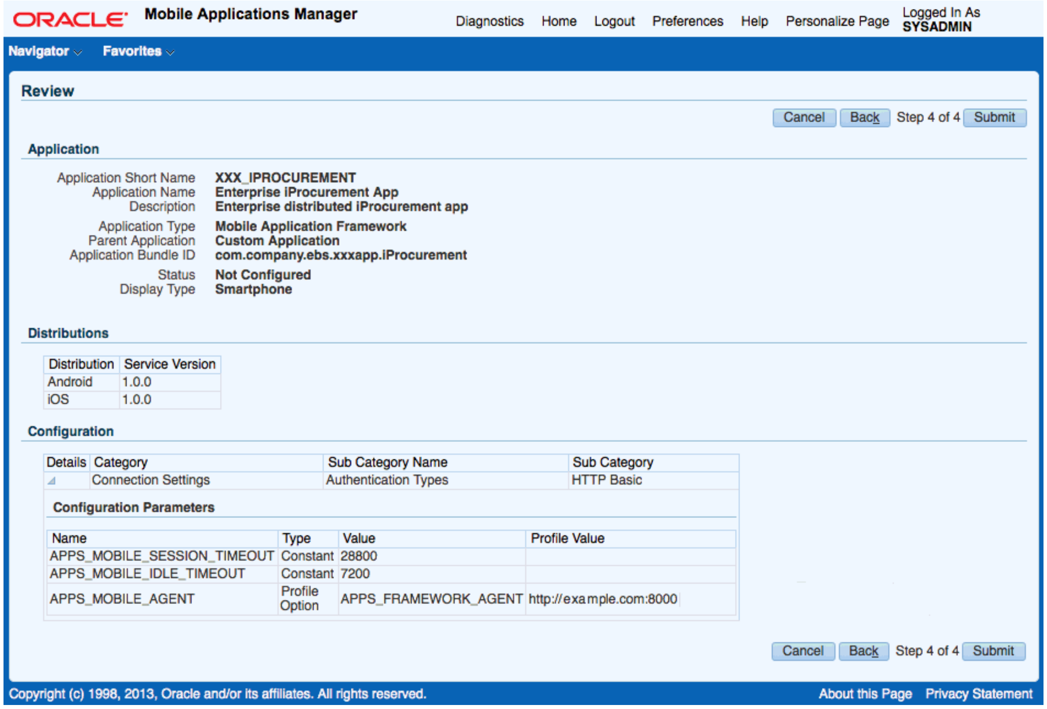
Click **Next** to access the Review page. See: Review Page, page 3-12.

Click **Back** to modify the configuration information if needed. See: Distributions Page, page 3-7.

For information on registering an enterprise app, see Registering an Enterprise Mobile App, page 3-6.

Review Page

Once the developer completes the required registration information for the enterprise app, the read-only Review page appears. It displays all the metadata information, distributions, and configuration details that the developer specified earlier for the app.



Review

Application

Application Short Name	XXX_IPROCUREMENT
Application Name	Enterprise iProcurement App
Description	Enterprise distributed iProcurement app
Application Type	Mobile Application Framework
Parent Application	Custom Application
Application Bundle ID	com.company.ebs.xxxapp.iProcurement
Status	Not Configured
Display Type	Smartphone

Distributions

Distribution	Service Version
Android	1.0.0
iOS	1.0.0

Configuration

Details	Category	Sub Category Name	Sub Category
◿	Connection Settings	Authentication Types	HTTP Basic

Configuration Parameters

Name	Type	Value	Profile Value
APPS_MOBILE_SESSION_TIMEOUT	Constant	28800	
APPS_MOBILE_IDLE_TIMEOUT	Constant	7200	
APPS_MOBILE_AGENT	Profile Option	APPS_FRAMEWORK_AGENT	http://example.com:8000

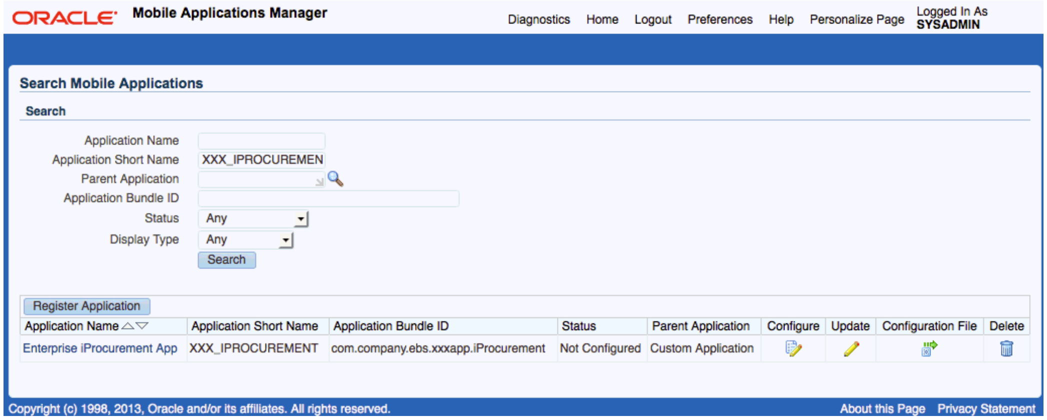
If no more change is required for the app, click **Submit** to save and register the app. A confirmation message appears indicating that the mobile app is successfully registered.

Click **Back** to modify the information if needed. See: Configurations Details Page, page 3-9.

For information on registering a mobile app, see Registering an Enterprise Mobile App, page 3-6.

Updating an Enterprise Mobile App Definition

To update the definition of an existing enterprise app, locate the app from the search result table in the Search Mobile Applications page.


ORACLE Mobile Applications Manager
Diagnostics Home Logout Preferences Help Personalize Page
Logged In As SYSADMIN
Search
Register Application
Copyright (c) 1998, 2013, Oracle and/or its affiliates. All rights reserved.
About this Page Privacy Statement

Search Mobile Applications

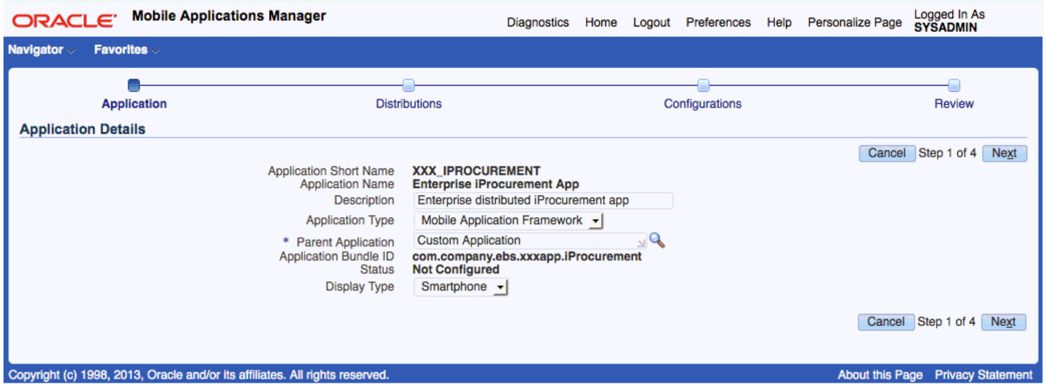
Search

Application Name	
Application Short Name	XXX_IPROCUREMEN
Parent Application	
Application Bundle ID	
Status	Any
Display Type	Any

Application Name	Application Short Name	Application Bundle ID	Status	Parent Application	Configure	Update	Configuration File	Delete
Enterprise iProcurement App	XXX_IPROCUREMENT	com.company.ebs.xxxapp.iProcurement	Not Configured	Custom Application				

Click the **Update** icon from the search result table. This action allows a developer to access the Application Details page and modify the definition of the selected enterprise app.

> **Warning:** Developers can update the application definitions of enterprise apps, but should never remove or modify the application definitions of Oracle E-Business Suite mobile apps, starting with `com.oracle.ebs*`.


ORACLE Mobile Applications Manager
Diagnostics Home Logout Preferences Help Personalize Page
Logged In As SYSADMIN
Navigator
Favorites
Application
Distributions
Configurations
Review
Cancel
Step 1 of 4
Next
Copyright (c) 1998, 2013, Oracle and/or its affiliates. All rights reserved.
About this Page Privacy Statement

Application Details

Application Short Name	XXX_IPROCUREMENT
Application Name	Enterprise iProcurement App
Description	Enterprise distributed iProcurement app
Application Type	Mobile Application Framework
* Parent Application	Custom Application
Application Bundle ID	com.company.ebs.xxxapp.iProcurement
Status	Not Configured
Display Type	Smartphone

> **Note:** Alternatively, a developer can click the Application Name link, such as XXX_IPROCUREMENT, from the search result table first to display the read-only Application Details page. Click the **Update** button in the page to enable the update for the app.

Similar to the app registration process, the developer can update the application definition metadata for the selected enterprise app.

- **Updating the application definition metadata in the Application Details Page**

  In the Application Details page, the developer can update the application metadata information including description, application type, parent application, and display type.

Please note that the Application Name, Application Short Name, and Application Bundle ID fields are not enabled for update.

- **Updating the distribution information in the Distributions Page**

  In the Distributions page, the developer can update the service version, and distribution methods for the selected enterprise app.

- **Updating the configuration information in the Configuration Details Page**

  In the Configuration Details page, the developer can change the authentication type from the Sub Category drop-down list if necessary, and then update the corresponding configuration parameters.

  As mentioned earlier during the app registration, if Web SSO is selected as the authentication type for an app, ensure that the Oracle E-Business Suite instance must be integrated with Oracle Access Manager. Refer to My Oracle Support Knowledge Document 1388152.1, *Overview of Single Sign-On Integration Options for Oracle E-Business Suite*. You must apply required patches and perform additional setup tasks to enable this feature. See: Additional Setup Tasks to Enable Web SSO Authentication Security, page 2-25.

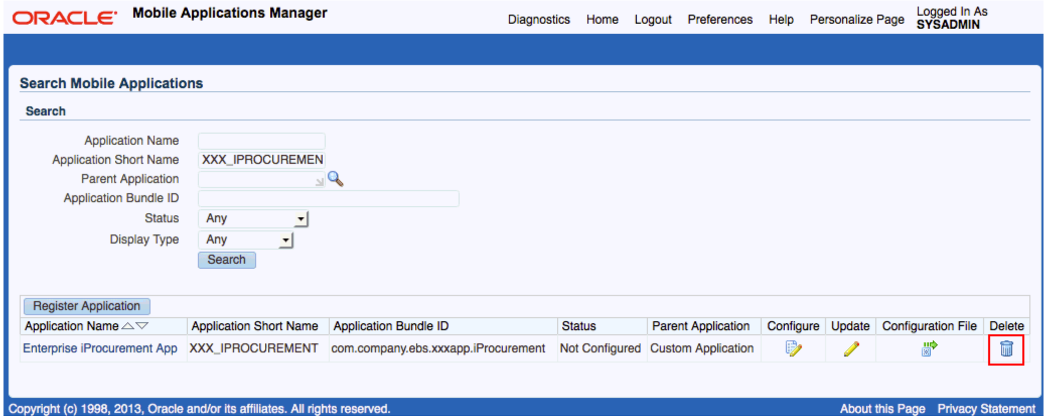
  Additionally, if you want to use single sign-on across Oracle E-Business Suite mobile apps through the use of Oracle Mobile Security Suite, you must select the "Web SSO" type as a prerequisite when configuring your mobile apps. See: Mobile Application Management (MAM) Support with Oracle Mobile Security Suite, page 5-1.

For information on registering an enterprise app, see Registering an Enterprise Mobile App, page 3-4.

Deleting an Enterprise Mobile App Definition

When the application definition of an enterprise app becomes invalid or is no longer needed, a developer can remove it from the server.

> **Warning:** Developers can delete or update the application definitions of enterprise apps, but should never remove or modify the seeded application definitions of Oracle E-Business Suite mobile apps, starting with `com.oracle.ebs*`.



Search Mobile Applications

Search

Application Name:
Application Short Name: XXX_IPROCUREMEN
Parent Application:
Application Bundle ID:
Status: Any
Display Type: Any

Application Name	Application Short Name	Application Bundle ID	Status	Parent Application	Configure	Update	Configuration File	Delete
Enterprise iProcurement App	XXX_IPROCUREMENT	com.company.ebs.xxxapp.iProcurement	Not Configured	Custom Application	✎	✎	➔	🗑

Copyright (c) 1998, 2013, Oracle and/or its affiliates. All rights reserved.
About this Page
Privacy Statement

To delete the definition of an enterprise app, click the **Delete** icon from the search result table. A confirmation message appears requiring the developer to confirm the delete action. Once it's confirmed, the definition of the selected enterprise app is removed from the database and it is no longer available for the enterprise users.

Creating and Using Mobile App Access Roles

Oracle E-Business Suite mobile apps use role-based access control to allow users who are assigned the appropriate access roles to access Oracle E-Business Suite. To secure the enterprise-distributed mobile apps, a mobile applications developer needs to set up required app-specific mobile app access roles first. A mobile applications administrator can then assign these roles to responsibilities that will have access to the mobile apps.

> **Important:** Oracle Mobile Approvals for Oracle E-Business Suite is the only app that does not have an app-specific access role required for users to access the app. Other than the Approvals app, a mobile applications developer must set up required roles for your enterprise apps.

1. Create mobile app access roles in Oracle E-Business Suite.

   See: Creating Mobile App Access Roles, page 3-16.

2. Assign the mobile app access roles to responsibilities.

   See: Assigning Mobile App Access Roles to Responsibilities, page 3-18.

3. Migrate the mobile app access role definitions to a target Oracle E-Business Suite instance where the enterprise app could connect.

   See: Downloading and Uploading Mobile App Access Roles, page 3-20.

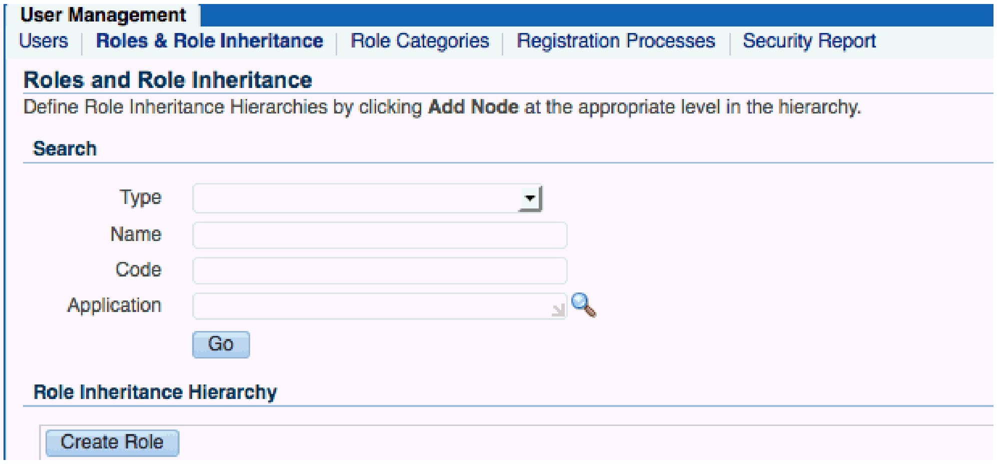
Creating Mobile App Access Roles

Perform the following steps to create mobile app access roles:

1. Log in to Oracle E-Business Suite as a user who has the User Management responsibility. For example, log in as `SYSADMIN`.

2. Select the User Management responsibility and navigate to the Roles and Role Inheritance page.

3. In the Roles and Role Inheritance page, click the **Create Role** button.



Define Role Inheritance Hierarchies by clicking **Add Node** at the appropriate level in the hierarchy.

4. Enter the following information in the Create Role page:

   - **Category:** Select "Security Administration" from the drop-down list.

   - **Role Code:** Enter the role code in the format of "`PROD_MBL_APP_NAME`", such as "`XXX_IPROCUREMENT_MBL_ROLE`".

     - A prefix "`UMX|`" is added to this value automatically.

       In this example, the entered code value is automatically converted to `UMX|XXX_IPROCUREMENT_MBL_ROLE`.

     - The Role Code information entered here should be specified in the `oracle.ebs.login.rolecode` property of the `ebs.properties` file later. See Assigning Mobile App Access Roles, page 3-34.

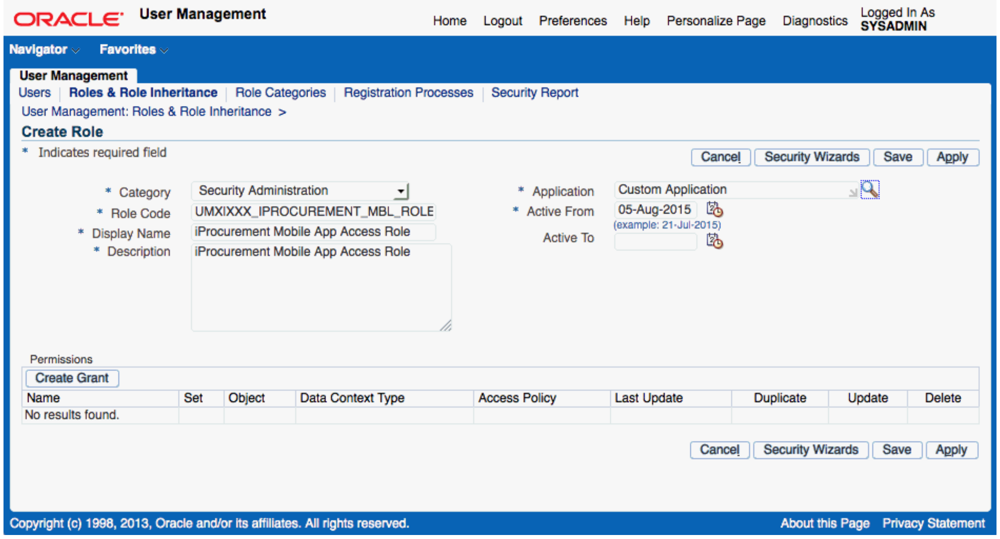
   - **Display Name:** Enter a valid display name, such as "iProcurement Mobile App Access Role".

   - **Description:** Enter a valid description information for the role, such as "iProcurement Mobile App Access Role".

   - **Application:** Select the application name. For example, "Custom Application".

     Similar to the Role Code value, the Application Short Name information entered here should be set up in the `oracle.ebs.login.roleappname` property of the `ebs.properties` file later. See Assigning Mobile App Access Roles, page 3-34.

- **Active From:** Leave the default unchanged.
- **Active To:** Leave this field blank.


ORACLE User Management
Home Logout Preferences Help Personalize Page Diagnostics
Logged In As SYSADMIN
Navigator Favorites
User Management
Users | Roles & Role Inheritance | Role Categories | Registration Processes | Security Report
User Management: Roles & Role Inheritance >
Cancel Security Wizards Save Apply
Create Grant

Create Role

* Indicates required field

* Category	Security Administration	* Application	Custom Application
* Role Code	UMXIXXX_IPROCUREMENT_MBL_ROLE	* Active From	05-Aug-2015 (example: 21-Jul-2015)
* Display Name	iProcurement Mobile App Access Role	Active To	
* Description	iProcurement Mobile App Access Role		

Permissions

Name	Set	Object	Data Context Type	Access Policy	Last Update	Duplicate	Update	Delete
No results found.								

Copyright (c) 1998, 2013, Oracle and/or its affiliates. All rights reserved.

5. Save your work.

For information on the seeded app-specific access roles for Oracle E-Business Suite mobile apps, see Appendix A: Mobile App Access Roles, page A-1.

Assigning Mobile App Access Roles to Responsibilities

After a mobile applications developer creates app-specific roles for an enterprise app, a mobile applications administrator can then assign these roles to responsibilities.

If the mobile app access roles were not assigned to any valid responsibilities that are assigned to the mobile users, those users will not be able to connect the mobile apps to Oracle E-Business Suite.

For information on assigning roles to responsibilities, see Setting Up Mobile App Access to Responsibilities, page 2-35.

Please note that on the client side, a mobile applications developer needs to specify these app-specific roles in the MAF application's `ebs.properties` file in order for the corresponding enterprise apps to use these roles. See: Using Mobile App Access Roles, page 3-34.

Configuring Your Enterprise Apps

Before deploying the enterprise app to the enterprise's own site, a mobile applications developer must work with a mobile applications administrator to perform needed administrative tasks to ensure the enterprise app can work as expected. These administrative tasks including enterprise app configuration and validation can be performed in a development instance.

For information on the administrative tasks, see Setting Up the Mobile Apps, page 2-1.

Migrating Enterprise App Metadata Between Instances

If there is a need to migrate the enterprise-distributed mobile application definition metadata and relevant mobile app access roles from one instance to another, developers can perform the following tasks to transport the needed information:

This section includes the following topics:

- Downloading and Uploading Mobile App Definitions, page 3-19

  Developers can download the app definition metadata into an LDT file and then upload the file to another instance if needed.

- Downloading and Uploading Mobile App Access Roles, page 3-20

  Similar to the migration of the app definition metadata, this allows developers to migrate mobile app access roles between instances.

Downloading and Uploading Mobile App Definitions

Once the application definition metadata has been registered in the database, developers can transport the metadata information between different instances for testing or migration purposes.

Downloading Mobile App Definition Metadata

This can be achieved by first downloading the metadata into an LDT file, based on a LCT file `$FND_TOP/patch/115/import/xxxiproc.lct` using the Application Short Name as the key.

For example, use the following commands to download the metadata to a LDT file:

```
FNDLOAD <APPS username> 0 Y DOWNLOAD
$FND_TOP/patch/115/import/afmobile.lct xxxiproc.ldt
FND_MBL_APPLICATION APPLICATION_SHORT_NAME=XXX_IPROCUREMENT

ORACLE Password:
```

Uploading Mobile App Definition Metadata

To upload the downloaded LDT file, such as `xxxiproc.ldt`, to another instance, use the following commands:

```
FNDLOAD <APPS username> 0 Y UPLOAD
$FND_TOP/patch/115/import/afmobile.lct xxxiproc.ldt

ORACLE Password:
```

Downloading and Uploading Mobile App Access Roles

Similar to the concepts of transporting application definition metadata information between instances, developers can migrate the mobile app access role definitions from one instance to another if required.

Downloading Mobile App Access Roles

Use the following commands to download the definition of mobile app access roles:

```
FNDLOAD <APPS username> 0 Y DOWNLOAD
$FND_TOP/patch/115/import/afrole.lct xxxapprole.ldt WF_ROLE
ROLE_NAME=UMX|XXX_IPROCUREMENT_MBL_ROLE
```

```
ORACLE Password:
```

Uploading Mobile App Access Roles

After downloading the definition of mobile app access roles, developers can upload the downloaded LDT file to another Oracle E-Business Suite instance to which the mobile app should connect. For example, use the following commands to upload the role definition:

```
FNDLOAD <APPS username> 0 Y UPLOAD
$FND_TOP/patch/115/import/afrole.lct xxxapprole.ldt
```

```
ORACLE Password:
```

Performing Client-Side Tasks

This section discusses the required procedures to create the enterprise apps on the client side before you can distribute these apps to an enterprise's own site for your enterprise users. It includes the following topics:

1. Setting Up a Development Environment, page 3-20
2. Creating an Oracle JDeveloper Application from a MAA File, page 3-22
3. Using Mobile App Access Roles, page 3-34
4. Customizing Mobile Apps for Corporate Branding (Optional), page 3-35
5. Modifying an Existing Deployment Profile (Conditional), page 3-36
6. Deploying Your Enterprise Mobile Apps, page 3-40

Setting Up a Development Environment

This section describes the following setup tasks:

1. Installing Development Tools and Setting Up a Development Environment, page 3-21

2. Downloading and Installing Oracle JDeveloper 12.1.3 Studio Edition, page 3-21

3. Downloading and Installing Oracle Mobile Application Framework 2.1.3 for Oracle E-Business Suite Mobile Foundation Release 4.0, page 3-21

Installing Development Tools and Setting Up a Development Environment

Install required development tools for the iOS and Android platforms:

- For the iOS platform, register with iOS Developer Program. Download Xcode and the iOS SDK.

- For the Android platform, set up the downloaded Android SDK.

For instructions on setting up development tools for the iOS and Android platforms, see:

- Installing Mobile Application Framework with JDeveloper, *Oracle Fusion Middleware Developing Mobile Applications with Oracle Mobile Application Framework*

- Setting Up the Development Environment, *Oracle Fusion Middleware Developing Mobile Applications with Oracle Mobile Application Framework*

Setting Up a Development Environment

Configure the environment for your target platform in Oracle JDeveloper. From the main menu, select **Tools** and then **Preferences** to open the Preferences dialog. Select your desired platform, either the Android Platform or iOS Platform, from the **Mobile Application Framework** tree node.

This opens a page for the selected platform. Specify the platform and SDK location and provide the information for the signing credentials.

For more information on setting up development environment, see Setting Up the Development Environment, *Oracle Fusion Middleware Developing Mobile Applications with Oracle Mobile Application Framework*.

Downloading and Installing Oracle JDeveloper 12.1.3 Studio Edition

To work with downloaded MAA files, ensure you have Oracle JDeveloper, version 12.1.3.0.0 Studio Edition.

For information on setting up Oracle JDeveloper, see *Oracle Fusion Middleware Installing Oracle JDeveloper*.

Downloading and Installing Oracle Mobile Application Framework 2.1.3 for Oracle E-Business Suite Mobile Foundation Release 4.0

To work with MAA files, in addition to Oracle JDeveloper, you need to download Oracle Mobile Application Framework 2.1.3 for Oracle E-Business Suite Mobile Foundation Release 4.0.

Downloading Oracle Mobile Application Framework

Oracle Mobile Application Framework 2.1.3 for Oracle E-Business Suite Mobile Foundation Release 4.0 is available for download from My Oracle Support through patch 21609151.

Additionally, you can download this specific Oracle MAF version that is included in the "Oracle E-Business Suite Mobile Application Archive 4.0" software distribution from the Oracle Software Delivery Cloud. For download instructions, see: Downloading MAF Application Archives Files, page 3-22.

Installing Oracle Mobile Application Framework

After you have installed the iOS and/or Android SDKs required for your platform(s) and downloaded the required Oracle Mobile Application Framework 2.1.3 version for Oracle E-Business Suite Mobile Foundation Release 4.0, follow the installation instructions described in the patch readme to install the downloaded Oracle Mobile Application Framework.

For more instructions on installing Oracle Mobile Application Framework, see Installing the MAF Extension in JDeveloper, Installing Mobile Application Framework with JDeveloper, *Oracle Fusion Middleware Developing Mobile Applications with Oracle Mobile Application Framework*, and *Oracle Mobile Application Framework Installing Oracle Mobile Application Framework*.

Creating an Oracle JDeveloper Application from a MAA File

Once a development environment is set up on the client side, a developer can download the MAA files and create an application from a downloaded MAA file.

To better understand each task performed on the client side, this section includes the following topics:

1. Downloading MAF Application Archives Files, page 3-22

2. Importing a MAA file to Create a MAF Application, page 3-27

3. Updating Plugin Configuration (Optional), page 3-29

4. Importing Additional Root-CA Certificates (Optional), page 3-30

5. Changing Application Bundle Id, page 3-30

6. Changing Privacy Policy Link, page 3-32

Downloading MAF Application Archives Files

Use the following steps to download Oracle E-Business Suite Mobile Application Archive (.maa) files, along with consolidated server-side patches and Oracle Mobile Application Framework 2.1.3 for Oracle E-Business Suite Mobile Foundation Release

4.0:

1. Log in to the Oracle Software Delivery Cloud (`https://edelivery.oracle.com/`) page.

2. Click the **Sign In** button.

   If you do not have an Oracle account, click the **New User? Register Here** link instead to create one.

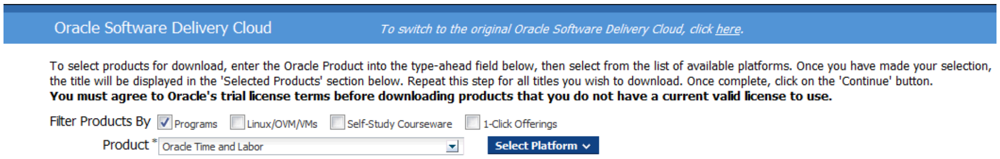
3. Read the Export Restrictions information and click the **Accept** button.

4. On the Oracle Service Delivery Cloud page, select the following values:

   - Filter Products By: Select the Programs check box

   - Product: Enter a licensed product name that lets you access the associated mobile app, such as "Oracle Time and Labor" for "Oracle Mobile Timecards for Oracle E-Business Suite".

   - Select Platform: Select a desired platform, such as Linux x86 64 bit.

   Oracle Software Delivery Cloud

   To switch to the original Oracle Software Delivery Cloud, click here.

   To select products for download, enter the Oracle Product into the type-ahead field below, then select from the list of available platforms. Once you have made your selection, the title will be displayed in the 'Selected Products' section below. Repeat this step for all titles you wish to download. Once complete, click on the 'Continue' button.
   You must agree to Oracle's trial license terms before downloading products that you do not have a current valid license to use.

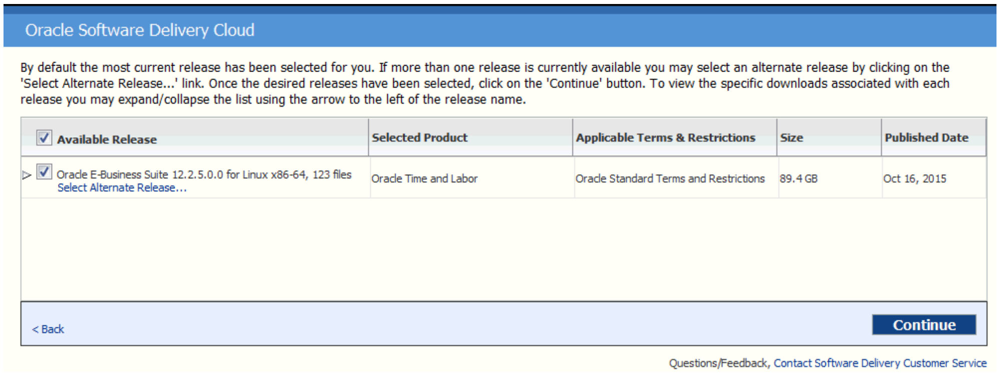
   Filter Products By ☑ Programs □ Linux/OVM/VMs □ Self-Study Courseware □ 1-Click Offerings

   Product * Oracle Time and Labor

5. Execute the search by clicking the **Continue** button.

   This should retrieve the corresponding Oracle E-Business Suite software distribution based on your search criteria.

6. Select "Oracle E-Business Suite 12.2.5.0.0 for Linux x86-64" from the search result table.



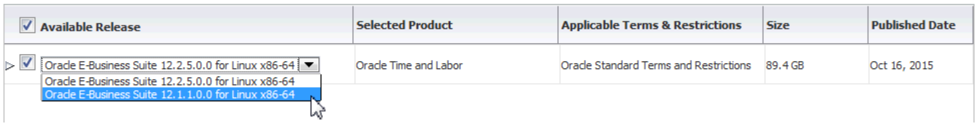
By default the most current release has been selected for you. If more than one release is currently available you may select an alternate release by clicking on the 'Select Alternate Release...' link. Once the desired releases have been selected, click on the 'Continue' button. To view the specific downloads associated with each release you may expand/collapse the list using the arrow to the left of the release name.

☑ Available Release	Selected Product	Applicable Terms & Restrictions	Size	Published Date
▷ ☑ Oracle E-Business Suite 12.2.5.0.0 for Linux x86-64, 123 files Select Alternate Release...	Oracle Time and Labor	Oracle Standard Terms and Restrictions	89.4 GB	Oct 16, 2015

Questions/Feedback, Contact Software Delivery Customer Service

Additionally, click the **Select Alternate Release** link in the Available Release column to switch to other available release version if needed.

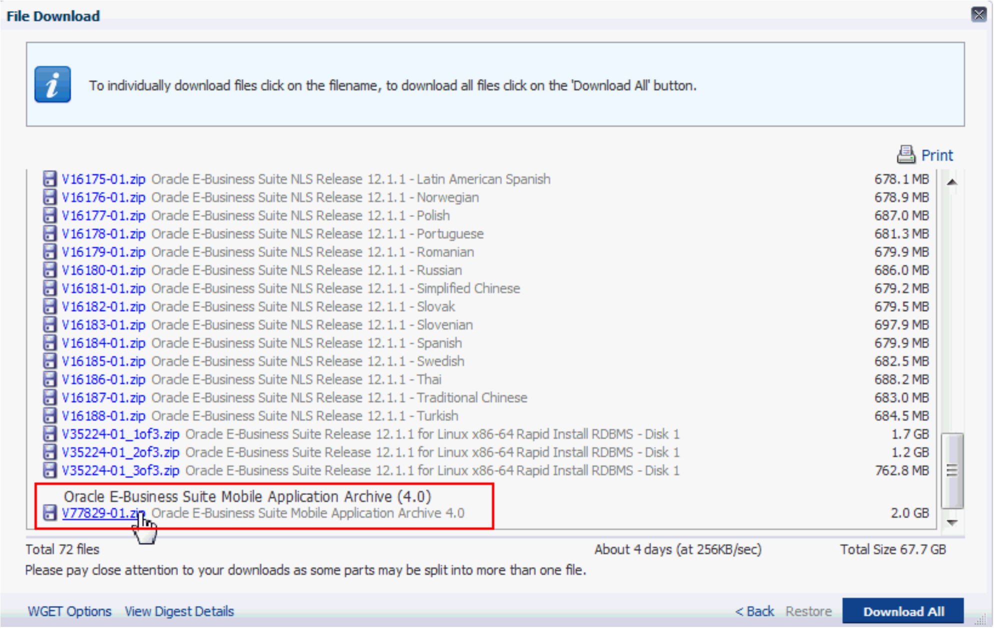
For example, select "Oracle E-Business Suite 12.1.1.0.0 for Linux x86-64" from the drop-down list if desired based on the version of your instance.



☑ Available Release	Selected Product	Applicable Terms & Restrictions	Size	Published Date
▷ ☑ Oracle E-Business Suite 12.2.5.0.0 for Linux x86-64 ▼ Oracle E-Business Suite 12.2.5.0.0 for Linux x86-64 Oracle E-Business Suite 12.1.1.0.0 for Linux x86-64	Oracle Time and Labor	Oracle Standard Terms and Restrictions	89.4 GB	Oct 16, 2015

7. Click the **Continue** button. You must accept the Oracle Standard Terms and Restrictions before you can get the list of software distributions included in your selected Oracle E-Business Suite release version.

   Download the V77829-01.zip file for "Oracle E-Business Suite Mobile Application Archive 4.0" only.



To individually download files click on the filename, to download all files click on the 'Download All' button.

V16175-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Latin American Spanish	678.1 MB
V16176-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Norwegian	678.9 MB
V16177-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Polish	687.0 MB
V16178-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Portuguese	681.3 MB
V16179-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Romanian	679.9 MB
V16180-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Russian	686.0 MB
V16181-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Simplified Chinese	679.2 MB
V16182-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Slovak	679.5 MB
V16183-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Slovenian	697.9 MB
V16184-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Spanish	679.9 MB
V16185-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Swedish	682.5 MB
V16186-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Thai	688.2 MB
V16187-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Traditional Chinese	683.0 MB
V16188-01.zip	Oracle E-Business Suite NLS Release 12.1.1 - Turkish	684.5 MB
V35224-01_1of3.zip	Oracle E-Business Suite Release 12.1.1 for Linux x86-64 Rapid Install RDBMS - Disk 1	1.7 GB
V35224-01_2of3.zip	Oracle E-Business Suite Release 12.1.1 for Linux x86-64 Rapid Install RDBMS - Disk 1	1.2 GB
V35224-01_3of3.zip	Oracle E-Business Suite Release 12.1.1 for Linux x86-64 Rapid Install RDBMS - Disk 1	762.8 MB
Oracle E-Business Suite Mobile Application Archive (4.0)		
V77829-01.zip	Oracle E-Business Suite Mobile Application Archive 4.0	2.0 GB

Total 72 files About 4 days (at 256KB/sec) Total Size 67.7 GB

Please pay close attention to your downloads as some parts may be split into more than one file.

This zip file contains the following components required for server-side configuration and enterprise distribution for Oracle E-Business Suite mobile apps:

- Consolidated server-side prerequisite patches

  For information about these server-side patches, see the *Oracle E-Business Suite Mobile Application Archive Release 4.0 Readme*, included in the downloaded zip file.

  Additionally, see Applying Prerequisite Patches on the Oracle E-Business Suite Server, page 2-2.

- Oracle Mobile Application Framework 2.1.3 for Oracle E-Business Suite Mobile Foundation Release 4.0, for working with downloaded Mobile Application Archive files

  > **Note:** Oracle Mobile Application Framework 2.1.3 for Oracle E-Business Suite Mobile Foundation Release 4.0 is also available for download from My Oracle Support through patch 21609151. See: Downloading and Installing Oracle Mobile Application Framework 2.1.3 for Oracle E-Business Suite Mobile Foundation Release 4.0, page 3-21.

- Mobile Application Archive (.maa) files delivered in zip files, along with the app-specific readme for each Oracle E-Business Suite mobile app

  The following table lists the MAA file information associated with each Oracle E-Business Suite mobile app:

Oracle E-Business Suite Mobile Application Archive Files

Mobile App Name	Associated MAA Patch	Associated MAA File
Oracle Mobile Approvals for Oracle E-Business Suite	Patch 20826606	p20826606_R12_GENERIC.zip
Oracle Mobile Timecards for Oracle E-Business Suite	Patch 21297127	p21297127_R12_GENERIC.zip
Oracle Mobile Learning for Oracle E-Business Suite	Patch 20913174	p20913174_R12_GENERIC.zip
Oracle Mobile Person Directory for Oracle E-Business Suite	Patch 21357158	p21357158_R12_GENERIC.zip
Oracle Mobile iProcurement for Oracle E-Business Suite	Patch 21293641	p21293641_R12_GENERIC.zip
Oracle Mobile Procurement for Oracle E-Business Suite	Patch 20755222	p20755222_R12_GENERIC.zip
Oracle Mobile Project Manager for Oracle E-Business Suite	Patch 21305145	p21305145_R12_GENERIC.zip
Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite	Patch 21109760	p21109760_R12_GENERIC.zip
Oracle Mobile Inventory for Oracle E-Business Suite	Patch 20754860	p20754860_R12_GENERIC.zip
Oracle Mobile Maintenance for Oracle E-Business Suite	Patch 20713862	p20713862_R12_GENERIC.zip
Oracle Mobile Process Production Supervisor for Oracle E-Business Suite	Patch 20754526	p20754526_R12_GENERIC.zip
Oracle Mobile Product Information for Oracle E-Business Suite	Patch 21318605	p21318605_R12_GENERIC.zip

Mobile App Name	Associated MAA Patch	Associated MAA File
Oracle Mobile Project Manufacturing for Oracle E-Business Suite	Patch 20759215	p20759215_R12_GENERIC.zip
Oracle Mobile Sales Orders for Oracle E-Business Suite	Patch 20780970	p20780970_R12_GENERIC.zip

You can use the app-specific MAA file to customize the app for enterprise distribution and corporate branding, and then distribute the updated version of the app to your users through your enterprise's own site rather than a public app store.

Additionally, you can further secure and manage the enterprise-distributed apps on a mobile device through integration with Oracle Mobile Security Suite (OMSS). See: Mobile Application Management (MAM) Support with Oracle Mobile Security Suite, page 5-1.

Importing a MAA File to Create a MAF Application

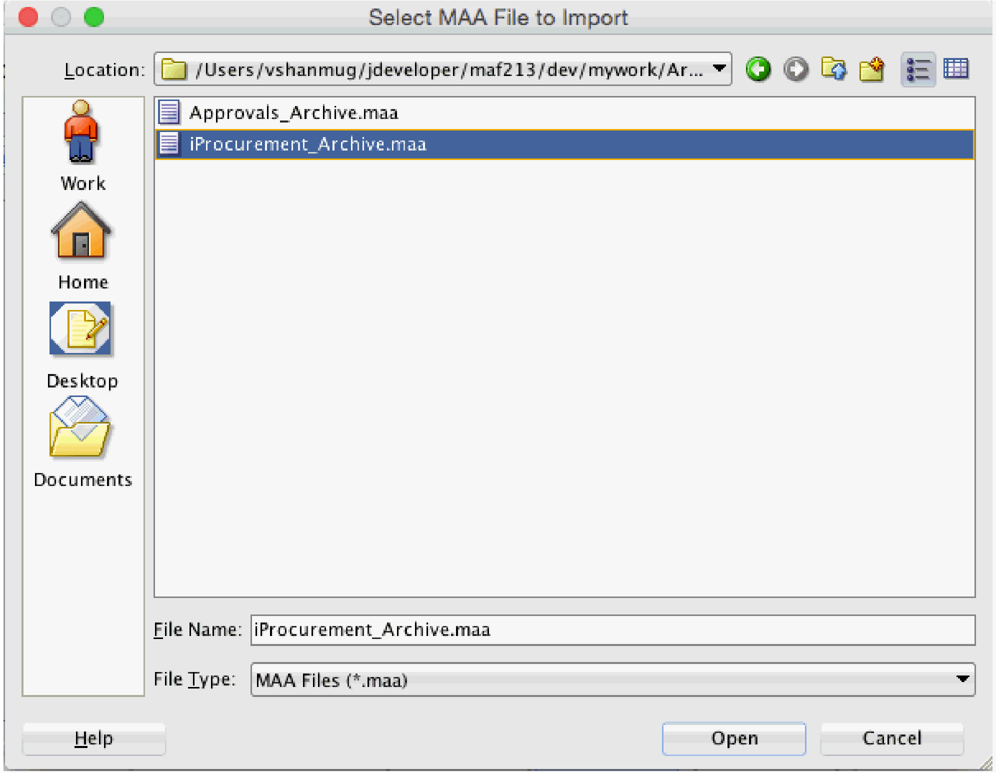
Use the following steps to create a MAF application by importing a downloaded MAA file:

1. In Oracle JDeveloper, choose **File** and then **New**.

2. In the New Gallery, choose **Applications** and then **MAF Application from Archive File** and click **OK**.

   Alternatively, choose **File**, then **File Import**, and then select **MAF Application from Archive File**.

3. In the Location page, choose **Browse** in the MAA File field to locate the .maa file (such as "iProcurement_Archive.maa") to be imported in the Select MAA File to Import page. Click **Open**.



Select MAA File to Import

Location: /Users/vshanmug/jdeveloper/maf213/dev/mywork/Ar...

Approvals_Archive.maa

iProcurement_Archive.maa

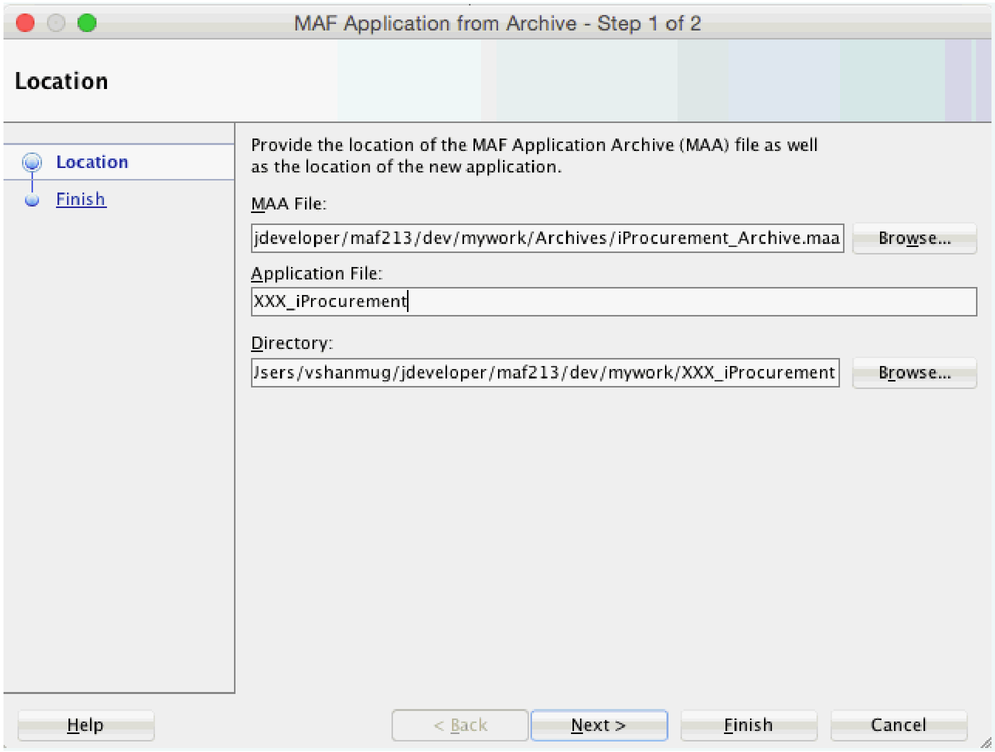
File Name: iProcurement_Archive.maa

File Type: MAA Files (*.maa)

Note: The screenshots in this guide show the appearance of the pages on a Mac system. The look and feel may vary on a PC.

The selected iProcurement_Archive.maa file is displayed in the MAA File field.

4. Perform the following steps if needed or accept the default values in the Location page:



MAF Application from Archive - Step 1 of 2

Location

Provide the location of the MAF Application Archive (MAA) file as well as the location of the new application.

MAA File: jdeveloper/maf213/dev/mywork/Archives/iProcurement_Archive.maa

Application File: XXX_iProcurement

Directory: Jsers/vshanmug/jdeveloper/maf213/dev/mywork/XXX_iProcurement

1. In the Application File field, enter a name of the mobile application derived from .maa file, such as "XXX_iProcurement".

2. In the Directory field, click **Browse** to retrieve the directory of the mobile application.

5. Click **Next**.

6. Review the import summary information and then click **Finish**.

   A new MAF application is created.

For information on creating an unsigned application and what happens after importing a MAA file, refer to Creating Unsigned Deployment Packages, *Oracle Fusion Middleware Developing Mobile Applications with Oracle Mobile Application Framework*.

Updating Plugin Configuration (Optional)

If your mobile apps include a Cordova plugin, such as barcode scanner, to provide support for scanning barcodes to capture data, the related plugin library is already packaged with the associated MAA files. For information about Oracle E-Busness Suite mobile apps with barcode scanner, see Supporting for Barcodes, page 2-52

In order for your app to use the plugin, before you deploy the app, perform the following steps to update the plugin's path after creating the application:

1. Open Oracle JDeveloper.

2. In the Applications Navigator, expand the **Application Resources** panel, then the **Descriptors** folder, and then the **ADF META-INF** folder.

3. Double-click the **`maf-application.xml`** file.

4. In the overview editor that appears, click the Plugins navigation tab.

5. For the Cordova plugin, update the path to point to the `<Application Root Folder>/src` folder where barcode scanner is placed.

For more information on registering additional plugins in your MAF applications, see Using Plugins in MAF Applications, *Oracle Fusion Middleware Developing Mobile Applications with Oracle Mobile Application Framework*.

Importing Additional Root-CA Certificates (Optional)

If your Oracle E-Business Suite environment is SSL-enabled, for mobile apps with enterprise distribution, it is possible to import additional root-CA certificates into your MAF application's truststore if the HTTPS server contains certificates not present in your MAF application's cacerts file.

For information on updating and managing certificates in the cacerts file, see Migrating to New cacerts File for SSL in MAF 2.1.3, *Oracle Mobile Application Framework Installing Oracle Mobile Application Framework*.

For more information about HTTPS and how to validate your SSL certificates, see Secure Communication with HTTPS, page 6-3.

Changing Application Bundle Id

For enterprise distribution, even if no change is planned to a MAA file but simply distribute the associated app to an enterprise's own site, it is still required to make certain changes to the app. For example, the Application Bundle Id must be unique for each app installed on an iOS device, although the app content itself is exactly the same.

This change is internal to an app, but it helps technically differentiate an enterprise app from a public one in the backend.

Instructions to Change the Application Bundle Id

Perform the following steps to change the Application Bundle Id:

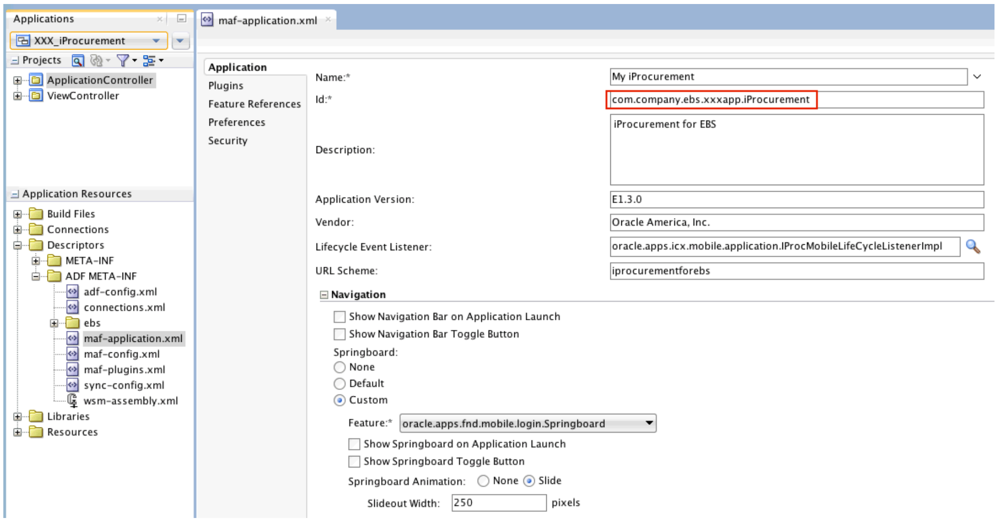
1. Open Oracle JDeveloper.

2. In the Applications Navigator, expand the **Application Resources** panel, then the **Descriptors** folder, and then the **ADF META-INF** folder.

   Double-click the **`maf-application.xml`** file to open the overview editor for the **`maf-application.xml`** file.

For information on the **`maf-application.xml`** file, see About the MAF Application Feature Configuration File, MAF Application and Project Files, *Oracle Fusion Middleware Developing Mobile Applications with Oracle Mobile Application Framework*.

Overview Editor for the maf-application.xml File



Name:* My iProcurement

Id:* com.company.ebs.xxxapp.iProcurement

Description: iProcurement for EBS

Application Version: E1.3.0

Vendor: Oracle America, Inc.

Lifecycle Event Listener: oracle.apps.icx.mobile.application.IProcMobileLifeCycleListenerImpl

URL Scheme: iprocurementforebs

Navigation

□ Show Navigation Bar on Application Launch

□ Show Navigation Bar Toggle Button

Springboard:

○ None

○ Default

● Custom

Feature:* oracle.apps.fnd.mobile.login.Springboard

□ Show Springboard on Application Launch

□ Show Springboard Toggle Button

Springboard Animation: ○ None ● Slide

Slideout Width: 250 pixels

3. Modify the Id field in the **`maf-application.xml`** file. Do not change any other fields in this file.

> **Important:** For enterprise distribution, the Application Version delivered in the MAA file for each app is prefixed with letter "E", such as "E1.3.0", to indicate this app is created from the MAA file. This helps distinguish the enterprise-distributed apps from the publicly-distributed ones. This app version information is displayed in the About page for each app.
>
> To keep track of the enterprise app versions used in your company, you must continue to use the version provided in the MAA file, but you can add additional decimals at the end of the version. For example,
>
> - Standard MAA version: E1.3.0
> - Suggested customized version: E1.3.0.x.x, such as E1.3.0.1.0

Id: Replace the Id with a unique Id to identify the mobile app for enterprise distribution.

The downloaded Oracle E-Business Suite mobile app MAA file contains the Application Bundle Id in the following format:

`com.company.ebs.<prodfamily>.<product>.<AppName>`

For example, the Bundle Id from the MAA file corresponding to Oracle Mobile iProcurement for Oracle E-Business Suite is `com.company.ebs.prc.icx.iProcurement`.

In this example, use `com.company.ebs.xxxapp.iProcurement` as the Id.

- `company`- This can be replaced with your company name.
- `xxxapp`- It indicates to which Oracle E-Business Suite application it belongs.

> **Important:** The Id value in the **`maf-application.xml`** file is used to download configuration details for the app. Therefore, use this Id as the Application Bundle Id value in the Application Details page when registering an enterprise app on the Oracle E-Business Suite server through the Mobile Applications Manager responsibility. See: Registering and Updating Your Enterprise Mobile App Definition Metadata, page 3-4.
>
> If the registration corresponding to this Id is not found on the server, the associated mobile app cannot connect to that Oracle E-Business Suite instance.

The Application Bundle Id is used to fetch the mobile app's configuration file from the Oracle E-Business Suite server. This change is internal to an app allowing administrators to quickly differentiate the enterprise version from the publicly-distributed one on the enterprise's server.

Administrators use the Application Bundle Id to construct and validate the configuration service URL to ensure the app can be accessible from mobile users. For information on how to construct the configuration service URL using the Application Bundle Id, see Validating the Configuration, page 2-32.

Additionally, use the Application Bundle Id to help diagnose and troubleshoot any potential issues if occur at a mobile client. See: Enabling Client Logging, page 7-2.

4. Leave the rest of the fields unchanged. Save your work.

Changing Privacy Policy Link

The privacy policy change is reflected in the About page of the app. After the change, when a user clicks the link, it should point to your company's privacy policy, not Oracle's Privacy Policy.

Instructions to Change the Privacy Policy Link

Perform the following steps to change the privacy policy URL link:

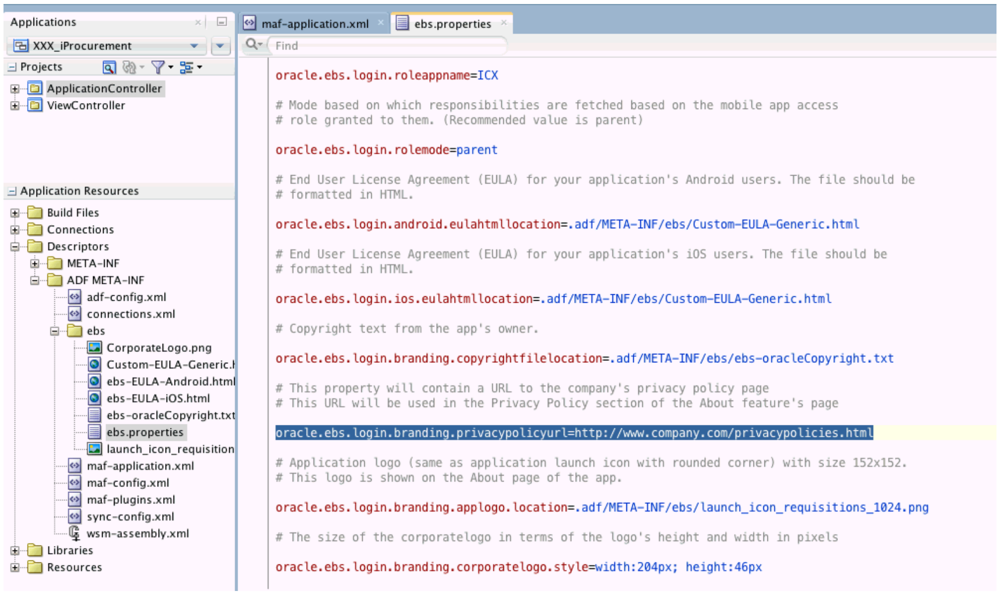
1. Open Oracle JDeveloper.

2. In the Applications Navigator, expand the **Application Resources** panel, then the **Descriptors** folder, then the **ADF META-INF** folder, and then the **ebs** folder.

   Double-click the **`ebs.properties`** file to open it in an editor.

3. Replace the following privacy policy URL in the **`ebs.properties`** file with your company's policy URL:

   `oracle.ebs.login.branding.privacypolicyurl`
   `=http://www.company.com/privacy-policy.html`

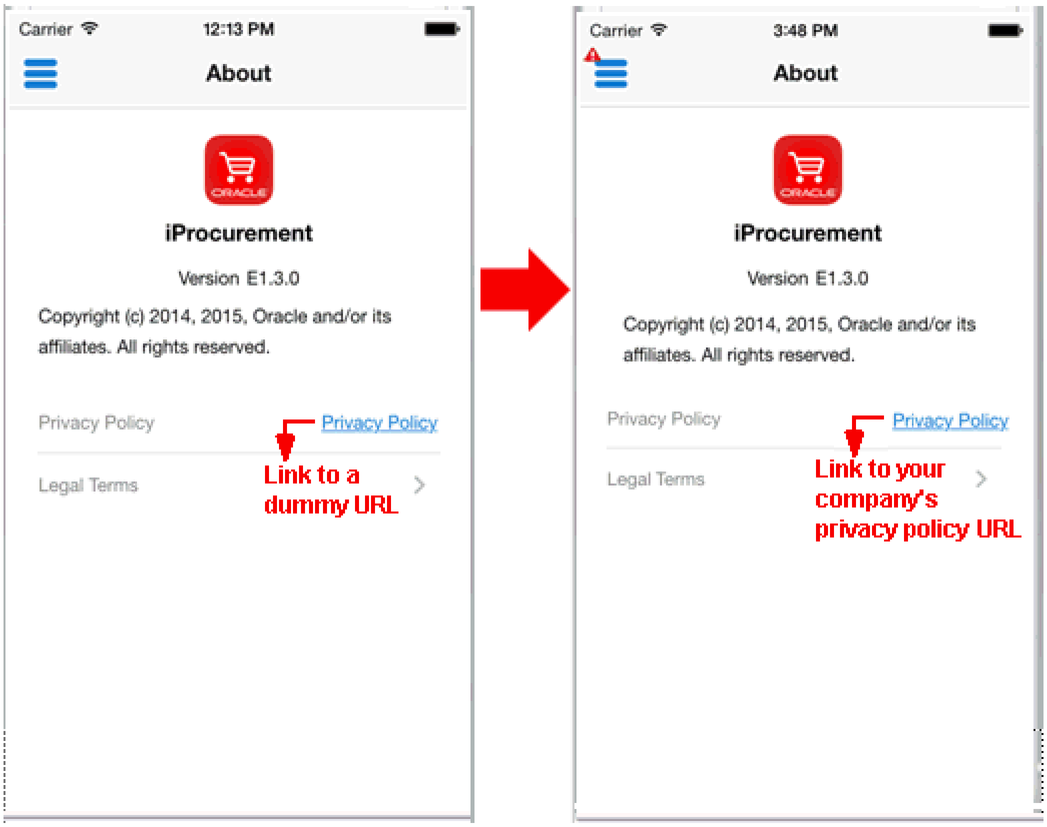
   ```
   oracle.ebs.login.roleappname=ICX

   # Mode based on which responsibilities are fetched based on the mobile app access
   # role granted to them. (Recommended value is parent)

   oracle.ebs.login.rolemode=parent

   # End User License Agreement (EULA) for your application's Android users. The file should be
   # formatted in HTML.

   oracle.ebs.login.android.eulahtmllocation=.adf/META-INF/ebs/Custom-EULA-Generic.html

   # End User License Agreement (EULA) for your application's iOS users. The file should be
   # formatted in HTML.

   oracle.ebs.login.ios.eulahtmllocation=.adf/META-INF/ebs/Custom-EULA-Generic.html

   # Copyright text from the app's owner.

   oracle.ebs.login.branding.copyrightfilelocation=.adf/META-INF/ebs/ebs-oracleCopyright.txt

   # This property will contain a URL to the company's privacy policy page
   # This URL will be used in the Privacy Policy section of the About feature's page

   oracle.ebs.login.branding.privacypolicyurl=http://www.company.com/privacypolicies.html

   # Application logo (same as application launch icon with rounded corner) with size 152x152.
   # This logo is shown on the About page of the app.

   oracle.ebs.login.branding.applogo.location=.adf/META-INF/ebs/launch_icon_requisitions_1024.png

   # The size of the corporatelogo in terms of the logo's height and width in pixels

   oracle.ebs.login.branding.corporatelogo.style=width:204px; height:46px
   ```

   Please note that the downloaded Oracle E-Business Suite mobile app MAA file contains the following dummy URL:
   `http://www.company.com/privacy-policy.html`

4. Save your work.

The following example shows the revised privacy policy URL link in the About page for the iProcurement app (Oracle Mobile iProcurement for Oracle E-Business Suite) on the iOS device.

In this example, nothing is changed in the app from the associated MAA file except that the privacy policy URL link is changed from pointing to a dummy URL to your company's privacy policy URL.



Copyright (c) 2014, 2015, Oracle and/or its affiliates. All rights reserved.

Copyright (c) 2014, 2015, Oracle and/or its affiliates. All rights reserved.

Using Mobile App Access Roles

Oracle E-Business Suite mobile apps use the app-specific roles that are set up in the MAF application's `ebs.properties` file for each app to validate whether a mobile user has the privileges to access a designated app and connect to Oracle E-Business Suite. Therefore, once mobile app access roles are defined in the Oracle E-Business Suite, a mobile applications developer needs to specify the corresponding access roles in the `ebs.properties` file for the enterprise apps.

For information on creating the mobile app access roles on the Oracle E-Business Suite server, see Creating Mobile App Access Roles, page 3-16.

Use the following steps to add the mobile app access roles in the `ebs.properties` file:

1. Open Oracle JDeveloper.

2. In the Application Navigator, expand the **Application Resources** panel.

3. Expand the **Descriptors** folder node and then the **ADF META-INF** folder node. Expand the **ebs** folder node.

   Double-click the **`ebs.properties`** file to open it in an editor.

4. Change the following properties to specify the role that your enterprise app (such as XXX_iProcurement) uses:

   - **`oracle.ebs.login.rolecode=`**`<UMX Role Code>`

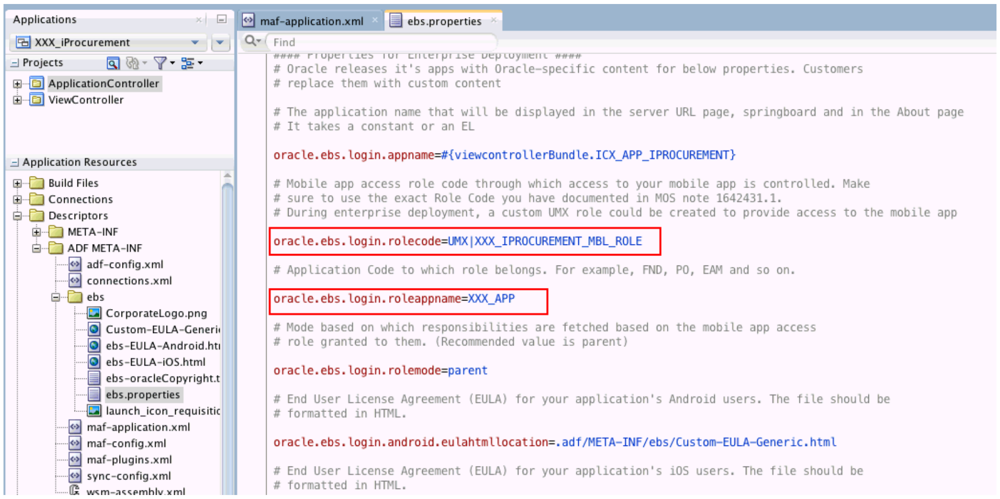
     If `UMX|XXX_IPROCUREMENT_MBL_ROLE` is a new role created earlier under the custom application called `XXX`, then replace `<UMX Role Code>` with this role `UMX|XXX_IPROCUREMENT_MBL_ROLE` in the property as shown here:

     `oracle.ebs.login.rolecode=``UMX|XXX_IPROCUREMENT_MBL_ROLE`

   - **`oracle.ebs.login.roleappname=`**`<Application Code>`

     Replace `<Application Code>` with `XXX_APP` in the property as shown here:

     `oracle.ebs.login.roleappname=``XXX_APP`



```
#### Properties for Enterprise Deployment ####
# Oracle releases it's apps with Oracle-specific content for below properties. Customers
# replace them with custom content

# The application name that will be displayed in the server URL page, springboard and in the About page
# It takes a constant or an EL

oracle.ebs.login.appname=#{viewcontrollerBundle.ICX_APP_IPROCUREMENT}

# Mobile app access role code through which access to your mobile app is controlled. Make
# sure to use the exact Role Code you have documented in MOS note 1642431.1.
# During enterprise deployment, a custom UMX role could be created to provide access to the mobile app

oracle.ebs.login.rolecode=UMX|XXX_IPROCUREMENT_MBL_ROLE

# Application Code to which role belongs. For example, FND, PO, EAM and so on.

oracle.ebs.login.roleappname=XXX_APP

# Mode based on which responsibilities are fetched based on the mobile app access
# role granted to them. (Recommended value is parent)

oracle.ebs.login.rolemode=parent

# End User License Agreement (EULA) for your application's Android users. The file should be
# formatted in HTML.

oracle.ebs.login.android.eulahtmllocation=.adf/META-INF/ebs/Custom-EULA-Generic.html

# End User License Agreement (EULA) for your application's iOS users. The file should be
# formatted in HTML.
```

5. Save your work.

Customizing Mobile Apps for Corporate Branding (Optional)

In addition to the required changes for enterprise app creation, you can further customize corporate branding for the app to establish corporate identity by replacing Oracle logo with your own company logo.

Instructions on replacing Oracle logo with your customized company and app logos or images are documented in a separate chapter in this book. See: Customizing Mobile Apps for Corporate Branding (Optional), page 4-1.

> **Note:** Please note that functional customization and personalization are not supported in this release.

Modifying an Existing Deployment Profile (Conditional)

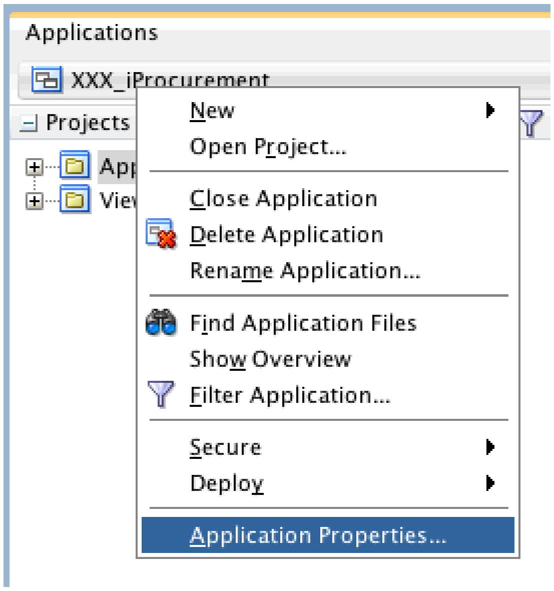
After modifying the required changes for enterprise distribution, a mobile applications developer needs to prepare the platform-specific deployment profile by editing the existing deployment profile associated with the app provided with the MAA file.

> **Important:** If you have customized the mobile app for corporate branding (described as an optional task in the previous section), you must have already created a new deployment profile. In this situation, skip this step and do not modify an existing deployment profile.

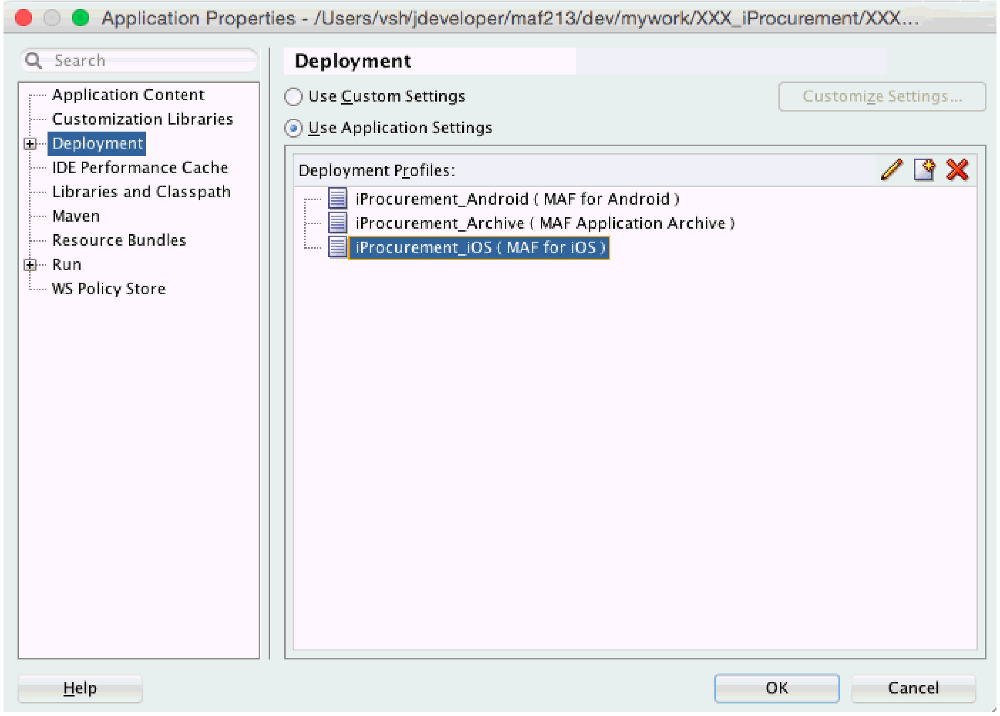
Please note that the deployment profile defines how an app will be deployed to iOS or Android powered devices, iOS simulators, or Android emulators.

Use the following steps to modify an existing deployment profile for your desired platform:

1. In the Applications Navigator of Oracle JDeveloper, select and right-click the **Application**. Choose **Application Properties** from the selection window.



2. In the Application Properties window, select the **Deployment** node from the left pane.



Application Properties - /Users/vsh/jdeveloper/maf213/dev/mywork/XXX_iProcurement/XXX...

Deployment

○ Use Custom Settings

● Use Application Settings

Deployment Profiles:

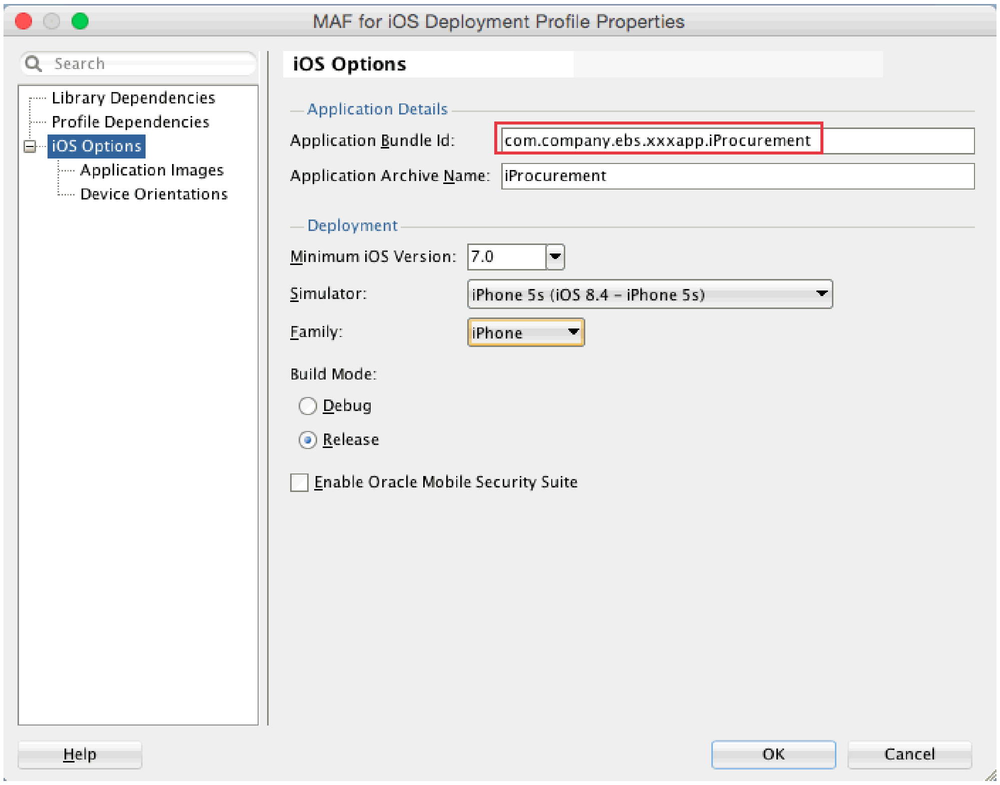
- iProcurement_Android (MAF for Android)
- iProcurement_Archive (MAF Application Archive)
- iProcurement_iOS (MAF for iOS)

In the Deployment Profiles region, select the deployment profile you want to edit based on the platform and click on the **Edit** icon.

> **Note:** For each mobile app, there are three deployment profiles delivered with the MAF archives. Specifically, one profile (<AppName>_iOS) for the iOS platform, another one (<AppName>_Android) for the Android platform, and the other one (<AppName>_Archive) for the MAA file.

3. Editing MAF for iOS Deployment Profile

If the selected deployment profile (such as iProcurement_iOS) is for the iOS platform, the MAF for iOS Deployment Profile Properties page appears.



Application Bundle Id: com.company.ebs.xxxapp.iProcurement

Application Archive Name: iProcurement

Minimum iOS Version: 7.0

Simulator: iPhone 5s (iOS 8.4 – iPhone 5s)

Family: iPhone

Build Mode:

○ Debug

● Release

□ Enable Oracle Mobile Security Suite

Replace the Application Bundle Id with a unique Id for your app, such as `com.company.ebs.xxxapp.iProcurement`. It is recommended that use the same value from the Id field that you modified in the **`maf-application.xml`** file, as described earlier in the Changing Application Bundle Id, page 3-30.

The Application Bundle Id is used to package the application binary for iOS. Please note that the Bundle Id must be unique for each app installed on an iOS or Android device. Even if the same app has been deployed twice for an enterprise, different Bundle Id uniquely represents each individual app. For example, one app can be used for production and the other one can be for testing purposes if desired.

Additionally, the Application Bundle Id used here impacts only the application binary packaging and its installation on mobile devices. It does not have any impact on the Oracle E-Business Suite server. For example, you could have packaged two apps with two different Application Bundle Ids in the MAF deployment profiles, such as `com.company.ebs.xxxapp.XXiProcurement` and `com.company.ebs.xxxapp.YYiProcurement`, but both could have the same Id in the **`maf-application.xml`** file, such as `com.company.ebs.xxxapp.iProcurement`. Both apps can be installed on the same mobile device and both apps can connect to the same Oracle E-Business Suite server using one single registration on the Oracle E-Business Suite server.

This is useful that you create one single app registration on the Oracle E-Business Suite server, and you can download and apply them to other Oracle E-Business

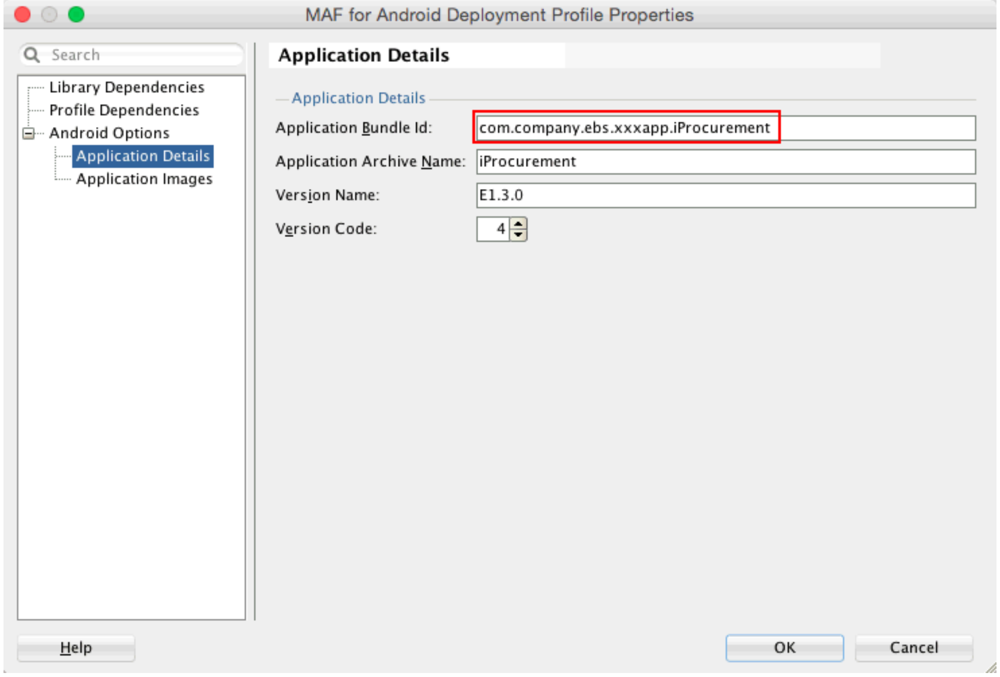
Suite instances. You can then use multiple installations of the same app on a single test device and test against different Oracle E-Business Suite instances.

4. This Application Bundle Id is the only field you need to modify in this page. Click **OK**.

5. **Editing MAF for Android Deployment Profile**

   If the selected deployment profile (such as iProcurement_Android) is for the Android platform, the MAF for Android Deployment Profile Properties page appears.

   Select "Application Details" from the Android Options tree node.



Application Details

Application Details

Application Bundle Id: com.company.ebs.xxxapp.iProcurement

Application Archive Name: iProcurement

Version Name: E1.3.0

Version Code: 4

   Similar to the update for the iOS deployment profile, you only need to replace the Application Bundle Id with a unique Id, such as `com.company.ebs.xxxapp.iProcurement` in this page. Use the same value from the Id field that you modified in the **`maf-application.xml`** file, as described earlier in the Changing Application Bundle Id, page 3-30.

   Click **OK** to save your work.

For information on creating deployment profiles, see Working with Deployment Profiles, *Oracle Fusion Middleware Developing Mobile Applications with Oracle Mobile Application Framework*.

Deploying Your Enterprise Mobile Apps

Deploying the Generated Application Binary Files

After completing the required changes for the enterprise app, a developer can deploy the app for the iOS, Android, or both platforms. At this stage, the developer has already performed either one of the following for the deployment profile(s):

- Modified an existing deployment profile to change only the Application Bundle ID for enterprise distribution

  See: Modifying an Existing Deployment Profile (Conditional), page 3-36.

- Created a new deployment profile with customized app images for corporate branding

  See: Creating a New Deployment Profile with Customized App Logos and Splash Screen, page 4-10.

Use the appropriate deployment profile to deploy and test the app in the iOS simulators or Android emulators. For information on setting up the iOS and Android simulators, see: Installing Development Tools and Setting Up a Development Environment, page 3-21.

If the test results are successful, the developer can generate the application binary file. For iOS, the archive format is an IPA file, known as an iOS application bundle. For Android, the format is an Android application package (APK) file.

> **Important:** The enterprise app must be distributed to an enterprise's own site and is only available to the enterprise's internal users. It cannot be distributed to any third party users. Additionally, this app cannot be redistributed to a public app store.

For more information on deploying the app to an iOS simulator or an Android emulator as well as deploying the app to an iOS-powered or Android-powered device, see Deploying MAF Applications, *Oracle Fusion Middleware Developing Mobile Applications with Oracle Mobile Application Framework*.

For information on deploying the apps with Oracle Mobile Security Suite, see Containerizing Enterprise-Distributed Oracle E-Business Suite Mobile Apps Using OMSS, page 5-2.

4

Customization Support for Corporate Branding

Overview

In addition to performing the required changes to an app for enterprise distribution, you can customize corporate branding for your app.

> **Important:** Changing icons or logos is to establish corporate branding for your enterprise app and this is not considered as functional change. In this release, functional customization is not supported.

To implement corporate branding to replace the Oracle logos with your enterprise logo, you must change:

- App logo
- Company logo
- Splash screen

Additionally, you can change the following attributes to distinguish your customizations:

- App Name
- End User License Agreement
- Copyright

Specifically, the following table lists the corporate branding available in Oracle E-Business Suite Mobile Foundation Release 4.0. Developers can modify these artifacts included in a MAA file for corporate branding.

Allowed Artifact Modification	Impacted Mobile App Page or Icon	Associated Change Instructions
App Logo	• Updated through a deployment profile: • Launcher icon for an app on a mobile device's home screen, including both iOS and Android platforms • Settings icon against the app name on an iOS device • Spotlight search on an iOS device • Updated in the Oracle JDeveloper project: • About page of the app for both iOS and Android • Page header on an Android device	• Customizing App Logo through a deployment profile: 1. Creating a New Deployment Profile, page 4-10 2. Changing App Logo and Splash Screen through a Deployment Profile, page 4-16 • Customizing App Logo through an Oracle JDeveloper project: Changing App Logo in the About Page and Android Page Header, page 4-21
Splash Screen	• Shown after the Sign In screen	1. Creating a New Deployment Profile, page 4-10 2. Changing App Logo and Splash Screen through a Deployment Profile, page 4-16
Company Logo	• Sign In screen • Server URL screen	Customizing the Company Logo, page 4-22

Allowed Artifact Modification	Impacted Mobile App Page or Icon	Associated Change Instructions
App Name (Optional)	• Sign In screen • Server URL screen • Springboard • About page	Changing the App Name (Optional), page 4-26
Legal Terms including End User License Agreement and Copyright (Optional)	• End User License Agreement shown during the initial launch of an app • Copyright shown in the About page	• Customizing End User License Agreement or Legal Terms (Optional), page 4-31 • Customizing the Copyright in the About Page (Optional), page 4-33

The image sizing requirements for app logo, company logo, and splash screen listed in the table are described in the next section, Required Image Sizing Information for Corporate Branding, page 4-3.

For step-by-step instructions on customizing the app for corporate branding, see:

- Creating a New Deployment Profile, page 4-10
- Changing App Logo and Splash Screen through a Deployment Profile, page 4-16
- Changing App Logo in the About Page and Android Page Header, page 4-21
- Customizing the Company Logo, page 4-22
- Changing the App Name (Optional), page 4-26
- Customizing the Legal Related Information (Optional), page 4-31

Required Image Sizing Information for Corporate Branding

Before you begin the customization for corporate branding, prepare the images or icons based on the sizing requirements described in the following sections:

- Required Image Sizing Information for the iOS Platform, page 4-4
- Required Image Sizing Information for the Android Platform, page 4-7

- Common Sizing Requirements for the iOS and Android Platforms, page 4-9

Please note that all dimensions for images described in this section are in pixels.

Required Image Sizing Information for the iOS Platform

This section describes custom icons in specific sizes for application images if required to customize corporate branding for the iOS platform.

- Application Icon
- Splash Screen
- Spotlight
- Settings

For more information on iOS application icon images, see the "Icon and Image Design" section in the iOS Human Interface Guidelines. This document is available from the iOS Developer Library (http://developer.apple.com/library/ios/navigation/).

> **Note:** Oracle E-Business Suite mobile apps use squared corner icons since iOS automatically rounds them in the corner.

For required image sizing information for app logo and company logo, see Common Sizing Requirements for the iOS and Android Platforms, page 4-9.

Sizing Requirements for Application Icon

The following table describes the sizing information for application icons:

> **Note:** To easily distinguish the custom icons for corporate branding from the default icons used in the Oracle E-Business Suite mobile apps, a prefix "XXX_" is added to the custom icon file names.

Sizing Requirements for Application Icon

Device Type	Description	Size	Recommended File Names
iPhone App 2x	Application icon for iPhone/iPod touch Retina	120x120	XXX_Icon-120.png

Device Type	Description	Size	Recommended File Names
iPhone App 3x	Application icon for iPhone 6 Plus	180x180	XXX_Icon-60@3x.png
iPad App 1x	Application icon for iPad Non-Retina	76x76	XXX_Icon-76.png
iPad App 2x	Application icon for iPad Retina	152x152	XXX_Icon-76@2x.png

Sizing Requirements for Splash Screen

The following table describes the sizing information for splash screen:

Sizing Requirements for Splash Screen

Device Type	Description	Size	Recommended File Names
Portrait iPhone 4S	Launch screen for iPhone 4S	640x960	XXX_Default@2x.png
Portrait iPhone 2x	Launch screen for iPhone/iPod touch Retina	640x1136	XXX_Default-568h@2x.png
Portrait iPhone 6	Launch screen for iPhone 6	750x1334	XXX_Default-667h@2x.png
Portrait iPhone 6 Plus	Portrait launch screen for iPhone 6 Plus	1242x2208	XXX_Default-1104h@2x.png
Landscape iPhone 6 Plus	Landscape launch screen for iPhone 6 Plus	2208x1242	XXX_Default-Landscape-621@2x.png
Portrait iPad 1x	Portrait launch screen for iPad Non-Retina	768x1024	XXX_Default-PortraitRetina.png
Portrait iPad 2x	Portrait launch screen for iPad Retina	1536x2048	XXX_Default-PortraitRetina@2x.png

Device Type	Description	Size	Recommended File Names
Landscape iPad 1x	Landscape launch screen for iPad Non-Retina	1024x768	XXX_Default-LandscapeRetina.png
Landscape iPad 2x	Landscape launch screen for iPad Retina	2048x1536	XXX_Default-LandscapeRetina@2x.png

Sizing Requirements for Spotlight

The following table describes the sizing information for spotlight:

Please note all spotlight icons should be squared corner.

Sizing Requirements for Spotlight

Device Type	Description	Size	Recommended File Names
Spotlight 1x	Spotlight icon for iPad Non-Retina	40x40	XXX_Icon-40.png
Spotlight 2x	Spotlight icons for Retina devices	80x80	XXX_Icon-40@2x.png
Spotlight 3x	Spotlight icon for iPhone 6 Plus	120x120	XXX_Icon-40@3x.png

Sizing Requirements for Settings

The following table describes the sizing information for settings:

Please note all settings icons should be squared corner.

Sizing Requirements for Settings

Device Type	Description	Size	Recommended File Names
Settings 1x	Settings icon for iPad Non-Retina	29x29	XXX_Icon-29.png

Device Type	Description	Size	Recommended File Names
Settings 2x	Settings icon for Retina devices	58x58	XXX_Icon-29@2x.png
Settings 3x	Settings icon for iPhone 6 Plus	87x87	XXX_Icon-29@3x.png

For instructions on customizing app icon, splash screen, spotlight, and settings, see Instructions to Create a New Deployment Profile for the iOS Platform, page 4-10 and Changing App Logo and Splash Screen through a Deployment Profile, page 4-16.

Required Image Sizing Information for the Android Platform

This section describes custom icons in specific sizes for application images if required to customize corporate branding for the Android platform.

> **Note:** Oracle E-Business Suite mobile apps use rounded corner icons for Android apps since Android does not round them automatically.

- Application Launch Icon
- Splash Screen (Portrait)
- Splash Screen (Landscape)

For required image sizing information for app logo and company logo, see Common Sizing Requirements for the iOS and Android Platforms, page 4-9.

Sizing Requirements for Application Launch Icon, Splash Screen (Portrait), and Splash Screen (Landscape)

The following table describes the image sizing information for application launch icon, splash screen (portrait), and splash screen (landscape):

> **Note:** To easily distinguish the custom icons for corporate branding from the default icons used in the Oracle E-Business Suite mobile apps, a prefix "XXX_" is added to the custom icon file names as shown in this table.

Sizing Requirements for Application Launch Icon, Splash Screen (Portrait), and Splash Screen (Landscape)

Platform Display Type	Icon	Size	Recommended File Names
Low Density	Application Launch Icon	36x36	XXX_display-ldpi-icon.png
	Splash Screen (Portrait)	480x800	XXX_display-port-ldpi-splashscreen.png
	Splash Screen (Landscape)	800x480	XXX_display-land-ldpi-splashscreen.png
Medium Density	Application Launch Icon	48x48	XXX_display-mdpi-icon.png
	Splash Screen (Portrait)	480x800	XXX_display-port-mdpi-splashscreen.png
	Splash Screen (Landscape)	800x480	XXX_display-land-mdpi-splashscreen.png
High Density	Application Launch Icon	72x72	XXX_display-hdpi-icon.png
	Splash Screen (Portrait)	800x1280	XXX_display-port-hdpi-splashscreen.png
	Splash Screen (Landscape)	1280x800	XXX_display-land-hdpi-splashscreen.png
High Density	Application Launch Icon	72x72	XXX_display-hdpi-icon.png
	Splash Screen (Portrait)	800x1280	XXX_display-port-hdpi-splashscreen.png
	Splash Screen (Landscape)	1280x800	XXX_display-land-hdpi-splashscreen.png
Extra High Density	Application Launch Icon	96x96	XXX_display-xhdpi-icon.png

Platform Display Type	Icon	Size	Recommended File Names
	Splash Screen (Portrait)	768x1024	XXX_display-port-xhdpi-splashscreen.png
	Splash Screen (Landscape)	1024x768	XXX_display-land-xhdpi-splashscreen.png

For instructions on customizing application logo and splash screen through a deployment profile, see Instructions to Create a New Deployment Profile for the Android Platform, page 4-14 and Changing App Logo and Splash Screen through a Deployment Profile, page 4-16.

Common Sizing Requirements for the iOS and Android Platforms

This section includes the following sizing requirements for the iOS and Android platforms:

- App Logo
- Company Logo

Sizing Requirements for App Logo

The following table describes the sizing information for app logo:

- Similar to the application's launch icon, the app logo uses the same rounded corners.
- Image files should be in `.png` format.

Sizing Requirements for App Logo

Use	Size	Recommended File Names
App Logo on About page	152x152	Add a prefix "XXX_" to the custom app logo file name
App Logo on Page Header (Android Only)	80x80	android_app_header_icon.png

For instructions on customizing application logo in the About page and page header, see Changing App Logo in the About Page and Android Page Header, page 4-21.

Sizing Requirements for Company Logo

The following table describes the sizing information for company logo:

Sizing Requirements for Company Logo

Description	Size
Maximum width	400
Minimum width	100
Maximum height	200
Minimum height	50

Once the company logo is created, name the image file as `CorporateLogo.png`.

For instructions on how to change the company logo, see Customizing the Company Logo, page 4-22.

Creating a New Deployment Profile

In addition to the required changes for enterprise distribution, you can further customize corporate branding with custom app logos or images through a new deployment profile.

This section provides information on how to create a new deployment profile for each platform.

- Instructions to Create a New Deployment Profile for the iOS Platform, page 4-10
- Instructions to Create a New Deployment Profile for the Android Platform, page 4-14

Instructions to Create a New Deployment Profile for the iOS Platform

To customize corporate branding for your app, instead of editing an existing deployment profile, a developer needs to create a new deployment profile first, and then replace the default Oracle image used for the app icons with custom images. All images should be in `.png` format.

Copying the Custom Icons

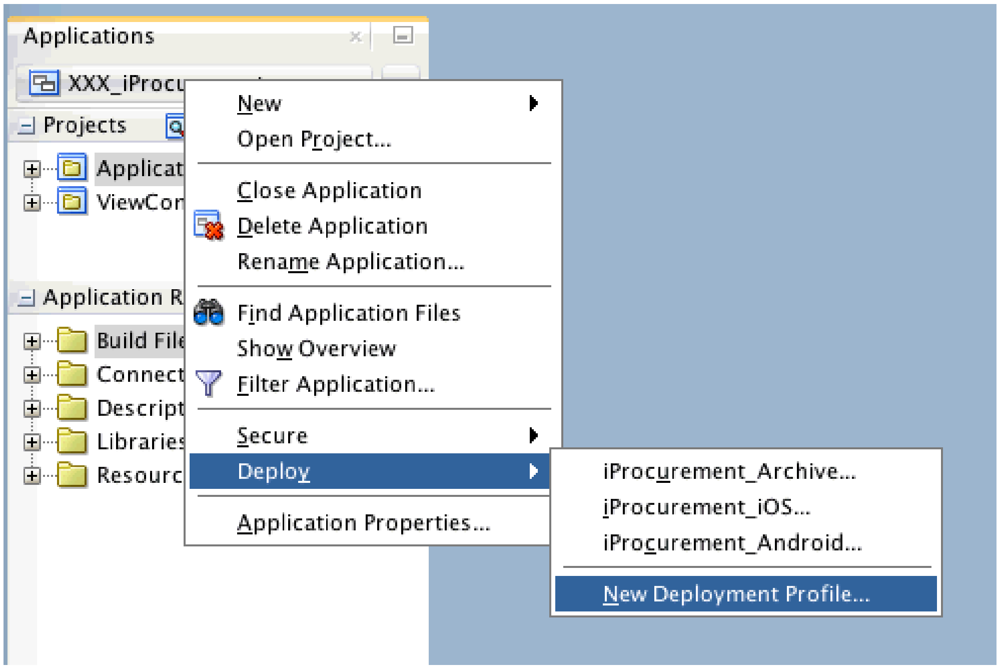
Before creating a new deployment profile, copy the custom icon files to the following location where the default icons are also placed:

```
<Application Root Folder>/resources/ios
```

Creating a New Deployment Profile

Perform the following steps to create a new deployment profile:

1. In the Applications Navigator of Oracle JDeveloper, select "XXX_iProcurement" application and then right-click on it. Select **Deploy** and then **New Deployment Profile...** from the selection window.



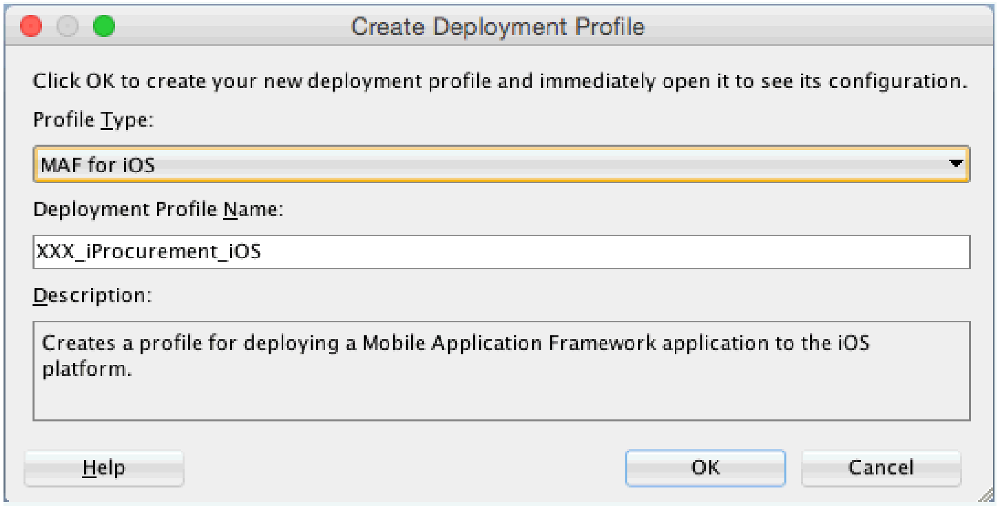
2. In the Create Deployment Profile page, enter the following information:

   - Select **MAF for iOS** as the Profile Type field.

     If "MAF for Android" is selected as the deployment profile type, see Instructions to Create a New Deployment Profile with Customized App Logos for the Android Platform, page 4-14.

   - Enter a new name, such as "XXX_iProcurement_iOS", as the Deployment Profile Name if required.

   Click **OK**.



Create Deployment Profile

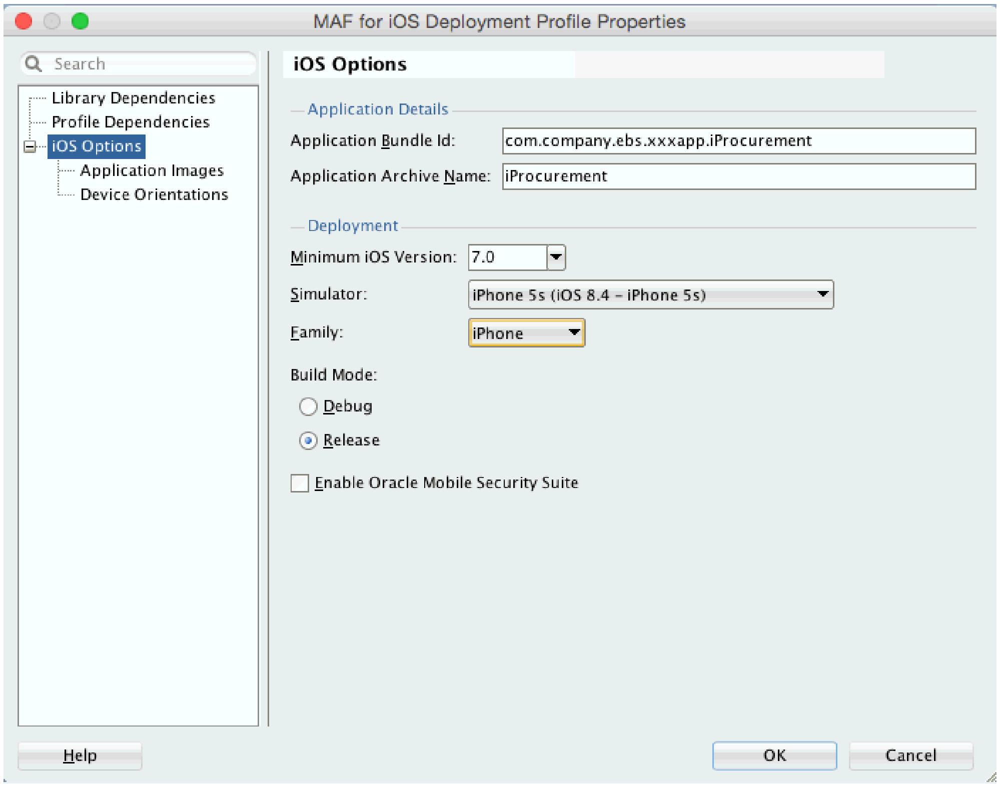
Click OK to create your new deployment profile and immediately open it to see its configuration.

Profile Type: MAF for iOS

Deployment Profile Name: XXX_iProcurement_iOS

Description: Creates a profile for deploying a Mobile Application Framework application to the iOS platform.

3. Enter the following information in the MAF for iOS Deployment Profile Properties page:



iOS Options

Application Details

Application Bundle Id: com.company.ebs.xxxapp.iProcurement

Application Archive Name: iProcurement

Deployment

Minimum iOS Version: 7.0

Simulator: iPhone 5s (iOS 8.4 - iPhone 5s)

Family: iPhone

Build Mode:

○ Debug

● Release

□ Enable Oracle Mobile Security Suite

- Application Bundle Id: Use this Application Bundle Id to package the application binary for iOS, such as `com.company.ebs.xxxapp.iProcurement`.

  Please note that the Id must be a unique Id for each app installed on an iOS mobile device and must follow the reverse-package style naming conventions:

  `com.<companyname>.<organizationname>.<appname>`

  Once you register the app on Oracle E-Business Suite using a given Application Bundle Id and the same Id is used in the **`maf-applicaiton.xml`** Id field, you do not have to change it at all during the development and deployment process. The Id information could remain the same. For information about the Id field in the **`maf-applicaiton.xml`** file, see Changing Application Bundle Id, page 3-30.

  When you register the app with Apple to obtain a provisioning profile, this is the Bundle Id used. The provisioning profile and certificate are issued by Apple specific to this Bundle Id. For more information, see the *App Distribution Guide*, available through the iOS Developer Library at http://developer.apple.com/library/ios/navigation/).

  Therefore, while it is recommended that use the same Id value entered in the **`maf-application.xml`** file in this Application Bundle Id field, the Application Bundle Id in the deployment profile could change depending on how it is set up with Apple for the provisioning profile and certificate.

- Application Archive Name: Enter the name of the .ipa file created by MAF. For example, iProcurement.
- Minimum iOS Version: This should be 7.0. Oracle E-Business Suite certifies all Oracle E-Business Suite mobile apps for iOS 7.0 and above.
- Simulator: Select from a list of iOS simulators to which you want to deploy the mobile app.
- Family: iPhone. Oracle E-Business Suite mobile apps are designed and tested for iPhones.

  Please note that mobile users can run the mobile apps on any devices that are capable of running iOS 7.0 or higher. However, the UI design is specific to iPhones only.
- Build Mode: Select the **Debug** radio button for development and testing. Select the **Release** radio button for production deployment.

Click **OK**.

4. Save your work.

Instructions to Create a New Deployment Profile for the Android Platform

Similar to the creation of a new iOS deployment profile, when customizing the app for corporate branding, a developer needs to create a new deployment profile for the Android platform first, and then replace the default Oracle image used for the app icons with custom images. All images should be in `.png` format.

Copying the Custom Icons

Before creating a new deployment profile, copy the custom icon files to the following location where the default icons are also placed:

```
<Application Root Folder>/resources/android
```

Creating a New Deployment Profile

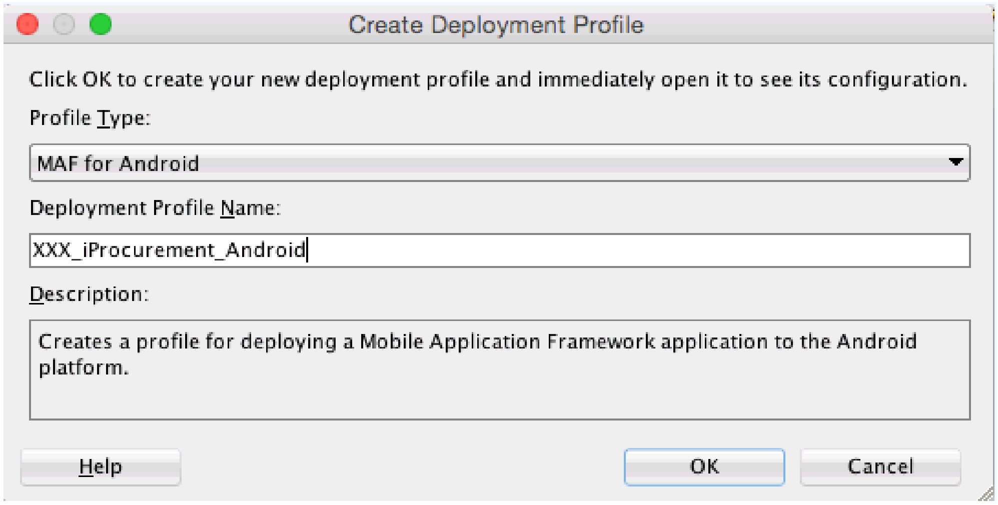
Use the following steps to create a new deployment profile:

1. In the Applications Navigator of Oracle JDeveloper, select "XXX_iProcurement" application and then right-click on it. Select **Deploy** and then **New Deployment Profile...** from the selection window.
2. In the Create Deployment Profile page, select **MAF for Android** as the Profile Type field.

   If "MAF for iOS" is selected as the deployment profile type, see Instructions to

Create a New Deployment Profile with Customized App Logos for the iOS Platform, page 4-10.

Enter a new name, such as "XXX_iProcurement_Android", as the Deployment Profile Name if required.



Create Deployment Profile

Click OK to create your new deployment profile and immediately open it to see its configuration.

Profile Type:

MAF for Android

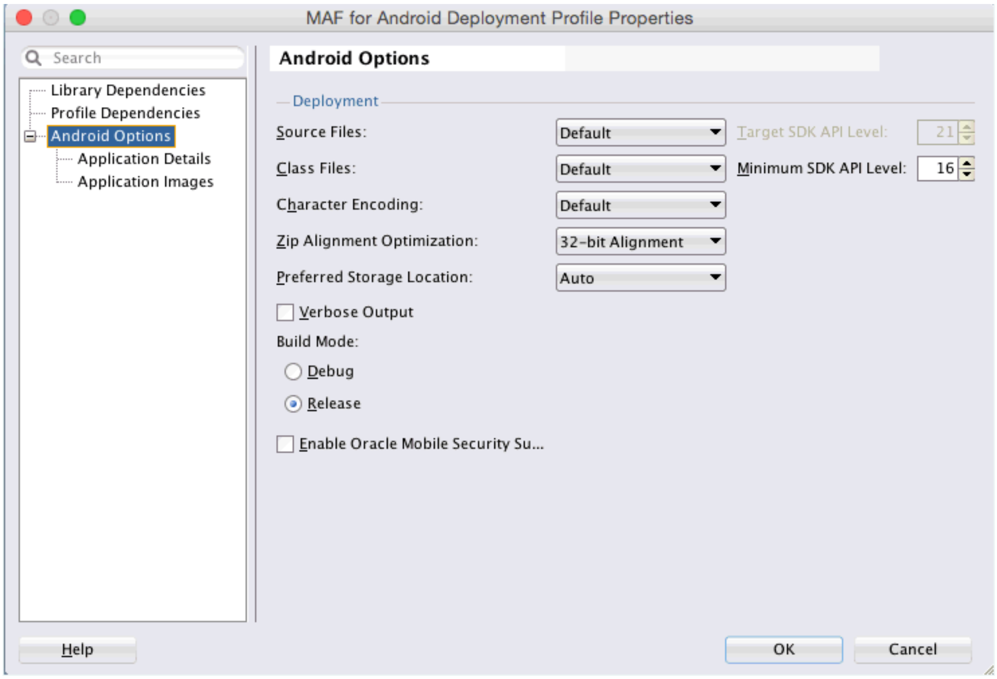
Deployment Profile Name:

XXX_iProcurement_Android

Description:

Creates a profile for deploying a Mobile Application Framework application to the Android platform.

3. Enter the following information in the MAF for Android Deployment Profile Properties page:



Android Options

Deployment

Source Files: Default

Class Files: Default

Character Encoding: Default

Zip Alignment Optimization: 32-bit Alignment

Preferred Storage Location: Auto

Target SDK API Level: 21

Minimum SDK API Level: 16

□ Verbose Output

Build Mode:

○ Debug

● Release

□ Enable Oracle Mobile Security Su...

- Target SDK API Level: 21. Oracle E-Business Suite mobile apps are compatible with Android 4.1 and higher, but the target SDK API level that Oracle E-Business Suite certifies for the Android platform is from Android 4.1 to 5.0. The value 21 here corresponds to the SDK API level for Android 5.0.

- Minimum SDK API Level: Select "16" from the drop-down list as the minimum SDK API level that the mobile app supports for the Android platform. This value 16 corresponds to the SDK API level for Android 4.1.

- Build Mode: Select the **Debug** radio button for development and testing. Select the **Release** radio button for production deployment.

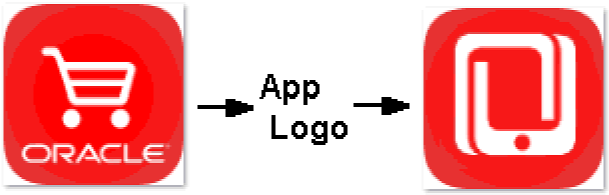
Click **OK**.

4. Save your work.

Changing App Logo and Splash Screen through a Deployment Profile

Once a new deployment profile is created, a developer can replace the default Oracle image used for the app icons with custom app logos or images.

For example, the app logo of Oracle Mobile iProcurement for Oracle E-Business Suite is modified from a "shopping cart" symbol to a "box" or "square" symbol.

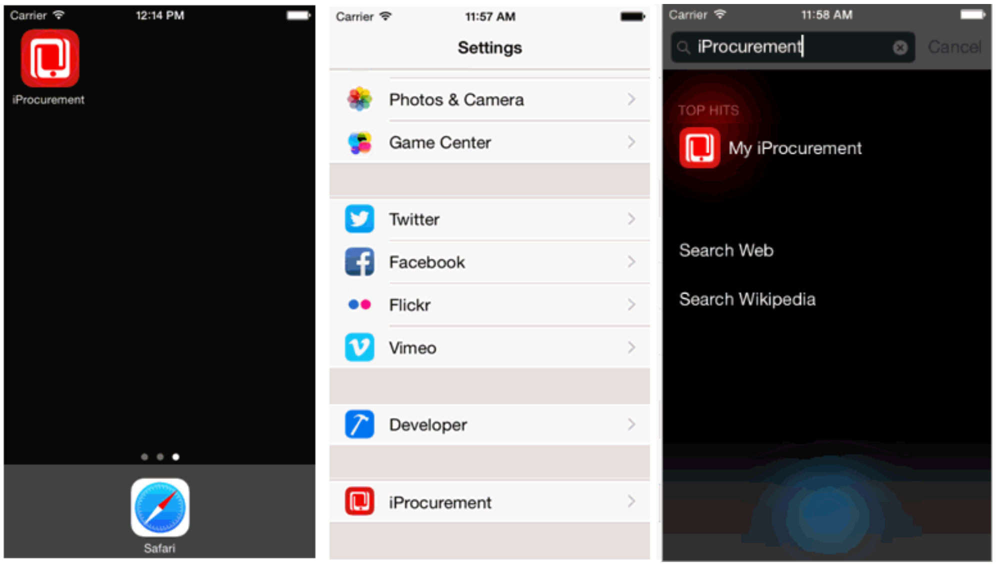


Customized App Logo for Corporate Branding

The app logo or icon is displayed in the About page. It can also be shown on an iOS device in the following places:

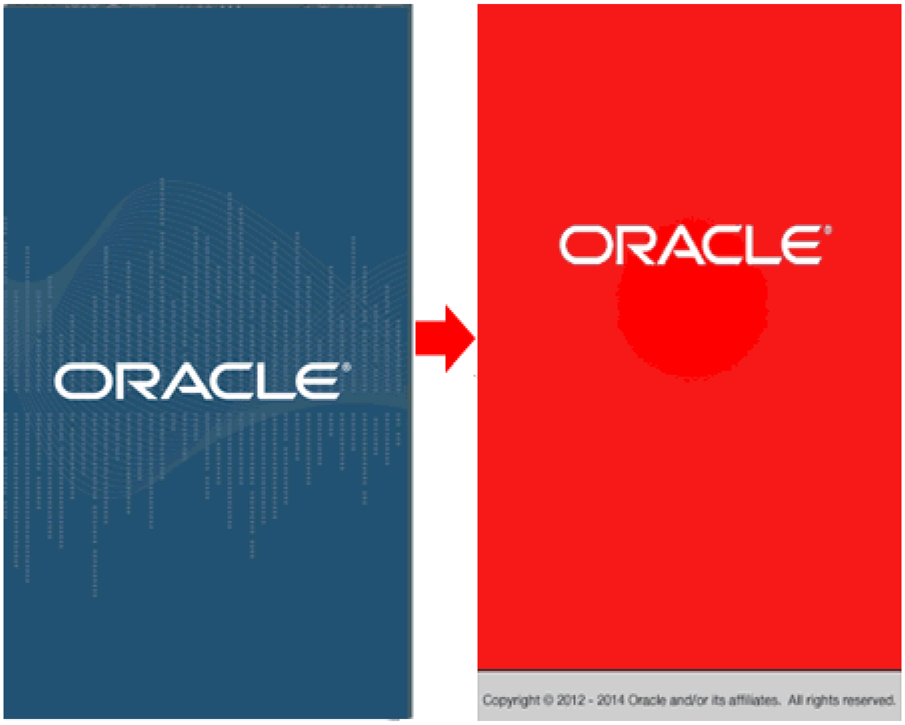
- A launcher icon on an iOS device's home screen (shown in the left of the screenshot)
- In Settings icon against the app name (shown in the middle of the screenshot)
- In Spotlight search when the app is searched for (shown in the right of the screenshot)

  In this example, the app logo in the launcher icon is changed, but the app name "iProcurement" remains the same.



Customized Splash Screen for Corporate Branding

Splash screen is usually the first screen mobile users will see when launching an app. After you change the image for the splash screen to match your corporate theme standards, the splash screen on an iOS device can be like:


ORACLE
ORACLE
Copyright © 2012 - 2014 Oracle and/or its affiliates. All rights reserved.

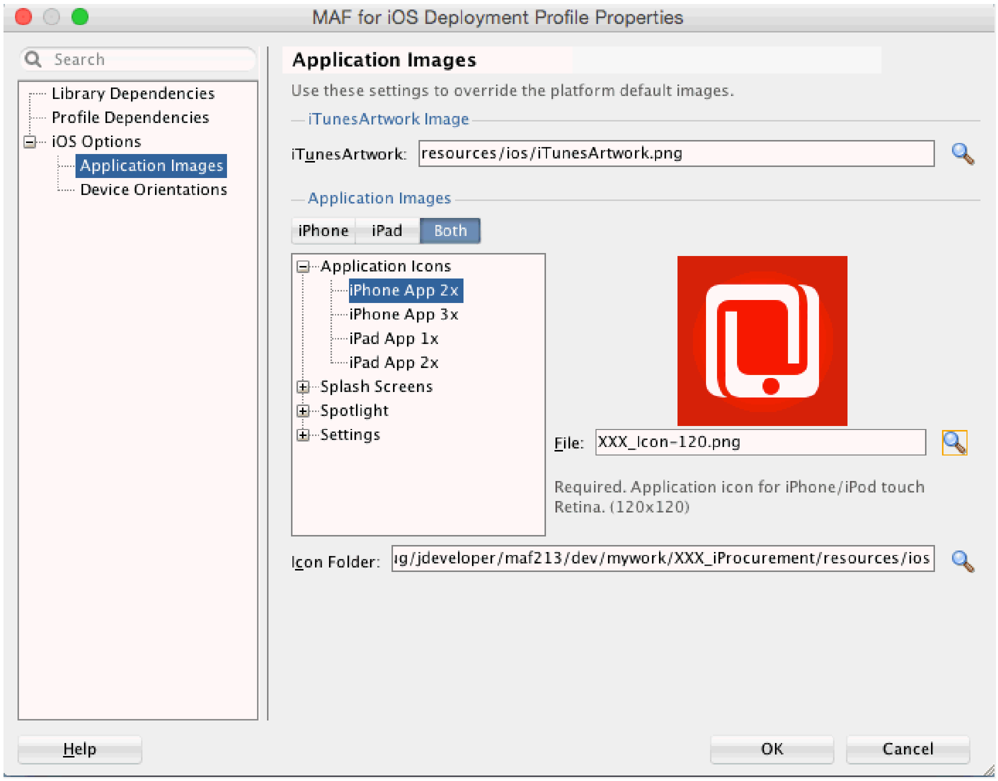
This section includes the following topics:

- Instructions to Change App Logos and Splash Screen for the iOS Platform, page 4-18
- Instructions to Change App Logos and Splash Screen for the Android Platform, page 4-19

Instructions to Change App Logo and Splash Screen for the iOS Platform

Use the following steps to change the mobile app images for corporate branding:

1. In the MAF for iOS Deployment Profile Properties page, select "Application Images" from the iOS Options tree node.



MAF for iOS Deployment Profile Properties

Application Images

Use these settings to override the platform default images.

iTunesArtwork: resources/ios/iTunesArtwork.png

File: XXX_Icon-120.png

Required. Application icon for iPhone/iPod touch Retina. (120x120)

Icon Folder: ig/jdeveloper/maf213/dev/mywork/XXX_iProcurement/resources/ios

2. In the Application Images region, select each device type tab if desired. Then choose an appropriate icon for the following categories, based on image sizing tables described in Required Image Sizing Information for the iOS Platform, page 4-4:

   Note: All images must be in `.png` format.

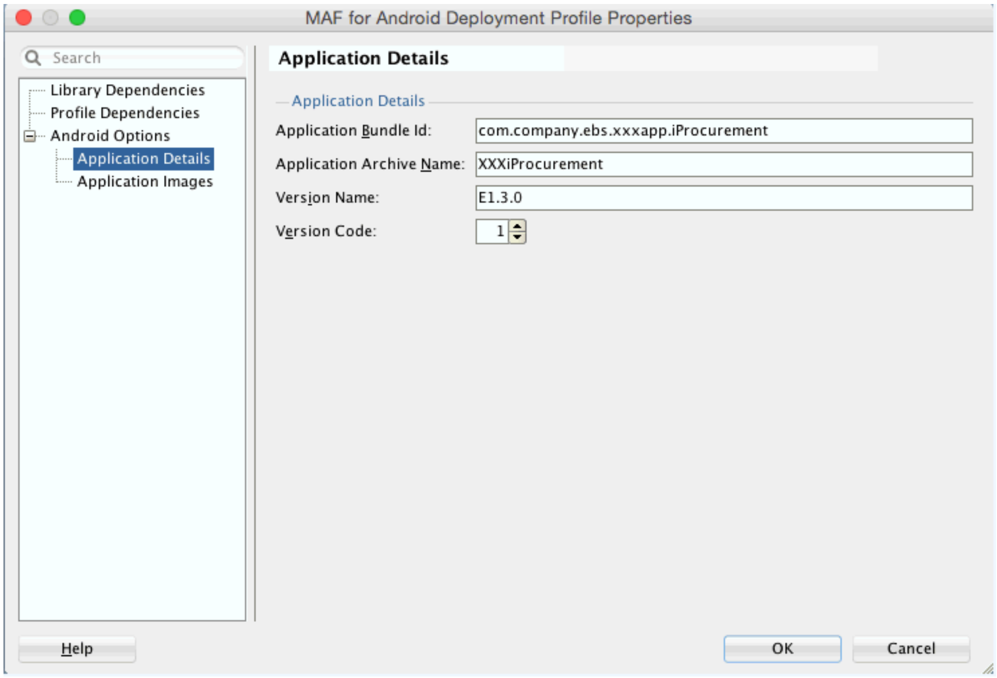
   - Application Icons
   - Splash Screens
   - Spotlight
   - Settings

   Click **OK** to save the changes.

Instructions to Change App Logo and Splash Screen for the Android Platform

Perform the following steps to change the app images for the Android platform:

1. In the MAF for Android Deployment Profile Properties page, select "Application Details" from the Android Options tree node and enter the following information:



Application Details

Application Details

Application Bundle Id: com.company.ebs.xxxapp.iProcurement

Application Archive Name: XXXiProcurement

Version Name: E1.3.0

Version Code: 1

- Application Bundle Id: Enter a unique Id for the mobile app on Android, such as `com.company.ebs.xxxapp.iProcurement`. Each app deployed to an Android device must have a unique Id, and this Id cannot start with a numeric value. Follow the same bundle Id naming conventions as described earlier in step 3, Instructions to Create a New Deployment Profile with Customized App Logos for the iOS Platform, page 4-10.

  Please note that use the same Id value specified in the configuration file **`maf-application.xml`** for the Application Bundle Id. For information on defining the Id in the configuration file, see: Changing Application Bundle Id, page 3-30.

- Application Archive Name: Enter the name of the .apk file created by MAF if needed. For example, XXXiProcurement.

- Version Name: The release version of the application code that displays for the mobile users. For example, E1.3.0 (with prefix letter "E" to indicate an enterprise-distributed app).

- Version Code: Select an appropriate value from the drop-down list to represent the version of the application code. This code is checked programmatically by other applications for upgrades or downgrades.

  Please note that the minimum and default value is 1. This value is incremented by 1 for each subsequent release.

Click **OK** to save your work.

2. In the Platform Display Types field, select each display type if appropriate and then choose an appropriate image for the Application Icon, Splash Screen (Portrait), and Splash Screen (Landscape) fields.

   For required image sizing information and file names, see Required Image Sizing Information for the Android Platform, page 4-7.

   > **Note:** All images must be in `.png` format.

   Click **OK** to save the changes.

Changing App Logo in the About Page and Android Page Header

App logo within an app is shown in the following places:

- About page of both iOS and Android devices (size 152x152)

  See: Displaying the App Logo in the About Page, page 4-21.

- Page header of Android device (size 80x80)

  See: Displaying the App Logo in the Page Header for Android, page 4-22.

Both images should be rounded corners and in `.png` format.

Displaying the App Logo in the About Page

Perform the following steps to display your custom app logo in the About page for the iOS and Android platforms:

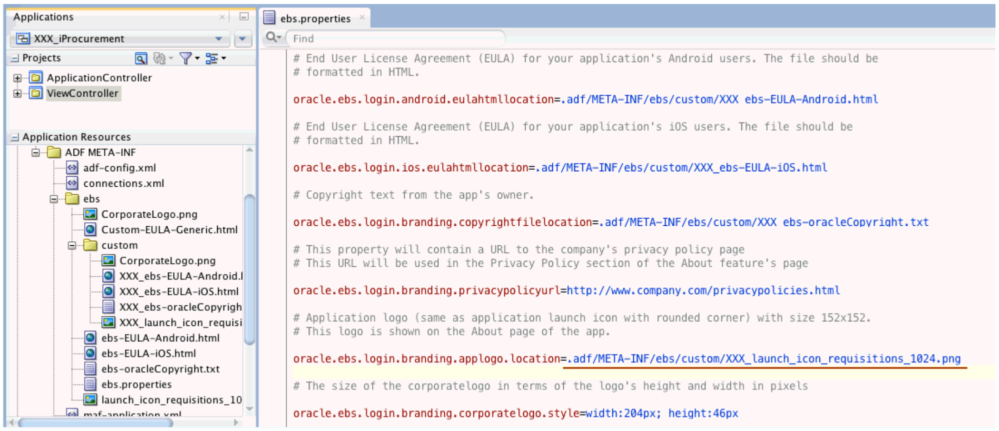
1. Copy the `.png` file whose image size is 152x152 to the `<ApplicationRootFolder>/.adf/META-INF/ebs/custom` directory.

2. In Oracle JDeveloper, expand the **Application Resources** panel, then the **Descriptors** folder, then the **ADF META-INF** folder, and then the **ebs** folder.

   Double click the **`ebs.properties`** file.

3. Update the `oracle.ebs.login.branding.applogo.location` property with the following information:

   ```
   oracle.ebs.login.branding.applogo.location
   =.adf/META-INF/ebs/custom/XXX_launch_icon_requisitions_1024.p
   ng
   ```



```
# End User License Agreement (EULA) for your application's Android users. The file should be
# formatted in HTML.

oracle.ebs.login.android.eulahtmllocation=.adf/META-INF/ebs/custom/XXX ebs-EULA-Android.html

# End User License Agreement (EULA) for your application's iOS users. The file should be
# formatted in HTML.

oracle.ebs.login.ios.eulahtmllocation=.adf/META-INF/ebs/custom/XXX_ebs-EULA-iOS.html

# Copyright text from the app's owner.

oracle.ebs.login.branding.copyrightfilelocation=.adf/META-INF/ebs/custom/XXX ebs-oracleCopyright.txt

# This property will contain a URL to the company's privacy policy page
# This URL will be used in the Privacy Policy section of the About feature's page

oracle.ebs.login.branding.privacypolicyurl=http://www.company.com/privacypolicies.html

# Application logo (same as application launch icon with rounded corner) with size 152x152.
# This logo is shown on the About page of the app.

oracle.ebs.login.branding.applogo.location=.adf/META-INF/ebs/custom/XXX_launch_icon_requisitions_1024.png

# The size of the corporatelogo in terms of the logo's height and width in pixels

oracle.ebs.login.branding.corporatelogo.style=width:204px; height:46px
```

Note that you can use any file name for the image file with size 152x152 as long as you refer to the correct name in this property.

Displaying the App Logo in the Page Header for Android

Perform the following steps to display your custom app logo in the page header for Android apps:

1. Name the `.png` file whose image size is 80x80 as `android_app_header_icon.png`.

   It is important to note that the image file name should be exactly as mentioned here to display the app logo in the page header.

2. Copy the `.png` file to the `<ApplicationRootFolder>/ViewController/public_html/resources/images` directory.

3. Repeat the same step 2 and step 3, as described in Displaying the App Logo in the About Page, page 4-21, to locate the **`ebs.properties`** file and update the `oracle.ebs.login.branding.applogo.location` property.

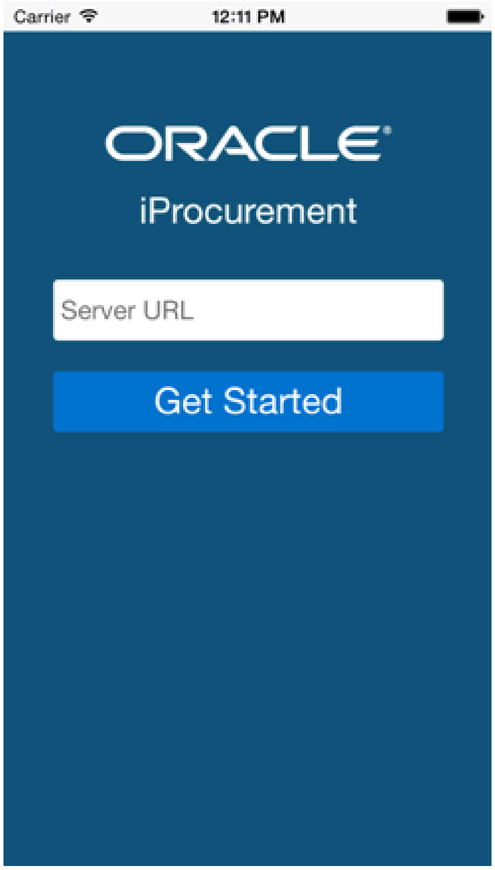
Customizing the Company Logo

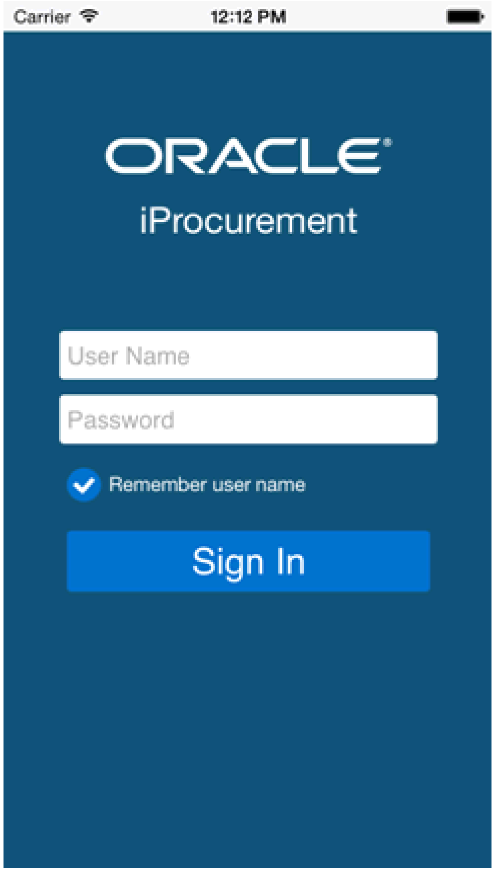
Mobile users can find a company logo in the following places within an app:

- Server URL screen (shown in the left of the screenshot)

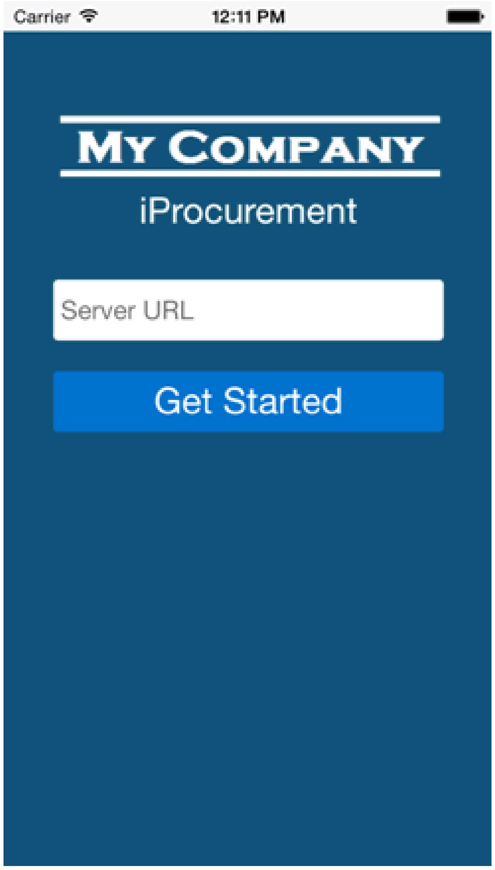
  This Server URL screen is displayed only during the initial launch of the app or when the app is reconfigured.

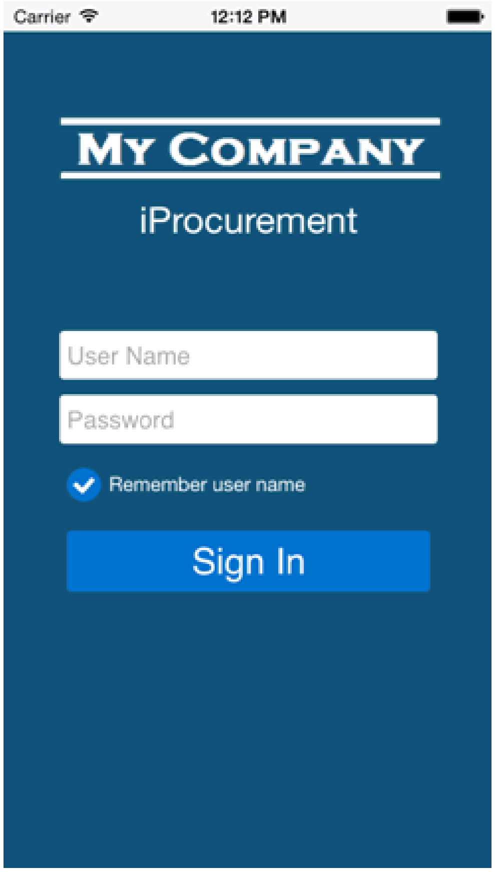
- Sign In screen (shown in the right of the screenshot)





When an enterprise user tries to connect to an Oracle E-Business Suite instance from the enterprise-distributed iProcurement app (Oracle Mobile iProcurement for Oracle E-Business Suite), the white Oracle logo is replaced with a new company logo in the Server URL screen (left) and the Sign In screen (right) as shown in this example.





Instructions to Customize the Company Logo:

Perform the following steps to replace Oracle logo with your company logo:

1. Create and name the image file name as `CorporateLogo.png` and copy it to the following locations in the Oracle JDeveloper application folder:

   > **Note:** The image file name should be `CorporateLogo.png`. For required sizing information, see Required Image Sizing Information for Corporate Branding, page 4-3.

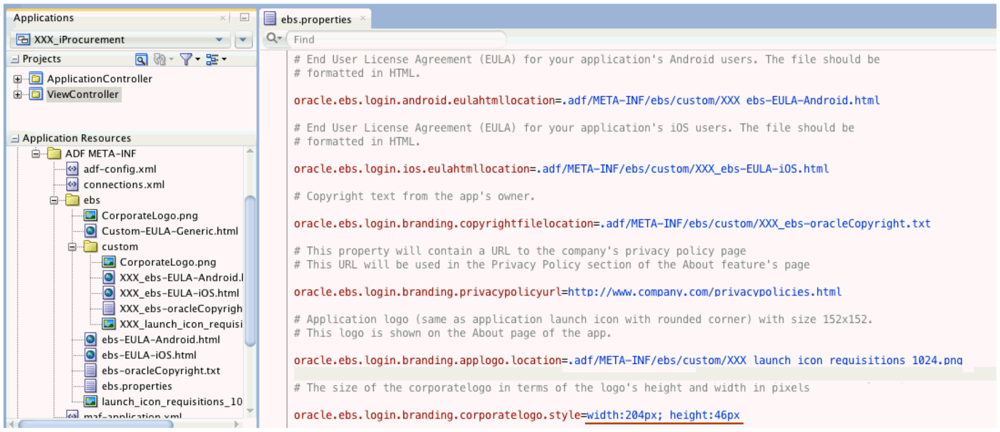
   - `<ApplicationRootFolder>/.adf/META-INF/ebs/custom`
   - `<ApplicationRootFolder>/ApplicationController/public_html/resources/images`

2. In Oracle JDeveloper, expand the **Application Resources** panel, then the **Descriptors** folder, then the **ADF META-INF** folder, and then the **ebs** folder.

   Double click the **`ebs.properties`** file.

3. Update the following information in the **`ebs.properties`** file to change the

company logo in the Server URL screen:



```
# End User License Agreement (EULA) for your application's Android users. The file should be
# formatted in HTML.

oracle.ebs.login.android.eulahtmllocation=.adf/META-INF/ebs/custom/XXX ebs-EULA-Android.html

# End User License Agreement (EULA) for your application's iOS users. The file should be
# formatted in HTML.

oracle.ebs.login.ios.eulahtmllocation=.adf/META-INF/ebs/custom/XXX_ebs-EULA-iOS.html

# Copyright text from the app's owner.

oracle.ebs.login.branding.copyrightfilelocation=.adf/META-INF/ebs/custom/XXX_ebs-oracleCopyright.txt

# This property will contain a URL to the company's privacy policy page
# This URL will be used in the Privacy Policy section of the About feature's page

oracle.ebs.login.branding.privacypolicyurl=http://www.company.com/privacypolicies.html

# Application logo (same as application launch icon with rounded corner) with size 152x152.
# This logo is shown on the About page of the app.

oracle.ebs.login.branding.applogo.location=.adf/META-INF/ebs/custom/XXX launch icon requisitions 1024.png

# The size of the corporatelogo in terms of the logo's height and width in pixels

oracle.ebs.login.branding.corporatelogo.style=width:204px; height:46px
```

`oracle.ebs.login.branding.corporatelogo.style``=width:204px; height:46px`

- This property lets you define an appropriate CSS style for your company logo.

- The width and height in pixels should be 50% of the actual size. For example, if your image is 100x100, the CSS style should be `width=50px;height=50px;`.

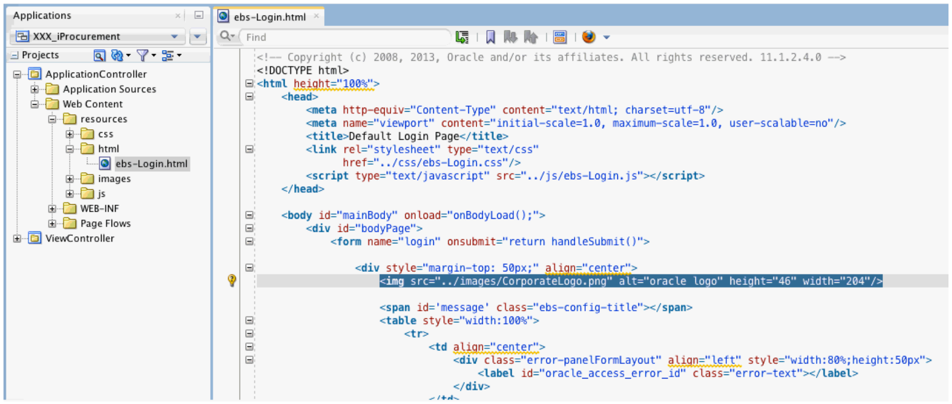
4. The image is automatically shown in the Sign In screen based on the name `CorporateLogo.png`. Use the following steps to customize the CSS style so that the size of the logo is displayed correctly:

   1. Expand the **ApplicationController** folder, then the **Web Content** folder, then the **resources** folder, and then the **html** folder.

   2. Double click the **`ebs-Login.html`** file and then select the Source tab

   3. Search and locate "`CorporateLogo.png`" in the following HTML tag:

      ```
      <img src="../images/CorporateLogo.png" alt="oracle logo"
      height="46" weight="204"/>
      ```



```
<!-- Copyright (c) 2008, 2013, Oracle and/or its affiliates. All rights reserved. 11.1.2.4.0 -->
<!DOCTYPE html>
<html height="100%">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
        <meta name="viewport" content="initial-scale=1.0, maximum-scale=1.0, user-scalable=no"/>
        <title>Default Login Page</title>
        <link rel="stylesheet" type="text/css"
              href="../css/ebs-Login.css"/>
        <script type="text/javascript" src="../js/ebs-Login.js"></script>
    </head>

    <body id="mainBody" onload="onBodyLoad();">
        <div id="bodyPage">
            <form name="login" onsubmit="return handleSubmit()">

                <div style="margin-top: 50px;" align="center">
                    <img src="../images/CorporateLogo.png" alt="oracle logo" height="46" width="204"/>

                    <span id='message' class="ebs-config-title"></span>
                    <table style="width:100%">
                        <tr>
                            <td align="center">
                                <div class="error-panelFormLayout" align="left" style="width:80%;height:50px">
                                    <label id="oracle_access_error_id" class="error-text"></label>
                                </div>
                            </td>
```

4. Update the height and width attributes with the same values used to update property `oracle.ebs.login.branding.corporatelogo.style` as described in step 3.

Changing the App Name (Optional)

A mobile user can find the app name in many places when using or launching a mobile app. In addition to replacing Oracle logos or images with your company logos for corporate branding, you can customize app name if necessary.

Specifically, app name can be displayed in the following screens:

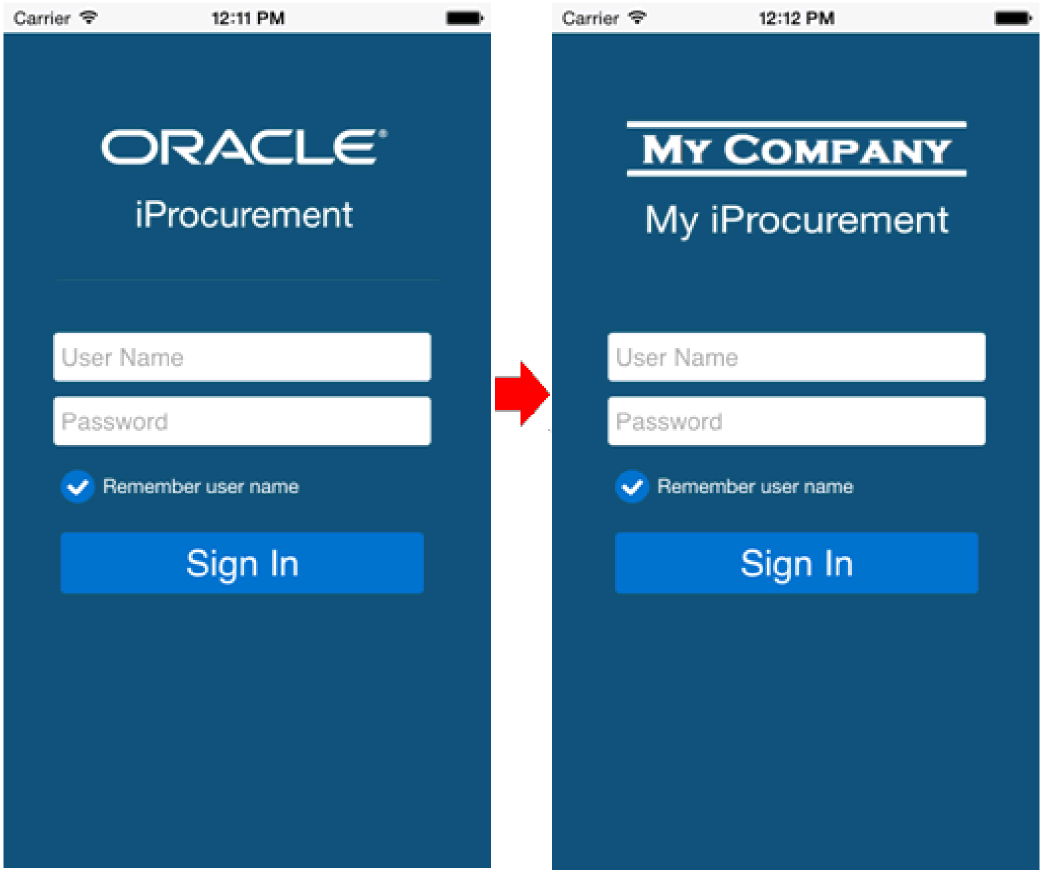
- Server URL screen
- Sign In screen
- Springboard
- About page

The app name shown in the Sign In screen comes from a specific file which is different from the rest of the screens in the list mentioned earlier.

- For instructions on changing the app name in the Sign In screen, see Instructions to Customize the App Name in the Sign In Screen, page 4-26.
- For instructions on changing the app name in the Server URL screen, Springboard, and the About page, see Instructions to Customize the App Name in the Sign In Other Screens, page 4-29.

Instructions to Customize the App Name in the Sign In Screen

The following screenshots represent the app name change shown in the Sign In screen (from "iProcurement" to "My iProcurement"), along with the customized company logo for corporate branding.



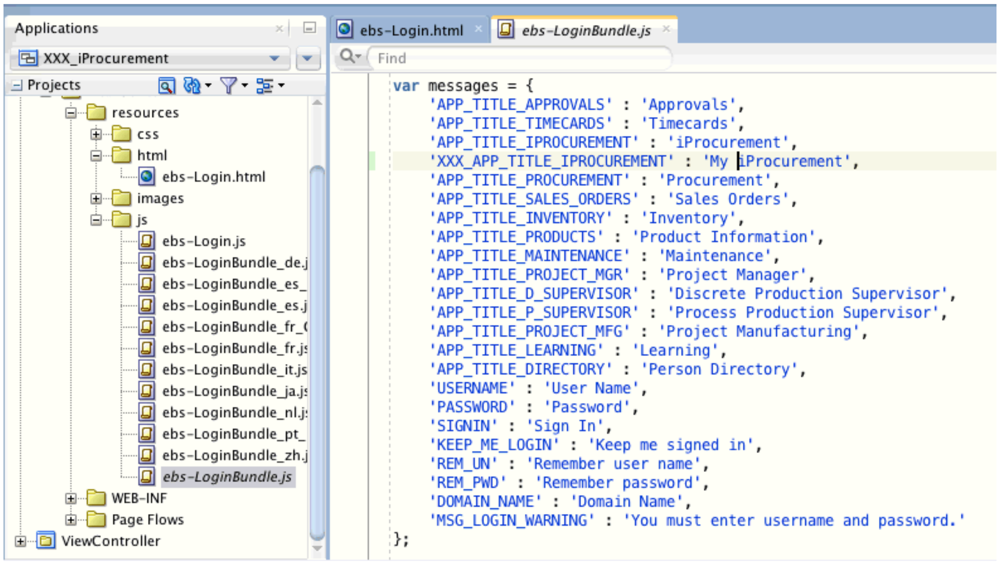
Perform the following steps to modify the app name in the Sign In screen:

1. In Oracle JDeveloper, select your mobile application project.

2. Expand the **ApplicationController** folder, then the **Web Content** folder, then the **resources** folder, and then the **js** folder.

3. Double click the **`ebs-LoginBundle.js`** file.

4. Add a string in the **`ebs-LoginBundle.js`** file for your custom app name. For example, `'XXX_APP_TITLE_IPROCUREMENT' : 'My iProcurement',`.



```
var messages = {
    'APP_TITLE_APPROVALS' : 'Approvals',
    'APP_TITLE_TIMECARDS' : 'Timecards',
    'APP_TITLE_IPROCUREMENT' : 'iProcurement',
    'XXX_APP_TITLE_IPROCUREMENT' : 'My iProcurement',
    'APP_TITLE_PROCUREMENT' : 'Procurement',
    'APP_TITLE_SALES_ORDERS' : 'Sales Orders',
    'APP_TITLE_INVENTORY' : 'Inventory',
    'APP_TITLE_PRODUCTS' : 'Product Information',
    'APP_TITLE_MAINTENANCE' : 'Maintenance',
    'APP_TITLE_PROJECT_MGR' : 'Project Manager',
    'APP_TITLE_D_SUPERVISOR' : 'Discrete Production Supervisor',
    'APP_TITLE_P_SUPERVISOR' : 'Process Production Supervisor',
    'APP_TITLE_PROJECT_MFG' : 'Project Manufacturing',
    'APP_TITLE_LEARNING' : 'Learning',
    'APP_TITLE_DIRECTORY' : 'Person Directory',
    'USERNAME' : 'User Name',
    'PASSWORD' : 'Password',
    'SIGNIN' : 'Sign In',
    'KEEP_ME_LOGIN' : 'Keep me signed in',
    'REM_UN' : 'Remember user name',
    'REM_PWD' : 'Remember password',
    'DOMAIN_NAME' : 'Domain Name',
    'MSG_LOGIN_WARNING' : 'You must enter username and password.'
};
```

- Please note that **`ebs-LoginBundle.js`** is a JSON file. Except for the last key-value pair, all pairs should end with a comma.

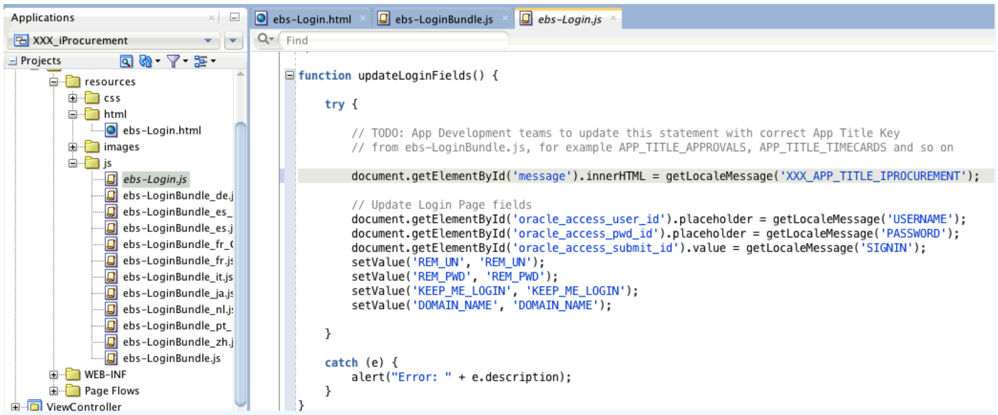
- This **`ebs-LoginBundle.js`** file can be translated into different languages if required. Place the translated files under the following folder for the mobile app:

  ```
  <ApplicationRootFolder>/ApplicationController/public_html/
  resources/js/
  ```

Save your work.

5. Double click the **`ebs-Login.js`** file.

6. Replace the existing app name with your custom app name in the **`ebs-Login.js`** file.



```
function updateLoginFields() {

    try {

        // TODO: App Development teams to update this statement with correct App Title Key
        // from ebs-LoginBundle.js, for example APP_TITLE_APPROVALS, APP_TITLE_TIMECARDS and so on

        document.getElementById('message').innerHTML = getLocaleMessage('XXX_APP_TITLE_IPROCUREMENT');

        // Update Login Page fields
        document.getElementById('oracle_access_user_id').placeholder = getLocaleMessage('USERNAME');
        document.getElementById('oracle_access_pwd_id').placeholder = getLocaleMessage('PASSWORD');
        document.getElementById('oracle_access_submit_id').value = getLocaleMessage('SIGNIN');
        setValue('REM_UN', 'REM_UN');
        setValue('REM_PWD', 'REM_PWD');
        setValue('KEEP_ME_LOGIN', 'KEEP_ME_LOGIN');
        setValue('DOMAIN_NAME', 'DOMAIN_NAME');

    }

    catch (e) {
        alert("Error: " + e.description);
    }
}
```

Search for a string starting with `APP_TITLE` and replace the full string with your new app name key. For example, replace `APP_TITLE_IPROCUREMENT` with `XXX_APP_TITLE_IPROCUREMENT`.

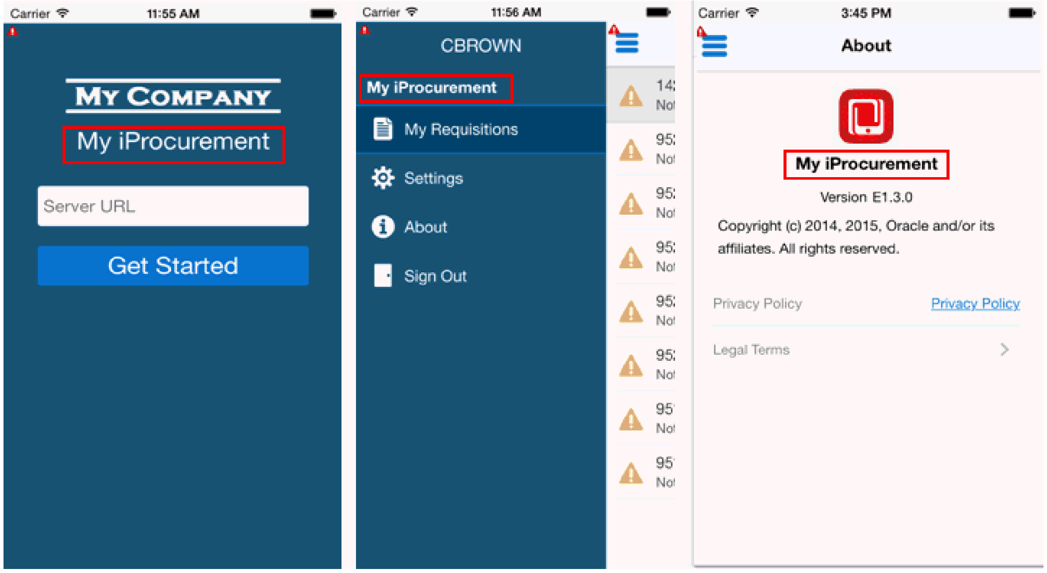
7. Save your work.

Instructions to Customize the App Name in Other Screens

In addition to the Sign In screen, customized app name can be displayed in the Server URL screen, Springboard, and the About page.

For example, the app name is changed from "iProcurement" to "My iProcurement" in the Server URL screen (shown in the left) and the About page (shown in the right), along with the customized company logo for corporate branding.

The changed app name "My iProcurement" is displayed at the top of the Springboard (shown in the middle) for corporate branding.



Instructions to Customize the App Name in Other Screens

Perform the following steps to change the app name in the Server URL screen, Springboard, and the About page:

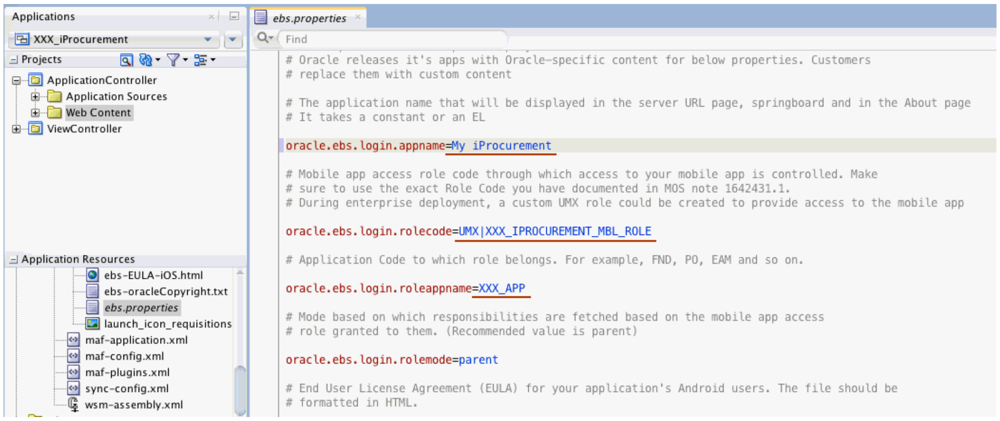
1. Open Oracle JDeveloper.

2. In the Application Navigator, expand the **Application Resources** panel, then the **Descriptors** folder, then the **ADF META-INF** folder, and then the **ebs** folder.

   Double click the **`ebs.properties`** file.

3. Update the following property in the **`ebs.properties`** file:

   `oracle.ebs.login.appname=My iProcurement`

```
# Oracle releases it's apps with Oracle-specific content for below properties. Customers
# replace them with custom content

# The application name that will be displayed in the server URL page, springboard and in the About page
# It takes a constant or an EL

oracle.ebs.login.appname=My iProcurement

# Mobile app access role code through which access to your mobile app is controlled. Make
# sure to use the exact Role Code you have documented in MOS note 1642431.1.
# During enterprise deployment, a custom UMX role could be created to provide access to the mobile app

oracle.ebs.login.rolecode=UMX|XXX_IPROCUREMENT_MBL_ROLE

# Application Code to which role belongs. For example, FND, PO, EAM and so on.

oracle.ebs.login.roleappname=XXX_APP

# Mode based on which responsibilities are fetched based on the mobile app access
# role granted to them. (Recommended value is parent)

oracle.ebs.login.rolemode=parent

# End User License Agreement (EULA) for your application's Android users. The file should be
# formatted in HTML.
```

   Ensure that the customized name (`My iProcurement`) matches exactly what is used in the Sign In screen described earlier.

4. Save your work.

Customizing the Legal Related Information (Optional)

In addition to the company logo, app logo, splash screen, and app name changes, you can optionally customize legal related information specifically for your company. This includes:

- End User License Agreement (EULA) or Legal Terms

  This information is displayed during the initial launch of an app. For information on customizing the EULA, see Customizing End User License Agreement or Legal Terms (Optional), page 4-31.

- Copyright in the About Page

  Oracle allows you to modify the copyright information for corporate branding by optionally adding your own copyright information along with Oracle's copyright.

  See: Customizing Copyright in the About Page (Optional), page 4-33.

Customizing End User License Agreement or Legal Terms (Optional)

When an app is launched for the first time, the End User License Agreement (EULA) or Legal Terms screen appears. The app user needs to accept the license agreement in order to use the app.

Mobile users can also find the same content through the About page by tapping the **Legal Terms** link. This content is stored in the following directory:

`<ApplicationRootFolder>/.adf/META-INF/ebs`

To display customized End User License Agreement (EULA) or Legal Terms, perform the following steps:

1. Copy a generic file `Custom-EULA-Generic.html` that can be customized to the following folder:

   `<ApplicationRootFolder>/.adf/META-INF/ebs/custom`

2. Modify the generic `Custom-EULA-Generic.html` file to include the EULA content specific to your company.

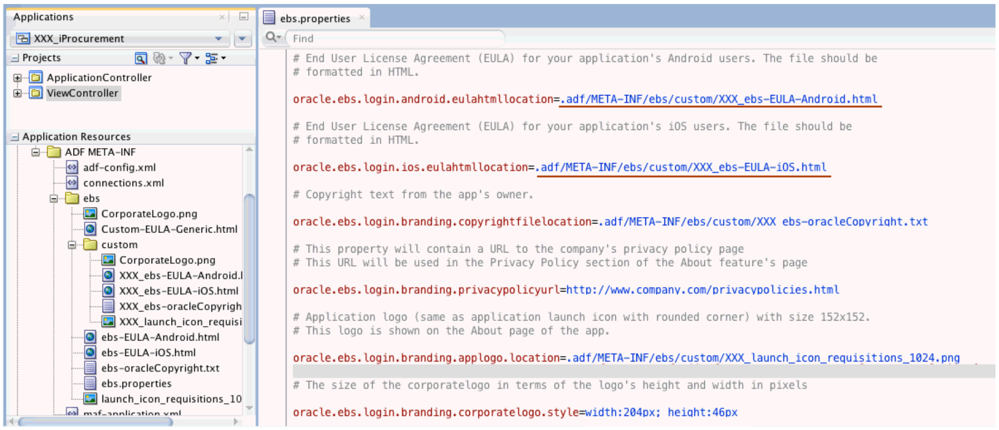
3. Rename the customized files, such as `XXX_ebs-EULA-Android.html` for Android and `XXX_ebs-EULA-iOS.html` for iOS.

   If the EULA content is the same for both iOS and Android, you could have the content in one file and update both properties with the same file.

4. After creating the customized EULA files, update the following properties in the **`ebs.properties`** file:

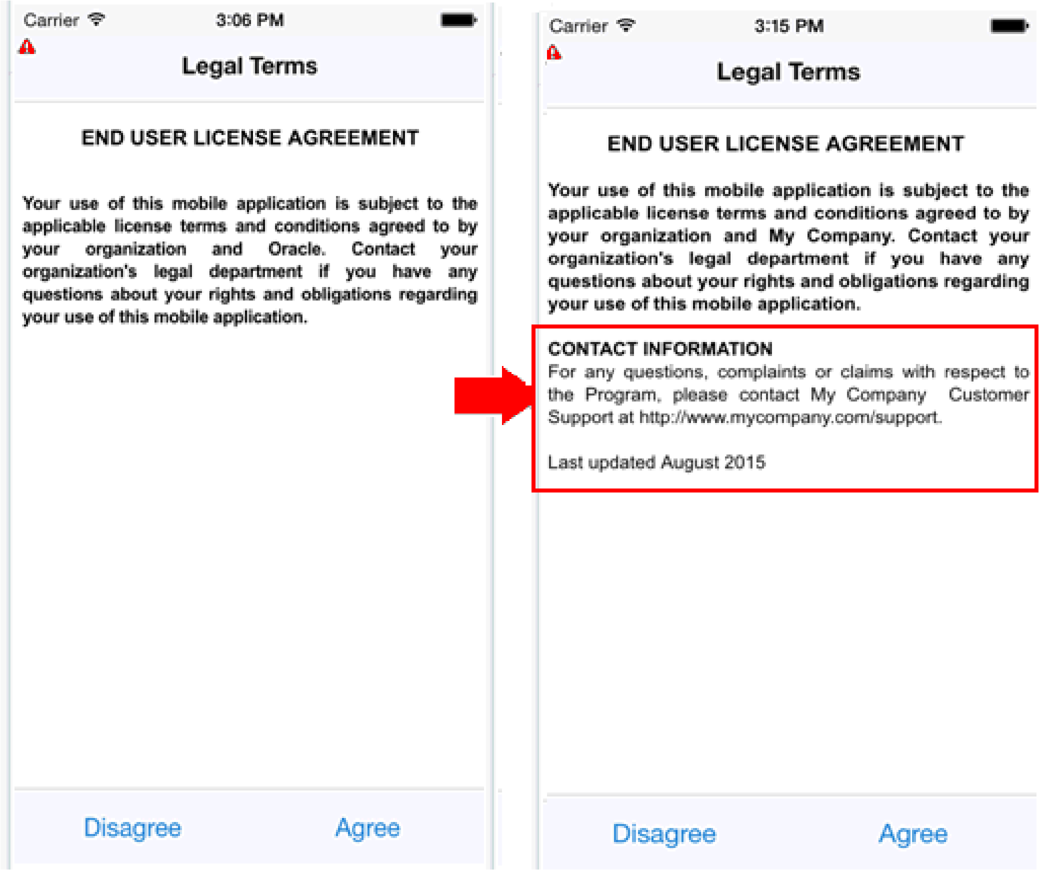
- **`oracle.ebs.login.android.eulahtmllocation`** `=.adf/META-INF/ebs/custom/XXX_ebs-EULA-Android.html`

- **`oracle.ebs.login.ios.eulahtmllocation`** `=.adf/META-INF/ebs/custom/XXX_ebs-EULA-iOS.html`



```
# End User License Agreement (EULA) for your application's Android users. The file should be
# formatted in HTML.

oracle.ebs.login.android.eulahtmllocation=.adf/META-INF/ebs/custom/XXX_ebs-EULA-Android.html

# End User License Agreement (EULA) for your application's iOS users. The file should be
# formatted in HTML.

oracle.ebs.login.ios.eulahtmllocation=.adf/META-INF/ebs/custom/XXX_ebs-EULA-iOS.html

# Copyright text from the app's owner.

oracle.ebs.login.branding.copyrightfilelocation=.adf/META-INF/ebs/custom/XXX ebs-oracleCopyright.txt

# This property will contain a URL to the company's privacy policy page
# This URL will be used in the Privacy Policy section of the About feature's page

oracle.ebs.login.branding.privacypolicyurl=http://www.company.com/privacypolicies.html

# Application logo (same as application launch icon with rounded corner) with size 152x152.
# This logo is shown on the About page of the app.

oracle.ebs.login.branding.applogo.location=.adf/META-INF/ebs/custom/XXX_launch_icon_requisitions_1024.png

# The size of the corporatelogo in terms of the logo's height and width in pixels

oracle.ebs.login.branding.corporatelogo.style=width:204px; height:46px
```

After the modification, when an app is launched for the first time, the customized End User License Agreement content appears on an iOS device as shown this example.



END USER LICENSE AGREEMENT

Your use of this mobile application is subject to the applicable license terms and conditions agreed to by your organization and Oracle. Contact your organization's legal department if you have any questions about your rights and obligations regarding your use of this mobile application.

END USER LICENSE AGREEMENT

Your use of this mobile application is subject to the applicable license terms and conditions agreed to by your organization and My Company. Contact your organization's legal department if you have any questions about your rights and obligations regarding your use of this mobile application.

CONTACT INFORMATION

For any questions, complaints or claims with respect to the Program, please contact My Company Customer Support at http://www.mycompany.com/support.

Last updated August 2015

Customizing Copyright in the About Page (Optional)

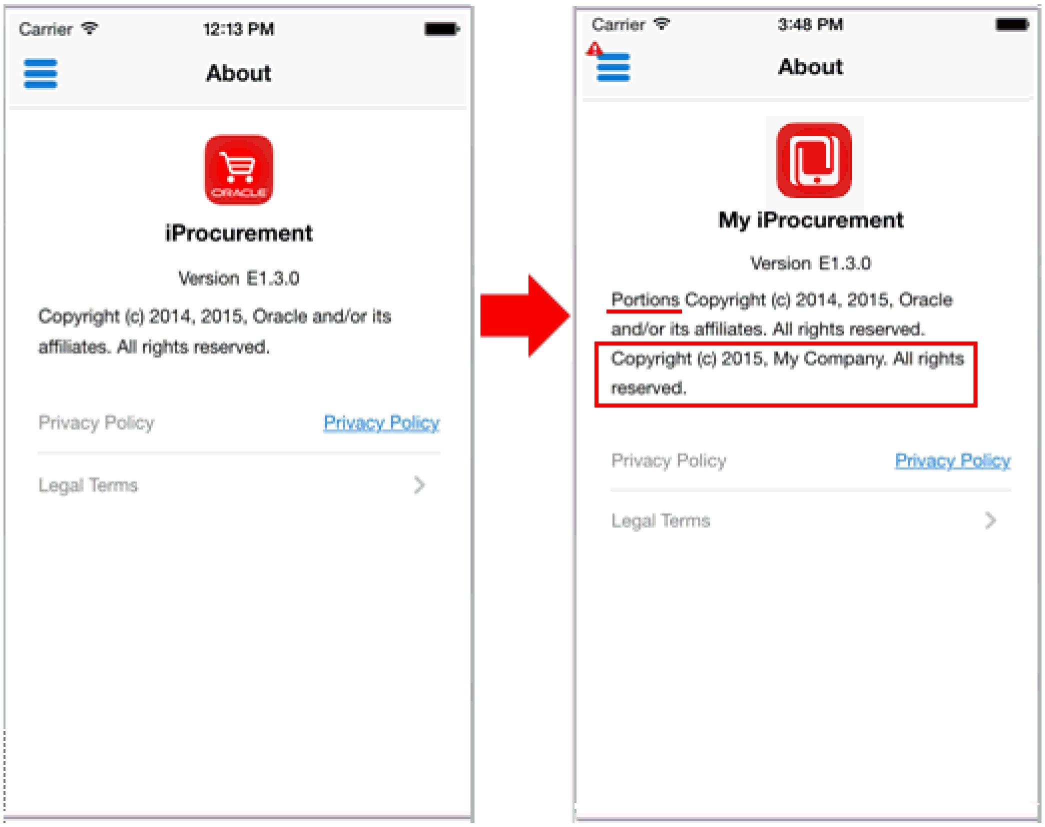
Copyright information is displayed in the About page which is accessible from the Springboard of an Oracle E-Business Suite mobile app by tapping the **About** link.

Information displayed in the About page, such as copyright, privacy policy URL, is specific to Oracle E-Business Suite mobile app. In addition to the required privacy policy change described earlier for enterprise distribution, you can modify the copyright information for corporate branding by optionally adding your company's own copyright information along with Oracle's copyright.

Example of Customized Copyright for Corporate Branding

The following example shows the revised copyright in the About page for the iProcurement app (Oracle Mobile iProcurement for Oracle E-Business Suite) on an iOS device.

In this example, app logo, company logo, and copyright text have been modified specifically for corporate branding, along with the privacy policy URL change.



Copyright (c) 2014, 2015, Oracle and/or its affiliates. All rights reserved.

Portions Copyright (c) 2014, 2015, Oracle and/or its affiliates. All rights reserved.

Copyright (c) 2015, My Company. All rights reserved.

- For information on updating the app name, see Changing the App Name, page 4-26 .
- For information on changing privacy policy URL, see Enterprise Distribution with Minimum Changes to an App, page 3-30.

Instructions to Customize the Copyright Information in the About page

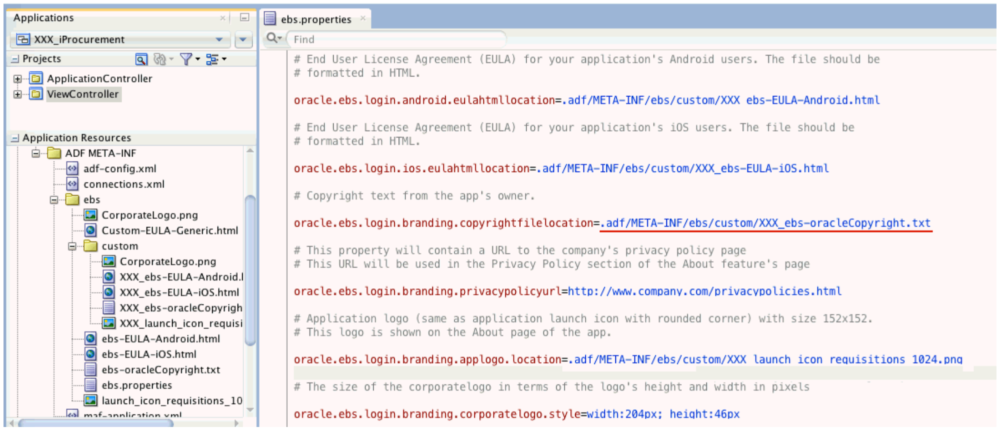
Perform the following steps to customize the copyright information:

1. Open Oracle JDeveloper.
2. Create a file `<ApplicationRootFolder>/.adf/META-INF/ebs/custom/XXX_ebs-oracleCopyright.txt` and include your own copyright information if needed.
3. In the Application Navigator, expand the **Application Resources** panel, then the **Descriptors** folder, then the **ADF META-INF** folder, and then the **ebs** folder.

   Double click the **`ebs.properties`** file.
4. Update the copyright information in the **`ebs.properties`** file:

   ```
   oracle.ebs.login.branding.copyrightfilelocation
   =.adf/META-INF/ebs/custom/XXX_ebs-oracleCopyright.txt
   ```

Note: Leave the Oracle copyright information unchanged in the About page and it should not be removed.



```
# End User License Agreement (EULA) for your application's Android users. The file should be
# formatted in HTML.

oracle.ebs.login.android.eulahtmllocation=.adf/META-INF/ebs/custom/XXX ebs-EULA-Android.html

# End User License Agreement (EULA) for your application's iOS users. The file should be
# formatted in HTML.

oracle.ebs.login.ios.eulahtmllocation=.adf/META-INF/ebs/custom/XXX_ebs-EULA-iOS.html

# Copyright text from the app's owner.

oracle.ebs.login.branding.copyrightfilelocation=.adf/META-INF/ebs/custom/XXX_ebs-oracleCopyright.txt

# This property will contain a URL to the company's privacy policy page
# This URL will be used in the Privacy Policy section of the About feature's page

oracle.ebs.login.branding.privacypolicyurl=http://www.company.com/privacypolicies.html

# Application logo (same as application launch icon with rounded corner) with size 152x152.
# This logo is shown on the About page of the app.

oracle.ebs.login.branding.applogo.location=.adf/META-INF/ebs/custom/XXX launch icon requisitions 1024.png

# The size of the corporatelogo in terms of the logo's height and width in pixels

oracle.ebs.login.branding.corporatelogo.style=width:204px; height:46px
```

5. Save your work.

5

Mobile Application Management (MAM) Support with Oracle Mobile Security Suite

Overview

To secure and manage enterprise-distributed Oracle E-Business Suite mobile apps and relevant data on mobile devices, you can optionally containerize these apps with Oracle Mobile Security Suite (OMSS) as a mobile application management (MAM) solution.

Prerequisites

Before you begin, ensure that you have the following software components in place:

- Oracle Mobile Security Suite 11*g* Release 2 (11.1.2.3.2)

  Oracle Mobile Security Suite (11.1.2.3.2) is available for download from My Oracle Support through patch 21870612.

  For installation instructions, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

- Oracle Access Manager 11.1.2.2+ (Required Only if Enabling Single Sign-On for Containerized Oracle E-Business Suite Mobile Apps, page 5-5)

  To configure single sign-on for enterprise-distributed Oracle E-Business Suite mobile apps containerized in Oracle Mobile Security Suite, you must integrate Oracle E-Business Suite with Oracle Access Manager. Refer to My Oracle Support Knowledge Document 1388152.1, *Overview of Single Sign-On Integration Options for Oracle E-Business Suite*.

- Oracle Identity Management 11.1.1.7.0+ (Required Only if Enabling Single Sign-On for Containerized Oracle E-Business Suite Mobile Apps, page 5-5)

  For configuration and installation instructions, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Oracle Mobile Security Suite is a mobile security system which provides capabilities of securing and managing enterprise app access right from the mobile devices. It provides a Secure Enterprise Workspace that serves as a container on a mobile device to separate the enterprise apps from other apps. This way, the enterprise-distributed apps can be securely "wrapped" and protected in the container from unauthorized access.

> **Note:** Oracle Mobile Security Suite supports containerizing mobile apps developed using Oracle Mobile Application Framework (Oracle MAF). To enable the containerization feature with OMSS, you must prepare Oracle E-Business Suite mobile apps as enterprise apps first. You can then containerize and distribute the mobile apps through Oracle Mobile Security Suite rather than through a public app store.

With this containerization feature, OMSS eliminates the need for device-level VPN and supports single sign-on for these containerized enterprise apps deployed to the secure workspace. Please note that this containerization feature is transparent to the containerized enterprise apps. OMSS containerization works seamlessly with Oracle E-Business Suite mobile apps for OMSS integration. For more information about Oracle Mobile Security Suite, refer to *Oracle Fusion Middleware Administering Oracle Mobile Security Suite* and other Oracle Mobile Security Suite documentation.

Furthermore, OMSS provides an alternative option to access the Oracle E-Business Suite mobile apps over the Internet by using Mobile Security Access Server (MSAS), an essential component in OMSS. MSAS runs in the demilitarized zone (DMZ) and acts as a proxy to secure traffic between mobile apps and internal resources.

For more information about Mobile Security Access Server, see *Oracle Fusion Middleware Installing Oracle Mobile Security Access Server* and *Oracle Fusion Middleware Administering Oracle Mobile Security Access Server*.

For more information about DMZ, see Demilitarized Zone (DMZ), page 6-1.

To better understand how to containerize enterprise-distributed apps and enable the single sign-on feature, this chapter includes the following sections:

- Containerizing Enterprise-Distributed Oracle E-Business Suite Mobile Apps Using OMSS, page 5-2

- Enabling Single Sign-On for Containerized Oracle E-Business Suite Mobile Apps, page 5-5

For troubleshooting information about Oracle Mobile Security Suite, see the Troubleshooting Oracle Mobile Security Suite chapter, *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*.

Containerizing Enterprise-Distributed Oracle E-Business Suite Mobile Apps Using OMSS

Before you begin the containerization, you must prepare Oracle E-Business Suite mobile apps as enterprise apps first. You can then containerize and distribute the enterprise apps through Oracle Mobile Security Suite.

For information on preparing the mobile apps for enterprise distribution, see Working with Mobile Application Archives for Enterprise Distribution, page 3-1.

Setting Up Oracle Mobile Security Suite

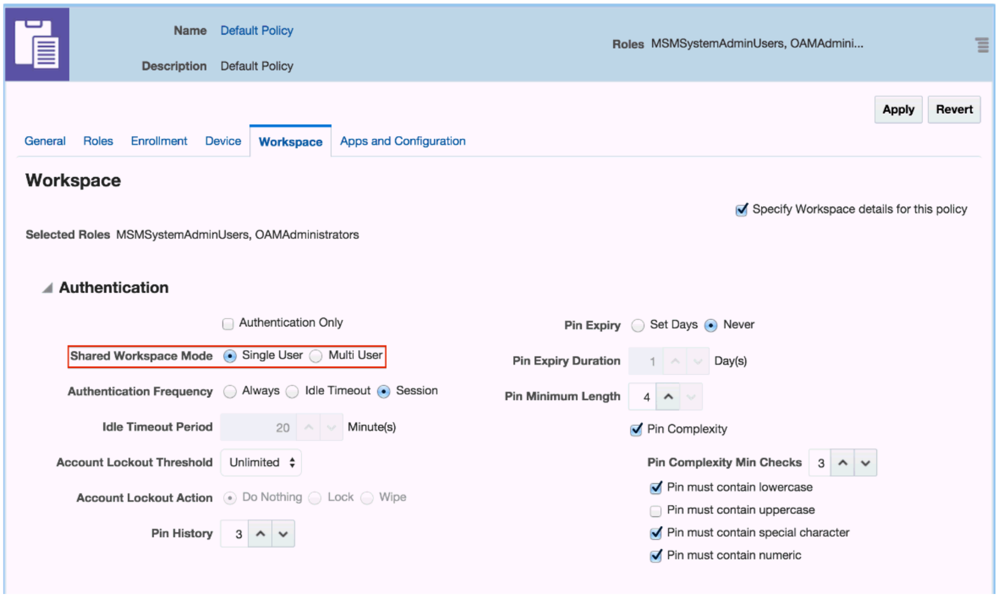
While setting up your Oracle Mobile Security Suite environment, ensure to perform the following steps:

1. In the Oracle Mobile Security Suite console page, navigate to the **Mobile Security** tab.

   Under **Mobile Security Manager**, click **View** and choose **Mobile Security Policies** from the View drop-down menu.

2. Click **Default Policy**, and then select the **Workspace** tab.

   In the Shared Workspace Mode field, select the **Single User** radio button.



Name Default Policy

Description Default Policy

Roles MSMSystemAdminUsers, OAMAdmini...

Workspace

☑ Specify Workspace details for this policy

Selected Roles MSMSystemAdminUsers, OAMAdministrators

Authentication

□ Authentication Only

Shared Workspace Mode ● Single User ○ Multi User

Authentication Frequency ○ Always ○ Idle Timeout ● Session

Idle Timeout Period 20 Minute(s)

Account Lockout Threshold Unlimited

Account Lockout Action ● Do Nothing ○ Lock ○ Wipe

Pin History 3

Pin Expiry ○ Set Days ● Never

Pin Expiry Duration 1 Day(s)

Pin Minimum Length 4

☑ Pin Complexity

Pin Complexity Min Checks 3

☑ Pin must contain lowercase

□ Pin must contain uppercase

☑ Pin must contain special character

☑ Pin must contain numeric

3. If you have more than one policy defined in the "Mobile Security Policies", ensure that all the policies have the Shared Workspace Mode field set to "Single User".

For more administrative information, see *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*.

Instructions to Containerize an Enterprise App:

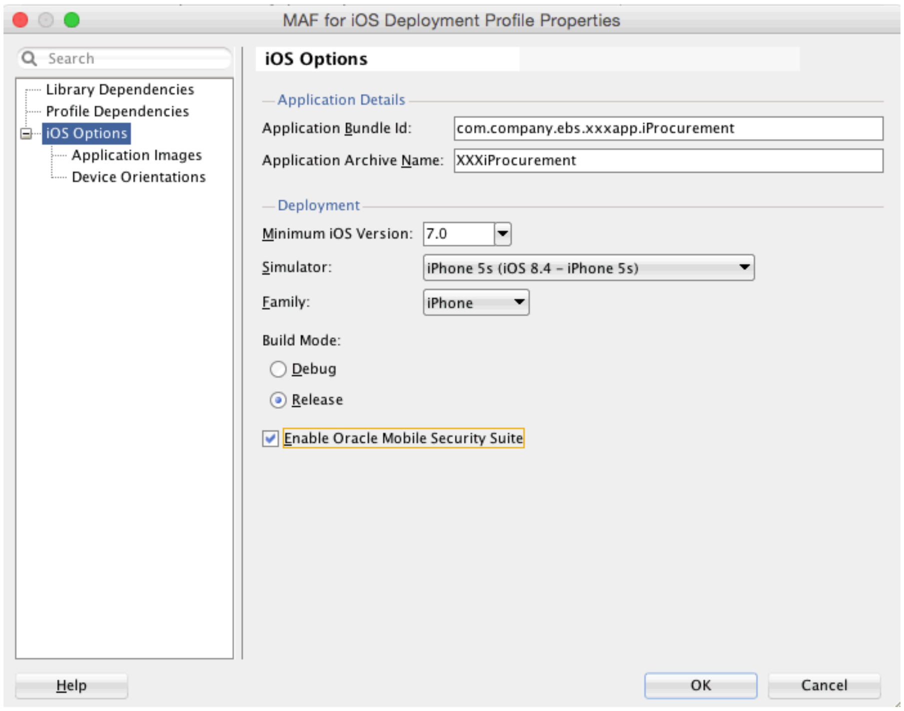
Use the following steps to containerize an enterprise app:

1. Prepare the app for enterprise distribution. See Working with Mobile Application Archives for Enterprise Distribution, page 3-1.

2. Deploy the app through either of the following options:

   - Deploy the app with deployment option "Enable Oracle Mobile Security Suite".

     - In the MAF for iOS Deployment Profile Properties page, select the **Enable Oracle Mobile Security Suite** check box. This action enables the deployment option to automatically invoke the OMSS containerization tool C14N that creates a containerized version of the app.



Application Bundle Id: com.company.ebs.xxxapp.iProcurement

Application Archive Name: XXXiProcurement

Minimum iOS Version: 7.0

Simulator: iPhone 5s (iOS 8.4 - iPhone 5s)

Family: iPhone

Build Mode:

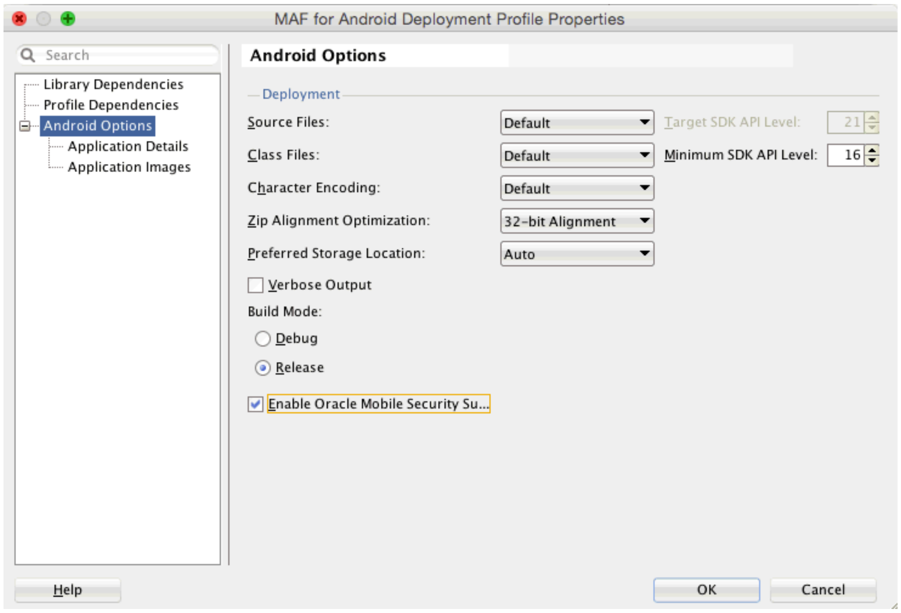
○ Debug

● Release

☑ Enable Oracle Mobile Security Suite

     - In the MAF for Android Deployment Profile Properties page, select the **Release** radio button for the Build Mode.

       Select the **Enable Oracle Mobile Security Suite** check box. This action enables the deployment option to automatically invoke the OMSS containerization tool C14N that creates a containerized version of the app.



Android Options

Deployment

Source Files: Default

Class Files: Default

Character Encoding: Default

Zip Alignment Optimization: 32-bit Alignment

Preferred Storage Location: Auto

Target SDK API Level: 21

Minimum SDK API Level: 16

□ Verbose Output

Build Mode:

○ Debug

● Release

☑ Enable Oracle Mobile Security Su...

For instructions on containerizing the app using OMSS, see Deploying with Oracle Mobile Security Suite, Deploying MAF Applications chapter, *Developing Mobile Applications with Oracle Mobile Application Framework*.

- Deploy the app by manually creating the containerized version of the app using the OMSS containerization tool `c14n`.

  For information on using the containerization tool, see Running the Containerization Tool, Using the Oracle Mobile Security Suite Application Containerization Tool chapter, *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*.

3. Use the Oracle Mobile Security Suite console to upload the containerized app to the mobile app Catalog.

   For instructions on uploading the containerized app, see Adding Native Apps, Managing Mobile Apps chapter, *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*.

For troubleshooting information on using containerized apps, see Troubleshooting Tips for Containerized, Enterprise-Distributed Apps, page 7-17.

Enabling Single Sign-On for Containerized Oracle E-Business Suite Mobile Apps

If your Oracle E-Business Suite is integrated with Oracle Access Manager (OAM) and Oracle Mobile Security Suite, you can enable the single sign-on (SSO) feature for your containerized, enterprise-distributed Oracle E-Business Suite mobile apps.

Once this feature is enabled, instead of logging in to each containerized app individually from your mobile device, you can log in once to access multiple enterprise-distributed Oracle E-Business Suite mobile apps.

> **Note:** Oracle Mobile Security Suite supports single sign-on with Oracle Access Manager when the OAM login page is exposed using the embedded credential collector (ECC) mode. If the OAM login page is exposed using the distributed credential collector (DCC) mode, single sign-on with OAM is not supported. Therefore, you must protect Oracle E-Business Suite using OAM with the embedded credential collector mode to configure OMSS and enable single sign-on for Oracle E-Business Suite mobile apps.

Instructions to Enable the Single Sign-On Feature

When configuring enterprise-distributed Oracle E-Business Suite mobile apps in the Configure Mobile Applications page, you must select "Web SSO" as the authentication type in the Configuration Categories region and then configure the associated parameters to enable the single sign-on feature.

For information on configuring mobile apps, see Enabling a Mobile App Individually and Specifying the Configuration through the UI, page 2-11.

To enable this feature in SSL-based Oracle E-Business Suite environments, you need to perform additional setup tasks, as described in Additional Setup Tasks to Enable Web SSO Authentication Security, page 2-25.

6

Advanced Configurations

Overview

This chapter describes requirements for using advanced configurations with Oracle E-Business Suite mobile apps. It includes the following sections:

1. Demilitarized Zone (DMZ), page 6-1

2. Secure Communication with HTTPS, page 6-3

3. Single Sign-On (SSO), page 6-6

Demilitarized Zone (DMZ)

If your mobile users need to access the Oracle E-Business Suite mobile apps over the Internet, your Oracle E-Business Suite environment must be set up in a DMZ configuration.

> **Note:** Alternative to a DMZ configuration in Oracle E-Business Suite, you can optionally choose to use Oracle Mobile Security Suite (OMSS). In OMSS, only Mobile Security Access Server (MSAS) is deployed in a DMZ configuration and acts as a proxy to internal resources, including Oracle E-Business Suite internal deployments. For more information about Oracle Mobile Security Suite, refer to Mobile Application Management (MAM) Support with Oracle Mobile Security Suite, page 5-1.

Please note that DMZ configuration is supported only for mobile apps with a client version of 1.1.0 or higher, with Oracle E-Business Suite Mobile Foundation Release 2.1 or later on the Oracle E-Business Suite server.

- For DMZ configuration instructions on Oracle E-Business Suite Release 12.1, see My

Oracle Support Knowledge Document 380490.1.

- For DMZ configuration instructions on Oracle E-Business Suite Release 12.2, see My Oracle Support Knowledge Document 1375670.1.

> **Note:** For any responsibility to which you have assigned the mobile app access role, as described in Setting Up Mobile App Access to Responsibilities, page 2-35, to allow mobile users to access the responsibility from an external node in a DMZ configuration, set the "Responsibility Trust Level" profile value to External for that responsibility at the responsibility level.
>
> Please note that any responsibility with this profile value set to External will also be exposed on all other nodes in the DMZ. Any standard web tier set up in the DMZ for limited access will now have this responsibility visible.
>
> For more information on setting the trust level, refer to the following knowledge documents:
>
> - For Oracle E-Business Suite Release 12.1, see My Oracle Support Knowledge Document 380490.1, Section 5.3 Update List of Responsibilities.
>
> - For Oracle E-Business Suite Release 12.2, see My Oracle Support Knowledge Document 1375670.1, Section 4.4 Update List of Responsibilities.

Additionally, when setting up the configuration file for your mobile app, ensure that the service endpoint (or server host URL in Oracle E-Business Suite Mobile Foundation releases earlier than Release 2.1) is set to your external web entry point.

For information on configuring your mobile app, see Enabling a Mobile App Individually and Specifying the Configuration through the UI, page 2-11.

> **Note:** If you use the Configure Mobile Applications page to set up the configuration parameters, note that the value for the service endpoint parameter defaults to the current value of the APPS_FRAMEWORK_AGENT profile option. However, if you are accessing this page from your intranet, then the current value of the APPS_FRAMEWORK_AGENT profile option will be your internal web entry point. In this case, to allow access from mobile apps to Oracle E-Business Suite over the Internet, you must manually specify an override value for the server host URL parameter to set it to the external web entry point.

Secure Communication with HTTPS

Built on Oracle Mobile Application Framework (Oracle MAF), Oracle E-Business Suite mobile apps support the HTTPS protocol for certificates from commercial Certificate Authority (CA) vendors. Such public certificates are included within Application Resource Security cacerts file. Oracle MAF recognize only commercial CA-issued SSL certificates. For more information on mobile security, refer to the Securing Mobile Applications, *Oracle Fusion Middleware Developing Mobile Applications with Oracle Mobile Application Framework*.

Oracle E-Business Suite mobile apps version 1.2.x, with Oracle E-Business Suite Mobile Foundation Release 3.0, are based on Oracle MAF 2.1.0. Oracle E-Business Suite mobile apps with Oracle E-Business Suite Mobile Foundation Release 4.0 are based on Oracle MAF 2.1.3. For the list of certificates supported by MAF 2.1.x, see Migrating to New cacerts File for SSL in MAF 2.1.0 (or Migrating to New cacerts File for SSL in MAF 2.1.3), *Oracle Mobile Application Framework Installing Oracle Mobile Application Framework*.

> **Note:** If your mobile apps are deployed on Android 5 devices, you must apply appropriate Oracle Fusion Middleware January 2015 Oracle Critical Patch Updates to bring the required TLS (Transport Layer Security) version and negotiation support for SSL-based connection to Oracle E-Business Suite.
>
> - For Oracle E-Business Suite 12.1.3, apply appropriate Oracle Fusion Middleware 10.1.3.5 patches.
> - For Oracle E-Business Suite 12.2, apply appropriate Oracle Fusion Middleware 11.1.1.7 patches.
>
> See the Patch Set Update and Critical Patch Update January 2015 Availability Document, My Oracle Support Knowledge Document 1942215.1.

Additionally, to support "Web SSO" authentication security in Oracle E-Business Suite Mobile Foundation Release 4.0, you must perform additional setup tasks to enable this feature on SSL-based Oracle E-Business Suite environments. See: Additional Setup Tasks to Enable Web SSO Authentication Security, page 2-25.

If you plan to distribute mobile apps through your enterprise's own site rather than through a public app store, and your Oracle E-Business Suite environment is SSL enabled, you may import additional root-CA certificates into to your MAF application's truststore. For more information on setting up environment for enterprise distribution, see Importing Additional Root-CA Certificates (Optional), page 3-30.

Validating if the SSL Certificate is Valid or Trusted

Use the following steps to validate if your mobile app can perform a successful SSL handshake with the Oracle E-Business Suite SSL endpoint:

1. Validate that the JDK 8 client can connect to the Oracle E-Business Suite SSL endpoint.

    1. Install JDK 8 on a computer.

    2. Create a file named Url.java with the following content:

       ```
       /* * @(#)Url.java 1.3 01/05/10
       */
       import java.net.*;
       import java.io.*;

       /* This example illustrates using a URL to access resources
       * on any site, including a secure site. */

       public class Url {
            public static void main(String[] args) throws Exception {
                 String url =   "https://apps.example.com/robots.txt" ;
                 if( args.length >= 1 ) // get URL from command line
                    url = args[0] ;

            System.out.println( "###### Hitting URL " + url  );
            URL site = new URL( url );
            BufferedReader in = new BufferedReader(
                                     new InputStreamReader(
                                     site.openStream()));

            String inputLine;
            while ((inputLine =   in.readLine()) != null)
              System.out.println(inputLine);
           in.close();
           }
         }
       ```

    3. Compile Url.java using the following command, assuming that you have Java 8 JDK installed in the `~/jdk1.8/directory`:

       ```
       $ ~/jdk1.8/bin/javac Url.java
       ```

    4. Run Url.class using the following commands, assuming that you have Java 8 JDK installed in the `~/jdk1.8/directory`:

       ```
       $ ~/jdk1.8/jre/bin/java -Dhttps.protocols=TLSv1 Url
       https://ebs.example.com:4443/robots.txt
       ```

       Replace the sample input URL in this example with the specific URL for your Oracle E-Business Suite SSL endpoint.

       If HTML content is returned as the result after you execute these commands, then the SSL handshake is successful. If the following exceptions appear instead, then the SSL certificate on the server is not recognized by the JDK 8 client. You need to configure the Oracle E-Business Suite SSL endpoint with a server certificate issued by a commercial CA as listed in Migrating to New cacerts File for SSL in MAF 2.1.x, *Oracle Mobile Application Framework Installing Oracle Mobile Application Framework*.

```
Exception in thread "main" javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building
failed:
sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target.
```

Please note that these exceptions could also happen for a trusted certificate if the certificate chain is incomplete.

2. Validate that the Oracle E-Business Suite SSL endpoint presents the complete certificate chain.

   Please note that even if the Oracle E-Business Suite SSL endpoint is configured with a certificate from a commercial CA, the SSL handshake could still fail. Use the following steps to verify if the server presents the full certificate chain where the CA's certificate is present:

   1. Connect to the SSL endpoint using openssl with the `-showcerts` option:

      ```
      openssl s_client -connect ebs.example.com:4443 -showcerts
      ```

      Alternatively, use the following commands for more condensed results:

      ```
      openssl s_client -connect ebs.example.com:4443 -showcerts
      2>/dev/null | sed '/BEGIN CERT/,/END CERT/d' | sed -n
      '/^Certificate chain/,/^---/ p'
      ```

      These commands should display the complete certificate chain and the actual certificate content. For example,

      - The certificate chain is displayed as 0 -> 1.

      - The condensed version of the actual certificate chain content can be:

        ```
        Certificate chain
        0 s:/C=US/ST=California/L=Redwood City/O=Oracle
        Corporation/OU=FOR TESTING PURPOSES ONLY/CN=ebs.example.com
           i:/C=US/O=Oracle Corporation/OU=VeriSign Trust
        Network/OU=Class 3 MPKI Secure Server CA/CN=Oracle SSL CA

        1 s:/C=US/O=Oracle Corporation/OU=VeriSign Trust
        Network/OU=Class 3 MPKI Secure Server CA/CN=Oracle SSL CA
           i:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c)
        1999 VeriSign, Inc. - For authorized use only/CN=VeriSign
        Class 3 Public Primary Certification Authority - G3
        ```

        In this example certificate chain:

        - 0 is the server certificate, issued to `CN=ebs.example.com` by the intermediate CA, `CN=Oracle SSL CA`.

        - 1 is the intermediate CA certificate, issued to `CN=Oracle SSL CA` by the root CA certificate, `CN=VeriSign Class 3 Public Primary Certification Authority - G3`.

- The intermediate CA certificate is signed by a VeriSign root CA certificate that is in the client's truststore.

2. Ensure that the displayed certificate chain refers to a root CA whose certificate exists in the mobile client's truststore. In addition, ensure that the last certificate states that this root CA is its issuer.

   For a list of root CAs trusted by the mobile client, see Migrating to New cacerts File for SSL in MAF 2.1.0 (or Migrating to New cacerts File for SSL in MAF 2.1.3 for the apps with Oracle E-Business Suite Mobile Foundation Release 4.0), *Oracle Mobile Application Framework Installing Oracle Mobile Application Framework*.

3. Ensure that you not only configure the server certificate, but also provide the certificates of any intermediate CAs.

Single Sign-On (SSO)

Oracle provides single sign-on across Oracle E-Business Suite mobile apps through the use of Oracle Mobile Security Suite in Oracle E-Business Suite Mobile Foundation Release 4.0. Oracle Mobile Security Suite provides single sign-on to a mobile container, and thus all mobile apps in that container.

For information about containerizing Oracle E-Business Suite mobile apps, see Mobile Application Management (MAM) Support with Oracle Mobile Security Suite, page 5-1.

If you are not using Oracle Mobile Security Suite, you will need to be re-authenticated by providing your login credentials as you navigate from one Oracle E-Business Suite mobile app to another on the same mobile device. Re-authentication is required for Oracle E-Business Suite mobile apps even if you have integrated Oracle E-Business Suite with Oracle Access Manager (OAM) for single sign-on.

If your Oracle E-Business Suite is integrated with Oracle Access Manager as described in My Oracle Support Knowledge Document 1388152.1, *Overview of Single Sign-On Integration Options for Oracle E-Business Suite*, then you can choose either one of the following authentication types to configure your mobile app:

- HTTP Basic

  - Externally managed users require the APPS_SSO_LDAP_SYNC profile value set to 'Y' (enabled).

  - Users connecting to an Oracle E-Business Suite environment must have their passwords accessible from Oracle E-Business Suite. For instances integrated with single sign-on, if those users' passwords are not stored locally, Oracle E-Business Suite delegates authentication to Oracle Directory Services, a LDAP directory.

  - If passwords are stored in a third-party LDAP server, you must configure the external authentication plugin for the third-party LDAP with Oracle Directory Services. This is required in order to authenticate the users' credentials. This type of authentication is currently supported only with Oracle Directory Services 11g. For more information, refer to the Oracle Fusion Middleware Identity Management documentation.

  - If user passwords are not accessible, neither in Oracle E-Business Suite, nor Oracle Directory Services, nor the third-party LDAP server configured with Oracle Directory Services 11*g* external authentication plugin, such users cannot be authorized. Therefore, the login fails with a 401 Not Authorized error.

- Web SSO (Oracle E-Business Suite Mobile Foundation Release 4.0 only)

  - Oracle E-Business Suite mobile apps delegate user authentication to Oracle Access Manager.

  - For both browser-based applications and mobile apps, Oracle E-Business Suite certifies the form-based challenge method only.

  - In addition to the form-based challenge method, Oracle Access Manager supports several alternative authentication methods, including Oracle Identity Federation or integration with other third-party access management systems. You may leverage Oracle Access Manager to further integrate with any of the alternative authentication mechanisms supported by Oracle Access Manager. Integration with Oracle E-Business Suite is expected to work, regardless of how Oracle Access Manager authenticates the user, provided that Oracle Access Manager protects the resources, enforces authentication, and returns the configured response headers. Oracle E-Business Suite does not certify these alternative authentication methods. You may be asked to revert Oracle Access Manager to the certified form-based authentication before further investigation on any issues in Oracle E-Business Suite can take place. If you encounter issues during the configuration of Oracle Access Manager with alternative authentication mechanisms, you may contact Oracle Support for diagnosing issues related to Oracle Access Manager.

For more information about the HTTP Basic and Web SSO authentication types, see Enabling and Configuring a Mobile App Individually, page 2-14.

7

Diagnostics and Troubleshooting

Overview

This chapter describes how to enable logging and diagnostics features as well as how to troubleshoot possible issues from the mobile client and the server. It includes the following sections:

- Enabling the Logging and Diagnostics Features, page 7-1
- Troubleshooting Tips, page 7-6

Enabling the Logging and Diagnostics Features

Troubleshooting Oracle E-Business Suite mobile apps involves the following high level options:

- Server logging
- Client logging
- REST service auditing

To better understand these logging and auditing features, this section includes the following topics:

- Enabling Server Logging, page 7-2
- Enabling Client Logging, page 7-2
- Enabling REST Service Auditing, page 7-5

Enabling Server Logging

Oracle E-Business Suite mobile apps use the common logging and diagnostics features in Oracle E-Business Suite to enable the logging for REST services used by mobile apps. Once these features are enabled for Oracle E-Business Suite applications, administrators can use the log messages to diagnose and troubleshoot potential issues on the Oracle E-Business Suite server.

If a mobile app user reports a problem, an administrator can set the following Oracle Application Object Library (FND) profile options for that user to enable logging, control the logging level, and set the module for which logs are recorded. These profile options are also used if app users need to upload their client log files to the server.

- FND: Debug Log Enabled (AFLOG_ENABLED)
- FND: Debug Log Module (AFLOG_MODULE)
- FND: Debug Log Level (AFLOG_LEVEL)

> **Note:** Use the app-specific REST service module names to set the FND: Debug Log Module profile option. These module names are listed in Appendix B: Mobile App Module Names, page B-1.

For information on enabling the logging and diagnostics features, refer to the *Oracle E-Business Suite Maintenance Guide*.

Retrieving Server Logs

To retrieve the server logs recorded for your mobile app, perform the following steps:

1. Log in to Oracle E-Business Suite as the SYSADMIN user. Select the System Administrator (or System Administration) responsibility and choose the **Oracle Applications Manager** link and then the **Logs** link from the navigation menu.
2. In the Search System Logs page, click the **Advanced Search** button.
3. Enter the following information in the Advanced Search region:
   - **User:** Enter the mobile app user name.
   - **Module:** Enter the REST service module name of the mobile app.
4. Execute the search to retrieve and download the desired server logs.

Enabling Client Logging

If a user of Oracle E-Business Suite mobile apps reports a problem when using the app, and Oracle Support requests client logs, the following profile options set on the server for the server logging are also required for the client logging. These profile options enable the log upload service invoked by the mobile app to provide the upload feature.

- FND: Debug Log Enabled (AFLOG_ENABLED)

  Set this profile option to Yes to enable the debug logging.

- FND: Debug Log Module (AFLOG_MODULE)

  - For Oracle E-Business Suite Mobile Foundation Release 2.1 and onwards, set this profile option to your Application Bundle Id.

    For information on Application Bundle Id for each mobile app, see Appendix C: Application Definition Metadata, page C-1.

  - For Oracle E-Business Suite Mobile Foundation Release 2.0, set this profile option to "MOBILE".

- FND: Debug Log Level (AFLOG_LEVEL)

  Set this profile option to the level of detail you want to record, such as STATEMENT.

Note that the same logging profile options are used to enable the server and client logging, as well as the REST service auditing. It is recommended that you use the following sequence when troubleshooting both server and client code at the same time.

1. Turn on the server logging to obtain log statements written by REST services. For information on setting profile options for server logging, see Enabling Server Logging, page 7-2.

2. Direct the app user to turn on diagnostics logging on the mobile client.

3. Direct the app user to reproduce the issue that invokes the REST services.

   Log statements from the REST services should be recorded. However, the server cannot receive the client log file at this point.

4. Set the profile options as described in this section for the user to receive the client log file.

   The client and server logging can happen at the same time when an issue is being reproduced. However, to upload the log file, the profile options should be changed to receive the log file after the issue is reproduced.

5. Request the mobile app user to upload the log file from the mobile client to the server.

6. Retrieve the REST service log statements based on the profile options set in step 1.

7. Retrieve the mobile client log file uploaded based on profile options set in step 4.

Retrieving Client Logs

Direct mobile app users to perform the following steps to collect the logs from the mobile client:

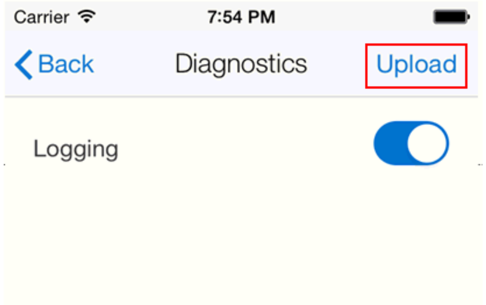
1. In the navigation menu of the mobile app, tap **Settings** and then the **Diagnostics**.

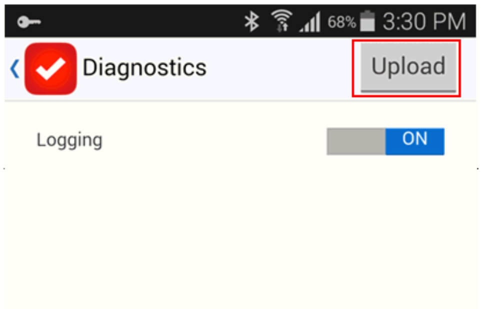
   In the Diagnostics screen, enable the client logging feature by turning on the **Logging** option.

2. Return to the navigation menu and reproduce the reported issue.

3. In the menu, tap **Settings** and then the **Diagnostics** again.

4. In the Diagnostics screen, tap the **Upload** icon on the top right corner. This displays the upload screen where app users can upload the log files recorded for the app to the Oracle E-Business Suite server.





5. You can then download the uploaded log files from the Oracle E-Business Suite server.

   To retrieve client logs, follow the steps described in Enabling Server Logging, page 7-2. However, use the following search criteria to locate the client logs:

   - **User:** Enter the mobile app user name.

   - **Module:** Enter appropriate information based on the Oracle E-Business Suite Mobile Foundation release:

     - For Oracle E-Business Suite Mobile Foundation Release 2.0, enter "MOBILE" as the Module name.

     - For Oracle E-Business Suite Mobile Foundation Release 2.1 and onwards, enter your Application Bundle Id as the Module name.

       For information on Application Bundle Id for each mobile app, see Appendix C: Application Definition Metadata, page C-1.

Please note that if the FND: Diagnostics profile option is enabled for a user, the complete error stack from the service invocation failure is displayed. Otherwise, only a simple error message is shown instead.

Enabling REST Service Auditing

Perform the following steps to enable auditing for REST service request and response payloads during the service invocation for Oracle E-Business Suite mobile apps:

> **Note:** The REST service payloads can be logged for auditing only when the server logging is also enabled.
>
> If the REST service auditing feature is not required, you can choose to enable the server logging only. See Enabling Server Logging, page 7-2.

1. Set the FND: OA Framework REST Service Audit Enabled (FND_OAF_REST_LOG_ENABLED) profile option to Yes.

   This enables the REST service auditing feature. The default value is No.

2. Set the following server logging profile options for the app users:

   - FND: Debug Log Enabled (AFLOG_ENABLED)

     Set this profile option to Yes to enable the debug logging.

   - FND: Debug Log Module (AFLOG_MODULE)

     Set this profile option to f`nd.framework.rest.Auditing%, <other REST service modules as applicable>`

     For example, to obtain logs for the Oracle Mobile Approvals for Oracle E-Business Suite app, set the profile option to the following: `fnd.framework.rest.Auditing%, fnd.wf.worklist%`

     To retrieve logs for auditing, follow the steps described earlier in Enabling Server Logging, page 7-2. However, use `fnd.framework.rest.Auditing` as the Module name instead of the module name of the app, along with the app user name as the search criteria to locate the logs.

   - FND: Debug Log Level (AFLOG_LEVEL)

     Set this profile option to at least the EVENT level in order for the auditing feature to work.

   If you want to use both logs and auditing to troubleshoot an issue with the underlying REST services, set the FND: Debug Log Level profile option to STATEMENT and set the FND: Debug Log Module profile option as described in this section.

Troubleshooting Tips

This section includes the following troubleshooting information on potential problem symptoms and corresponding solutions.

- Troubleshooting Tips on the Mobile Client, page 7-6

- Troubleshooting Tips on the Oracle E-Business Suite Server, page 7-20

For information about each app's definition metadata that may help identify the app in various troubleshooting processes, see Appendix C: Application Definition Metadata, page C-1.

If you contact Oracle Support about an app, specify the associated product name for that app. See Appendix E: Associated Products in My Oracle Support, page E-1.

Troubleshooting Tips on the Mobile Client

This section describes the troubleshooting tips on the mobile client. It includes the following topics:

- Directing Users to Obtain Connection Details and Initiate Server Updates, page 7-6

- Troubleshooting Tips for Oracle E-Business Suite Mobile Apps, page 7-8

- Troubleshooting Tips for Containerized, Enterprise-Distributed Apps, page 7-17

Directing Users to Obtain Connection Details and Initiate Server Updates

In Oracle E-Business Suite Mobile Foundation Release 2.1 or later releases, while trying to diagnose and troubleshoot issues encountered on the mobile client, you can direct users to obtain the server connection details from their mobile devices and check if any new updates from the server are required.

Perform the following steps to obtain the connection details and initiate server updates:

1. In the navigation menu of the mobile app, tap **Settings** and then **Connection Details**. The Connection Details screen appears.

2. The Connection Details screen displays the server URL field and the Server Configuration region.

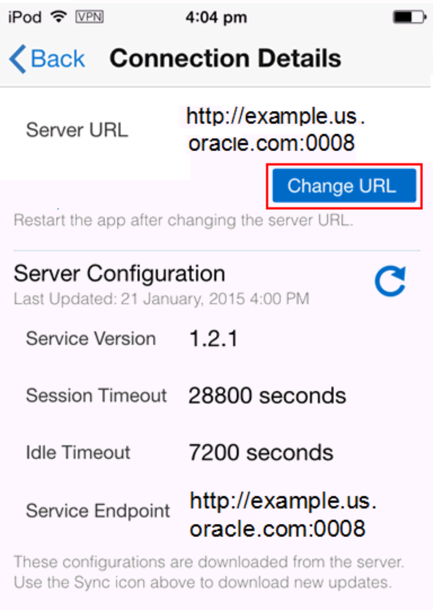
   - **Server URL field:** This is the URL value entered by the mobile user during the initial launch of the app. This value is retrieved from the local database in the device.

     Please note that if the mobile user wants to reconfigure the app to a different

Oracle E-Business Suite instance after the initial setup is complete, the user can change the server URL value by tapping the **Change URL** button. The app displays the device's Settings screen where the user can update the server URL directly.

> **Note:** When a user reconfigures an app from one Oracle E-Business Suite instance to another, the local preferences are completely removed. After the configuration, the user is required to set the preferences again.

> **Note:** The **Change URL** button is available in Oracle E-Business Suite Mobile Foundation Release 3.0 and onwards.
>
> To initiate the reconfiguration process in Oracle E-Business Suite Mobile Foundation Release 2.1, mobile users must manually navigate to the iOS device's Settings screen to update the URL value.



Connection Details

Server URL http://example.us.oracle.com:0008

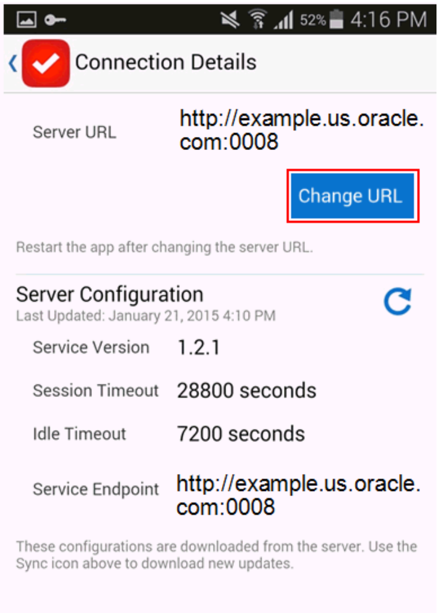
Restart the app after changing the server URL.

Server Configuration

Last Updated: 21 January, 2015 4:00 PM

Service Version	1.2.1
Session Timeout	28800 seconds
Idle Timeout	7200 seconds
Service Endpoint	http://example.us.oracle.com:0008

These configurations are downloaded from the server. Use the Sync icon above to download new updates.



Connection Details

Server URL http://example.us.oracle.com:0008

Restart the app after changing the server URL.

Server Configuration

Last Updated: January 21, 2015 4:10 PM

Service Version	1.2.1
Session Timeout	28800 seconds
Idle Timeout	7200 seconds
Service Endpoint	http://example.us.oracle.com:0008

These configurations are downloaded from the server. Use the Sync icon above to download new updates.

Additionally, the user can navigate to the device's Settings screen to change the server URL if desired:

- From the iOS device's Settings screen, tap **Settings**, then **App Name**, and then **Server URL**.
- From the Android devices with the app open, tap **Settings**, then **Settings or Preferences**, and then **Server URL**.

- **Server Configuration region:** This region displays the parameter values in the configuration file downloaded from the server.
  - **Last Updated:** The date and time when the app was last updated.
  - **Session Timeout:** The number of seconds that a user can remain logged in to the app.
  - **Idle Timeout:** The number of seconds that the app can remain idle.
  - **Service Endpoint:** The value used to invoke Oracle E-Business Suite services. This value can either be the same as the server URL entered by the user, or a dedicated web entry point for this app.
  - **Service Version:** The internal version of the mobile services used by the app, obtained from the app's definition metadata. For example, 1.0.0.

3. To check if any new updates from the server are required for the app, tap the **Sync** icon next to the Server Configuration region in the Connection Details screen. Direct users to follow the instructions on the mobile device to continue the updates from the server.

   For example, a user must restart the app immediately to apply the updates if either one of the following attributes from the server is different from the value in the device:

   - service endpoint
   - authentication type (Oracle E-Business Suite Mobile Foundation Release 4.0 only)

   If only the timeout values need to be updated, the user can choose to continue using the app without restarting it immediately. In this case the updates will be applied the next time the app is launched.

Troubleshooting Tips for Oracle E-Business Suite Mobile Apps

The following table lists common issues that might occur while using Oracle E-Business Suite mobile apps as well as the corresponding solutions.

Troubleshooting Tips on the Mobile Client

Issue	Tip
When a user enters a server URL in a mobile device using HTTPS, if the SSL certificate is invalid or untrusted and cannot be recognized by the mobile app, the following error message may appear: `"Please enter a valid URL."`	Ensure that your mobile app can perform a successful SSL handshake with the Oracle E-Business Suite SSL endpoint. 1. Validate that the JDK 8 client can connect to the Oracle E-Business Suite SSL endpoint. 2. Validate that the Oracle E-Business Suite SSL endpoint presents the complete certificate chain. For validation instructions, see the detailed steps as described in Secure Communication with HTTPS, page 6-3. For a list of root CAs trusted by the mobile client, see Migrating to New cacerts File for SSL in MAF 2.1.x, *Oracle Mobile Application Framework Installing Oracle Mobile Application Framework*.
After a user enters valid user credentials in the standard login screen, the app displays the loading indicator for a few seconds and then redirects the user back to the login screen.	Ensure that the Server URL used by the user to configure the app matches the Oracle E-Business Suite web entry URL. Otherwise, Oracle E-Business Suite server might reject the REST requests from the mobile app which will result in redirecting the user to the login screen.

Issue	Tip
When a user initiates the check for updates process by tapping **Settings** from the mobile app navigation menu, then tapping **Connection Details**, and then tapping the **Sync** icon in the Connection Details screen, the user is redirected to the login screen. After logging in to the app, the user is taken to the default landing screen. The same issue also occurs if a user tries to navigate to a different feature after the app has idle timed out, the user is redirected to the login screen. After the user logs in to the app, instead of taking the user to the desired screen before the timeout, the app redirects the user to the default landing screen.	To resolve the issue, apply the following patch for your release: • For Oracle E-Business Suite 12.1.3, apply patch 21643419:R12.FND.B • For Oracle E-Business Suite 12.2, apply patch 22046560:R12.FND.C It is recommended that you apply this patch after the corresponding consolidated product family patch for your app to avoid the issue.
The configuration server URL is not accessible when tested from a web browser. An HTTP 404 error appears. (For Oracle E-Business Suite Mobile Foundation Release 3.0 and earlier)	Verify that AutoConfig was run after you applied the appropriate consolidated patch for your Oracle E-Business Suite release.

Issue	Tip
After a user enters valid user credentials in the standard login screen after the configuration screen, the following error occurs: `The login server is not reachable.`	The cause of the issue could be either that the HTTP server is down or the login server was not installed and set up during installation of the appropriate patch on your Oracle E-Business Suite server. The URL for the login server used by mobile apps is in the following format: `http(s)://<hostname>:<port>/OA_HTML/RF.jsp?function_id=mLogin` Please note that this is not a URL that the app users would enter or edit. It is constructed during the app setup and loaded to the mobile app through the configuration file. If this URL value is invalid in the configuration file, the users will not be able to log in to Oracle E-Business Suite. Before allowing users to connect to Oracle E-Business Suite from mobile apps, ensure the right login server URL is set up in the configuration file described in Validating the Configuration, page 2-32. Additionally, you can test the login server URL by copying the URL and pasting it in a web browser. A pop-up window should appear for user name and password. After you successfully enter valid user credentials, an XML response should appear with the following elements: accessToken, accessTokenName, ebsVersion, and userName.

Issue	Tip

A mobile user fails to log in to an app. When an administrator tests the standalone mLogin REST service by entering the URL `http(s)://<hostname>:<port>OA_HTML/RF.jsp?function_id=mLogin` or tests the configuration service URL `http(s)://<hostname>:<port>OA_HTML/RF.jsp?function_id=mConfig&bundleId=<application bundle id>&file=ebs-mobile-config.xml`, one of the following errors occurs:
`Resource/rest NOT found`
or
`HTTP 500 Internal server error`
	Perform the following steps to resolve the issue:
	1. Verify if `AOLJRestServlet` exists in the following file:
	- For Oracle E-Business Suite Release 12.2.x, locate the servlet in the `$OA_HTML/WEB-INF/web.xml` file.
	- For Oracle E-Business Suite Release 12.1.3, locate the servlet in the `INST_TOP/ora/10.1.3/j2ee/oacore/application-deployments/oacore/html/orion-web.xml` file.
	2. If `AOLJRestServlet` does not exist, then verify if the app uses a custom template.
	- If a custom template is used, the custom template must be synchronized with the seeded templates. See the Section 4.2 Implementing AutoConfig Customizations, My Oracle Support Document 387859.1.
	- If a custom template is not used, continue to the next step.
	3. Run AutoConfig and ensure there is no error.
	4. Stop and restart the application tier server and then verify the issue.

After a user enters user credentials in the standard login screen after the configuration screen, the following error occurs: `Invalid username/password. If the problem persists, please contact your system administrator`	To resolve the issue, ensure that the user enters a valid user name and password. Verify the user name is still valid in the system and reset the password if required.

Issue	Tip
After a user enters valid user credentials in the standard login screen after the configuration screen, the following error occurs: `One or more parameters downloaded from the server are invalid.` The same error can also occur after the user initiates the check for updates process by tapping **Settings** from the mobile app navigation menu, then tapping **Connection Details** and then tapping the **Sync** icon in the Connection Details screen.	This is due to invalid configuration data, such as invalid service endpoint, in the downloaded configuration file. To resolve the issue, ensure that a valid service endpoint is specified in the Configure Mobile Applications page while setting up the mobile app.
After a user enters valid user credentials in the standard login screen after the configuration screen, the following error occurs: `An error occurred when downloading updates from the server.` The same error can also occur after the user initiates the check for updates process as described above.	To resolve the issue, ensure that there is no server or network connection issue.
After a user logs in to an app, while on the landing page of the app, the user leaves the device idle for a period of time beyond the value set in the Idle Timeout parameter (default value is 7200 seconds). When the user attempts to open the Springboard from the landing page, a blank page appears with a lock.	This issue is a known limitation in Oracle MAF, where after the idle period exceeds the value set in the Idle Timeout parameter, when the user accesses the Springboard, the app does not automatically display the login screen. To resolve the issue, close the Springboard and access other links in the landing page. The user should be redirected to the login screen.
A mobile user may find that the date and time information in the mobile device is different from that in the desktop pages.	This difference occurs because the mobile app displays the time zone and date and time information based on the settings specified in the mobile client's Settings screen. Tap **Settings**, then **General**, and then **Date & Time** in the iOS mobile Settings screen or tap **Settings** and then **Date & Time** in the Android Settings screen to set your preferences.

Issue	Tip
After modifying the Server URL through the iOS mobile Settings screen (tap **Settings**, then **App Name**, and then **Server URL**) or the Android device's Settings screen (tap **Settings**, then **Settings or Preferences**, and then **Server URL**), the user closes and restarts the app. The app displays the page with the message "The server URL has changed.", but the Server URL field is blank.	If the user removed the previous URL in the device settings but did not enter a new URL, then no value is shown for the Server URL field.
During the initial configuration of an app, after a mobile user enters a server URL and taps **Get Started**, the following error message appears: `Please enter a valid URL.`	Ensure the server URL is valid by performing the following steps: 1. Check if the user has entered `http://` or `https://` as appropriate for accessing your Oracle E-Business Suite server. 2. Make sure that the user has entered the correct host name and domain. 3. Make sure that the port number if used is valid.
During the initial configuration of an app, after a mobile user enters a server URL and taps **Get Started**, the following error message appears: `This mobile application is not currently configured on this server.`	This message appears because the required Oracle E-Business Suite Mobile Foundation patches have not been applied on the Oracle E-Business Suite server to which the app is connecting. Apply the patches described in Applying Prerequisite Patches, page 2-2 in order for the user to proceed through the page where the server URL value is entered.
After a user enters valid user credentials in the standard login screen after the configuration screen, the following error occurs: `Configuration Error - This mobile application is not currently enabled on this server. Please close the application.`	The app may be already configured but the status is set to "Disabled". In order for the apps to successfully access the configuration files, set the status of the app to "Enabled". For information on configuring Oracle E-Business Suite mobile apps, see Configuring the Mobile Apps on the Oracle E-Business Suite Server, page 2-11.

Issue	Tip
After entering a new Server URL through the Connection Details page in Oracle E-Business Suite Mobile Foundation Release 3.0 or later releases, or through the mobile Settings screen (tap **Settings**, then **App Name**, and then **Server URL** from the iOS Settings screen or tap **Settings**, then **Settings or Preferences**, and then **Server URL** from the Android Settings screen), the user returns to the app. The app still connects to the previous Oracle E-Business Suite instance.	After changing the server URL, the user must restart the app to initiate the reconfiguration flow.
A user taps **Settings** from the mobile app navigation menu, then taps **Connection Details** to display the Connection Details screen. However, the **Sync** icon is not shown.	If the app is connected to Oracle E-Business Suite Mobile Foundation releases earlier than Release 2.1, the **Sync** icon is automatically hidden. This **Sync** icon is shown only if the server is configured for Oracle E-Business Suite Mobile Foundation Release 2.1 or later releases.
After a user enters valid user credentials in the standard login screen after the configuration screen, the following error occurs: `Configuration Error - This mobile application is not currently configured on this server. Please close the application.` (For Oracle E-Business Suite Mobile Foundation Release 2.1 or later)	This error indicates that the app's status is "Not Configured". This means the administrator has not yet configured the app with appropriate configuration parameters or has not completed a mandatory setup required to use the mobile app. For information on setting the configuration parameters for your mobile app, see Configuring the Mobile Apps on the Oracle E-Business Suite Server, page 2-11.

Issue	Tip
After a mobile user enters a valid server URL in the Server URL screen, and then enters his or her user name and password in the login screen, the following message appears: `Configuration Error - This mobile application is not currently configured on this server. Please close the application.` (For Oracle E-Business Suite Mobile Foundation Release 2.0 only)	This message indicates that the app is unable to access the configuration service URL. Perform the following steps to resolve the issue: 1. Verify if the configuration service URL is accessible through a web browser by performing the following steps: 1. Construct the configuration service URL in the following format: `http(s)://<hostname>:<port>/OA_HTML/config/<application bundle id>/connections.xml` For the Application Bundle Id information for each mobile app, see Appendix C: Application Definition Metadata, page C-1. 2. Copy the configuration service URL you just constructed and paste it into a browser window. When prompted, enter the Oracle E-Business Suite user name and password. The browser loads the configuration file `connections.xml`. The file is loaded only if the app is configured and enabled on the server. 3. Verify the content to ensure that the configuration file for your mobile app is valid, well-formed XML, and validate that the configuration parameter values are the same values as configured from the Mobile Applications Manager UI pages. 2. Verify if the app is enabled by performing the following steps: 1. Log in to Oracle E-Business Suite as SYSADMIN user. Select the Mobile Applications Manager responsibility and choose the **Applications** link.

Issue	Tip
	2. Search and locate your mobile app. 3. Ensure the status of your app is set to "Enabled".

Troubleshooting Tips for Containerized, Enterprise-Distributed Apps

The following table lists the issues and solutions that are particularly related to containerized, enterprise-distributed apps, available in Oracle E-Business Suite Mobile Foundation Release 4.0.

For information about containerizing your enterprise-distributed apps using Oracle Mobile Security Suite (OMSS), see Mobile Application Management (MAM) Support with Oracle Mobile Security Suite, page 5-1.

For more troubleshooting information, see the Troubleshooting Oracle Mobile Security Suite chapter, *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*.

Troubleshooting Tips for Containerized, Enterprise-Distributed Apps

Issue	Tip
When a user loads maps for a containerized app on a mobile device, the message "Loading maps ..." appears, but the maps do not render in the containerized app.	Rendering maps may leverage external services. Perform the following steps to ensure that Oracle Mobile Security Suite MSAS (Mobile Security Access Server) server is configured to proxy to the required external services: 1. Review MSAS server proxy settings: `http://<msmhost.example.com>:<port>/access` 2. Navigate to the Mobile Security tab. 3. From the Mobile Security Launch Pad, click **Environments** in the Mobile Security Access Server section. 4. Click **Instances** in the MSAS tile. 5. Locate the instance for your gateway, click **Configure**. 6. Click the System Settings tab. Set the required Proxy Server Settings. For example, • Name: Company Proxy • Host Name: `proxy.example.com` • Port: 80 • User Name: Enter appropriate user name. • Password: Enter the password corresponding to the user name. • Hostnames without proxy: 127.0.0.1, `*.example.com`

Issue	Tip
After a user logs in to the Workspace app and starts an Oracle E-Business Suite mobile app on a mobile device, the user is forced to log in again to the mobile app.	To resolve the dual login issue, perform the following tasks: • Verify that if you correctly associate your Oracle E-Business Suite instance with Oracle Directory Services, a LDAP directory, and Oracle Access Manager (OAM). Ensure that the user can log in to Oracle E-Business Suite web applications (`http://<hostname>:<port>/OA_HTML/AppsLogin`). • Verify that if you configure the mobile app with the "WebSSO" authentication type through the Oracle E-Business Suite Mobile Application Manager UI pages. If the "HTTP Basic" authentication type is selected instead, the user could encounter the dual login issue. • Log in to your OMSS Workspace app as an Oracle Directory Services user. Start the OMSS Secure Browser, and then navigate to the AppsLogin page for Oracle E-Business Suite through a browser: `http://<hostname>:<port>/OA_HTML/AppsLogin` If both OMSS and Oracle E-Business Suite are associated with the same OAM and Oracle Directory Services, you should not be forced to log in again. The Oracle E-Business Suite home page should appear for the user who logged in to the OMSS Workspace. **Important:** **Disclaimer:** The steps described here serve as troubleshooting tips only. Oracle E-Business Suite browser-based apps are currently not certified to run on the OMSS Secure Browser.

Issue	Tip
When a user logs in to the Workspace app with valid credentials, the following error may appear: `Error - Authentication failure (MSAS 403). Please check your login information and try again.`	This error occurs because the clock on the Mobile Security Access Server and the clock on the mobile device are out of synchronization. If the difference between the clocks is more than 5 minutes, the authentication fails. This issue is also included in the Troubleshooting Oracle Mobile Security Suite chapter, *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*.
After a user logs in to a containerized, enterprise-distributed app configured with the WebSSO authentication type, if an empty Responsibility screen appears, the user is immediately re-directed to the login page again.	Ensure that the Oracle Directory Services user is associated with a valid Oracle E-Business Suite user. Additionally, the same Oracle Directory Services user can log in to Oracle E-Business Suite web applications (`http://<hostname>:<port>/OA_HTML/AppsLogin`).
When a user tries to access a containerized, enterprise-distributed app on a mobile device, the following error may appear: `The operation couldn't be completed (TransportErrors error 3.)`	Ensure that the Oracle Mobile Security Suite server and the Oracle E-Business Suite server are both configured against the same Oracle Access Manager server.

Troubleshooting Tips on the Oracle E-Business Suite Server

The following table describes common issues that might occur on the Oracle E-Business Suite server as well as the corresponding solutions.

Troubleshooting Tips on the Oracle E-Business Suite Server

Issue	Tip
After applying the appropriate patch for your Oracle E-Business Suite release, the Mobile Applications Manager responsibility is still not visible for SYSADMIN user by default.	Perform the following steps to resolve the issue: 1. Make sure the concurrent manager is running. 2. Submit a concurrent request for the "Workflow Directory Services User/Role Validation" concurrent program (FNDWFDSURV). Ensure that you set the "Add missing user/role assignments" parameter to Yes. You can leave the other parameters set to the default values. 3. Submit a concurrent request for the "Compile Security" concurrent program.
Users need to access the Mobile Applications Manager responsibility.	The SYSADMIN user is granted the Mobile Applications Manager responsibility by default. The SYSADMIN user can assign the responsibility to other users through the "Mobile Application Administrator" user role in User Management.
After you select the Mobile Applications Manager responsibility and the Applications link from the navigation menu and perform a search in the Search Mobile Applications page, no mobile applications are listed in the search result table.	Ensure all the prerequisite patches required for your mobile apps are applied. If the desired applications still do not appear in the search result table, contact Oracle Support.

Issue	Tip
A configuration parameter such as Timeout was modified on the server and the configuration file is regenerated. The current app users do not have the parameters updated.	In Oracle E-Business Suite Mobile Foundation releases earlier than Release 2.1, the configuration file is not updated to the client automatically when it is changed. To obtain the updated configuration file, users must uninstall the mobile app and then install it again. In Oracle E-Business Suite Mobile Foundation Release 2.1 and onwards, a mobile user can initiate the server updates from the mobile device. See Directing Users to Obtain Connection Details and Initiate Server Updates, page 7-6.

A

Mobile App Access Roles

Mobile App Access Roles

Oracle E-Business Suite mobile apps use access roles to protect mobile app data from unauthorized access. The following table lists the role name and internal role code for each Oracle E-Business Suite mobile app.

For information on how to assign these roles to responsibilities, see Setting Up Mobile App Access to Responsibilities, page 2-35.

Mobile App Access Roles

Mobile App Name	Role Name	Role Code
Oracle Mobile Approvals for Oracle E-Business Suite	N/A	N/A
Oracle Mobile Timecards for Oracle E-Business Suite	Mobile Time Entry	UMX|HXC_MBL_TIME_ENTRY
Oracle Mobile Learning for Oracle E-Business Suite	OLM Learner Mobile Application Role	UMX|MBL|OTA_LRNR_MOB_ACC
Oracle Mobile Person Directory for Oracle E-Business Suite	Access Role for Person Directory Mobile App	UMX|MBL|PERSON_DIRECTORY_APP_ACCES
Oracle Mobile iProcurement for Oracle E-Business Suite	iProcurement Mobile App Enquiry Role	UMX|ICX_MBL_REQ_ENQUIRY

Mobile App Name	Role Name	Role Code
Oracle Mobile Procurement for Oracle E-Business Suite	Purchasing Mobile App Role	UMX|PO_MOBILE_APP_ROLE
Oracle Mobile Project Manager for Oracle E-Business Suite	PA Mobile Project Manager App Access	UMX|MBL|PA_MBL_PRJ_MGR_APP_ACCESS
Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite	Mobile Discrete Manufacturing Supervisor	UMX|WIP_MOBILE_SUPERVISOR_ROLE
Oracle Mobile Inventory for Oracle E-Business Suite	INV Mobile Inventory App Access	UMX|MBL|INV_MBL_INV_APP_ACCESS
Oracle Mobile Maintenance for Oracle E-Business Suite	EAM Mobile Maintenance App Access	UMX|MBL|EAM_MBL_MAINT_APP_ACCESS
Oracle Mobile Process Production Supervisor for Oracle E-Business Suite	Mobile Supervisor	UMX|GME_MOBILE_SUPERVISOR
Oracle Mobile Product Information for Oracle E-Business Suite	PIM Restful Services Role	UMX|PIM_RESTFUL_SERVICES_ROLE
Oracle Mobile Project Manufacturing for Oracle E-Business Suite	PJM Mobile Project Manufacturing App Access	UMX|MBL|PJM_MBL_PROJMFG_APP_ACCESS
Oracle Mobile Sales Orders for Oracle E-Business Suite	ONT Mobile Inquiry App Access	UMX|MBL|ONT_MBL_INQ_APP_ACCESS

B

Mobile App Module Names

Mobile App Module Names

This section lists the REST service module name for each mobile app. Use this module name to set the FND: Debug Log Module (AFLOG_MODULE) profile option for enabling server logging. See: Enabling Server Logging, page 7-2.

Mobile App Module Names

Mobile App Name	Module Name
Oracle Mobile Approvals for Oracle E-Business Suite	fnd.wf.worklist%
Oracle Mobile Timecards for Oracle E-Business Suite	com.oracle.ebs.hr%
Oracle Mobile Learning for Oracle E-Business Suite	ota.mobile
Oracle Mobile Person Directory for Oracle E-Business Suite	per.mobile
Oracle Mobile iProcurement for Oracle E-Business Suite	icx.mobile
Oracle Mobile Procurement for Oracle E-Business Suite	po.mobile

Mobile App Name	Module Name
Oracle Mobile Project Manager for Oracle E-Business Suite	PA
Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite	WIP%
Oracle Mobile Inventory for Oracle E-Business Suite	MobileInventory
Oracle Mobile Maintenance for Oracle E-Business Suite	eam%
Oracle Mobile Process Production Supervisor for Oracle E-Business Suite	gme.maf.supervisor%
Oracle Mobile Product Information for Oracle E-Business Suite	com.oracle.ebs.scm.ego.products
Oracle Mobile Project Manufacturing for Oracle E-Business Suite	pjm.mobile%
Oracle Mobile Sales Orders for Oracle E-Business Suite	ont.mobile

C

Application Definition Metadata

Application Definition Metadata

This section describes the application definition metadata for each mobile app. You can use this information to search for an app through the Mobile Applications Manager UI pages, to construct and validate the configuration service URL with the Application Bundle Id, and to identify the app in some troubleshooting processes.

For more information on how the application definition metadata is used, see:

- Enabling a Mobile App Individually and Specifying the Configuration through the UI, page 2-11

- Validating the Configuration, page 2-32

- Troubleshooting Tips on the Mobile Client, page 7-6

The following table lists the application definition metadata for each mobile app:

Application Definition Metadata

Mobile App Name	Application Name	Application Short Name	Application Bundle Id	Parent Application Name
Oracle Mobile Approvals for Oracle E-Business Suite	EBS Approvals	WF_APPROVALS	com.oracle.ebs.atg.owf.Approvals	Application Object Library

Mobile App Name	Application Name	Application Short Name	Application Bundle Id	Parent Application Name
Oracle Mobile Timecards for Oracle E-Business Suite	EBS Timecards	HXC_TMECARDS	com.oracle.ebs.hr.hxc.timecards	Time and Labor Engine
Oracle Mobile Learning for Oracle E-Business Suite	Learning	OTA_ML	com.oracle.ebs.hr.ota.MobileLearning	Learning Management
Oracle Mobile Person Directory for Oracle E-Business Suite	Directory	PER	com.oracle.ebs.per.ebspersondirectory	Human Resources
Oracle Mobile iProcurement for Oracle E-Business Suite	iProcurement	ICX_IPROCUREMENT	com.oracle.ebs.prc.icx.iProcurement	iProcurement
Oracle Mobile Procurement for Oracle E-Business Suite	Procurement	PO_PROCUREMENT	com.oracle.ebs.prc.po.procurement	Purchasing
Oracle Mobile Project Manager for Oracle E-Business Suite	Project Manager	Project Mgr	com.oracle.ebs.pj.pa.ProjectMgr	Projects
Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite	Discrete Production Supervisor	WIP_MBL_SUPERVISOR	com.oracle.ebs.scm.wip.Supervisor	Work in Process
Oracle Mobile Inventory for Oracle E-Business Suite	Inventory	INV_INVENTORY	com.oracle.ebs.scm.inv.Inventory	Inventory

Mobile App Name	Application Name	Application Short Name	Application Bundle Id	Parent Application Name
Oracle Mobile Maintenance for Oracle E-Business Suite	Maintenance	EAM_MAINTENANCE	com.oracle.ebs.scm.eam.Maintenance	Enterprise Asset Management
Oracle Mobile Process Production Supervisor for Oracle E-Business Suite	Process Production Supervisor	GME_MBL_SUPERVISOR	com.oracle.ebs.scm.gme.Supervisor	Process Manufacturing Process Execution
Oracle Mobile Product Information for Oracle E-Business Suite	Product Information	EGO_PRODUCTS	com.oracle.ebs.scm.ego.products	Oracle Product Hub (formerly known as Oracle Product Information Management)
Oracle Mobile Project Manufacturing for Oracle E-Business Suite	Project Manufacturing	PJM_PROJMFG	com.oracle.ebs.scm.pjm.ProjectManufacturing	Project Manufacturing
Oracle Mobile Sales Orders for Oracle E-Business Suite	Sales Orders	ONT_SALES_ORDERS	com.oracle.ebs.scm.ont.SalesOrders	Order Management

D

Setting Up and Using the Supported Languages

Overview

Supported Languages

In the mobile app version 1.3.0 and the version 1.0.x for Person Directory and Learning apps, with Oracle E-Business Suite Mobile Foundation Release 4.0, Oracle E-Business Suite mobile apps are available in the following languages only, although other languages are listed in the app stores, such as Apple App Store:

- Brazilian Portuguese
- Canadian French
- Dutch
- English
- French
- German
- Italian
- Japanese
- Latin American Spanish
- Simplified Chinese
- Spanish

Note that the initial releases of our mobile apps were distributed in English only.

Mobile Device Locale Settings

To use these languages, set your mobile device locale to a desired language setting.

The following table lists the iOS mobile device locale settings:

> **Note:** For iOS mobile devices, set the same language for the iOS language and the preferred language. Using different languages for the iOS language and the preferred language could result in mixture of these languages in the UI pages where UI labels are shown in the language set for the iOS language, but the language data from Oracle E-Business Suite is shown in the preferred language.

iOS Mobile Device Locale Settings

Language	iOS Language	iOS Region
Brazilian Portuguese	Portuguese (Brazil)	Brazil
Canadian French	French (Canada)	Canada
Dutch	Dutch	*
English	English	*
French	French	*
German	German	*
Italian	Italian	*
Japanese	Japanese	*
Latin American Spanish	Spanish (Mexico)	*
Simplified Chinese	Chinese, Simplified	China
Spanish	Spanish	Spain

> **Note:** * indicates you can set the language for any country or region except for the region or country used by its variant language. For

example, you can set the language French for France or Swiss except Canada because Canada uses Canadian French.

The following table lists the Android mobile device locale settings:

Android Mobile Device Locale Settings

Language	Android Language	Android Region
Brazilian Portuguese	Portuguese (Brazil)	N/A
Canadian French	French (Canada)	N/A
Dutch	Dutch (*)	N/A
English	English (*)	N/A
French	French (*)	N/A
German	German (*)	N/A
Italian	Italian (*)	N/A
Japanese	Japanese	N/A
Latin American Spanish	Spanish (United States)	N/A
Simplified Chinese	Chinese (Simplified)	N/A
Spanish	Spanish (Spain)	N/A

If your Oracle E-Business Suite environment supports multiple languages and you set your mobile device language to a language that is supported by Oracle E-Business Suite, but not by Oracle E-Business Suite mobile apps, then the data retrieved from the Oracle E-Business Suite server will be displayed in the mobile device specified language. However, the user interface labels within the app will appear in English.

If you set your mobile device language to a language that is neither supported by Oracle E-Business Suite nor enabled in your Oracle E-Business Suite environment, then the data coming from the Oracle E-Business Suite server will be displayed in the Oracle E-Business Suite base language.

Oracle Access Manager Language Configuration

If you want your Oracle Access Manager (OAM) login page to be displayed in one of the supported languages for the mobile apps, perform the following tasks to configure OAM for the supported languages:

> **Note:** Before you begin the configuration, ensure that you understand how OAM handles the languages in the login page, and then properly configure the default language which is used, if OAM cannot determine the device language. See "2.5 Choosing a Language for Oracle Access Management Login", *Fusion Middleware Administrator's Guide for Oracle Access Management*.

- Log on to the OAM server.
- Navigate to the OAM domain, such as `</base_dir>/Middleware/user_projects/domains/oam_domain/`.
- Back up the original `oam-config.xml` file.
- Edit the `oam-config.xml` file.

  1. Search for "LoginPageLocales". Navigate to the end of setting definition to find the last language code entry.
  2. Copy the last language code entry.

     Change the languages to the corresponding language codes listed in the following table and increase the number by 1.

Language	Language Code
Brazilian Portuguese	pt-BR
Canadian French	fr-CA
Dutch	nl-NL, nl-BE
English	en-US, en-AU, en-CA, en-IN, en-IE, en-NZ, en-SG, en-ZA, en-GB
French	fr-FR, fr-BE, fr-CH

Language	Language Code
German	de-DE, de-LI, de-AT, de-CH
Italian	it-IT, it-CH
Japanese	ja-JP
Latin American Spanish	es-US, es-XL
Simplified Chinese	zh-CN
Spanish	es-ES

3. Repeat the previous step 2 for the all languages you plan to use. For example,

```
<Setting Name="27" Type="xsd:string">fr-CA</Setting>
<Setting Name="28" Type="xsd:string">fr-FR</Setting>
<Setting Name="29" Type="xsd:string">fr-BE</Setting>
<Setting Name="30" Type="xsd:string">fr-CH</Setting>
<Setting Name="31" Type="xsd:string">nl-NL</Setting>
<Setting Name="32" Type="xsd:string">nl-BE</Setting>
<Setting Name="33" Type="xsd:string">de-DE</Setting>
<Setting Name="34" Type="xsd:string">de-LI</Setting>
<Setting Name="35" Type="xsd:string">de-AT</Setting>
<Setting Name="36" Type="xsd:string">de-CH</Setting>
<Setting Name="37" Type="xsd:string">en-AU</Setting>
<Setting Name="38" Type="xsd:string">en-CA</Setting>
<Setting Name="39" Type="xsd:string">en-IN</Setting>
<Setting Name="40" Type="xsd:string">en-IE</Setting>
<Setting Name="41" Type="xsd:string">en-NZ</Setting>
<Setting Name="42" Type="xsd:string">en-SG</Setting>
<Setting Name="43" Type="xsd:string">en-ZA</Setting>
<Setting Name="44" Type="xsd:string">en-GB</Setting>
<Setting Name="45" Type="xsd:string">en-US</Setting>
<Setting Name="46" Type="xsd:string">ja-JP</Setting>
<Setting Name="47" Type="xsd:string">it-IT</Setting>
<Setting Name="48" Type="xsd:string">it-CH</Setting>
<Setting Name="49" Type="xsd:string">es-US</Setting>
<Setting Name="50" Type="xsd:string">es-XL</Setting>
<Setting Name="51" Type="xsd:string">es-ES</Setting>
```

- Stop and restart the OAM server.

E

Associated Products in My Oracle Support

Associated Products in My Oracle Support

The following table lists the associated product for each Oracle E-Business Suite mobile app in My Oracle Support. If you contact Oracle Support about an app, specify the associated product name for that app as shown here so that Oracle Support can direct your query appropriately.

Associated Products in My Oracle Support

Mobile App Name	Module Name
Oracle Fusion Expenses	Oracle Internet Expenses
Oracle Mobile Approvals for Oracle E-Business Suite	Oracle Workflow
Oracle Mobile Timecards for Oracle E-Business Suite	Oracle Time and Labor
Oracle Mobile Learning for Oracle E-Business Suite	Oracle Learning Management
Oracle Mobile Person Directory for Oracle E-Business Suite	Oracle Human Resources
Oracle Mobile iProcurement for Oracle E-Business Suite	Oracle iProcurement

Mobile App Name	Module Name
Oracle Mobile Procurement for Oracle E-Business Suite	Oracle Purchasing
Oracle Mobile Project Manager for Oracle E-Business Suite	• Oracle E-Business Suite Release 12.1.3: Oracle Project Management • Oracle E-Business Suite Release 12.2: Oracle Project Planning and Control
Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite	Oracle Work in Process Oracle MES for Discrete Manufacturing
Oracle Mobile Inventory for Oracle E-Business Suite	Oracle Inventory Management
Oracle Mobile Maintenance for Oracle E-Business Suite	Oracle Enterprise Asset Management
Oracle Mobile Process Production Supervisor for Oracle E-Business Suite	Oracle Process Manufacturing Process Execution
Oracle Mobile Product Information for Oracle E-Business Suite	Oracle Item Master Oracle Product Hub
Oracle Mobile Project Manufacturing for Oracle E-Business Suite	Oracle Project Manufacturing
Oracle Mobile Sales Orders for Oracle E-Business Suite	Oracle Order Management