Oracle® E-Business Suite

Mobile Apps Administrator's Guide

Release 12.1 and 12.2

Part No. E64384-22

September 2023

ORACLE

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

Part No. E64384-22

Primary Author: Vijay Shanmugam, Melody Yang

Contributing Author: Tushar Abedin, Tahir Ahmad, Prasad Akkiraju, Hadi Alatasi, Sugathan Aravindan, Prasanna Athota, Srinivasa Rao Atla, Rekha Ayothi, Krishna Botta, John Brazier, Hubert Ferst, Sunil Ghosh, Erik Graversen, Sri Ramya Inturi, Clara Jaeckel, Anupam Johri, Jeanne Lowell, Saritha Merugu, Lohit Moripalli, Ravindra Nadakuditi, Sanyukta Palod, Chidananda Pati, Balakrishna Pulivarthi, Arun Purushothaman, Tirupathi Rao PVS, Esteban Rodriguez, Dilbagh Singh, Ryoji Suzuki, Sukanya Tadepalli, Venkatakalpanarani Thota, Arvin Tjen, Erik Wu, Ice Yu

Contents

3 Advanced Configurations for Demilitarized Zone

Part 2 Oracle E-Business Suite Mobile Apps Release 9.x and Earlier

8 Introduction to Oracle E-Business Suite Mobile Apps 9.x and Earlier

9 Setting Up the Mobile Apps

10 Setting Up Push Notifications for Mobile Apps

11 Administering the Mobile Apps

12 Advanced Configurations for Demilitarized Zone

13 Advanced Configurations for Secure Communication with HTTPS

Send Us Your Comments

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

Part No. E64384-22

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 xiv 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 Help Center, provides the latest updates to Oracle E-Business Suite

documentation. See https://docs.oracle.com/cd/E26401_01/index.htm for the latest Release 12.2 documentation or https://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 as an application in Oracle E-Business Suite.

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 Cloud Manager Guide

This guide describes how to manage Oracle E-Business Suite environments on Oracle Cloud Infrastructure (OCI) using the automated tooling in Oracle E-Business Suite Cloud Manager.

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 any installation and configuration choices that are 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 Oracle E-Business Suite

Development. 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 Electronic Technical Reference Manual User's Guide

This guide describes how to set up and navigate Oracle E-Business Suite Electronic Technical Reference Manual (eTRM) user interface in Oracle E-Business Suite. It also explains how to browse and search the Oracle eTRM repository to locate desired FND and database metadata and objects, and how to view object details, reports, and diagrams.

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 designed to help keep a system running smoothly.

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

This guide includes information for the latest mobile release with new underlying technologies, as well as the earlier mobile releases built with Oracle Mobile Application Framework (MAF). For mobile releases built with MAF, this guide describes how to develop enterprise-distributed mobile apps by using mobile application archive (MAA) files and how to implement corporate branding. It also explains required tasks on implementing push notifications for supported mobile apps. In addition, it includes how to implement Oracle E-Business Suite REST services to develop custom mobile apps by using the Login component from Oracle E-Business Suite Mobile Foundation or using any mobile app development framework if desired.

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, secure configuration, 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 products, enter and query data, and run concurrent requests by means of the user interfaces (UI) of Oracle E-Business Suite. It includes basic information on setting preferences and customizing the UI. An

introduction to Oracle Enterprise Command Centers is also included. Lastly, this guide describes accessibility features and keyboard shortcuts for Oracle E-Business Suite.

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

This guide contains the user interface (UI) standards followed by Oracle E-Business Suite Development. It describes the UI for Oracle E-Business Suite products based on Oracle Forms, and how to apply this UI to the design of such applications.

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 configure message metadata for Oracle Mobile Approvals for Oracle E-Business Suite and 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.

Part 1

Oracle E-Business Suite Mobile Apps Release 10.x

1

Introduction to Oracle E-Business Suite Mobile Apps Release 10.x

Overview

To provide state-of-the-art features and enhanced functionality for mobile app users, Oracle E-Business Suite Mobile Release 10.x apps uptake new underlying technologies to allow app development in a more agile and hybrid way. These underlying technologies such as Oracle JavaScript Extension Toolkit (JET) and Cordova frameworks are no longer dependent on Oracle MAF.

The Mobile Release 10.x apps are made available on separate release cycles. Collectively they represent the next version of Oracle E-Business Suite mobile apps known as Mobile Release 10.x.

> **Note:** Oracle E-Business Suite Mobile Release 10.x apps have been renamed to distinguish them from the app versions built with earlier technology. These Mobile Release 10.x apps are:
>
> - Oracle Approvals for EBS, with Oracle JavaScript Extension Toolkit (JET) 14.0 Framework uptake (see Document 1642423.1)
> - Oracle Field Service for EBS, with Cordova Framework uptake (see Document 2188514.1)
> - Oracle Maintenance for EBS, with Oracle JavaScript Extension Toolkit (JET) 13.0 Framework uptake (see Document 1923702.1)
> - Oracle Mobile SCM for EBS (MSCA), with Oracle JavaScript Extension Toolkit (JET) 13.0 Framework uptake (see Document 2108155.1)
> - Oracle Self-Service HR for EBS, with Oracle JavaScript Extension

Toolkit (JET) 14.0 Framework uptake (See Document 2105189.1 for details)

- Oracle Timecards for EBS, with Oracle JavaScript Extension Toolkit (JET) 14.0 Framework uptake (See Document 1669224.1 for details)

Some 10.x apps are available for download from the Apple App Store and Google Play Store, and some apps are available through web page URLs provided by their administrators. For information about the app deployment availability and the names used in this release, see *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*, My Oracle Support Knowledge Document 1641772.1.

To use the Mobile Release 10.x apps, users must be licensed for the base products, with mobile services configured on the Oracle E-Business Suite server. To find the apps available for download on the stores, search for the keywords "Oracle America EBS" in the Apple App Store and Google Play Store.

This guide describes how to set up an Oracle E-Business Suite instance to support connections from these mobile apps. It also describes required setup tasks for advanced configurations and troubleshooting information for Oracle E-Business Suite mobile apps.

- 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 *Oracle E-Business Suite Mobile Apps Frequently Asked Questions (FAQ)*, My Oracle Support Knowledge Document 2064887.1.

- To share ideas with Oracle related to mobile apps, see *Oracle E-Business Suite Product Enhancement Request to My Oracle Support Community FAQ*, My Oracle Support Knowledge Document 1584210.2.

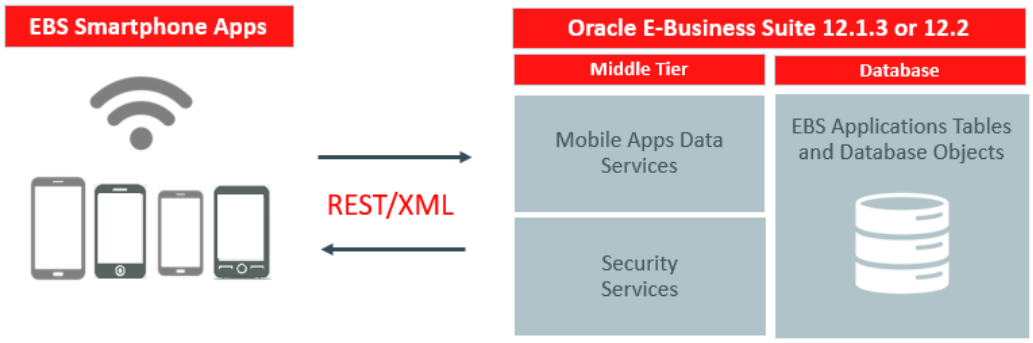
For information about the available languages in Oracle E-Business Suite Mobile Release 10.x apps, see Setting Up and Using Supported Languages, page E-1.

Technical Overview

Similar to earlier releases, Mobile Release 10.x apps interact with the application 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 overview for Oracle E-Business Suite Mobile Release 10.x apps:

Technical Architecture Overview



> **Note:** Oracle Maintenance for EBS and Oracle Field Service for EBS provide both online and offline (disconnected) modes to meet their core business functions. For information about the architecture diagram for the offline (disconnected) mode for Oracle Maintenance for EBS, see My Oracle Support Knowledge Document 1923702.1, *Oracle Mobile Maintenance for Oracle E-Business Suite Release Notes*. For information about Oracle Field Service for EBS, see My Oracle Support Knowledge Document 2188514.1, *Oracle Mobile Field Service for Oracle E-Business Suite Release Notes*.

Oracle E-Business Suite Mobile Release 10.x apps are compatible with Oracle E-Business Suite Release 12.2.3 and later, as well as iOS 15.5 or later and Android 12.0 or later. Oracle Field Service for EBS 10.x and Oracle Mobile SCM for EBS 10.x also support Oracle E-Business Suite Release 12.1.3.

- On iOS platform - Users can run the mobile apps on any devices that are capable of running iOS 15.5 or later. Oracle E-Business Suite primarily tests its iOS mobile apps with iPhones, iPod Touches, and iPads.

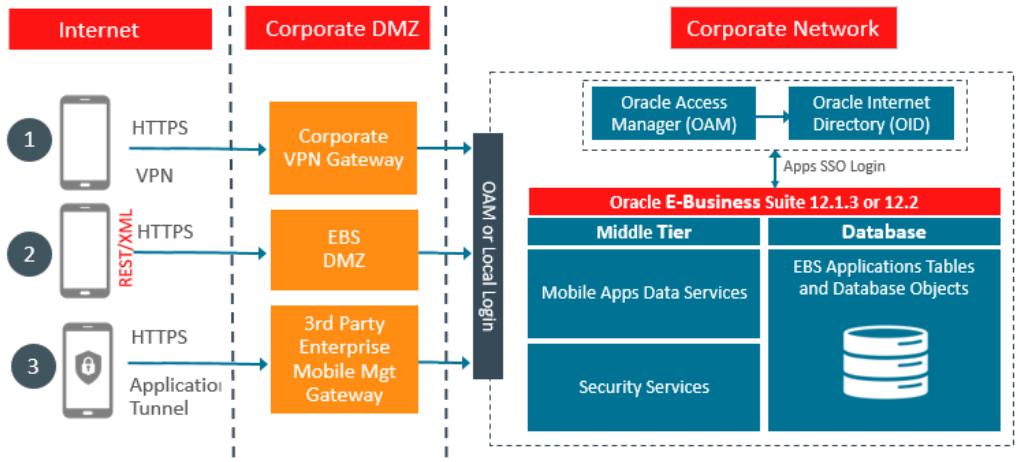
- On Android platform- Users can run Android mobile apps on any devices that are capable of running Android 12.0 or later. Android device manufacturers often customize their Android distributions. Due to the degree of Android fragmentation, Oracle E-Business Suite cannot perform comprehensive device-specific 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 one-on-one basis and may need additional assistance from the device vendors first.

To use the Oracle E-Business Suite mobile apps, you need to apply server-side patches and perform some setup tasks to configure your mobile app on the server. Before you begin configuring these apps, Oracle recommends that you review the apps and perform the configuration steps described in their app-specific product release notes. For information about the product release notes, see "Oracle E-Business Suite Mobile Apps" in My Oracle Support Knowledge Document 1641772.1, *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*.

Oracle E-Business Suite Mobile Apps Server Connectivity Options

Oracle E-Business Suite mobile app users have the following server connectivity options, as shown in the following diagram, to access the mobile apps:

Oracle E-Business Suite Mobile Apps Server Connectivity Options



1. Over the Internet

   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. For additional information on performing this configuration, see Advanced Configurations for Demilitarized Zone, page 3-1.

   > **Note:** This connectivity option is currently not available for Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA).

2. Over the Intranet

   If your Oracle E-Business Suite environment is not set up in a DMZ configuration, mobile app users must access the Oracle E-Business Suite mobile apps through an intranet connection, such as a virtual private network (VPN).

3. Through Enterprise Mobility Management (EMM) Solutions

Oracle E-Business Suite Mobile Release 10.x provides this connectivity option allowing supported apps to integrate with third-party Enterprise Mobility Management solutions that support common AppConfig standards, such as VMware AirWatch.

> **Note:** This connectivity option has been tested on iOS devices for Oracle Maintenance for EBS, Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS.

For more information, see Integrating Oracle E-Business Suite Mobile Apps with Enterprise Mobility Management Solutions, page 6-1.

Additionally, refer to the following advanced configurations to have secured server access for your mobile apps:

- Advanced Configurations for Secure Communication with HTTPS, page 4-1
- Advanced Configurations for Single Sign-On, page 5-1

Sizing Requirements

Because there are different product combinations, different user profiles, and different configurations, there is no one sizing answer for all hardware platforms. Some hardware vendors have sizing worksheets that model the CPU and memory requirements of Oracle E-Business Suite on their hardware. The most reliable strategy to ensure that the hardware is sized appropriately is to install a test environment, and then conduct a benchmark test with a configuration, product mix, and user load that simulates your own current and expected workloads. These conditions can help verify performance before you install your production-ready environment. An alternative is to ask Oracle Consulting Services or your hardware vendor to find another Oracle E-Business Suite system running a product mix and user profile similar to yours.

General Sizing Guidelines

When planning your Oracle E-Business Suite mobile app deployment, consider the following:

- You can support 150 to 180 mobile users per 2 GB of JVM heap.
- The initial heap size (Xms) and maximum allocated heap (Xmx) should both be set to 2 GB per 150 to 180 users.
- One JVM is allocated per 2 CPUs in general. This is an actual CPU core rather than a logical core.
- Use JVMs with a maximum of 4 GB, and scale for more users by using additional JVMs. The benefits are:

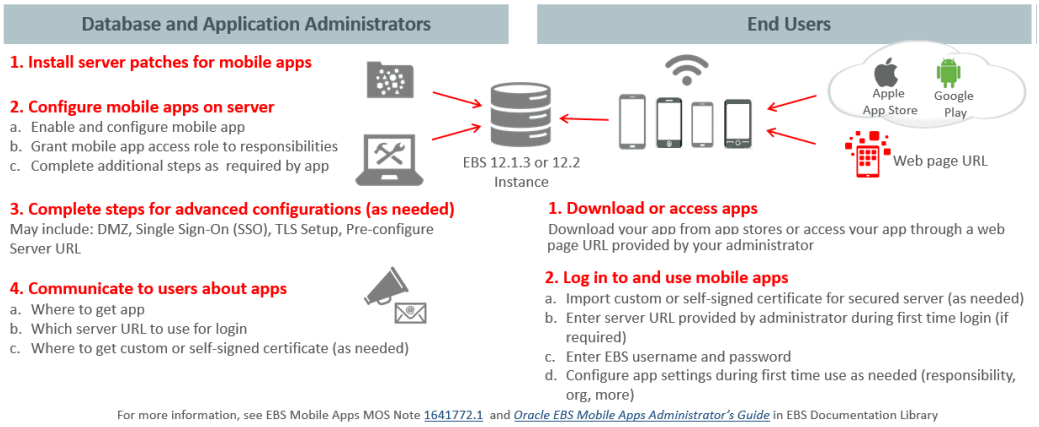
- Garbage collection (GC) activity is easily balanced (automatically) with multiple JVMs.
- Each instance will be able to utilize a separate connection pool. In essence, you need to maintain a balance between the allocated JVM heap size per instance and the available connection pool for that instance.

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.

The following diagram illustrates the 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 or access the app on the go.

Oracle E-Business Suite Mobile Apps High Level Implementation Steps



As illustrated in the diagram, these high level tasks are:

- Setup tasks on the server:
  1. Apply prerequisite patches on the Oracle E-Business Suite server
  2. Configure the mobile apps on the Oracle E-Business Suite server

     This may include enabling a mobile app, setting up the mobile app access to responsibilities, and completing additional setup tasks if required for the app.
  3. Complete the setup tasks for advanced configurations if required for an app

     This may include the setup tasks for a DMZ configuration, Single Sign-On (SSO), secure communication with HTTPS, and pre-configure server URL.

4. Communicate the mobile app information to users

   This information includes where to download or access an app, which server to use for login, and where to get custom or self-signed certificates if required.

- Tasks on the mobile client:

  1. Download or access your app

     As instructed by your administrator, mobile users can download an app from a public store, such as Apple App Store and Google Play Store, or can access an app through a web page URL if applicable.

  2. Log in and use your app

     This task includes importing custom or self-signed certificates if required for secured server access, entering server URL provided by your administrator for the initial login, entering user name and password, and configuring app settings for the initial use if needed.

The setup details of these tasks are further explained in the remaining chapters of this book.

2

Setting Up the Mobile Apps

Overview

This chapter describes the setup tasks that administrators must perform first to ensure that the 10.x apps are ready to use.

Depending on your app requirements, administrators may perform different tasks to set up your app before communicating the information to the app users. These setup tasks are described as follows:

- Setup Tasks for Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS, page 2-1
- Setup Tasks for Oracle Maintenance for EBS, page 2-14
- Setup Tasks for Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA), page 2-48

Setup Tasks for Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS

Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS are developed using a similar approach with the same Oracle JavaScript Extension Toolkit (JET) 14.0 Framework. Therefore, the setup tasks of these apps are described in the same section.

> **Note:** These three apps are available through web page URLs, not through the Apple App Store or Google Play Store. Users can access the apps using the URLs provided by their administrators.

1. Applying Server-Side Patches for Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS, page 2-2

2. Setting Up MIME Type Mappings, page 2-8
3. Setting Up Mobile App Access to Responsibilities (for Oracle Self-Service HR for EBS and Oracle Timecards for EBS), page 2-8
4. Performing Additional App-Specific Setup, page 2-10
5. Communicating Mobile App Information to Users, page 2-11
6. Performing Advanced Configurations, page 2-12
7. Enabling the Server Logging and REST Service Auditing Features, page 2-13

Task 1: Applying Server-Side Patches for Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS

Apply the corresponding consolidated product family patch and conditionally required patches if needed for your apps.

> **Note:** In Oracle E-Business Suite Release 12.2, when you apply patches using the adop (AD Online Patching) utility, adop runs AutoConfig by default.

Perform the required tasks to apply prerequisite patches in the following sequence:

1. Applying Product Family Level Patches, page 2-2
2. Applying Conditional Post-Install Patches, page 2-6

Step 1: Applying the Product Family Level Patches for Oracle Release 10.x Apps

Apply the server-side patches for Release 12.2 using either the Oracle E-Business Suite level consolidated patch or the individual product family patches, depending on your needs.

- **Apply the Oracle E-Business Suite level patch for Release 12.2**

  To simplify the patching efforts, the server-side product family patches are consolidated into a single Oracle E-Business Suite level patch for Release 12.2. This consolidated patch includes each product family patch that is listed in the product family level patch table.

  If you intend to uptake all the product family patches, simply apply the higher level consolidated patch, Patch 35706735:12.2.0.

- **Apply the relevant product family level patches for Release 12.2**

  If you only use certain product families, then apply the relevant individual product

family level patches for your Oracle E-Business Suite mobile apps.

The following table lists the mobile apps covered by each product family and the corresponding product family level consolidated patches:

Oracle E-Business Suite Product Family Level Patches for Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS Release 10.x

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.2
Oracle E-Business Suite Applications Technology (atg_pf) (See **Footnote 1**, page 2-6)	• Oracle Approvals for EBS	Patch 35481482:R12.ATG_PF.C- 12.2 Consolidated Patch For Mobile Applications Release 10 Apply the product family patches for the seeded approval types you want to use, as shown in subsequent rows in this table. If you want to use all the seeded approval types, see **Footnote 2**, page 2-6.

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

Oracle Financials (fin_pf)	• Oracle Approvals for EBS (for Expense approvals)
	• Oracle Approvals for EBS (for Supplier Invoices approvals)
	• Oracle Approvals for EBS (Lease and Finance Management approvals only)
		• For Expense approvals and Supplier Invoices approvals only
		  • Patch 30107297:R12.FIN_PF.C: FIN - 12.2 Consolidated Patch For Mobile Applications Foundation V9
		• For Lease and Finance Management approvals only
		Apply the following individual patches:
		  • Patch 28969483:R12.OKL.C
		  • Patch 29143795:R12.OKL.C
		See My Oracle Support Knowledge Document 2610782.1 and each patch Readme for additional patch prerequisites.

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.2
Oracle Human Resources (hr_pf)	• Oracle Approvals for EBS (for Human Resources approvals) • Oracle Approvals for EBS (for Timecard approvals) • Oracle Self-Service HR for EBS • Oracle Timecards for EBS	Patch 35706722:R12. HR_PF. C: HRMS - 12.2 Consolidated Patch For Mobile Applications Release 10
Oracle Interaction Center Family (cc_pf)	• Oracle Approvals for EBS (for Channel Revenue Management approvals) • Oracle Approvals for EBS (for Quoting approvals)	Patch 24383599:R12.CC_PF. C: CRM - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied
Oracle Procurement (prc_pf)	• Oracle Approvals for EBS (for Purchase Order approvals) • Oracle Approvals for EBS (for Requisition approvals)	Patch 24383558:R12.PRC_PF. C: PRC - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied
Oracle Projects (pj_pf)	• Oracle Approvals for EBS (for Projects approvals)	Patch 24383522:R12.PJ_PF.C: PROJ - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.2
Oracle Supply Chain Management (scm_pf)	• Oracle Approvals for EBS (for Inventory approvals) • Oracle Approvals for EBS (for Product Information approvals) • Oracle Approvals for EBS (for Order Management approvals) • Oracle Approvals for EBS (for Maintenance approvals) • Oracle Approvals for EBS (for Service Contracts approvals)	Patch 30144036:R12. SCM_PF.C: SCM -12.2 Consolidated Patch For Mobile Applications Foundation V9

Footnote 1: This Oracle E-Business Suite Applications Technology (atg_pf) product family level patch for mobile Release 10 includes the previous atg_pf Patch 30144032:R12.ATG_PF.C for Mobile Applications Foundation V9, and is specifically built for Oracle Approvals for EBS Release 10.x.

Footnote 2: If you plan to use all the seeded approval types for Oracle Approvals for EBS, to simplify the patching efforts, you can apply the Oracle E-Business Suite 12.2 level consolidated Patch 35706735:12.2.0, which includes all the product family patches listed in the table.

Step 2: Applying Conditional Post-Install Patches

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

Conditional Post-Install Patches for Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS Release 10.x

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 • Oracle E-Business Suite Mobile Release 10.0 Online Help	Required for Oracle E-Business Suite 10 mobile apps, leveraging Oracle E-Business Suite Mobile Foundation Release 9.1, connected to Oracle E-Business Suite Release 12.2	• Release 12.2: Patch 35622500
Oracle E-Business Suite Release 12.2	Required only if your Oracle E-Business Suite environment has the following patches applied: • Release 12.2 - Patch 27761509:12.2.0 (Oracle Applications Release 12.2 : Consolidated Patch for Data Removal Tool) **Note:** If your environment has the following Data Removal Tool consolidated patches applied instead, then the post-install tasks specified in the next column are not required: • Release 12.2 - Patch 29206195:12.2.0 (Oracle Applications Release 12.2 Data Removal Tool - One-off Consolidation - January 2020)	Perform the following steps in the specified order: • Release 12.2: 1. Apply Patch 28295762:R12.PER.C. 2. Apply Patch 28303904:R12.FND.C. 3. Recompile the data removal metadata by running the concurrent program "Recompile Metadata for Data Removal Tool", with the "Entity Type" parameter set to "ALL".

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 • Oracle Approvals for EBS • Oracle Self-Service HR for EBS • Oracle Timecards for EBS	Required for Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS after applying NLS language patches.	Patch 35742307:12.2.0

Task 2: Setting Up MIME Type Mappings

After applying required server-side patches, you need to set up MIME type mappings for web application manifest file using the following steps:

1. Add the following entry in the `$EBS_DOMAIN_HOME/config/mimemappings.properties` file:

   ```
   webmanifest=application/manifest+json
   ```

2. Restart all services on the application tier.

Task 3: Setting Up Mobile App Access to Responsibilities (for Oracle Self-Service HR for EBS and Oracle Timecards for EBS)

Oracle Self-Service HR for EBS and Oracle Timecards for EBS use role-based access control to protect the mobile app data from unauthorized access.

Oracle Self-Service HR for EBS and Oracle Timecards for EBS 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 Approvals for EBS is available through global grant to all Oracle E-Business Suite users.

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.

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 Mobile App Access Roles, page B-1.

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*.

Task 4: Performing Additional App-Specific Setup

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

- Oracle Approvals for EBS (see Document 1642423.1)

- Oracle Self-Service HR for EBS (see Document 2105189.1)

- Oracle Timecards for EBS (see Document 1669224.1)

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.

Task 5: Communicating Mobile App Information to Users

After you have completed the setup tasks for your app, provide the following information to the users who access the app through a web page URL:

- Name of the app

  For the name of the mobile app to download or access through a URL, see the *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*, My Oracle Support Knowledge Document 1641772.1.

- Where to access the app

  Provide the URL information in the following format to your app users:

  - For Oracle Approvals for EBS:

    ```
    http(s)://<E-Business Suite Host Name>:<Port>/OA_HTML/RF.
    jsp?function_id=WF_APPROVALS_PWA
    ```

    See My Oracle Support Knowledge Document 1642423.1, *Oracle Mobile Approvals for Oracle E-Business Suite Release Notes*.

  - For Oracle Self-Service HR for EBS:

    ```
    http(s)://<E-Business Suite Host Name>:<Port>/OA_HTML/RF.
    jsp?function_id=PER_MSSHR
    ```

    See My Oracle Support Knowledge Document 2105189.1, *Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite Release Notes*.

  - For Oracle Timecards for EBS:

    ```
    http(s)://<E-Business Suite Host Name>:<Port>/OA_HTML/RF.
    jsp?function_id=HXC_MTIME_ENTRY
    ```

    See My Oracle Support Knowledge Document 1669224.1, *Oracle Mobile Timecards for Oracle E-Business Suite Release Notes*.

- 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.

- Where to get custom or self-signed certificates if required

  For information on using custom or self-signed certificates, see Using Custom or Self-signed Certificates with Oracle E-Business Suite Mobile Apps, page 4-2.

Task 6: Performing Advanced Configurations

This section describes the following advanced configuration tasks for Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS:

- **Demilitarized Zone**

  Perform the following tasks if your mobile users need to access the Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS apps over the Internet:

  1. Setting Up Oracle E-Business Suite Environment in a DMZ Configuration, page 3-2

     If your mobile users need to access any of the three apps over the Internet, your Oracle E-Business Suite environment must be set up in a demilitarized zone (DMZ) configuration.

  2. Performing Mobile Apps Specific Setup Tasks for DMZ, page 3-2

     Additionally, you need to perform app-specific tasks to complete the advanced configurations for DMZ.

  For more information about DMZ, see Advanced Configurations for Demilitarized Zone, page 3-1.

- **Secure Communication with HTTPS**

  Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS can connect to a TLS-enabled Oracle E-Business Suite environment. This section describes the tasks required for enabling TLS in these apps.

  1. Setup Tasks for Enabling TLS in Oracle E-Business Suite, page 4-2

     Perform this task to ensure that your Oracle E-Business Suite environment is TLS enabled.

  2. Mobile Specific Setup Tasks for TLS Connections, page 4-2

     Additionally, you need to perform app-specific tasks to support the connection to a TLS-enabled Oracle E-Business Suite environment.

  For additional information about secure communication with HTTPS, see Advanced Configurations for Secure Communication with HTTPS, page 4-1.

- **Single Sign-On**

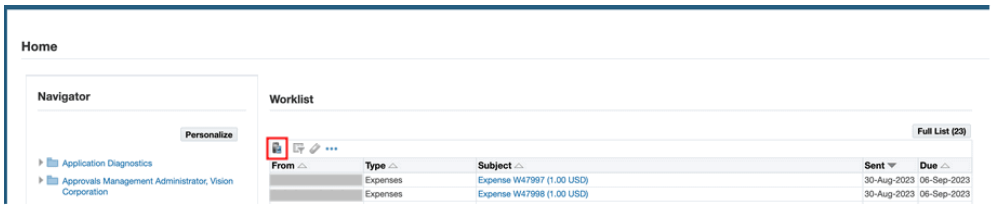
  If your Oracle E-Business Suite environment is configured with single sign-on (SSO), then SSO is available for the Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS apps through the SSO configuration of your Oracle E-Business Suite instance.

Perform the following tasks to ensure that Oracle E-Business Suite is configured with SSO:

1. Configuring Oracle E-Business Suite with Single Sign-On, page 5-2
2. Performing Additional Configurations in Oracle Access Manager, page 5-2
3. Accessing the Apps for Oracle E-Business Suite Configured with Oracle Access Manager, page 5-3

For example, in Oracle Approvals for EBS if Oracle E-Business Suite is configured for SSO, a user of the Approvals app with the SSO authentication type can directly access the app through a web page URL. If the Oracle E-Business Suite user is configured with the local authentication type, the user can access the app by clicking the Mobile icon above the Worklist table in the Oracle E-Business Suite Home page.

Oracle E-Business Suite Home Page with the Mobile Icon Highlighted



- **Enterprise Mobility Management Solutions**

  To support the integration with Enterprise Mobility Management (EMM) solutions, administrators need to configure these three apps as web link applications in EMM which allows the app users to access the app by tapping an icon on their devices. Note that EMM configuration has been tested on iOS devices for these three apps.

  For information about integration with EMM solutions, see Integrating Oracle E-Business Suite Mobile Apps with Enterprise Mobility Management Solutions, page 6-1.

Task 7: Enabling the Server Logging and REST Service Auditing Features

This section describes the following logging and auditing features that is applicable for Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS.

- Enabling Server Logging, page 7-2
- Enabling REST Service Auditing, page 7-3

> **Note:** Client logging and troubleshooting tips described later in the Diagnostics and Troubleshooting chapter of this guide are not applicable for these three apps.

For more information about logging and how to troubleshoot issues, see Diagnostics and Troubleshooting, page 7-1.

Setup Tasks for Oracle Maintenance for EBS

This section includes the following setup tasks for Oracle Maintenance for EBS:

1. Applying Server-Side Patches for Oracle Maintenance for EBS, page 2-14
2. Configuring the Mobile Apps on the Oracle E-Business Suite Server, page 2-18
3. Setting Up Mobile App Access to Responsibilities, page 2-35
4. Performing Additional Setup for Device Integration, page 2-37
5. Performing Additional App-Specific Setup, page 2-39
6. Communicating Mobile App Information to Users, page 2-40
7. Performing Advanced Configurations, page 2-41
8. Enabling the Logging and Diagnostics Features, page 2-42

Additionally, administrators can track the app usage and user installation through the Mobile Applications Manager UI page. See: Managing Usage Metrics for Oracle Maintenance for EBS, page 2-42.

Task 1: Applying Server-Side Patches for Oracle Maintenance for EBS

Perform the required tasks to apply prerequisite patches in the following sequence:

1. Performing Conditional Pre-Install Tasks, page 2-14
2. Applying Product Family Level Patches, page 2-15
3. Applying Conditional Post-Install Patches, page 2-16

Step 1: Performing Conditional Pre-Install Tasks

For Oracle Maintenance for EBS Only

Apply the corresponding consolidated product family patch and conditionally required patches if needed.

Note: In Oracle E-Business Suite Release 12.2, when you apply patches using the adop (AD Online Patching) utility, adop runs AutoConfig by default.

To support the "Apps SSO Login" authentication in Mobile Release 10.x, you must also apply required patches and perform additional setup tasks to enable the feature. See: Setup Tasks to Enable the Apps SSO Login Authentication Security, page 5-5.

Perform any additional conditionally required pre-install tasks from the following list for Oracle Maintenance for EBS only:

Conditional Pre-Install Tasks for Oracle Maintenance for EBS 10.x App

Oracle E-Business Suite Release or Mobile App Name	Requirement	Pre-Install Task
Oracle E-Business Suite Release 12.2 • Oracle Maintenance for EBS	Required only if you plan to implement Oracle Maintenance for EBS	Oracle Mobile Maintenance "Disconnected" feature uses the Oracle Mobile Field Service Multiplatform framework, which does not require Oracle Lite and consequently Oracle Lite should be uninstalled. If the "mobileadmin" schema exists, refer to My Oracle Support Knowledge Document 1564644.1, *Oracle Mobile Field Service Store and Forward Multiple Platforms Support*.

Step 2: Applying the Product Family Level Patches for Oracle Release 10.x Apps

Apply the server-side patches for Release 12.2 using either the Oracle E-Business Suite level consolidated patch or the individual product family patches, depending on your needs.

- **Apply the Oracle E-Business Suite level patch for Release 12.2**

  To simplify the patching efforts, the server-side product family patches are consolidated into a single Oracle E-Business Suite level patch for Release 12.2. This consolidated patch includes each product family patch for the corresponding mobile apps.

For example if you plan to use Oracle Approvals for EBS and Oracle Maintenance for EBS, instead of applying each product family patch for the supported approval types described earlier for Oracle Approvals for EBS and the Oracle Supply Chain Management product family patch for Oracle Maintenance for EBS, you can simply apply the higher level consolidated patch, Patch 35706735:12.2.0 to meet your needs.

- **Apply the relevant product family level patches for Release 12.2**

  If you only use certain product families, then apply the relevant individual product family level patches for your Oracle E-Business Suite mobile apps.

  For example, apply the Oracle Supply Chain Management product family patch listed in the following table for Oracle Maintenance for EBS:

Oracle Supply Chain Management Product Family Level Patch for Oracle Maintenance for EBS Release 10.x

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.2
Oracle Supply Chain Management (scm_pf)	• Oracle Maintenance for EBS	Patch 30144036:R12. SCM_PF.C: SCM -12.2 Consolidated Patch For Mobile Applications Foundation V9

Step 3: Applying Conditional Post-Install Patches

Apply additional conditionally required post-install patches from the following list for Oracle Maintenance for EBS:

Conditional Post-Install Patches for Oracle Maintenance for EBS Release 10.x

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 • Oracle E-Business Suite Mobile Release 10.0 Online Help	Required for Oracle E-Business Suite mobile apps, leveraging Oracle E-Business Suite Mobile Foundation Release 9.1, connected to Oracle E-Business Suite Release 12.2	• Release 12.2: Patch 35622500

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2	Required only if your Oracle E-Business Suite environment has the following patches applied: • Release 12.2 - Patch 27761509:12.2.0 (Oracle Applications Release 12.2 : Consolidated Patch for Data Removal Tool) **Note:** If your environment has the following Data Removal Tool consolidated patches applied instead, then the post-install tasks specified in the next column are not required: • Release 12.2 - Patch 29206195:12.2.0 (Oracle Applications Release 12.2 Data Removal Tool - One-off Consolidation - January 2020)	Perform the following steps in the specified order: • Release 12.2: 1. Apply Patch 28295762:R12.PER.C. 2. Apply Patch 28303904:R12.FND.C. 3. Recompile the data removal metadata by running the concurrent program "Recompile Metadata for Data Removal Tool", with the "Entity Type" parameter set to "ALL".
Oracle E-Business Suite Release 12.2 • Oracle Maintenance for EBS	Required if you connect to an Oracle E-Business Suite 12.2 instance with Oracle Maintenance for EBS	1. Apply the Mobile Maintenance Release 10 Consolidated Patch 34116139:R12.EAM.C. 2. If your instance is Release 12.2.10 or later, apply an additional Patch 34439382:R12.EAM.C.

Task 2: Configuring the Mobile Apps on the Oracle E-Business Suite Server

> **Note:** Information described in this section applies to Oracle Maintenance for EBS only. It does not apply to all other Oracle E-Business Suite Mobile Release 10.x apps.

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 Pages, page 2-18
- Enabling and Setting Up Multiple Mobile Apps Using a Script, page 2-30
- Validating the Configuration, page 2-33

> **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. If the configuration is changed after the initial setup is complete and loaded to a user's app, the updated parameters will be automatically downloaded to the app every five logins. See Directing Users to Obtain Connection Details and Download Updates from the Server, page 7-9.

Enabling a Mobile App Individually and Specifying the Configuration Through the UI Pages

To access Oracle E-Business Suite 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 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*.

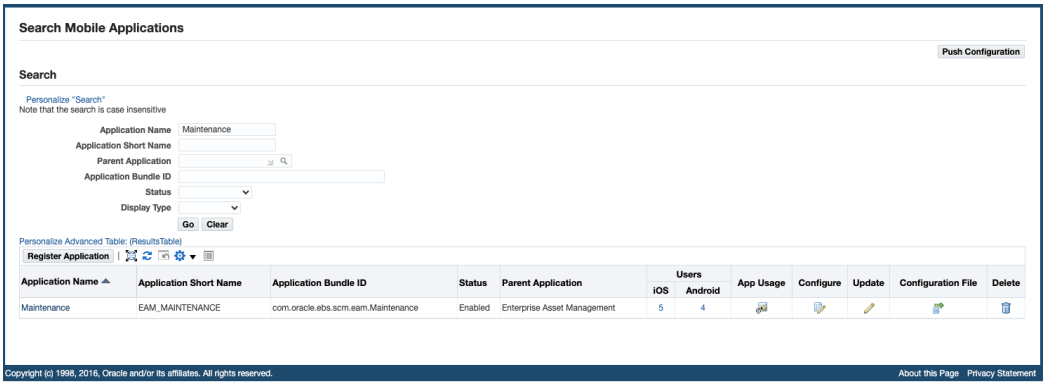
Users granted different roles can perform various tasks as described in the following table:

Privileges	Mobile Applications Administrator	Mobile Applications Developer
Search enterprise apps	Yes	Yes
Register enterprise apps	Yes	Yes
Configure enterprise apps	Yes	Yes
Update application definitions	Yes	Yes
Delete application definitions	Yes	Yes
View configuration files	Yes	Yes
View mobile app installation details	Yes	No
View mobile app usage metrics	Yes	No

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.

The Search Mobile Applications Page



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:

> **Important:** For Oracle E-Business Suite Mobile Release 10.x, push notifications is currently not available, although **Push Configuration** is present in the Search Mobile Applications page.

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

  See: Enabling and Configuring a Mobile App Individually, page 2-20.

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

  See: Viewing and Validating Your Mobile App Configuration, page 2-29.

- 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 2-29.

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.

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

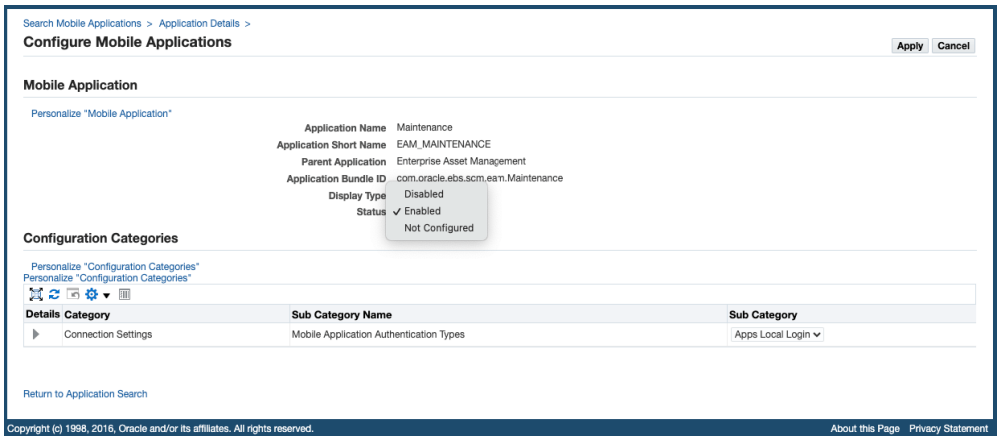
   - Enabled: This allows you to configure the app against Oracle E-Business Suite.

   - 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 Page to Enable a Mobile App



6. 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. See: Configurations for Local and SSO Login Types, page 2-23.

If you want to proceed with the default parameter values, skip the next step 7, and go to step 8.

7. 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, for the authentication type, 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 with the custom profile option name. For information on configuring parameters in the Configuration Parameters region, see:

   - Configuring Parameters for the Apps Local Login Authentication Type, page 2-24.

   - Configuring Parameters for the Apps SSO Login Authentication Type, page 2-26.

   Configuration parameters to be included in the configuration file depends on the selected authentication type in the Sub Category field. For example, if "Apps SSO Login" is selected for an app, the corresponding parameters of the "Apps SSO Login" authentication type are included in the configuration file.

   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.

8. Click the **Apply** button. This action saves the selected authentication type and relevant 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.

To validate the configuration, click the **Configuration File** icon from the search result table. See: Viewing and Validating Your Mobile App Configuration, page 2-29.

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.

Mobile apps may have configuration updates after the initial launch. 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 the Oracle E-Business Suite Mobile Release 10.x, app users can manually check if any new updates from the server are required in the app if necessary. See Directing Users to Obtain Connection Details and Initiate Server Updates, page 7-9.

Configurations for Local and SSO Login Types

Oracle E-Business Suite mobile apps support "Apps Local Login" and "Apps SSO Login" authentication types that are displayed under the "Connection Settings" category in the Configuration Categories region.

Authentication type is preselected or defined for an app during the app registration. Each authentication type is associated with a set of configuration parameters required to set for an app. When you enable or configure an app, the preselected type (either "Apps Local Login" or "Apps SSO Login") is displayed in the Sub Category field in the Configuration Categories region. You can override the selected type if needed by selecting a different value from the Sub Category drop-down list. After the change, the parameters corresponding to the selected authentication type will be loaded and displayed in the Configuration Parameters region.

> **Important:** Make sure Oracle E-Business Suite mobile apps work with "Apps Local Login" before you change it to the "Apps SSO Login" authentication type. If an app initially connects to Oracle E-Business Suite through "Apps Local Login", and later its authentication type is changed to "Apps SSO Login", the app users should initiate the manual update to refresh the configuration. This is performed by tapping **Settings** from the mobile app navigation menu, then tapping **Connection Details**, and then tapping the **Sync** icon.

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

- **Apps Local Login (default) - for local authentication**

  Apps Local Login is the default type for a mobile app to authenticate mobile users locally against the Oracle E-Business Suite server. When this type is selected for a mobile app, the user passwords must be stored in Oracle E-Business Suite.

  > **Note:** If user passwords are externally stored and are not accessible which indicates that your instance is single sign-on enabled, configure your app with the "Apps SSO Login" authentication type instead.

  When "Apps Local Login" is selected as the type, three associated parameters, that is, Session Timeout, Idle Timeout, and Service Endpoint, are displayed in the

Configuration Parameters region. You can override the default Apps Local Login type if needed by selecting a desired authentication type, such as "Apps SSO Login", in the Sub Category field. After the change, the parameters associated with the new type "Apps SSO Login" are displayed in the Configuration Parameters region.

For information on setting configuration parameters for the Apps Local Login authentication type, see Configuring Parameters for the Apps Local Login Authentication Type, page 2-24.

- **Apps SSO Login - for remote authentication**

  When the "Apps SSO Login" type is selected for a mobile app, the mobile app users are not authenticated against Oracle E-Business Suite, but 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.

  To use "Apps SSO Login" as the authentication type, ensure the following:

  - 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: Advanced Configurations for Single Sign-On, page 5-1.

  For information on setting configuration parameters for the Apps SSO Login authentication type, see Configuring Parameters for the Apps SSO Login Authentication Type, page 2-26.

  For troubleshooting information, see: Troubleshooting Tips on Configuring Apps with Apps SSO Login Authentication Type, page 7-21.

Configuring Parameters for the Apps Local Login Authentication Type

If the default "Apps Local Login" type is used as the authentication type to authenticate users locally, update the following parameter values:

Configuration Categories Region with the "Apps Local Login" Parameters

Configuration Categories

Details	Category	Sub Category Name	Sub Category
	Connection Settings	Mobile Application Authentication Types	Apps Local Login

Configuration Parameters

Name	Code	Defaults			Data Type	Override Type	Override Value
		Type	Value	Current Profile Value			
Idle Timeout	APPS_MOBILE_IDLE_TIMEOUT	Constant	7200		Number	Constant	7200
Session Timeout	APPS_MOBILE_SESSION_TIMEOUT	Constant	28800		Number	Constant	28800
Service Endpoint	APPS_MOBILE_AGENT	Profile Option	APPS_FRAMEWORK_AGENT	https:// .com:	URL	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. 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.

  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 value of the Service Endpoint

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 parameter value 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 parameter, 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 Apps SSO Login Authentication Type

Important: Before configuring apps with "Apps SSO Login", make sure

your apps work with "Apps Local Login" first. If an app initially connects to Oracle E-Business Suite through "Apps Local Login", and later its authentication type is changed to "Apps SSO Login", the app users should initiate the manual update to refresh the configuration. This is performed by tapping **Settings** from the mobile app navigation menu, then tapping **Connection Details**, and then tapping the **Sync** icon.

- Select "Apps SSO Login" as the authentication type if you want to delegate authentication to Oracle Access Manager based on a protected Login URL.
- You must apply required patches and perform additional setup tasks including common tasks and mobile specific setup tasks to enable this feature.

  See: Advanced Configurations for Single Sign-On (SSO), page 5-1.

Configuration Categories Region with the "Apps SSO Login" Parameters

Configuration Categories

Details	Category	Sub Category Name	Sub Category
	Connection Settings	Mobile Application Authentication Types	Apps SSO Login

Configuration Parameters

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

If "Apps SSO Login" is selected as the authentication type to authenticate users remotely, update the following parameter values:

- **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 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.

- 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 that indicates the user has logged in successfully.

  To determine the correct value for this parameter, navigate to the configured SSO Login URL in a web browser session and then submit valid login credentials. The URL that you are re-directed to after successful login is your SSO Login Success URL.

  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.

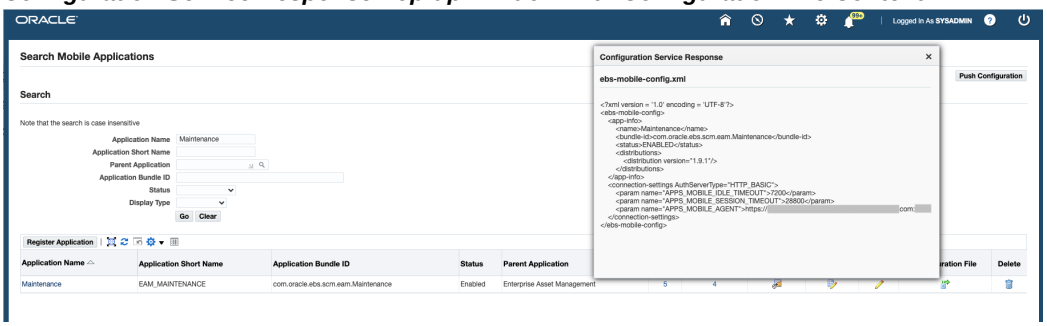
  The usage of this parameter is the same as the Service Endpoint parameter described earlier for the HTTP Basic authentication type. See: Service Endpoint (APPS_MOBILE_AGENT), page 2-25.

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.

Configuration Service Response Pop-up Window with Configuration File Content



Additionally, you can validate the configuration by accessing the configuration service URL through a web browser. See Validating the Configuration, page 2-33.

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 "Maintenance" link to view the Application, Distributions, and Configuration regions in the Application Details page for Oracle Maintenance for EBS.

- **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 2-20.

- **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.

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` and the script `EBSMblConfigApps.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

file:

> **Note:** The script supports the selection of the Sub Category (`<sub-category>`) attribute that indicates either of the following authentication types to be used by a mobile app.
>
> - HTTP_BASIC: The type corresponds to "Apps Local Login" (display name) from the Mobile Applications Manager UI pages.
> - WEB_SSO: The type corresponds to "Apps SSO Login" (display name) from the Mobile Applications Manager UI pages.

```
<applications configureAll="N">
  <application configure="N">
   <app-info>
    <name>Maintenance</name>
    <app-short-name>EAM_MAINTENANCE</app-short-name>
    <bundle-id>com.oracle.ebs.scm.eam.Maintenance</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 (Apps Local Login) is set to `Y`.

   Note: If the `select` attribute for the "WEB_SSO" type (Apps SSO Login) 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 Maintenance).
   [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 Region with the "Apps Local Login" Parameters

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

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<applications configureAll="N">
  <application configure="Y">
   <app-info>
    <name>Maintenance</name>
    <app-short-name>EAM_MAINTENANCE</app-short-name>
    <bundle-id>com.oracle.ebs.scm.eam.Maintenance</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`, run 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 2-33 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:** 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 2-18.

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=mConfig&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 D-1.

   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.

      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>Maintenance</name>
    <bundle-id>com.oracle.ebs.scm.eam.Maintenance</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>
```

      Please note that 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.

3. Make sure the setup is valid at this point and ensure that your app works with the "Apps Local Login" authentication type before proceeding to any advanced configurations.

   1. In the Mobile Applications Manager UI pages, configure the mobile app with authentication type as "Apps Local Login".

      See: Configuring Parameters for the Apps Local Login Authentication Type, page 2-24.

   2. Log in to the mobile app as a user whose password is stored in Oracle E-Business Suite, such as `sysadmin`.

      You should be able to successfully log in and view the mobile app pages.

Task 3: Setting Up Mobile App Access to Responsibilities

Oracle Maintenance for EBS uses 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.

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.

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 Mobile App Access Roles, page B-1.

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*.

Task 4: Performing Additional Setup for Device Integration

This section describes additional setup steps for Oracle Maintenance for EBS when it integrates with maps on the mobile devices and barcodes. It includes the following topics:

1. Setting Up Maps, page 2-38

2. Support for Barcodes, page 2-38

Setting Up Maps

Oracle Maintenance for EBS integrates with maps through 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 Maintenance for EBS presents the asset information and its geographical location in an Oracle map.

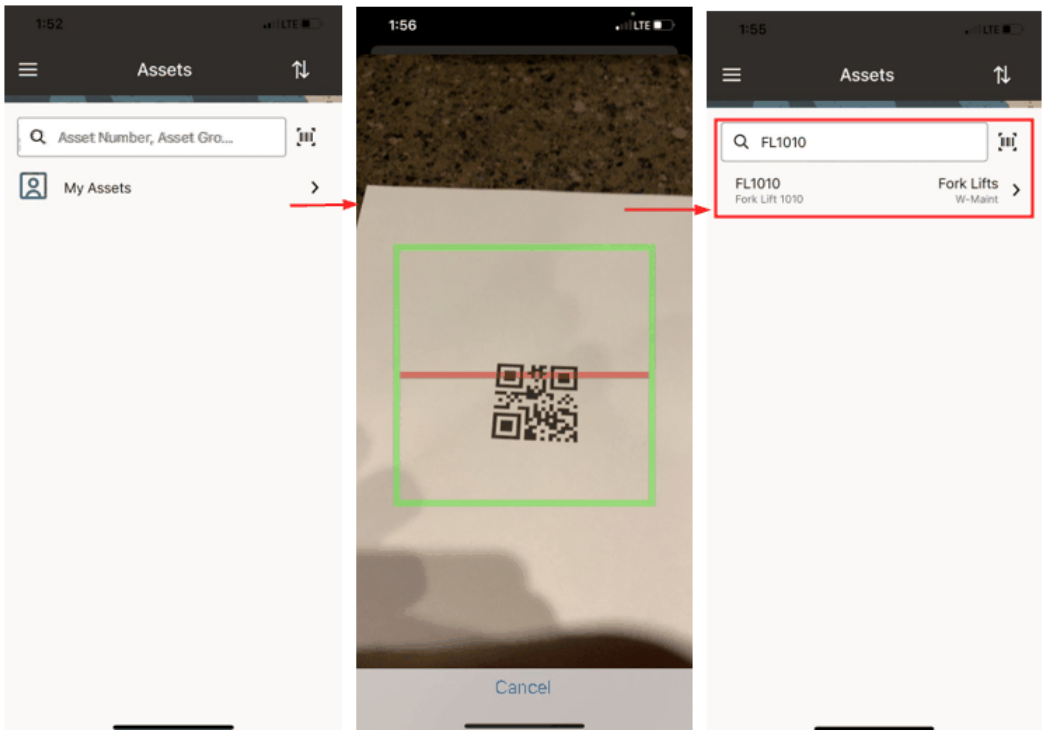
Support for Barcodes

Some Oracle E-Business Suite mobile apps provide support through the Cordova plug-in 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 Maintenance for EBS uses barcode scanning to capture data for assets, work orders, and work requests.

Data Captured and Shown in the Mobile Page Using Barcode Scanning



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

Task 5: Performing Additional App-Specific Setup

Perform the additional app-specific implementation steps described in the My Oracle

Support Knowledge Document 1923702.1, *Oracle Mobile Maintenance for Oracle E-Business Suite Release Notes*.

Task 6: Communicating Mobile App Information to Users

After you have completed the setup tasks for your app, provide the following information to the users who will install the app from the Apple App Store or Google Play Store:

- Name of the app

  For the name of the mobile app to download or access through a URL, see the *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 information, refer to the *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>`

  Be aware of 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, Validating the Configuration, page 2-33.

  > **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 host name 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 host name. Refer to:
  >
  > - *Using Load-Balancers with Oracle E-Business Suite Release 12.2*, My Oracle Support Knowledge Document 1375686.1
  > - *Using Load-Balancers with Oracle E-Business Suite Release 12.0 and 12.1*, My Oracle Support Knowledge Document 380489.1

  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.

> **Additional Information:** The latest server-side patches must be applied to enable new features and fixes that require those patches. Oracle recommends that you define a plan to maintain the mobile server side on a regular basis that is aligned with the Oracle E-Business Suite mobile releases, if you are using the standard apps installed from public app stores.

Task 7: Performing Advanced Configurations

This section describes the following advanced configuration tasks for Oracle Maintenance for EBS:

- **Demilitarized Zone**

  Perform the following tasks if your mobile users need to access the Oracle Maintenance for EBS app over the Internet:

  1. Setting Up Oracle E-Business Suite Environment in a DMZ Configuration, page 3-4
  2. Performing Mobile Apps Specific Setup Tasks for DMZ, page 3-4

  For more information about DMZ, see Advanced Configurations for Demilitarized Zone, page 3-1.

- **Secure Communication with HTTPS**

  Oracle Maintenance for EBS supports the connection to a TLS-enabled Oracle E-Business Suite environment as long as the server uses public or commercial-CA issued TLS certificates. Self-signed or custom certificates are currently not supported.

  For additional information about secure communication with HTTPS, see Advanced Configurations for Secure Communication with HTTPS, page 4-1.

- **Single Sign-On**

  Oracle Maintenance for EBS is not configured for SSO by default even if you have integrated Oracle E-Business Suite with Oracle Access Manager for single sign-on. However, you can configure SSO for this app using the setup tasks described in this section.

  1. Configuring Oracle E-Business Suite with Single Sign-On, page 5-4

2. Setup Tasks to Enable the Apps SSO Login Authentication Security, page 5-5
3. Testing the Setup for the Apps SSO Login Authentication Security, page 5-9
4. Setting the Mobile App Connection to Use Apps SSO Login, page 5-10

For additional information about single sign-on, see Advanced Configurations for Single Sign-On, page 5-1.

- **Enterprise Mobility Management Solutions**

  To support the integration with Enterprise Mobility Management (EMM) solutions, administrators need to perform required setup tasks to preconfigure the Server URL that Oracle Maintenance for EBS will use to connect to Oracle E-Business Suite. Once the setup tasks are complete, the app users no longer need to enter this URL manually after launching an app installed from an EMM's app catalog. Note that this EMM configuration has been tested on iOS devices for Oracle Maintenance for EBS.

  For information about integration with EMM solutions and the setup tasks to preconfigure the Server URL for mobile apps, see Integrating Oracle E-Business Suite Mobile Apps with Enterprise Mobility Management Solutions, page 6-1.

Task 8: Enabling the Logging and Diagnostics Features

Oracle Maintenance for EBS uses the logging and diagnostics features described later in the Diagnostics and Troubleshooting chapter. Specifically, it includes the following logging and diagnostics features for Oracle Maintenance for EBS.

- Enabling Server Logging, page 7-4
- Enabling REST Service Auditing, page 7-4
- Enabling Client Logging, page 7-4
- Troubleshooting Tips on the Mobile Client, page 7-9
- Troubleshooting Tips on the Oracle E-Business Suite Server, page 7-19

For more information about logging and diagnostics, see Diagnostics and Troubleshooting, page 7-1.

Managing Usage Metrics for Oracle Maintenance for EBS

Administrators of the Oracle Maintenance for EBS app can track the app usage and user installation through the Mobile Applications Manager UI page. This section describes how to perform various administrative tasks to understand how Oracle Maintenance for EBS is installed and used.

- Viewing Mobile App Installation and Usage Metrics, page 2-43
- Purging Mobile App Usage Information, page 2-46

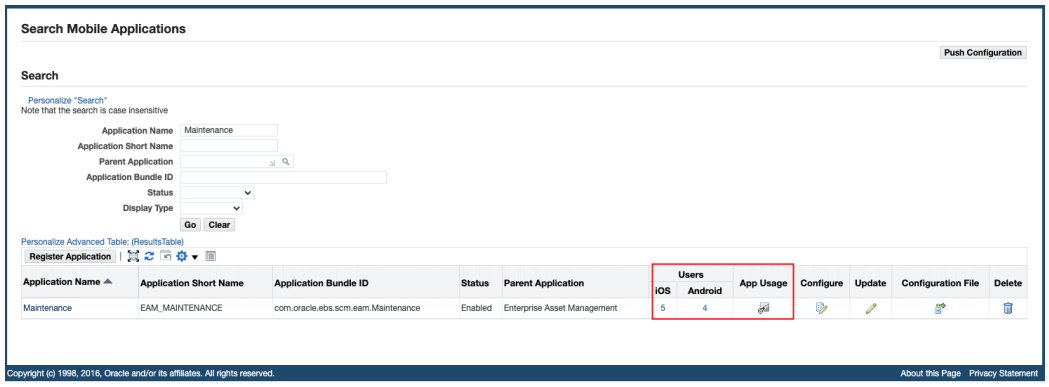
Viewing Mobile App Installation and Usage Metrics

Once users start using the Oracle Maintenance for EBS app, it is highly beneficial for administrators to gather statistics on the app. These statistics include platform-specific user installations and usage frequencies over a period of time for this app. Users who have the Mobile Applications Administrator role can obtain this essential information through the Mobile Applications Manager UI pages and provide needed support for their users more efficiently.

> **Note:** These features are available only for users who have the Mobile Applications Administrator role. Users who have the Mobile Applications Developer role cannot find the Users and App Usage columns from the search result table.

To view user installations and usage metrics for Oracle Maintenance for EBS app, select the **Mobile Applications Manager** responsibility and choose the **Applications** link from the navigator. The Search Mobile Applications page appears.

Search Mobile Applications Page with Mobile App Installation and Usage Information Highlighted



Perform the following tasks to view user installation and app usage information:

- Click the number of users link for iOS or Android to view the installation information for a desired app.

  See: Viewing Your Mobile App Installation Details, page 2-44.

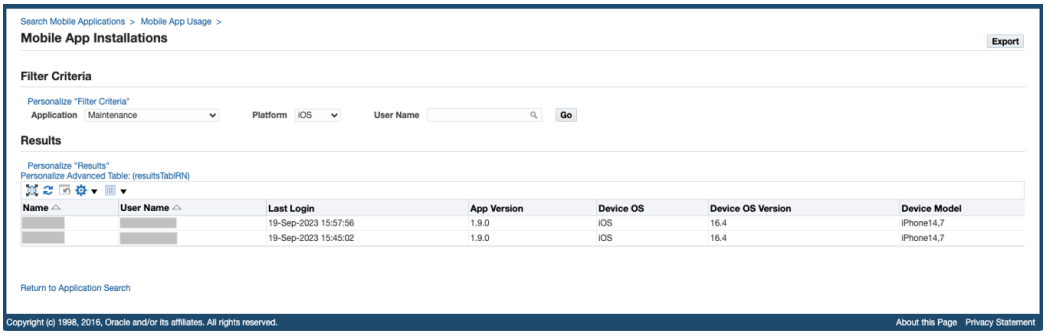
- Click the **App Usage** icon to view the mobile usage information.

  See: Viewing Your Mobile App Usage, page 2-45.

Viewing Your Mobile App Installation Details

To view user installation information for a specific app (such as "Maintenance), after locating the app in the Search Mobile Applications page, click the number of users link for iOS or Android in the Users column from the search result table. The Mobile App Installations page appears with the installation details for your selected app, such as "Maintenance".

Mobile App Installations Page



The installation details include the name of the users who have installed the app (such as "Maintenance"), last login date and time, app version, device or platform information (either iOS or Android, depending on your selection from the Users column in the search result table), device OS version, and device model information (such as iPhone, iPad, or Android).

In the Filter Criteria region, you can further refine the result by modifying the following fields for the same app or obtain the information for a different app.

- **Application:** This field is automatically displayed with your selected app name from the search result table.

  If you want to view the user installations for a different app, select a desired app from the Application drop-down menu.

- **Platform:** Either iOS or Android is selected automatically based on your selection from the search result table in the Search Mobile Applications page.

  You can select a different value, including "iOS", "Android", or "All", to view the platform-specific user installations for the selected app.

  If "All" is selected, then the user installation information for both iOS and Android are displayed.

- **User Name**: Specify a desired user name if you want to view the installation for that user.

You can click **Export** to export all the data to an Excel spreadsheet if desired.

Click the **Return to Application Search** link to return back to the Search Mobile

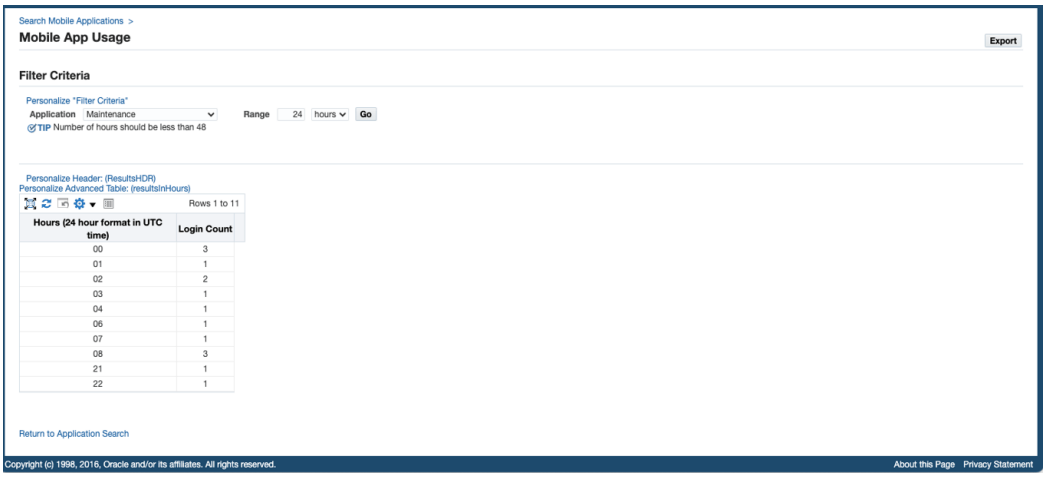
Applications page.

For information on viewing app usage information, see Viewing Your Mobile App Usage, page 2-45.

Viewing Your Mobile App Usage

To view the usage pattern for an app in terms of number of logins in the last few days or hours, click the **App Usage** icon from the search result table in the Search Mobile Applications page. The Mobile App Usage page appears for your desired app.

Mobile App Usage Page



In the Filter Criteria region, enter the following information to view the app usage information:

- **Application:** This field is automatically displayed with your desired app name.

  Select a different name if you want to view the usage information for another app.

- **Range:** Enter a numeric number in the text box as the time range, and select a desired range unit, such as "hours" or "days". For example, obtain the number of logins for an app within the last 47 hours or the last 24 days.

  Note that if "hours" is selected as the range unit, the number you specify in the text box should be less than "48" hours. Otherwise, an error message appears.

After you modify the filter criteria and click **Go**, the app usage information is displayed in a table with the app login date and login count.

To export the data to an Excel spreadsheet, click **Export**.

Click the **Return to Application Search** link to return back to the Search Mobile Applications page.

You can purge the app usage data if needed, see Purging Mobile App Usage Information, page 2-46.

For information on viewing user installations for an app, see Viewing Your Mobile App Installation Details, page 2-44.

Purging Mobile App Usage Information

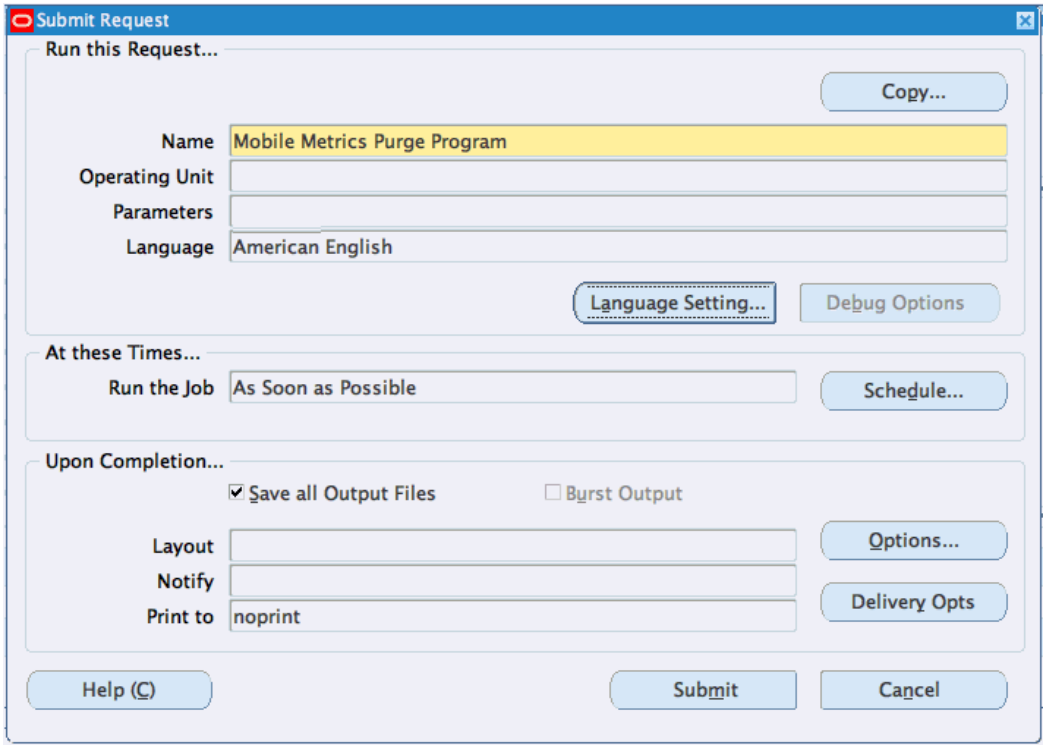
You can purge app usage data stored in the database that has been collected for a period of time by running a concurrent program called "Mobile Metrics Purge Program".

> **Important:** The "Mobile Metrics Purge Program" only purges the mobile app usage data. The data for user installations will not be purged.

To access this concurrent program, log in to Oracle E-Business Suite as a user who has the **System Administrator** responsibility. Select **Concurrent**, and then **Requests** from the navigation menu.

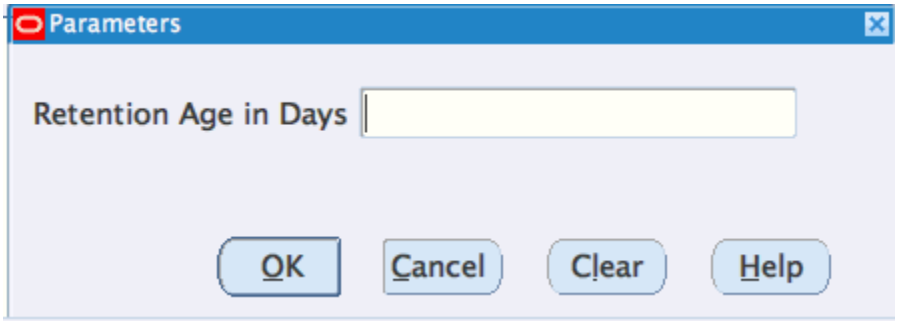
In the Submit Request window, select "Mobile Metrics Purge Program" as the Name from the drop-down list.

Submit Request Window with "Mobile Metrics Purge Program" Concurrent Program Selected



After you select "Mobile Metrics Purge Program" as the concurrent program name, the Parameters window appears. Specify a number of days in the Retention Age in Days field to indicate the desired days that you intend to retain the data. All the app usage data that is older than the specified days will be purged.

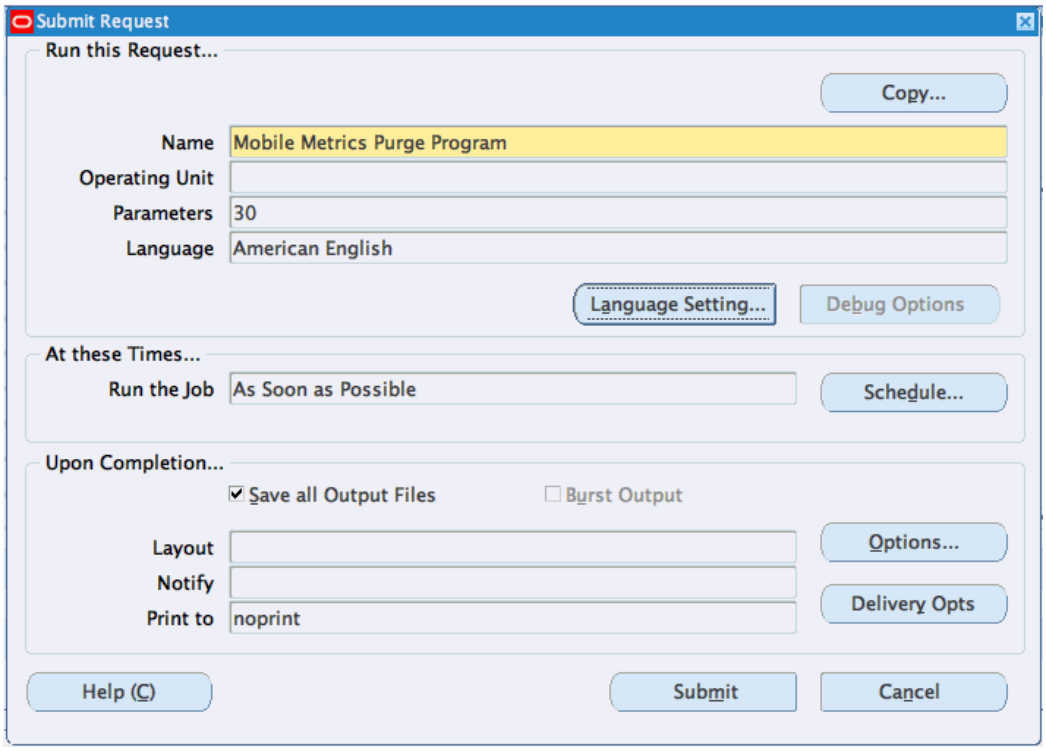
Parameters Window



For example, if you desire to keep the data within the last 30 days, then enter "30" in the Retention Age in Days field. The app usage data stored in the database older than the last 30 days will be removed, but the data for user installations remains intact and will not be purged.

After you specify the information in the Parameters window and click **OK**, the specified number of days, such as "30", is automatically displayed in the Parameters field.

Submit Request Window with Required Parameters



Click **Submit** to submit your concurrent request and start the process of purging the app usage data based on the specified parameter.

Setup Tasks for Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA)

This section includes the following setup tasks for Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA):

1. Applying Server-Side Patches for Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA), page 2-49
2. Support for Barcodes, page 2-51
3. Performing Additional App-Specific Setup, page 2-52
4. Communicating Mobile App Information to Users, page 2-52
5. Performing Advanced Configurations, page 2-53

Task 1: Applying Server-Side Patches for Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA)

Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA) are the only Release 10.x apps available for both Oracle E-Business Suite Release 12.1.3 and Release 12.2. If your Oracle E-Business Suite instance is on Release 12.1.3, apply the patches relevant to Release 12.1.3.

For Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA) Release 10.x

> **Note:** Oracle Field Service for EBS and Oracle Mobile SCM for EBS do not require any product family patches.

Apply any additional conditionally required patches from the following list for the Oracle Field Service for EBS and Oracle Mobile SCM for EBS apps:

Conditional Patches for Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA) Release 10.x

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 and 12.1.3	Required only if your Oracle E-Business Suite environment has the following patches applied: • Release 12.2 - Patch 27761509:12.2.0 (Oracle Applications Release 12.2 : Consolidated Patch for Data Removal Tool) • Release 12.1.3 - Patch 27822242:12.1.0 (Oracle Applications Release 12.1 : Consolidated Patch for Data Removal Tool) **Note:** If your environment has the following Data Removal Tool consolidated patches applied instead, then the post-install tasks specified in the next column are not required: • Release 12.2 - Patch 29206195:12.2.0 (Oracle Applications Release 12.2 Data Removal Tool - One-off Consolidation - January 2020) • Release 12.1.3 - Patch 29206188:12.1.0 (Oracle Applications Release 12.1 Data Removal Tool - One-off Consolidation -	Perform the following steps in the specified order: • Release 12.2: 1. Apply Patch 28295762:R12.PER.C. 2. Apply Patch 28303904:R12.FND.C. 3. Recompile the data removal metadata by running the concurrent program "Recompile Metadata for Data Removal Tool", with the "Entity Type" parameter set to "ALL". • Release 12.1.3: 1. Apply Patch 28295762:R12.PER.B. 2. Apply Patch 28303904:R12.FND.B. 3. Recompile the data removal metadata by running the concurrent program "Recompile Metadata for Data Removal Tool", with the "Entity Type"

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
	January 2020)	parameter set to "ALL".
Oracle E-Business Suite Release 12.2 and Release 12.1.3 • Oracle Field Service for EBS	Required if you connect to an Oracle E-Business Suite 12.2 or 12.1.3 instance with Oracle Field Service for EBS	• Release 12.2: Patch 34985819:R12.CSM.C • Release 12.1.3: Patch 34985819:R12.CSM.B
Oracle E-Business Suite Release 12.2 and Release 12.1.3 • Oracle Mobile SCM for EBS (MSCA)	Required if you connect to an Oracle E-Business Suite 12.2 or 12.1.3 instance with Oracle Mobile SCM for EBS (MSCA)	• Release 12.2: Patch 34986700:R12.MWA.C • Release 12.1.3: Patch 35042131:R12.MWA.B

Task 2: Support for Barcodes

Some Oracle E-Business Suite mobile apps provide support through the Cordova plug-in 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.

Supported Barcode Types

Oracle Mobile SCM for EBS (MSCA) supports the following barcode types:

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

- Code 128
- Code 39

Task 3: Performing Additional App-Specific Setup

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

- Oracle Field Service for EBS (see Document 2188514.1)
- Oracle Mobile SCM for EBS (MSCA) (see Document 2108155.1)

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.

Task 4: Communicating Mobile App Information to Users

After you have completed the setup tasks for your app, provide the following information to the users who will install the app from the Apple App Store or Google Play Store, or access the app through a web page URL:

- Name of the app

  For the name of the mobile app to download or access through a URL, see the *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*, My Oracle Support Knowledge Document 1641772.1.

- Where to locate the app

  For the download information, refer to the *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 Field Service for EBS only) Oracle E-Business Suite server URL in the following format: `http(s)://<hostname>:<port>`

  > **Note:** User can select the Lock icon next to the server URL if it is `https`.

  If at any point the server URL is changed, then you must inform the app users of the new URL. The app users must log out and synchronize the app again with the

new server URL.

> **Additional Information:** The latest server-side patches must be applied to enable new features and fixes that require those patches. Oracle recommends that you define a plan to maintain the mobile server side on a regular basis that is aligned with the Oracle E-Business Suite mobile releases, if you are using the standard apps installed from public app stores.

Task 5: Performing Advanced Configurations

This section describes the following advanced configuration tasks for Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA):

- **Demilitarized Zone**

  Oracle Field Service for EBS and Oracle Mobile SCM for EBS currently do not support for accessing these two apps over the Internet.

  The information about advanced configurations for demilitarized zone described later in this book does not apply to these two apps.

- **Secure Communication with HTTPS**

  For information on configuring TLS port and adding custom certificates to this app, see Document 2108155.1, *Oracle Mobile Supply Chain Applications for Oracle E-Business Suite Release Notes*.

  The information about advanced configurations for secure communication with HTTPS described later in this book does not apply to these two apps.

- **Single Sign-On**

  Oracle Field Service for EBS and Oracle Mobile SCM for EBS support single sign-on with their own app-specific configuration processes.

  The information about advanced configurations for SSO described later in this book does not apply to these two apps.

- **Enterprise Mobility Management Solutions**

  Oracle Field Service for EBS and Oracle Mobile SCM for EBS currently do not support this feature.

  The information about integrating mobile apps with Enterprise Mobility Management solutions described later in this book does not apply to these two apps.

3

Advanced Configurations for Demilitarized Zone

Overview

If your mobile users need to access Oracle E-Business Suite mobile apps over the Internet, your Oracle E-Business Suite environment must be set up in a demilitarized zone (DMZ) configuration.

To set up Oracle E-Business Suite mobile apps in a DMZ configuration, ensure that you complete the required tasks for your app:

> **Note:** Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA) currently do not support for accessing these two apps over the Internet. The information described in this chapter does not apply to these two apps.

- Setup Tasks for Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS, page 3-1
- Setup Tasks for Oracle Maintenance for EBS, page 3-4

Setup Tasks for Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS

To set up Oracle E-Business Suite mobile apps in a DMZ configuration, ensure that you complete the following required tasks:

1. Setting Up Oracle E-Business Suite Environment in a DMZ Configuration, page 3-2
2. Performing Mobile Apps Specific Setup Tasks for DMZ, page 3-2

Step 1: Setting Up Oracle E-Business Suite Environment in a DMZ Configuration

Before performing mobile app specific setup tasks, you need to ensure Oracle E-Business Suite is in a DMZ configuration.

For DMZ configuration instructions, see My Oracle Support Knowledge Document 1375670.1, *Oracle E-Business Suite Release 12.2 Configuration in a DMZ*.

> **Note:** For any responsibility to which you have assigned the mobile app access role, as described in Setting Up Mobile App Access to Responsibilities (for Oracle Self-Service HR for EBS and Oracle Timecards for EBS), page 2-8, 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 My Oracle Support Knowledge Document 1375670.1, Section 4.4 Update List of Responsibilities.

Step 2: Performing Mobile Apps Specific Setup Tasks for DMZ

Perform the following tasks to complete the app-specific setup for Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS:

- Web Entry Point Configuration in oacore WLS Properties, page 3-2
- URL Firewall Configuration, page 3-3

Web Entry Point Configuration in oacore WLS Properties

For these three Oracle JET-based apps (Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS) in an Oracle E-Business Suite environment with a DMZ configuration, the web entry points should be defined in `oracle.apps.fnd.sso.WebEntries` in `$INST_TOP/appl/admin/oacore_wls.properties`.

By default, the property is commented in `$INST_TOP/appl/admin/oacore_wls.properties`. Uncomment the property and provide comma-separated Oracle E-Business Suite URLs as:

```
oracle.apps.fnd.sso.WebEntries=http(s)://<EBS Internal Host>:
<port>,http(s)://<EBS External Host>:<port>
```

Use the following steps to add multiple web entry points to this property:

1. Copy the original `oacore_wls_properties.tmp` file from `<FND_TOP>/admin/template` to `<FND_TOP>/admin/template/custom`, if the customized template file does not already exist. Create the custom directory if it does not exist.

2. Modify `oacore_wls_properties.tmp` in the custom directory. Uncomment the property `oracle.apps.fnd.sso.WebEntries` and provide comma-separated EBS URLs as:

   ```
   oracle.apps.fnd.sso.WebEntries=http(s)://<EBS Internal Host:
   port>,http(s)://<EBS External Host:port>
   ```

3. Run AutoConfig in the application tier and restart the servers.

To ensure the change is preserved through patching and server restarts, follow the instructions in the "Customizing AutoConfig-Managed Configurations" section of the Technical Configuration chapter in *Oracle E-Business Suite Setup Guide*.

URL Firewall Configuration

If your Oracle E-Business Suite is configured for DMZ with URL Firewall enabled, then to access browser-based mobile apps over the Internet, add the following URL patterns to the allowlist in the URL Firewall configuration file (`url_fw.conf`).

> **Note:** Note that `url_fw.conf` will be generated on all the application tiers by the AutoConfig utility.

In order to preserve the configuration, perform the following steps to customize the template file:

1. Copy the original `url_fw_conf_FMW.tmp` file from `<FND_TOP>/admin/template` to `<FND_TOP>/admin/template/custom`, if the customized template file does not already exist. Create the custom directory if it does not exist.

2. Modify `url_fw_conf_FMW.tmp` in the custom directory. Perform the following steps to modify the existing rule and add new rules in the following URL patterns in STATIC block to make it accessible in the external web tier:

   1. Check for the existing rule: `RewriteRule ^/OA_HTML/.*\.(gif|jpg|jpeg|bmp|png)$ - [L]`

   2. Comment it and modify the existing rule to include `ico` and `svg` extensions as:

      ```
      #RewriteRule ^/OA_HTML/.*\.(gif|jpg|jpeg|bmp|png)$ - [L]
      RewriteRule ^/OA_HTML/.*\.(gif|jpg|jpeg|bmp|png|ico|svg)$ -
      [L]
      ```

   3. Add new rules:

```
RewriteRule ^/OA_HTML/.*\.(ttf|woff|woff2)$ - [L]
RewriteRule ^/OA_HTML/.*\.(webmanifest)$ - [L]
```

3. Run AutoConfig in the application tier and restart the servers.

For more information, refer to the "Customizing AutoConfig-Managed Configurations" section of the Technical Configuration chapter in *Oracle E-Business Suite Setup Guide*.

Setup Tasks for Oracle Maintenance for EBS

Perform the following tasks to complete the setup for Oracle Maintenance for EBS in a DMZ configuration:

1. Setting Up Oracle E-Business Suite Environment in a DMZ Configuration, page 3-4

2. Performing Mobile Apps Specific Setup Tasks for DMZ, page 3-4

Step 1: Setting Up Oracle E-Business Suite Environment in a DMZ Configuration

Before performing mobile app specific setup tasks, you need to ensure Oracle E-Business Suite is in a DMZ configuration.

For DMZ configuration instructions, see My Oracle Support Knowledge Document 1375670.1, *Oracle E-Business Suite Release 12.2 Configuration in a DMZ*.

> **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 My Oracle Support Knowledge Document 1375670.1, Section 4.4 Update List of Responsibilities.

Step 2: Performing Mobile Apps Specific Setup Tasks for DMZ

> **Important:** For Oracle Maintenance for EBS, before setting up your

mobile app with any of the advanced configurations, ensure basic mobile app configuration is performed and validated. See: Validating the Configuration, page 2-33.

Additionally, before connecting the mobile app using DMZ configuration, ensure that the app works with Service Endpoint (APPS_MOBILE_AGENT) set to an internal server of Oracle E-Business Suite. For information on the Service Endpoint (APPS_MOBILE_AGENT) parameters, see Configuring Parameters for the Apps Local Login Authentication Type, page 2-24.

For Oracle Maintenance for EBS, when setting up the configuration file for this app, ensure that the value of the Service Endpoint parameter 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 Pages, page 2-18.

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 Service Endpoint parameter to set it to the external web entry point.

4

Advanced Configurations for Secure Communication with HTTPS

Overview

Support for secure communication with HTTPS is available in some of the Oracle E-Business Suite 10.x mobile apps for certificates from commercial Certificate Authority (CA) vendors, as well as custom or self-signed certificates.

To enable TLS in Oracle E-Business Suite mobile apps, ensure that you complete the following tasks for your app:

> **Note:** The information described in this chapter does not apply to Oracle Mobile SCM for EBS (MSCA) and Oracle Field Service for EBS.
>
> For information on configuring TLS port and adding custom certificates to Oracle Mobile SCM for EBS, see Document 2108155.1, *Oracle Mobile Supply Chain Applications for Oracle E-Business Suite Release Notes*.

- Setup Tasks for Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS, page 4-1
- Setup Tasks for Oracle Maintenance for EBS, page 4-3

Setup Tasks for Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS

Perform the following tasks to enable TLS for your app:

1. Setup Tasks for Enabling TLS in Oracle E-Business Suite, page 4-2
2. Mobile Specific Setup Tasks for TLS Connections, page 4-2

Step 1: Setup Tasks for Enabling TLS in Oracle E-Business Suite

The setup tasks described in this section are common tasks for enabling TLS in Oracle E-Business Suite. These tasks serve as prerequisites for configuring Oracle E-Business Suite mobile apps for TLS connections. Oracle E-Business Suite mobile 10.x apps support TLS 1.2 only and TLS 1.2 with backward compatibility (recommended). Before performing setup tasks for mobile apps, ensure your Oracle E-Business Suite environment is TLS enabled.

For information on enabling TLS 1.2 only and TLS 1.2 with backward compatibility in Oracle E-Business Suite, see My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.

Step 2: Mobile Specific Setup Tasks for TLS Connections

Once your Oracle E-Business Suite is TLS enabled, perform the following additional app-specific setup task to ensure successful TLS connections for your app.

- Using Custom or Self-signed Certificates with Oracle E-Business Suite Mobile Apps, page 4-2

Using Custom or Self-signed Certificates with Oracle E-Business Suite Mobile Apps

For Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS, mobile users of these three apps can dynamically add custom CA or self-signed server certificates to the apps accessible through web page URLs for TLS connections to Oracle E-Business Suite.

Importing Certificates Dynamically for Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS

Perform the following steps to import certificates after accessing the app through a web page URL:

1. Save the custom CA or self-signed certificate file in binary format (DER), for example, `<ca-cert-filename>.cer`.

   > **Note:** Use keytool or an appropriate tool to view the contents of the certificate file `<ca-cert-filename>.cer` and confirm that the file is the correct self-signed or custom CA certificate for the Oracle E-Business Suite environment. If the correct certificate for the Oracle E-Business Suite environment is not imported to the app, then the app user cannot connect to the Oracle E-Business Suite server.

2. Change the extension of the certificate file to `<ca-cert-filename>.servercert`.

3. Upload the certificate file to an internal server where your mobile users can access from their mobile devices.

4. Ask your mobile users to access your desired Oracle E-Business Suite mobile apps.

5. Open the certificate file from the internal server using the mobile device's web browser.
   - For iOS devices, use Safari web browser to open the certificate file.
   - For Android devices, use Chrome web browser to open the certificate file.

6. When prompted, select the Oracle E-Business Suite mobile app to open the certificate file with so that it is imported into that app.

7. Restart the app and connect to Oracle E-Business Suite.

8. Repeat the tasks from step 5 to step 7 for each Oracle E-Business Suite mobile app that should connect to that server.

Setup Tasks for Oracle Maintenance for EBS

Oracle Maintenance for EBS supports TLS connection only when your Oracle E-Business Suite server certificates are public or commercial-CA issued TLS certificates. There is no app-specific setup task required for this app.

> **Note:** In this Release 10.x, Oracle Maintenance for EBS does not support custom or self-signed certificates.

The only setup task is to ensure that your Oracle E-Business Suite environment is TLS enabled. See: Setup Tasks for Enabling TLS in Oracle E-Business Suite, page 4-3.

> **Important:** Before setting up your mobile app with any of the advanced configurations, ensure basic mobile app configuration is performed and validated. See: Validating the Configuration, page 2-33.

Setup Tasks for Enabling TLS in Oracle E-Business Suite

This task is to ensure that your Oracle E-Business Suite environment is TLS enabled.

Note that Oracle E-Business Suite mobile 10.x apps support TLS 1.2 only and TLS 1.2 with backward compatibility (recommended).

For information on enabling TLS 1.2 only and TLS 1.2 with backward compatibility in Oracle E-Business Suite, see My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.

No App-Specific Setup Tasks

Once your Oracle E-Business Suite is TLS enabled, you can have TLS connection as long as the server uses public or commercial-CA issued TLS certificates. There is no additional setup task for Oracle Maintenance for EBS.

5

Advanced Configurations for Single Sign-On

Overview

Single sign-on (SSO) is available in some of the 10.x apps when authenticating a user from a mobile device. However, some apps do not currently support this feature even if you have integrated Oracle E-Business Suite with Oracle Access Manager for single sign-on. In this situation if the mobile device has multiple Oracle E-Business Suite mobile apps, then it is required to re-authenticate the user by providing user login credentials when the user navigates from one Oracle E-Business Suite mobile app to another on the same mobile device.

> **Note:** Oracle Maintenance for EBS is not configured for SSO by default. However, you can configure SSO for this app using the setup tasks described in this chapter. SSO is available for the Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS apps through the SSO configuration of your Oracle E-Business Suite instance.

When configuring Oracle E-Business Suite mobile apps with the "Apps SSO Login" authentication type, ensure that you complete the required tasks for your app:

- Setup Tasks for Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS, page 5-2
- Setup Tasks for Oracle Maintenance for EBS, page 5-4

> **Note:** Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA) support single sign-on with their own app-specific configuration processes. Therefore, the setup tasks described in this chapter do not apply to these two apps.

Setup Tasks for Oracle Approvals for EBS, Oracle Timecards for EBS, and Oracle Self-Service HR for EBS

Single sign-on is available for the Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS apps through the SSO configuration of your Oracle E-Business Suite instance. Therefore, you need to ensure that your Oracle E-Business Suite environment is configured for SSO first. You may need to perform additional configuration if Oracle E-Business Suite is configured with Oracle Access Manager 12c.

1. Configuring Oracle E-Business Suite with Single Sign-On, page 5-2
2. Performing Additional Configurations in Oracle Access Manager, page 5-2
3. Accessing the Apps for Oracle E-Business Suite Configured with Oracle Access Manager, page 5-3

Step 1: Configuring Oracle E-Business Suite with Single Sign-On

If your Oracle E-Business Suite is integrated with Oracle Access Manager (OAM), to authenticate users remotely with single sign-on, ensure that you complete the following prerequisites:

- Oracle E-Business Suite mobile apps delegate user authentication to Oracle Access Manager in the same way as supported for Oracle E-Business Suite browser-based applications. In this situation, mobile users are authenticated remotely against an external OAM server. Refer to My Oracle Support Knowledge Document 1388152.1, *Overview of Single Sign-On Integration Options for Oracle E-Business Suite*.
- For both browser-based applications and mobile apps, Oracle E-Business Suite certifies the form-based challenge method only.

Step 2: Performing Additional Configurations in Oracle Access Manager

If Oracle E-Business Suite is configured with Oracle Access Manager 12c, then perform the following steps on the OAM 12c instance:

1. Use the following commands to create a new '`esapi`' directory in `$DOMAIN_HOME/config/fmwconfig`:

   ```
   cd $DOMAIN_HOME/config/fmwconfig
   mkdir esapi
   cd esapi
   ```

2. Obtain the `ESAPI.properties` and `validation.properties` files from the release notes for your app:
   - Oracle Approvals for EBS: Section 5.1 in My Oracle Knowledge Document

1642423.1, *Oracle Mobile Approvals for Oracle E-Business Suite Release Notes*

- Oracle Self-Service HR for EBS: Section 5.1 in My Oracle Knowledge Document 2105189.1, *Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite Release Notes*

- Oracle Timecards for EBS: Section 5.1 in My Oracle Knowledge Document 1669224.1, *Oracle Mobile Timecards for Oracle E-Business Suite Release Notes*

3. Copy the `ESAPI.properties` and `validation.properties` files to `$DOMAIN_HOME/config/fmwconfig/esapi`.

4. Edit the `$DOMAIN_HOME/bin/setDomainEnv.sh` file, to add a new property (this is a reference to the directory where your new esapi files are located):

```
EXTRA_JAVA_PROPERTIES="-Doracle.oam.esapi.resources=<Enter the full
file path here to the esapi directory> ${EXTRA_JAVA_PROPERTIES}"
export EXTRA_JAVA_PROPERTIES
```

5. Restart OAM using the following commands:

```
Shutdown oam_policy_mgr1 then oam_server1
Startup oam_policy_mgr1 then oam_server1
```

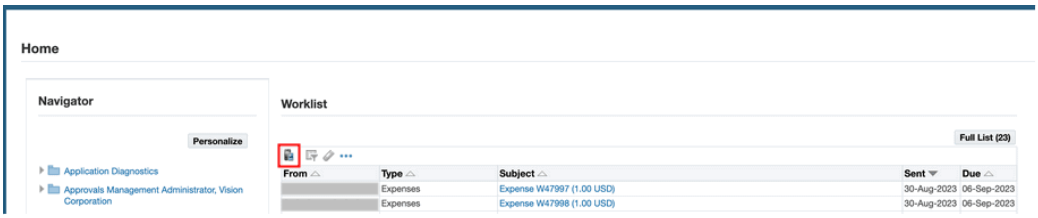
Step 3: Accessing the Apps for Oracle E-Business Suite Configured with Oracle Access Manager

When your Oracle E-Business Suite instance is configured for SSO, SSO is available for the Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS apps through the SSO configuration of your Oracle E-Business Suite instance.

Accessing the App from the Oracle E-Business Suite Home Page

For example, in Oracle Approvals for EBS if Oracle E-Business Suite is configured for SSO, a user of the Approvals app with the SSO authentication type can directly access the app through a web page URL. If the Oracle E-Business Suite user is configured with the local authentication type, the user can access the app by clicking the Mobile icon above the Worklist table in the Oracle E-Business Suite Home page.

Oracle E-Business Suite Home Page with the Mobile Icon Highlighted



Setup Tasks for Oracle Maintenance for EBS

This section describes the following setup tasks for Oracle Maintenance for EBS:

> **Important:** Before setting up your mobile app with any of the advanced configurations, ensure basic mobile app configuration is performed and validated. See: Validating the Configuration, page 2-33.

1. Configuring Oracle E-Business Suite with Single Sign-On, page 5-4
2. Setup Tasks to Enable the Apps SSO Login Authentication Security, page 5-5
3. Testing the Setup for the Apps SSO Login Authentication Security, page 5-9
4. Setting the Mobile App Connection to Use Apps SSO Login, page 5-10

Additionally, see Troubleshooting Tips on Configuring Apps With the Apps SSO Login Authentication Type, page 7-21.

Step 1: Configuring Oracle E-Business Suite with Single Sign-On

Before setting up app-specific tasks, you must ensure that your Oracle E-Business Suite is configured with SSO.

- Oracle E-Business Suite mobile apps delegate user authentication to Oracle Access Manager in the same way as supported for Oracle E-Business Suite browser-based applications. In this situation, mobile users are authenticated remotely against an external Oracle Access Manager (OAM) server. Refer to My Oracle Support Knowledge Document 1388152.1, *Overview of Single Sign-On Integration Options for Oracle E-Business Suite*.

- 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, integration with multi-factor authentication, 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.

  Note that 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.

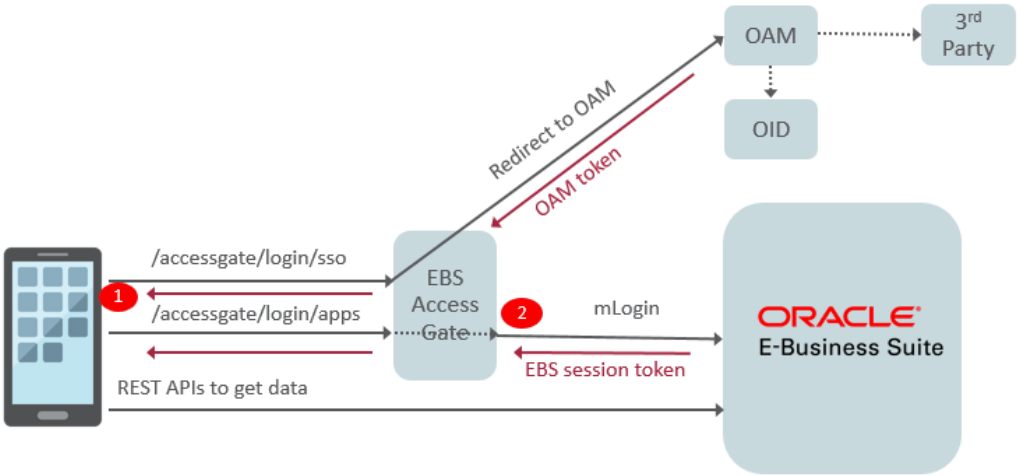
- If you encounter issues during the configuration of Oracle Access Manager with alternative authentication mechanisms, you may contact Oracle Support for diagnosing issues related to Oracle Access Manager.

Step 2: Setup Tasks to Enable the Apps SSO Login Authentication Security

To better understand the setup tasks specifically for mobile apps with Apps SSO Login, the following diagram illustrates the high level process flow when authenticating Oracle E-Business Suite mobile users using single sign-on in the case of TLS configuration:

> **Note:** Oracle E-Business Suite mobile apps work with any single sign-on configurations for Oracle E-Business Suite.

High Level Process Flow for Apps SSO Login Authentication with TLS Configuration



In this diagram, there are two different REST invocation points (client vs server) which require you to import certificates into appropriate truststores:

- **Scenario 1: TLS client invocation from a mobile app**

  This scenario invokes the following two endpoints:

  - Oracle E-Business Suite AccessGate

    A mobile user attempts to log in to an app through the value configured in the "SSO Login URL" (`login/sso`) parameter. The user is directed to Oracle E-Business Suite AccessGate (EAG) which is protected by the Oracle Access

Manager (OAM) server for user authentication. When the user enters the login credentials in the Sign In screen, OAM verifies the credentials against user directory. If the user is successfully authenticated, OAM returns a unique OAM access token to Oracle E-Business Suite AccessGate for further identification verification, as described in Scenario 2.

- Oracle E-Business Suite REST endpoint on the server

  Once the user is successfully authenticated to access Oracle E-Business Suite from the mobile app, the mobile app uses "EBS Session Service" (`login/apps`) to create a valid Oracle E-Business Suite session. The user then performs desired actions through Oracle E-Business Suite REST APIs to fetch Oracle E-Business Suite data for the app.

- **Scenario 2: TLS client invocation from Oracle E-Business Suite AccessGate to invoke Oracle E-Business Suite application tier**

  Oracle E-Business Suite AccessGate is a Java Enterprise Edition application that maps a single sign-on user to an Oracle E-Business Suite user. Once picking up the access token from OAM, Oracle E-Business Suite AccessGate verifies the user identification against the Oracle E-Business Suite database. If the verification is successful meaning that this is a valid Oracle E-Business Suite user, an Oracle E-Business Suite session token is returned. The session token that points to the user session will be passed to HTTP headers of all subsequent service calls for the user authentication.

  To successfully invoke the Oracle E-Business Suite application tier from Oracle E-Business Suite AccessGate as described in this scenario, custom CA or self-signed certificates used in Oracle E-Business Suite application tier should be imported to the Oracle E-Business Suite AccessGate truststore.

Based on the above high level invocation diagram, to enable the Apps SSO Login authentication for Oracle E-Business Suite mobile apps, you need to perform the following setup tasks to ensure Oracle E-Business Suite AccessGate is deployed properly and its required certificates are imported for a TLS-based environment.

For Oracle E-Business Suite Release 12.2

1. Download Oracle E-Business Suite AccessGate for your Oracle E-Business Suite release. For download and patch information, refer to My Oracle Support Knowledge Document 2202932.1, *Using the Latest Oracle E-Business Suite AccessGate for Single Sign-On Integration with Oracle Access Manager*.

2. Deploy Oracle E-Business Suite AccessGate by following the setup and configuration instructions described in one of the following My Oracle Support Knowledge Documents based on your Oracle Access Manager release:

   - For Oracle Access Manager 12c, see Document 2339348.1, *Integrating Oracle E-Business Suite Release 12.2 with Oracle Access Manager 12c using Oracle E-Business*

Suite AccessGate.

If you have already deployed an earlier version of Oracle E-Business Suite AccessGate, refer to Section 8.2 Oracle E-Business Suite AccessGate Upgrade, My Oracle Support Knowledge Document 2339348.1.

- For Oracle Access Manager 11g, see 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 Oracle E-Business Suite AccessGate, refer to Section 8.2 Oracle E-Business Suite AccessGate Upgrade, My Oracle Support Knowledge Document 1576425.1.

3. After Oracle E-Business Suite AccessGate 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 or later, then you need to re-register Oracle E-Business Suite and include an additional parameter `-policyUpdate=yes`. These actions add the newly-defined public resource `/accessgate/logout/sso` to your configuration.

   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. Additionally, add a 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. **Tasks for Enabling the feature on a TLS-based Oracle E-Business Suite environment**

   > **Note:** Oracle E-Business Suite mobile 10.x apps support TLS 1.2 only and TLS 1.2 with backward compatibility (recommended). For information on enabling TLS 1.2 only and TLS 1.2 with backward compatibility, see My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.

If your Oracle E-Business Suite instance is TLS enabled and Oracle Access Manager (OAM) configured, perform the following tasks:

1. Import the root-CA certificates from the OHS wallet into the truststore of the OAEA managed server where Oracle E-Business Suite AccessGate 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 certificates 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 in My Oracle Support Knowledge Document 2143101.1, *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 TLS in the Oracle E-Business Suite context file. 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 TLS. 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 TLS". Then choose the **OK** button.
   8. Run AutoConfig and restart all the application tier services. For more

information about AutoConfig, see: Technical Configuration, *Oracle E-Business Suite Setup Guide*.

Step 3: Testing the Setup for the Apps SSO Login Authentication Security

To successfully log in to an Oracle E-Business Suite mobile app configured with the Apps SSO Login security, you need to ensure successful HTTP(s) communication from the Oracle E-Business Suite AccessGate managed server to the Oracle E-Business Suite server.

1. Validate the communication by running the following WGET command from the managed server where Oracle E-Business Suite AccessGate is deployed:

   ```
   wget -d http(s)://<ebs_host>:<ebs_port>/OA_HTML/RF.jsp?
   function_id=mLogin
   ```

2. If this fails, verify the following tasks and ensure they are in place:

   1. The root-CA, intermediate, and server certificates from the Oracle HTTP Server (OHS) wallet and Oracle TLS CA certificates are imported into the truststore of the managed server where Oracle E-Business Suite AccessGate is deployed.

   2. Network port from the current managed server to the Oracle E-Business Suite web entry is NOT restricted.

   3. For an Oracle E-Business Suite environment configured in a DMZ configuration, if Oracle E-Business Suite AccessGate is deployed on your intranet server with firewalls and the Oracle E-Business Suite web entry point is a URL over the Internet, then make sure this Oracle E-Business Suite URL is NOT DIS_ALLOWED from the intranet server.

      Although this Oracle E-Business Suite web entry point URL can be your enterprise's own URL, this could still restrict access from your intranet server. If this network restriction policy cannot be exempted to ALLOW access from the intranet managed server where Oracle E-Business Suite AccessGate is deployed to the Oracle E-Business Suite web entry point over the Internet, then you can try the following option of configuring proxy host and port for the HTTP communication as a workaround.

      1. Restart with the following `-D` System settings on the managed server where Oracle E-Business Suite AccessGate is deployed.

      2. Use the `-D` settings for setting up proxy host and port through the System properties in JAVA_OPTIONS:

         - For the HTTP protocol communication:

```
-Dhttp.proxyHost
-Dhttp.proxyPort
```

- For the HTTPS protocol communication:

```
-Dhttps.protocols (TLSv1.1/SSL version)
-Dhttps.proxyHost
-Dhttps.proxyPort
```

For more information, refer to Oracle Networking Properties (https://docs.oracle.com/javase/7/docs/api/java/net/doc-files/net-properties.html), Oracle Java Documentation.

Step 4: Setting the Mobile App Connection to Use Apps SSO Login

After completing all the setup tasks on the server, you now need to configure the mobile client and set the mobile app connection to use Apps SSO Login authentication type.

See: Configuring Parameters for the Apps SSO Login Authentication Type, page 2-26.

6

Integrating Oracle E-Business Suite Mobile Apps with Enterprise Mobility Management Solutions

Overview

Oracle is an Independent Software Vendor (ISV) member of the AppConfig Community. The AppConfig Community provides tools and best practices to secure, configure, deploy, and manage mobile enterprise apps. In principle, Oracle E-Business Suite mobile apps are compatible with AppConfig-based Enterprise Mobility Management (EMM) integration, using native frameworks that are made available through operating systems (iOS and Android).

> **Note:** For Oracle E-Business Suite Mobile Release 10.x, this feature has been tested on iOS devices for Oracle Maintenance for EBS, Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS.

This chapter provides guidance on integrating Oracle E-Business Suite mobile apps with EMM solutions based on AppConfig standard. It also includes some setup tasks that administrators can manage Oracle E-Business Suite mobile app configuration when the apps are deployed with an EMM solution.

Oracle E-Business Suite Mobile Apps with Enterprise Mobility Management Solutions

Compatibility of Oracle E-Business Suite Mobile Apps with AppConfig EMM Providers

Oracle E-Business Suite mobile apps are expected to work with any EMM provider that supports common AppConfig standards provided by operating system vendors. Oracle does not explicitly certify permutations of Oracle E-Business Suite mobile app releases with given EMM providers and their releases. Oracle may test selected Oracle E-Business Suite mobile apps with selected AppConfig-compliant products, including VMware AirWatch. Oracle does not conduct comprehensive tests between all available Oracle E-Business Suite mobile app releases and all AppConfig-compliant products.

Support

Oracle Support does not have access to third-party EMM AppConfig products and is unable to reproduce or investigate AppConfig compatibility issues directly. Oracle Support will ask customers to validate if the reported issue reproduces without third-party EMM integration in order to determine if the issue is specific to the third-party EMM solution. Issues with AppConfig-based configurations should be first reported to the affected EMM provider.

Setup Tasks for Deploying Mobile Apps with Enterprise Mobility Management Solutions

Users can install Oracle E-Business Suite mobile apps from an Enterprise Mobility Management (EMM) solution's app catalog. To connect to Oracle E-Business Suite, users need to enter the Oracle E-Business Suite server URL after the initial launch of an app from an EMM console that the app is deployed. To simplify the deployment process for the app users, administrators can preconfigure the server URL in an EMM console. App users no longer need to enter this URL manually after launching an app from an EMM's app catalog.

EMM configuration is available for the following standard Oracle E-Business Suite mobile apps, either installed from the Apple App Store or Google Play Store or available through web page URLs:

- Installed from Apple App Store or Google Play Store - Oracle Maintenance for EBS
- Available through a URL - Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS

  Configure these three apps as web link applications in EMM which allows users to access the apps by tapping an icon on their devices.

Setup Tasks for Oracle Maintenance for EBS Only

To preconfigure the server URL for Oracle Maintenance for EBS, administrators need to configure the following String type properties in an EMM console to simplify the app deployment for users:

> **Note:** This feature has been tested on iOS devices. To leverage this feature on Android devices, it is required to register your EMM provider with Google Play.

- Server_URL

  This is the Oracle E-Business Suite server URL that an app should connect to by default. If a valid Oracle E-Business Suite server URL is entered in this property, the app users will not be prompted to enter the server URL when the app is launched for the first time.

  Ensure that the mobile app is already "Enabled" in the Mobile Applications Manager UI pages. For information on enabling an app, see Enabling a Mobile App Individually and Specifying the Configuration Through the UI Pages, page 2-18.

- Server_URL_Allow_Change

  If a default Oracle E-Business Suite server URL is entered in the Server_URL property, you need to explicitly indicate whether the app users can change the URL in the app. By default, users are not allowed to change. However, set it to "Y" only if you want to allow the app users to change the default URL.

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:

> **Note:** The logging and diagnostics information described in this chapter does not apply to Oracle Field Service for EBS and Oracle Mobile SCM for EBS (MSCA).

Enabling Logging for Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS

Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS use the server logging and REST service auditing features to troubleshoot or diagnostic issues if occur during the service invocation while using the apps:

> **Note:** Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS do not use the client logging feature.
>
> The troubleshooting tips described in later in this chapter does not

apply to these three apps.

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 D: Mobile App Module Names, page C-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. Run the search to retrieve and download the desired server logs.

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 `fnd.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.

Enabling Logging and Diagnostics for Oracle Maintenance for EBS

Oracle Maintenance for EBS uses the server logging, client logging, and REST auditing features to help troubleshoot any issues if occur.

- Enabling Server Logging, page 7-4
- Enabling REST Service Auditing, page 7-4
- Enabling Client Logging, page 7-4

Additionally, this section includes the following troubleshooting information on potential problem symptoms and corresponding solutions.

- Troubleshooting Tips on the Mobile Client, page 7-9
- Troubleshooting Tips on the Oracle E-Business Suite Server, page 7-19

Enabling Server Logging

Oracle Maintenance for EBS uses the same server logging feature, described earlier for Oracle Approvals for EBS, Oracle Self-Service HR for EBS, and Oracle Timecards for EBS.

If a user of the Oracle Maintenance for EBS app reports a problem, an administrator can set the following 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)

For more information on how to enable server logging, see Enabling Server Logging, page 7-2.

Enabling REST Service Auditing

Similar to enabling REST service auditing information explained earlier, Oracle Maintenance for EBS needs to enable the auditing feature for REST service request and response payloads during the service invocation.

For more information on how to enable REST service auditing, see Enabling REST Service Auditing, page 7-3.

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)

  - Set this profile option to your Application Bundle Id `com.oracle.ebs.scm.eam.Maintenance`.

    For information on Application Bundle Id for each mobile app, see Appendix C: Application Definition Metadata, page D-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.

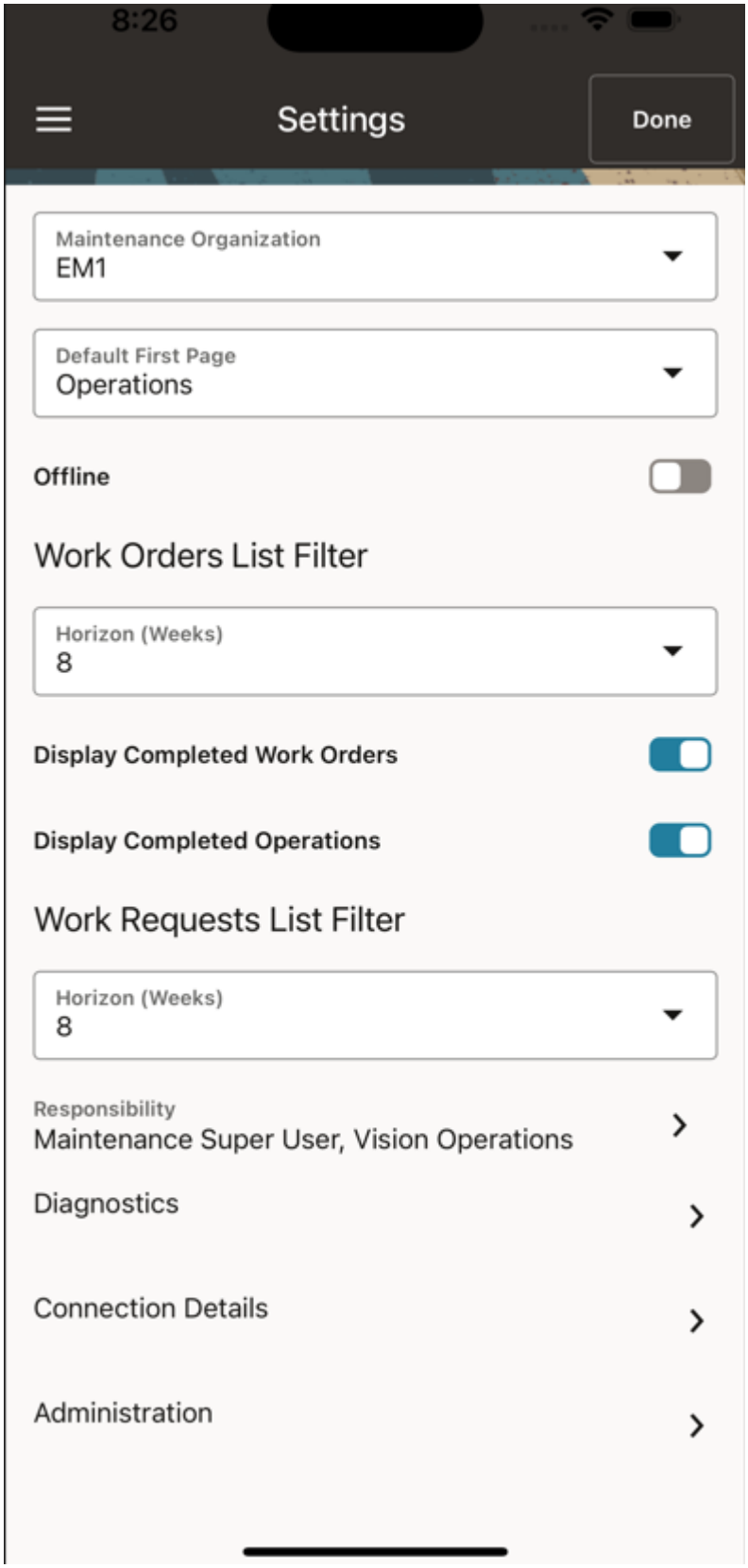
7. Retrieve the mobile client log file uploaded based on profile options set in step 4.

Uploading Client Logs to the Oracle E-Business Suite Server

If mobile app users can access to the app, direct the 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**.

On iOS: Settings Screen



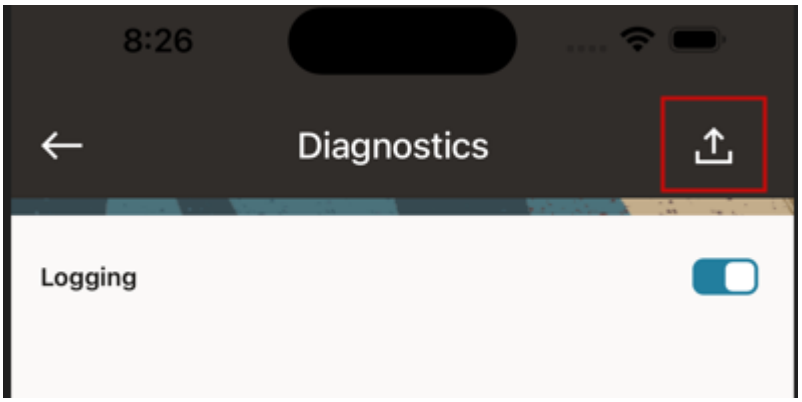
In the Diagnostics screen, enable the client logging feature by turning on the **Logging** option.

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.

On iOS: Diagnostics Screen with the Upload Icon Highlighted



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 your Application Bundle Id `com.oracle.ebs.scm.eam.Maintenance` as the Module name.

     For information on Application Bundle Id for each mobile app, see Appendix C: Application Definition Metadata, page D-1.

Please note that if the FND: Diagnostics profile option is enabled for a user, the complete error stack from the service invocation failure appears. Otherwise, only a simple error message is shown instead.

Retrieving Client Logs Directly From Android Mobile Devices

If mobile app users are unable to access or log in to the app, the users will not be able to upload the logs to the server from the mobile client. In this situation, direct the Android users to retrieve client logs directly from their mobile devices instead.

Note: The option of retrieving client logs directly from iOS devices is not available.

1. Use a file browser app on Android. For example, My Files, ES File Explorer.
2. Look for files that start with the app name. For example, `Maintenance.txt`, `Maintenance_bak.txt`.
3. Attach these files to an email through your preferred email app and upload to Oracle Support.

Troubleshooting Tips

This section includes the following troubleshooting information on potential problem symptoms and corresponding solutions.

- Troubleshooting Tips on the Mobile Client, page 7-9
- Troubleshooting Tips on the Oracle E-Business Suite Server, page 7-19

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 D-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 F-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 Download Updates from the Server, page 7-9
- Troubleshooting Tips for Oracle E-Business Suite Mobile Apps, page 7-13

Directing Users to Obtain Connection Details and Download Updates from the Server

When 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.

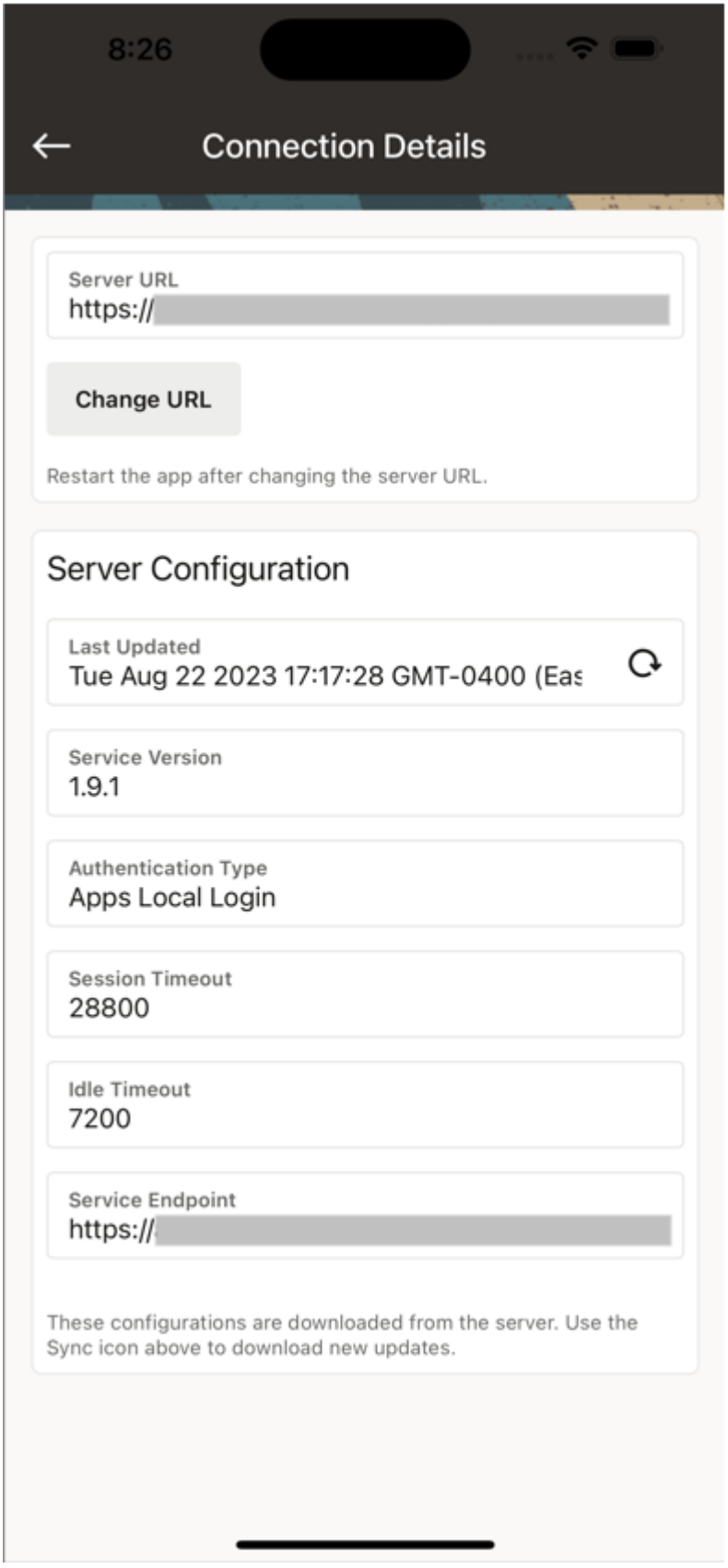
2. The Connection Details screen displays the server URL field and the Server Configuration region.

   - **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.

     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, as shown on the left. 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.

On iOS: Connection Details Screen with the "Change URL" Button



Note: Administrators can preconfigure the server URL and also determine if users can change the default URL value. If the server URL is preconfigured and users are not allowed to change the value, then **Change URL** will not be displayed. Instead, "Your administrator has configured the app to connect to this server URL. You cannot change this setting." message appears, as shown on the right.

For information on preconfiguring server URL, see Setup Tasks for Deploying Mobile Apps with Enterprise Mobility Management Solutions, page 6-2.

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.
  - **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.
  - **Authentication Type:** The selected authentication type is displayed.
  - **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.

3. Direct users to check if any new updates from the server are required for the app.

   Oracle E-Business Suite mobile apps automatically download the mobile app configuration updates from the Oracle E-Business Suite server. Users no longer need to initiate a download manually within an app. Instead, each app periodically checks for updates (once every five times the app is restarted) and downloads them to synchronize with the configuration details defined on the Oracle E-Business Suite

server. However, if required, users can still initiate the manual update by tapping the **Sync** icon as in the previous releases.

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 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

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 TLS certificate is untrusted and cannot be recognized by the mobile app, the following error message may appear: `"Unable to connect to the Oracle E-Business Suite server. Please enter a valid server URL."`	Ensure that your mobile app can perform a successful TLS handshake with the Oracle E-Business Suite TLS endpoint. 1. Validate that the JDK 8 client can connect to the Oracle E-Business Suite TLS endpoint. 2. Validate that the Oracle E-Business Suite TLS endpoint presents the complete certificate chain.
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 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.

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 or set up correctly during the 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, as described in Validating the Configuration, page 2-33. 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. **Note:** When an app user is authenticated, the `mLogin` REST service creates an Oracle E-Business Suite session for that user along with an XML response with authentication token (cookie) which uniquely identifies that session. To secure each user session, a profile option "FND: Authn Service Token Scope (`FND_AUTHN_SRVC_TOKEN_SCOPE`)" is introduced in the January 2023 Critical Patch Update with the default value "Header Only" at the Site level. This default value sets the ICX cookie only in the

Issue	Tip
	response header of the `mLogin` REST service, and will not return the cookie details in the response payload. If you have custom code that calls the `mLogin` REST service and requires the cookie details in the response payload, then you can optionally change the value to "Header and Body". In this case, the mLogin service sets the ICX cookie in the header and also returns the cookie name and value in the payload.

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 by locating the servlet in the `$OA_HTML/WEB-INF/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 Section 4.2: Implementing AutoConfig Customizations, My Oracle Support Knowledge 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.

Issue	Tip
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.
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.
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 Server-Side Patches for Oracle Maintenance for EBS, page 2-14 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 2-18.

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.
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.`	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 2-18.

Troubleshooting Tips on the Oracle E-Business Suite Server

This section describes the troubleshooting tips on the Oracle E-Business Suite server. It includes the following topics:

- Troubleshooting Tips on the Oracle E-Business Suite Server, page 7-19
- Troubleshooting Tips on Configuring Apps With the Apps SSO Login Authentication Type, page 7-21

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
If administrators preconfigure Server URL in an Enterprise Mobility Management (EMM) console through the Server_URL property or in **`ebs.properties`** when EMM is not used, after an app user launches the app, the following error may appear: `Unable to connect to the Oracle E-Business Suite server. The server URL may be invalid.`	To resolve this issue, perform the following steps to verify the preconfigured Server URL in **`ebs.properties`** or an EMM console to make sure: • This preconfigured URL has a valid format: `http(s)://<host>:<port>` • Enter the URL in a web browser and make sure that you are able to access the Oracle E-Business Suite home page successfully. • From a web browser, invoke the login service as `http(s)://<host>:<port>/OA_HTML/RF.jsp?function_id=mLogin` and verify that it prompts for user name and password.
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.

Issue	Tip
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.
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.	To resolve this issue, a mobile user can initiate the server updates from the mobile device. See Directing Users to Obtain Connection Details and Download Updates from the Server, page 7-9.

Troubleshooting Tips on Configuring Apps With the Apps SSO Login Authentication Type

This section describes the troubleshooting tips that are particularly related to configure mobile apps with the Apps SSO Login (previously known as "Web SSO") authentication type.

For information about configuring apps with the Apps SSO Login authentication type, see:

- Configuring Parameters for the Apps SSO Login Authentication Type, page 2-26
- Advanced Configurations for Single Sign-On, page 5-1

Troubleshooting Tips

Perform the following tasks to validate and troubleshoot potential issues for configuring mobile apps with the Apps SSO Login type:

1. **Verify prerequisite configuration for Oracle E-Business Suite, Oracle Access Manager (OAM), and Oracle Directory Services integration**
    1. Navigate to the application login page through a web browser. Verify the login redirects to Oracle Access Manager as configured during the Oracle E-Business Suite integration with Oracle Access Manager, and the same LDAP user that

will be using a mobile app can log in successfully to Oracle E-Business Suite framework based applications.

2. Verify after successful login and rendering of the Oracle E-Business Suite Home page, the user has Oracle E-Business Suite responsibilities assigned.

3. Ensure the administrator has configured the specific configuration tasks, as described in Setup Tasks for Oracle Maintenance for EBS, page 5-4.

2. **Test the configured "SSO Login URL", "SSO Login Success URL", and "SSO Logout URL" parameters**

   1. Navigate to the configured SSO Login URL through a web browser. After the login, the browser should return a protected page successfully (`Status 200 OK`). The URL for this page must be the same as the configured SSO Login Success URL.

      > **Note:** The "SSO Login URL" and "SSO Login Success URL" parameters relate to each other. The values of these two parameters can be the same.

      Do not configure a URL, such as `http://<hostname>:<port>/OA_HTML/AppsLogin`, as the SSO Login URL because this page would unnecessarily redirect to the Oracle E-Business Suite Home page after the login. Use the default SSO Login URL `http://<hostname>:<port>/accessgate/login/sso` instead.

   2. Navigate to the configured SSO Login URL through a web browser. For example, `http://<hostname>:<port>/accessgate/login/sso`.

      > **Note:** When you test the `login/sso` or `login/apps` (as described later in step 3 for "EBS Session Service") service standalone from a web browser, it is recommended sending the X-Ebs-Wep request parameter that is supported in Oracle E-Business Suite AccessGate (EAG) 1.3.2.1 and above with Oracle E-Business Suite web entry URL (`http(s)://<hostname>:<port>`).
      >
      > If EAG does not receive this parameter, the `login/apps` service may fail and an "`Initialization failed -1`" error is captured in EAG logs. In this situation, ensure you pass this X-Ebs-Wep request parameter while testing the service standalone from a browser.

      Expected result: Redirect to the OAM login page. Login successful after specifying the LDAP user name and password.

After the login, the resource `http://<hostname>:<port>/accessgate/login/sso` shows with no error message. This resource must be the configured "SSO Login Success URL" parameter value.

> **Note:** The "SSO Login URL" and "SSO Login Success URL" parameter values can be the same.

The browser shows a blank page successfully.

3. Navigate to the configured SSO Logout URL. For example, `http://<hostname>:<port>/accessgate/logout/sso`.

   Expected result: User logged out successfully.

4. Perform the same tests using your mobile device browser.

3. **Test the configured "EBS Session Service" parameter**

   1. Navigate to the configured EBS Session Service through a web browser. For example, `http://<hostname>:<port>/accessgate/login/apps`.

      Expected result: Redirect to the OAM login page. Login successful after specifying the LDAP user name and password.

      After the login, the browser returns an xml file containing an access token and the user name for the user that just logged in. For example:

      ```
      <response>
      <data>
      <accessToken>xxxxxxxxxxxxxxxxxxxxxxxxxx</accessToken>
      <accessTokenName>emsxxxxx</accessTokenName>
      <ebsVersion>12.2.5</ebsVersion>
      <userName>xxxxx</userName>
      </data>
      </response>
      ```

   2. Perform the same test using your mobile device browser.

4. **Collect HTTP header traces and logs**

   1. Collect HTTP Header traces during the implementation of the above test points.

   2. Collect log files for Oracle E-Business Suite AccessGate, Oracle E-Business Suite oacore, and the OAM server.

      Refer to My Oracle Support Knowledge Document 1077460.1, *Troubleshooting Oracle Access Manager and Oracle E-Business Suite AccessGate*, on how to generate Oracle E-Business Suite AccessGate logs.

Part 2

Oracle E-Business Suite Mobile Apps Release 9.x and Earlier

8

Introduction to Oracle E-Business Suite Mobile Apps 9.x and Earlier

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 administration tasks for viewing mobile app installation and usage metrics, as well as logging and troubleshooting information for Oracle E-Business Suite mobile apps.

> **Note:** This guide does not apply to the following mobile apps that are not developed based on Oracle E-Business Suite Mobile Foundation, except where specifically noted:
>
> - Oracle Fusion Expenses (see Document 1625446.1)
> - Oracle Mobile Field Service (see Document 2188514.1)
> - Oracle Mobile Service Manager for Oracle E-Business Suite (see Document 2107368.1)
> - Oracle Mobile Supply Chain Applications for Oracle E-Business Suite (see Document 2108155.1)

- 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 information on developing enterprise-distributed apps and custom apps for Oracle E-Business Suite, see the *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

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

- To share ideas with Oracle related to mobile apps, see *Oracle E-Business Suite Product Enhancement Request to My Oracle Support Community FAQ*, My Oracle Support Knowledge Document 1584210.2.

Oracle E-Business Suite mobile apps are available in the following languages: Brazilian Portuguese, Canadian French, Dutch, English, French, German, Italian, Japanese, Latin American Spanish, Simplified Chinese, and Spanish.

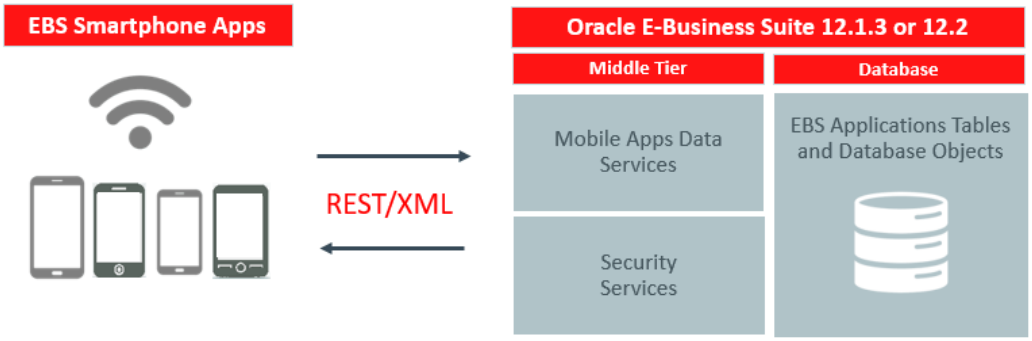
For information on using these languages, see Setting Up and Using Supported Languages, page E-1.

Technical Overview

Oracle E-Business Suite mobile apps interact with the application 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 overview for Oracle E-Business Suite mobile apps:

Technical Architecture Overview



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 12.3 or later and Android 6.0 or later.

Users can run the mobile apps on any devices that are capable of running iOS 12.3 or later. 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 6.0 or later. 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 one-on-one basis and may need additional assistance from the device vendors first.

The Oracle E-Business Suite mobile apps made through Mobile Release 9.1 and earlier 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 the Oracle E-Business Suite Mobile Foundation Release Update History section in *Oracle E-Business Suite Mobile Foundation Release Notes*, My Oracle Support Knowledge Document 1642431.1.

> **Note:** Oracle E-Business Suite Mobile Release 10.x apps leverage new underlying technologies such as Oracle JavaScript Extension Toolkit (JET) and Cordova Framework, etc. that are no longer dependent on Oracle MAF. For more information about Mobile Release 10.x, see Part I

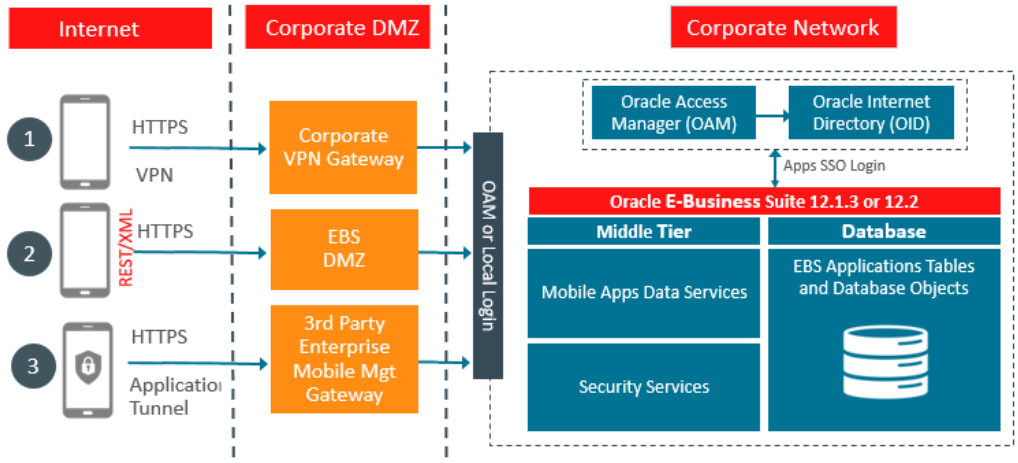
Oracle E-Business Suite Mobile Apps Release 10.x, page 1-1.

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.

Oracle E-Business Suite Mobile Apps Server Connectivity Options

Oracle E-Business Suite mobile app users have the following server connectivity options, as shown in the following diagram, to access the mobile apps:

Oracle E-Business Suite Mobile Apps Server Connectivity Options



1. Over the Internet

   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. For additional information on performing this configuration, see Advanced Configurations for Demilitarized Zone, page 12-1.

2. Over the Intranet

   If your Oracle E-Business Suite environment is not set up in a DMZ configuration, mobile app users must access the Oracle E-Business Suite mobile apps through an intranet connection, such as a virtual private network (VPN).

3. Through Enterprise Mobility Management (EMM) Solutions

   Oracle E-Business Suite mobile apps developed using Oracle Mobile Application Framework (MAF) can integrate with third-party Enterprise Mobility Management solutions that support common AppConfig standards, such as VMware AirWatch.

For more information, see Integrating Oracle E-Business Suite Mobile Apps with Enterprise Mobility Management Solutions, page 15-1.

Additionally, refer to the following advanced configurations to have secured server access for your mobile apps:

- Advanced Configurations for Secure Communication with HTTPS, page 13-1
- Advanced Configurations for Single Sign-On, page 14-1

Sizing Requirements

Because there are different product combinations, different user profiles, and different configurations, there is no one sizing answer for all hardware platforms. Some hardware vendors have sizing worksheets that model the CPU and memory requirements of Oracle E-Business Suite on their hardware. The most reliable strategy to ensure that the hardware is sized appropriately is to install a test environment, and then conduct a benchmark test with a configuration, product mix, and user load that simulates your own current and expected workloads. These conditions can help verify performance before you install your production-ready environment. An alternative is to ask Oracle Consulting Services or your hardware vendor to find another Oracle E-Business Suite system running a product mix and user profile similar to yours.

General Sizing Guidelines

When planning your Oracle E-Business Suite mobile app deployment, consider the following:

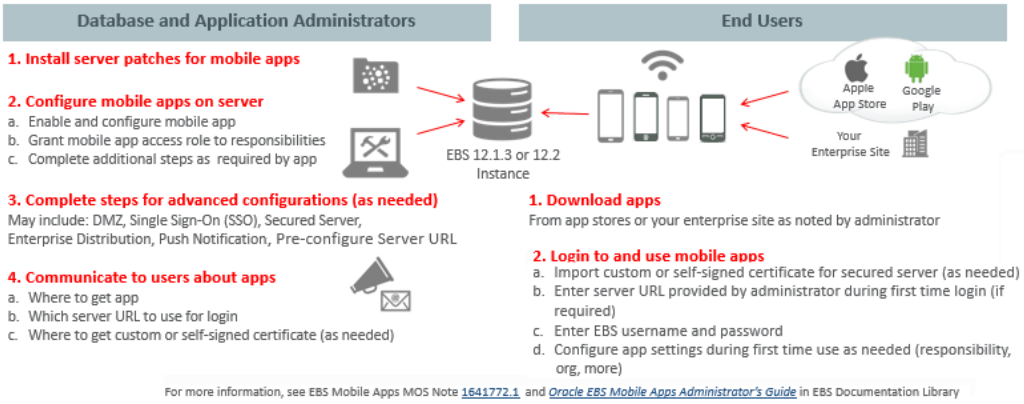
- You can support 150 to 180 mobile users per 2 GB of JVM heap.
- The initial heap size (Xms) and maximum allocated heap (Xmx) should both be set to 2 GB per 150 to 180 users.
- One JVM is allocated per 2 CPUs in general. This is an actual CPU core rather than a logical core.
- Use JVMs with a maximum of 4 GB, and scale for more users by using additional JVMs. The benefits are:
    - Garbage collection (GC) activity is easily balanced (automatically) with multiple JVMs.
    - Each instance will be able to utilize a separate connection pool. In essence, you need to maintain a balance between the allocated JVM heap size per instance and the available connection pool for that instance.

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.

The following diagram illustrates the 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.

Oracle E-Business Suite Mobile Apps High Level Implementation Steps



As illustrated in the diagram, these high level tasks are:

- Setup tasks on the server:
  1. Apply prerequisite patches on the Oracle E-Business Suite server
  2. Configure the mobile apps on the Oracle E-Business Suite server

     This includes enabling a mobile app, setting up the mobile app access to responsibilities, and completing additional setup tasks required for the app.
  3. Complete the setup tasks for advanced configurations if required for an app

     This may include the setup tasks for a DMZ configuration, Single Sign-On (SSO), secure communication with HTTPS, enterprise distribution, push notifications, and pre-configure server URL.
  4. Communicate the mobile app information to users

     This information includes where to download the app, which server to use for login, and where to get custom or self-signed certificates if required.
- Tasks on the mobile client:
  1. Download your app

As instructed by your administrator, mobile users can download the app from a public store, such as Apple App Store and Google Play, or from an enterprise-controlled location.

2. Log in and use your app

   This task includes importing custom or self-signed certificates if required for secured server access, entering server URL provided by your administrator for the initial login, entering user name and password, and configuring app settings for the initial use if needed.

The setup details of these tasks are further explained in the remaining chapters of this book.

9

Setting Up the Mobile Apps

Overview

This chapter describes the setup tasks that administrators must perform first to ensure the mobile apps are ready for users to download and use. 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, deploying the app with Enterprise Mobility Management (EMM) solutions if needed, and validating the server URL before communicating the information to the users.

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.

To support the "Apps SSO Login" authentication (previously known as "Web SSO") from Oracle E-Business Suite Mobile Foundation Release 4.0 and onwards, you must also apply required patches and perform additional setup tasks to enable the feature. See: Mobile Specific Setup Tasks to Enable Apps SSO Login Authentication Security, page 14-3.

Tasks and Patches Required for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0

This section describes the patch information and tasks required for the mobile apps that are built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0. Perform the required tasks to apply prerequisite patches in the following sequence:

1. Performing Conditional Pre-Install Tasks, page 9-2
2. Applying Patches for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0, page 9-3
3. Applying Conditional Post-Install Patches, page 9-16

For information on prerequisite patches for earlier Oracle E-Business Suite Mobile Foundation releases, see Product Family Patches for Earlier Oracle E-Business Suite Mobile Foundation Releases, page A-1.

Step 1: Performing Conditional Pre-Install Tasks

For Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0

Perform any additional conditionally required pre-install tasks from the following list for your apps built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0:

Conditional Pre-Install Tasks for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0

Oracle E-Business Suite Release or Mobile App Name	Requirement	Pre-Install Task
Oracle E-Business Suite Release 12.2 and 12.1.3 • Oracle Mobile Maintenance for Oracle E-Business Suite	Required only if you plan to implement Oracle Mobile Maintenance for Oracle E-Business Suite	Oracle Mobile Maintenance "Disconnected" feature uses the Oracle Mobile Field Service Multiplatform framework, which does not require Oracle Lite and consequently Oracle Lite should be uninstalled. If the "mobileadmin" schema exists, refer to My Oracle Support Knowledge Document 1564644.1, *Oracle Mobile Field Service Store and Forward Multiple Platforms Support*.

Step 2: Applying Patches for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0

Important: If you install or upgrade your apps to the version built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0, then you must apply the server-side prerequisites through one of the methods described in this section. However, if the upgrade is from Release 9.0 to Release 9.1, you do not need to apply these patches again as the server-side prerequisites are exactly the same in both releases.

Important: The Oracle E-Business Suite 12.2 server-side patches listed in this section for Oracle E-Business Suite Mobile Foundation Release 9.1 and Release 9.0 are already included in the respective product family patches in Oracle E-Business Suite Release 12.2.11 or later. If you have installed Oracle E-Business Suite 12.2.11 or later, skip this section and simply apply the post-install patches, as described in Applying Conditional Post-Install Patches, page 9-16.

Apply the server-side patches in either of the following ways based on your needs:

Note: Starting from Oracle E-Business Suite Mobile Foundation Release 7.0 and onwards, Oracle allows you to apply the server-side patches either through Oracle E-Business Suite level patch or product family level patch for your Oracle E-Business Suite release depending on your needs.

- **Apply the Oracle E-Business Suite level patch for your Oracle E-Business Suite release**

  To simplify the patching efforts, all product family patches except Oracle Yard Management (YMS) are consolidated into a single Oracle E-Business Suite level patch for a specific Oracle E-Business Suite release. Additionally, this Oracle E-Business Suite level patch includes the patch for Oracle Mobile Supply Chain Applications for Oracle E-Business Suite (MSCA), although this app is not built with Oracle E-Business Suite Mobile Foundation.

  - For Oracle E-Business Suite Release 12.1.3

    Patch 30107264:R12.SCM_PF.B: MSCA-12.1 Consolidated Patch For Mobile App V9

  - For Oracle E-Business Suite Release 12.2

    Patch 30107329:R12.SCM_PF.C: MSCA-12.2 Consolidated Patch For Mobile App V9

  If you intend to uptake all the product family patches and the patch for the MSCA app, simply apply this higher level consolidated patch for your Oracle E-Business Suite release that in turn contains all the patches corresponding to Oracle E-Business Suite mobile apps (including MSCA mentioned above) except Oracle Mobile Yard for Oracle E-Business Suite.

  For Oracle Mobile Yard for Oracle E-Business Suite, the required Patch 30144032: R12.ATG_PF.C is already contained in the Oracle E-Business Suite level patch. If you plan to use this app and have already applied Patch 24383610:R12.YMS.C as part of the Oracle E-Business Suite Mobile Release 7 uptake, then there is no additional patch to be applied in this release.

  The following table lists the Oracle E-Business Suite level consolidated patches:

Oracle E-Business Suite Level Patches for Oracle E-Business Suite Mobile Foundation Release 9.1 and Release 9.0

Oracle E-Business Suite Level Patch	Oracle E-Business Suite 12.1.3	Oracle E-Business Suite 12.2
Oracle E-Business Suite level patches contain: • All the product family level patches except Oracle Yard Management (yms) • Oracle Mobile Supply Chain Applications for Oracle E-Business Suite (MSCA), not built with Oracle E-Business Suite Mobile Foundation	Patch 30144061:12.1.0 • This Oracle E-Business Suite 12.1.3 patch includes Patch 30107264: R12.SCM_PF.B for MSCA, in addition to each product family patch listed in the product family level patch table.	Patch 30144066:12.2.0 • This Oracle E-Business Suite 12.2 patch includes Patch 30107329:R12.SCM_PF. C for MSCA, in addition to each product family patch listed in the product family level patch table except Oracle Yard Management. To use Oracle Mobile Yard for Oracle E-Business Suite, apply Patch 24383610:R12. YMS.C - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied.

- **Apply the product family level patch for your Oracle E-Business Suite release**

  If you plan to apply the patches only for the relevant product families, rather than for all product families, use this approach to apply the patches for your Oracle E-Business Suite mobile apps.

  > **Note:** The patch for Oracle Mobile Supply Chain Applications for Oracle E-Business Suite described earlier is only included in the Oracle E-Business Suite level patches; it is not included in the Oracle Supply Chain Management (scm_pf) product family patches. If you plan to use this app, and you do not plan to apply the Oracle E-Business Suite level patch, then you must apply the MSCA patch individually for your Oracle E-Business Suite release.

For example, if you use the Inventory and Timecards approval types in the Approvals app, and you are upgrading only the Approvals app to the version built with Oracle E-Business Suite Mobile Foundation 9.1 or 9.0, then you can apply the Oracle E-Business Suite level consolidated patch for all product families.

Alternatively, you can apply only the relevant product family patches for your Oracle E-Business Suite release level, in this case the Oracle Supply Chain Management product family patch for Inventory approvals and the Oracle Human Resources product family patch for Timecard approvals.

> **Important:** Oracle is discontinuing selected Oracle E-Business Suite mobile apps. Therefore, no patches for these discontinued apps are included in their respective product family patches released after their discontinuation dates. For information about the apps being discontinued, refer to the Discontinued Oracle E-Business Mobile Apps section in *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*, My Oracle Support Knowledge Document 1641772.1.

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

Oracle E-Business Suite Product Family Level Patches for Oracle E-Business Suite Mobile Foundation Release 9.1 and Release 9.0

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 (for developing custom approval types) • Custom mobile apps for Oracle E-Business Suite, including the REST services that the sample app uses to provide real app flows See: *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2.*	Patch 30144012:R12.ATG_PF.B: ATG -12.1 Consolidated Patch For Mobile Applications Foundation V9 Apply the product family patches for the seeded approval types you want to use, as shown in subsequent rows in this table.	Patch 30144032:R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V9 Apply the product family patches for the seeded approval types you want to use, as shown in subsequent rows in this table.

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
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 30107242:R12.FIN_PF.B: FIN - 12.1 Consolidated Patch For Mobile Applications Foundation V9	Patch 30107297:R12.FIN_PF.C: FIN - 12.2 Consolidated Patch For Mobile Applications Foundation V9

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 Human Resources 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 • Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite	Patch 30143992:R12.HR_PF.B: HRMS - 12.1 Consolidated Patch For Mobile Applications Foundation V9	Patch 30144049:R12.HR_PF.C: HRMS - 12.2 Consolidated Patch For Mobile Applications Foundation V9

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Interaction Center Family (cc_pf) (See **Footnote 3**, page 9-15)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Channel Revenue Management approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Quoting approvals)	Apply the following patches: • Patch 30144012: R12.ATG_PF.B: ATG - 12.1 Consolidated Patch For Mobile Applications Foundation V9 • Patch 24383355: R12.CC_PF.B: CRM - 12.1 Consolidated Patch For Mobile Applications Foundation V7 if not already applied	Apply the following patches: • Patch 30144032: R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V9 • Patch 24383599: R12.CC_PF.C: CRM - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied

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) (See **Footnote 3**, page 9-15)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Purchase Order approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Requisition approvals)	Apply the following patches: • Patch 30144012: R12.ATG_PF.B: ATG - 12.1 Consolidated Patch For Mobile Applications Foundation V9 • Patch 24383344: R12.PRC_PF.B: PRC - 12.1 Consolidated Patch For Mobile Applications Foundation V7 if not already applied	Apply the following patches: • Patch 30144032: R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V9 • Patch 24383558: R12.PRC_PF.C: PRC - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Projects (pj_pf) (See **Footnote 3**, page 9-15)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Projects approvals)	Apply the following patches: • Patch 30144012: R12.ATG_PF.B: ATG - 12.1 Consolidated Patch For Mobile Applications Foundation V9 • Patch 24383283: R12.PJ_PF.B: PROJ - 12.1 Consolidated Patch For Mobile Applications Foundation V7 if not already applied	Apply the following patches: • Patch 30144032: R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V9 • Patch 24383522: R12.PJ_PF.C: PROJ - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied

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 Inventory approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Product Information approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Order Management approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Maintenance approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Service Contracts approvals) • Oracle Mobile Discrete Production Supervisor for	Patch 30144006:R12.SCM_PF.B: SCM -12.1 Consolidated Patch For Mobile Applications Foundation V9	Patch 30144036:R12.SCM_PF.C: SCM -12.2 Consolidated Patch For Mobile Applications Foundation V9

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 • 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 Sales Orders for Oracle E-Business Suite		

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Yard Management (yms) (See **Footnote 3**, page 9-15)	• Oracle Mobile Yard for Oracle E-Business Suite	N/A	Apply the following patches: • Patch 30144032: R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V9 • Patch 24383610: R12.YMS.C:YMS - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied **Prerequisites:** • Oracle E-Business Suite Release 12.2.3 • R12.SCM_PF.C. Delta.4 • R12.AD.C.Delta. 9 & R12.TXK.C. Delta.9

Footnote 3: In this Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0, if you are upgrading any mobile apps within the product family to the version built with Oracle E-Business Suite Mobile Foundation 9.1 or Release 9.0, then apply the following patches:

- Oracle E-Business Suite Applications Technology (atg_pf) patch corresponding to Oracle E-Business Suite Mobile Foundation Release 9.0

- Product family patch from the Oracle E-Business Suite Mobile Foundation Release 7.0 if not already applied

Step 3: Applying Conditional Post-Install Patches

For Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0

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

Conditional Post-Install Patches for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 and 12.1.3 • Oracle E-Business Suite Mobile Foundation Release 9.0 Online Help	Required for all Oracle E-Business Suite mobile apps, built with Oracle E-Business Suite Mobile Foundation Release 9.1 or Release 9.0, connected to Oracle E-Business Suite Release 12.1.3 or Release 12.2	• Release 12.2 and 12.1.3: Patch 28879188

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 and 12.1.3	Required only if your Oracle E-Business Suite environment has the following patches applied: • Release 12.2 - Patch 27761509:12.2.0 (Oracle Applications Release 12.2 : Consolidated Patch for Data Removal Tool) • Release 12.1.3 - Patch 27822242:12.1.0 (Oracle Applications Release 12.1 : Consolidated Patch for Data Removal Tool) **Note:** If your environment has the following Data Removal Tool consolidated patches applied instead, then the post-install tasks specified in the next column are not required: • Release 12.2 - Patch 29206195:12.2.0 (Oracle Applications Release 12.2 Data Removal Tool - One-off Consolidation - January 2020) • Release 12.1.3 - Patch 29206188:12.1.0 (Oracle Applications Release 12.1 Data Removal Tool - One-off Consolidation - January 2020)	Perform the following steps in the specified order: • Release 12.2: 1. Apply Patch 28295762:R12.PER.C. 2. Apply Patch 28303904:R12.FND.C. 3. Recompile the data removal metadata by running the concurrent program "Recompile Metadata for Data Removal Tool", with the "Entity Type" parameter set to "ALL". • Release 12.1.3: 1. Apply Patch 28295762:R12.PER.B. 2. Apply Patch 28303904:R12.FND.B. 3. Recompile the data removal metadata by running the concurrent program "Recompile Metadata for Data Removal Tool", with the "Entity Type" parameter set to "ALL".

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information

Oracle E-Business Suite Release 12.2 and 12.1.3
• Oracle Mobile Approvals for Oracle E-Business Suite (Lease and Finance Management approvals only)
	Required if you connect to an Oracle E-Business Suite 12.2 or 12.1.3 instance with Oracle Mobile Approvals for Oracle E-Business Suite (Lease and Finance Management approvals only)	• Release 12.2
		  • Patch 28969483:R12.OKL.C
		  • Patch 29143795:R12.OKL.C
		• Release 12.1.3
		  • Patch 28140398:R12.OKL.B
		  • Patch 30343199:R12.OKL.B
		See My Oracle Support Knowledge Document 2610782.1 and each patch Readme for additional patch prerequisites.

Oracle E-Business Suite Release 12.2 and 12.1.3 • Oracle Mobile Learning for Oracle E-Business Suite	Required if you connect to an Oracle E-Business Suite 12.2 or 12.1.3 instance with Oracle Mobile Learning for Oracle E-Business Suite	• Release 12.2: Patch 31006617:R12.OTA.C • Release 12.1.3: Patch 31006617:R12.OTA.B
Oracle E-Business Suite Release 12.2 and 12.1.3 • Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite	Required if you connect to an Oracle E-Business Suite 12.2 or 12.1.3 instance with Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite	• Release 12.2: Patch 31165250:R12.PER.C • Release 12.1.3: Patch 31165250:R12.PER.B

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 and 12.1.3 • Oracle Mobile Supply Chain Applications for Oracle E-Business Suite	Required if you connect to an Oracle E-Business Suite 12.2 or 12.1.3 instance with Oracle Mobile Supply Chain Applications for Oracle E-Business Suite	• Release 12.2: Patch 31135896:R12.MWA.C • Release 12.1.3: Patch 31135896:R12.MWA.B
Oracle E-Business Suite Release 12.2 and 12.1.3 • Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite • Oracle Mobile Person Directory for Oracle E-Business Suite	Required only if you connect to an Oracle E-Business Suite 12.2 or 12.1.3 instance and if you are using or upgrading your database to Oracle Database 19c for Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite or Oracle Mobile Person Directory for Oracle E-Business Suite	• Release 12.2: Patch 32122438:R12.PER.C • Release 12.1.3: Patch 31379163:R12.PER.B
Oracle E-Business Suite Release 12.2 and 12.1.3 • Enterprise version of Oracle Mobile Approvals for Oracle E-Business Suite, developed from Oracle E-Business Suite Mobile Foundation Release 9.0 or Release 9.1, with push notifications enabled • Custom Oracle E-Business Suite mobile apps developed based on Oracle E-Business Suite Mobile Foundation Release 9.0 or Release 9.1 Login component, with push notifications enabled	Required only if your custom app or enterprise version of the Approvals app implements push notifications, including the support for Oracle Mobile Hub (OMH) or Oracle Mobile Cloud Service (MCS), and connects to an Oracle E-Business Suite 12.2 or 12.1.3 instance	• Release 12.2: Patch 33404902:R12.FND.C • Release 12.1.3: Patch 33404902:R12.FND.B

Additional Information: To develop custom apps for Oracle E-Business Suite, you need to download the following client-side patches appropriate for your app's Oracle E-Business Suite Mobile Foundation release. These patches apply for Oracle E-Business Suite Release 12.1.3 and Release 12.2:

- For Release 9.1 - Patch 32284288 - Oracle E-Business Suite Mobile Foundation (Login component) Release 9.1
- For Release 9.0 - Patch 30914694 - Oracle E-Business Suite Mobile Foundation (Login component) Release 9.0

These patches enable the Oracle E-Business Suite Mobile Foundation client libraries, application template, and sample app; therefore, apply the patches on the mobile client, not on the Oracle E-Business Suite server.

For information on developing custom apps for Oracle E-Business Suite and using the sample app. See: *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

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:

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. If the configuration is changed after the initial setup is complete and loaded to a user's app, starting from the Oracle E-Business Suite Mobile Foundation Release 7.0, the updated parameters will be automatically downloaded to the app every five logins. See Directing Users to Obtain Connection Details and Download Updates from the Server, page 16-6.

Enabling a Mobile App Individually and Specifying the Configuration Through the UI Pages

To access Oracle E-Business Suite 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 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:

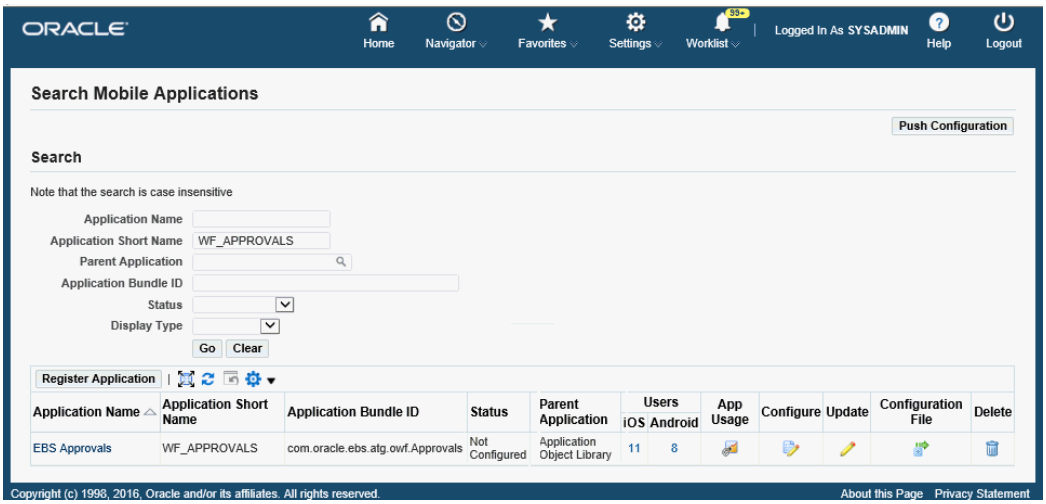
Privileges	Mobile Applications Administrator	Mobile Applications Developer
Search enterprise apps	Yes	Yes
Configure the Push Notification System	Yes	Yes
Register enterprise apps	Yes	Yes
Configure enterprise apps	Yes	Yes
Update application definitions	Yes	Yes

Privileges	Mobile Applications Administrator	Mobile Applications Developer
Delete application definitions	Yes	Yes
View configuration files	Yes	Yes
View mobile app installation details	Yes	No
View mobile app usage metrics	Yes	No

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.

The Search Mobile Applications Page



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:

Additional Information: A user who has the Mobile Applications Developer role can register, update, and delete the application metadata definition of an app modified from an MAA file for enterprise distribution or a custom app developed for Oracle E-Business Suite. For information on these tasks, see Registering and Updating Your Mobile App Definition Metadata, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

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

  See: Enabling and Configuring a Mobile App Individually, page 9-23.

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

  See: Viewing and Validating Your Mobile App Configuration, page 9-35.

- 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 9-37.

- View the device installation information for a mobile app by clicking the number of users link either for iOS or Android.

  See: Viewing Your Mobile App Installation Details, page 11-2.

- View the overall usage details for an app by clicking the **App Usage** icon.

  See: Viewing Your Mobile App Usage, page 11-4.

- (Optional) Configure the required setup tasks for the Push Notification System by clicking the **Push Configuration** button.

  See: Configuring Oracle E-Business Suite Mobile Foundation Push Notification System, page 10-11.

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.

> **Note:** The Users and App Usage columns are available from Oracle E-Business Suite Mobile Foundation 5.0 and onwards for viewing user installation and app usage information. See: Viewing Mobile App Installation and Usage Metrics, page 11-1.

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

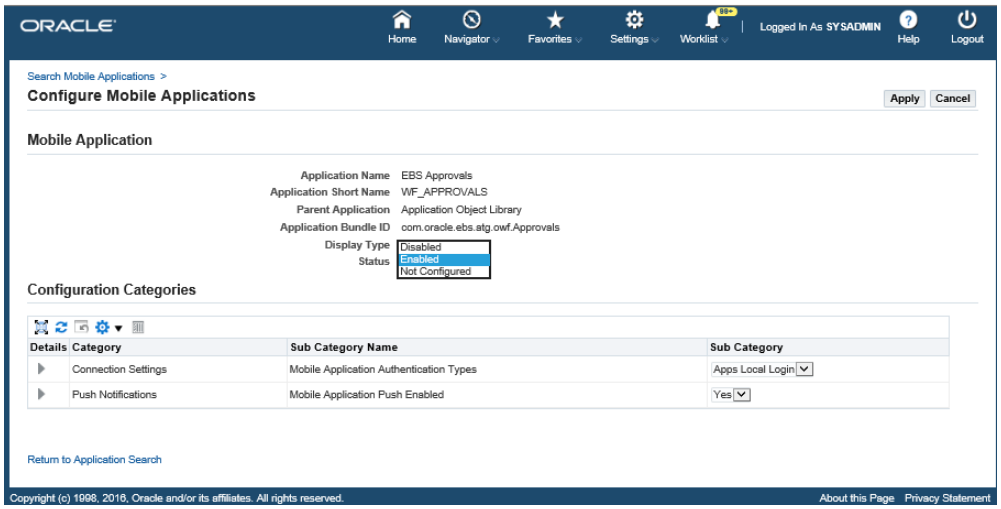
   - Enabled: This allows you to configure the app against Oracle E-Business Suite.

   - 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 Page to Enable a Mobile App



6. In the Configuration Categories region, two types of category values can be displayed depending on the selected app that you want to enable:

   - **"Connection Settings" for configuring authentication types for ALL mobile apps**

     See: Supporting Apps Local Login and Apps SSO Login Authentication Types for All Mobile Apps, page 9-27.

   - **"Push Notifications" for configuring push notifications for supported mobile apps (available from Oracle E-Business Suite Mobile Foundation 7.0 and onwards)**

     See: Configuring Push Notifications for Supported Mobile Apps, page 9-34.

7. In the Configuration Categories region, optionally choose the **Show** link next to the "Connection Settings" or "Push Notifications" category to display the parameters corresponding to the selected authentication type or the parameters for the push notifications. 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, for the authentication type, 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 with the custom profile option name. For information on configuring parameters in the Configuration Parameters region, see:

- Configuring Parameters for the Apps Local Login Authentication Type, page 9-29.
- Configuring Parameters for the Apps SSO Login Authentication Type, page 9-31.
- Configuring Parameters for Push Notifications, page 9-34

Configuration parameters to be included in the configuration file depends on the selected authentication type in the Sub Category field. For example, if "Apps SSO Login" is selected for an app, the corresponding parameters of the "Apps SSO Login" authentication type are included in the configuration file. Additionally, if the app is enabled with push notifications available from Oracle E-Business Suite Mobile Foundation Release 7.0 and onwards, the relevant parameter settings for push notifications are also included in the configuration file, along with the "Apps SSO Login" associated parameters.

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.

9. Click the **Apply** button. This action saves the selected authentication type and relevant 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 including the parameter settings for push notifications if available 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.

To validate the configuration, click the **Configuration File** icon from the search result table. See: Viewing and Validating Your Mobile App Configuration, page 9-35.

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.

Mobile apps may have configuration updates after the initial launch. 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. Starting from the Oracle E-Business Suite Mobile Foundation Release 7.0 and onwards, each app periodically checks for configuration updates and automatically downloads them to the app from the Oracle E-Business Suite server. Additionally, the user can still manually check if any new updates from the server are required in the app if necessary. See Directing Users to Obtain Connection Details and Initiate Server Updates, page 16-6.

Supporting Apps Local Login and Apps SSO Login Authentication Types for All Mobile Apps

Oracle E-Business Suite mobile apps support "Apps Local Login" and "Apps SSO Login" authentication types that are displayed under the "Connection Settings" category in the Configuration Categories region.

> **Note:** The "Apps Local Login" type (previously known as "HTTP Basic") corresponds to the "HTTP Basic" authentication server type used in Oracle Mobile Application Framework; the "Apps SSO Login" type (previously known as "Web SSO") corresponds to the "Web SSO" authentication server type used in Oracle Mobile Application Framework.

Authentication type is preselected or defined for an app during the app registration. Each authentication type is associated with a set of configuration parameters required to set for an app. When you enable or configure an app, the preselected type (either "Apps Local Login" or "Apps SSO Login") is displayed in the Sub Category field in the Configuration Categories region. You can override the selected type if needed by selecting a different value from the Sub Category drop-down list. After the change, the parameters corresponding to the selected authentication type will be loaded and displayed in the Configuration Parameters region.

> **Important:** Make sure Oracle E-Business Suite mobile apps work with "Apps Local Login" before you change it to the "Apps SSO Login" authentication type. If an app initially connects to Oracle E-Business Suite through "Apps Local Login", and later its authentication type is changed to "Apps SSO Login", the app users should initiate the manual update to refresh the configuration. This is performed by tapping **Settings** from the mobile app navigation menu, then tapping **Connection Details**, and then tapping the **Sync** icon.
>
> Please note that for an app built with Oracle E-Business Suite Mobile Foundation Release 7.0 or later, if this manual update process is not initiated, the new configuration will be downloaded at a later time during the automatic check for updates. See: Directing Users to Obtain Connection Details and Initiate Server Updates, page 16-6.

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

- **Apps Local Login (default) - for local authentication**

Apps Local Login is the default type for a mobile app to authenticate mobile users locally against the Oracle E-Business Suite server. When this type is selected for a mobile app, the user passwords must be stored in Oracle E-Business Suite.

> **Note:** If user passwords are externally stored and are not accessible which indicates that your instance is single sign-on enabled, configure your app with the "Apps SSO Login" authentication type instead.

When "Apps Local Login" is selected as the type, three associated parameters, that is, Session Timeout, Idle Timeout, and Service Endpoint, are displayed in the Configuration Parameters region. You can override the default Apps Local Login type if needed by selecting a desired authentication type, such as "Apps SSO Login", in the Sub Category field. After the change, the parameters associated with the new type "Apps SSO Login" are displayed in the Configuration Parameters region.

For information on setting configuration parameters for the Apps Local Login authentication type, see Configuring Parameters for the Apps Local Login Authentication Type, page 9-29.

- **Apps SSO Login - for remote authentication**

  Starting from Oracle E-Business Suite Mobile Foundation Release 4.0, the "Apps SSO Login" authentication type is available for selection in addition to the "Apps Local Login" type.

  When the "Apps SSO Login" type is selected for a mobile app, the mobile app users are not authenticated against Oracle E-Business Suite, but 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.

  To use "Apps SSO Login" as the authentication type, ensure the following:

  - 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: Prerequisites for Setting Up Mobile Apps with Single Sign-On (SSO), page 14-2 and Mobile Specific Setup Tasks to Enable Apps SSO Login Authentication Security, page 14-3.

  For information on setting configuration parameters for the Apps SSO Login

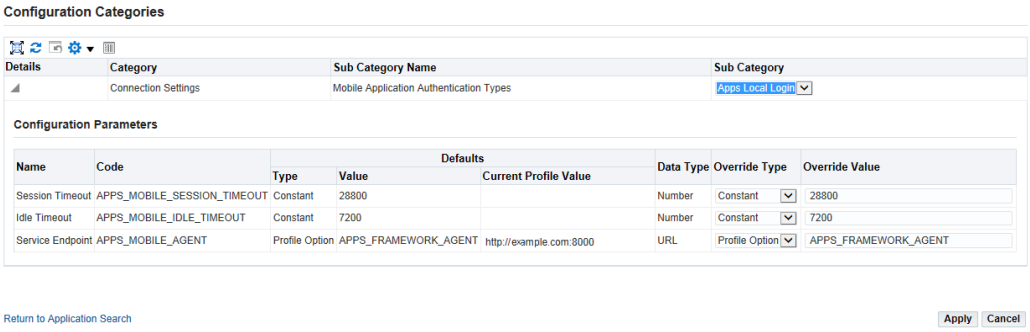
authentication type, see Configuring Parameters for the Apps SSO Login Authentication Type, page 9-31.

For troubleshooting information, see: Troubleshooting Tips on Configuring Apps with Apps SSO Login Authentication Type, page 16-22.

Configuring Parameters for the Apps Local Login Authentication Type

If the default "Apps Local Login" type (previously known as "HTTP Basic") is used as the authentication type to authenticate users locally, update the following parameter values:

Configuration Categories Region with "Apps Local Login" Parameters



Configuration Categories

Details	Category	Sub Category Name	Sub Category
	Connection Settings	Mobile Application Authentication Types	Apps Local Login

Configuration Parameters

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

Return to Application Search

Apply Cancel

- **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. 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 value of the Service Endpoint parameter 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 parameter value 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 parameter, 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 Apps SSO Login Authentication Type

Important: Before configuring apps with "Apps SSO Login" (previously known as the "Web SSO" type), make sure your apps work with "Apps Local Login" first. If an app initially connects to Oracle E-Business Suite through "Apps Local Login", and later its authentication type is changed to "Apps SSO Login", the app users should initiate the manual update to refresh the configuration. This is performed by tapping **Settings** from the mobile app navigation menu, then tapping **Connection Details**, and then tapping the **Sync** icon.

For an app built with Oracle E-Business Suite Mobile Foundation Release 7.0 or later, if this manual update process is not initiated, the new configuration will be downloaded at a later time during the automatic check for updates. See: Directing Users to Obtain Connection Details and Initiate Server Updates, page 16-6.

- Select "Apps SSO Login" as the authentication type if you want to delegate authentication to Oracle Access Manager based on a protected Login URL.
- You must apply required patches and perform additional setup tasks including common tasks and mobile specific setup tasks to enable this feature.

  See: Advanced Configurations for Single Sign-On (SSO), page 14-1.

Configuration Categories Region with "Apps SSO Login" Parameters

Configuration Categories

Details	Category	Sub Category Name	Sub Category
	Connection Settings	Mobile Application Authentication Types	Apps SSO Login

Configuration Parameters

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

Return to Application Search

Apply Cancel

If "Apps SSO Login" is selected as the authentication type to authenticate users remotely, update the following parameter values:

- **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 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.

- 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 that indicates the user has logged in successfully.

  To determine the correct value for this parameter, navigate to the configured SSO Login URL in a web browser session and then submit valid login credentials. The URL that you are re-directed to after successful login is your SSO Login Success URL.

  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 9-30.

Configuring Push Notifications for Supported Mobile Apps

Starting from Oracle E-Business Suite Mobile Foundation 7.0 and onwards, push notifications are supported when using Oracle Mobile Cloud Service in the following apps:

- Custom Oracle E-Business Suite mobile apps developed using the Login component from Oracle E-Business Suite Mobile Foundation

- Oracle Mobile Approvals for Oracle E-Business Suite, when provided to users through enterprise distribution

If a selected app is one of the above supported apps for push notifications, a mobile applications developer can add the "Push Notifications" category while registering the app and defining the application definition metadata. For information on adding the "Push Notifications" category during the app registration, see Adding Push Notifications to App Configuration, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

In order to receive push notifications from your mobile devices, ensure to complete the following required setup tasks both on the server and mobile client. See:

- Setting Up and Enabling Push Notifications for Oracle E-Business Suite Mobile Apps, page 10-5

- Implementing Push Notifications, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*

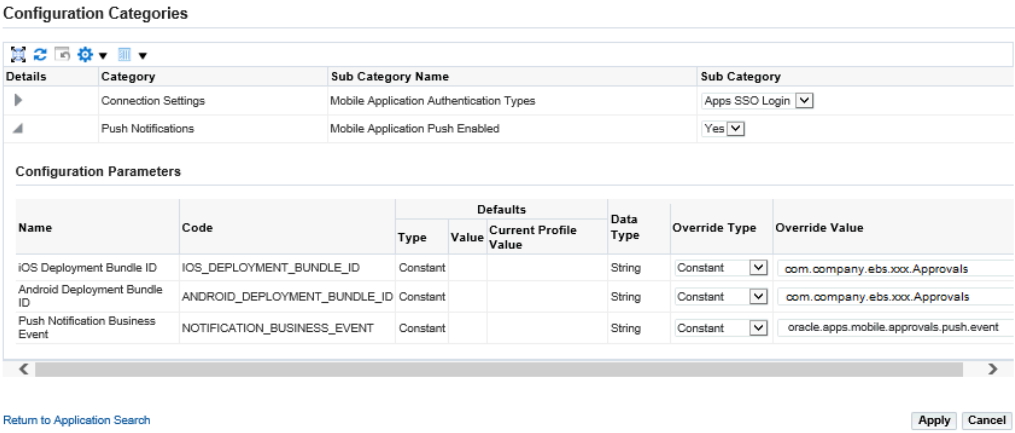
Configuring Parameters for Push Notifications

If the "Push Notifications" category appears in the Configuration Categories region, and if you also want to implement push notifications for the app, select "Yes" in the Sub Category.

> **Note:** Although the "Push Notifications" category appears, you can still leave the default "No" value unchanged if you do not want the app to be enabled with push notifications. The app still works simply without push notifications.

You can update the following parameter values for push notifications:

Configuration Categories Region with "Push Notifications" Parameters



- **Push Notifications Business Event (NOTIFICATION_BUSINESS_EVENT)**
- **Android Deployment Bundle ID (ANDROID_DEPLOYMENT_BUNDLE_ID)**
- **iOS Deployment Bundle ID (IOS_DEPLOYMENT_BUNDLE_ID)**

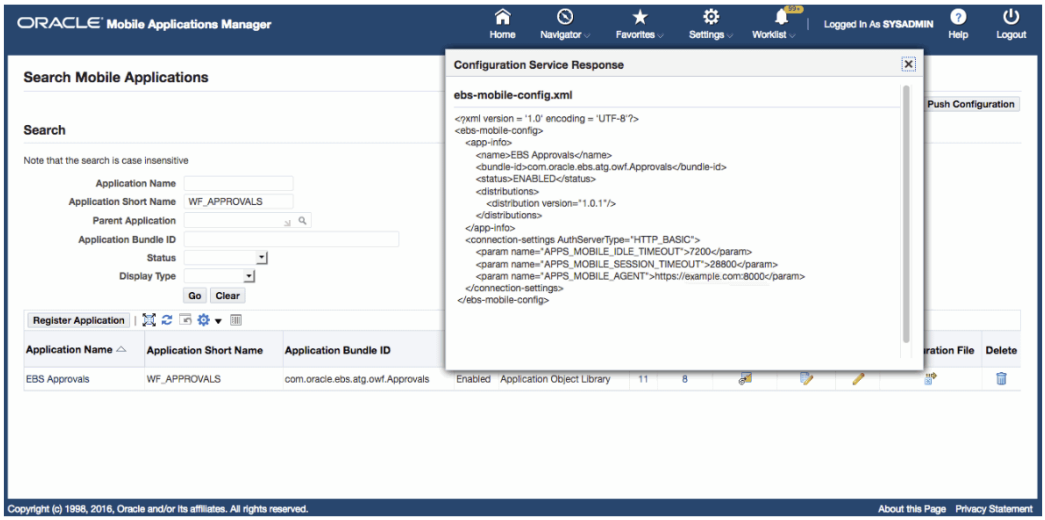
For information on entering these push notification parameters, see Configuring Supported Mobile Apps with Push Notifications, page 10-14.

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.

Configuration Service Response Pop-up Window with Configuration File Content



Note that if the selected app is configured with push notifications, the relevant parameter settings are also displayed as part of the configuration file.

Configuration File with Push Notifications Parameters Highlighted

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="HTTP_BASIC">
    <param name="APPS_MOBILE_IDLE_TIMEOUT">7200</param>
    <param name="APPS_MOBILE_SESSION_TIMEOUT">28800</param>
    <param name="APPS_MOBILE_AGENT">https://example.com:8000</param>
  </connection-settings>
  <push-notifications>
    <param name="PUSH_STATUS">ENABLED</param>
    <param name="ANDROID_SENDER_ID">[redacted]</param>
  </push-notifications>
</ebs-mobile-config>
```

Additionally, you can validate the configuration by accessing the configuration service URL through a web browser. See Validating the Configuration, page 9-42.

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 9-23.

- **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.

  If the app can be enabled with push notifications, this region may also include the push notifications related parameters.

To update the selected mobile app details, click the **Update** button. See: Updating Your Mobile App Definition, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

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` and the script `EBSMblConfigApps.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:** From Oracle E-Business Suite Mobile Foundation Release 4.0, the script supports the selection of the Sub Category (`<sub-category>`) attribute that indicates either of the following authentication types to be used by a mobile app.
   >
   > - HTTP_BASIC: The type corresponds to "Apps Local Login" (display name) from the Mobile Applications Manager UI pages.

- WEB_SSO: The type corresponds to "Apps SSO Login" (display name) from the Mobile Applications Manager UI pages.

Note: If an app supports push notifications, available from Oracle E-Business Suite Mobile Foundation Release 7.0 and onwards, it cannot be configured using the script. Instead, configure the app with push notifications from the Mobile Applications Manager UI pages. See: Enabling a Mobile App Individually and Specifying the Configuration Through the UI Pages, page 9-21.

```
<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 (Apps Local Login) is set to `Y`.

   Note: If the `select` attribute for the "WEB_SSO" type (Apps SSO Login) 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.

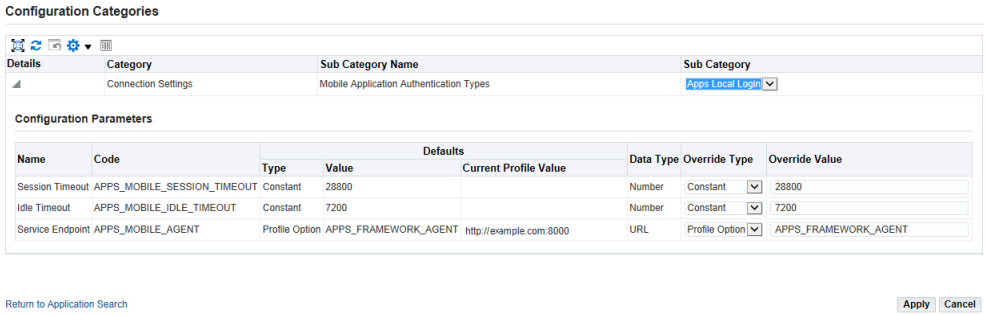
   - **SERVER_DEFAULT:** The default value of the parameter is used to configure the app. For example, 28800 is the server default for Session Timeout parameter.

   - **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 Region with "Apps Local Login" Parameters



The following example shows a sample custom template `Applications.xml` file after setting the parameters with the Apps Local Login (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`, run 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 9-42 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 9-21.

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=mConfig&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 D-1.

   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.

      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>
```

Please note that 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.

Starting from Oracle E-Business Suite Mobile Foundation Release 7.0 and onwards, the "Push Notifications" configuration category is added to a mobile app to implement push notifications, the associated `ebs-mobile-config.xml` file (as shown below) will include relevant XML elements indicating whether the push notifications feature is enabled for this app, as well as the Android Sender ID for use in the Android mobile apps.

```
<?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="1.0.1"
    </distributions>
  </app-info>
  <connection-settings AuthServerType="HTTP_BASIC">
    <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>
     <push-notifications>
    <param name="PUSH_STATUS">ENABLED</param>
    <param name="ANDROID_SENDER_ID">xxxxxxxxxxxx</param>
     </push-notifications>
  </ebs-mobile-config>
```

For information on enabling push notifications for mobile apps, see Configuring Supported Mobile Apps with Push Notifications, page 10-14.

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.

3. Make sure the setup is valid at this point and ensure that your app works with the "Apps Local Login" (previously known as "HTTP Basic") authentication type before proceeding to any advanced configurations.

   1. In the Mobile Applications Manager UI pages, configure the mobile app with authentication type as "Apps Local Login".

      See: Configuring Parameters for the Apps Local Login Authentication Type, page 9-29.

   2. Log in to the mobile app as a user whose password is stored in Oracle E-Business Suite, such as `sysadmin`.

      You should be able to successfully log in and view the mobile app pages.

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 in *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 Mobile App Access Roles, page B-1.

For information on creating new mobile app access roles if needed for enterprise distribution or custom apps for Oracle E-Business Suite, see Creating and Using Mobile App Access Roles, *Oracle E-Business Suite Mobile Apps Developer's Guide Release 12.1 and 12.2*.

> **Note:** For the access roles created for enterprise-distributed apps, ensure to grant the REST services permission sets of the corresponding seeded apps to the app access roles. See: Mobile App REST Services Permission Sets, page B-3.

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 9-47
2. Setting Up Maps, page 9-59
3. Support for Barcodes, page 9-60

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 Discrete Production Supervisor for Oracle E-Business Suite
- Oracle Mobile Discrete Quality Manager for Oracle E-Business Suite
- Oracle Mobile iProcurement for Oracle E-Business Suite
- Oracle Mobile Procurement for Oracle E-Business Suite
- Oracle Mobile Process Quality Manager for Oracle E-Business Suite
- Oracle Mobile Project Manager for Oracle E-Business Suite
- Oracle Mobile Project Manufacturing for Oracle E-Business Suite
- Oracle Mobile Sales Orders 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 9-48
2. Step 2: Scheduling the "HR Mobile Utils Person Data Full Synch" Concurrent Program, page 9-57
3. Step 3: Allowing Apps to Access Local Contacts, page 9-58

Step 1: Setting Up a Qualifier

Setting up a qualifier involves the following key steps:

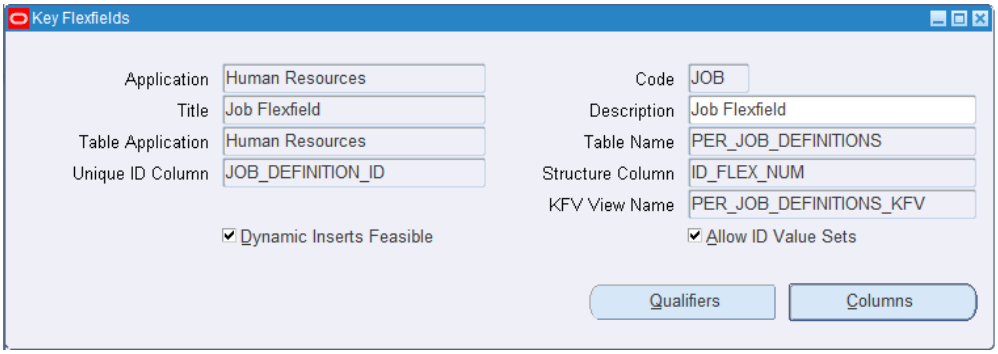
1. Step 1.1: Creating a Qualifier, page 9-48
2. Step 1.2: Identifying the Flexfield Structure for Your Business Group, page 9-49
3. Step 1.3: Enabling the Qualifier for the Flexfield Segment, page 9-52
4. Step 1.4: Adding the "HR Mobile Utils Person Data Full Synch" Concurrent Program to a Request Group, page 9-54

Step 1.1: Creating a Qualifier

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

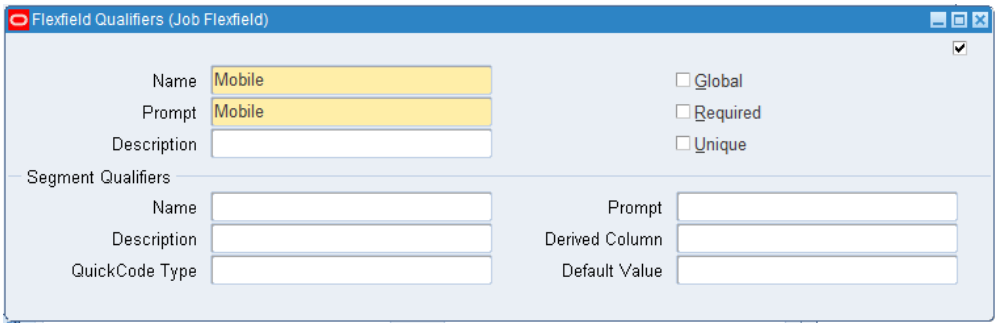
1. Log in to Oracle E-Business Suite as a user who has access to the Application Developer responsibility. For example, log in as `SYSADMIN`.
2. Select the Application Developer responsibility. Choose the **Flexfield** link, then the **Key** link, and then the **Register** link from the navigator. This 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".

Key Flexfields Window



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 Window



Step 1.2: Identifying the Flexfield Structure for Your Business Group

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

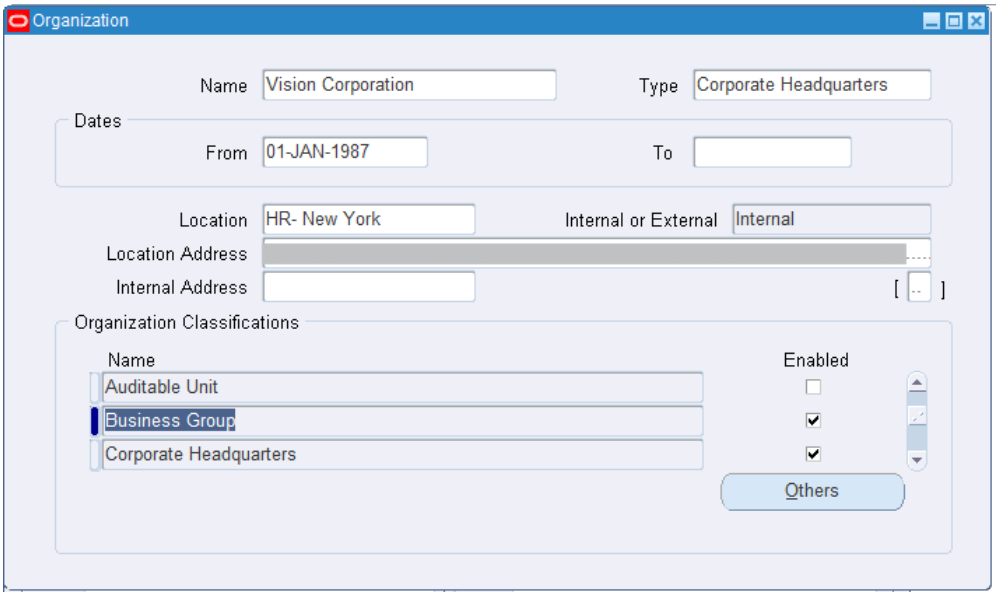
1. Log in to Oracle E-Business Suite as a user who has the HRMS Manager responsibility.

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.

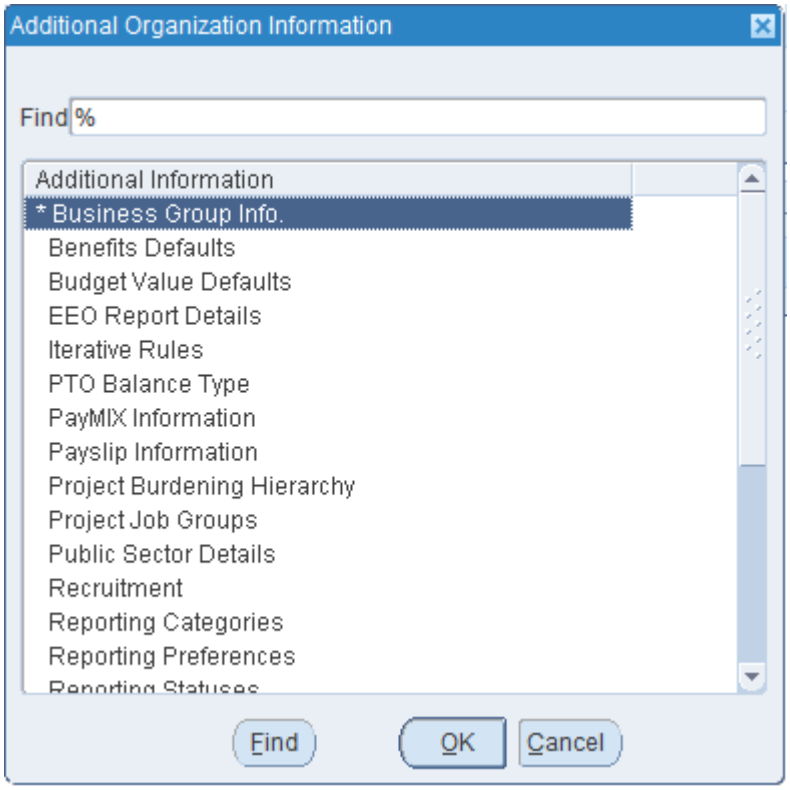
4. In the Organization Classifications region, select "Business Group" and click the **Others** button.

Flexfield Structure in the Organization Window



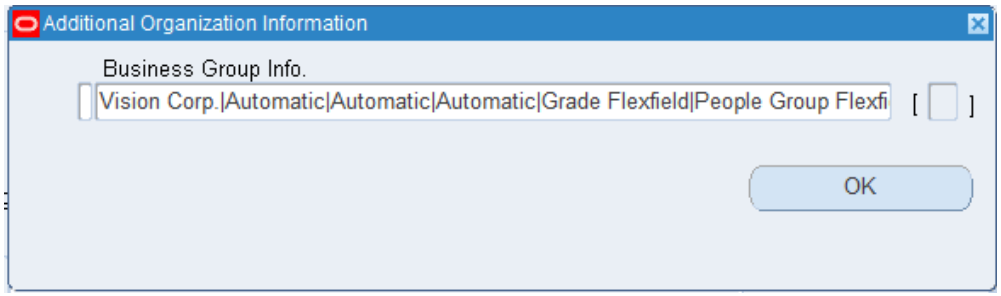
5. The Additional Organization Information window appears. Select "Business Group Info".

Additional Organization Information Window



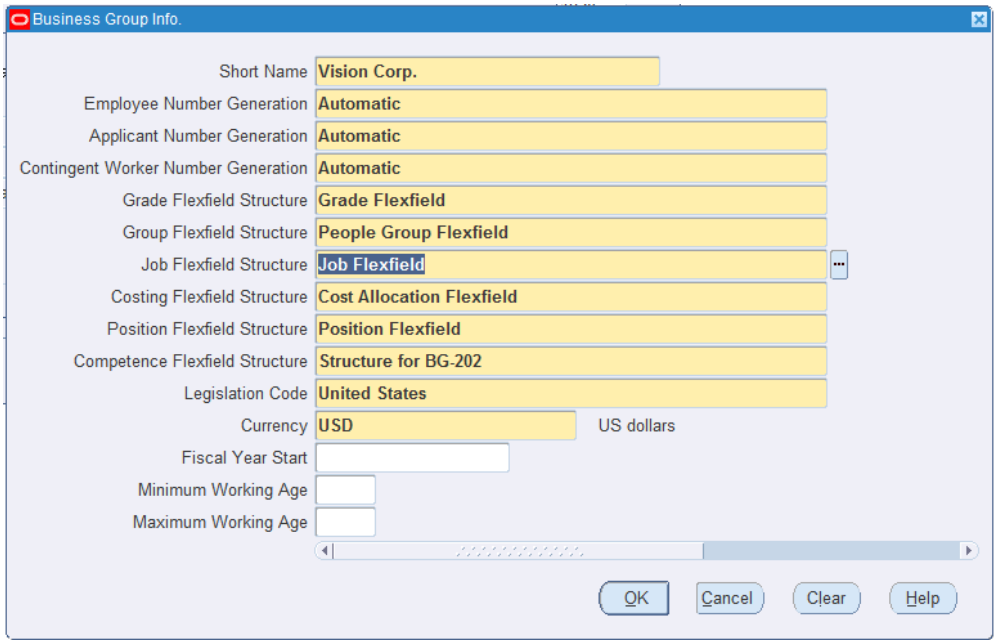
6. Place the cursor in the Business Group Info field.

Business Group Info Field in the Additional Organization Information Window



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.

Business Group Info Window



Step 1.3: Enabling the Qualifier for the Flexfield Segment

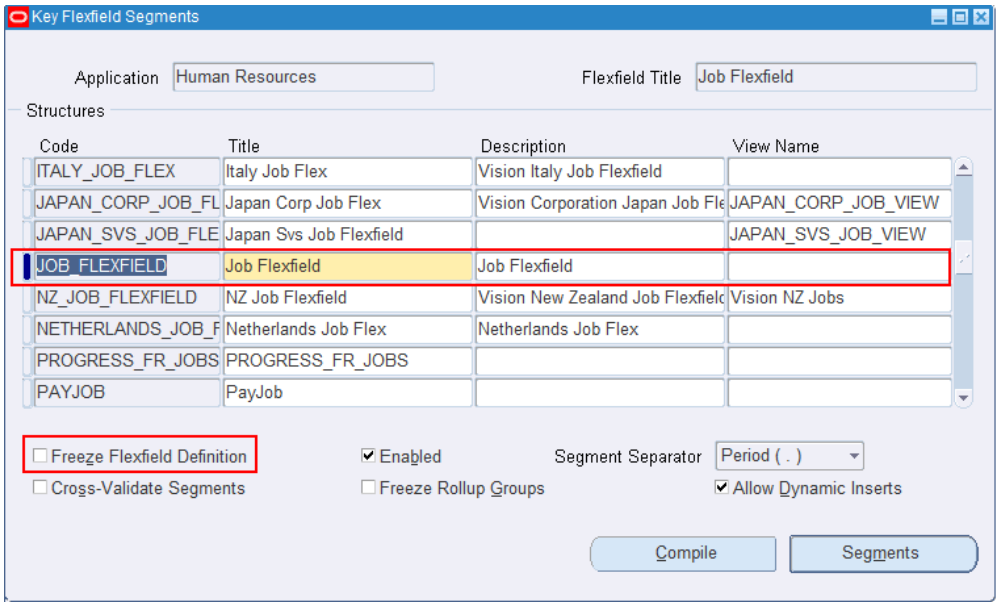
After obtaining the key flexfield structure name for your business group, perform the following steps to qualify the key flexfield segment:

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 9-49, such as "Job Flexfield".

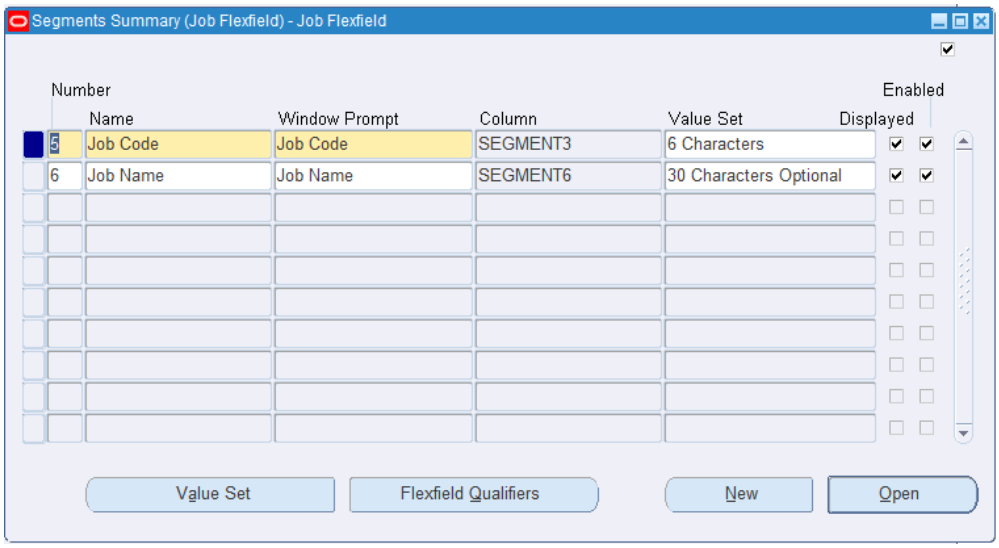
3. In the Structures region, select the Job Flexfield and then deselect the **Freeze Flexfield Definition** check box. This allows you to update the selected Job Flexfield definition. Click the **Segments** button. This displays the Segments Summary window for the selected Job Flexfield.

Key Flexfield Segments Window with "Freeze Flexfield Definition" Check Box Highlighted



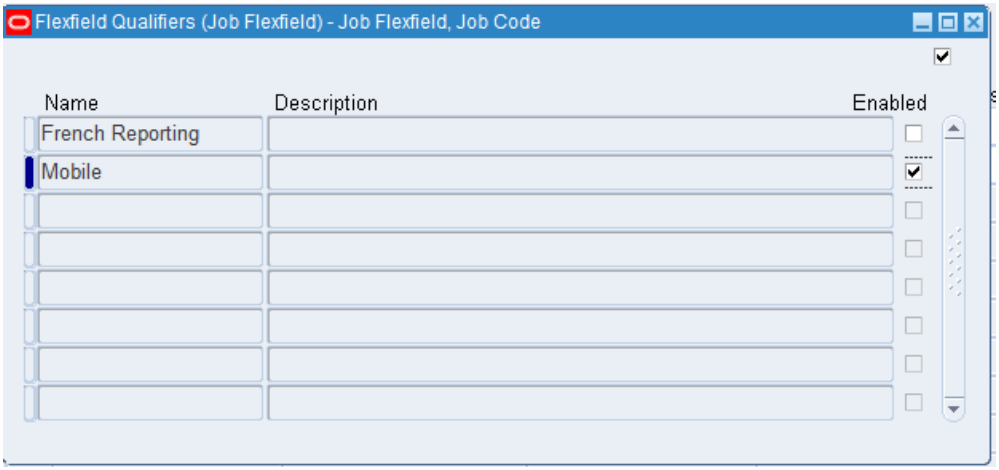
4. Select the segment you want to qualify and click the **Flexfield Qualifiers** button.

Segments Summary Window for Job Flexfield



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 Window with "Enabled" Selected for Segment "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:

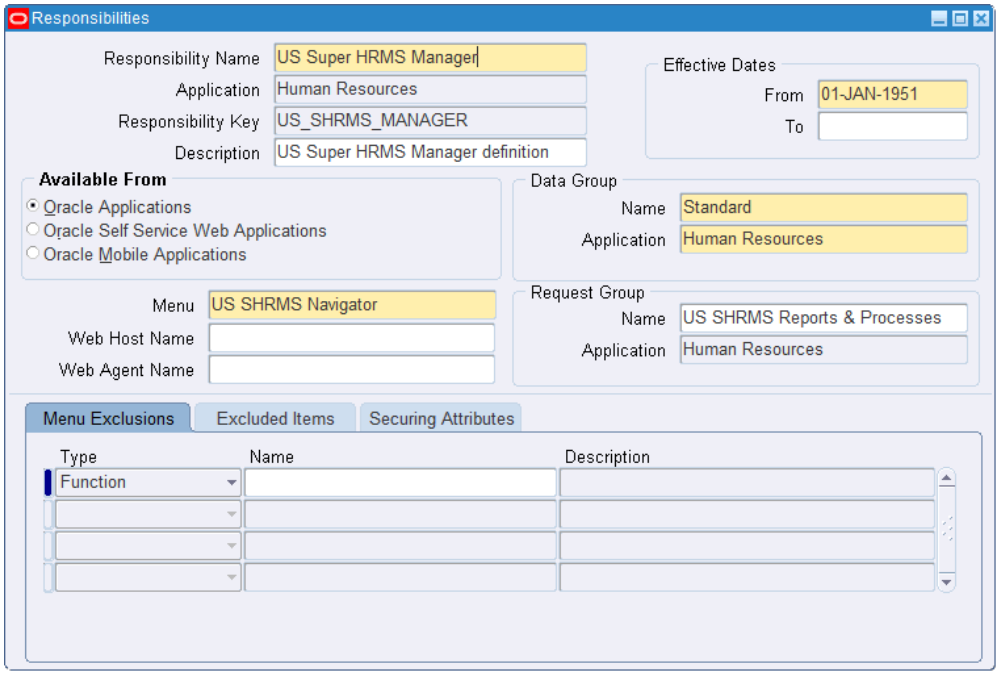
> **Note:** Ensure that you have applied the patches for your app. The "HR Mobile Utils Person Data Full Synch" concurrent program should then be automatically created.
>
> For patch information for each app, see Applying Prerequisite Patches, page 9-1.

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 Window



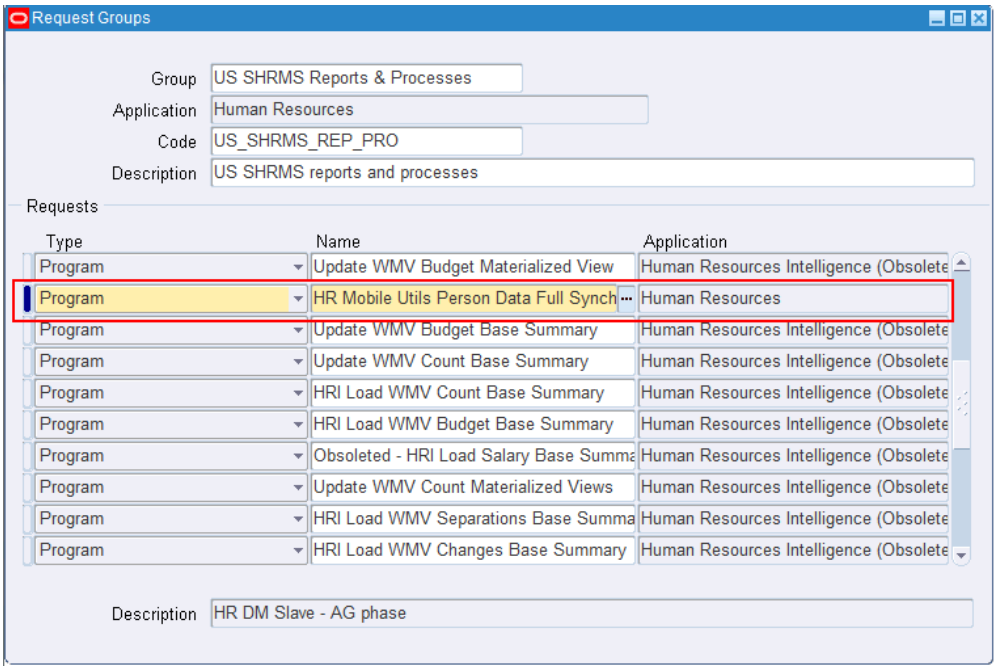
4. In the Request Group region, record the value of the request group Name field which in this example is "US SHRMS Reports & Processes" for the "US Super HRMS Manager" responsibility. Close the window.

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.

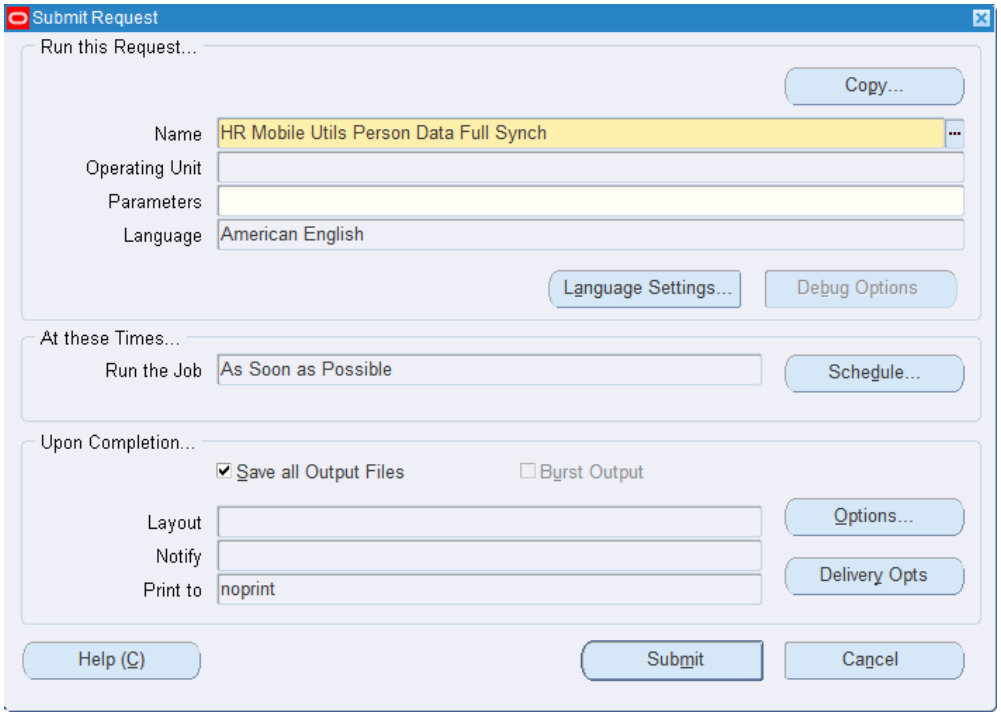
Request Groups Window for Adding the "HR Mobile Utils Person Data Full Synch" Concurrent Program



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

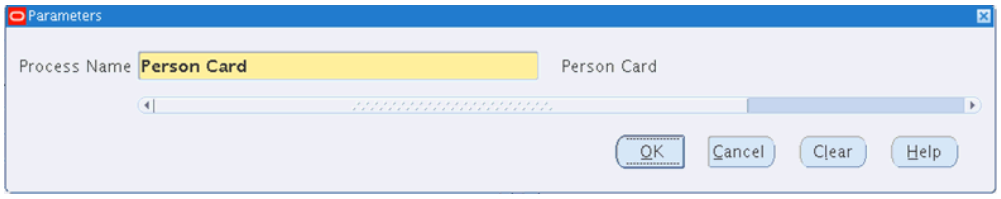
9. Enter the "HR Mobile Utils Person Data Full Synch" concurrent program as the request name.

Submit Request Window for Selecting the Concurrent Program



The Parameters window appears.

Parameters Window



10. Select "Person Card" as the Process Name parameter. Click **OK** and **Submit** to process 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 submitting the concurrent request for the first time, you can schedule the concurrent request to run at the desired frequency to refresh the related tables with the latest person data.

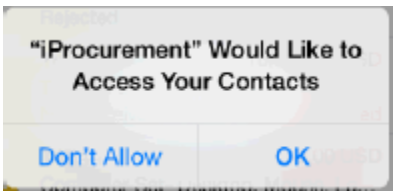
Step 3: Allowing Apps to Access Local Contacts

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:

Permission to Access Local Contacts Dialog Box



> **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.

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 shows a blank page with no data on it or the person contact details are not shown on the page.

For information on setting up person contact cards, see Setting Up Person Contact Cards, page 9-47.

Setting Up Maps

Mobile Apps Integrated with Maps

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

- Oracle Mobile Learning 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.

- Oracle Mobile Person Directory for Oracle E-Business Suite (Google Maps)
- Oracle Mobile Product Information for Oracle E-Business Suite (Google Maps)
- Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite (Google Maps)

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

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

Setting Up Google Maps

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

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*.

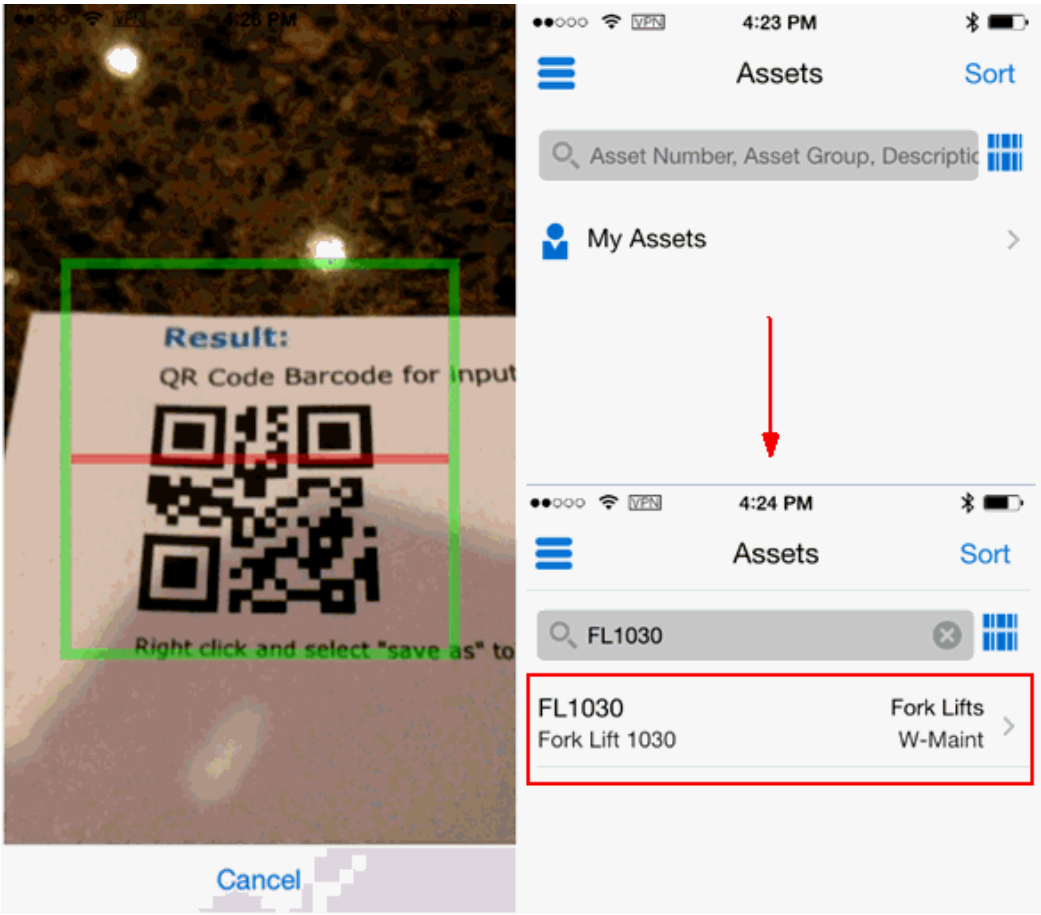
Support for Barcodes

Some Oracle E-Business Suite mobile apps provide support through the Cordova plug-in 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.

Data Captured and Shown in the Mobile Page Using Barcode Scanning



Mobile Apps Integrated with Barcodes

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

- Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite
- Oracle Mobile Discrete Quality Manager 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 Process Quality Manager for Oracle E-Business Suite
- Oracle Mobile Product Information for Oracle E-Business Suite
- Oracle Mobile Yard for Oracle E-Business Suite

- Oracle Mobile Supply Chain Applications for Oracle E-Business Suite

  Note: Although Oracle Mobile Supply Chain Applications for Oracle E-Business Suite is not developed based on Oracle E-Business Suite Mobile Foundation, the barcode information described in this section also applies to this app.

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 Discrete Production Supervisor for Oracle E-Business Suite
- Oracle Mobile Discrete Quality Manager for Oracle E-Business Suite
- Oracle Mobile Learning for Oracle E-Business Suite
- Oracle Mobile Maintenance for Oracle E-Business Suite (for the "Disconnected" functionality)
- Oracle Mobile Person Directory for Oracle E-Business Suite
- Oracle Mobile Product Information for Oracle E-Business Suite

- Oracle Mobile Sales Orders for Oracle E-Business Suite
- Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite
- Oracle Mobile Timecards 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.

Additional Setup for Deploying Mobile Apps with Enterprise Mobility Management Solutions

Starting from Oracle E-Business Suite Mobile Foundation 8.0, administrators can preconfigure Server URL in an Enterprise Mobility Management (EMM) console before deploying Oracle E-Business Suite mobile apps to users. These apps include:

- Standard apps installed from the Apple App Store or Google Play
- Apps provided to users through enterprise distribution
- Custom apps developed based on Oracle E-Business Suite Mobile Foundation

To enable this feature, administrators need to perform required setup tasks to preconfigure the Server URL that the apps will use to connect to Oracle E-Business Suite. Once the setup tasks are complete, app users no longer need to enter this URL manually after launching an app installed from an EMM's app catalog.

For information about integration with EMM solutions and the setup tasks to preconfigure the Server URL for mobile apps, see Integrating Oracle E-Business Suite Mobile Apps with Enterprise Mobility Management Solutions, page 15-1.

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 the *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 the *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>`

  Be aware of 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, Validating the Configuration, page 9-42.

  > **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 host name 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 host name. Refer to:
  >
  > - *Using Load-Balancers with Oracle E-Business Suite Release 12.2*, My Oracle Support Knowledge Document 1375686.1
  > - *Using Load-Balancers with Oracle E-Business Suite Release 12.0 and 12.1*, My Oracle Support Knowledge Document 380489.1

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.

> **Additional Information:** Please note that Oracle tests the client app and server patch combinations with `N-1` policy where `N` is the latest Oracle E-Business Suite mobile app release that contains both the corresponding client app version and the associated server patches. The latest client app version will work with the current version (`N`) and one previous version (`N-1`) of the server patches.
>
> The latest server-side patches must be applied to enable new features and fixes that require those patches. Oracle recommends that you define a plan to maintain the mobile server side on a regular basis that is aligned with the Oracle E-Business Suite mobile releases, if you are using the standard apps installed from public app stores.

For required patch information for each Oracle E-Business Suite Mobile Foundation release, refer to Applying Prerequisite Patches on the Oracle E-Business Suite Server, page 9-1.

- Where to get custom or self-signed certificates if required

  For information on using custom or self-signed certificates, see Using Custom or Self-signed Certificates with Oracle E-Business Suite Mobile Apps, page 13-3.

10

Setting Up Push Notifications for Mobile Apps

Overview

This chapter explains the concept and architecture of Oracle E-Business Suite Mobile Foundation Push Notification System (or the Push Notification System thereafter) and the required configuration tasks to enable this feature for the supported mobile apps. Specifically, this chapter includes the following topics:

Understanding Oracle E-Business Suite Mobile Foundation Push Notification System

What is a push notification?

Push notifications are messages that a server can send to the mobile devices to inform the mobile app users of some events. For example, when a new expense report is submitted to an approver for approval, the Oracle E-Business Suite server can send a push notification to the approver's mobile device where the Approvals mobile app is installed. This helps to inform the approver of the new expense report for timely approval. These notifications can appear as alerts or banners based on the state of the app and the notification settings.

Starting from Oracle E-Business Suite Mobile Foundation 7.0 and onwards, you can optionally set up and enable push notifications for supported Oracle E-Business Suite mobile apps.

Important: Push notifications are supported when using Oracle Mobile

Hub (OMH) or Oracle Mobile Cloud Service (MCS) in the following apps. Note that in addition to MCS, starting from Oracle E-Business Suite Mobile Foundation Release 9.0 and onwards, Oracle Mobile Hub provides support for push notifications through Patch 33404902:R12.FND.C for Oracle E-Business Suite 12.2, and Patch 33404902:R12.FND.B for Oracle E-Business Suite 12.1.3.

- Oracle Mobile Approvals for Oracle E-Business Suite, when provided to users through enterprise distribution

- Custom Oracle E-Business Suite mobile apps developed using the Login component from Oracle E-Business Suite Mobile Foundation

  See: Using the Login Component to Develop Mobile Apps, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

Standard Oracle E-Business Suite mobile apps installed directly from the Apple App Store or Google Play do not support push notifications.

Note that push notifications require enterprise distribution due to iOS requirements. The provisioning profile used to build the iOS app and the certificate and private key presented by the Oracle E-Business Suite server to send the push notifications are specific to the iOS app to be used in your organization; therefore, you must obtain your own profile and certificate from the Apple Developer Program. You can then use these to build and deploy the iOS app through enterprise distribution.

- For information on editing application bundle ID or package name in the platform-specific deployment profile, see Modifying an Existing Deployment Profile (Conditional), *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

- For information about enterprise distribution, see Using Mobile Application Archives for Enterprise Distribution, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

What is Oracle E-Business Suite Mobile Foundation Push Notification System?

In order for the Oracle E-Business Suite server to send push notifications to the mobile devices of designated mobile app users, the server must have a way to identify those users and to deliver the notifications whenever there is a need. To achieve this goal, Oracle E-Business Suite Mobile Foundation Push Notification System provides the underlying components allowing the supported mobile apps to register the mobile devices and receive push notifications.

Specifically, the Push Notification System contains the following essential components:

- **Push Notification Client - Login Component**

The Login component is used to develop the mobile apps and implement the ability to receive the push notifications from the server.

- **Push Notification Server**

  Push notification server contains the data model to store information about mobile users and the unique IDs (iOS push tokens and Android registration IDs) from their mobile apps to which push notifications should be sent, plus the components to send push notifications to the mobile apps.

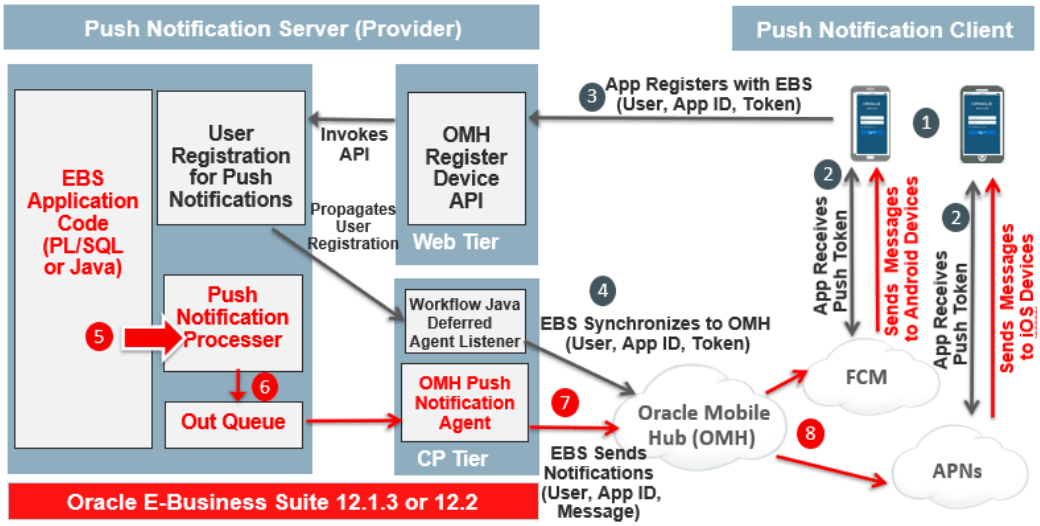
  Push notification server uses **Oracle Mobile Hub,** from Oracle E-Business Suite Mobile Foundation 9.0 and onwards, or **Oracle Mobile Cloud Service** to send the notifications. OMH or MCS serves as an intermediary between the push notification server and client to manage the device registrations as well as connect to the following platform-specific push notification services to send the notifications.

  - iOS - Apple Push Notification service (APNs)
  - Android - Firebase Cloud Messaging (FCM), new version of Google Cloud Messaging (GCM)

    Important: Oracle E-Business Suite Mobile Foundation Push Notification System requires Oracle Mobile Hub or Oracle Mobile Cloud Service subscription to enable push notifications for mobile apps. OMH or MCS handles platform-specific delivery of push notifications and provides monitoring and error handling capabilities for administrators. If you have already subscribed to OMH or MCS for your enterprise mobile app requirements, you can use the same subscription to enable push notifications for Oracle E-Business Suite. Otherwise, you must obtain a new OMH subscription to use push notifications. In order to use Oracle E-Business Suite Mobile Foundation Push Notification System, the OMH or MCS instance should be set up and registered with Oracle E-Business Suite Mobile Foundation. See: Setting Up an Oracle Mobile Hub or Oracle Mobile Cloud Service Instance, page 10-6.

To better understand these components and how the system works to deliver push notifications, the following diagram illustrates the high level architecture of the Push Notifications System:

Oracle E-Business Suite Mobile Foundation Push Notifications System High Level Architecture



Push notifications can be sent from the server to supported mobile apps using the following flows:

> **Note:** Although Oracle Mobile Hub (OMH) is used in this diagram to explain the architecture components, push notifications are supported when using Oracle Mobile Hub or Oracle Mobile Cloud Service.

- **A Mobile App Registers to Receive Push Notifications**

  In order for the Oracle E-Business Suite server to send push notifications to mobile devices, it needs a list of mobile users, the apps that those users have installed, and the unique IDs corresponding to the apps on each user's device where the notifications will be sent.

  - **Step 1:** A mobile user launches a mobile app.

  - **Step 2:** The mobile app connects to the corresponding platform's push notification service (APNs or FCM) to receive a unique ID known as a push token on iOS or registration ID on Android for that app.

    The unique ID is the address to which the push notification will be delivered. The mobile app registers that unique ID with the server from which it would receive push notifications. For example, the server sends iOS push notifications to APNs and Android push notifications to FCM.

  - **Step 3:** When the user signs in to the app, the mobile app invokes the Oracle E-Business Suite REST API called "Push Register" (`mPushRegister`) to register the push token or registration ID with Oracle E-Business Suite Mobile

Foundation for that user and the mobile app.

- **Step 4:** Oracle E-Business Suite invokes the OMH "Register Device" REST API (`/mobile/platform/devices/register`) to propagate the push token or registration ID from Oracle E-Business Suite to Oracle Mobile Hub through Workflow Java Deferred Agent Listener.

The same user can install the same app on multiple devices. A registration is created for each installation of the app to receive push notifications.

- **Oracle E-Business Suite Server Sends Push Notifications to Mobile Apps**

  Once the Oracle E-Business Suite server receives the list of users registered to receive push notifications, push notifications are delivered to the users.

  - **Step 5:** Oracle E-Business Suite application product code calls the PL/SQL API `FND_MBL_NOTIFICATION.Send` which internally raises the push notification business event to send a notification to the user of a given mobile app.

  - **Step 6:** The Push Notification System builds the notification payload targeted for that user and the app, and enqueues the payload to the FND_MBL_NOTIFICATION_OUT queue.

  - **Step 7:** Generic Service Component (GSC) OMH Push Notification Agent retrieves the push notification from the queue, builds the OMH payload, and delivers the payload to Oracle Mobile Hub using the "Notification" REST API `(/mobile/system/notifications/notifications/)` for the user.

  - **Step 8:** Oracle Mobile Hub delivers the notification to all registered devices for that Oracle E-Business Suite user through the corresponding platform's push notification service, such as APNs for iOS and FCM for Android.

  Note that Oracle E-Business Suite only delivers one push notification for the user of a given app to Oracle Mobile Hub. If the user had installed the same app on multiple devices, Oracle Mobile Hub delivers the same notification to all the devices for that user.

Setting Up and Enabling Push Notifications for Oracle E-Business Suite Mobile Apps

To set up the Push Notification System and enable the mobile apps, you need to perform the following setup tasks:

1. Setting Up a FCM Project for Android Push Notifications Only (Optional), page 10-6

2. Setting Up an Oracle Mobile Cloud Service Instance, page 10-6

3. Configuring Oracle E-Business Suite for Push Notifications, page 10-11

- Configuring Oracle E-Business Suite Mobile Foundation Push Notification System, page 10-11
- Configuring Supported Mobile Apps with Push Notifications, page 10-14

In addition to the above administrative tasks performed on the server, a mobile applications developer needs to complete the following tasks to implement push notifications for the supported mobile apps. For more information, refer to:

- Adding Push Notifications to App Configuration, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*
- Implementing Push Notifications, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*

For information on troubleshooting issues related to the setup or processing of push notifications, see Troubleshooting Tips for Push Notifications, page 16-25.

Setting Up a FCM Project for Android Push Notifications (Optional)

Android push notifications sent from Oracle E-Business Suite are delivered to Android devices through Firebase Cloud Messaging (FCM). In order for FCM to recognize the Oracle E-Business Suite server from where the notifications are sent and the Android apps that receive them, you are required to create a Firebase project.

Perform the following steps to set up a FCM project:

1. Go to the Firebase console (`https://console.firebase.google.com`) and create a project.
2. In the Project Settings, record the values of the Server Key and Sender ID for Cloud Messaging.

   You will use the Sender ID and Server Key you recorded here when creating the Android mobile client in Oracle Mobile Hub for Oracle E-Business Suite Mobile Foundation 9.0 and onwards or in Oracle Mobile Cloud Service. See: Creating Mobile Clients, page 10-7.

   You will use the same Sender ID when configuring the Push Notification System in the Mobile Push Notification Configuration page. See: Configuring Oracle E-Business Suite Mobile Foundation Push Notification System, page 10-11.

For more information, refer to the Firebase documentation at `https://firebase.google.com/docs/cloud-messaging/`.

Setting Up an Oracle Mobile Hub or Oracle Mobile Cloud Service Instance

In order for the Oracle E-Business Suite Mobile Foundation Push Notification System to

connect to Oracle Mobile Hub or Oracle Mobile Cloud Service to deliver push notifications, complete the following setup tasks on the Oracle Mobile Hub or the Oracle Mobile Cloud Service instance first:

> **Note:** You must use a single Oracle Mobile Hub or Oracle Mobile Cloud Service instance for a given Oracle E-Business Suite. If the instance is changed after the initial setup, the earlier registrations for Oracle E-Business Suite mobile apps will not be automatically synchronized.

1. Creating a Mobile Backend, page 10-7
2. Creating Mobile Clients, page 10-7
3. Creating an Oracle Mobile Hub or Oracle Mobile Cloud Service User Account, page 10-9
4. Enabling HTTP Basic Authentication, page 10-10

Creating a Mobile Backend

To create a mobile backend on the Oracle Mobile Hub or Oracle Mobile Cloud Service instance, perform the following tasks:

1. Log in to your Oracle Mobile Hub instance or your Oracle Mobile Cloud Service instance.
2. Create a mobile backend to be used specifically for Oracle E-Business Suite push notifications.

   For more information, refer to the following documents:

   - For Oracle Mobile Hub, see Backend in *Developing Applications with Oracle Mobile Hub* (https://docs.oracle.com/en/cloud/paas/mobile-hub/develop/index.html).
   - For Oracle Mobile Cloud Service, see Mobile Backends in *Using Oracle Mobile Cloud Service* (https://docs.oracle.com/en/cloud/paas/mobile-cloud/mcsua/index.html).

Creating Mobile Clients

In order for Oracle Mobile Hub or Oracle Mobile Cloud Service to deliver push notifications on behalf of the Oracle E-Business Suite Mobile Foundation Push Notification System, the Oracle E-Business Suite mobile apps to which push notifications should be delivered need to be registered on the Oracle Mobile Hub or Oracle Mobile Cloud Service instance.

1. Log in to your Oracle Mobile Hub or Oracle Mobile Cloud Service instance.

2. In your instance, click the menu icon to open the side menu.

   - For Oracle Mobile Hub, select **Development**, and then **Notification Profiles**. Create a client for each Oracle E-Business Suite mobile app distribution.

   - For Oracle Mobile Cloud Service, select **Application**, and then **Client Management**. Create a client for each Oracle E-Business Suite mobile app distribution.

   For example, if you would like to receive push notifications for both iOS and Android distributions of an enterprise-distributed Approvals app, you have to register one client each for each platform.

3. When creating a client, use correct Bundle ID or Package Name that has been used to deploy your mobile app.

   - Bundle ID (iOS): The Bundle ID registered with Apple to receive the iOS provisioning profile. This is the bundle ID used in the deployment profile to create the iOS app.

     For information on the platform-specific deployment profile, see Modifying an Existing Deployment Profile (Conditional), *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

   - Package Name (Android): The Package Name used in the deployment profile to create the Android app.

4. For each client, create a required push notification profile.

   - iOS: Use the APNs certificate issued by Apple.

   - Android: Use the values of Sender ID and Server Key you recorded earlier for the Firebase project.

     For information on obtaining the project number and the Server Key, see: Setting Up a FCM Project for Android Push Notifications Only (Optional), page 10-6.

5. Associate each client with the mobile backend that you created earlier for Oracle E-Business Suite.

   See: Creating a Mobile Backend, page 10-7.

For more information about client management, see the following documents:

- For Oracle Mobile Hub, see "Set Up a Mobile App for Notifications" section in "Notifications" chapter from *Developing Applications with Oracle Mobile Hub* (https://docs.oracle.com/en/cloud/paas/mobile-hub/develop/index.html).

- For Oracle Mobile Cloud Service, see Client Management in *Using Oracle Mobile Cloud Service* (https://docs.oracle.com/en/cloud/paas/mobilecloud/mcsua/index.html).

Creating an Oracle Mobile Hub or Oracle Mobile Cloud Service User Account

In order for the Oracle E-Business Suite Mobile Foundation Push Notification System to connect to Oracle Mobile Hub or Oracle Mobile Cloud Service to deliver push notifications, you should create a user account on Oracle Mobile Hub or Oracle Mobile Cloud Service, assign required roles to that account, and then configure it in the Push Notification System.

Steps to create an Oracle Mobile Hub user account:

Use the following steps to create an Oracle Mobile Hub user account:

1. Log in to Oracle Identity Cloud Service (IDCS) and click **Users** or click the **Users** tab in Oracle Cloud My Services.

2. Click **Add**.

3. Enter the first name and last name of the user in the corresponding fields.

   - If the user is going to log in with a user name, enter the user name in the User Name field and enter the user's email address in the Email field. Be sure to clear the **Use the email address as the user name** option, which makes the user name the same as the user's email address.

   - If the user is going to log in using an email address, make sure the **Use the email address as the user name** option is checked and enter the email address for the user account in the User Name/Email field.

4. Click **Next** if you want to assign the user to a group or click **Finish**. To assign a group, select the groups that you want to assign to this user account and click **Finish**.

5. From the Details page displayed for the new user, click the **Access** tab.

6. Search for your Mobile Hub mobile core application and click **Assign**.

For more information, see "Mobile Users and Roles" in *Developing Applications with Oracle Mobile Hub* (https://docs.oracle.com/en/cloud/paas/mobile-hub/develop/index.html).

Steps to create an Oracle Mobile Cloud Service user account:

Use the following steps to create an Oracle Mobile Cloud Service user account:

1. Log in to your Oracle Mobile Cloud Service instance.

2. Click the menu icon to open the side menu. Select **Application**, and then **Mobile User Management**.

3. Either create a new realm or use a default realm.

4. Create a user who will be used to register this backend with Oracle E-Business Suite.

5. Go to Oracle Cloud My Services, and select the **Users** page.

6. The user created in the backend appears with a default role associated with the MCS instance.

   For example, the default role is **Default (mcsinst_MobileEnvironment_Default_1_0_Realm)**.

7. Assign the "Mobile Notifications" role to this user.

   For example, the role is **mcsinst Mobile Notifications**.

These two roles described here are important for Oracle E-Business Suite to connect to this Oracle Mobile Cloud Service instance to deliver push notifications.

For more information, see Mobile User Management in *Using Oracle Mobile Cloud Service* (https://docs.oracle.com/en/cloud/paas/mobile-cloud/mcsua/index.html).

Enabling HTTP Basic Authentication

Oracle E-Business Suite uses the HTTP Basic authentication to connect to Oracle Mobile Hub or Oracle Mobile Cloud Service. Enable the HTPP Basic authentication and record required connection details for the Oracle Mobile Hub or Oracle Mobile Cloud Service instance to be registered in the Oracle E-Business Suite Mobile Foundation Push Notification System.

1. Log in to your Oracle Mobile Hub or Oracle Mobile Cloud Service instance.

2. Open the mobile backend you created earlier for Oracle E-Business Suite. Select the **Settings** page.

3. Under **Access Keys**, enable the "HTTP Basic" authentication by turning the switch to ON.

   When switched to ON, the access keys that you need are displayed.

4. Record the following information that will be used later in Configuring Oracle E-Business Suite Mobile Foundation Push Notification System, page 10-11.

   - Mobile Backend ID under HTTP Basic

   - Base URL under Environment URLs

- Username (created earlier)
- Password for this user

Once the setup is complete, you are ready to configure the Push Notification System to connect to Oracle Mobile Hub or Oracle Mobile Cloud Service.

Configuring Oracle E-Business Suite for Push Notifications

Besides the setup tasks on Oracle Mobile Cloud Service, you need to perform required configuration on Oracle E-Business Suite so that Oracle E-Business Suite can accept push notification registrations from mobile users and send push notifications to the registered devices. These setup tasks on Oracle E-Business Suite include:

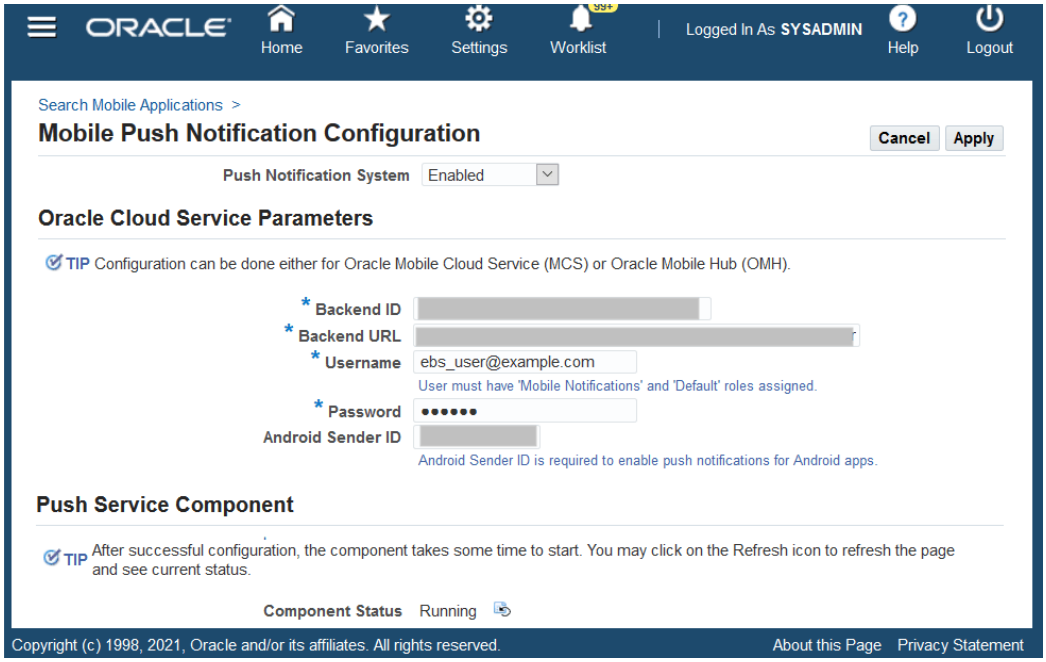
- Configuring Oracle E-Business Suite Mobile Foundation Push Notification System, page 10-11
- Configuring Supported Mobile Apps with Push Notifications, page 10-14

Configuring Oracle E-Business Suite Mobile Foundation Push Notification System

To configure the Push Notification System from Oracle E-Business Suite Mobile Foundation, select the **Mobile Applications Manager** responsibility and choose the **Applications** link from the navigator. The Search Mobile Applications page appears.

Click **Push Configuration** on the upper right corner to access the Mobile Push Notification Configuration page.

Mobile Push Notification Configuration Page



Perform the following tasks to configure the Push Notification System and required component parameters:

1. Specify the following information to enable the Push Notification System:

   - **Push Notification System:** Enabled

2. In the Oracle Cloud Service Parameters region, enter the following information:

   > **Note:** For the Backend ID, URL, Username, and Password fields, use the information you recorded earlier while enabling the HTTP Basic authentication in Oracle Mobile Cloud Service or Oracle Mobile Hub, see: Enabling HTTP Basic Authentication, page 10-10.

   - **Backend ID:** Enter the value that you recorded earlier when creating the backend for Oracle E-Business Suite push notifications.

     See: Creating a Mobile Backend, page 10-7.

   - **Backend URL:** Specify the desired URL for Oracle Mobile Cloud Service or Oracle Mobile Hub.

   - **Username:** Enter the Oracle Mobile Cloud Service or Oracle Mobile Hub user who has appropriate notification user roles.

The username credentials are used by the Push Notifications System to connect to Oracle Mobile Cloud Service or Oracle Mobile Hub to register devices and send push notifications. The user must have the following roles assigned:

- Mobile Notifications (`mcsinst Mobile Notifications`)
- Default (`mcsinst_MobileEnvironment_Default_1_0_Realm`)

If the credentials are invalid or if required roles are not granted to the user in Oracle Mobile Cloud Service or Oracle Mobile Hub, the configuration will fail.

For information on creating a mobile user with credentials, see: Creating an Oracle Mobile Hub or Oracle Mobile Cloud Service User Account, page 10-9.

- **Password:** Enter the associated user password.
- **Android Sender ID:** Enter the Sender ID used to create the Android push notification profile when creating the Android client in Oracle Mobile Cloud Service or Oracle Mobile Hub. See: Creating Mobile Clients, page 10-7.

  Note: Sender ID is used to register the Android client in Oracle Mobile Cloud Service or Oracle Mobile Hub; Android Sender ID is used in the Mobile Push Notification Configuration page here. These two values should be the same.

  Android Sender ID is downloaded to Oracle E-Business Suite Android mobile apps through the configuration service. Android apps then use this Android Sender ID to register for push notifications with FCM.

  See: Setting Up a FCM Project for Android Push Notifications Only (Optional), page 10-6.

3. In the Push Service Component region, notice the following information:
   - **Component Status:** This displays the current component status, such as Running.
4. Click **Apply** to save the configuration.

In order for the Push Notification System to work correctly, the following Service Components should be running.

- Workflow Java Deferred Agent Listener - Processes business events to synchronize device registrations for push notifications from Oracle E-Business Suite to Oracle Mobile Cloud Service or Oracle Mobile Hub.
- Push Notification Provider - Processes push notifications triggered by Oracle E-Business Suite application code to its corresponding mobile app. It connects to

Oracle Mobile Cloud Service or Oracle Mobile Hub to send the push notifications.

Log in to Oracle E-Business Suite as a user who has the **System Administrator** responsibility. Select the **Oracle Applications Manager** link, and then **Workflow Manager** to ensure these two components are running.

Configuring Supported Mobile Apps with Push Notifications

After the setup for the Push Notification System is complete, it is important to configure each supported mobile app that should receive push notifications from the Oracle E-Business Suite server.

> **Important:** Starting from Oracle E-Business Suite Mobile Foundation Release 7.0 and onwards, push notifications are supported in the following apps when using Oracle Mobile Cloud Service or using Oracle Mobile Hub, from Release 9.0 when an appropriate patch is applied:
>
> - Oracle Mobile Approvals for Oracle E-Business Suite, when provided to users through enterprise distribution
> - Custom Oracle E-Business Suite mobile apps developed using the Login component from Oracle E-Business Suite Mobile Foundation
>
> Standard Oracle E-Business Suite mobile apps installed directly from the Apple App Store or Google Play do not support push notifications.

> **Note:** If an app can be enabled with push notifications, during the app registration, a developer can define the application definition metadata by adding the "Push Notifications" category along with the relevant parameters in the Configuration Details page for the app. See: Registering Your Mobile App, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.
>
> After the registration, you can enable the app and update the push notifications parameters if desired in the Configure Mobile Applications page.

Perform the following steps to configure a mobile app that supports push notifications:

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.

   The Search Mobile Applications page appears.

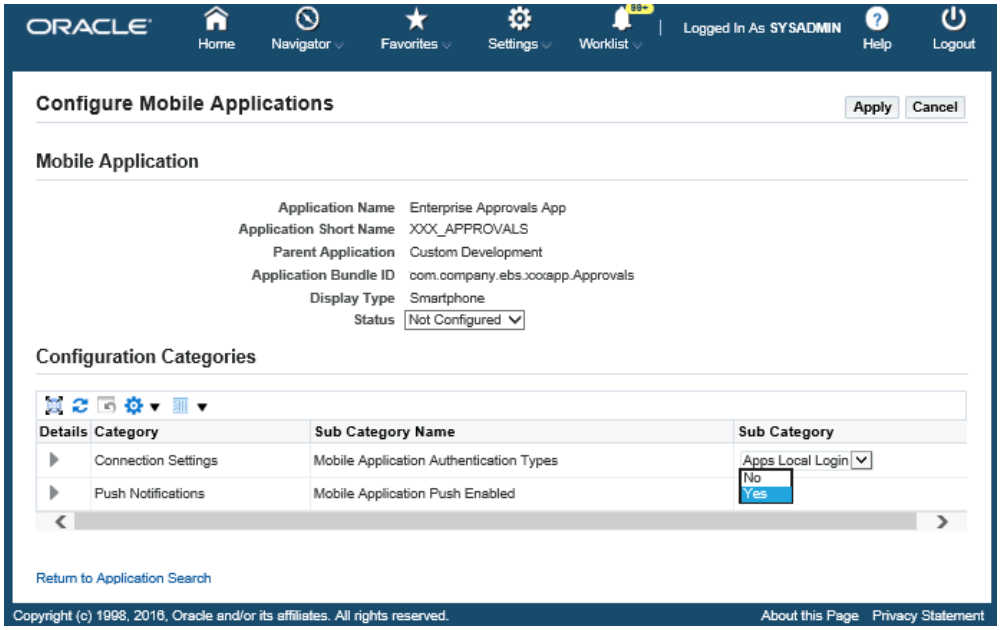
3. Search for the app that supports push notifications. For example, select the enterprise-distributed Approvals app called XXX_APPROVALS.

4. Click the **Configure** icon for the selected app XXX_APPROVALS that you want to configure with push notifications from the search result table.

   The Configure Mobile Applications page appears.

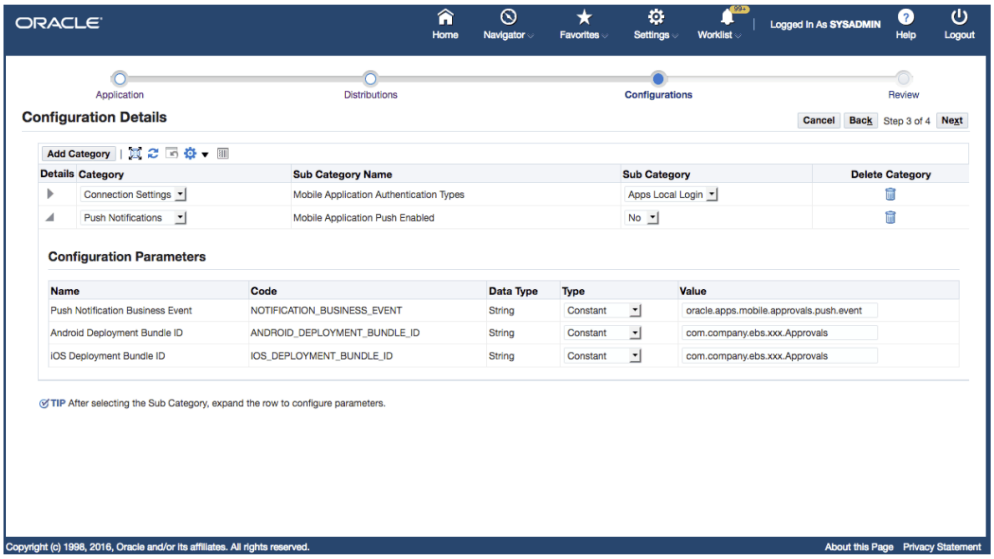
5. Select **Yes** for the "Push Notifications" category.

Configure Mobile Applications Page with "Push Notifications" Selected



6. Expand the "Push Notifications" category by clicking the **Details** icon. Enter the following values:

Configuration Details Page to Configure Parameters for Push Notifications



- **iOS Deployment Bundle ID (IOS_DEPLOYMENT_BUNDLE_ID):** Enter the same bundle ID used to create the iOS client on Oracle Mobile Cloud Service or Oracle Mobile Hub for this selected mobile app.

- **Android Deployment Bundle ID (ANDROID_DEPLOYMENT_BUNDLE_ID):** Enter the same Package Name used to create the Android client on Oracle Mobile Cloud Service or Oracle Mobile Hub for this selected mobile app.

- **Push Notifications Business Event (NOTIFICATION_BUSINESS_EVENT):** Enter the app-specific business event used to trigger push notifications when the event is raised. For example, enter `oracle.apps.mobile.approvals.push.event` for the enterprise-distributed Approvals app.

  This business event along with other app-specific events are included in an event group called `oracle.apps.mobile.foundation.push.group`. Oracle E-Business Suite Mobile Foundation uses the event group that has the default event subscription to process the push notifications.

7. Save your mobile app configuration.

Additionally, after configuring the mobile app, you can invoke the configuration service corresponding to that mobile app and confirm the following values:

- Android Sender ID

  This value is the same as the following:

  - Sender ID: It is used to create the Android push notification profile in Oracle

Mobile Cloud Service or Oracle Mobile Hub. See: Creating Mobile Clients, page 10-7.

- Android Sender ID: It is used to set up the Oracle E-Business Suite Mobile Foundation Push Notification System. See: Configuring Oracle E-Business Suite Mobile Foundation Push Notification System, page 10-11.

- Push Status

  This should be ENABLED for the mobile app to successfully receive push notifications.

For information on invoking the configuration service, see Validating the Configuration, page 9-42.

11

Administering the Mobile Apps

Overview

This chapter describes various administrative tasks that you would perform to better understand how your app is currently installed and used. It includes the following topics:

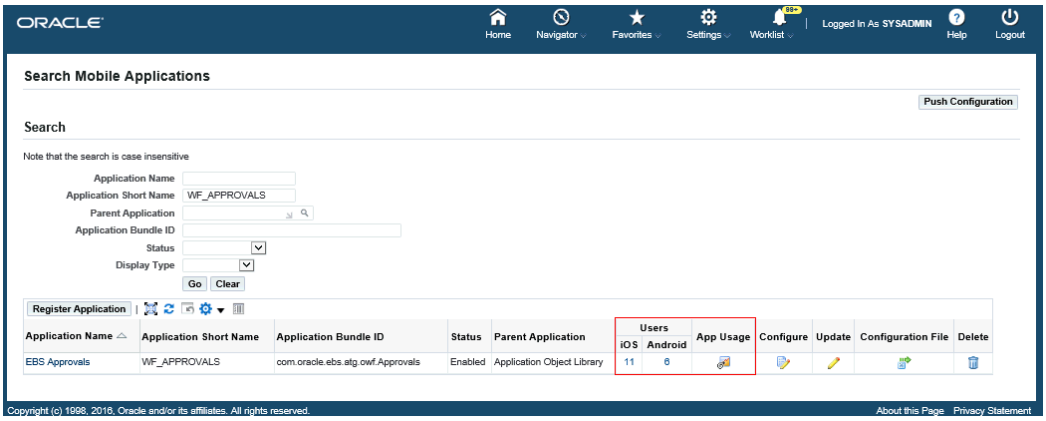
Viewing Mobile App Installation and Usage Metrics

Once users start using mobile apps, it is highly beneficial for administrators to gather statistics on these apps. These statistics include platform-specific user installations and usage frequencies over a period of time for any app. Users who have the Mobile Applications Administrator role can obtain this essential information through the Mobile Applications Manager UI pages and provide needed support for their users more efficiently.

> **Note:** These features are available from Oracle E-Business Suite Mobile Foundation Release 5.0 and are only available for users who have the Mobile Applications Administrator role. Users who have the Mobile Applications Developer role cannot find the Users and App Usage columns from the search result table.

To view user installations and usage metrics for an app, select the **Mobile Applications Manager** responsibility and choose the **Applications** link from the navigator. The Search Mobile Applications page appears.

Search Mobile Applications Page with Mobile App Installation and Usage Information Highlighted



Perform the following tasks to view user installation and app usage information:

- Click the number of users link for iOS or Android to view the installation information for a desired app.

  See: Viewing Your Mobile App Installation Details, page 11-2.

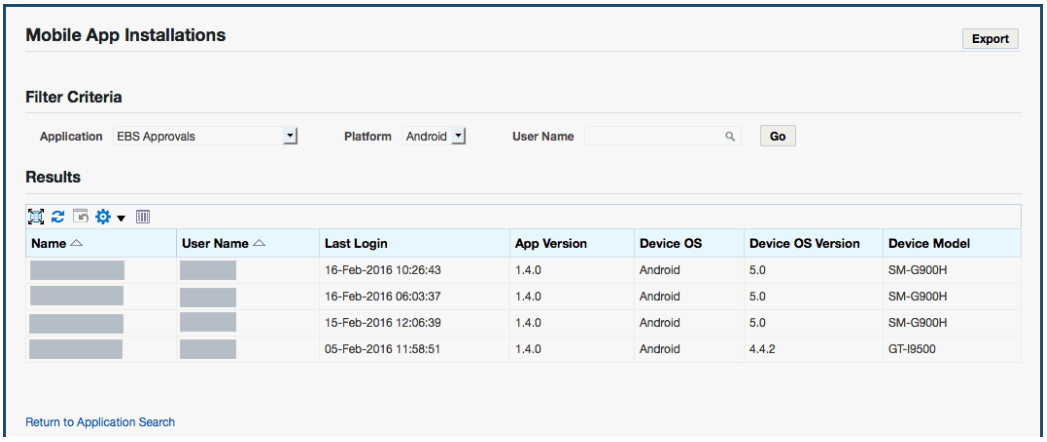
- Click the **App Usage** icon to view the mobile usage information.

  See: Viewing Your Mobile App Usage, page 11-4.

Viewing Your Mobile App Installation Details

To view user installation information for a specific app (such as "EBS Approvals"), after locating the app in the Search Mobile Applications page, click the number of users link for iOS or Android in the Users column from the search result table. The Mobile App Installations page appears with the installation details for your selected app, such as "EBS Approvals".

Mobile App Installations Page



The installation details include the name of the users who have installed the app (such as "EBS Approvals"), last login date and time, app version, device or platform information (either iOS or Android, depending on your selection from the Users column in the search result table), device OS version, and device model information (such as iPhone, iPad, or Android).

In the Filter Criteria region, you can further refine the result by modifying the following fields for the same app or obtain the information for a different app.

- **Application:** This field is automatically displayed with your selected app name from the search result table.

  If you want to view the user installations for a different app, select a desired app from the Application drop-down menu.

- **Platform:** Either iOS or Android is selected automatically based on your selection from the search result table in the Search Mobile Applications page.

  You can select a different value, including "iOS", "Android", or "All", to view the platform-specific user installations for the selected app.

  If "All" is selected, then the user installation information for both iOS and Android are displayed.

- **User Name**: Specify a desired user name if you want to view the installation for that user.

You can click **Export** to export all the data to an Excel spreadsheet if desired.

Click the **Return to Application Search** link to return back to the Search Mobile Applications page.

For information on viewing app usage information, see Viewing Your Mobile App Usage, page 11-4.

Viewing Your Mobile App Usage

To view the usage pattern for an app in terms of number of logins in the last few days or hours, click the **App Usage** icon from the search result table in the Search Mobile Applications page. The Mobile App Usage page appears for your desired app.

Mobile App Usage Page

In the Filter Criteria region, enter the following information to view the app usage information:

- **Application:** This field is automatically displayed with your desired app name.

  Select a different name if you want to view the usage information for another app.

- **Range:** Enter a numeric number in the text box as the time range, and select a desired range unit, such as "hours" or "days". For example, obtain the number of logins for an app within the last 47 hours or the last 24 days.

  Please note that if "hours" is selected as the range unit, the number you specify in the text box should be less than "48" hours. Otherwise, an error message appears.

After you modify the filter criteria and click **Go**, the app usage information is displayed in a table with the app login date and login count.

To export the data to an Excel spreadsheet, click **Export**.

Click the **Return to Application Search** link to return back to the Search Mobile Applications page.

You can purge the app usage data if needed, see Purging Mobile App Usage Information, page 11-5.

For information on viewing user installations for an app, see Viewing Your Mobile App Installation Details, page 11-2.

Purging Mobile App Usage Information

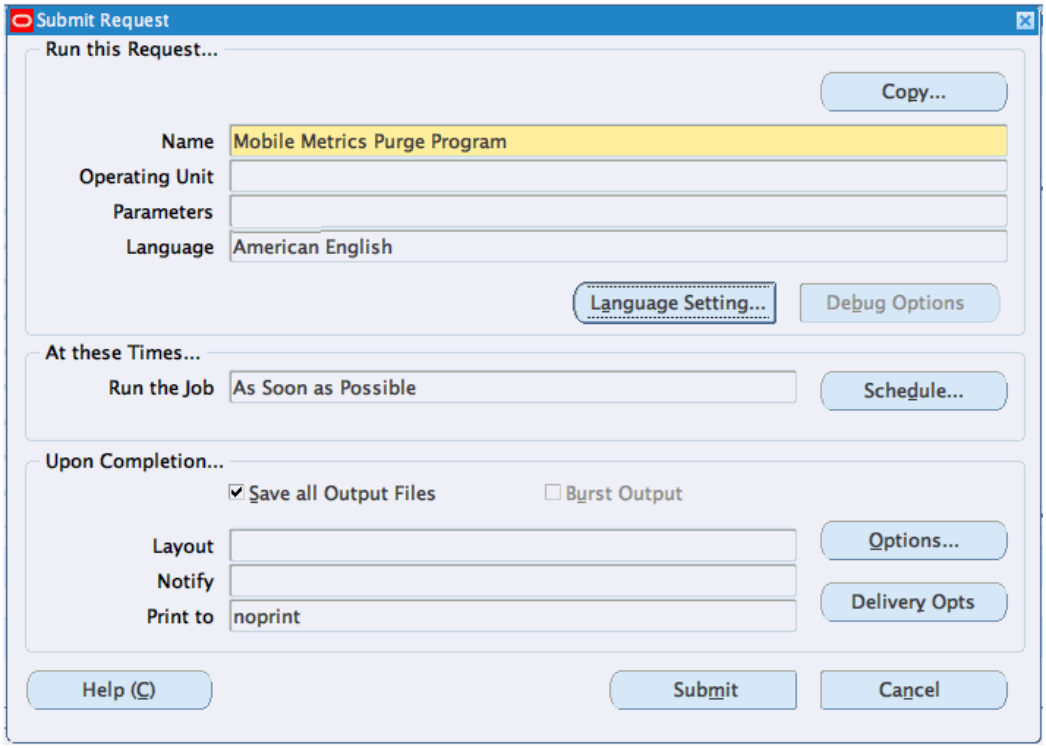
Oracle E-Business Suite mobile apps allow you to purge app usage data stored in the database that has been collected for a period of time. This can be achieved through a concurrent program called "Mobile Metrics Purge Program".

> **Important:** The "Mobile Metrics Purge Program" only purges the mobile app usage data. The data for user installations will not be purged.

To access this concurrent program, log in to Oracle E-Business Suite as a user who has the **System Administrator** responsibility. Select **Concurrent**, and then **Requests** from the navigation menu.

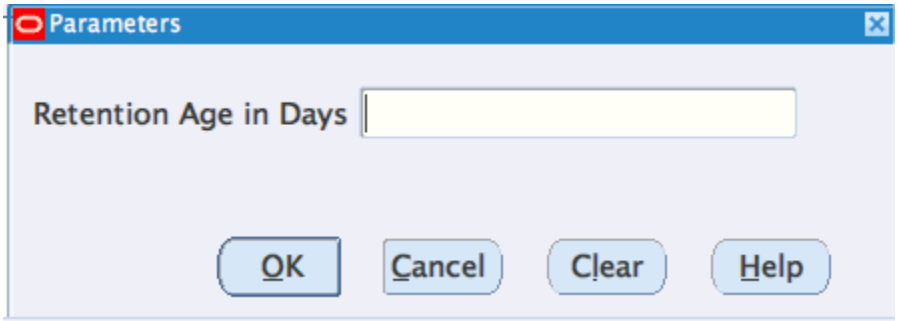
In the Submit Request window, select "Mobile Metrics Purge Program" as the Name from the drop-down list.

Submit Request Window with "Mobile Metrics Purge Program" Concurrent Program Selected



After you select "Mobile Metrics Purge Program" as the concurrent program name, the Parameters window appears. Specify a number of days in the Retention Age in Days field to indicate the desired days that you intend to retain the data. All the app usage data that is older than the specified days will be purged.

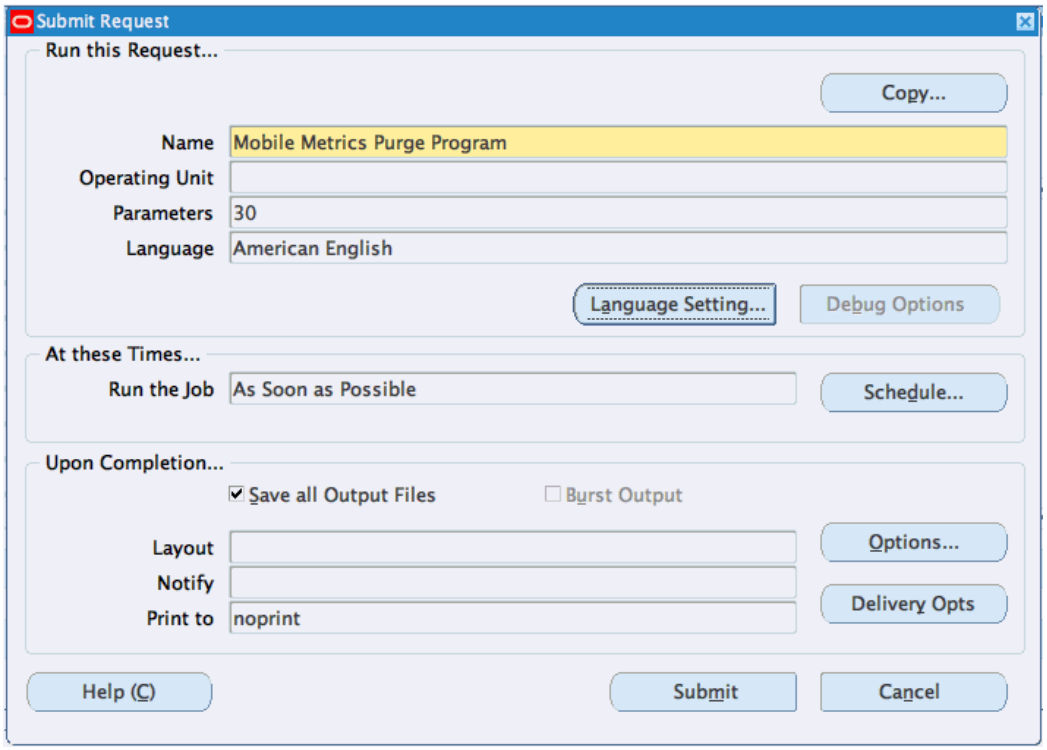
Parameters Window



For example, if you desire to keep the data within the last 30 days, then enter "30" in the Retention Age in Days field. The app usage data stored in the database older than the last 30 days will be removed, but the data for user installations remains intact and will not be purged.

After you specify the information in the Parameters window and click **OK**, the specified number of days, such as "30", is automatically displayed in the Parameters field.

Submit Request Window with Required Parameters



Click **Submit** to submit your concurrent request and start the process of purging the app usage data based on the specified parameter.

12

Advanced Configurations for Demilitarized Zone

Overview

If your mobile users need to access Oracle E-Business Suite mobile apps over the Internet, your Oracle E-Business Suite environment must be set up in a demilitarized zone (DMZ) configuration.

To set up Oracle E-Business Suite mobile apps in a DMZ configuration, ensure that you complete the following required tasks:

> **Important:** Before setting up your mobile app with any of the advanced configurations, ensure basic mobile app configuration is performed and validated. See: Validating the Configuration, page 9-42.
>
> Additionally, before connecting the mobile app using DMZ configuration, ensure that the app works with Service Endpoint (APPS_MOBILE_AGENT) set to an internal server of Oracle E-Business Suite. For information on the Service Endpoint (APPS_MOBILE_AGENT) parameters, see Configuring Parameters for the Apps Local Login Authentication Type, page 9-29.

1. **Common Tasks for DMZ Configuration (Prerequisite Tasks)**

   This section describes the common tasks for setting up Oracle E-Business Suite in a DMZ configuration, even if Oracle E-Business Suite mobile apps are currently not used. In other words, you need to complete these tasks that serve as prerequisites for configuring Oracle E-Business Suite mobile apps if mobile users need to access the apps in a DMZ configuration.

   See: Setting Up Oracle E-Business Suite Environment in a DMZ Configuration, page 12-2.

2. **Mobile Apps Specific Setup Tasks for DMZ**

   After completing the common or prerequisite tasks for configuring Oracle E-Business Suite in a DMZ, you can perform additional setup tasks specifically for Oracle E-Business Suite mobile apps.

   See: Mobile Specific Setup Tasks for DMZ, page 12-2.

Setting Up Oracle E-Business Suite Environment in a DMZ Configuration

Before performing mobile app specific setup tasks, you need to ensure Oracle E-Business Suite is in a DMZ configuration.

- 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 9-44, 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 My Oracle Support 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.

Mobile Specific Setup Tasks for DMZ

Once your Oracle E-Business Suite environment is configured with DMZ, when setting up the configuration file for your mobile app, ensure that the value of the Service

Endpoint parameter 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 Pages, page 2-18.

> **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 Service Endpoint parameter to set it to the external web entry point.

13

Advanced Configurations for Secure Communication with HTTPS

Overview

Oracle E-Business Suite mobile apps support the HTTPS protocol for certificates from commercial Certificate Authority (CA) vendors, as well as custom or self-signed certificates. This support is based on capability provided by Oracle Mobile Application Framework (Oracle MAF).

To enable TLS in Oracle E-Business Suite mobile apps, ensure that you complete the following required tasks:

> **Important:** Before setting up your mobile app with any of the advanced configurations, ensure basic mobile app configuration is performed and validated. See: Validating the Configuration, page 9-42.

1. **Common Tasks for Enabling TLS in Oracle E-Business Suite (Prerequisite Tasks)**

   This section describes the common setup tasks for enabling TLS in Oracle E-Business Suite. These tasks serve as prerequisites for configuring Oracle E-Business Suite mobile apps for TLS connections.

   See: Setup Tasks for Enabling TLS in Oracle E-Business Suite, page 13-2.

2. **Mobile Apps Specific Setup Tasks for TLS Connections**

   After completing the common or prerequisite tasks for enabling TLS in Oracle E-Business Suite, you can perform additional setup tasks specifically to enable TLS connections for Oracle E-Business Suite mobile apps.

   See: Mobile Specific Setup Tasks for TLS Connections, page 13-2.

Setup Tasks for Enabling TLS in Oracle E-Business Suite

Oracle E-Business Suite mobile apps built with Oracle E-Business Suite Mobile Foundation Release 6.0 or later support TLS 1.2 only and TLS 1.2 with backward compatibility (recommended). Before performing setup tasks for mobile apps, ensure your Oracle E-Business Suite environment is TLS enabled.

For information on enabling TLS 1.2 only and TLS 1.2 with backward compatibility in Oracle E-Business Suite, see:

- For Oracle E-Business Suite Release 12.1, see My Oracle Support Knowledge Document 376700.1, *Enabling TLS in Oracle E-Business Suite Release 12.1*.
- For Oracle E-Business Suite Release 12.2, see My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.

Please note that Oracle E-Business Suite mobile apps built with Oracle E-Business Suite Mobile Foundation Release 5.0 only support TLS 1.0.

Mobile Specific Setup Tasks for TLS Connections

Once your Oracle E-Business Suite is TLS enabled, you can perform the following additional setup tasks and validation to ensure successful TLS connections for mobile apps.

> **Note:** Prior to Oracle E-Business Suite Mobile Foundation Release 9.0, if your mobile apps are deployed on Android 5 devices, you must apply Oracle Fusion Middleware January 2017 Oracle Critical Patch Updates (minimum requirement) (see Document 2203916.1) to bring the required TLS (Transport Layer Security) version and negotiation support for TLS-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. See My Oracle Support Knowledge Document 376700.1.
> - For Oracle E-Business Suite 12.2, apply appropriate Oracle Fusion Middleware 11.1.1.9 patches. See My Oracle Support Knowledge Document 1367293.1.

- Using Public Certificates with Oracle E-Business Suite Mobile Apps, page 13-3
- Using Custom or Self-signed Certificates with Oracle E-Business Suite Mobile Apps, page 13-3
- Validating and Testing the TLS Handshake, page 13-5

Using Public Certificates with Oracle E-Business Suite Mobile Apps

Public certificates are included within Application Resource Security cacerts file. Oracle MAF recognizes only commercial CA-issued TLS certificates.

- For a list of certificates supported by Oracle MAF, see Migrating to New cacerts File for SSL in MAF 2.x.x, *Installing Oracle Mobile Application Framework*.

  For example, for Oracle E-Business Suite mobile apps built with Oracle E-Business Suite Mobile Foundation Release 9.1, refer to the following certificates information, plus the migration note specifically for this release:

  - Migrating to New cacerts File for SSL in MAF 2.6.0, *Installing Oracle Mobile Application Framework*

  - Oracle Mobile Application Framework 2.6.3 Migration Notes (from MAF 2.6.2) (https://www.oracle.com/application-development/technologies/maf/maf263migration.html)

  For the apps built with the MAF version earlier than 2.6.3, locate the Oracle MAF documentation from "Previous releases of Oracle Mobile Application Framework Documentation" (https://www.oracle.com/application-development/technologies/maf/maf-prev-rel.html).

- For information on the Oracle MAF version required for your mobile app, see *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*, My Oracle Support Knowledge Document 1641772.1, and Section 1: Oracle E-Business Suite Mobile Foundation Release Update History in *Oracle E-Business Suite Mobile Foundation Release Notes*, My Oracle Support Knowledge Document 1642431.1.

- For more information on mobile security, refer to Securing MAF Applications, *Developing Mobile Applications with Oracle Mobile Application Framework*.

Using Custom or Self-signed Certificates with Oracle E-Business Suite Mobile Apps

Mobile users can dynamically add custom CA or self-signed server certificates to the standard Oracle E-Business Suite mobile apps downloaded from the Apple App Store or Google Play for TLS connections to Oracle E-Business Suite, starting with Oracle E-Business Suite Mobile Foundation Release 7.0 and onwards.

Importing Certificates Dynamically for Standard Oracle E-Business Suite Mobile Apps

Perform the following steps to import certificates after a standard app is installed:

1. Save the custom CA or self-signed certificate file in binary format (DER), for example, `<ca-cert-filename>.cer`.

> **Note:** Use keytool or an appropriate tool to view the contents of the certificate file `<ca-cert-filename>.cer` and confirm that the file is the correct self-signed or custom CA certificate for the Oracle E-Business Suite environment. If the correct certificate for the Oracle E-Business Suite environment is not imported to the app, then the app user cannot connect to the Oracle E-Business Suite server.

2. Change the extension of the certificate file to `<ca-cert-filename>.servercert`.
3. Upload the certificate file to an internal server where your mobile users can access from their mobile devices.
4. Ask your mobile users to install required Oracle E-Business Suite mobile apps.
5. Open the certificate file from the internal server using the mobile device's web browser.
   - For iOS devices, use Safari web browser to open the certificate file.
   - For Android devices, use Chrome web browser to open the certificate file.
6. When prompted, select the Oracle E-Business Suite mobile app to open the certificate file with so that it is imported into that app.
7. Restart the app and connect to Oracle E-Business Suite.
8. Repeat the tasks from step 5 to step 7 for each Oracle E-Business Suite mobile app that should connect to that server.

> **Note:** For Oracle Mobile Learning for Oracle E-Business Suite, apart from importing the certificate with extension `.servercert` to the app, download and install the original certificate `<ca-cert-filename>.cer` to the device's user truststore (not system truststore) in order to play the course content.

Importing Certificates to cacerts for Enterprise-distributed Mobile Apps

You need to create a custom version of an app through enterprise distribution and import additional root-CA certificates into to the MAF application's truststore. The app is distributed through your enterprise's own site, rather than through a public app store.

For more information on setting up environment for enterprise distribution, see Importing Additional Root-CA Certificates (Optional), *Oracle E-Business Suite Mobile*

Apps Developer's Guide, Release 12.1 and 12.2.

Validating and Testing the TLS Handshake

Use the following steps to validate if your mobile app can perform a successful TLS handshake with the Oracle E-Business Suite TLS endpoint:

1. Validate that the JDK 8 client can connect to the Oracle E-Business Suite TLS 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 TLS endpoint.

      If HTML content is returned as the result after you run these commands, then the TLS handshake is successful. If the following exceptions appear instead, then the TLS certificate on the server is not recognized by the JDK 8 client. You

need to configure the Oracle E-Business Suite TLS endpoint with a server certificate issued by a commercial CA, as listed in Migrating to New cacerts File for SSL in MAF 2.x.x, *Installing Oracle Mobile Application Framework*.

> **Note:** For information on the Oracle MAF version required for your mobile app, see Section 1: Oracle E-Business Suite Mobile Foundation Release Update History, *Oracle E-Business Suite Mobile Foundation Release Notes*, Oracle Support Knowledge Document 1642431.1.

```
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 TLS endpoint presents the complete certificate chain.

   Please note that even if the Oracle E-Business Suite TLS endpoint is configured with a certificate from a commercial CA, the TLS 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 TLS 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.x.x, *Installing Oracle Mobile Application Framework*.

3. Ensure that you not only configure the server certificate, but also provide the certificates of any intermediate CAs.

14

Advanced Configurations for Single Sign-On

Overview

Single sign-on (SSO) across Oracle E-Business Suite mobile apps when authenticating a user from a mobile device is not currently supported even if you have integrated Oracle E-Business Suite with Oracle Access Manager for single sign-on. If the mobile device has multiple Oracle E-Business Suite mobile apps, then it is required to re-authenticate the user by providing user login credentials when the user navigates from one Oracle E-Business Suite mobile app to another on the same mobile device.

When configuring Oracle E-Business Suite mobile apps with the "Apps SSO Login" authentication type available from Oracle E-Business Suite Mobile Foundation Release 4.0 and onwards, ensure that you complete the following required tasks:

> **Note:** The "Apps SSO Login" type corresponds to the "Web SSO" authentication server type used in Oracle Mobile Application Framework.

> **Important:** Before setting up your mobile app with any of the advanced configurations, ensure basic mobile app configuration is performed and validated. See: Validating the Configuration, page 9-42.

1. **Common Tasks for Single Sign-On (Prerequisite Tasks)**

   Regardless of using Oracle E-Business Suite mobile apps or not, you need to perform some common tasks for configuring Oracle E-Business Suite with single sign-on. This section describes these common tasks which serve as prerequisites for mobile apps configuration with single sign-on.

   See: Prerequisites for Setting Up Mobile Apps with Single Sign-On, page 14-2.

2. **Specific Tasks for Mobile Apps with Single Sign-On**

After completing the common or prerequisite tasks for Oracle E-Business Suite with single sign-on, you can proceed with the rest of single sign-on configuration specifically for Oracle E-Business Suite mobile apps.

See: Mobile Specific Setup Tasks to Enable Apps SSO Login Authentication Security, page 14-3.

For troubleshooting information, see Troubleshooting Tips on Configuring Apps With the Apps SSO Login Authentication Type, page 16-22.

Prerequisites for Setting Up Mobile Apps with Single Sign-On

If your Oracle E-Business Suite is integrated with Oracle Access Manager, to authenticate users remotely with single sign-on, ensure that you complete the following prerequisites:

- Oracle E-Business Suite mobile apps delegate user authentication to Oracle Access Manager in the same way as supported for Oracle E-Business Suite browser-based applications. In this situation, mobile users are authenticated remotely against an external Oracle Access Manager (OAM) server. Refer to My Oracle Support Knowledge Document 1388152.1, *Overview of Single Sign-On Integration Options for Oracle E-Business Suite*.

- 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, integration with multi-factor authentication, 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.

  Note that 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.

To support "Apps SSO Login" (previously known as "Web SSO") authentication security, after completing these common or prerequisite tasks for Oracle E-Business Suite with single sign-on, you must perform additional setup tasks to enable this

feature. See: Mobile Specific Setup Tasks to Enable Apps SSO Login Authentication Security, page 14-3.

Mobile Specific Setup Tasks to Enable Apps SSO Login Authentication Security

This section describes additional setup tasks to support "Apps SSO Login" (previously known as "Web SSO") authentication type for Oracle E-Business Suite mobile apps. It includes the following topics:

- Setup Tasks to Enable the Apps SSO Login Authentication Security, page 14-3
- Testing the Setup for the Apps SSO Login Authentication Security, page 14-10

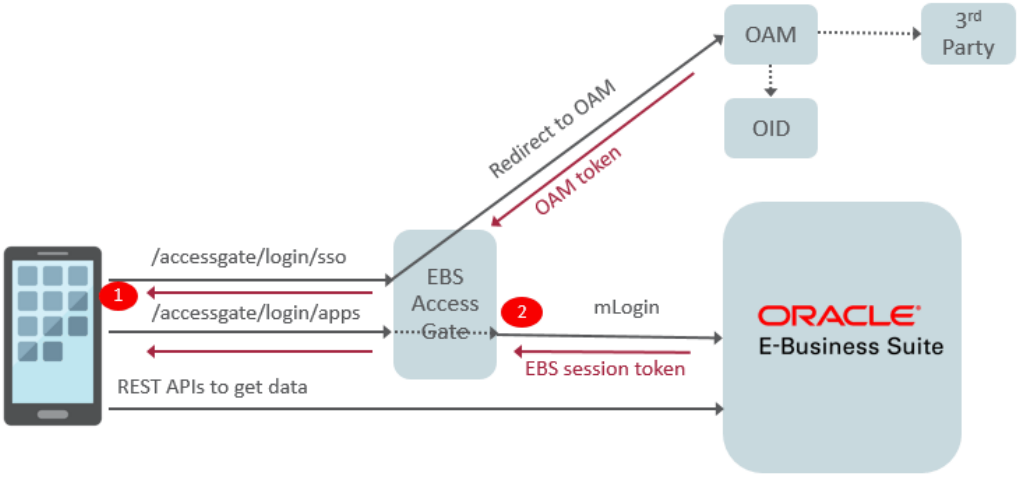
Additionally, see Troubleshooting Tips on Configuring Apps With the Apps SSO Login Authentication Type, page 16-22.

Setup Tasks to Enable the Apps SSO Login Authentication Security

To better understand the setup tasks specifically for mobile apps with Apps SSO Login, the following diagram illustrates the high level process flow when authenticating Oracle E-Business Suite mobile users using single sign-on in the case of TLS configuration:

> **Note:** Oracle E-Business Suite mobile apps work with any single sign-on configurations for Oracle E-Business Suite.

High Level Process Flow for Apps SSO Login Authentication with TLS Configuration



In this diagram, there are two different REST invocation points (client vs server) which require you to import certificates into appropriate truststores:

- **Scenario 1: TLS client invocation from a mobile app**

  This scenario invokes the following two endpoints:

  - Oracle E-Business Suite AccessGate

    A mobile user attempts to log in to an app through the value configured in the "SSO Login URL" (`login/sso`) parameter. The user is directed to Oracle E-Business Suite AccessGate (EAG) which is protected by the Oracle Access Manager (OAM) server for user authentication. When the user enters the login credentials in the Sign In screen, OAM verifies the credentials against user directory. If the user is successfully authenticated, OAM returns a unique OAM access token to Oracle E-Business Suite AccessGate for further identification verification, as described in Scenario 2.

  - Oracle E-Business Suite REST endpoint on the server

    Once the user is successfully authenticated to access Oracle E-Business Suite from the mobile app, the mobile app uses "EBS Session Service" (`login/apps`) to create a valid Oracle E-Business Suite session. The user then performs desired actions through Oracle E-Business Suite REST APIs to fetch Oracle E-Business Suite data for the app.

  If your Oracle E-Business Suite AccessGate server and Oracle E-Business Suite server use custom CA or self-signed certificates, these certificates should be imported to your Oracle E-Business Suite mobile app. For information on importing these certificates to an app, see Using Custom or Self-signed Certificates with Oracle E-Business Suite Mobile Apps, page 13-3.

- **Scenario 2: TLS client invocation from Oracle E-Business Suite AccessGate to invoke Oracle E-Business Suite application tier**

  Oracle E-Business Suite AccessGate is a Java Enterprise Edition application that maps a single sign-on user to an Oracle E-Business Suite user. Once picking up the access token from OAM, Oracle E-Business Suite AccessGate verifies the user identification against the Oracle E-Business Suite database. If the verification is successful meaning that this is a valid Oracle E-Business Suite user, an Oracle E-Business Suite session token is returned. The session token that points to the user session will be passed to HTTP headers of all subsequent service calls for the user authentication.

  To successfully invoke the Oracle E-Business Suite application tier from Oracle E-Business Suite AccessGate as described in this scenario, custom CA or self-signed certificates used in Oracle E-Business Suite application tier should be imported to the Oracle E-Business Suite AccessGate truststore.

Based on the above high level invocation diagram, to enable the Apps SSO Login authentication for Oracle E-Business Suite mobile apps, you need to ensure Oracle E-Business Suite AccessGate is deployed properly and its required certificates are imported for a TLS-based environment. This section includes the following setup tasks for mobile apps based on your Oracle E-Business Suite release:

- Setup Tasks for Oracle E-Business Suite 12.1.3, page 14-5
- Setup Tasks for Oracle E-Business Suite 12.2, page 14-7

For Oracle E-Business Suite Release 12.1.3

1. Download Oracle E-Business Suite AccessGate for your Oracle E-Business Suite release. For download and patch information, refer to My Oracle Support Knowledge Document 2202932.1, *Using the Latest Oracle E-Business Suite AccessGate for Single Sign-On Integration with Oracle Access Manager*.

2. Deploy Oracle E-Business Suite AccessGate by following the setup and configuration instructions described in one of the following My Oracle Support Knowledge Documents based on your Oracle Access Manager release:

   - For Oracle Access Manager 12c, see Document 2339337.1, *Automating Integration of Oracle E-Business Suite Release 12.1.3 With Oracle Access Manager 12c*.

   - For Oracle Access Manager 11g, see Document 2045154.1, *Automating Integration of Oracle E-Business Suite Release 12.1 With Oracle Access Manager 11gR2 (11.1.2)*.

3. After Oracle E-Business Suite AccessGate 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. **Tasks for Enabling the feature on a TLS-based Oracle E-Business Suite environment**

   Note: Oracle E-Business Suite mobile apps built with Oracle E-Business Suite Mobile Foundation Release 6.0 or later support TLS 1.2 only and TLS 1.2 with backward compatibility (recommended). For information on enabling TLS 1.2 only and TLS 1.2 with backward compatibility, see My Oracle Support Knowledge Document 376700.1, *Enabling TLS in Oracle E-Business Suite Release*

12.1.

Please note that Oracle E-Business Suite mobile apps built with Oracle E-Business Suite Mobile Foundation Release 5.0 support TLS 1.0 only.

If your Oracle E-Business Suite instance is TLS enabled and Oracle Access Manager (OAM) configured, ensure you perform the following tasks:

1. If your mobile apps are built with Oracle E-Business Suite Mobile Foundation Release 6.0 or later, you need to configure the Oracle E-Business Suite AccessGate (EAG) managed server with required TLS parameters so that the same TLS security protocol is used for outbound communication.

   For information on adding the required parameters for the EAG managed server, refer to one of the following My Oracle Support Knowledge Documents based on your Oracle Access Manager release:

   - For Oracle Access Manager 12c, see Document 2339337.1, *Automating Integration of Oracle E-Business Suite Release 12.1.3 With Oracle Access Manager 12c* - "Configuring Oracle E-Business Suite AccessGate (EAG) Managed Server to use the TLS Protocol for Outbound Communication" in Section 9.1 Configuring Transport Layer Security (TLS).

   - For Oracle Access Manager 11g, see the following Knowledge Documents:

     - Document 2045154.1, *Automating Integration of Oracle E-Business Suite Release 12.1 With Oracle Access Manager 11gR2 (11.1.2)* - "Configuring Oracle E-Business Suite AccessGate (EAG) Managed Server to use the TLS Protocol for Outbound Communication" in Section 9.1 Configuring Transport Layer Security (TLS).

     - Document 1484024.1, *Integrating Oracle E-Business Suite Release 12 with Oracle Access Manager 11gR2 (11.1.2) using Oracle E-Business Suite AccessGate* - "Configuring Oracle E-Business Suite AccessGate (EAG) Managed Server to use the TLS Protocol for Outbound Communication" in Section 9.2 Configuring Transport Layer Security (TLS).

2. Import the root-CA certificates from the Oracle HTTP Server (OHS) wallet and Oracle TLS CA certificates into the truststore of the managed server where Oracle E-Business Suite AccessGate 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. Download Oracle E-Business Suite AccessGate for your Oracle E-Business Suite release. For download and patch information, refer to My Oracle Support Knowledge Document 2202932.1, *Using the Latest Oracle E-Business Suite AccessGate for Single Sign-On Integration with Oracle Access Manager*.

2. Deploy Oracle E-Business Suite AccessGate by following the setup and configuration instructions described in one of the following My Oracle Support Knowledge Documents based on your Oracle Access Manager release:

   - For Oracle Access Manager 12c, see Document 2339348.1, *Integrating Oracle E-Business Suite Release 12.2 with Oracle Access Manager 12c using Oracle E-Business Suite AccessGate*.

     If you have already deployed an earlier version of Oracle E-Business Suite AccessGate, refer to Section 8.2 Oracle E-Business Suite AccessGate Upgrade, My Oracle Support Knowledge Document 2339348.1.

   - For Oracle Access Manager 11g, see 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 Oracle E-Business Suite AccessGate, refer to Section 8.2 Oracle E-Business Suite AccessGate Upgrade, My Oracle Support Knowledge Document 1576425.1.

3. After Oracle E-Business Suite AccessGate 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 or later, then you need to re-register Oracle E-Business Suite and include an additional parameter `-policyUpdate=yes`. These actions add the newly-defined public resource `/accessgate/logout/sso` to your configuration.

   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. Additionally, add a 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. **Tasks for Enabling the feature on a TLS-based Oracle E-Business Suite environment**

> **Note:** Oracle E-Business Suite mobile apps built with Oracle E-Business Suite Mobile Foundation Release 6.0 or later support TLS 1.2 only and TLS 1.2 with backward compatibility (recommended). For information on enabling TLS 1.2 only and TLS 1.2 with backward compatibility, see My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.
>
> Please note that TLS 1.0 is required for Oracle E-Business Suite mobile apps built with Oracle E-Business Suite Mobile Foundation Release 5.0.

If your Oracle E-Business Suite instance is TLS enabled and Oracle Access Manager (OAM) configured, perform the following tasks:

1. Import the root-CA certificates from the OHS wallet into the truststore of the OAEA managed server where Oracle E-Business Suite AccessGate 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 certificates 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 in My Oracle Support Knowledge Document 2143101.1, *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 TLS in the Oracle E-Business Suite context file. 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 TLS. 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 TLS". Then choose the **OK** button.

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

Testing the Setup for the Apps SSO Login Authentication Security

To successfully log in to an Oracle E-Business Suite mobile app configured with the Apps SSO Login security, you need to ensure successful HTTP(s) communication from the Oracle E-Business Suite AccessGate managed server to the Oracle E-Business Suite server.

1. Validate the communication by running the following WGET command from the managed server where Oracle E-Business Suite AccessGate is deployed:

   ```
   wget -d http(s)://<ebs_host>:<ebs_port>/OA_HTML/RF.jsp?
   function_id=mLogin
   ```

2. If this fails, verify the following tasks and ensure they are in place:

   1. The root-CA, intermediate, and server certificates from the Oracle HTTP Server (OHS) wallet and Oracle TLS CA certificates are imported into the truststore of the managed server where Oracle E-Business Suite AccessGate is deployed.

   2. Network port from the current managed server to the Oracle E-Business Suite web entry is NOT restricted.

   3. For an Oracle E-Business Suite environment configured in a DMZ configuration, if Oracle E-Business Suite AccessGate is deployed on your intranet server with firewalls and the Oracle E-Business Suite web entry point is a URL over the Internet, then make sure this Oracle E-Business Suite URL is NOT DIS_ALLOWED from the intranet server.

Although this Oracle E-Business Suite web entry point URL can be your enterprise's own URL, this could still restrict access from your intranet server. If this network restriction policy cannot be exempted to ALLOW access from the intranet managed server where Oracle E-Business Suite AccessGate is deployed to the Oracle E-Business Suite web entry point over the Internet, then you can try the following option of configuring proxy host and port for the HTTP communication as a workaround.

1. Restart with the following `-D` System settings on the managed server where Oracle E-Business Suite AccessGate is deployed.

2. Use the `-D` settings for setting up proxy host and port through the System properties in JAVA_OPTIONS:

   - For the HTTP protocol communication:

     ```
     -Dhttp.proxyHost
     -Dhttp.proxyPort
     ```

   - For the HTTPS protocol communication:

     ```
     -Dhttps.protocols (TLSv1.1/SSL version)
     -Dhttps.proxyHost
     -Dhttps.proxyPort
     ```

For more information, refer to Oracle Networking Properties (https://docs.oracle.com/javase/7/docs/api/java/net/doc-files/net-properties.html), Oracle Java Documentation.

15

Integrating Oracle E-Business Suite Mobile Apps with Enterprise Mobility Management Solutions

Overview

Oracle is an Independent Software Vendor (ISV) member of the AppConfig Community. The AppConfig Community provides tools and best practices to secure, configure, deploy, and manage mobile enterprise apps. Oracle E-Business Suite mobile apps are built using Oracle Mobile Application Framework (MAF). Oracle MAF applications are compatible with AppConfig-based Enterprise Mobility Management (EMM) integration, using native frameworks that are made available through operating systems (iOS and Android).

This chapter provides guidance on integrating Oracle E-Business Suite mobile apps with EMM solutions based on AppConfig standard. It also includes some setup tasks that administrators can manage Oracle E-Business Suite mobile app configuration when the apps are deployed with an EMM solution.

Oracle E-Business Suite Mobile Apps with Enterprise Mobility Management Solutions

About the MAF Approach to Enterprise Mobile Apps

Oracle E-Business Suite mobile apps are built using Oracle Mobile Application

Framework (MAF). Mobile apps built with MAF work with AppConfig Enterprise Mobile Management solutions. The MAF integration with EMM following AppConfig standards helps building EMM-compatible applications. MAF applications support AppConfig capabilities such as Per-App VPN app tunnelling, application configuration, and implementations of security policies and access control.

For more information, refer to Integrating MAF Applications with EMM Solutions, *Developing Mobile Applications with Oracle Mobile Application Framework*.

Compatibility of Oracle E-Business Suite Mobile Apps with AppConfig EMM Providers

Oracle E-Business Suite mobile apps are expected to work with any EMM provider that supports common AppConfig standards provided by operating system vendors. Oracle does not explicitly certify permutations of Oracle E-Business Suite mobile app releases with given EMM providers and their releases. Oracle may test selected Oracle E-Business Suite mobile apps with selected AppConfig-compliant products, including VMware AirWatch. Oracle does not conduct comprehensive tests between all available Oracle E-Business Suite mobile app releases and all AppConfig-compliant products.

Support

Oracle Support does not have access to third-party EMM AppConfig products and is unable to reproduce or investigate AppConfig compatibility issues directly. Oracle Support will ask customers to validate if the reported issue reproduces without third-party EMM integration in order to determine if the issue is specific to the third-party EMM solution. Issues with AppConfig-based configurations should be first reported to the affected EMM provider. The EMM provider may engage Oracle for interoperability issues between Oracle MAF and the third-party EMM solution as needed.

Setup Tasks for Deploying Mobile Apps with Enterprise Mobility Management Solutions

Users can install Oracle E-Business Suite mobile apps from an Enterprise Mobility Management (EMM) solution's app catalog. To connect to Oracle E-Business Suite, users need to enter the Oracle E-Business Suite server URL after the initial launch of an app from an EMM console that the app is deployed. To simplify the deployment process for the app users, starting from Oracle E-Business Suite Mobile Foundation 8.0, administrators can preconfigure the server URL in an EMM console. App users no longer need to enter this URL manually after launching an app installed from an EMM's app catalog.

These apps include:

- Standard apps installed from the Apple App Store or Google Play
- Apps provided to users through enterprise distribution

- Custom apps developed based on Oracle E-Business Suite Mobile Foundation

  Important: For custom apps built with Oracle E-Business Suite Mobile Foundation, if these apps are deployed with EMM solutions, mobile applications developers need to enable the server URL related properties required for use by EMM solutions in `maf-application.xml`. For more information on defining these properties in Oracle JDeveloper, see Step 9: Setting Up Default Server URL (Optional), *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

To preconfigure the server URL, administrators need to configure the following String type properties in an EMM console to simplify the app deployment for users:

Note: This feature has been tested on iOS devices. To leverage this feature on Android devices, it is required to register your EMM provider with Google Play.

- Server_URL

  This is the Oracle E-Business Suite server URL that an app should connect to by default. If a valid Oracle E-Business Suite server URL is entered in this property, the app users will not be prompted to enter the server URL when the app is launched for the first time.

  Ensure that the mobile app is already "Enabled" in the Mobile Applications Manager UI pages. For information on enabling an app, see Enabling a Mobile App Individually and Specifying the Configuration Through the UI Pages, page 9-21.

- Server_URL_Allow_Change

  If a default Oracle E-Business Suite server URL is entered in the Server_URL property, you need to explicitly indicate whether the app users can change the URL in the app. By default, users are not allowed to change. However, set it to "Y" only if you want to allow the app users to change the default URL.

For enterprise-distributed apps and custom apps developed based on Oracle E-Business Suite Mobile Foundation, if these apps will not be deployed using EMM solutions, mobile applications developers can preconfigure the server URL during the app development. See: Configuring Default Server URL (Optional), *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

16

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

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

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 D: Mobile App Module Names, page C-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. Run 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 D-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 16-2.

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.

Uploading Client Logs to the Oracle E-Business Suite Server

If mobile app users can access to the app, direct the 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**.

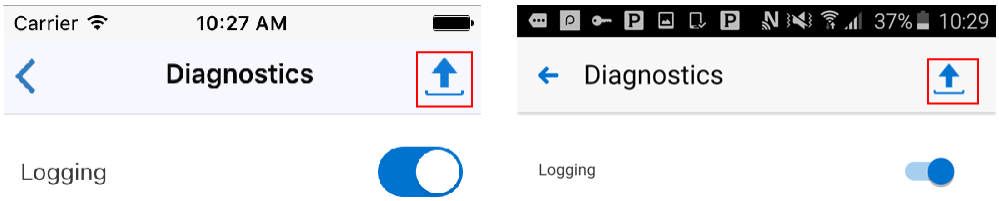
   In the Diagnostics screen, enable the client logging feature by turning on the **Logging** option.

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.

Diagnostics Screen with Upload Icon Highlighted in iOS and Android Devices



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 16-2. However, use the following search criteria to locate the client logs:

   - **User:** Enter the mobile app user name.

   - **Module:** 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 D-1.

Please note that if the FND: Diagnostics profile option is enabled for a user, the complete error stack from the service invocation failure appears. Otherwise, only a simple error message is shown instead.

Retrieving Client Logs Directly From Android Mobile Devices

If mobile app users are unable to access or log in to the app, the users will not be able to upload the logs to the server from the mobile client. In this situation, direct the Android users to retrieve client logs directly from their mobile devices instead.

Note: The option of retrieving client logs directly from iOS devices is not available.

1. Use a file browser app on Android. For example, My Files, ES File Explorer.
2. Look for files that start with the app name. For example, `Approvals.txt`, `Approvals_bak.txt`.
3. Attach these files to an email through your preferred email app and upload to Oracle Support.

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 16-2.

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 `fnd.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 16-2. 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 16-6
- Troubleshooting Tips on the Oracle E-Business Suite Server, page 16-20

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 D-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 F-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 Download Updates from the Server, page 16-6
- Troubleshooting Tips for Oracle E-Business Suite Mobile Apps, page 16-10

Directing Users to Obtain Connection Details and Download Updates from the Server

When 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:

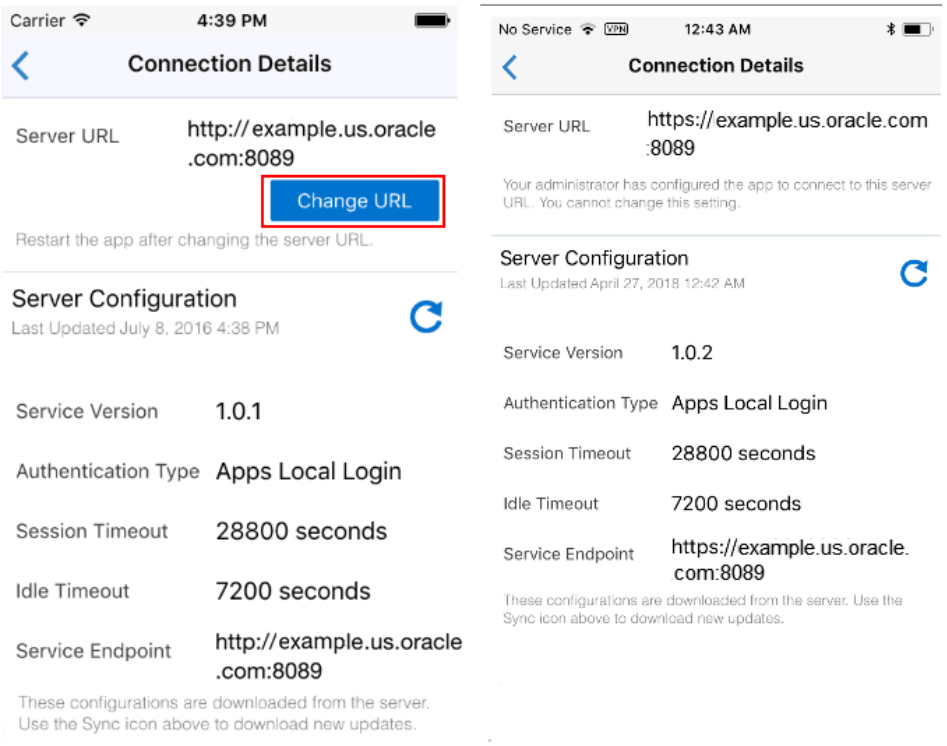
1. In the navigation menu of the mobile app, tap **Settings** and then **Connection Details**. The Connection Details screen appears.
2. The Connection Details screen displays the server URL field and the Server Configuration region.

- **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.

  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, as shown on the left. 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.

Connection Details Screen with "Change URL" Button Highlighted (Left) and without the Button (Right)



Note: Starting from Oracle E-Business Suite Mobile Foundation Release 8.0 and onwards, administrators can preconfigure the server URL and also determine if users can change the default URL value. If the server URL is preconfigured and users are not allowed to change the value, then **Change URL** will not be displayed. Instead, "Your administrator has configured the app to connect to this server URL. You cannot change this setting." message appears, as shown on the right.

For information on preconfiguring server URL, see Setup Tasks for Deploying Mobile Apps with Enterprise Mobility Management (EMM) Solutions, page 15-2.

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.

    This field appears only when the "Apps Local Login" (previously known as "HTTP Basic") authentication type is selected for your app.
  - **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. Direct users to check if any new updates from the server are required for the app.

   Starting from Oracle E-Business Suite Mobile Foundation Release 7.0 and onwards, Oracle E-Business Suite mobile apps automatically download the mobile app configuration updates from the Oracle E-Business Suite server. Users no longer need to initiate a download manually within an app. Instead, each app periodically checks for updates (once every five times the app is restarted) and downloads them to synchronize with the configuration details defined on the Oracle E-Business Suite server. However, if required, users can still initiate the manual update by tapping the **Sync** icon as in the previous releases.

   > **Note:** For releases earlier than Oracle E-Business Suite Mobile Foundation 7.0, users need to manually tap the **Sync** icon next to the Server Configuration region to check if any new updates from the server are required for the app.

   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 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 and onwards 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
For a mobile app built with Oracle E-Business Suite Mobile Foundation 7.0 and onwards, when a user enters a server URL in a mobile device using HTTPS, if the TLS certificate is untrusted and cannot be recognized by the mobile app, the following error message may appear: `"Unable to make a secure connection to the Oracle E-Business Suite server. Please verify the TLS setup for the app and the server."`	Ensure that your mobile app can perform a successful TLS handshake with the Oracle E-Business Suite TLS endpoint. 1. Validate that the JDK 8 client can connect to the Oracle E-Business Suite TLS endpoint. 2. Check the list of root CAs trusted by the mobile client. • For apps built with Oracle E-Business Suite Mobile Foundation 9.1 and 9.0, refer to "Migrating to New cacerts File for SSL in MAF 2.6.0", *Installing Oracle Mobile Application Framework*, plus the following migration motes: • For Release 9.1- Oracle Mobile Application Framework 2.6.3 Migration Notes (https://www.oracle.com/applicationdevelopment/technologies/maf/maf263migration.htm) • For Release 9.0 - Oracle Mobile Application Framework 2.6.2 Migration Notes (https://www.oracle.com/applicationdevelopment/technologies/maf/maf262migration.htm) • For apps built with Oracle E-Business Suite Mobile Foundation 8.0 and 7.0, refer to Migrating to New cacerts File for SSL in MAF 2.5.0 and Migrating to New cacerts File for SSL in MAF 2.4.0 respectively. To locate the Oracle MAF documentation for the apps built with the MAF version

Issue	Tip
	earlier than 2.6.3, see "Previous releases of Oracle Mobile Application Framework Documentation" (https://www.oracle.com/application-development/technologies/maf/maf-prev-rel. html). If the root CA that issued the certificate for Oracle E-Business Suite is not part of the mobile app, or if your Oracle E-Business Suite environment is TLS-enabled using a self-signed or certificate issued by a custom CA, make sure to import the CA's root certificate to the mobile app. For instructions on importing the CA's root certificate to Oracle E-Business Suite mobile apps, see Advanced Configurations for Secure Communication with HTTPS, page 13-1.

Issue	Tip
For a mobile app built with Oracle E-Business Suite Mobile Foundation releases earlier than 7.0, when a user enters a server URL in a mobile device using HTTPS, if the TLS certificate is untrusted and cannot be recognized by the mobile app, the following error message may appear: `"Unable to connect to the Oracle E-Business Suite server. Please enter a valid server URL."`	Ensure that your mobile app can perform a successful TLS handshake with the Oracle E-Business Suite TLS endpoint. 1. Validate that the JDK 8 client can connect to the Oracle E-Business Suite TLS endpoint. 2. Validate that the Oracle E-Business Suite TLS endpoint presents the complete certificate chain. For validation instructions, see the detailed steps as described in Advanced Configurations for Secure Communication with HTTPS, page 13-1. For a list of root CAs trusted by the mobile client, see Migrating to New cacerts File for SSL in MAF 2.x.x, *Installing Oracle Mobile Application Framework*. For information on the Oracle MAF version required 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, and Section 1: Oracle E-Business Suite Mobile Foundation Release Update History in *Oracle E-Business Suite Mobile Foundation Release Notes*, Oracle Support Knowledge Document 1642431.1.
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.

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 or set up correctly during the 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, as described in Validating the Configuration, page 9-42. 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. test for PID **Note:** When an app user is authenticated, the `mLogin` REST service creates an Oracle E-Business Suite session for that user along with an XML response with authentication token (cookie) which uniquely identifies that session. To secure each user session, a profile option "FND: Authn Service Token Scope (`FND_AUTHN_SRVC_TOKEN_SCOPE`)" is introduced in the January 2023 Critical Patch Update with the default value

Issue	Tip
	"Header Only" at the Site level. This default value sets the ICX cookie only in the response header of the `mLogin` REST service, and will not return the cookie details in the response payload. If you have custom code that calls the `mLogin` REST service and requires the cookie details in the response payload, then you can optionally change the value to "Header and Body". In this case, the mLogin service sets the ICX cookie in the header and also returns the cookie name and value in the payload.

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 Section 4.2: Implementing AutoConfig Customizations, My Oracle Support Knowledge 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 9-1 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 9-20.

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.
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.`	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 9-20.

Troubleshooting Tips on the Oracle E-Business Suite Server

This section describes the troubleshooting tips on the Oracle E-Business Suite server. It includes the following topics:

- Troubleshooting Tips on the Oracle E-Business Suite Server, page 16-20
- Troubleshooting Tips on Configuring Apps With the Apps SSO Login Authentication Type, page 16-22
- Troubleshooting Tips for Push Notifications, page 16-25

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
For Oracle E-Business Suite Mobile Foundation 8.0 and onwards, if administrators preconfigure Server URL in an Enterprise Mobility Management (EMM) console through the Server_URL property or in **`ebs.properties`** when EMM is not used, after an app user launches the app, the following error may appear: `Unable to connect to the Oracle E-Business Suite server. The server URL may be invalid.`	To resolve this issue, perform the following steps to verify the preconfigured Server URL in **`ebs.properties`** or an EMM console to make sure: • This preconfigured URL has a valid format: `http(s)://<host>:<port>` • Enter the URL in a web browser and make sure that you are able to access the Oracle E-Business Suite home page successfully. • From a web browser, invoke the login service as `http(s)://<host>:<port>/OA_HTML/RF.jsp?function_id=mLogin` and verify that it prompts for user name and password.
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.

Issue	Tip
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.
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.	To resolve this issue, a mobile user can initiate the server updates from the mobile device. See Directing Users to Obtain Connection Details and Download Updates from the Server, page 16-6.

Troubleshooting Tips on Configuring Apps With the Apps SSO Login Authentication Type

This section describes the troubleshooting tips that are particularly related to configure mobile apps with the Apps SSO Login (previously known as "Web SSO") authentication type.

For information about configuring apps with the Apps SSO Login authentication type, see:

- Configuring Parameters for the Apps SSO Login Authentication Type, page 9-31
- Advanced Configurations for Single Sign-On, page 14-1

Troubleshooting Tips

Perform the following tasks to validate and troubleshoot potential issues for configuring mobile apps with the Apps SSO Login type:

1. **Verify prerequisite configuration for Oracle E-Business Suite, Oracle Access Manager (OAM), and Oracle Directory Services integration**
    1. Navigate to the application login page through a web browser. Verify the login redirects to Oracle Access Manager as configured during the Oracle E-Business Suite integration with Oracle Access Manager, and the same LDAP user that

will be using a mobile app can log in successfully to Oracle E-Business Suite framework based applications.

2. Verify after successful login and rendering of the Oracle E-Business Suite Home page, the user has Oracle E-Business Suite responsibilities assigned.

3. Ensure the administrator has configured the specific configuration tasks, as described in Prerequisites for Setting Up Mobile Apps with Single Sign-On, page 14-2 and Mobile Specific Setup Tasks to Enable Apps SSO Login Authentication Security, page 14-3.

2. **Test the configured "SSO Login URL", "SSO Login Success URL", and "SSO Logout URL" parameters**

   1. Navigate to the configured SSO Login URL through a web browser. After the login, the browser should return a protected page successfully (`Status 200 OK`). The URL for this page must be the same as the configured SSO Login Success URL.

      > **Note:** The "SSO Login URL" and "SSO Login Success URL" parameters relate to each other. The values of these two parameters can be the same.

      Do not configure a URL, such as `http://<hostname>:<port>/OA_HTML/AppsLogin`, as the SSO Login URL because this page would unnecessarily redirect to the Oracle E-Business Suite Home page after the login. Use the default SSO Login URL `http://<hostname>:<port>/accessgate/login/sso` instead.

   2. Navigate to the configured SSO Login URL through a web browser. For example, `http://<hostname>:<port>/accessgate/login/sso`.

      > **Note:** When you test the `login/sso` or `login/apps` (as described later in step 3 for "EBS Session Service") service standalone from a web browser, it is recommended sending the X-Ebs-Wep request parameter that is supported in Oracle E-Business Suite AccessGate (EAG) 1.3.2.1 and above with Oracle E-Business Suite web entry URL (`http(s)://<hostname>:<port>`).
      >
      > If EAG does not receive this parameter, the `login/apps` service may fail and an "`Initialization failed -1`" error is captured in EAG logs. In this situation, ensure you pass this X-Ebs-Wep request parameter while testing the service standalone from a browser.

Expected result: Redirect to the OAM login page. Login successful after specifying the LDAP user name and password.

After the login, the resource `http://<hostname>:<port>/accessgate/login/sso` shows with no error message. This resource must be the configured "SSO Login Success URL" parameter value.

> **Note:** The "SSO Login URL" and "SSO Login Success URL" parameter values can be the same.

The browser shows a blank page successfully.

3. Navigate to the configured SSO Logout URL. For example, `http://<hostname>:<port>/accessgate/logout/sso`.

   Expected result: User logged out successfully.

4. Perform the same tests using your mobile device browser.

3. **Test the configured "EBS Session Service" parameter**

   1. Navigate to the configured EBS Session Service through a web browser. For example, `http://<hostname>:<port>/accessgate/login/apps`.

      Expected result: Redirect to the OAM login page. Login successful after specifying the LDAP user name and password.

      After the login, the browser returns an xml file containing an access token and the user name for the user that just logged in. For example:

      ```
      <response>
      <data>
      <accessToken>xxxxxxxxxxxxxxxxxxxxxxxxxx</accessToken>
      <accessTokenName>emsxxxxx</accessTokenName>
      <ebsVersion>12.2.5</ebsVersion>
      <userName>xxxxx</userName>
      </data>
      </response>
      ```

   2. Perform the same test using your mobile device browser.

4. **Collect HTTP header traces and logs**

   1. Collect HTTP Header traces during the implementation of the above test points.

   2. Collect log files for Oracle E-Business Suite AccessGate, Oracle E-Business Suite oacore, and the OAM server.

      Refer to My Oracle Support Knowledge Document 1077460.1, *Troubleshooting Oracle Access Manager and Oracle E-Business Suite AccessGate*, on how to generate Oracle E-Business Suite AccessGate logs.

Troubleshooting Tips for Push Notifications

If you have enabled push notifications for the supported mobile apps, you would want to troubleshoot setup and processing of push notifications if users report that they are not receiving push notifications. This section includes the following topics:

- Troubleshooting Tips for Enabling Push Notifications on the Mobile Client, page 16-25
- Troubleshooting Tips for Common Setup Issues on the Oracle E-Business Suite Server, page 16-26
- Steps to Troubleshoot Push Notification Issues, page 16-41

For more information about push notifications, see Setting Up Push Notifications for Mobile Apps, page 10-1.

Troubleshooting Tips for Enabling Push Notifications on the Mobile Client

The following table lists the troubleshooting tips for enabling push notifications on the mobile client:

Troubleshooting Tips for Enabling Push Notifications on the Mobile Client

Issue	Tip
A mobile app user is not able to receive push notifications in the mobile device, while other users of the same app do not have this issue.	Provide the following instructions to the mobile user to change the device settings: • For the iOS devices 1. Tap **Settings**. 2. Open the mobile app enabled with push notifications. 3. Enable the **Allow Notifications** option. • For the Android devices 1. Tap **Settings**. 2. Navigate to **Application Manager**. 3. Open the mobile app enabled with push notifications. 4. Tap **Notifications**, and then enable the **Allow Notifications** option.

Troubleshooting Tips for Common Setup Issues on the Oracle E-Business Suite Server

The following table describes the common setup issues, possible causes, and corresponding solutions in the Oracle E-Business Suite Mobile Foundation Push Notification System:

> **Note:** Oracle E-Business Suite Mobile Foundation uses Oracle Mobile Hub (OMH) or Oracle Mobile Cloud Service (MCS) to provide support for push notifications.

Troubleshooting Tips for Common Setup Issues in the Oracle E-Business Suite Mobile Foundation Push Notifications System

Issue	Root Cause	Resolution
A mobile user has installed the mobile app that supports push notifications. When the user signs in to the app, no record is created in the `FND_MBL_NOTIF_REGISTRATIONS` table for the user's app For a mobile app to receive push notifications, the push token (iOS) or registration ID (Android) should be stored in Oracle E-Business Suite.	**Possible Cause 1:** For the mobile app developed using Oracle Mobile Application Framework and Oracle E-Business Suite Mobile Foundation Login Component, the push plug-in is not enabled.	Before deploying the mobile app, a developer needs to enable the push plug-in by selecting the **PushPlugin** check box in the associated `maf-application.xml` file. See: Enabling the Push Plug-in, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*. Once the push plug-in is enabled, deploy the app and test it again.
Same issue as the described above	**Possible Cause 2:** When the mobile device is launched, the device is not connected to the Internet.	If the device is not connected to the Internet, the mobile device cannot connect to its corresponding push notification service. For example, an iOS device connects to APNs to receive push token and an Android device connects to FCM to receive registration ID. To resolve this issue, perform the following tasks: 1. Make sure the device is connected to the Internet. 2. Restart the app. 3. Sign in to Oracle E-Business Suite and check again.

Issue	Root Cause	Resolution
Same issue as the described above	**Possible Cause 3:** When the mobile app invokes the Oracle E-Business Suite REST API `mPushRegister` after the user signs in, it fails.	You can invoke the Oracle E-Business Suite REST API `mPushRegister` from a REST client, such as Advanced REST Client, to verify if it can successfully create a record in the `FND_MBL_NOTIF_REGISTRATIONS` table. For instructions on invoking this API, see Checking the mPushRegister REST API, page 16-42.

Issue	Root Cause	Resolution
Same issue as the described above	**Possible Cause 4:** The Push Notification System is not enabled and configured with valid Oracle Mobile Hub (OMH) or Oracle Mobile Cloud Service (MCS) credentials. If this configuration is not completed, push notification registrations are not synchronized with OMH or MCS. As a result, push notifications are not sent to users.	You need to ensure the Push Notification System is configured properly. 1. Log in to Oracle E-Business Suite as a user who has the **Mobile Applications Manager** responsibility. Click the **Push Configuration** button to open the Mobile Push Notification Configuration page. 2. Verify if the Push Notification System field is set to "ENABLED" in the Mobile Push Notification Configuration page. 3. Verify if the setup for Oracle Mobile Hub or Oracle Mobile Cloud Service is completed with valid credentials. 4. To support Android push notifications, make sure you enter a valid Android Sender ID value. For information on configuring global push notifications, see Configuring Oracle E-Business Suite Mobile Foundation Push Notification System, page 10-11.

Issue	Root Cause	Resolution

A mobile user has installed the mobile app that supports push notifications. When the user signs in to the app, no record is created in the `FND_MBL_NOTIF_REGISTRATIONS` table for the user's **Android** app	Android Sender ID and Server Key are not set up correctly.	To resolve the issue, perform the following tasks:
		1. Go to the Firebase console (`https://console.firebase.google.com`). Open the project created for the Android push notifications and record the Sender ID and Server Key values.
		2. Make sure these values are entered correctly in the following setup tasks:
		• Android Sender ID in the Mobile Push Notification Configuration page
		See: Configuring Oracle E-Business Suite Mobile Foundation Push Notification System, page 10-11.
		• Android profile for the Android client registration in Oracle Mobile Hub or Oracle Mobile Cloud Service
		  • API Key: Ensure the "Server Key" value is entered in this field.
		  • Sender ID: Ensure the correct "Sender ID" value is entered.

Issue	Root Cause	Resolution
		See: Creating Mobile Clients, page 10-7.
When you submit the Mobile Push Notification Configuration page with user credentials, an error occurs indicating that the credentials are invalid.	This issue may occur due to either one of the following: • The user name, password, backend ID, or URL is invalid. • The user does not have the "Default" and "Mobile Notifications" roles assigned in the Oracle Cloud My Services portal. • Oracle E-Business Suite to MCS or OMH REST service invocation failed due to TLS handshake.	Use the following steps to resolve this issue: 1. Check the OACORE logs to see if the REST service invocation failed with TLS handshake when Oracle E-Business Suite invoked the MCS or OMH URL for validation. 2. If yes, download the MCS or OMH URL's CA certificate and import the certificate to the truststore in Oracle E-Business Suite. For instructions on importing the certificates to the truststore in Oracle E-Business Suite, see Fixing the SSL Handshake Error, page 16-48.

Issue	Root Cause	Resolution
Push notification registration STATUS for a user in the `FND_MBL_NOTIF_REGISTRATIONS` table is "READY". However, it is not changing to "REGISTERED".	**Possible Cause 1:** This issue may occur due to either one of the following: • The Push Notification System is not enabled and configured with valid user credentials. • Oracle E-Business Suite to MCS or OMH REST service invocation failed due to TLS handshake.	To resolve this issue, ensure the following tasks are in place: • The Push Notification System is configured properly. 1. Log in to Oracle E-Business Suite as a user who has the **Mobile Applications Manager** responsibility. Click the **Push Configuration** button. 2. Verify if the Push Notification System field is set to "ENABLED" in the Mobile Push Notification Configuration page. 3. Verify if the setup for Oracle Mobile Hub or Oracle Mobile Cloud Service is completed with valid credentials. 4. To support Android push notifications, make sure you enter a valid Android Sender ID value. • Oracle E-Business Suite can successfully invoke the MCS or OMH REST service.

Issue	Root Cause	Resolution
		Download the MCS or OMH URL's CA certificate and import the certificate to the truststore in Oracle E-Business Suite. See Fixing the SSL Handshake Error, page 16-48.
Same issue as described above.	**Possible Cause 2:** This issue could also be caused by either of the following: • The business event used to synchronize the registration from Oracle E-Business Suite to Oracle Mobile Hub or Oracle Mobile Cloud Service is not enabled. • The Workflow Java Deferred Agent Listener is not running.	Although the business event `oracle.apps.mobile.foundation.push.synch` for synchronization is enabled by default, ensure that the event and the subscription are enabled using the Oracle Workflow Business Event user interface through the **Workflow Administrator Web Applications** responsibility. Additionally, the business event is processed through the WF_JAVA_DEFERRED queue. You need to log in to Oracle E-Business Suite, select the **Oracle Applications Manager** link, and then **Workflow Manager** to ensure the Workflow Java Deferred Agent Listener is running.

Issue	Root Cause	Resolution
Same issue as described above.	**Possible Cause 3:**The invocation of MCS or OMH REST service from Oracle E-Business Suite to register the mobile device failed because there is no client registered on MCS or OMH corresponding to the Oracle E-Business Suite mobile app distribution.	Use the following steps to ensure the correct distribution is selected for the mobile app: 1. Log in to Oracle E-Business Suite as a user who has the **Mobile Applications Manager** responsibility. 2. Locate the mobile app and click **Configure**. 3. Under the "Push Notifications" configuration category, make sure the following parameters are valid: • Android Deployment Bundle ID: Enter the same Package Name used to package the Android app. Make sure in MCS or OMH, an Android client is created with the same Package Name. • iOS Deployment Bundle Id: Enter the same Application Bundle ID used to package the iOS app. Make sure in MCS or OMH, an iOS client is created with the same Application Bundle ID.

Issue	Root Cause	Resolution
A push registration with status REGISTERED is found for a user, but the push notifications are not delivered to the mobile device.	**Possible Cause 1:** The possible root causes can be: • On Oracle E-Business Suite, the Push Notification Agent service component is not running. • On MCS or OMH, the notification could not be delivered to APNs or FCM for delivery to the mobile device.	You can check the notification status: • If the notification status is "QUEUED" in the `FND_MBL_NOTIFICATIONS` table, verify and ensure that the service component Push Notification Agent is running. • If the status is "SENT" indicating that Oracle E-Business Suite has sent the notification to MCS or OMH, log in to MCS or OMH to check the API log and confirm MCS or OMH has delivered the notification to APNs for an iOS device, and FCM for an Android device. Please note that after the Push Notification Agent successfully sent the notification to MCS or OMH and changed the status to "SENT", it is the responsibility of MCS or OMH to deliver the notifications to the user's devices.

Issue	Root Cause	Resolution
Same issue as the described above	**Possible Cause 2:** The possible causes can be: • The push notification business event associated with the mobile app is not enabled. Each app has its own business event. For example, the Approvals app with enterprise distribution uses business event `oracle.apps.mobile.approvals.push.event`. For information on creating an event for your app, see Creating Push Notification Business Events, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*. • The push notification business event is not added to the Push Notification System's business event group `oracle.apps.mobile.foundation.push.group`. For information on adding an event to the event group, see Adding the Push Notification Business Events to the Push Notification System's Event Group, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.	To resolve the issue, you need to log in to the Oracle Workflow Business Event user interface through the **Workflow Administrator Web Applications** responsibility. • Verify the push notification business event for the mobile app is Enabled. • Verify the business event is added to the business event group. • Verify the subscription to the business event group is Enabled. The subscription processes the push notifications and enqueues them to the FND_MBL_NOTIFICATION_OUT queue.

Issue	Root Cause	Resolution
Same issue as the described above	**Possible Cause 3:** The user uninstalled the app and then reinstalled it again. However, for the new installation, the registration is not yet created in Oracle E-Business Suite.	Although a valid registration appears in the `FND_MBL_NOTIF_REGISTRATIONS` table, if the user uninstalled the app that created this registration, Oracle E-Business Suite does not know the app has been uninstalled, so the registration remains in the table. If the user reinstalled the app, then a new push token for iOS or registration ID for Android is issued to the app which is stored in Oracle E-Business Suite again and synchronized with MCS or OMH.

Issue	Root Cause	Resolution
Same issue as the described above	**Possible Cause 4:** OMH or MCS is unable to deliver the push notifications.	For each valid record in the `FND_MBL_NOTIF_REGISTRATIONS` table with status REGISTERED, the corresponding registration should be found in OMH or MCS. Use the following steps to validate: 1. Log in to your Oracle Mobile Hub or Oracle Mobile Cloud Service instance. 2. Click the menu icon to open the side menu. • For OMH, select **Development**, and then **Mobile Backends**. • For MCS, select **Applications**, and then **Mobile Backends** 3. Select your mobile backend and click **Open**. 4. Select **Notifications**, then **TEST**, and then **Manage Devices**. 5. Check if you can find a valid OMH or MCS registration for the corresponding record in the `FND_MBL_NOTIF_REGISTRATIONS` table. Please note that push registrations are stored in the following format:

Issue	Root Cause	Resolution
		• Service: iOS or Android • Username: `<EBS username>@<EBS system guid>.<EBS DB SID>` • Application Id: iOS Application Bundle Id or Android Package Name used to create the mobile client.

Issue	Root Cause	Resolution
A push registration with status REGISTERED is found for a user, but it is not found in the OMH or MCS's Manage Devices page.	OMH or MCS removed the entry from its registration because it was unable to deliver notifications to the device.	A push notification will not be delivered to the device if the user uninstalled the app after the registration was created earlier. In this situation, there is an entry in the `FND_MBL_NOTIF_REGISTRATIONS` table, but the corresponding entry is removed by OMH or MCS in its registry. This is expected. The old record in the table is obsolete if OMH or MCS removed the corresponding registration from its registry. To resolve this issue, the user can reinstall the app. The new registration will be created for that user and push notifications can be sent to the device. **Note:** Currently Oracle E-Business Suite does not remove the registration automatically from the table after OMH or MCS removes it from its registry.

Issue	Root Cause	Resolution
Push notification is delivered to the device, but it is not translated to the preferred language set in the user's mobile device.	Possible causes for this issue can be: • The user's mobile device language preference is not installed or supported by Oracle E-Business Suite mobile apps. • The user has installed the same app in multiple devices and each device has a different language setting.	When a registration is created in the `FND_MBL_NOTIF_REGISTRATIONS` table, the user's device locale is captured in the `DEVICE_LANG` column in ISO format, such as `en-US`, `ko-KR`, etc. It can be translated to the languages supported by Oracle E-Business Suite mobile apps and the notification messages can be translated by the server code that triggers the push notification messages. If the user has multiple devices registered for the same app, the language from the last registration is used to translate the messages. To resolve this issue, set the same language preference in multiple mobile devices.

Steps to Troubleshoot Push Notification Issues

In addition to the troubleshooting tips described earlier, this section provides detailed steps to troubleshoot push notifications on the mobile app and the Oracle E-Business Suite server.

1. Checking the Mobile Application Log, page 16-41
2. Checking the Oracle E-Business Suite REST API, page 16-42
3. Checking the Oracle Mobile Hub or Oracle Mobile Cloud Service Setup, page 16-46

Step 1: Checking the Mobile Application Log

If a mobile app does not register for push notifications, you should first review the mobile application log. The mobile app log provides the following details:

- Configuration service XML downloaded from the server
- The push token received during the launch of the app

- Any errors when registering the push token with Oracle E-Business Suite

Step 2: Checking the Oracle E-Business Suite REST API

When a user signs in to an app, as the first step to receive push notifications, the app registers with Oracle E-Business Suite using a REST API. Perform the following tasks to validate the Oracle E-Business Suite REST API:

1. Authenticating and Obtaining Required Authentication Token for Oracle E-Business Suite, page 16-42
2. Checking the mPushRegister REST API, page 16-42
3. Removing the Registration Using the mPushRegister REST API, page 16-44

Step 1: Authenticating and Obtaining Required Authentication Token for Oracle E-Business Suite

Use the following steps to authenticate and obtain required token for Oracle E-Business Suite:

1. Enter the following URL in a web browser and log in with local user name and password to obtain the authentication token.

   ```
   http://<hostname>:<port>/OA_HTML/RF.jsp?function_id=mLogin
   ```

2. In the response XML, note the following values:

   - `<accessTokenName>`**`ebstest`**`</accessTokenName>`
   - `<accessToken>`**`xxxxxxxxxxxxxxxxxxxxxxxxxxx`**`</accessToken>`

3. Use these values to form the Cookie header to be used in subsequent REST requests. For example,

   ```
   Cookie: ebstest=xxxxxxxxxxxxxxxxxxxxxxxxxxx
   ```

Step 2: Checking the mPushRegister REST API

Use this step to check if the `mPushRegister` REST API works and stores data in the `FND_MBL_NOTIF_REGISTRATIONS` table.

> **Note:** To invoke the REST API directly, install a browser extension, such as Advanced REST Client (ARC) or Postman. You can use any GUI-based REST client to test the REST service.

REST API Details and Payload

- HTTP Operation: `POST`
- REST Endpoint: `http://<hostname>:<port>/OA_HTML/RF.jsp?function_id=mPushRegister`

- HTTP Headers:
  - `Content-Type: application/xml`
  - `Cookie: ebstest=xxxxxxxxxxxxxxxxxxxxxxxxxx`
- HTTP Payload:

```
<params>
 <param name="Action">REGISTER</param>
 <param name="Platform">ANDROID</param>
 <param name="App Bundle Id">com.oracle.ebs.atg.owf.
Approvals</param>
 <param name="Push Token">xxxxxxxxxxxxxxxxxxxxxxxxxxx-dummy</param>
 <param name="Device Lang">en-US</param>
</params>
```

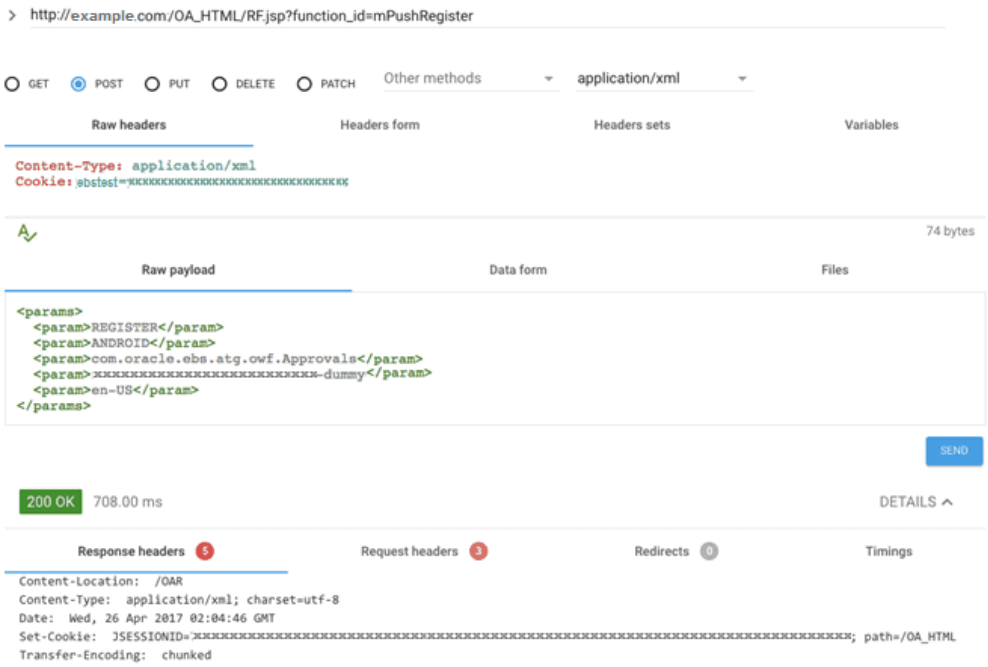
> **Note:** The "App Bundle Id" parameter should be the same as the one used to register the mobile app in the Mobile Applications Manager UI page. This is the same value used in the Id field of `maf-application.xml` in the MAF application.

Invoking the REST API to REGISTER

The following steps describe an example of invoking the REST service directly from the REST client:

1. Invoke the REST service using the REST Client.

Invocation of the REST API to Register an App in the REST Client



```
Content-Type: application/xml
Cookie: ebstest=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
<params>
  <param>REGISTER</param>
  <param>ANDROID</param>
  <param>com.oracle.ebs.atg.owf.Approvals</param>
  <param>xxxxxxxxxxxxxxxxxxxxxxxxxxx-dummy</param>
  <param>en-US</param>
</params>
```

```
Content-Location:  /OAR
Content-Type:  application/xml; charset=utf-8
Date:  Wed, 26 Apr 2017 02:04:46 GMT
Set-Cookie:  JSESSIONID=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx; path=/OA_HTML
Transfer-Encoding:  chunked
```

2. In the HTTP response of REGISTER action, note the `JSESSIONID` cookie in the `Set-Cookie` header.

   This will be passed later in the REST request to remove the registration to make sure the HTTP session is reclaimed on the server.

3. Check in the `FND_MBL_NOTIF_REGISTRATIONS` table for the registration entry for the user entered in the Step 1: Authenticating and Obtaining Required Authentication Token for Oracle E-Business Suite, page 16-42.

   Note that the initial status of the registration is "READY". After this registration is synchronized with Oracle Mobile Hub or Oracle Mobile Cloud Service, the status is changed to "REGISTERED".

Step 3: Removing the Registration Using the mPushRegister REST API

This step checks if the same `mPushRegister` REST API will remove the registration for the app you registered earlier.

REST API Details and Payload

- HTTP Operation: `POST`
- REST Endpoint: `http://<hostname>:<port>/OA_HTML/RF.jsp?function_id=mPushRegister`

- HTTP Headers:
  - `Content-Type: application/xml`
  - `Cookie: ebstest=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx`
  - `JSESSIONID=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx`
- HTTP Payload:

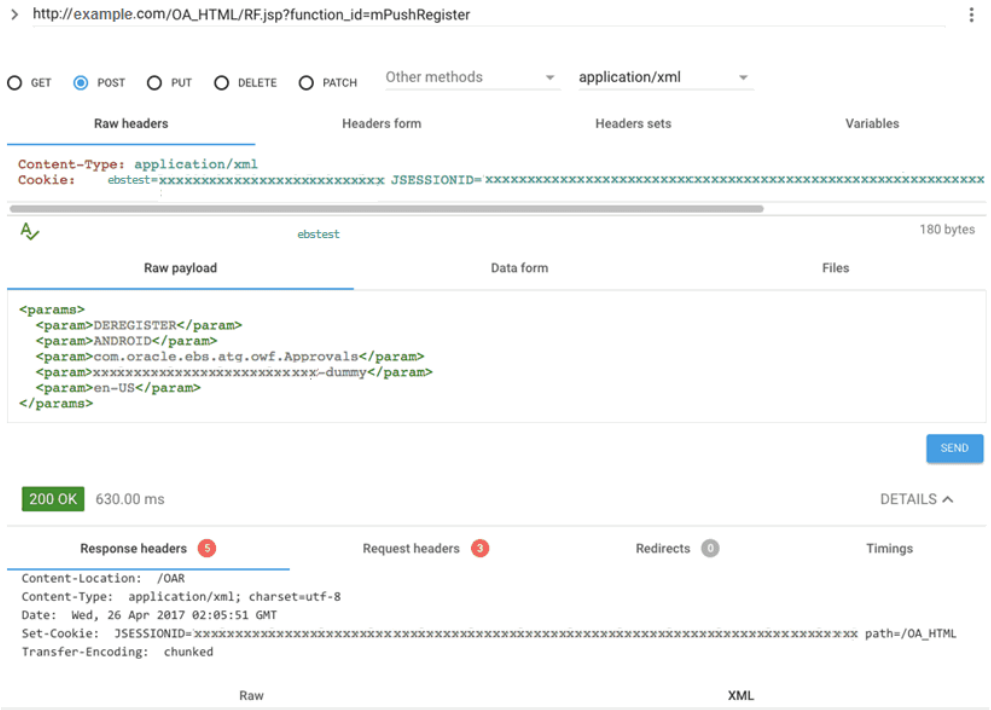
```
<params>
 <param name="Action">DEREGISTER</param>
 <param name="Platform">ANDROID</param>
 <param name="App Bundle Id">com.oracle.ebs.atg.owf.
Approvals</param>
 <param name="Push Token">xxxxxxxxxxxxxxxxxxxxxxxxxx-dummy</param>
 <param name="Device Lang">en-US</param>
</params>
```

Invoking the REST API to Remove the Registration

The following steps describe an example of invoking the REST service directly from the REST client:

1. Invoke the REST service using the Advanced REST Client.

Invocation of the REST API to Remove the Registration in the REST Client



```
Content-Type: application/xml
Cookie:    ebstest=xxxxxxxxxxxxxxxxxxxxxxxxxx JSESSIONID=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
<params>
  <param>DEREGISTER</param>
  <param>ANDROID</param>
  <param>com.oracle.ebs.atg.owf.Approvals</param>
  <param>xxxxxxxxxxxxxxxxxxxxxxxxx-dummy</param>
  <param>en-US</param>
</params>
```

```
200 OK   630.00 ms
```

```
Content-Location:  /OAR
Content-Type:  application/xml; charset=utf-8
Date:  Wed, 26 Apr 2017 02:05:51 GMT
Set-Cookie:  JSESSIONID=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx path=/OA_HTML
Transfer-Encoding:  chunked
```

2. Note that the `JSESSIONID` cookie from the `REGISTER` action is used here.

3. Validate the FND_MBL_NOTIF_REGISTRATIONS table that the registration is removed.

If this `mPushRegister` API works, the mobile app with the given App Bundle Id should be able to register successfully.

Step 3: Checking the Oracle Mobile Hub or Oracle Mobile Cloud Service Setup

Perform the following tasks to validate the setup in Oracle Mobile Hub or Oracle Mobile Cloud Service:

1. Examining Any Synchronization Issues from Oracle E-Business Suite to Oracle Mobile Hub or Oracle Mobile Cloud Service, page 16-46

2. Fixing the SSL Handshake Error, page 16-48

3. Checking the Oracle Mobile Hub REST API or Oracle Mobile Cloud Service REST API, page 16-49

Step 1: Examining Any Synchronization Issues from Oracle E-Business Suite to Oracle Mobile Hub or Oracle Mobile Cloud Service

After a mobile app registers with Oracle E-Business Suite, if the setup tasks performed in Oracle Mobile Hub or Oracle Mobile Cloud Service are successful, the status of the

registration should be changed from "READY" to "REGISTERED". If it is not changed to "REGISTERED", you need to check if there is any issue when Oracle E-Business Suite attempts to synchronize with Oracle Mobile Hub or Oracle Mobile Cloud Service. See: Troubleshooting Tips for Common Setup Issues on the Oracle E-Business Suite Server, page 16-26.

1. Enable the STATEMENT level logging for the Workflow Java Deferred Agent Listener and verify that the business event `oracle.apps.mobile.foundation.push.synch` is processed successfully.

   > **Note:** The business event to synchronize the registration from Oracle E-Business Suite to Oracle Mobile Hub or Oracle Mobile Cloud Service carries information about the user, app's bundle Id, and mobile platform that you can check for issues with the specific user.

2. Following are possible errors reported by Oracle Mobile Hub or Oracle Mobile Cloud Service when the registration is synchronized from Oracle E-Business Suite to Oracle Mobile Hub or Oracle Mobile Cloud Service.

   - `HTTP 401`
     - Check the user name and password registered in Oracle E-Business Suite.

       The user credentials are validated at the time of configuration. Most likely the credentials are still valid.

     - Check if the user has the "Mobile Notifications" and "Default – (MCS backend realm)" roles assigned.
   - `HTTP 400`
     - Check if the mobile client is registered on Oracle Mobile Hub or Oracle Mobile Cloud Service with appropriate deployment bundle Id.
   - `HTTP 500`
     - Check if the Oracle Mobile Hub or Oracle Mobile Cloud Service instance is accessible.
   - SSL handshake error with the following exception:

     ```
     sun.security.validator.ValidatorException: PKIX path
     building failed: sun.security.provider.certpath.
     SunCertPathBuilderException: unable to find valid
     certification path to requested target
     ```

     - Make sure to import the OMH or MCS REST endpoint certificates into the truststore in Oracle E-Business Suite.

See: Fixing the SSL Handshake Error, page 16-48.

Step 2: Fixing the SSL Handshake Error

Perform the following steps to download the OMH or MCS REST endpoint's CA certificate and import to the truststore in Oracle E-Business Suite:

1. Access the Oracle Mobile Hub or Oracle Mobile Cloud Service endpoint URL in a web browser. For example,

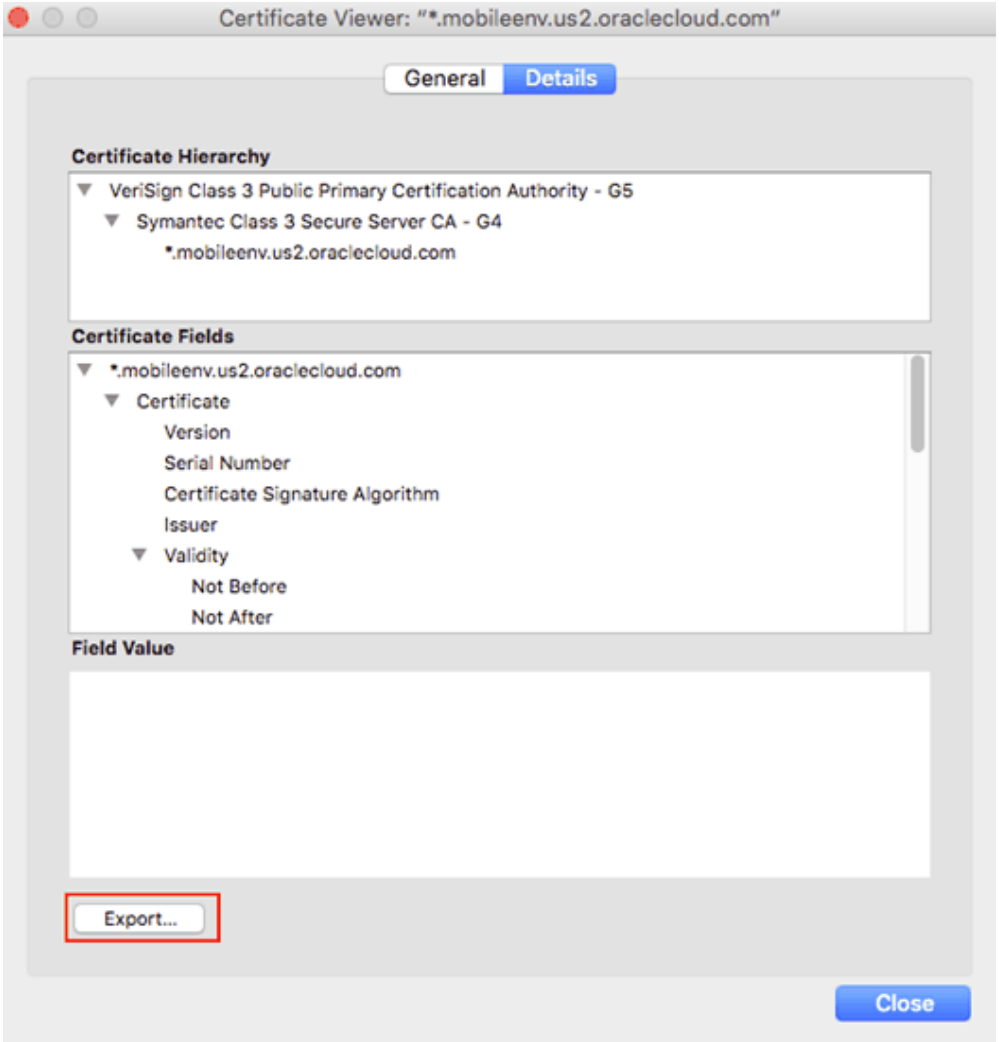
   ```
   http://<hostname>:<port>
   ```

   > **Note:** This is the same value entered in the Backend URL field when configuring the Push Notification System. See: Configuring Oracle E-Business Suite Mobile Foundation Push Notification System, page 10-11.

2. Click the **Padlock** icon next to the URL in a web browser (such as in Firefox) or use browser-specific steps to export the CA certificate for the OMH or MCS endpoint to a local certificate file.

3. Export the CA certificate from the browser.

Certificate Viewer Screen with Export Button Highlighted



4. Import the certificate to the truststore in Oracle E-Business Suite.

```
keytool -import -trustcacerts -keystore
$AF_JRE_TOP/lib/security/cacerts -storepass password -alias
verisignclass3g5ca -file verisign.crt
```

Step 3: Checking the Oracle Mobile Hub or Oracle Mobile Cloud Service REST API

Every device registered in Oracle E-Business Suite is synchronized with Oracle Mobile Hub or Oracle Mobile Cloud Service using the following REST API. It is important that you run this API standalone to make sure the REST API works fine.

MCS REST API Details and Payload Example

- HTTP Operation: `POST`

- REST Endpoint: `http://<hostname>:<port>/mobile/platform/devices/register`

- HTTP Headers:

  - `Content-Type: application/json; charset=UTF-8`

  - `Oracle-Mobile-Backend-ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`

  - `Authorization: Basic <MCS credentials>`

- HTTP Payload:

```
{
    "notificationToken":"xxxxxxxxxx-xxxxxxxxxx-
xx_xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx-
xxxxxxxxxxxxxxxxxxxxxxx_xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx-
xxxxxxxxxxxxxxxxxxxxxxxxxxxx",
    "notificationProvider":"GCM",
    "user":"xxxxxx@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.xxxxxxx",
    "mobileClient":{
        "id":"com.oracle.ebs.atg.wf.Approvals",
        "version":"1.5.0",
        "platform":"ANDROID"
    }
}
```

> **Note:** The "`user`" attribute could be any string value when testing this API directly. Oracle Mobile Hub or Oracle Mobile Cloud Service does not validate the "`user`" attribute against any user repository.
>
> The "`mobileClient`" and "`id`" attributes should be the same values used to create the mobile client in Oracle Mobile Hub or Oracle Mobile Cloud Service.

The following steps describe an example of invoking the MCS REST service directly using Advanced REST Client:

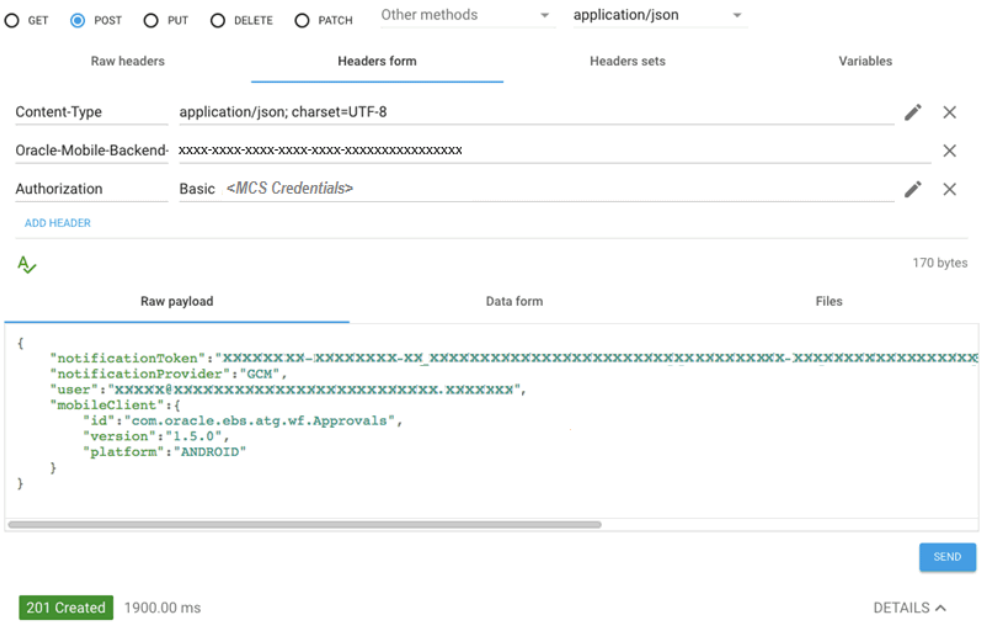
1. Invoke the Oracle Mobile Cloud Service REST API from the REST client.

2. Use the same user name and password registered with Oracle E-Business Suite.

3. Enter the payload information. Make sure to use the correct Backend ID (`Oracle-Mobile-Backend-ID`) that is used to configure the Oracle E-Business Suite Mobile Foundation Push Notification System.

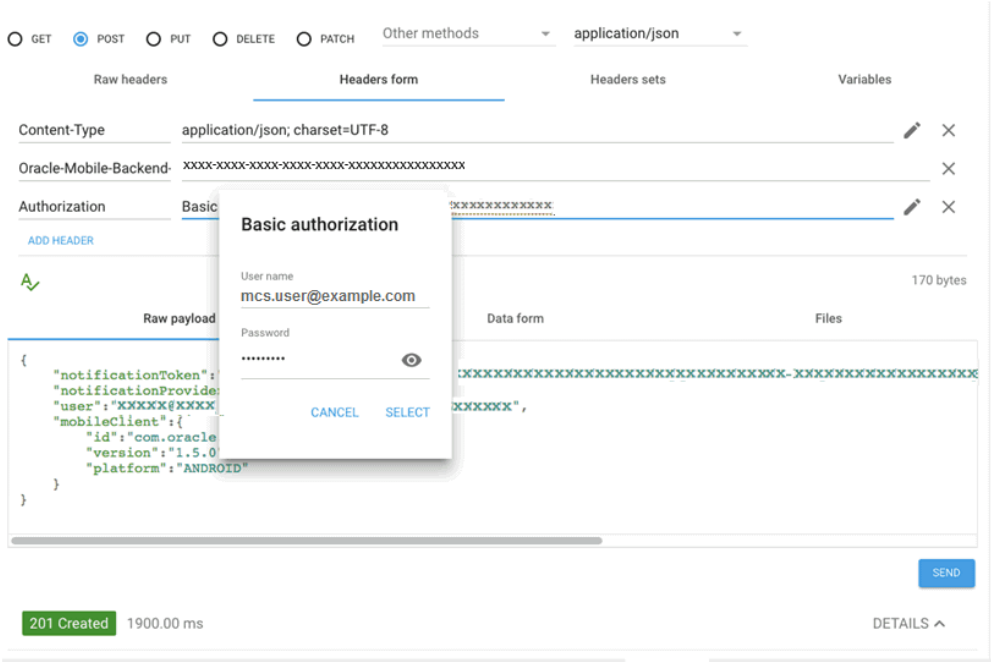
   See: Configuring Oracle E-Business Suite Mobile Foundation Push Notification System, page 10-11.

Example of an Oracle Mobile Cloud Service REST Service Invocation in the Advanced REST Client



4. In the Advanced REST Client, you can click the **Edit** icon for the Authorization header to enter the Basic Auth user name and password. The tool automatically encodes it to `Base64`.

Basic Authentication User Name and Password Directly Entered to the Advanced REST Client



5. This should return `HTTP 201 Created` to indicate the device registration with Oracle Mobile Cloud Service was successful.

   Note if you used a dummy value, you could clear it from Oracle Mobile Cloud Service or leave it as is.

A

Product Family Patches for Earlier Oracle E-Business Suite Mobile Foundation Releases

Overview

This appendix lists the Oracle E-Business Suite mobile apps server-side patches for the most recent releases prior to the current release, Oracle E-Business Suite Mobile Foundation 9.1, and an earlier Release 9.0. These patches include Oracle E-Business Suite level patch if available, consolidated product family patches, and conditionally required pre-install and post-install patches if needed.

These server-side patches for Oracle E-Business Suite Mobile Foundation releases are described as follows:

- Product Family Patches for Oracle E-Business Suite Mobile Foundation Release 8.0, page A-1
- Product Family Patches for Oracle E-Business Suite Mobile Foundation Release 7.0, page A-17

For more information on server-side prerequisite patches and patches for Oracle E-Business Suite Mobile Foundation 9.1 and 9.0, refer to Applying Prerequisite Patches on the Oracle E-Business Suite Server, page 9-1.

Product Family Patches for Oracle E-Business Suite Mobile Foundation Release 8.0

This section describes the patch information and tasks required for the mobile apps that are built with Oracle E-Business Suite Mobile Foundation Release 8.0. Perform the required tasks to apply prerequisite patches in the following sequence:

1. Performing Conditional Pre-Install Tasks, page A-2

2. Applying Patches for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 8.0, page A-2

3. Applying Conditional Post-Install Patches, page A-15

Step 1: Performing Conditional Pre-Install Tasks

For Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 8.0

Perform any additional conditionally required pre-install tasks from the following list for your apps built with Oracle E-Business Suite Mobile Foundation Release 8.0:

Conditional Pre-Install Tasks for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 8.0

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 and 12.1.3 • Oracle Mobile Maintenance for Oracle E-Business Suite	Required only if you plan to implement Oracle Mobile Maintenance for Oracle E-Business Suite	Oracle Mobile Maintenance "Disconnected" feature uses the Oracle Mobile Field Service Multiplatform framework, which does not require Oracle Lite and consequently Oracle Lite should be uninstalled. If the "mobileadmin" schema exists, refer to My Oracle Support Knowledge Document 1564644.1, *Oracle Mobile Field Service Store and Forward Multiple Platforms Support*.

Step 2: Applying Patches for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 8.0

Important: If you install or upgrade your apps to the version built with Oracle E-Business Suite Mobile Foundation Release 8.0, then you must apply the server-side prerequisites through one of the methods described in this section.

Important: The Oracle E-Business Suite 12.2 server-side patches listed in this section for Oracle E-Business Suite Mobile Foundation Release 8.0 are already included in the respective product family patches in Oracle E-Business Suite Release 12.2.8. If you have installed Oracle E-Business Suite 12.2.8, skip this section and simply apply the post-install patches, as described in Applying Conditional Post-Install Patches, page A-15.

Apply the server-side patches in either of the following ways based on your needs:

Note: Starting from Oracle E-Business Suite Mobile Foundation Release 7.0 and onwards, Oracle allows you to apply the server-side patches either through Oracle E-Business Suite level patch or product family level patch for your Oracle E-Business Suite release depending on your needs.

- **Apply the Oracle E-Business Suite level patch for your Oracle E-Business Suite release**

  To simplify the patching efforts, all product family patches except Oracle Yard Management (YMS) are consolidated into a single Oracle E-Business Suite level patch for a specific Oracle E-Business Suite release. Additionally, this Oracle E-Business Suite level patch includes the patch for Oracle Mobile Supply Chain Applications for Oracle E-Business Suite (MSCA), although this app is not built with Oracle E-Business Suite Mobile Foundation.

  - For Oracle E-Business Suite Release 12.1.3

    Patch 26965481:R12.SCM_PF.B: MSCA-12.1 Consolidated Patch For Mobile App V8

  - For Oracle E-Business Suite Release 12.2

    Patch 26965486:R12.SCM_PF.C: MSCA-12.2 Consolidated Patch For Mobile App V8

  If you intend to uptake all the product family patches and the patch for the MSCA app, simply apply this higher level consolidated patch for your Oracle E-Business Suite release that in turn contains all the patches corresponding to Oracle E-Business Suite mobile apps (including MSCA mentioned above) except Oracle Mobile Yard for Oracle E-Business Suite.

  For Oracle Mobile Yard for Oracle E-Business Suite, the required Patch 26728820: R12.ATG_PF.C is already contained in the Oracle E-Business Suite level patch. If you plan to use this app and have already applied Patch 24383610:R12.YMS.C as part of the Oracle E-Business Suite Mobile Release 7 uptake, then there is no additional patch to be applied in this release.

The following table lists the Oracle E-Business Suite level consolidated patches:

Oracle E-Business Suite Level Patches for Oracle E-Business Suite Mobile Foundation Release 8.0

Oracle E-Business Suite Level Patch	Oracle E-Business Suite 12.1.3	Oracle E-Business Suite 12.2
Oracle E-Business Suite level patches contain: • All the product family level patches except Oracle Yard Management (yms) • Oracle Mobile Supply Chain Applications for Oracle E-Business Suite (MSCA), not built with Oracle E-Business Suite Mobile Foundation	Patch 26733898:12.1.0 • This Oracle E-Business Suite 12.1.3 patch includes Patch 26965481: R12.SCM_PF.B for MSCA, in addition to each product family patch listed in the product family level patch table.	Patch 26733910:12.2.0 • This Oracle E-Business Suite 12.2 patch includes Patch 26965486:R12.SCM_PF.C for MSCA, in addition to each product family patch listed in the product family level patch table except Oracle Yard Management. To use Oracle Mobile Yard for Oracle E-Business Suite, apply Patch 24383610:R12.YMS.C - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied.

- **Apply the product family level patch for your Oracle E-Business Suite release**

  If you plan to apply the patches only for the relevant product families, rather than for all product families, use this approach to apply the patches for your Oracle E-Business Suite mobile apps.

  > **Note:** The patch for Oracle Mobile Supply Chain Applications for Oracle E-Business Suite described earlier is only included in the Oracle E-Business Suite level patches; it is not included in the Oracle Supply Chain Management (scm_pf) product family patches. If you plan to use this app, and you do not plan to apply the Oracle E-Business Suite level patch, then you must apply the MSCA patch individually for your Oracle E-Business Suite release.

For example, if you use the Inventory and Timecards approval types in the Approvals app, and you are upgrading only the Approvals app to the version built with Oracle E-Business Suite Mobile Foundation 8.0, then you can apply the Oracle

E-Business Suite level consolidated patch for all product families. Alternatively, you can apply only the relevant product family patches for your Oracle E-Business Suite release level, in this case the Oracle Supply Chain Management product family patch for Inventory approvals and the Oracle Human Resources product family patch for Timecard approvals.

> **Important:** Oracle is discontinuing selected Oracle E-Business Suite mobile apps. Therefore, no patches for these apps are included in their respective product family patches released after their discontinuation dates. For information about the apps being discontinued, refer to the Discontinued Oracle E-Business Mobile Apps section in *Oracle E-Business Suite Mobile Apps, Release 12.1 and 12.2 Documentation Index*, My Oracle Support Knowledge Document 1641772.1.

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

Oracle E-Business Suite Product Family Level Patches for Oracle E-Business Suite Mobile Foundation Release 8.0

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 (for developing custom approval types) • Custom mobile apps for Oracle E-Business Suite, including the REST services that the sample app uses to provide real app flows See: *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2.*	Patch 26728355:R12.ATG_PF.B: ATG -12.1 Consolidated Patch For Mobile Applications Foundation V8 Apply the product family patches for the seeded approval types you want to use, as shown in subsequent rows in this table.	Patch 26728820:R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V8 Apply the product family patches for the seeded approval types you want to use, as shown in subsequent rows in this table.

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Financials (fin_pf) (See **Footnote 4**, page A-14)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Expense approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Supplier Invoices approvals)	Apply the following patches: • Patch 26728355: R12.ATG_PF.B: ATG - 12.1 Consolidated Patch For Mobile Applications Foundation V8 • Patch 24383296: R12.FIN_PF.B: FIN - 12.1 Consolidated Patch For Mobile Applications Foundation V7 if not already applied	Apply the following patches: • Patch 26728820: R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V8 • Patch 24383588: R12.FIN_PF.C: FIN - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied

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 Human Resources 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 • Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite	Patch 26728771:R12.HR_PF.B: HRMS - 12.1 Consolidated Patch For Mobile Applications Foundation V8	Patch 26728887:R12.HR_PF.C: HRMS - 12.2 Consolidated Patch For Mobile Applications Foundation V8

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Interaction Center Family (cc_pf) (See **Footnote 4**, page A-14)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Channel Revenue Management approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Quoting approvals)	Apply the following patches: • Patch 26728355: R12.ATG_PF.B: ATG - 12.1 Consolidated Patch For Mobile Applications Foundation V8 • Patch 24383355: R12.CC_PF.B: CRM - 12.1 Consolidated Patch For Mobile Applications Foundation V7 if not already applied	Apply the following patches: • Patch 26728820: R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V8 • Patch 24383599: R12.CC_PF.C: CRM - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied

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) (See **Footnote 4**, page A-14)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Purchase Order approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Requisition approvals)	Apply the following patches: • Patch 26728355: R12.ATG_PF.B: ATG - 12.1 Consolidated Patch For Mobile Applications Foundation V8 • Patch 24383344: R12.PRC_PF.B: PRC - 12.1 Consolidated Patch For Mobile Applications Foundation V7 if not already applied	Apply the following patches: • Patch 26728820: R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V8 • Patch 24383558: R12.PRC_PF.C: PRC - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Projects (pj_pf) (See **Footnote 4**, page A-14)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Projects approvals)	Apply the following patches: • Patch 26728355: R12.ATG_PF.B: ATG - 12.1 Consolidated Patch For Mobile Applications Foundation V8 • Patch 24383283: R12.PJ_PF.B: PROJ - 12.1 Consolidated Patch For Mobile Applications Foundation V7 if not already applied	Apply the following patches: • Patch 26728820: R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V8 • Patch 24383522: R12.PJ_PF.C: PROJ - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied

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 Inventory approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Product Information approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Order Management approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Maintenance approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Service Contracts approvals) • Oracle Mobile Discrete Production Supervisor for	Patch 26728381:R12.SCM_PF.B: SCM -12.1 Consolidated Patch For Mobile Applications Foundation V8	Patch 26728844:R12.SCM_PF.C: SCM -12.2 Consolidated Patch For Mobile Applications Foundation V8

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 • 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 Sales Orders for Oracle E-Business Suite		

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Yard Management (yms) (See **Footnote 4**, page A-14)	• Oracle Mobile Yard for Oracle E-Business Suite	N/A	Apply the following patches: • Patch 26728820: R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V8 • Patch 24383610: R12.YMS.C:YMS - 12.2 Consolidated Patch For Mobile Applications Foundation V7 if not already applied **Prerequisites:** • Oracle E-Business Suite Release 12.2.3 • R12.SCM_PF.C. Delta.4 • R12.AD.C.Delta. 9 & R12.TXK.C. Delta.9

Footnote 4: In this Oracle E-Business Suite Mobile Foundation Release 8, if you are upgrading any mobile apps within the product family to the version built with Oracle E-Business Suite Mobile Foundation 8.0, then apply the following patches:

- Oracle E-Business Suite Applications Technology (atg_pf) patch corresponding to Oracle E-Business Suite Mobile Foundation Release 8.0

- Product family patch from the Oracle E-Business Suite Mobile Foundation Release 7.0 if not already applied

Step 3: Applying Conditional Post-Install Patches

For Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 8.0

Apply any additional conditionally required post-install patches from the following list for your apps built with Oracle E-Business Suite Mobile Foundation Release 8.0:

Conditional Post-Install Patches for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 8.0

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 and 12.1.3 • Oracle E-Business Suite Mobile Foundation Release 8.0 Online Help	Required for all Oracle E-Business Suite mobile apps, built with Oracle E-Business Suite Mobile Foundation Release 8.0, connected to Oracle E-Business Suite Release 12.1.3 or Release 12.2	• Release 12.2 and 12.1.3: Patch 27678444

Oracle E-Business Suite Release 12.2 and 12.1.3	Required for all Oracle E-Business Suite mobile apps, built with Oracle E-Business Suite Mobile Foundation Release 8.0, connected to Oracle E-Business Suite Release 12.1.3 or Release 12.2	• Release 12.2
		  • Patch 28278350:R12.OWF.C
		  • Patch 23717395:R12.FND.C
		• Release 12.1.3
		  • Patch 28278350:R12.OWF.B
		  • Patch 23717395:R12.FND.B

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 and 12.1.3	Required only if your Oracle E-Business Suite environment has the following patches applied: • Release 12.2 - Patch 27761509:12.2.0 (Oracle Applications Release 12.2 : Consolidated Patch for Data Removal Tool) • Release 12.1.3 - Patch 27822242:12.1.0 (Oracle Applications Release 12.1 : Consolidated Patch for Data Removal Tool)	Perform the following steps in the specified order: • Release 12.2: 1. Apply Patch 28295762:R12.PER.C. 2. Apply Patch 28303904:R12.FND.C. 3. Recompile the data removal metadata by running the concurrent program "Recompile Metadata for Data Removal Tool", with the "Entity Type" parameter set to "ALL". • Release 12.1.3: 1. Apply Patch 28295762:R12.PER.B. 2. Apply Patch 28303904:R12.FND.B. 3. Recompile the data removal metadata by running the concurrent program "Recompile Metadata for Data Removal Tool", with the "Entity Type" parameter set to "ALL".

Additional Information: To develop custom apps for Oracle E-Business Suite, you need to download the following client-side patch for Oracle E-Business Suite Release 12.1.3 and Release 12.2:

- Patch 27958894 - Oracle E-Business Suite Mobile Foundation (Login component) Release 8.0

This patch enables the Oracle E-Business Suite Mobile Foundation client libraries, application template, and sample app; therefore, apply this patch on the mobile client, not on the Oracle E-Business Suite server.

For information on developing custom apps for Oracle E-Business Suite and using the sample app. See: *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

Product Family Patches for Oracle E-Business Suite Mobile Foundation Release 7.0

This section describes the patch information and tasks required for the mobile apps that are built with Oracle E-Business Suite Mobile Foundation Release 7.0. Perform the required tasks to apply prerequisite patches in the following sequence:

1. Performing Conditional Pre-Install Tasks, page A-17
2. Applying Patches for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 7.0, page A-18
3. Applying Conditional Post-Install Patches, page A-27

For information on prerequisite patches for earlier Oracle E-Business Suite Mobile Foundation releases, see Product Family Patches for Earlier Oracle E-Business Suite Mobile Foundation Releases, page A-1.

Step 1: Performing Conditional Pre-Install Tasks

For Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 7.0

Perform any additional conditionally required pre-install tasks from the following list for your apps built with Oracle E-Business Suite Mobile Foundation Release 7.0:

Conditional Pre-Install Tasks for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 7.0

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 and 12.1.3 • Oracle Mobile Maintenance for Oracle E-Business Suite	Required only if you plan to implement Oracle Mobile Maintenance for Oracle E-Business Suite	Oracle Mobile Maintenance "Disconnected" feature uses the Oracle Mobile Field Service Multiplatform framework, which does not require Oracle Lite and consequently Oracle Lite should be uninstalled. If the "mobileadmin" schema exists, refer to My Oracle Support Knowledge Document 1564644.1, *Oracle Mobile Field Service Store and Forward Multiple Platforms Support*.

Step 2: Applying Patches for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 7.0

Important: If you install or upgrade your apps to the version built with Oracle E-Business Suite Mobile Foundation Release 7.0, then you must apply the server-side prerequisites through one of the methods described in this section.

Important: The Oracle E-Business Suite 12.2 server-side patches listed in this section for Oracle E-Business Suite Mobile Foundation Release 7.0 are already included in the respective product family patches in Oracle E-Business Suite Release 12.2.7. If you have installed Oracle E-Business Suite 12.2.7, skip this section and simply apply the post-install patches, as described in Applying Conditional Post-Install Patches, page A-27.

Starting from Oracle E-Business Suite Mobile Foundation Release 7.0, you can apply the server-side patches in either of the following ways based on your needs:

- **Apply the Oracle E-Business Suite level patch for your Oracle E-Business Suite**

release

To simplify the patching efforts, starting from Oracle E-Business Suite Mobile Foundation Release 7.0, all product family patches except Oracle Yard Management (YMS) are consolidated into a single Oracle E-Business Suite level patch for a specific Oracle E-Business Suite release.

If you intend to uptake all the product family patches, simply apply this higher level consolidated patch for your Oracle E-Business Suite release that in turn contains all the patches corresponding to Oracle E-Business Suite mobile apps except Oracle Mobile Yard for Oracle E-Business Suite. Then apply patch 24383610: R12.YMS.C if you plan to use Oracle Mobile Yard for Oracle E-Business Suite.

The following table lists the Oracle E-Business Suite level consolidated patches:

Oracle E-Business Suite Level Patches for Oracle E-Business Suite Mobile Foundation Release 7.0

Oracle E-Business Suite Level Patch	Oracle E-Business Suite 12.1.3	Oracle E-Business Suite 12.2
Oracle E-Business Suite level patches contain all the product family level patches except Oracle Yard Management (yms).	Patch 25486920:12.1.0	Patch 25486940:12.2.0 • To use Oracle Mobile Yard for Oracle E-Business Suite, apply the additional patch 24383610:R12.YMS.C, as listed in the product family level patch table for Oracle Yard Management (yms).

- **Apply the product family level patch for your Oracle E-Business Suite release**

  If you plan to apply the patches only for the relevant product families, rather than for all product families, use this approach to apply the patches for your Oracle E-Business Suite mobile apps.

  For example, if you use the Supplier Invoices and Timecards approval types in the Approvals app, and you are upgrading only the Approvals app to the version built with Oracle E-Business Suite Mobile Foundation 7.0, then you can apply the Oracle E-Business Suite level consolidated patch for all product families. Alternatively, you can apply only the relevant product family patches for your Oracle E-Business Suite release level, in this case the Oracle Financials product family patch for Supplier Invoices approvals and the Oracle Human Resources product family patch for Timecard approvals.

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

Oracle E-Business Suite Product Family Level Patches for Oracle E-Business Suite Mobile Foundation Release 7.0

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 (for developing custom approval types) • Custom mobile apps for Oracle E-Business Suite, including the REST services that the sample app uses to provide real app flows See: *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2.*	Patch 24383252:R12.ATG_PF.B: ATG -12.1 Consolidated Patch For Mobile Applications Foundation V7 Apply the product family patches for the seeded approval types you want to use, as shown in subsequent rows in this table.	Patch 24383477:R12.ATG_PF.C - 12.2 Consolidated Patch For Mobile Applications Foundation V7 Apply the product family patches for the seeded approval types you want to use, as shown in subsequent rows in this table.

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
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 24383296:R12.FIN_PF.B: FIN - 12.1 Consolidated Patch For Mobile Applications Foundation V7	Patch 24383588:R12.FIN_PF.C: FIN - 12.2 Consolidated Patch For Mobile Applications Foundation V7

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 Human Resources 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 • Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite	Patch 24383330:R12.HR_PF.B: HRMS - 12.1 Consolidated Patch For Mobile Applications Foundation V7	Patch 24383538:R12.HR_PF.C: HRMS - 12.2 Consolidated Patch For Mobile Applications Foundation V7

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Interaction Center Family (cc_pf)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Channel Revenue Management approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Quoting approvals)	Patch 24383355:R12.CC_PF.B: CRM- 12.1 Consolidated Patch For Mobile Applications Foundation V7	Patch 24383599:R12.CC_PF.C: CRM- 12.2 Consolidated Patch For Mobile Applications Foundation V7
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 24383344:R12.PRC_PF.B: PRC - 12.1 Consolidated Patch For Mobile Applications Foundation V7	Patch 24383558:R12.PRC_PF.C: PRC - 12.2 Consolidated Patch For Mobile Applications Foundation V7

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
Oracle Projects (pj_pf)	• Oracle Mobile Approvals for Oracle E-Business Suite (for Projects approvals) • Oracle Mobile Project Manager for Oracle E-Business Suite	Patch 24383283:R12.PJ_PF.B: PROJ - 12.1 Consolidated Patch For Mobile Applications Foundation V7	Patch 24383522:R12.PJ_PF.C: PROJ - 12.2 Consolidated Patch For Mobile Applications Foundation V7

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 Inventory approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Product Information approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Order Management approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Maintenance approvals) • Oracle Mobile Approvals for Oracle E-Business Suite (for Service Contracts approvals) • Oracle Mobile Discrete Production Supervisor for	Patch 24383271:R12.SCM_PF.B: SCM -12.1 Consolidated Patch For Mobile Applications Foundation V7	Merge and apply the following patches using the command: • Patch 26571092: R12.EAM.C • Patch 24383496: R12.SCM_PF.C: SCM -12.2 Consolidated Patch For Mobile Applications Foundation V7 `adop phase=apply patches=26571092,24383496 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 E-Business Suite • Oracle Mobile Discrete Quality Manager 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 Process Quality Manager for Oracle E-Business Suite • Oracle Mobile Product Information for Oracle E-Business Suite • Oracle Mobile Project Manufacturing		

Product Family	Mobile App Name	Patch for Oracle E-Business Suite 12.1.3	Patch for Oracle E-Business Suite 12.2
	for Oracle E-Business Suite • Oracle Mobile Sales Orders for Oracle E-Business Suite		
Oracle Yard Management (yms)	• Oracle Mobile Yard for Oracle E-Business Suite	N/A	Patch 24383610:R12.YMS.C: YMS - 12.2 Consolidated Patch For Mobile Applications Foundation V7 **Prerequisites:** • Oracle E-Business Suite Release 12.2.3 • R12.SCM_PF.C.Delta.4 • R12.AD.C.Delta.9 & R12.TXK.C.Delta.9

Step 3: Applying Conditional Post-Install Patches

For Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 7.0

Apply any additional conditionally required post-install patches from the following list for your apps built with Oracle E-Business Suite Mobile Foundation Release 7.0:

Conditional Post-Install Patches for Mobile Apps Built with Oracle E-Business Suite Mobile Foundation Release 7.0

Oracle E-Business Suite Release or Mobile App Name	Requirement	Patch Information
Oracle E-Business Suite Release 12.2 and 12.1.3 • Oracle E-Business Suite Mobile Foundation Release 7.0 Online Help	Required for all Oracle E-Business Suite mobile apps, with Oracle E-Business Suite Mobile Foundation Release 7.0, connected to Oracle E-Business Suite Release 12.1.3 or Release 12.2	• Release 12.2 and 12.1.3: Patch 26000442
Oracle E-Business Suite Release 12.2 only	Required for all Oracle E-Business Suite mobile apps, with Oracle E-Business Suite Mobile Foundation Release 7.0, connected to Oracle E-Business Suite 12.2 instances with either one of the following conditions: • Oracle E-Business Suite Release 12.2.x with patch 26721370:R12.FND.C applied • Oracle E-Business Suite Release 12.2.7 only	• Patch 26980344:R12.FND.C

Additional Information: To develop custom apps for Oracle E-Business Suite, you need to download the following client-side patch for Oracle E-Business Suite Release 12.1.3 and Release 12.2:

- Patch 26023015 - Oracle E-Business Suite Mobile Foundation (Login component) Release 7.0

This patch enables the Oracle E-Business Suite Mobile Foundation client libraries, application template, and sample app; therefore, apply this patch on the mobile client, not on the Oracle E-Business Suite server.

For information on developing custom apps for Oracle E-Business Suite and using the sample app. See: *Oracle E-Business Suite Mobile Apps*

Developer's Guide, Release 12.1 and 12.2.

To implement Oracle seeded APIs for custom app development, the following patches are available in Oracle E-Business Suite Mobile Foundation 7.1 for the APIs associated with the Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite mobile app for Pay Information, Pay Simulator, and Change Pay:

- For Oracle E-Business Suite 12.2: patch 26831849:R12.PER.C
- For Oracle E-Business Suite 12.1.3: patch 26831849:R12.PER.B

For more information about these APIs, see My Oracle Support Knowledge Document 2312158.1, *FAQ for Accessing the Payslip and Pay Simulator REST APIs*.

For implementation information on using these APIs, see: Implementing Oracle E-Business Suite REST Services, *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

B

Mobile App Access Roles

Overview

Oracle E-Business Suite mobile apps use access roles to protect mobile app data from unauthorized access. The appendix includes the following topics:

Mobile App Access Roles

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, refer to the following section based on your mobile release:

- For Oracle E-Business Suite Mobile Apps Release 10.x, see Setting Up Mobile App Access to Responsibilities (for Oracle Self-Service HR for EBS and Oracle Timecards for EBS), page 2-8 and Setting Up Mobile App Access to Responsibilities (for Oracle Maintenance for EBS), page 2-35.
- For Oracle E-Business Suite Mobile Apps Release 9.x and Earlier, see Setting Up Mobile App Access to Responsibilities, page 9-44.

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
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 Discrete Quality Manager for Oracle E-Business Suite	Mobile Discrete Quality Manager	UMX|MOBILE DISCRETE QUALITY MANAGER
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

Mobile App Name	Role Name	Role Code
Oracle Mobile Process Quality Manager for Oracle E-Business Suite	Mobile Process Quality Manager	UMX|GMD_MOBILE_QUALITY_MANAGER
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	OM Mobile Sales Order Inquiry App Access	UMX|MBL|ONT_MBL_INQ_APP_ACCESS
Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite	App Access Role for Self-Service HR	UMX|MBL|SELFSERVICE_HR_APP_ACCES_ROLE
Oracle Mobile Yard for Oracle E-Business Suite	YMS ADF Mobile App Access	UMX|UNMX|MBL|YMS_MBL_ADF_APP_ACCESS

Mobile App REST Services Permission Sets

If you create a new mobile app access role for an enterprise app built from the associated mobile application archive file for enterprise distribution, make sure that the corresponding REST services permission set of the seeded app is granted to the new access role.

For information on creating enterprise-distributed mobile apps from mobile application archives, see *Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2*.

The following table lists the REST services permission set information for each Oracle E-Business Suite mobile app:

Mobile App REST Services Permission Sets

Mobile App Name	Permission Set Name	Permission Set Code
Oracle Mobile Approvals for Oracle E-Business Suite	N/A	N/A

Mobile App Name	Permission Set Name	Permission Set Code
Oracle Mobile Timecards for Oracle E-Business Suite	Mobile Time Entry	HXC_MOB_TIME_ENTRY
Oracle Mobile Learning for Oracle E-Business Suite	OLM Learner Mobile Application Menu	OTA_LRNR_MOB_APP_MENU
Oracle Mobile Person Directory for Oracle E-Business Suite	Person Directory Mobile App Menu	PER_MOB_PERSON_DIRECTORY_MENU
Oracle Mobile iProcurement for Oracle E-Business Suite	ICX Mobile iProcurement Inquiry App REST Services	ICX_MBL_INQ_REST_SERVICES
Oracle Mobile Procurement for Oracle E-Business Suite	PO Mobile Purchasing App REST Services	PO_MBL_REST_SERVICES
Oracle Mobile Project Manager for Oracle E-Business Suite	PA Mobile Project Manager App REST Services	PA_MBL_PRJ_MGR_REST_SERVICES
Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite	WIP Rest Service	WIP_REST_SERVICE
Oracle Mobile Discrete Quality Manager for Oracle E-Business Suite	Quality REST Access Permission Set	QA_REST_MENU
Oracle Mobile Inventory for Oracle E-Business Suite	INV Mobile Inventory App REST Services	INV_MBL_INV_REST_SERVICES
Oracle Mobile Maintenance for Oracle E-Business Suite	EAM Menu for Rest functions	EAM_REST_MENU
Oracle Mobile Process Production Supervisor for Oracle E-Business Suite	GME Mobile Supervisor Permission Set	PS_GME_MOBILE_SUPERVISOR
Oracle Mobile Process Quality Manager for Oracle E-Business Suite	GMD Mobile Quality Manager Permission Set	PS_GMD_MOBILE_QUALITY_MANAGER

Mobile App Name	Permission Set Name	Permission Set Code
Oracle Mobile Product Information for Oracle E-Business Suite	PIM Restful Services	PIM_REST_SERVICES
Oracle Mobile Project Manufacturing for Oracle E-Business Suite	PJM Mobile Project Manufacturing App REST Services	PJM_MBL_PROJMFG_REST_SERVICES
Oracle Mobile Sales Orders for Oracle E-Business Suite	PJM Mobile Project Manufacturing App REST Services	PJM_MBL_PROJMFG_REST_SERVICES
Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite	App Access Permission Set for Self-Service HR Mobile	PER_SSHR_MOB_APP_ACCESS_PS
Oracle Mobile Yard for Oracle E-Business Suite	YMS Mobile ADF App REST Services	YMS_MBL_ADF_REST_SERVICES

C

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.

- For Oracle E-Business Suite Mobile Apps Release 10.x, see Enabling Server Logging, page 7-2.
- For Oracle E-Business Suite Mobile Apps Release 9.1 and Earlier, see Enabling Server Logging, page 16-2.

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

Mobile App Name	Module Name
Oracle Mobile Procurement for Oracle E-Business Suite	po.mobile
Oracle Mobile Project Manager for Oracle E-Business Suite	PA
Oracle Mobile Discrete Production Supervisor for Oracle E-Business Suite	WIP%
Oracle Mobile Discrete Quality Manager for Oracle E-Business Suite	qa.maf.quality%
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 Process Quality Manager for Oracle E-Business Suite	gmd.maf.quality%
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
Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite	com.oracle.ebs.hr.per.Selfservice
Oracle Mobile Yard for Oracle E-Business Suite	yms.mobapp%

D

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:

- For Oracle E-Business Suite Mobile Apps Release 10.x, see Enabling a Mobile App Individually and Specifying the Configuration Through the UI Pages, page 2-18 and Troubleshooting Tips on the Mobile Client, page 7-9.

- For Oracle E-Business Suite Mobile Apps Release 9.1 and Earlier, see Enabling a Mobile App Individually and Specifying the Configuration Through the UI Pages, page 9-21 and Troubleshooting Tips on the Mobile Client, page 16-6.

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 Discrete Quality Manager for Oracle E-Business Suite	Discrete Quality Manager	QA_QUALITY_MANAGER	com.oracle.ebs.scm.qa.QualityMgr	Quality

Mobile App Name	Application Name	Application Short Name	Application Bundle Id	Parent Application Name
Oracle Mobile Inventory for Oracle E-Business Suite	Inventory	INV_INVENTORY	com.oracle.ebs.scm.inv.Inventory	Inventory
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 Process Quality Manager for Oracle E-Business Suite	Process Quality Manager	GMD_MBL_QUALITY_MANAGER	com.oracle.ebs.scm.gmd.QualityManager	Process Manufacturing Product Development
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

Mobile App Name	Application Name	Application Short Name	Application Bundle Id	Parent Application Name
Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite	Self-Service HR	MOBILE_SELF_SERVICE_HR	com.oracle.ebs.hr.per.Selfservice	Human Resources
Oracle Mobile Yard for Oracle E-Business Suite	Yard	YMS	com.oracle.ebs.scm.yms.YardManager	Yard Management

E

Setting Up and Using the Supported Languages

Overview

Supported Languages

From Oracle E-Business Suite Mobile Release 4.0 to Mobile Release 9.1, 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:

> **Note:** The initial releases of our mobile apps were distributed in English only.

- Brazilian Portuguese
- Canadian French
- Dutch
- English
- French
- German
- Italian
- Japanese
- Latin American Spanish
- Simplified Chinese

- Spanish

Additionally, Oracle Mobile Maintenance for Oracle E-Business Suite app version 1.7.4 and onwards is available in Russian. See *Oracle Mobile Maintenance for Oracle E-Business Suite Release Notes*, My Oracle Support Document 1923702.1.

For Oracle E-Business Suite Mobile Release 10.x:

- Oracle Approvals for EBS is available in the languages supported by Oracle E-Business Suite.
- Oracle Field Service for EBS supports multiple languages for all the languages which have language patches that are available for the Oracle E-Business Suite server. Labels and messages are downloaded in the app user's selected language and applied and shown in the app.
- Oracle Maintenance for EBS supports Russian, plus all the eleven languages mentioned earlier for Release 9.1 and earlier.
- Oracle Mobile SCM for EBS supports all the eleven languages mentioned earlier for Release 9.1 and earlier.
- Oracle Self-Service HR for EBS is available in the languages supported by Oracle E-Business Suite based on the language set in the user preference, including bi-directional support (Left to Right and Right to Left).
- Oracle Timecards for EBS is available in the languages supported by Oracle E-Business Suite based on the language set in the user preference, including bi-directional support (Left to Right and Right to Left).

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: An asterisk (*) 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 Switzerland or any other country 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

Language	Android Language	Android Region
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: Selecting a Language for Oracle Access

Management Login, *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

1. Log on to the OAM server.
2. Navigate to the OAM domain, such as `</base_dir>/Middleware/user_projects/domains/oam_domain/`.
3. Back up the original `oam-config.xml` file.
4. 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
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

Language	Language Code
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>
```

5. Stop and restart the OAM server.

F

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	Associated Product 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	Associated Product 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 Discrete Quality Manager for Oracle E-Business Suite	Oracle Quality
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 Process Quality Manager for Oracle E-Business Suite	Oracle Process Manufacturing Product Development
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
Oracle Mobile Self-Service Human Resources for Oracle E-Business Suite	• For Self-Service Human Resources: Oracle Self-Service Human Resources • For Payslip: Oracle HRMS (US)

Mobile App Name	Associated Product Name
Oracle Mobile Service Manager for Oracle E-Business Suite	Oracle TeleService
Oracle Mobile Supply Chain Applications for Oracle E-Business Suite	Oracle Mobile Application Server
Oracle Mobile Yard for Oracle E-Business Suite	Oracle Yard Management