JD Edwards EnterpriseOne

Mobile Applications Installation and Configuration Guide

Release 9.0 and 9.1

E24286-13

December 2015

Describes how to configure an Oracle WebLogic Server with ADF Runtime for a JD Edwards EnterpriseOne mobile smartphone applications installation and deployment.

JD Edwards EnterpriseOne Mobile Applications Installation and Configuration Guide, Release 9.0 and 9.1

E24286-13

Contents

3 Installing EnterpriseOne Mobile Applications

4 Troubleshooting

Preface

Welcome to the *JD Edwards EnterpriseOne Mobile Applications Installation and Configuration Guide*. This guide has been updated with instructions on how to install and deploy the EnterpriseOne 9.1.2 mobile applications. See What's New in JD Edwards EnterpriseOne 9.1.2 Mobile Applications.

> **Important:** This guide does NOT provide configuration instructions for the next generation of mobile applications referred to as EnterpriseOne mobile *enterprise* applications. For EnterpriseOne mobile enterprise applications configuration instructions, see the *JD Edwards EnterpriseOne Application Interface Services Server for Mobile Enterprise Applications Configuration Guide*.

Audience

This documentation is written for the individuals responsible for installing and administering the JD Edwards EnterpriseOne environment.

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

- JD Edwards EnterpriseOne system, including all servers and environments
- JD Edwards EnterpriseOne Tools
- JD Edwards EnterpriseOne Applications

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.

Related Documents

Refer to the following guides for additional information about components related to the implementation of JD Edwards EnterpriseOne mobile applications:

- *JD Edwards EnterpriseOne Applications Functionality for Mobile Devices Implementation Guide*
- *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*

Also, document 1387796.1 in My Oracle Support lists and provides links to documentation related to EnterpriseOne mobile applications. Use the following URL to access and sign into My Oracle Support:

`https://support.oracle.com`

Conventions

The following text conventions are used in this document:

Convention	Meaning
Bold	Indicates field values.
Italics	Indicates emphasis and JD Edwards EnterpriseOne or other book-length publication titles.
`Monospace`	Indicates a JD Edwards EnterpriseOne program, other code example, or URL.

What’s New in JD Edwards EnterpriseOne 9.1.2 Mobile Applications

> **Important:** Before continuing, read the Preface of this guide for important information about the next generation of mobile applications called EnterpriseOne mobile *enterprise* applications.

This chapter provides an overview of the JD Edwards EnterpriseOne 9.1.2 mobile applications features and deployment. It contains the following topics:

- "Overview of EnterpriseOne 9.1.2 Mobile Applications Features and Supported Functionality"
- "About the Deployment of EnterpriseOne 9.1.2 Mobile Applications"

Overview of EnterpriseOne 9.1.2 Mobile Applications Features and Supported Functionality

An EnterpriseOne 9.1.2 mobile applications deployment supports:

- EnterpriseOne application security for authorizing user access to mobile applications.

  For more information about application security for mobile applications, see Configuring Support for EnterpriseOne Application Security for 9.1.2 Mobile Applications in this guide.

- JAX-RPC based and JAX-WS based business services.

  > **Note:** Support of JAX-WS based business services requires running a minimum of EnterpriseOne Tools release 9.1.2.4.

- The use of the native camera feature with the Mobile Expense Management application for iOS and Android mobile device users.

  Support of the native camera feature enables users to attach photos of receipts or other documents in the Mobile Expense Management application. To use this feature, users must download the *JD Edwards EnterpriseOne Mobile Applications* application on their mobile device and run the Mobile Expense Management application from this application. See "Understanding Photo Attachments" in the *JD Edwards EnterpriseOne Applications Functionality for Mobile Devices Implementation Guide* for more information. See the following section for information about the deployment requirements for supporting this feature.

About the Deployment of EnterpriseOne 9.1.2 Mobile Applications

If you have an existing mobile applications deployment with EnterpriseOne 9.1 and you want to install 9.1.2 mobile applications, you must install and deploy 9.1.2 mobile applications on a new domain following the instructions in this guide. After configuring and testing the deployment on the new domain, you can direct pre-9.1.2 mobile applications users to switch over to the 9.1.2 mobile applications.

> **Important:** You cannot install and deploy 9.1.2 mobile applications in an existing pre-9.1.2 mobile applications configuration.

In preparation for a 9.1.2 mobile applications installation and deployment, you must download:

- EnterpriseOne ESUs, which enable support for 9.1.2 mobile applications in EnterpriseOne.
- 9.1.2 Mobile Foundation.
- 9.1.2 mobile applications.

See Prerequisites - Mobile Application Downloads (Release 9.1.2 Update) in this guide for information about the required downloads.

To support the use of the native camera feature on iOS and Android devices for Mobile Expense Management users, in addition to installing and deploying the 9.1.2 mobile applications, you must:

- Deploy a JAX-WS business services package on the Business Services Server.

  Make sure that Media Object Settings on the Business Services Server are configured to support media object operations. See "Configuring the Business Services Server for Media Object Operations" in the *JD Edwards EnterpriseOne Tools Business Services Server Reference Guide* for more information about these settings.

- Host a connections.xml file on a WebDAV server.

  See Hosting a Connection for the Native JD Edwards EnterpriseOne Mobile Applications Application (Mobile Applications Release 9.1.2) for more information.

> **Note:** Mobile Expense Management application users must access the application from the *JD Edwards EnterpriseOne Mobile Applications* application, which can be downloaded from the Google Play store or Apple App Store.

1 JD Edwards EnterpriseOne Mobile Applications Overview

Important: Before continuing, read the Preface of this guide for important information about the documentation for the different EnterpriseOne mobile application solutions.

This chapter contains the following topics:

- Section 1.1, "Understanding EnterpriseOne Mobile Applications"
- Section 1.2, "Understanding the EnterpriseOne Mobile Applications Environment"
- Section 1.3, "Understanding EnterpriseOne Mobile Applications Security"
- Section 1.4, "Configuring Support for EnterpriseOne Application Security for 9.1.2 Mobile Applications"
- Section 1.5, "EnterpriseOne Mobile Applications Installation and Implementation Checklist"
- Section 1.6, "Minimum Technical Requirements"
- Section 1.7, "Prerequisites - Mobile Application Downloads (Release 9.1.2 Update)"

Note: This chapter has been updated to support the release of EnterpriseOne 9.1.2 mobile applications.

1.1 Understanding EnterpriseOne Mobile Applications

JD Edwards EnterpriseOne mobile applications are applications built for the following mobile devices:

- Apple iOS-based mobile devices, such as iPhone and iPad
- Blackberry

Note: The photo attachment feature that is available with EnterpriseOne mobile applications 9.1.2 is not supported on Blackberry.

- Android

EnterpriseOne mobile applications provide users in the field access to timely and critical data to meet their business needs and quickly and efficiently perform tasks, such as:

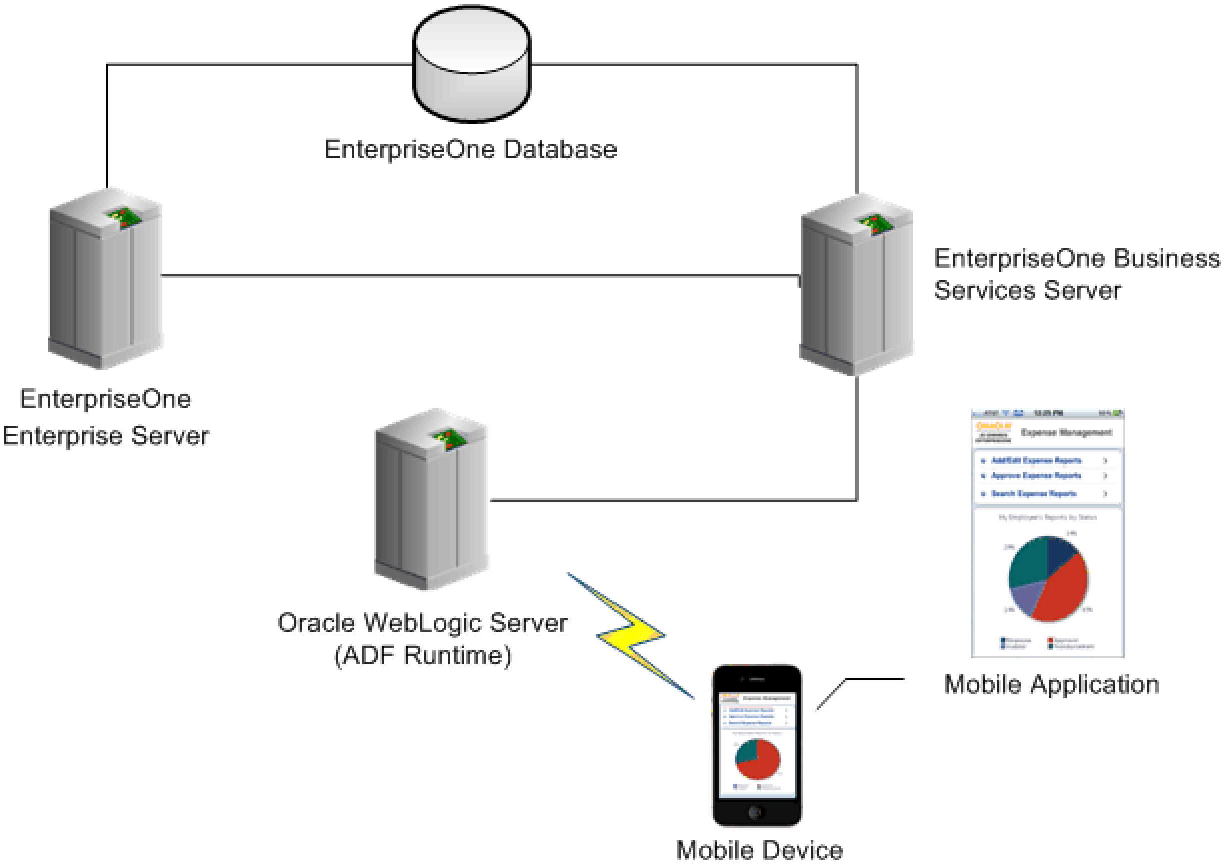
- Entering expense reports
- Reviewing and approving expense reports
- Reviewing and approving purchase orders
- Reviewing and approving requisitions entered through Requisition Self Service
- Reviewing current and historical sales orders
- Querying item price and availability information

The mobile applications were developed using Oracle Application Development Framework Mobile (ADF Mobile), a component of Oracle Fusion Middleware.

Deploying EnterpriseOne mobile applications requires installing ADF Runtime, EnterpriseOne Mobile Foundation, and EnterpriseOne mobile applications on Oracle WebLogic Server. See Prerequisites - Mobile Application Downloads (Release 9.1.2 Update) in this guide for a list of components that you must download to install EnterpriseOne mobile applications.

1.2 Understanding the EnterpriseOne Mobile Applications Environment

The following illustration shows the EnterpriseOne mobile applications environment:


EnterpriseOne Database
EnterpriseOne Business Services Server
EnterpriseOne Enterprise Server
Oracle WebLogic Server (ADF Runtime)
Mobile Application
Mobile Device

This list describes each of the components in the EnterpriseOne mobile applications environment:

- Oracle WebLogic Server

  The application server for installing and deploying EnterpriseOne Mobile Foundation and mobile applications. The Mobile Foundation contains scripts that ensure that the applications render properly on the mobile device, as well as an Authentication Provider, which provides user sign-in security for deployed mobile applications.

  ADF runtime must be installed on WebLogic Server before installing EnterpriseOne Mobile Foundation and mobile applications.

- EnterpriseOne Enterprise Server and database

  The EnterpriseOne Enterprise Server processes logic and requests data from the database.

- Business Services Server

  This server contains a business services package built with mobile applications business services that enable data transfer between the mobile applications and EnterpriseOne.

  The Business Services Server can run on WebLogic Server or IBM WebSphere Application Server. It does not have to run on the same server as the mobile applications, which can only be deployed on WebLogic Server with ADF runtime. If both are installed on the same WebLogic Server, the Business Services Server must be installed in a separate domain. If the Business Services Server is on a separate machine, you have to configure a certificate to enable the transmission of requests from WebLogic Server to the Business Services Server. See Configuring Web Service Requests Between a WebLogic Server and a Business Services Server Deployed on Separate Machines.

  > **Important:**
  >
  > Starting with EnterpriseOne mobile applications release 9.1.2, JAX-WS based business services are supported with a minimum EnterpriseOne Tools release 9.1.2.4.
  >
  > For 9.1 and earlier releases, JD Edwards EnterpriseOne mobile applications support only JAX-RPC based business services; they do not support JAX-WS based business services. Therefore, the business services server in the mobile applications environment must contain a package built with JAX-RPC based business services.

- Mobile device

  EnterpriseOne mobile applications can run on Apple iOS, Blackberry, and Android mobile devices.

1.3 Understanding EnterpriseOne Mobile Applications Security

> **Note:** Starting with EnterpriseOne mobile applications release 9.1.2, in addition to authentication security and business services security described in this section, mobile applications support EnterpriseOne application security. The support of EnterpriseOne application security does not supplant, but is in addition to, the security described in this section. See Configuring Support for EnterpriseOne Application Security for 9.1.2 Mobile Applications for more information.

Two levels of security ensure secure access to JD Edwards EnterpriseOne mobile applications: sign-in security for user authentication and published business services security for application authorization.

Sign-in Security

EnterpriseOne mobile applications use an Authentication Provider for sign-in security to ensure that users of mobile applications are authenticated EnterpriseOne users. The Authentication Provider eliminates having to set up additional sign-in security for EnterpriseOne mobile application users.

After a user enters their credentials in the mobile application login screen, a login module calls the AuthenticationManager business service, which is used to authenticate the user.

The Authentication Provider also provides single sign-on functionality so that users only have to sign in once when using multiple EnterpriseOne mobile applications. After a user signs into their first EnterpriseOne mobile application, any subsequent EnterpriseOne mobile applications launched by the user automatically use the credentials from the original sign-in.

The JD Edwards EnterpriseOne Mobile Foundation download includes two jar files, JDEADFMobileAuthenticationProvider.jar and JDEADFMobileLoginModule.jar. Both files are used in configuring the Authentication Provider.

Published Business Services Security

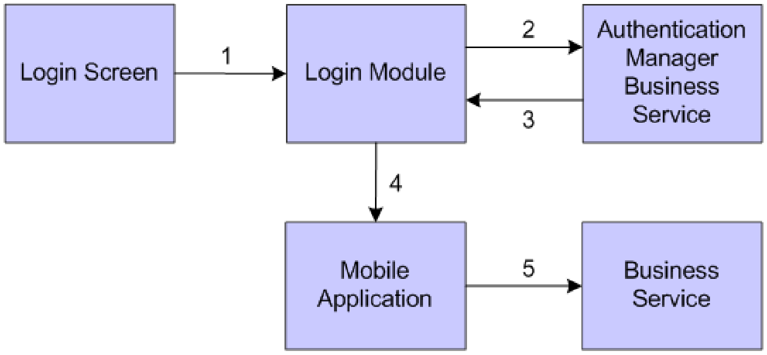
EnterpriseOne mobile applications use published business services to pass data between the mobile device and the EnterpriseOne database. Mobile applications also use published business services to pass the credentials of a mobile application user to the EnterpriseOne security server to verify that the user is authorized to access the published business service. If the user is not authorized, access to the EnterpriseOne system is denied.

Therefore, you must set up published business services security records in EnterpriseOne to provide mobile application users with access to published business services. By setting up security records for mobile applications published business services, you are essentially setting up security for the mobile applications.

See "Securing Mobile Applications" in the *JD Edwards EnterpriseOne Applications Functionality for Mobile Devices Implementation Guide* for more information about securing mobile application published business services.

Security Process Flow

The following diagram shows the security process flow for EnterpriseOne mobile applications:



The following list describes the security process flow:

1. A user launches a mobile application and is directed to the JD Edwards EnterpriseOne mobile application login screen wherein the user signs in with an EnterpriseOne user name, password, role, and environment. The J2EE application server invokes the login module through the registered authentication provider, and the login module retrieves the user credentials from the sign-in screen.
2. The login module invokes the Authentication Manager business service, which performs the following security checks:
    a. User authentication. The Authentication Manager business service performs user authentication by verifying that the user credentials represent a valid EnterpriseOne user.
    b. User authorization. Starting with the EnterpriseOne mobile applications release 9.1.2, if user authentication is successful, the Authentication Manager business service checks for application security or exclusive application security. It verifies that the user is authorized to run a particular mobile application based on security records in the Security Workbench table (F00950). See Configuring Support for EnterpriseOne Application Security for 9.1.2 Mobile Applications for more information.
3. If the user authentication or user authorization fails, an error message appears on the sign-in screen.
4. If both authentication and authorization are successful, the mobile application is displayed.
5. The mobile application uses a security token from the Authentication Manager business service for subsequent calls to business services used by the mobile application. The user must be an authorized user of the business services to use the mobile application.

1.4 Configuring Support for EnterpriseOne Application Security for 9.1.2 Mobile Applications

This section contains the following topics:

- Section 1.4.1, "Overview of Application Security for EnterpriseOne Mobile Applications"
- Section 1.4.2, "Configuration Requirements to Support EnterpriseOne Application Security for Mobile Applications"
- Section 1.4.3, "Verifying ESU Objects in EnterpriseOne"

1.4.1 Overview of Application Security for EnterpriseOne Mobile Applications

Starting with EnterpriseOne mobile applications release 9.1.2, mobile applications support EnterpriseOne application security and exclusive application security. The support of EnterpriseOne application security does not replace, but is in addition to the support of authentication security and business services security for mobile applications.

You use Security Workbench in EnterpriseOne to set up application security or exclusive application security for mobile applications. EnterpriseOne mobile applications are secure by default; that is, out of the box, users cannot access them. Therefore, you have to create security records in Security Workbench to allow users access to mobile applications.

You can set up security records for a user, role, or *PUBLIC. See the *JD Edwards EnterpriseOne Tools Security Administration Guide* for more information about the sequence EnterpriseOne uses to check security records.

The following list contains the application IDs of the EnterpriseOne mobile applications. Refer to these application IDs when creating application security or exclusive application security records in Security Workbench:

- M09E2011 (Mobile Expense Management)
- M43081 (Mobile Purchase Order Approval
- M43E82 (Mobile Requisition Approval)
- M4200010 (Mobile Sales Inquiry)
- M311221 (Mobile Service Order Time Entry)
- M0001 (Mobile Menu)

For instructions on how to set up application security records, see the following sections in the *JD Edwards EnterpriseOne Tools Security Administration Guide*:

- "Managing Application Security"
- "Managing Exclusive Application Security"

1.4.2 Configuration Requirements to Support EnterpriseOne Application Security for Mobile Applications

The Prerequisites - Mobile Application Downloads (Release 9.1.2 Update) section in this guide lists the required downloads for an EnterpriseOne 91.2 mobile applications deployment, including the Mobile Foundation. The Mobile Foundation includes an EnterpriseOne ESU that contains EnterpriseOne tasks and the JPH90I01 and JH90I01 business services, which are required for an administrator to set up application security in EnterpriseOne for 9.1.2 mobile applications.

After applying the ESU from the Mobile Foundation:

- Verify the ESU objects in EnterpriseOne. See Verifying ESU Objects in EnterpriseOne in this guide.
- Deploy a new business services package that includes the JPH90I01 and JH90I01 business services on the Business Services Server instance.

  See "Working with Packages for Business Services" in the *JD Edwards EnterpriseOne Tools Package Management Guide* for more information about how to deploy a business services package.

1.4.3 Verifying ESU Objects in EnterpriseOne

After downloading the appropriate ESU for 9.1.2 mobile applications, verify that the following objects were added to EnterpriseOne from the ESU:

- EnterpriseOne tasks for mobile applications

  These tasks, along with the business service properties, are used by the Authentication Manager business service (JPH90I01) to enable EnterpriseOne application security for mobile applications.

- Authentication Manager Query Processor business service (JH90I01)

  This is an internal business service that processes the getAuthData method of the JPH90I01 business service.

- Authentication Manager business service (JPH90I01)

  This business service was updated to support the use of EnterpriseOne application security for mobile applications. It contains two new properties that are used in conjunction with mobile application tasks to enable EnterpriseOne application security for mobile applications.

In EnterpriseOne, verify that the tasks, task relationships, and the business service properties provided by the ESU are in the system.

> **Note:** You do not have to set up any of the tasks or task relationships described in this section. Also, you do not have to set up task security because the tasks are not part of any task view and therefore are not available in either the EnterpriseOne Windows client or web client.

To verify tasks for mobile applications in EnterpriseOne:

On the Work With Tasks form in P9000, use the QBE row to locate and verify the tasks listed in the following table:

Task ID	Task Name	Type	Description	App	System	Description
812JP017833	Mobile Expense Management	01	Interactive Application	M09E2011	09E	Expense Reimbursement
812JP017834	Mobile Purchase Order Approval	01	Interactive Application	M43081	43	Procurement
812JP017835	Mobile Requisition Approval	01	Interactive Application	M43E82	43E	Requisition Self Service
812JP017836	Mobile Sales Inquiry	01	Interactive Application	M4200010	42	Sales Management
812JP017837	Mobile Menu	01	Interactive Application	M0001	00	Foundation Environment
812JP017838	Mobile Service Order Time Entry	01	Interactive Application	M311221	31	Shop Floor Control
JDE030504	EnterpriseOne Mobile Apps	07	Folder	n/a	00	Foundation Environment

To verify parent-child task relationships for mobile applications in EnterpriseOne:

1. On the Work With Task Relationships - Task Where Used form in P9000, enter the parent task JDE030504 in the Task field and click the Find button.
2. Verify the parent-child task relationships listed in the following table:

Parent Task	Parent Task Name	Child Task	Child Task Name	Presentation Seq.	Task View
JDE030504	EnterpriseOne Mobile Apps	812JP017833	Mobile Expense Management	1	91
JDE030504	EnterpriseOne Mobile Apps	812JP017834	Mobile Purchase Order Approval	2	91
JDE030504	EnterpriseOne Mobile Apps	812JP017835	Mobile Requisition Approval	3	91
JDE030504	EnterpriseOne Mobile Apps	812JP017836	Mobile Sales Inquiry	4	91
JDE030504	EnterpriseOne Mobile Apps	812JP017837	Mobile Menu	5	91
JDE030504	EnterpriseOne Mobile Apps	812JP017838	Mobile Service Order Time Entry	6	91

To verify business service properties for mobile applications:

Access the Business Service Property Admin application (P951000) and search for and verify the Business Service properties listed in the following table:

Key	Value	Description	Level	Group
JPH90I01_FOLDER_TASK_ID	JDE030504	Task ID for Folder Type Parent Task for EOne Mobile Apps	BSSV	JPH90I01
JPH90I01_FOLDER_TASK_NAME	EnterpriseOne Mobile Apps	Task Name for Folder Type Parent Task for EOne Mobile Apps	BSSV	JPH90I01

1.5 EnterpriseOne Mobile Applications Installation and Implementation Checklist

Use the following lists of installation and implementation tasks as a high-level checklist for installing and deploying EnterpriseOne mobile applications:

Installation Tasks

- Install Oracle WebLogic Server and create a new domain for the mobile applications deployment.

  See *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server.*

- From the Oracle Software Delivery Cloud, download the software required for installing and configuring EnterpriseOne mobile applications.

  See Prerequisites - Mobile Application Downloads (Release 9.1.2 Update) in this guide.

- Use the following link to access the Update Center to check for updates to the mobile components. Perform a search after selecting EnterpriseOne Mobile in the Type field:

  `https://updatecenter.oracle.com/apps/WebSearch/updatecenter.jsp?action=news&pkgType=06&`

- Install and configure Oracle Application Developer Runtime (ADF runtime) for an EnterpriseOne mobile applications deployment.

  See Installing ADF Runtime in this guide.

- Extend the Oracle WebLogic domain for ADF runtime.

  See Extending the WebLogic Server Domain For ADF Runtime in this guide.

- Create and deploy the EnterpriseOne Shared Library on WebLogic Server.

  See Creating and Deploying the EnterpriseOne Shared Library on WebLogic Server in this guide.

- Create a managed server for EnterpriseOne mobile applications.

  See Creating a Managed Server for an EnterpriseOne Mobile Applications Deployment in this guide.

- Install and configure the Authentication Provider on WebLogic Server.

  See Configuring the Authentication Provider in this guide.

- Configure the EnterpriseOne shared library on WebLogic Server.

  See Configuring Shared Library on WebLogic Server in this guide.

- Install EnterpriseOne mobile applications.

  See Installing EnterpriseOne Mobile Applications in this guide.

- Host a connection for the native *JD Edwards EnterpriseOne Mobile Applications* application (Release 9.1.2 only)

  See Hosting a Connection for the Native JD Edwards EnterpriseOne Mobile Applications Application (Mobile Applications Release 9.1.2).

Implementation Tasks

- Provide users the URLs of the deployed mobile applications.

  See Obtaining the URL to a Mobile Application in this guide.

- Configure the system to support the native camera feature with Mobile Expense Management (Release 9.1.2 only).

  See What’s New in JD Edwards EnterpriseOne 9.1.2 Mobile Applications for information about configuration requirements.

- Set up mobile applications.

  See the *JD Edwards EnterpriseOne Applications Functionality for Mobile Devices Implementation Guide*.

- Set up security for business services used by the mobile applications.

  See "Securing Mobile Applications" in the *JD Edwards EnterpriseOne Applications Functionality for Mobile Devices Implementation Guide*.

- For EnterpriseOne 9.1.2 mobile applications, in addition to business services security, you must set up application security for mobile applications in the EnterpriseOne Security Workbench.

  See Configuration Requirements to Support EnterpriseOne Application Security for Mobile Applications.

1.6 Minimum Technical Requirements

See document 745831.1 (JD Edwards EnterpriseOne Minimum Technical Requirements Reference) on My Oracle Support:

`https://support.oracle.com/epmos/faces/DocumentDisplay?id=745831.1`

1.7 Prerequisites - Mobile Application Downloads (Release 9.1.2 Update)

Download the following software before installing and configuring EnterpriseOne mobile applications:

- ADF Runtime
- EnterpriseOne Mobile Foundation
- EnterpriseOne Mobile Applications
- JD Edwards EnterpriseOne Mobile Applications Application (Optional)

1.7.1 ADF Runtime

ADF runtime is not included with the JD Edwards EnterpriseOne mobile applications download. ADF runtime is available for download from the Oracle Software Delivery Cloud Web site: `https://edelivery.oracle.com/`.

1.7.2 EnterpriseOne Mobile Foundation

The EnterpriseOne Mobile Foundation download contains the following components:

- Electronic Software Updates (ESUs)

  Important: You must install the ESU for the AuthenticationManager Business Service before configuring the Authentication Provider.

- SharedLibraryScripts

  The scripts ensure that mobile applications render properly on the mobile device.

- Authentication JAR files

  The download includes the JDEADFMobileAuthenticationProvider.jar and JDEADFMobileLoginModule.jar, which are required to implement the Authentication Provider.

  Important: For EnterpriseOne mobile applications release 9.1.2, there is a new Mobile Foundation with an updated JDEADFMobileLoginModule.jar to enable support for EnterpriseOne application security in 9.1.2 mobile applications. It also enables support for JAX-WS based business services as long as you are running a minimum of EnterpriseOne Tools Release 9.1.2.4. If you do not deploy the updated JDEADFMobileLoginModule.jar file, you cannot use EnterpriseOne application security or support JAX-WS based business services.

For new EnterpriseOne mobile applications customers:

The Mobile Foundation is available for download from the Oracle Software Delivery Cloud Web site:

https://edelivery.oracle.com/.

For existing EnterpriseOne mobile applications customers:

The Mobile Foundation is available for download from the JD Edwards Update Center (login required):

https://updatecenter.oracle.com/apps/WebSearch/updatecenter.jsp?action=news&pkgType=06&

Make sure to select "EnterpriseOne Mobile" in the Type field when searching for the download.

1.7.3 EnterpriseOne Mobile Applications

Each EnterpriseOne mobile application is available as a separate download.

For new EnterpriseOne mobile applications customers:

The mobile applications are available for download from the Oracle Software Delivery Cloud Web site:

https://edelivery.oracle.com/.

For existing EnterpriseOne mobile applications customers:

The mobile applications are available for download from the JD Edwards Update Center (login required):

https://updatecenter.oracle.com/apps/WebSearch/updatecenter.jsp?action=news&pkgType=06&

Make sure to select "EnterpriseOne Mobile" in the Type field when searching for the mobile applications.

1.7.4 JD Edwards EnterpriseOne Mobile Applications Application (Optional)

EnterpriseOne 9.1.2 Mobile Expense Management application users can download the *JD Edwards EnterpriseOne Mobile Applications* application onto their mobile device from the Google Play store or the Apple App Store. This application enables Mobile Expense Management users to capture and upload photos of receipts or other documents using the mobile device's native camera feature.

2 Configuring Oracle WebLogic Server for an EnterpriseOne Mobile Applications Deployment

This chapter contains the following topics:

- Section 2.1, "Installing ADF Runtime"
- Section 2.2, "Extending the WebLogic Server Domain For ADF Runtime"
- Section 2.3, "Creating and Deploying the EnterpriseOne Shared Library on WebLogic Server"
- Section 2.4, "Configuring the Authentication Provider"
- Section 2.5, "Configuring Shared Library on WebLogic Server"
- Section 2.6, "Configuring Web Service Requests Between a WebLogic Server and a Business Services Server Deployed on Separate Machines"

2.1 Installing ADF Runtime

An EnterpriseOne mobile applications deployment requires installing ADF runtime on Oracle WebLogic Server. If you have not downloaded ADF runtime, see ADF Runtime in this guide.

> **Important:** Before installing ADF runtime, create a new domain on Oracle WebLogic Server. See "Creating a WebLogic Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for more information.
>
> If you are deploying 9.1.2 mobile applications, you cannot deploy them in a pre-9.1.2 mobile applications configuration. You must create a new domain for deploying the 9.1.2 mobile applications. See What’s New in JD Edwards EnterpriseOne 9.1.2 Mobile Applications before continuing.

To install ADF runtime:

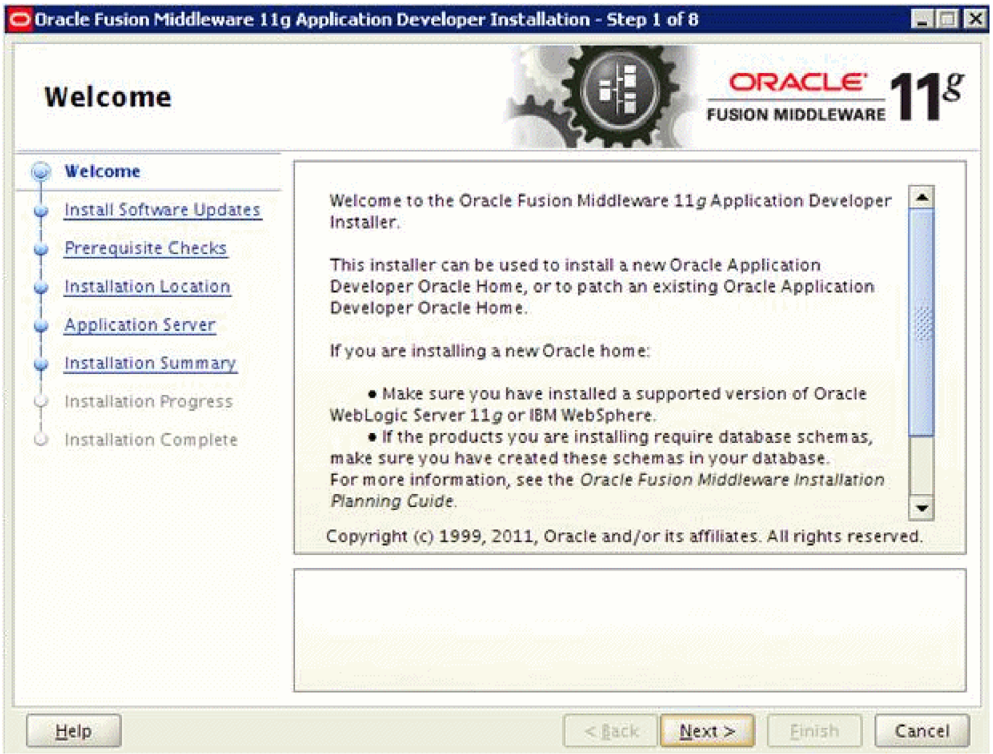
1. Launch the installation wizard for ADF runtime:

   On Windows, double-click the Oracle Application Developer setup.exe file. If prompted, enter credentials to run the wizard as an administrator.

   On UNIX, run the following commands:

```
export DISPLAY=IPAddress:0
./runInstaller-jreLocJRELocation
```

This launches the Oracle Fusion Middleware 11g Application Developer Installer.



Oracle Fusion Middleware 11g Application Developer Installation - Step 1 of 8

Welcome

Welcome to the Oracle Fusion Middleware 11*g* Application Developer Installer.

This installer can be used to install a new Oracle Application Developer Oracle Home, or to patch an existing Oracle Application Developer Oracle Home.

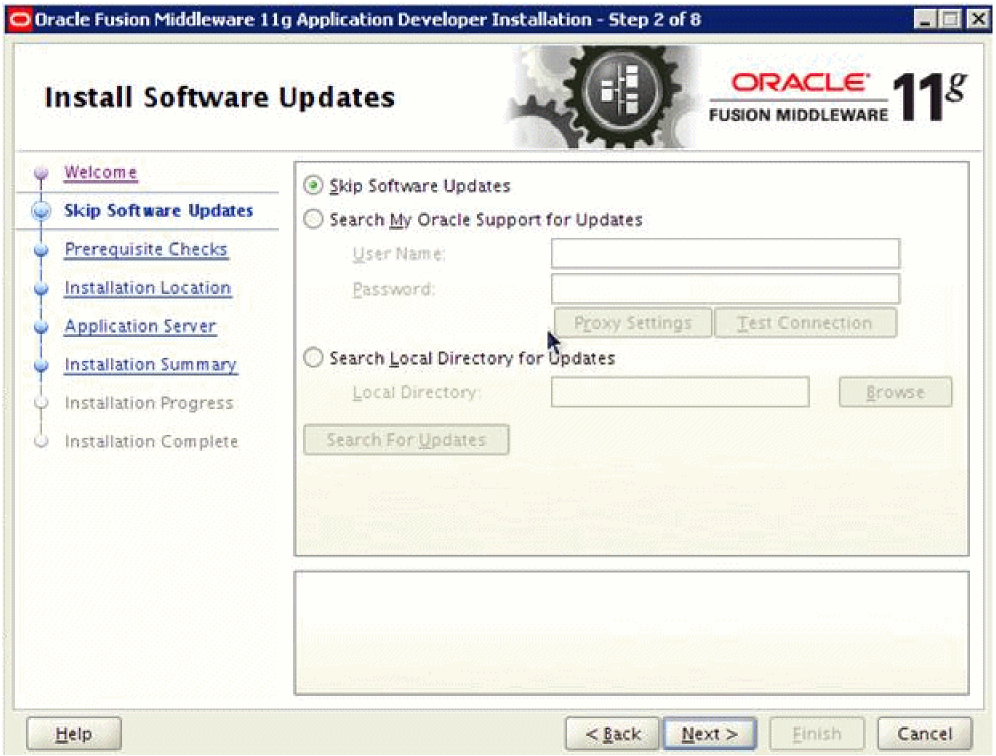
If you are installing a new Oracle home:

- Make sure you have installed a supported version of Oracle WebLogic Server 11*g* or IBM WebSphere.
- If the products you are installing require database schemas, make sure you have created these schemas in your database.

For more information, see the *Oracle Fusion Middleware Installation Planning Guide*.

Copyright (c) 1999, 2011, Oracle and/or its affiliates. All rights reserved.

2. On the Welcome page, click Next.



Oracle Fusion Middleware 11g Application Developer Installation - Step 2 of 8

Install Software Updates

● Skip Software Updates

○ Search My Oracle Support for Updates

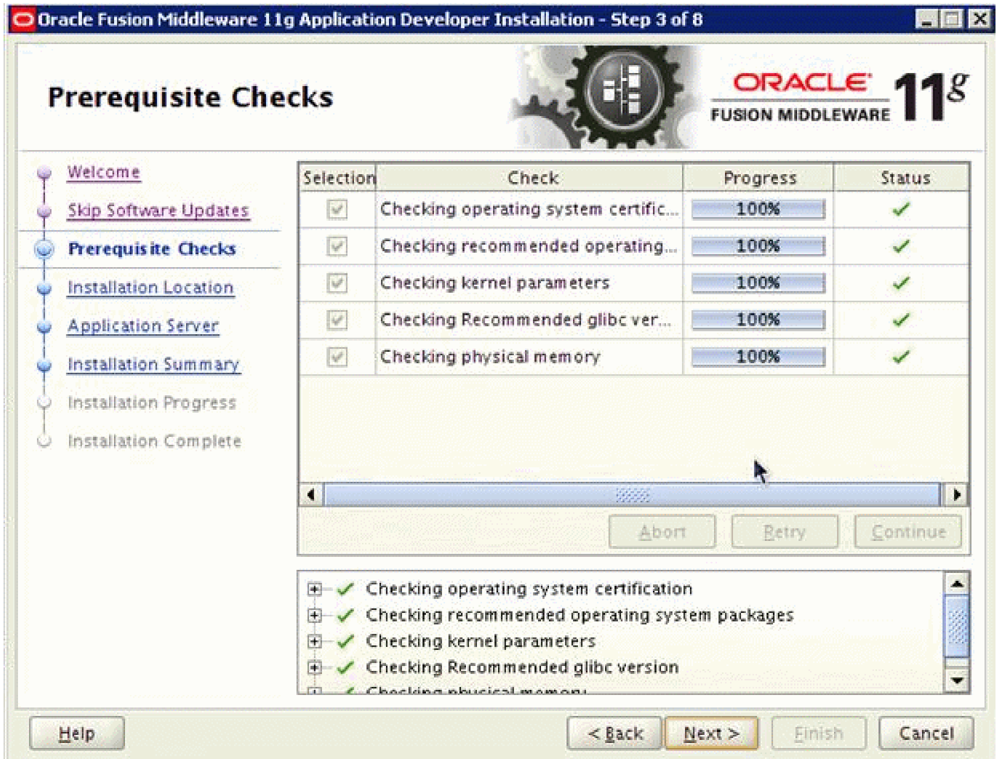
User Name:

Password:

○ Search Local Directory for Updates

Local Directory:

3. On Install Software Updates, select the "Skip Software Updates" option, and then click Next.



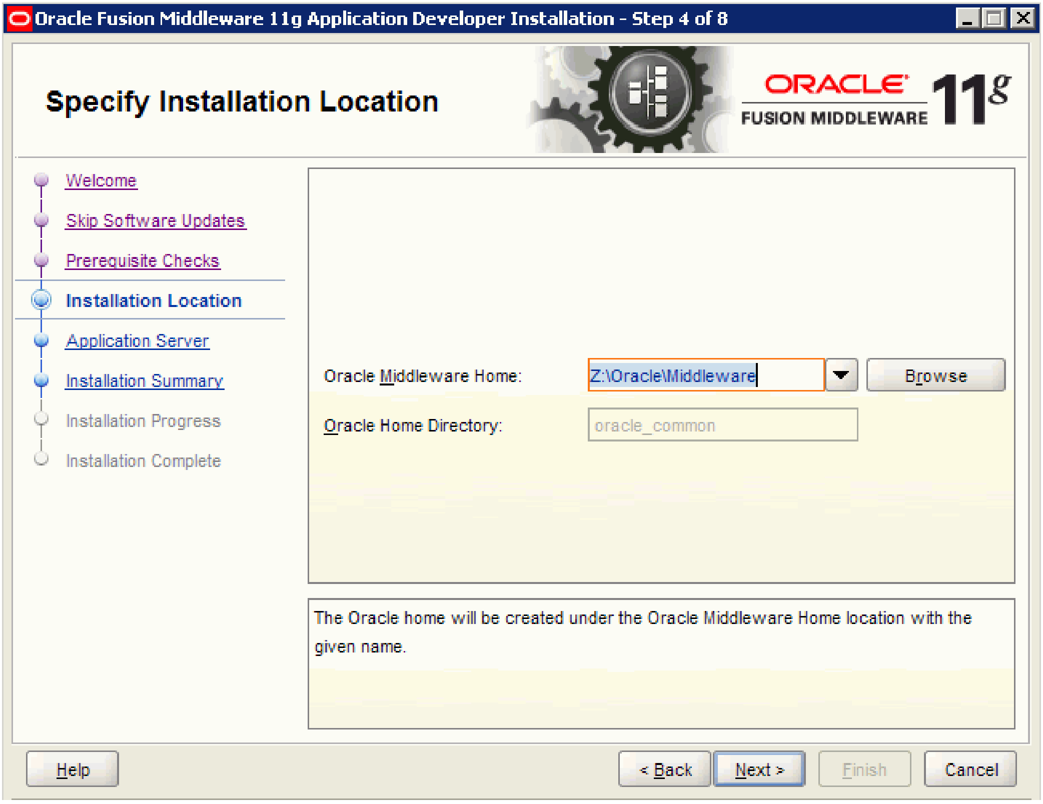
Oracle Fusion Middleware 11g Application Developer Installation - Step 3 of 8

Prerequisite Checks

Selection	Check	Progress	Status
☑	Checking operating system certific...	100%	✓
☑	Checking recommended operating...	100%	✓
☑	Checking kernel parameters	100%	✓
☑	Checking Recommended glibc ver...	100%	✓
☑	Checking physical memory	100%	✓

✓ Checking operating system certification
✓ Checking recommended operating system packages
✓ Checking kernel parameters
✓ Checking Recommended glibc version
✓ Checking physical memory

4. On Prerequisite Checks, click Next.



Oracle Fusion Middleware 11g Application Developer Installation - Step 4 of 8

Specify Installation Location

Oracle Middleware Home: Z:\Oracle\Middleware

Oracle Home Directory: oracle_common

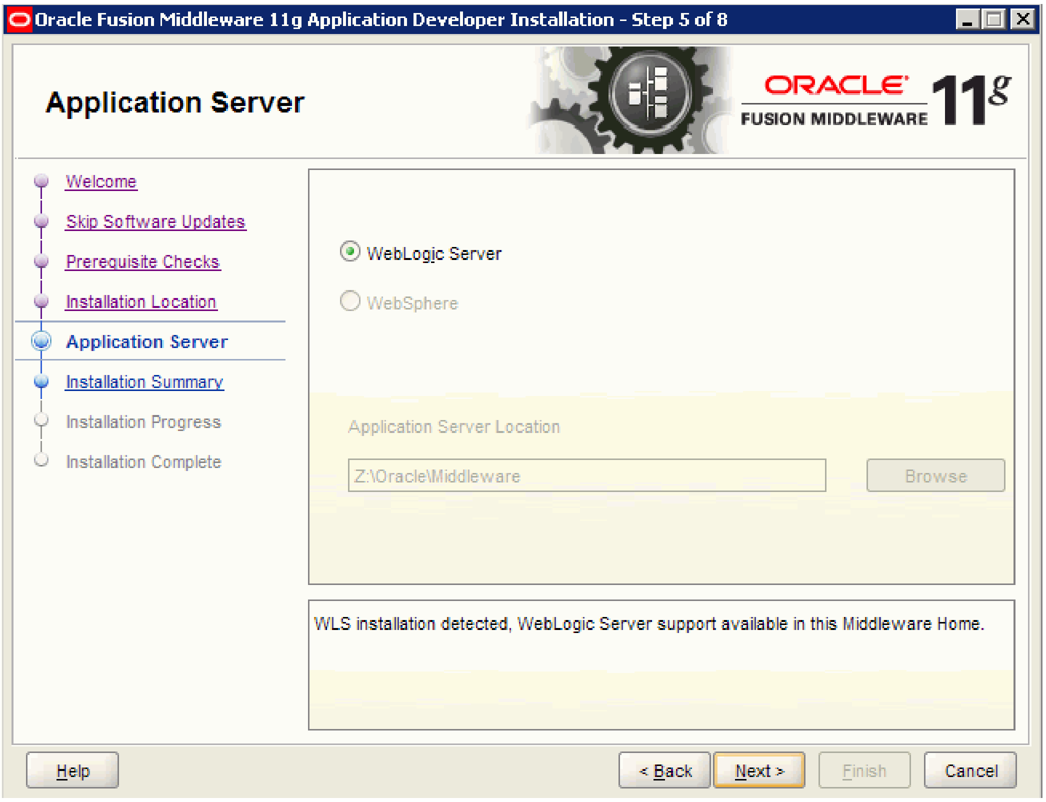
The Oracle home will be created under the Oracle Middleware Home location with the given name.

5. On Specify Installation Location, in the Oracle Middleware Home field, enter your Middleware Home location where Oracle WebLogic Server is installed.

   For Windows: `<drive>:\oracle\Middleware`

   For UNIX: `/home/oracle/Oracle/Middleware`

6. Click Next.



Oracle Fusion Middleware 11g Application Developer Installation - Step 5 of 8

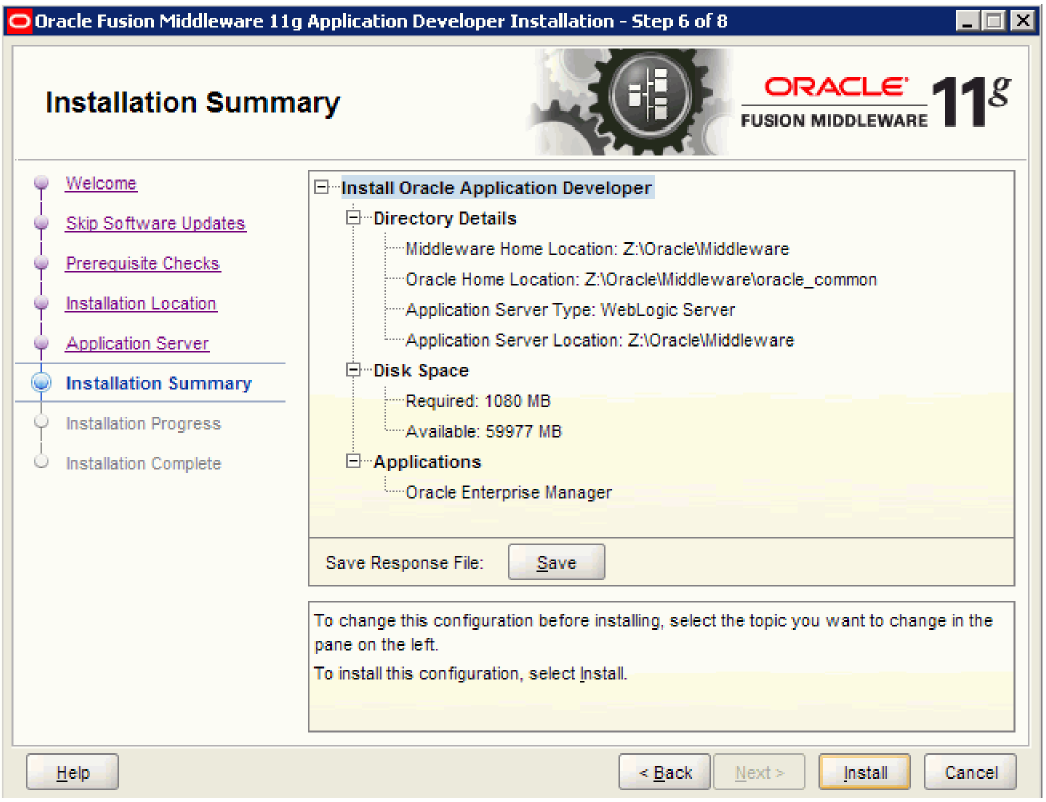
Application Server

● WebLogic Server
○ WebSphere

Application Server Location: Z:\Oracle\Middleware

WLS installation detected, WebLogic Server support available in this Middleware Home.

7. On Application Server, accept the defaults and click Next.



Installation Summary

- Install Oracle Application Developer
  - Directory Details
    - Middleware Home Location: Z:\Oracle\Middleware
    - Oracle Home Location: Z:\Oracle\Middleware\oracle_common
    - Application Server Type: WebLogic Server
    - Application Server Location: Z:\Oracle\Middleware
  - Disk Space
    - Required: 1080 MB
    - Available: 59977 MB
  - Applications
    - Oracle Enterprise Manager

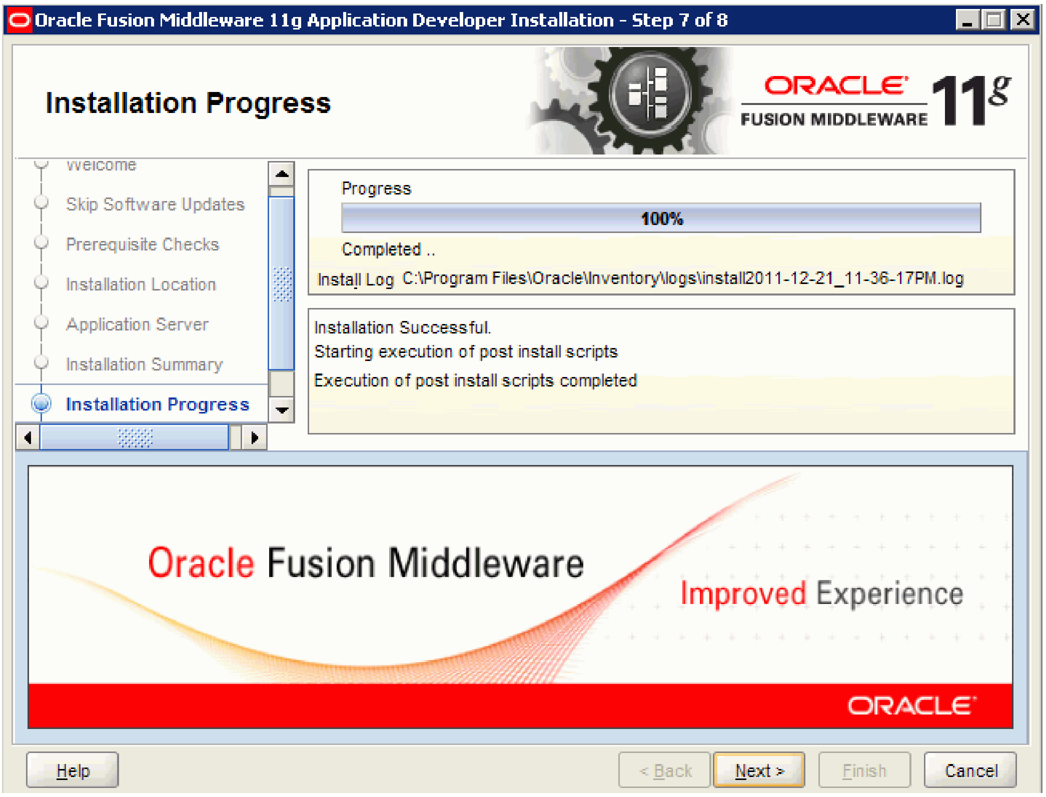
Save Response File:

To change this configuration before installing, select the topic you want to change in the pane on the left.

To install this configuration, select Install.

8. On Installation Summary, review your installation details and then click the Install button.

If you need to make a correction, click the Back button and modify your details.



Installation Progress

Progress

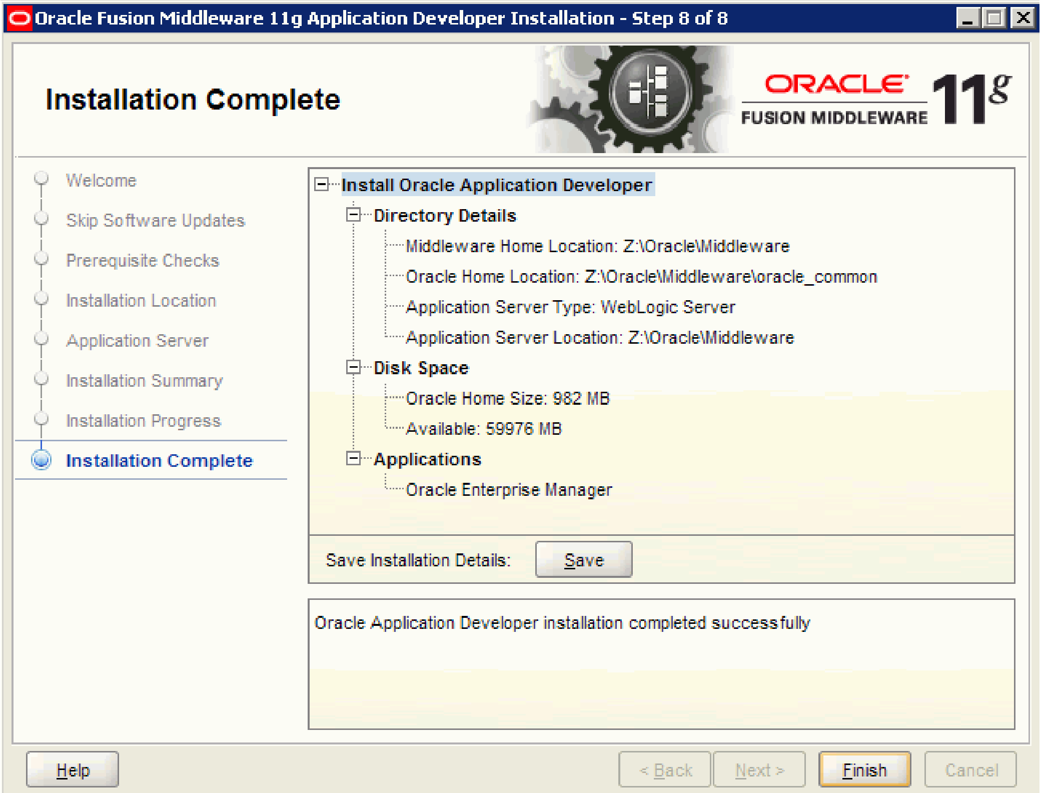
100%

Completed ..

Install Log C:\Program Files\Oracle\Inventory\logs\install2011-12-21_11-36-17PM.log

Installation Successful.
Starting execution of post install scripts
Execution of post install scripts completed

9. On Installation Progress, after the installation progress reaches 100%, click the Next button.



- Install Oracle Application Developer
  - Directory Details
    - Middleware Home Location: Z:\Oracle\Middleware
    - Oracle Home Location: Z:\Oracle\Middleware\oracle_common
    - Application Server Type: WebLogic Server
    - Application Server Location: Z:\Oracle\Middleware
  - Disk Space
    - Oracle Home Size: 982 MB
    - Available: 59976 MB
  - Applications
    - Oracle Enterprise Manager

Oracle Application Developer installation completed successfully

10. On Installation Complete, click Finish.

2.2 Extending the WebLogic Server Domain For ADF Runtime

After you create a new domain and install ADF runtime on WebLogic Server (as described in the previous section), extend the new domain to make ADF runtime available to other applications on that domain.

Caution: If the Business Services Server is deployed on the same WebLogic Server, you do NOT need to extend the new domain to the Business Services Server.

If the Business Services Server is deployed on a different machine than WebLogic Server with ADF runtime, you must configure WebLogic Server to accept certificates coming from the Business Services Server. See Configuring Web Service Requests Between a WebLogic Server and a Business Services Server Deployed on Separate Machines for more information.

In releases prior to EnterpriseOne mobile applications release 9.1.2, only JAX-RPC based business services are supported by mobile applications; JAX-WS based business services are not supported. Therefore, the Business Services Server in the mobile applications environment must contain a package built with JAX-RPC based business services.

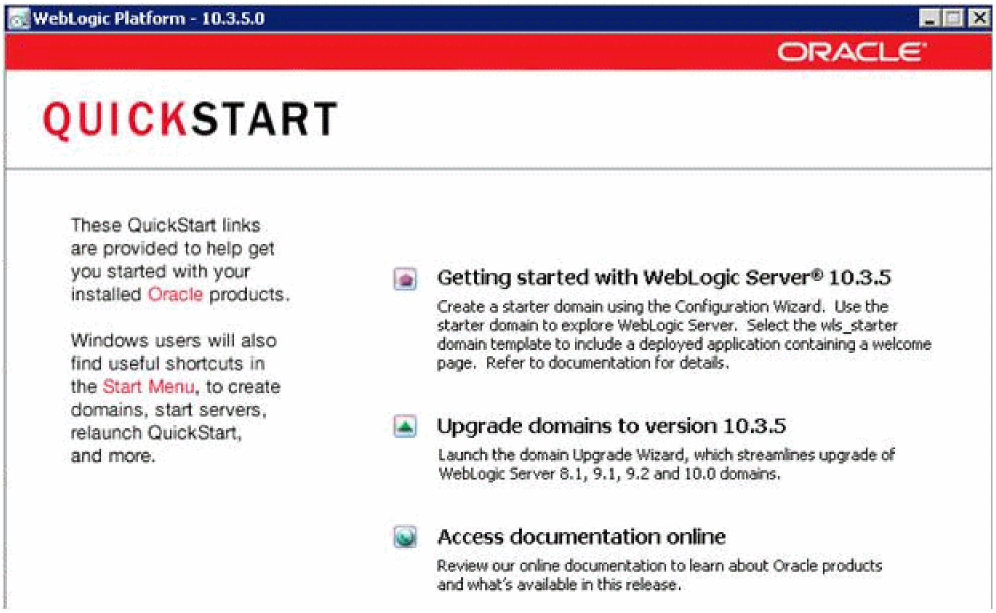
Starting with release 9.1.2 of the mobile applications, JAX-WS based business services are supported with a minimum EnterpriseOne Tools release 9.1.2.4.

This is a one-time task for the domain; you do not need to perform this task again if you install additional mobile applications on the same domain.

1. Use the following command to launch Quickstart:

   On Windows: `<Oracle Middleware>/utils/quickstart/quickstart.cmd`

   On UNIX: `<Oracle Middleware>/utils/quickstart/quickstart.sh`



These QuickStart links are provided to help get you started with your installed Oracle products.

Windows users will also find useful shortcuts in the Start Menu, to create domains, start servers, relaunch QuickStart, and more.

Getting started with WebLogic Server® 10.3.5

Create a starter domain using the Configuration Wizard. Use the starter domain to explore WebLogic Server. Select the wls_starter domain template to include a deployed application containing a welcome page. Refer to documentation for details.

Upgrade domains to version 10.3.5

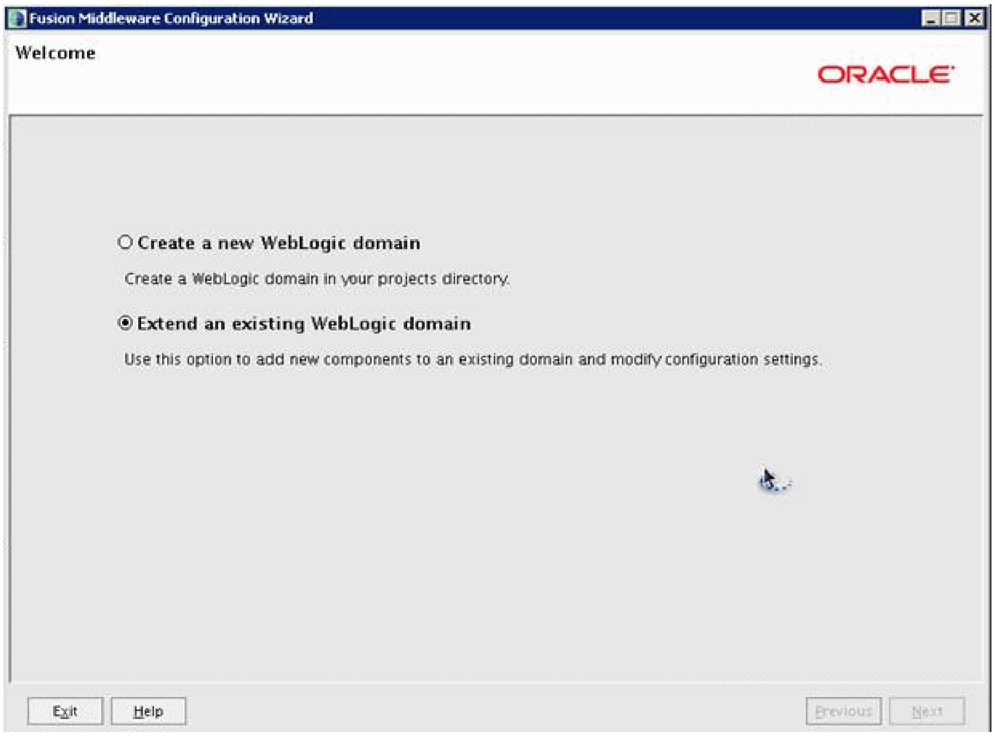
Launch the domain Upgrade Wizard, which streamlines upgrade of WebLogic Server 8.1, 9.1, 9.2 and 10.0 domains.

Access documentation online

Review our online documentation to learn about Oracle products and what's available in this release.

2. On the QuickStart page, click the "Getting Started with WebLogic Server 10.3.5" option to extend the existing Oracle WebLogic domain.

   The Fusion Middleware Configuration Wizard - Welcome page appears.



Welcome

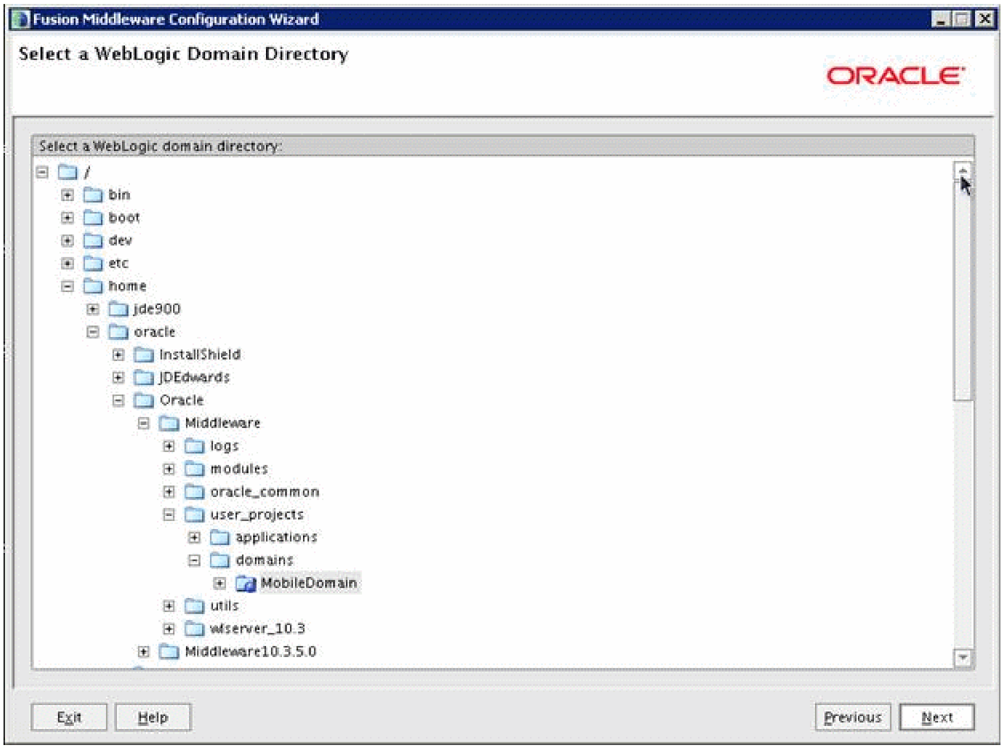
○ Create a new WebLogic domain

Create a WebLogic domain in your projects directory.

● Extend an existing WebLogic domain

Use this option to add new components to an existing domain and modify configuration settings.

3. On the Welcome page, select the "Extend an existing WebLogic domain" option, and then click Next.



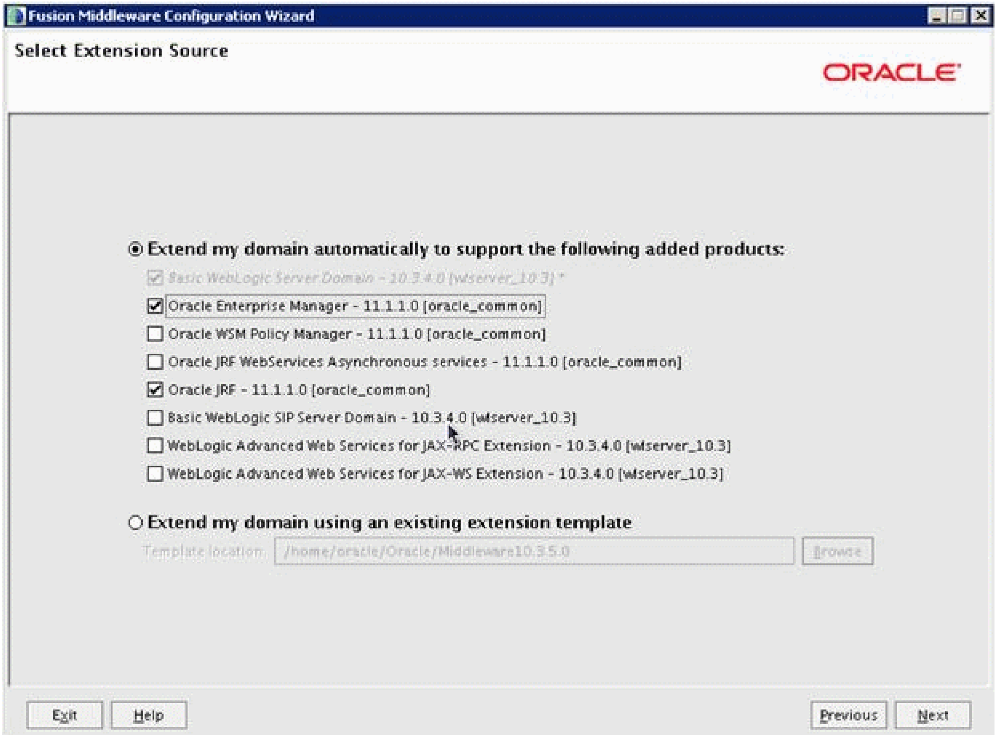
Select a WebLogic Domain Directory

Select a WebLogic domain directory:

```
⊟ /
  ⊞ bin
  ⊞ boot
  ⊞ dev
  ⊞ etc
  ⊟ home
    ⊞ jde900
    ⊟ oracle
      ⊞ InstallShield
      ⊞ JDEdwards
      ⊟ Oracle
        ⊟ Middleware
          ⊞ logs
          ⊞ modules
          ⊞ oracle_common
          ⊟ user_projects
            ⊞ applications
            ⊟ domains
              ⊞ MobileDomain
          ⊞ utils
          ⊞ wlserver_10.3
        ⊞ Middleware10.3.5.0
```

4. On Select a WebLogic domain directory, navigate to the directory of the newly created domain that you created for the mobile applications deployment.

5. Click Next.



Fusion Middleware Configuration Wizard

Select Extension Source

● Extend my domain automatically to support the following added products:

- ☑ Basic WebLogic Server Domain - 10.3.4.0 [wlserver_10.3] *
- ☑ Oracle Enterprise Manager - 11.1.1.0 [oracle_common]
- □ Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]
- □ Oracle JRF WebServices Asynchronous services - 11.1.1.0 [oracle_common]
- ☑ Oracle JRF - 11.1.1.0 [oracle_common]
- □ Basic WebLogic SIP Server Domain - 10.3.4.0 [wlserver_10.3]
- □ WebLogic Advanced Web Services for JAX-RPC Extension - 10.3.4.0 [wlserver_10.3]
- □ WebLogic Advanced Web Services for JAX-WS Extension - 10.3.4.0 [wlserver_10.3]

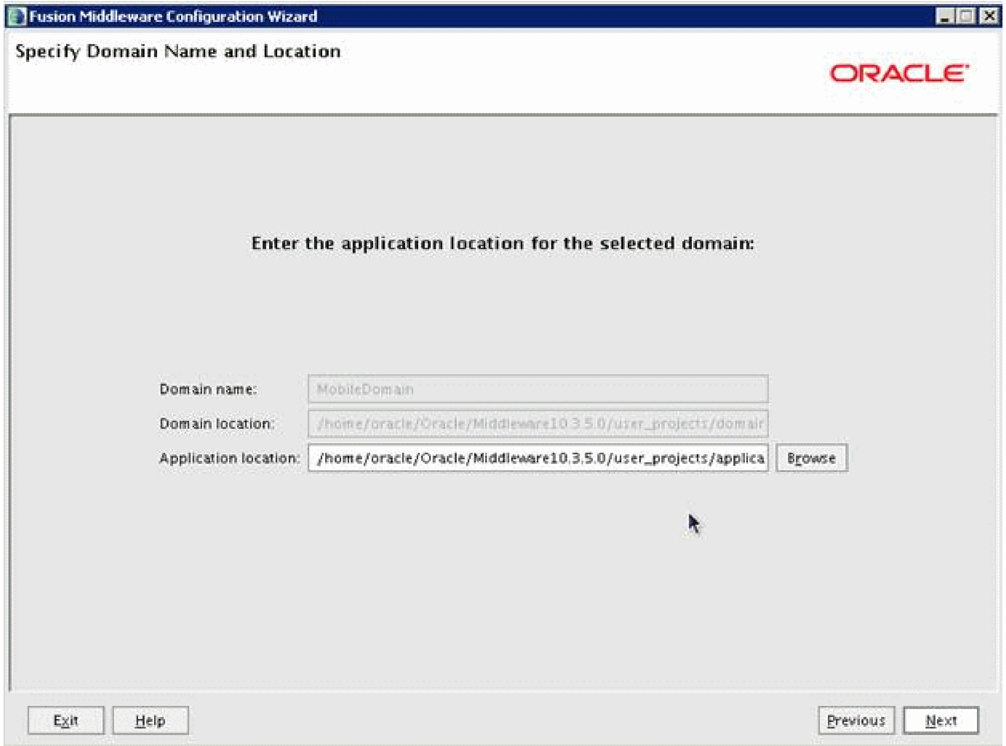
○ Extend my domain using an existing extension template

Template location: /home/oracle/Oracle/Middleware10.3.5.0

6. On Select Extension Source, select the "Extend my domain automatically to support the following added products" option, and then select the following products:

   - Oracle Enterprise Manager - 11.1.1.0 [oracle_common]
   - Oracle JRF - 11.1.1.0 [oracle_common]

7. Click Next.



Fusion Middleware Configuration Wizard

Specify Domain Name and Location

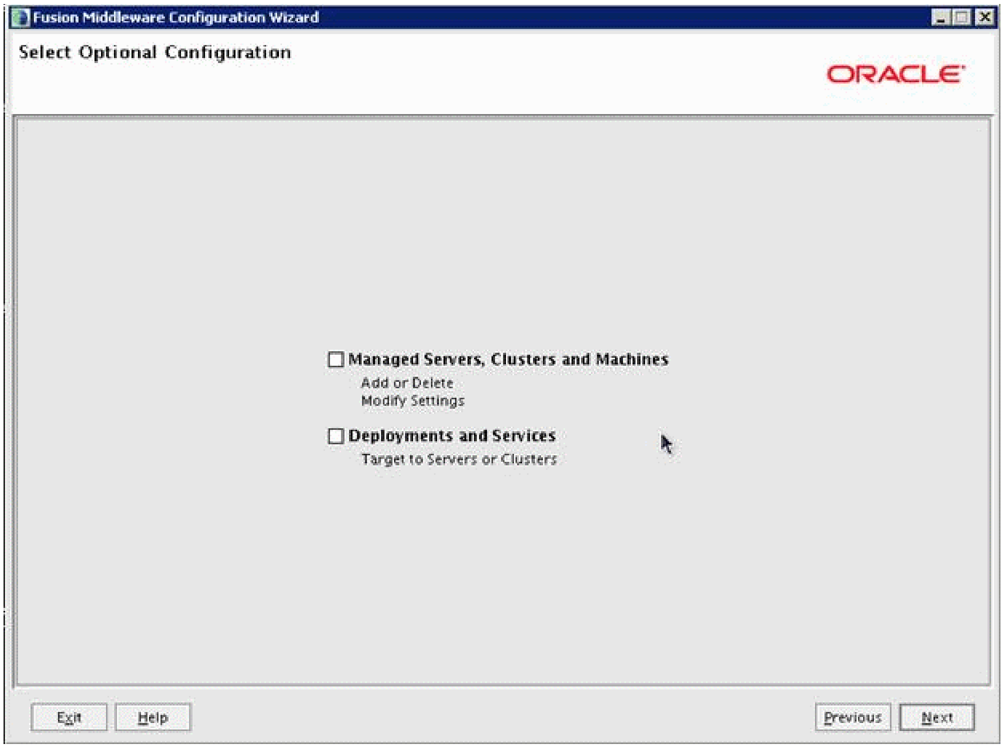
Enter the application location for the selected domain:

Domain name: MobileDomain

Domain location: /home/oracle/Oracle/Middleware10.3.5.0/user_projects/domair

Application location: /home/oracle/Oracle/Middleware10.3.5.0/user_projects/applica

8. On Specify Domain Name and Location, click Next.

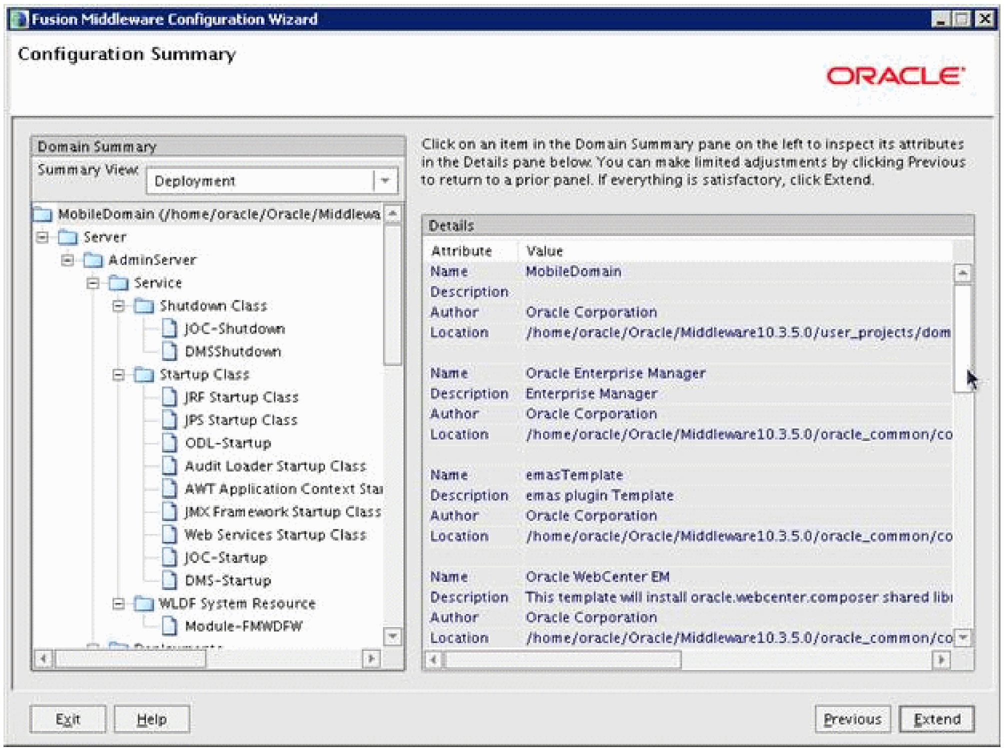


Select Optional Configuration

□ **Managed Servers, Clusters and Machines**
Add or Delete
Modify Settings

□ **Deployments and Services**
Target to Servers or Clusters

9. On Select Optional Configuration, no action is required. Click Next.



Configuration Summary

Domain Summary
Summary View: Deployment

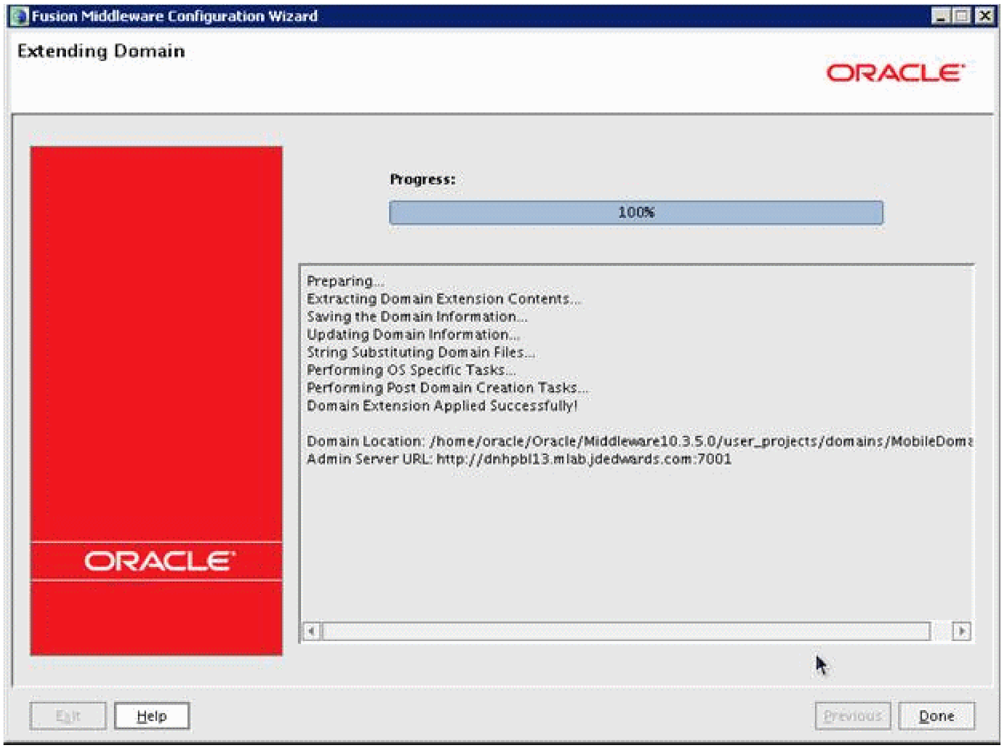
```
MobileDomain (/home/oracle/Oracle/Middlewa
  Server
    AdminServer
      Service
        Shutdown Class
          JOC-Shutdown
          DMSShutdown
        Startup Class
          JRF Startup Class
          JPS Startup Class
          ODL-Startup
          Audit Loader Startup Class
          AWT Application Context Star
          JMX Framework Startup Class
          Web Services Startup Class
          JOC-Startup
          DMS-Startup
        WLDF System Resource
          Module-FMWDFW
```

Click on an item in the Domain Summary pane on the left to inspect its attributes in the Details pane below. You can make limited adjustments by clicking Previous to return to a prior panel. If everything is satisfactory, click Extend.

Details

Attribute	Value
Name	MobileDomain
Description	
Author	Oracle Corporation
Location	/home/oracle/Oracle/Middleware10.3.5.0/user_projects/dom
Name	Oracle Enterprise Manager
Description	Enterprise Manager
Author	Oracle Corporation
Location	/home/oracle/Oracle/Middleware10.3.5.0/oracle_common/co
Name	emasTemplate
Description	emas plugin Template
Author	Oracle Corporation
Location	/home/oracle/Oracle/Middleware10.3.5.0/oracle_common/co
Name	Oracle WebCenter EM
Description	This template will install oracle.webcenter.composer shared libı
Author	Oracle Corporation
Location	/home/oracle/Oracle/Middleware10.3.5.0/oracle_common/co

10. On Configuration Summary, review your configuration details, and then click the Extend button.



```
Preparing...
Extracting Domain Extension Contents...
Saving the Domain Information...
Updating Domain Information...
String Substituting Domain Files...
Performing OS Specific Tasks...
Performing Post Domain Creation Tasks...
Domain Extension Applied Successfully!

Domain Location: /home/oracle/Oracle/Middleware10.3.5.0/user_projects/domains/MobileDoma
Admin Server URL: http://dnhpbl13.mlab.jdedwards.com:7001
```

11. On Extending Domain, after the progress reaches 100%, click Done.
12. Update the NodeManager.properties file:
    a. In a text editor, open the NodeManager.properties file from the following directory:

       ```
       <wls_home>/wlserver_10.3/common/nodemanager/nodemanager.properties
       ```

    b. Set the StartScriptEnabled parameter to true:

       ```
       StartScriptEnabled=true
       ```

    c. Save and close the file.
    d. Restart nodemanager.
13. Start the Administration Server for the WebLogic Server domain by selecting Oracle WebLogic, User Projects, mobile_domain, Start Admin Server for WebLogic Server Domain.

2.3 Creating and Deploying the EnterpriseOne Shared Library on WebLogic Server

The JD Edwards EnterpriseOne Mobile Foundation download contains a shared library with Trinidad and ADF jar files that are required to run EnterpriseOne mobile applications. Follow the steps in this section to deploy the shared library to the newly created domain for the mobile applications deployment.

> **Important:** If you are deploying 9.1.2 mobile applications, you must use the updated EnterpriseOne Mobile Foundation. It contains an updated Shared Library with an additional jar file to support the EnterpriseOne Mobile Menu application. See Prerequisites - Mobile Application Downloads (Release 9.1.2 Update) in this guide for more information.

1. Open the Build.properties file and update the following attributes for your environment.

   - `host`

     Enter the WebLogic Server host name or IP address of the machine where the WebLogic domain is extended for ADF runtime. This is the domain for hosting the mobile applications.

   - `port`

     Enter the port number of the port on which the Administration Console is running.

2. To run the script that deploys the shared library, open a command prompt and access the directory that contains the shared library script.

3. Enter the following command to configure the WLS_HOME parameter to point to the `middleware\wlserver_10.3\server` directory:

   ```
   set WLS_HOME=<drive>:\Oracle\Middleware\wlserver_10.3\server
   ```

4. Enter the following command to configure the DOMAIN_NAME parameter to point to the domain to which the shared library will be deployed:

   ```
   set DOMAIN_NAME=<mobile_domain>
   ```

   > **Note:** Make sure that the domain that you specify is the same domain that you extended in Section 2.2, "Extending the WebLogic Server Domain For ADF Runtime." This is the domain to which you will deploy EnterpriseOne mobile applications.

5. Run JDECreateSharedLib.cmd and JDECreateSharedLib.sh on Windows and UNIX platforms respectively.

   - Use the following command to deploy the shared library:

     ```
     JDECreateSharedLib.cmd -Dmode=D
     ```

   - If you need to remove the shared library, use the following command:

     ```
     JDECreateSharedLib.cmd -Dmode=U
     ```

6. At the prompt, enter the user ID and password for the WebLogic Admin server, and then press Enter.

7. Wait for the Build Successful message to appear.

   To confirm that shared library built successfully, log in to the Admin Console and confirm that it is listed on the Deployments page.

2.4 Configuring the Authentication Provider

> **Important:** Before completing the tasks in this section, you must:
>
> 1. Make sure that you have downloaded the JD Edwards EnterpriseOne Mobile Foundation, which contains the JDEADFMobileAuthenticationProvider.jar and JDEADFMobileLoginModule.jar files.
> 2. Install the ESU for the Authentication Business Service before configuring the jar files.
>
> See EnterpriseOne Mobile Foundation in this guide for more information.

This section contains the following topics:

- Section 2.4.1, "Creating a Managed Server for an EnterpriseOne Mobile Applications Deployment"
- Section 2.4.2, "Deploying the JDEADFMobileAuthenticationProvider.jar"
- Section 2.4.3, "Adding the Authentication Provider to the Security Realm"
- Section 2.4.4, "Configuring and Deploying the JDEADFMobileLoginModule.jar"

2.4.1 Creating a Managed Server for an EnterpriseOne Mobile Applications Deployment

Create a new managed server in the WebLogic Server domain to host the EnterpriseOne mobile applications. After you create the managed server, map the machine within the managed server configuration so that Node Manager can start and stop the managed server.

When you perform the steps in the following sections, you will use this server for the configuration and deployment of the EnterpriseOne mobile components.

To create a managed server:

1. In the Admin Console, click the Environment link, and then Servers.
2. Click the Lock & Edit button.
3. In the Servers area, click the New button.
4. On Create a New Server, complete these fields:
   - **Server Name:** Enter a unique name.
   - **Server Listener Port:** Enter a unique port number.
5. Click the Next button, and then click Finish.
6. Click the Activate Changes button.
7. To start the server, click the link of the new managed server.

2.4.2 Deploying the JDEADFMobileAuthenticationProvider.jar

Deploying the JDEADFMobileAuthenticationProvider.jar is a one-time task that you perform on the newly created domain for the mobile applications deployment. You do not need to be perform this task again if you install additional mobile applications on the same domain.

Deploy the JDEADFMobileAuthenticationProvider.jar on the same server as ADF runtime and EnterpriseOne mobile applications.

To deploy the JDEADFMobileAuthenticationProvider.jar:

1. Copy JDEADFMobileAuthenticationProvider.jar to the following location:

   For UNIX: `/u01/Oracle/Middleware/wlserver_10.3/server/lib/mbeantypes`

   For Windows: `X:\Oracle\Middleware\wlserver_10.3\server\lib\mbeantypes`

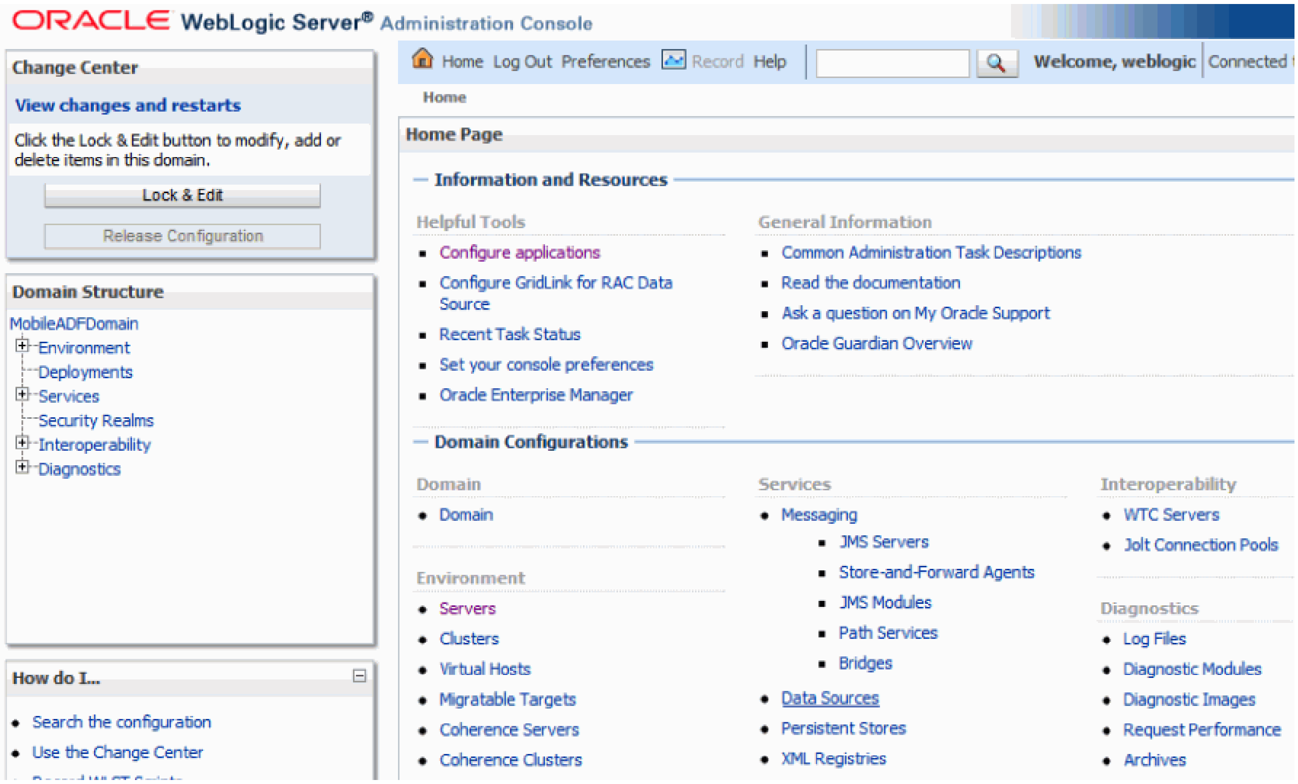
2. Restart the WebLogic Administration Server and all servers.

2.4.3 Adding the Authentication Provider to the Security Realm

This is a one-time task for the domain; you do not need to perform this task again if you install additional mobile applications on the same domain.

To add the Authentication Provider to the Security Realm:

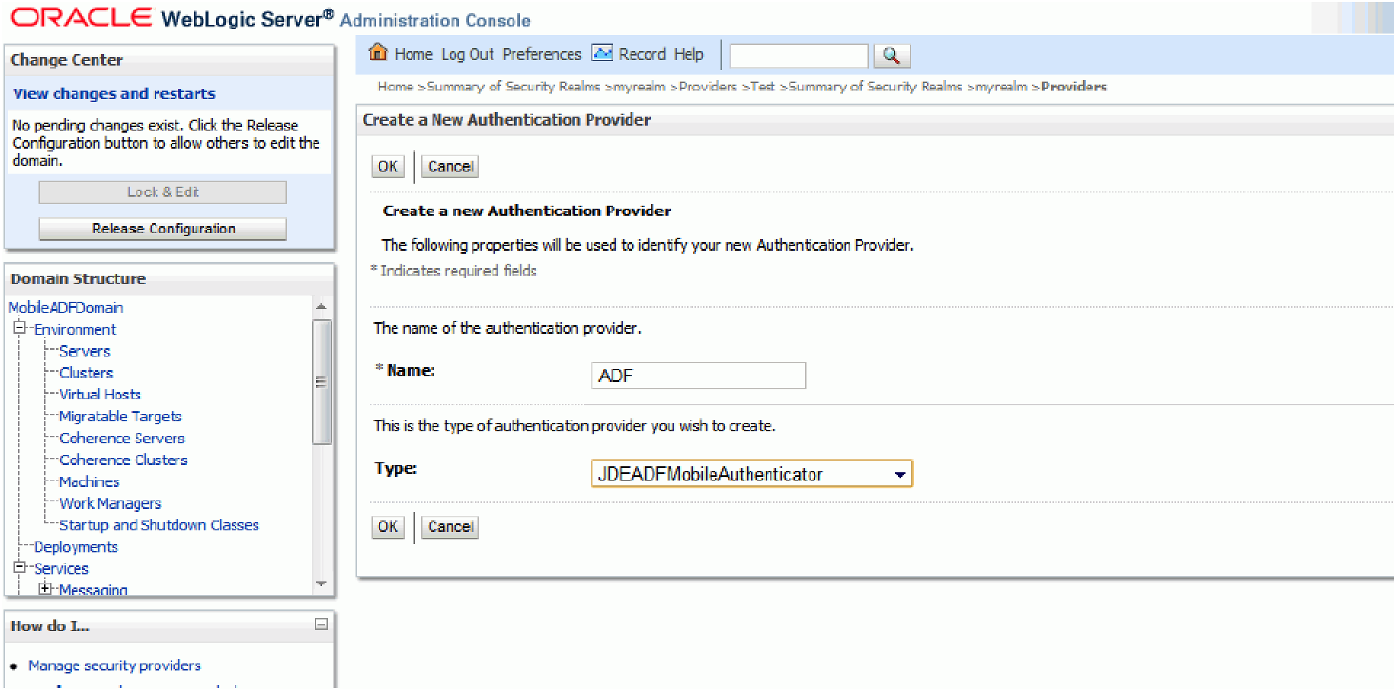
1. Log in to the Oracle WebLogic Server Administration Console.



Click the Lock & Edit button to modify, add or delete items in this domain.

2. On the Administration Console, select Security Realms, myrealm, and then select the Providers tab.

3. Click the New button.



ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Home >Summary of Security Realms >myrealm >Providers >Test >Summary of Security Realms >myrealm >**Providers**

Change Center

View changes and restarts

No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Lock & Edit

Release Configuration

Domain Structure

MobileADFDomain
- Environment
  - Servers
  - Clusters
  - Virtual Hosts
  - Migratable Targets
  - Coherence Servers
  - Coherence Clusters
  - Machines
  - Work Managers
  - Startup and Shutdown Classes
- Deployments
- Services
  - Messaging

How do I...

- Manage security providers

Create a New Authentication Provider

OK Cancel

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.

* Indicates required fields

The name of the authentication provider.

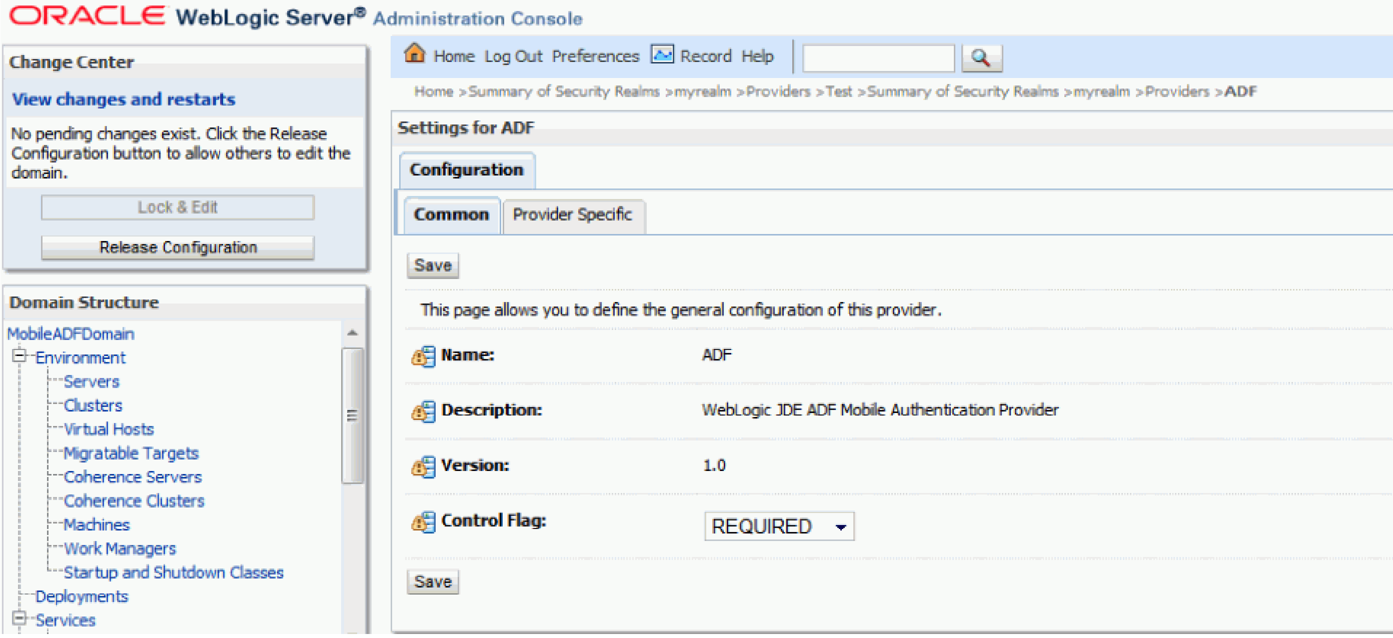
* **Name:** ADF

This is the type of authentication provider you wish to create.

Type: JDEADFMobileAuthenticator

OK Cancel

4. In the Name field, enter a name for the Authentication Provider.
5. From the Type drop-down menu, select JDEADFMobileAuthenticator.
6. Click OK to add it.



ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Home >Summary of Security Realms >myrealm >Providers >Test >Summary of Security Realms >myrealm >Providers >**ADF**

Change Center

View changes and restarts

No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Lock & Edit

Release Configuration

Domain Structure

MobileADFDomain
- Environment
  - Servers
  - Clusters
  - Virtual Hosts
  - Migratable Targets
  - Coherence Servers
  - Coherence Clusters
  - Machines
  - Work Managers
  - Startup and Shutdown Classes
- Deployments
- Services

Settings for ADF

Configuration

Common | Provider Specific

Save

This page allows you to define the general configuration of this provider.

Name: ADF

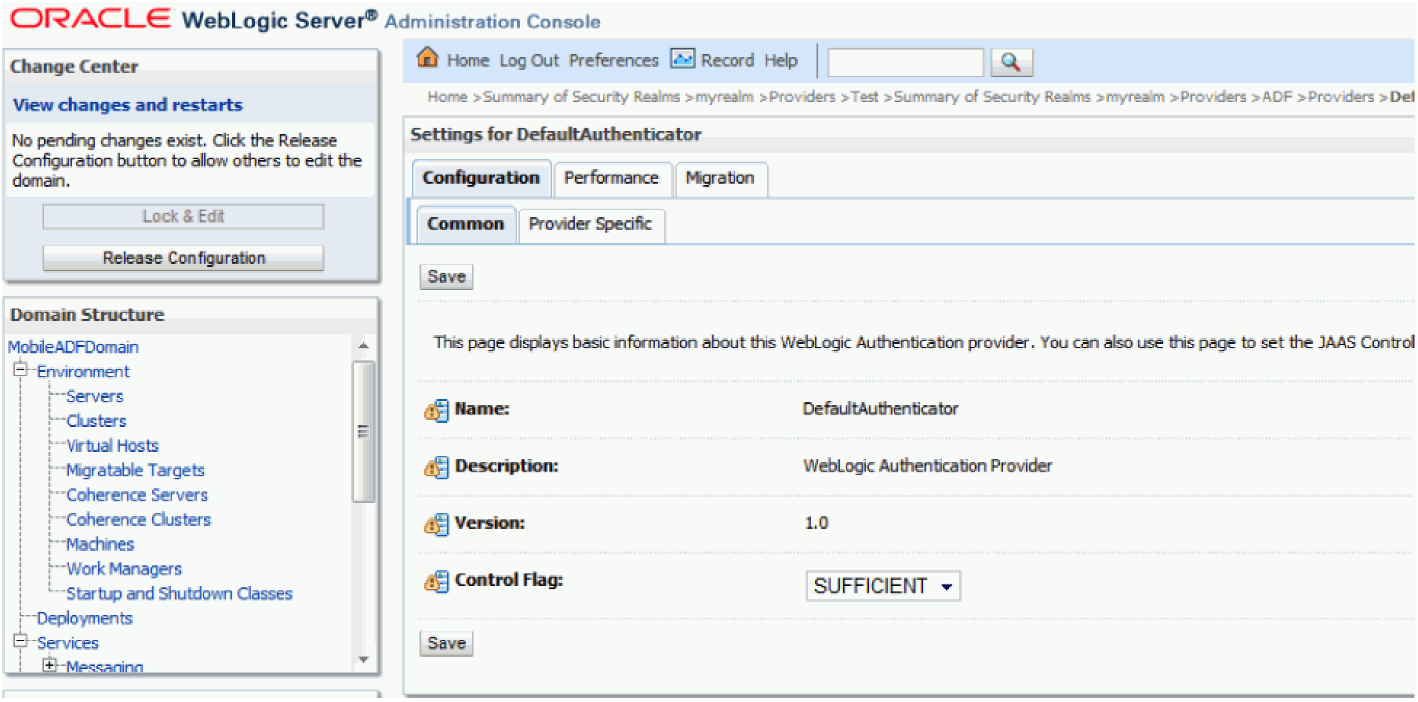
Description: WebLogic JDE ADF Mobile Authentication Provider

Version: 1.0

Control Flag: REQUIRED

Save

7. Select the newly added Authentication Provider, and change the Control Flag to REQUIRED.
8. Click the Save button and then return to the Providers tab by clicking Security Realms, myrealm, and then the Providers tab.
9. Click the DefaultAuthenticator.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Home >Summary of Security Realms >myrealm >Providers >Test >Summary of Security Realms >myrealm >Providers >ADF >Providers >Def

Settings for DefaultAuthenticator

This page displays basic information about this WebLogic Authentication provider. You can also use this page to set the JAAS Control

Name: DefaultAuthenticator

Description: WebLogic Authentication Provider

Version: 1.0

Control Flag: SUFFICIENT

10. Select SUFFICIENT from the Control Flag drop-down menu.
11. Click Save.
12. Click the Activate Changes button.
13. Restart the WebLogic Administration Server and all servers.

Note: You must restart the servers for the changes to take affect.

2.4.4 Configuring and Deploying the JDEADFMobileLoginModule.jar

The JDEADFMobileLoginModule.jar contains parameters for configuring the login options available to mobile application users. You can determine whether the login screen:

- Displays the Role and Environment fields so that users have to manually enter a role and environment.

  or

- Hides the Role and Environment fields so that users have to use a preset role and environment.

To configure and deploy the login module:

1. Copy JDEADFMobileLoginModule.jar to a folder on Oracle WebLogic Server.
2. On the Server Start tab of the new managed server, which you created as directed in Section 2.4.1, enter the path to the JDEADFMobileLoginModule.jar file in the Class Path field.
3. In the Arguments field, add the following parameters: (See step 4 for parameters for an EnterpriseOne 9.1.2 mobile applications deployment; see step 5 for an additional parameter for EnterpriseOne Tools Release 9.1 Update 4.)

Parameter	Value Description
DBSSVSERVER_URL	Enter the URL of the Business Services Server used for authentication.
DBSSVSERVER_TYPE	Enter WLS for WebLogic Server or WAS for WebSphere Application Server.
DDEFAULT_ENV	Use this parameter only if DDISPLAY_ENV_ROLE is set to false. Enter the name of the EnterpriseOne environment. The environment that you enter will appear by default in the login screen for the mobile applications.
DDEFAULT_ROLE	Use only if DDISPLAY_ENV_ROLE is set to false. Enter the role to be used for sign-in. The role that you enter will appear by default in the login screen for the mobile applications.
DDISPLAY_ENV_ROLE	Valid values are: ■ true Displays the Role and Environment fields on the login screen so users can manually enter a role and environment for sign-in. ■ false Hides the Role and Environment fields on the login screen. If you set this parameter to false, then you must add the DDEFAULT_ENV and DDEFAULT_ROLE parameters to the Arguments field.

The following is an example of the Arguments field completed for WebLogic Server:

```
-DBSSVSERVER_URL=https://servername:port/STAGINGA/AuthenticationManager
-DBSSVSERVER_TYPE=WLS -DDEFAULT_ENV=STGAWSC1 -DDEFAULT_ROLE=*ALL -DDISPLAY_ENV_
ROLE=true
```

4. For EnterpriseOne 9.1.2 and 9.0.2 mobile applications, enter the following parameters in the Arguments field, which include additional parameters for the EnterpriseOne Mobile Menu application and JAX-WS support:

Parameter	Value Description
DBSSVSERVER_URL	Enter the URL of the Business Services Server used for authentication, for example: `https://<BSSV_Server_Name>:<BSSV_Server_Port>/<URI_To_AuthenticationManager_Business_Service>`
DBSSVSERVER_TYPE	Enter WLS for WebLogic Server or WAS for WebSphere Application Server.
DBSSVDEPLOY_TYPE	Valid values are: ■ RPC Enter this value if the Business Services Server has a JAX-RPC based business services package. ■ WS Enter this value if the Business Services Server has a JAX-WS based business services package.

Parameter	Value Description
DDEFAULT_ENV	Use this parameter only if DDISPLAY_ENV_ROLE is set to false. Enter the name of the EnterpriseOne environment. The environment that you enter will appear by default in the login screen for the mobile applications.
DDEFAULT_ROLE	Use only if DDISPLAY_ENV_ROLE is set to false. Enter the role to be used for sign-in. The role that you enter will appear by default in the login screen for the mobile applications.
DDISPLAY_ENV_ROLE	Valid values are: ■ true Displays the Role and Environment fields on the login screen so users can manually enter a role and environment for sign-in. ■ false Hides the Role and Environment fields on the login screen. If you set this parameter to false, then you must add the DDEFAULT_ENV and DDEFAULT_ROLE parameters to the Arguments field.
DDEPLOYED_APPS	Enter the names of the mobile applications that you are deploying in the order that you want them to appear in the EnterpriseOne Mobile Menu application. See "Using the Mobile Menu" in the *JD Edwards EnterpriseOne Applications Functionality for Mobile Devices Implementation Guide* for more information. For multiple applications, separate values by commas. Valid values are: MobileSales, RequisitionSelfServiceApproval, ExpenseManagement, PurchaseOrderApproval, ServiceTimeEntry

DUPLOAD_PATH	The file folder location on the ADF server's file system for temporarily storing uploaded images (for Mobile Expense Management) before they are uploaded to EnterpriseOne media object storage. For example, the folder location could be:
	`C:\temp\uploads\`
	or
	`\u01\temp\uploads`
	The ADF server runtime must have read / write access to this folder.

The following is an example of the Arguments field completed for WebLogic Server:

```
-DBSSVSERVER_URL=https://<server>:<port>/STABLEA/AuthenticationManager
-DUPLOAD_PATH=/slot/u01/appmgr/wls1035/Middleware/user_projects/domains/E1_
Apps/tmp -DBSSVSERVER_TYPE=WLS -DBSSVDEPLOY_TYPE=WS -DDEFAULT_ENV=STBAWSC1
-DDEFAULT_ROLE=*ALL -DDISPLAY_ENV_ROLE=FALSE  -DDEPLOYED_
APPS=ExpenseManagement,MobileSales,RequisitionSelfServiceApproval,PurchaseOrder
Approval, ServiceTimeEntry
```

5. If your configuration meets the following conditions, perform the steps that follow as appropriate:

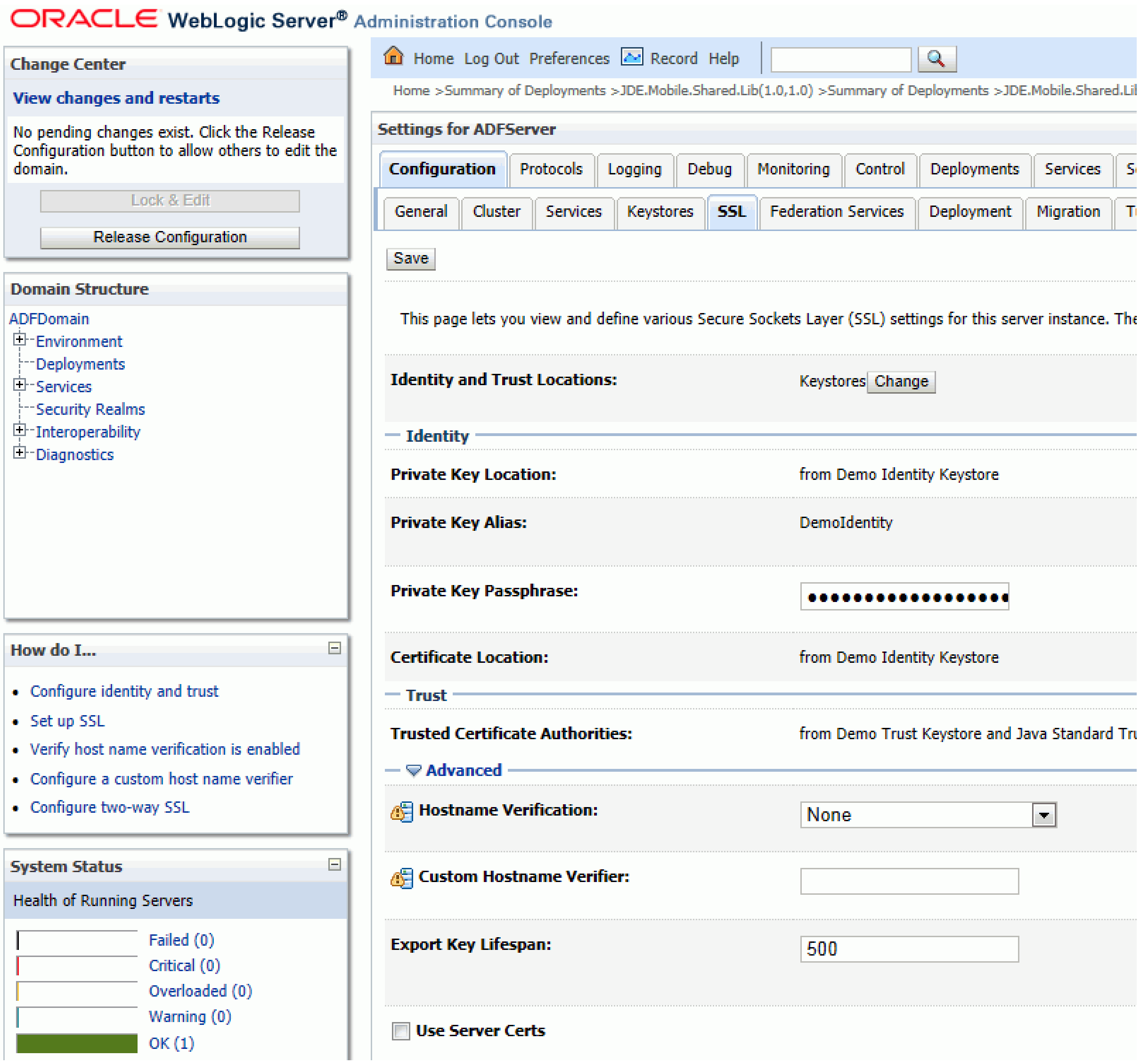
- The Business Services Server is on Oracle WebLogic Server 12.1.2, which is supported beginning with EnterpriseOne Tools release 9.1 Update 4.
- The Mobile Application Server (ADF Server) is on Oracle WebLogic Server 10.3.5.

a. If a JAX-RPC business services package is deployed on the Business Services Server, append the following text in the Arguments field:

```
-Dweblogic.wsee.workarea.skipWorkAreaHeader=true
```

b. If you are using SSL with the Business Services Server, click the SSL tab, and then select the "Use JSSE SSL" check box in the Advanced section.

6. Select the new managed server, which you created as directed in Section 2.4.1, and then on the Configuration tab, select the SSL tab.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Settings for ADFServer

This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. The

Identity and Trust Locations:	Keystores
Private Key Location:	from Demo Identity Keystore
Private Key Alias:	DemoIdentity
Private Key Passphrase:	••••••••••••••••••
Certificate Location:	from Demo Identity Keystore
Trusted Certificate Authorities:	from Demo Trust Keystore and Java Standard Tru
Hostname Verification:	None
Custom Hostname Verifier:	
Export Key Lifespan:	500

☐ Use Server Certs

7. On the SSL tab, select Advanced.

8. In the Advanced section, select None from the Hostname Verification drop-down menu.

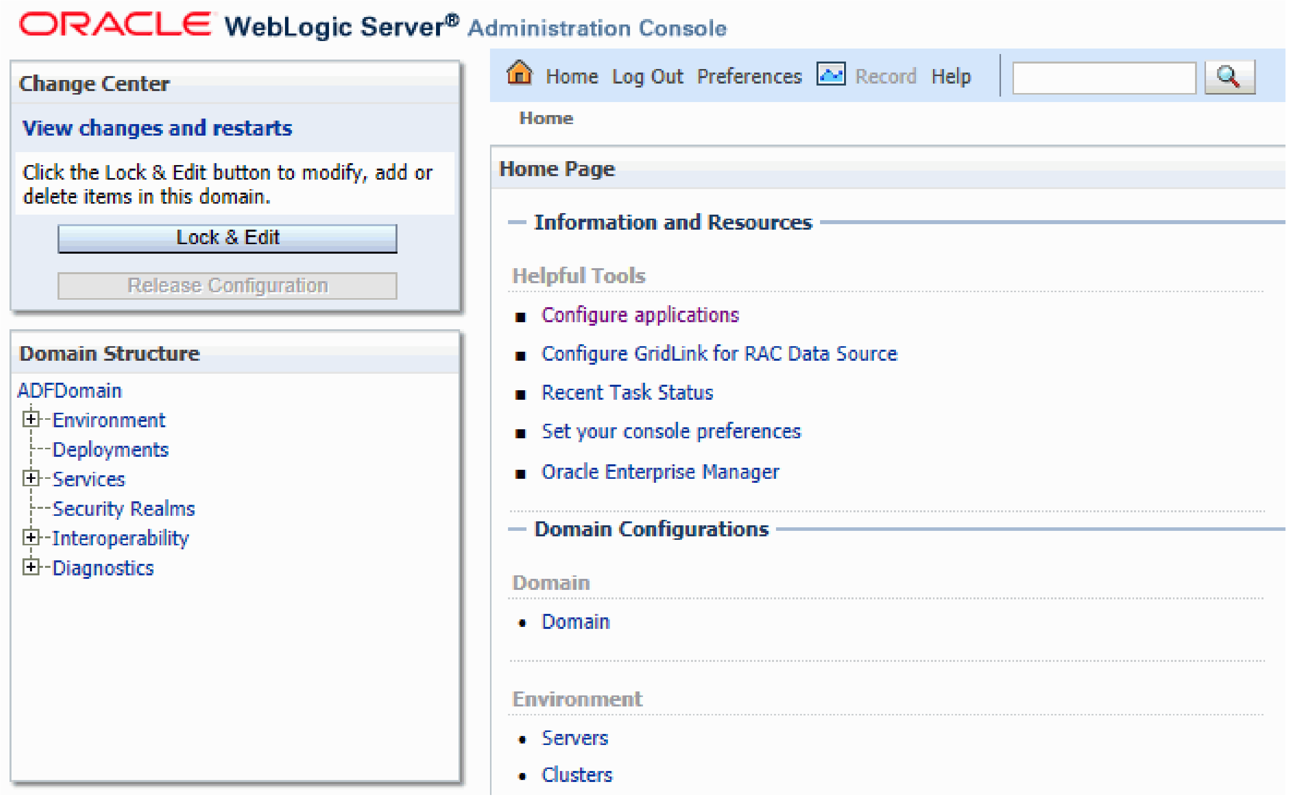
9. Click Save.

10. Click Activate Changes.
11. Restart the managed server.

2.5 Configuring Shared Library on WebLogic Server

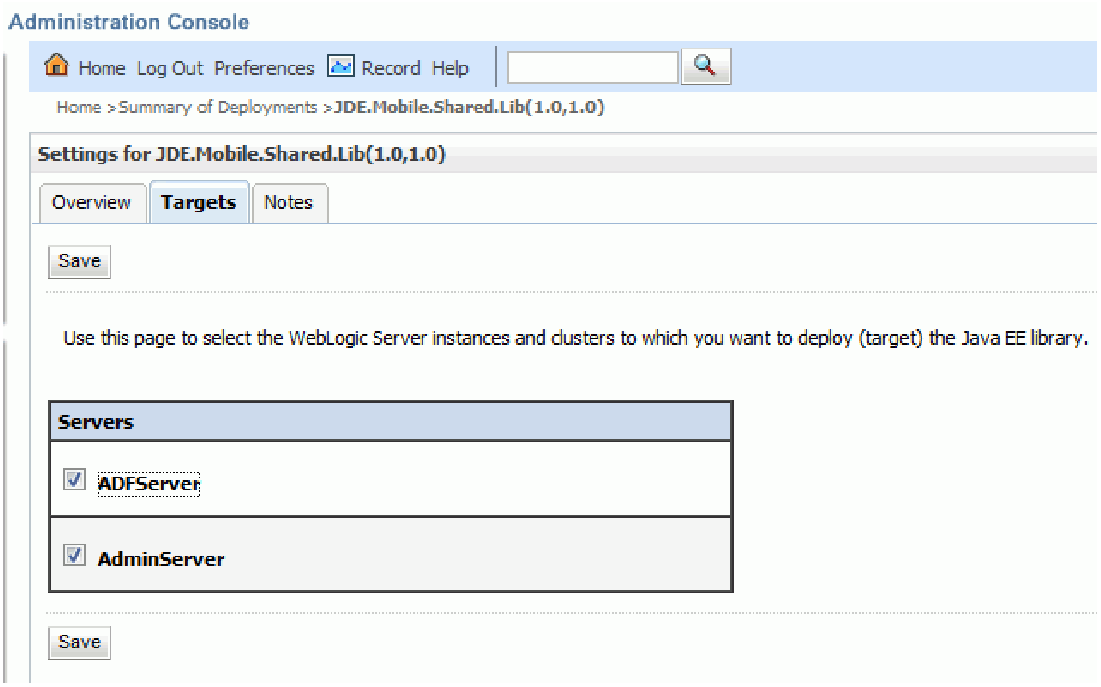
Configuring the shared library includes specifying the shared library and identifying the server on which the mobile applications will be deployed.

1. Log in to the WebLogic Server Administration Console:
   http://*hostname*:*port*/console



Click the Lock & Edit button to modify, add or delete items in this domain.

2. Click the Lock & Edit button.
3. In the Domain Structure area on the left side of the screen, click Deployments, and then select JDE.Mobile.Shared.Lib(1.0,1.0).
4. Click the Targets tab.



Administration Console
Home Log Out Preferences Record Help
Home >Summary of Deployments >JDE.Mobile.Shared.Lib(1.0,1.0)
Settings for JDE.Mobile.Shared.Lib(1.0,1.0)
Overview
Targets
Notes
Save

Use this page to select the WebLogic Server instances and clusters to which you want to deploy (target) the Java EE library.

Servers
☑ ADFServer
☑ AdminServer

5. On the Targets tab, click the check box next to the server on which the mobile applications will be deployed.
6. Click the Save button.
7. Click the Activate Changes button.
8. Restart the managed server.

2.6 Configuring Web Service Requests Between a WebLogic Server and a Business Services Server Deployed on Separate Machines

If the Business Services Server is deployed on a different machine than WebLogic Server with ADF runtime (ADF Server), you must configure the ADF Server to accept certificates coming from the Business Services Server. This enables web service requests from the ADF Server to pass through to the Business Services Server.

> **Important:**
>
> In releases prior to EnterpriseOne mobile applications release 9.1.2, only JAX-RPC based business services are supported by mobile applications; JAX-WS based business services are not supported. Therefore, the Business Services Server in the mobile applications environment must contain a package built with JAX-RPC based business services.
>
> Starting with release 9.1.2 of the mobile applications, JAX-WS based business services are supported with a minimum EnterpriseOne Tools release 9.1.2.4.

You must add the Self Signed Certificate issued by the Business Services Server into the keystore of the ADF Server instance, which involves importing the certificate into the ADF Server's DemoIdentity.jks and DemoTrust.jks files.

If the ADF Server is using a custom keystore and truststore, the certificate of the Business Services Server must be imported into the custom keystore and truststore.

The following steps describe how to add the Self Signed Certificate to the ADF Server when using a default keystore and truststore. These steps pertain to Microsoft Internet Explorer, but you can use any browser to add the certificate.

1. Create a back up of the following files located in the `\\Oracle\Middleware\wlserver_10.3\server\lib\` directory:
   - DemoTrust.jks
   - DemoIdentity.jks
2. To install and export the certificate:
   a. Open Internet Explorer and enter this URL:

      ```
      https://BSSVSERVER:PORT/DV900/AuthenticationManager
      ```

   b. Click the "Continue to this webbiest (not recommended)" link.

      The following message appears:

      ```
      Welcome to the
      {tap://oracle.e1.bssv.JPH90I01/}AuthenticationManager home page
      ```

      ```
      Test page
      ```

      ```
      WSDL page
      ```

      In the address bar, the Certificate Error button appears next to the Refresh button.

   c. Click the Certificate Error button and select View Certificate.

   d. Click the Install Certificate button.

   e. Continue through the wizard until you receive the "Import was successful" message, and then click Ok.

   f. In Internet Explorer, select the Tools menu, Internet Options, Content tab, and then the Certificates button.

   g. Click the Intermediate Certification Authorities or Other People tab and look for the Business Services Server machine name in the "Issue To" column.

   h. Click the Export button.

   i. Select the "DER encoded binary X.509 (.CER)" option.

   j. Browse to the location you want to export this file and enter this name for the file:

      ```
      myCertificate.cer
      ```

3. Enter the following commands to import the myCertificate.cer file created in the preceding step into the DemoIdentity.jks file:

   ```
   D:\jrockit-jdk1.6.0_24-R28.1.3-4.0.1\bin\keytool.exe -import -keystore
   ```

   ```
   C:\Oracle\Middleware\wlserver_10.3\server\lib\DemoIdentity.jks -alias
   myCertificate -file C:\myCertificate.cer
   ```

   Note: The passphrase for the Demo Identity keystore is DemoIdentityKeyStorePassPhrase; if using a custom keystore, the passphrase could be different.

4. Enter the following commands to import the myCertificate.cer file created in the preceding step into the DemoTrust.jks file:

   ```
   D:\jrockit-jdk1.6.0_24-R28.1.3-4.0.1\bin\keytool.exe -import -keystore
   ```

   ```
   C:\Oracle\Middleware\wlserver_10.3\server\lib\DemoTrust.jks -alias
   myCertificate -file C:\myCertificate.cer
   ```

   > **Note:** The passphrase for the Demo Identity keystore is DemoTrustKeyStorePassPhrase; if using a custom truststore, the passphrase could be different.

   After the import operations succeeds, the "Certificate was added to keystore" message is displayed.

5. For the changes to take affect, restart the managed servers and the Admin Server.

3 Installing EnterpriseOne Mobile Applications

This chapter contains the following topics:

- Section 3.1, "Installing an EnterpriseOne Mobile Application"
- Section 3.2, "Obtaining the URL to a Mobile Application"
- Section 3.3, "Hosting a Connection for the Native JD Edwards EnterpriseOne Mobile Applications Application (Mobile Applications Release 9.1.2)"

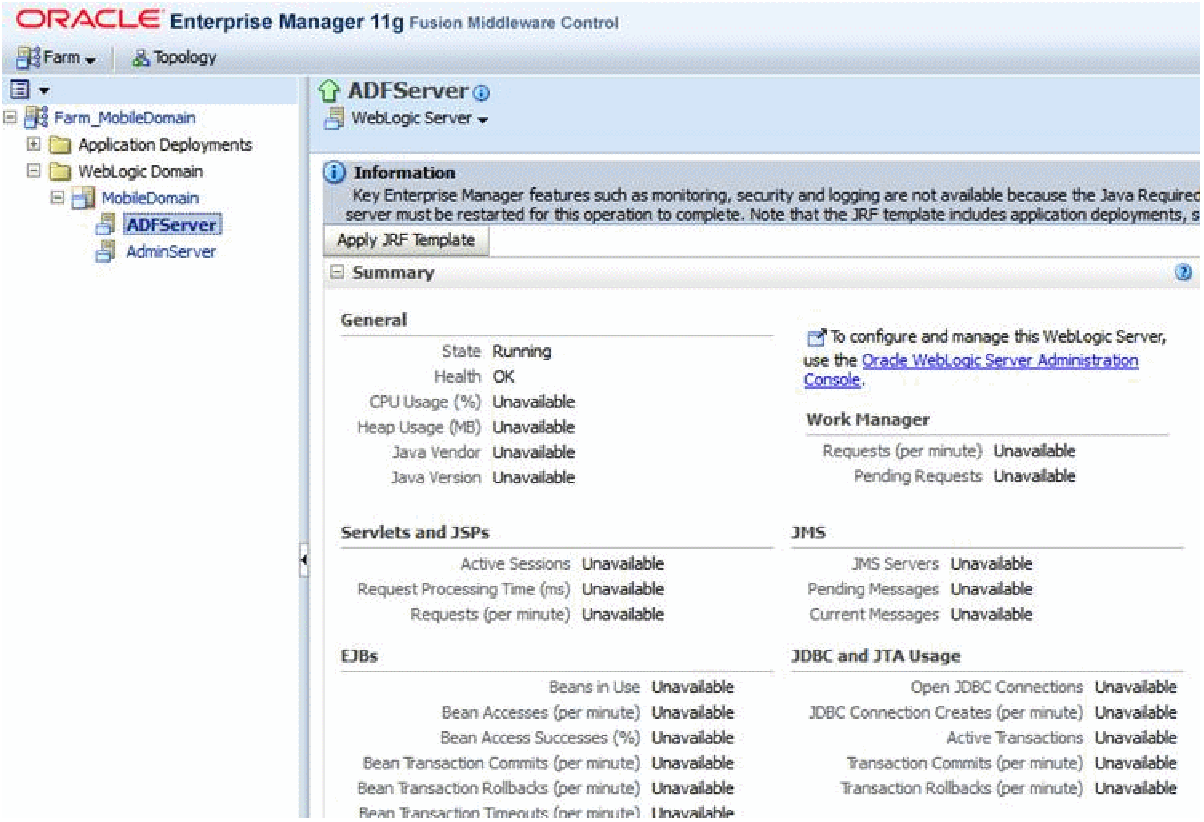
> **Important:** If you are deploying 9.1.2 mobile applications, you cannot deploy them in a pre-9.1.2 mobile applications configuration. You must create a new domain for deploying the 9.1.2 mobile applications. See What's New in JD Edwards EnterpriseOne 9.1.2 Mobile Applications in this guide before continuing.

3.1 Installing an EnterpriseOne Mobile Application

Each EnterpriseOne mobile application is packaged in a separate .ear file. Follow the steps in this section to install the .ear file of each mobile application that you want to deploy.

To install an EnterpriseOne mobile application .ear file:

1. Upload the mobile application .ear file on Oracle WebLogic Server.
2. Extract the file on the server.
3. Open a Web browser and navigate to http://*weblogicserver*:*port*/em
4. Log in to Oracle Enterprise Manager 11g Fusion Middleware Control.



Information

Key Enterprise Manager features such as monitoring, security and logging are not available because the Java Required server must be restarted for this operation to complete. Note that the JRF template includes application deployments, s

General

State	Running
Health	OK
CPU Usage (%)	Unavailable
Heap Usage (MB)	Unavailable
Java Vendor	Unavailable
Java Version	Unavailable

To configure and manage this WebLogic Server, use the Oracle WebLogic Server Administration Console.

Work Manager

Requests (per minute)	Unavailable
Pending Requests	Unavailable

Servlets and JSPs

Active Sessions	Unavailable
Request Processing Time (ms)	Unavailable
Requests (per minute)	Unavailable

JMS

JMS Servers	Unavailable
Pending Messages	Unavailable
Current Messages	Unavailable

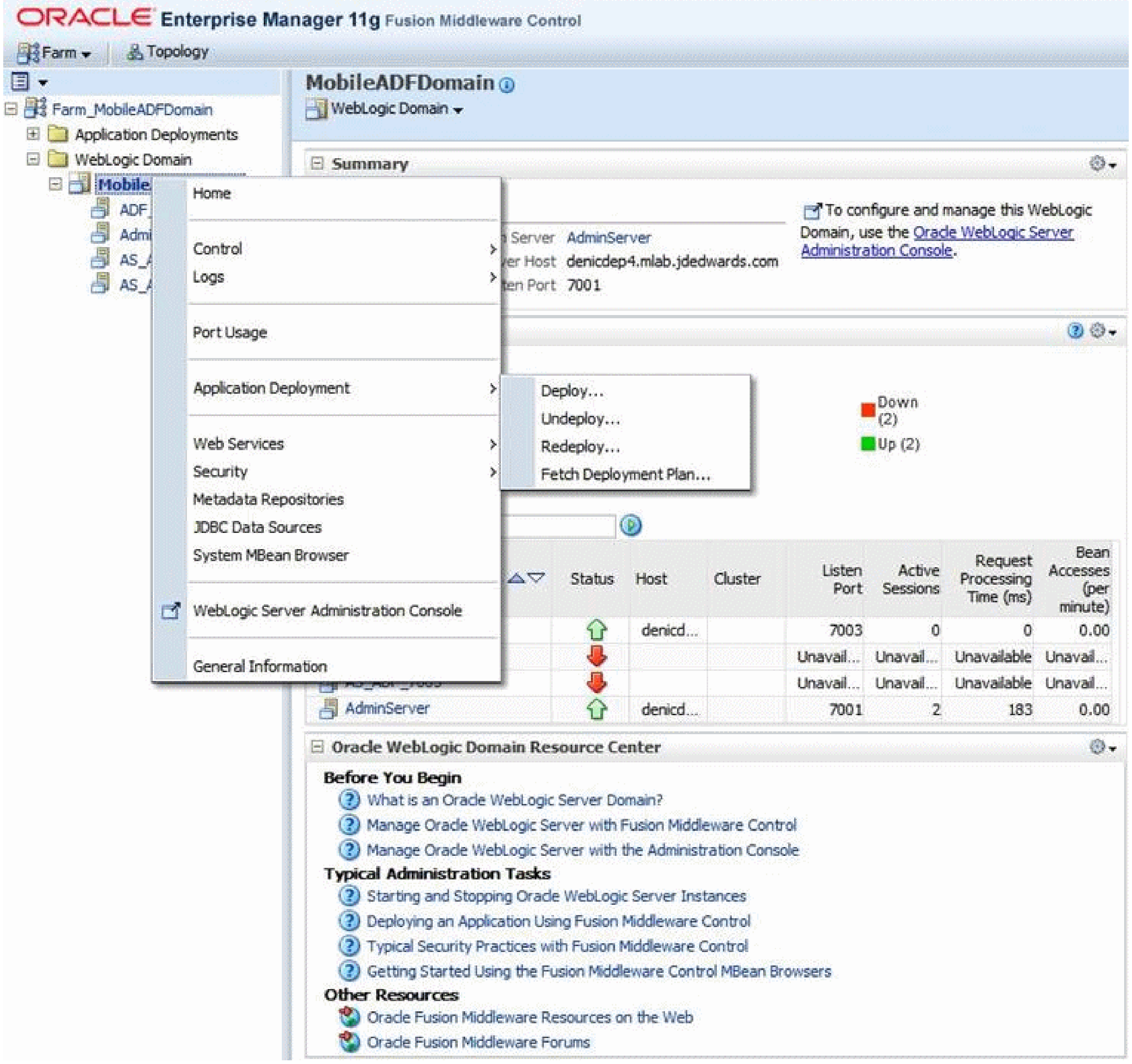
EJBs

Beans in Use	Unavailable
Bean Accesses (per minute)	Unavailable
Bean Access Successes (%)	Unavailable
Bean Transaction Commits (per minute)	Unavailable
Bean Transaction Rollbacks (per minute)	Unavailable
Bean Transaction Timeouts (per minute)	Unavailable

JDBC and JTA Usage

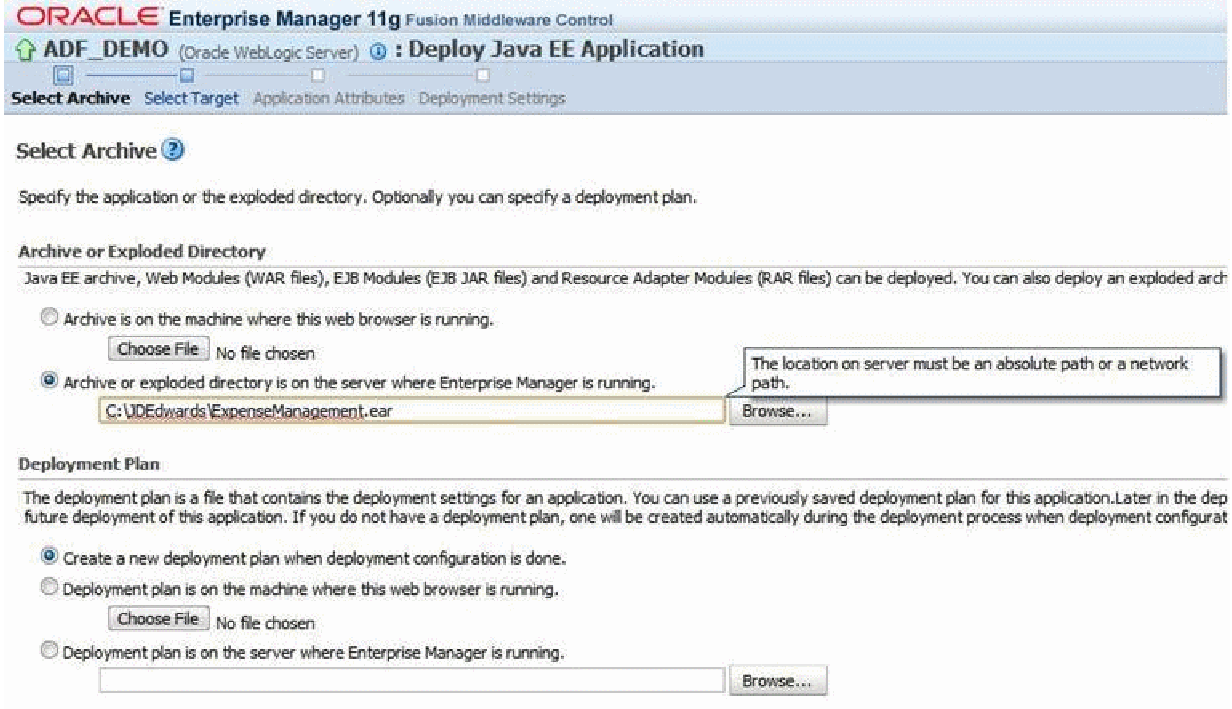
Open JDBC Connections	Unavailable
JDBC Connection Creates (per minute)	Unavailable
Active Transactions	Unavailable
Transaction Commits (per minute)	Unavailable
Transaction Rollbacks (per minute)	Unavailable

5. In the tree in the left pane, expand the Farm node and select the domain.
6. Under the domain, select the desired managed server, and then click the Apply JRF Template button.
7. Restart the managed server after applying the JRF template.


ORACLE Enterprise Manager 11g Fusion Middleware Control
Farm
Topology
Farm_MobileADFDomain
Application Deployments
WebLogic Domain
Mobile
ADF_
Admi
AS_A
AS_A
Home
Control
Logs
Port Usage
Application Deployment
Web Services
Security
Metadata Repositories
JDBC Data Sources
System MBean Browser
WebLogic Server Administration Console
General Information
Deploy...
Undeploy...
Redeploy...
Fetch Deployment Plan...
MobileADFDomain
WebLogic Domain
Summary
n Server AdminServer
er Host denicdep4.mlab.jdedwards.com
ten Port 7001
To configure and manage this WebLogic Domain, use the Oracle WebLogic Server Administration Console.
Down (2)
Up (2)
Oracle WebLogic Domain Resource Center
Before You Begin
What is an Oracle WebLogic Server Domain?
Manage Oracle WebLogic Server with Fusion Middleware Control
Manage Oracle WebLogic Server with the Administration Console
Typical Administration Tasks
Starting and Stopping Oracle WebLogic Server Instances
Deploying an Application Using Fusion Middleware Control
Typical Security Practices with Fusion Middleware Control
Getting Started Using the Fusion Middleware Control MBean Browsers
Other Resources
Oracle Fusion Middleware Resources on the Web
Oracle Fusion Middleware Forums

	Status	Host	Cluster	Listen Port	Active Sessions	Request Processing Time (ms)	Bean Accesses (per minute)
	↑	denicd...		7003	0	0	0.00
	↓			Unavail...	Unavail...	Unavailable	Unavail...
AS_ADF_7003	↓			Unavail...	Unavail...	Unavailable	Unavail...
AdminServer	↑	denicd...		7001	2	183	0.00

8. In Oracle Enterprise Manager, right-click the domain and select the Application Deployment menu, and then select Deploy.



ORACLE Enterprise Manager 11g Fusion Middleware Control

ADF_DEMO (Oracle WebLogic Server) : Deploy Java EE Application

Select Archive

Specify the application or the exploded directory. Optionally you can specify a deployment plan.

Archive or Exploded Directory

Java EE archive, Web Modules (WAR files), EJB Modules (EJB JAR files) and Resource Adapter Modules (RAR files) can be deployed. You can also deploy an exploded arch

○ Archive is on the machine where this web browser is running.

Choose File No file chosen

● Archive or exploded directory is on the server where Enterprise Manager is running.

C:\JDEdwards\ExpenseManagement.ear Browse...

The location on server must be an absolute path or a network path.

Deployment Plan

The deployment plan is a file that contains the deployment settings for an application. You can use a previously saved deployment plan for this application.Later in the dep future deployment of this application. If you do not have a deployment plan, one will be created automatically during the deployment process when deployment configurat

● Create a new deployment plan when deployment configuration is done.

○ Deployment plan is on the machine where this web browser is running.

Choose File No file chosen

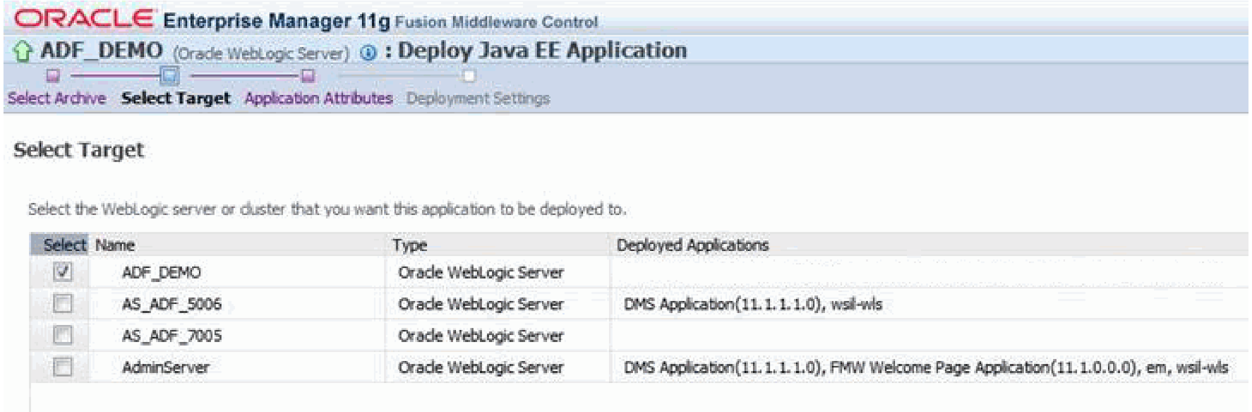
○ Deployment plan is on the server where Enterprise Manager is running.

Browse...

9. On Deploy Java EE Application, in the Archive or Exploded Directory area, select this option – "Archive or exploded directory is on the server where Enterprise Manager is running."

10. In field below this option, enter the path to the exploded folder on the server.

11. Click Next.



ORACLE Enterprise Manager 11g Fusion Middleware Control

ADF_DEMO (Oracle WebLogic Server) : Deploy Java EE Application

Select Target

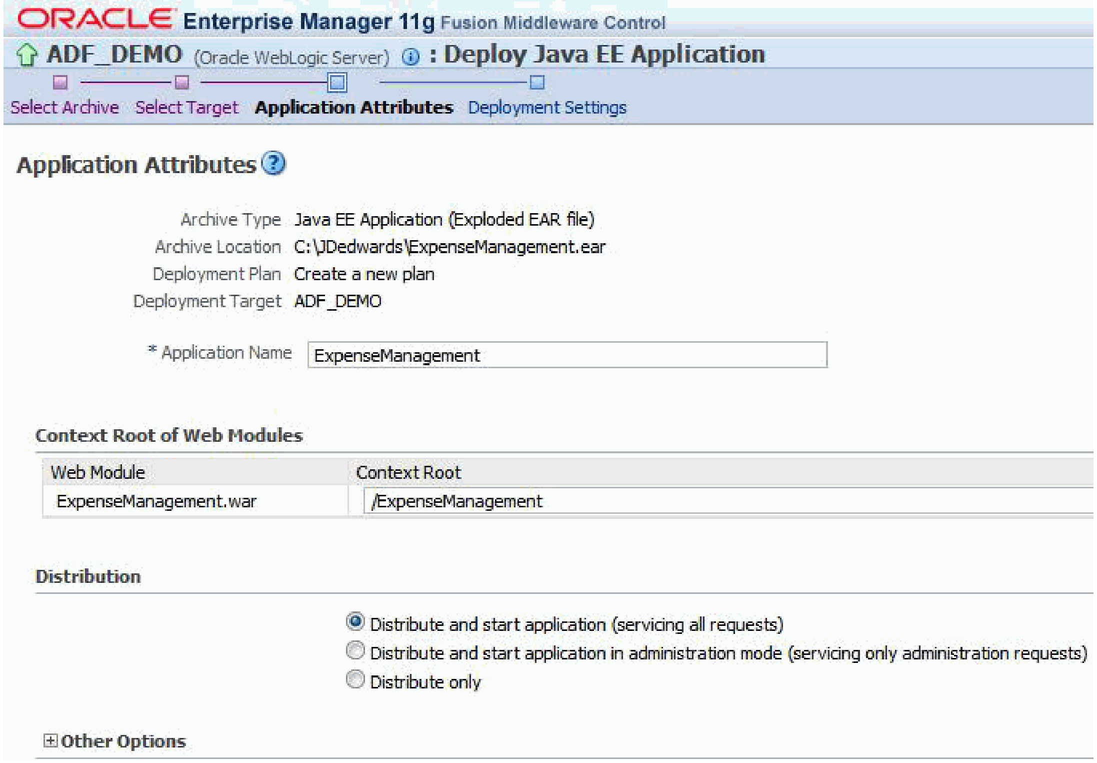
Select the WebLogic server or cluster that you want this application to be deployed to.

Select	Name	Type	Deployed Applications
☑	ADF_DEMO	Oracle WebLogic Server	
□	AS_ADF_5006	Oracle WebLogic Server	DMS Application(11.1.1.1.0), wsil-wls
□	AS_ADF_7005	Oracle WebLogic Server	
□	AdminServer	Oracle WebLogic Server	DMS Application(11.1.1.1.0), FMW Welcome Page Application(11.1.0.0.0), em, wsil-wls

12. On Select Target, select the managed server for deploying the mobile application.

    Important: You must deploy the EnterpriseOne Mobile Menu application and all of the applications to be displayed on the Mobile Menu to the same managed server. References from the Mobile Menu to the other applications are relative. Applications that are not deployed to the same managed server will not be displayed on the Mobile Menu, regardless of the DDEPLOYED_APPS Java argument configuration.

13. Click Next.


ORACLE Enterprise Manager 11g Fusion Middleware Control
ADF_DEMO (Oracle WebLogic Server) : Deploy Java EE Application
Select Archive
Select Target
Application Attributes
Deployment Settings

Application Attributes

Archive Type Java EE Application (Exploded EAR file)
Archive Location C:\JDedwards\ExpenseManagement.ear
Deployment Plan Create a new plan
Deployment Target ADF_DEMO

* Application Name ExpenseManagement

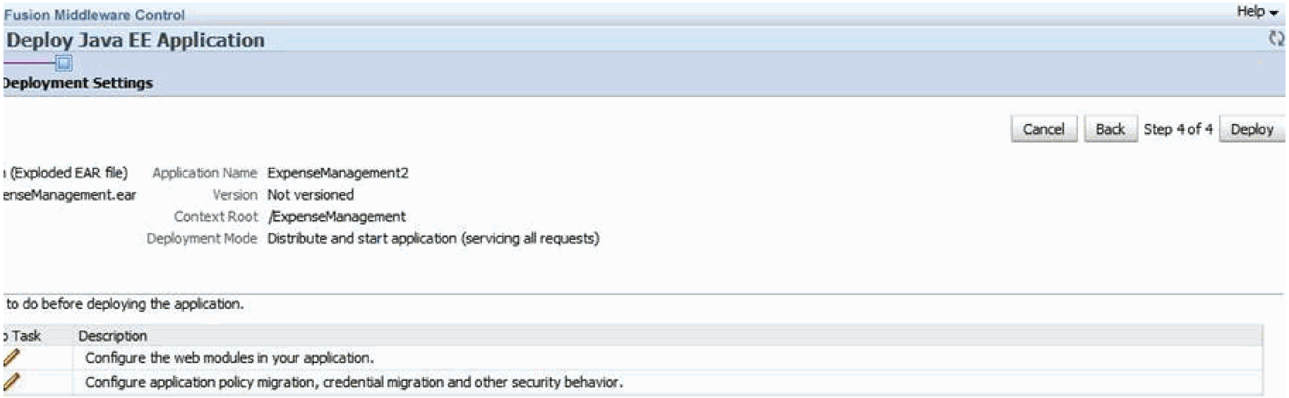
Context Root of Web Modules

Web Module	Context Root
ExpenseManagement.war	/ExpenseManagement

Distribution

● Distribute and start application (servicing all requests)
○ Distribute and start application in administration mode (servicing only administration requests)
○ Distribute only

14. On Application Attributes, click Next.



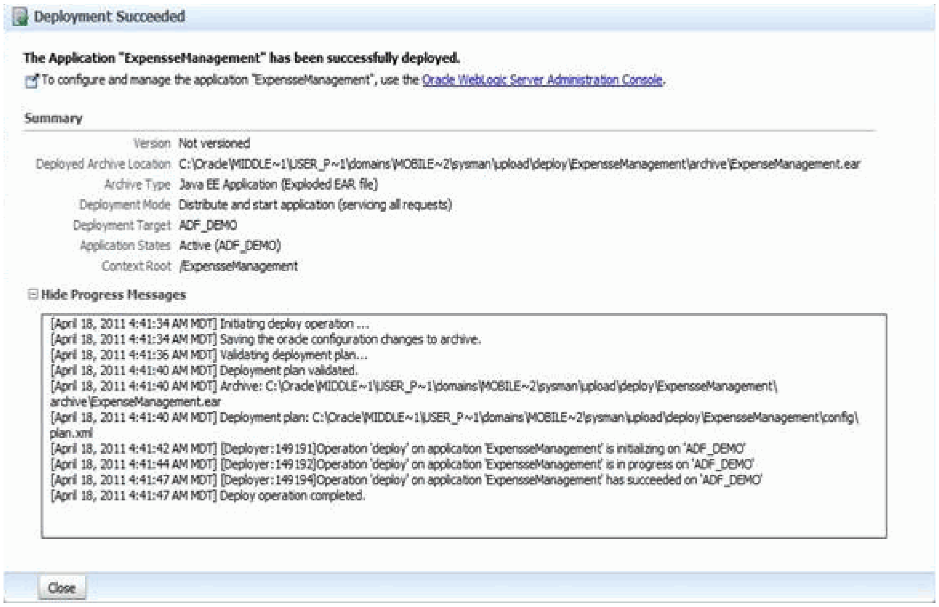
n (Exploded EAR file)
enseManagement.ear

Application Name ExpenseManagement2
Version Not versioned
Context Root /ExpenseManagement
Deployment Mode Distribute and start application (servicing all requests)

to do before deploying the application.

o Task	Description
✎	Configure the web modules in your application.
✎	Configure application policy migration, credential migration and other security behavior.

15. On Deployment Settings, click the Deploy button.



The Application "ExpensseManagement" has been successfully deployed.

To configure and manage the application "ExpensseManagement", use the Oracle WebLogic Server Administration Console.

Summary

Version	Not versioned
Deployed Archive Location	C:\Oracle\MIDDLE~1\USER_P~1\domains\MOBILE~2\sysman\upload\deploy\ExpensseManagement\archive\ExpenseManagement.ear
Archive Type	Java EE Application (Exploded EAR file)
Deployment Mode	Distribute and start application (servicing all requests)
Deployment Target	ADF_DEMO
Application States	Active (ADF_DEMO)
Context Root	/ExpensseManagement

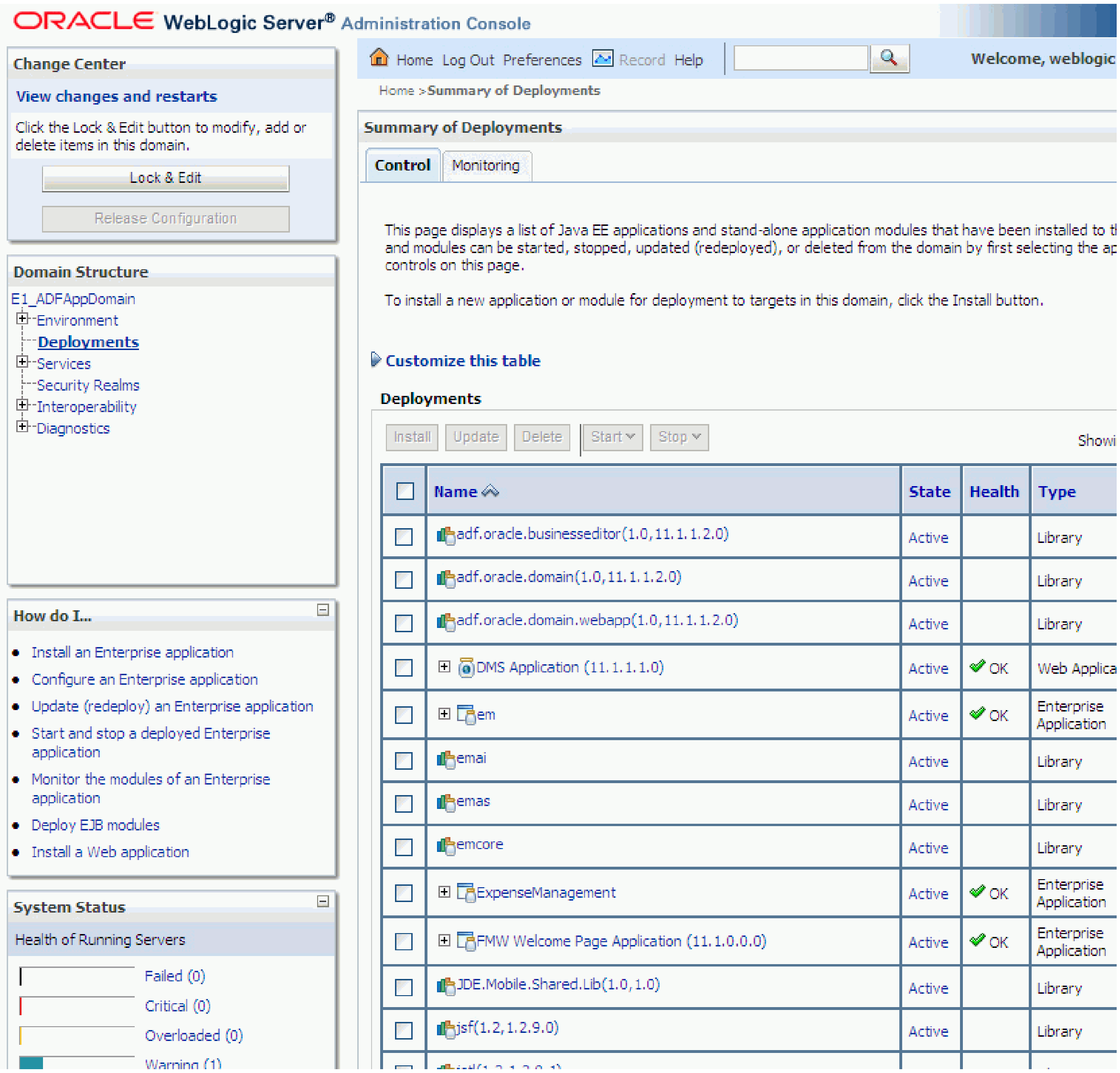
```
[April 18, 2011 4:41:34 AM MDT] Initiating deploy operation ...
[April 18, 2011 4:41:34 AM MDT] Saving the oracle configuration changes to archive.
[April 18, 2011 4:41:36 AM MDT] Validating deployment plan...
[April 18, 2011 4:41:40 AM MDT] Deployment plan validated.
[April 18, 2011 4:41:40 AM MDT] Archive: C:\Oracle\MIDDLE~1\USER_P~1\domains\MOBILE~2\sysman\upload\deploy\ExpensseManagement\
archive\ExpenseManagement.ear
[April 18, 2011 4:41:40 AM MDT] Deployment plan: C:\Oracle\MIDDLE~1\USER_P~1\domains\MOBILE~2\sysman\upload\deploy\ExpensseManagement\config\
plan.xml
[April 18, 2011 4:41:42 AM MDT] [Deployer:149191]Operation 'deploy' on application 'ExpensseManagement' is initializing on 'ADF_DEMO'
[April 18, 2011 4:41:44 AM MDT] [Deployer:149192]Operation 'deploy' on application 'ExpensseManagement' is in progress on 'ADF_DEMO'
[April 18, 2011 4:41:47 AM MDT] [Deployer:149194]Operation 'deploy' on application 'ExpensseManagement' has succeeded on 'ADF_DEMO'
[April 18, 2011 4:41:47 AM MDT] Deploy operation completed.
```

If the deployment succeeded screen appears, congratulations! You have successfully installed and deployed an EnterpriseOne mobile application.

3.2 Obtaining the URL to a Mobile Application

After completing the mobile application installation, obtain the URL to the deployed mobile application from Oracle WebLogic Server.

1. Log in to the WebLogic Server Administration Console.
2. In the Domain Structure pane on the left side of the screen, click the Deployments link.



ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Welcome, weblogic

Home >Summary of Deployments

Change Center

View changes and restarts

Click the Lock & Edit button to modify, add or delete items in this domain.

Lock & Edit

Release Configuration

Domain Structure

E1_ADFAppDomain
- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

How do I...

- Install an Enterprise application
- Configure an Enterprise application
- Update (redeploy) an Enterprise application
- Start and stop a deployed Enterprise application
- Monitor the modules of an Enterprise application
- Deploy EJB modules
- Install a Web application

System Status

Health of Running Servers

Failed (0)
Critical (0)
Overloaded (0)
Warning (1)

Summary of Deployments

Control | Monitoring

This page displays a list of Java EE applications and stand-alone application modules that have been installed to t and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the ap controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

Customize this table

Deployments

Install | Update | Delete | Start | Stop

Showi

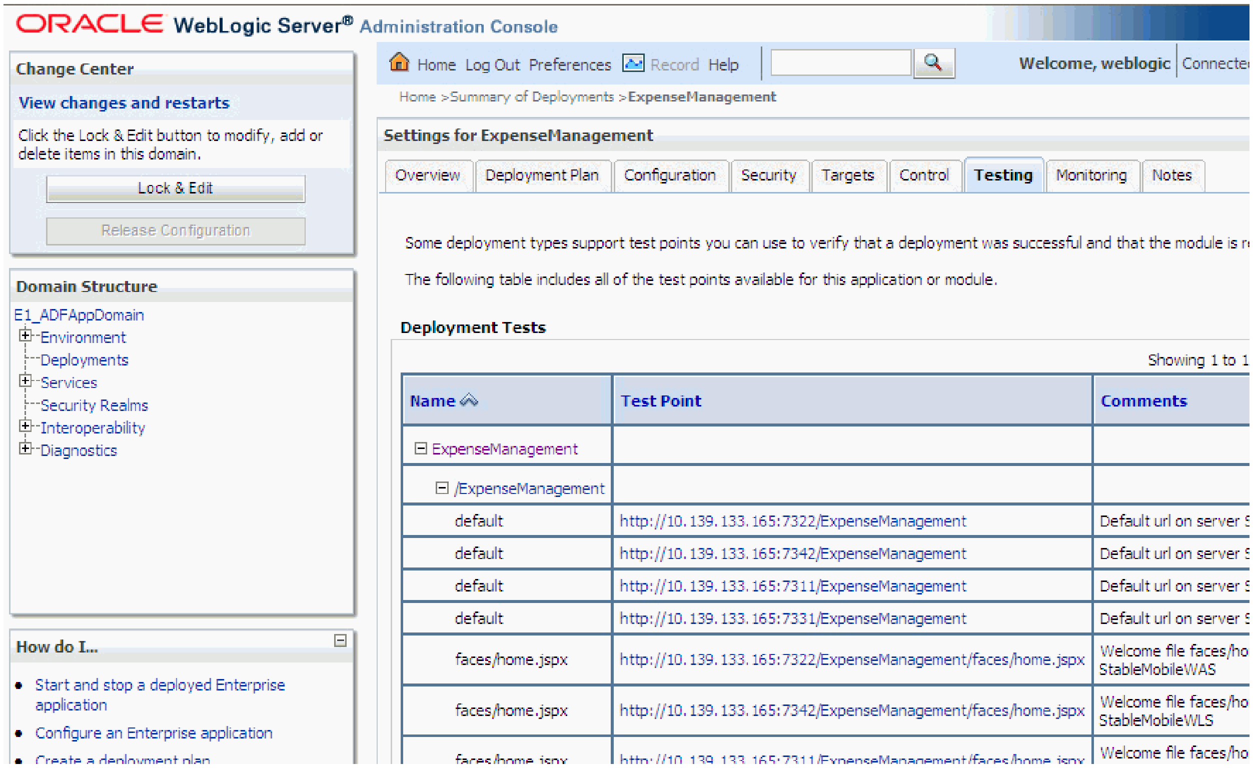
□	Name	State	Health	Type
□	adf.oracle.businesseditor(1.0,11.1.1.2.0)	Active		Library
□	adf.oracle.domain(1.0,11.1.1.2.0)	Active		Library
□	adf.oracle.domain.webapp(1.0,11.1.1.2.0)	Active		Library
□	⊞ DMS Application (11.1.1.1.0)	Active	✓ OK	Web Applica
□	⊞ em	Active	✓ OK	Enterprise Application
□	emai	Active		Library
□	emas	Active		Library
□	emcore	Active		Library
□	⊞ ExpenseManagement	Active	✓ OK	Enterprise Application
□	⊞ FMW Welcome Page Application (11.1.0.0.0)	Active	✓ OK	Enterprise Application
□	JDE.Mobile.Shared.Lib(1.0,1.0)	Active		Library
□	jsf(1.2,1.2.9.0)	Active		Library

3. In the Deployments section on the Control tab, select the mobile application deployment.

   The Settings screen appears.

4. On the Settings screen, select the Testing tab and then select the plus symbol next to the application name to expand it.

   The system displays two URL entries for each instance of a deployed mobile application, as shown here:



Click the Lock & Edit button to modify, add or delete items in this domain.

Some deployment types support test points you can use to verify that a deployment was successful and that the module is r

The following table includes all of the test points available for this application or module.

Name	Test Point	Comments
⊟ ExpenseManagement		
⊟ /ExpenseManagement		
default	http://10.139.133.165:7322/ExpenseManagement	Default url on server S
default	http://10.139.133.165:7342/ExpenseManagement	Default url on server S
default	http://10.139.133.165:7311/ExpenseManagement	Default url on server S
default	http://10.139.133.165:7331/ExpenseManagement	Default url on server S
faces/home.jspx	http://10.139.133.165:7322/ExpenseManagement/faces/home.jspx	Welcome file faces/ho StableMobileWAS
faces/home.jspx	http://10.139.133.165:7342/ExpenseManagement/faces/home.jspx	Welcome file faces/ho StableMobileWLS
faces/home.jspx	http://10.139.133.165:7311/ExpenseManagement/faces/home.jspx	Welcome file faces/ho

5. Use the URL that contains `faces/`. This is the URL that the user must use to access the mobile application from a mobile device.

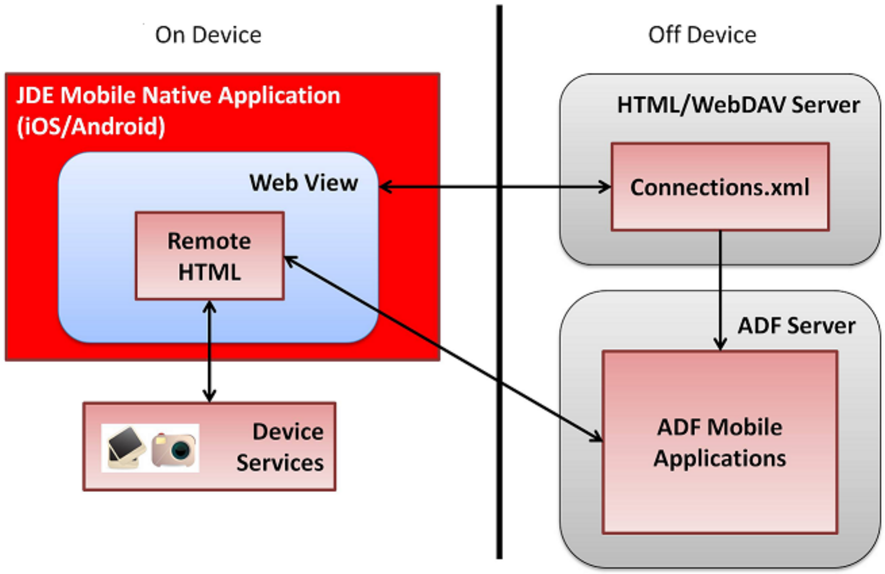
3.3 Hosting a Connection for the Native JD Edwards EnterpriseOne Mobile Applications Application (Mobile Applications Release 9.1.2)

This section describes how to host a connections.xml on a WebDAV server, which is required for mobile users to run the *JD Edwards EnterpriseOne Mobile Applications* application. When mobile users access the 9.1.2 Mobile Expense Management application from the *JD Edwards EnterpriseOne Mobile Applications* application, they can use the mobile device's native camera feature to upload and attach photos to an expense report.

Note: In addition to hosting a connection, to support the attachment of photos in Mobile Expense Management, you must deploy a JAX-WS business services package on the Business Services Server.

After the configuration is complete, mobile applications users must install the *JD Edwards EnterpriseOne Mobile Applications* application from the application store for their mobile device. For more information, see "Understanding Photo Attachments" in the *JD Edwards EnterpriseOne Applications Functionality for Mobile Devices Implementation Guide*.

The following illustration shows a mobile applications environment with the connections.xml on a WebDAV server:



SSL Support

SSL is supported for both the WebDAV server and the ADF Server. If you enable SSL on one server, you do not have to enable SSL on the other server.

On Oracle WebLogic Server, the default (demo) certificate does not work with the native *JD Edwards EnterpriseOne Mobile Applications* application. Therefore, you must enable SSL using a valid purchased SSL certificate from a recognized signing authority.

To host a connection for running the *JD Edwards EnterpriseOne Mobile Applications* application:

1. On an HTTP server, host a directory with the name:

   ```
   com.oracle.JDEdwards.EnterpriseOne.JDEMobile
   ```

2. In the directory, create a connections.xml file using the following code, replacing <adf_server> and <port> in the URL below with the name of your ADF server and port number:

   ```
   <?xml version = '1.0' encoding = 'UTF-8'?>
   <References xmlns="http://xmlns.oracle.com/adf/jndi">
      <Reference name="Menu"
   className="oracle.adf.model.connection.url.HttpURLConnection" xmlns="">
         <Factory
   className="oracle.adf.model.connection.url.URLConnectionFactory"/>
         <RefAddresses>
            <XmlRefAddr addrType="Menu">
               <Contents>
   <urlconnection name="Menu" url="http://<adf_server>:<port>/Menu"/>
               </Contents>
            </XmlRefAddr>
         </RefAddresses>
      </Reference>
   ```

```
</References>
```

The next step describes the credentials, including the URL, that you provide to mobile device users for the connection between the mobile devices and the WebDav server. The URL that you provide is to the parent folder of the directory created in step 1.

3. Direct mobile device users to launch the native *JD Edwards EnterpriseOne Mobile Applications* application on their device. When prompted, a user must complete these fields:

    - **Server**: Enter the following URL:

      http://<*http_server*>:<*port*>/mobile

      Note: Users can also modify the URL in the application settings on their device.

      The server configuration can also support SSL.

    - **Username**: Provide the mobile user with the username for accessing the WebDav server.

    - **Password**: Provide the mobile user with the password for accessing the WebDAV server.

This completes the installation and configuration of the EnterpriseOne mobile applications environment. See the *JD Edwards EnterpriseOne Applications Functionality for Mobile Devices Implementation Guide* for additional implementation instructions, including how to:

- Set up mobile applications.
- Set up security for business services used by mobile applications.

Also, document 1387796.1 in My Oracle Support lists and provides links to documentation related to EnterpriseOne mobile applications. Use the following URL to access and sign into My Oracle Support:

https://support.oracle.com

4 Troubleshooting

This chapter contains the following topics:

- Section 4.1, "Login Issues"
- Section 4.2, "Mobile Applications Issues"

4.1 Login Issues

Login fails on all mobile applications

The ADF server logs (.log and .out) show that the mobile attempts to call the AuthenticationManager business service, but fails and shows this exception: `java.io.IOException: Connection closed, EOF detected`

To resolve this issue, add these server start arguments:

```
-DUseSunHttpHandler=true-Dssl.SocketFactory.provider=sun.security.ssl.SSLSocketFac
toryImpl -Dssl.ServerSocketFactory.provider=sun.security.ssl.SSLSocketFactoryImpl
```

Login screen does not display

If more than one EnterpriseOne mobile application is deployed, single sign-on functionality is employed so that the user only has to sign in once. After a user signs in to the first mobile application, any subsequent mobile applications launched by the user automatically use the credentials from the original sign-in.

Login fails on WebLogic Server

If the login fails on the WebLogic Server, check the configuration by performing the following tasks:

- Verify that the JDEADFMobileLoginModule.jar is loaded:
  1. Open the WebLogic server .out log file and look for this message - "JDE ADFMobileLoginModule is loaded." The .out log file is typically under *weblogicserver*/servers/*server*/logs on production WLS.
  2. If "JDEADFMobileLoginModule is loaded" message is not shown:

     Using the WebLogic Server Administration Console, verify whether JDEADFMobileAuthenticationProvider is configured in the WebLogic Server realm.

     Verify JDEADFMobileLoginModule.jar is in the classpath.

     Make sure that the WebLogic Administration server and all servers have been restarted.

3. If the "JDEADFMobileLoginModule is loaded" message appears in the .out log file:

   Make sure that the Business Services Server is running properly.

   Check -DBSSVSERVER_URL and -DBSSVSERVER_TYPE JVM settings.

   Check the Business Services Server log files.

- Ensure that the published business services for the mobile applications are properly secured. Users must have authorized access to published business services used by mobile applications.

  See "Securing Mobile Applications" in the *JD Edwards EnterpriseOne Applications Functionality for Mobile Devices Implementation Guide* for more information about securing mobile application published business services.

- If the WebLogic Server extended for ADF runtime (the ADF Server) is configured to accept certificates from a Business Services Server that is installed on WebLogic Server 12c on a different machine, check for the following exception in the ADF Server logs:

  ```
  Calling BSSV to authenticate user on server =
  https://machine:portnumber/pathcode/AuthenticationManager failed.
  javax.xml.ws.WebServiceException: javax.net.ssl.SSLKeyException: FATAL
  Alert:BAD_CERTIFICATE - A corrupt or unuseable certificate was
  received.
  ```

  To fix this issue, on the ADF Server, you must check the "Use JSSE SSL" box in the Advanced tab and restart the ADF Server. See step 5 in the Configuring and Deploying the JDEADFMobileLoginModule.jar section in this guide.

Login fails on integrated WebLogic Server in JDeveloper 11g

Verify whether "JDEADFMobileLoginModule is loaded" message appears in the Integrated WLS console window.

If the "JDEADFMobileLoginModule is loaded" message is not shown, then check following:

- Verify whether JDEADFMobileAuthenticationProvider is configured in Integrated WLS realm using WLS console
- Verify JDEADFMobileLoginModule.jar is set in startWebLogic.cmd
- Make sure integrated WLS server is restarted

If the "JDEADFMobileLoginModule is loaded" message is displayed, check the following:

- Make sure that the Business Services Server is running properly.
- Check -DBSSVSERVER_URL and -DBSSVSERVER_TYPE JVM settings in startWebLogic.cmd.
- Check the Business Services Server log files.

Login succeeds, but the application home page is not shown

Make sure the URL entered is the URL to the home page, not the login page, as in the following example:

```
http://server:port/ExpenseManagement-ViewController-context-root/faces/hom
e.jspx
```

4.2 Mobile Applications Issues

Calling business service fails from WebLogic Server - "Security token failed to validate"

The following errors might appear when the calling business service fails from the WebLogic Server:

```
Security token failed to validate.
weblogic.xml.crypto.wss.SecurityTokenValidateResult@8e7d9fb[status: false][msg UNT
Error:Message Created time past the current time even accounting for set clock
skew.

Security token failed to validate.
weblogic.xml.crypto.wss.SecurityTokenValidateResult@9bd3ce8[status: false][msg UNT
Error:Message older than allowed
```

To resolve this issue:

1. In the WebLogic Server Administration Console, click Environment/Servers.
2. Click the server on which the mobile application has been deployed.
3. Click the Server Start tab.
4. Click the Lock & Edit button.
5. In the Arguments text box, append the following text:
   `-Dweblogic.wsee.security.clock.skew=7200000`
   `-Dweblogic.wsee.security.delay.max=7200000`.
6. Click Save.
7. Click Activate Changes.
8. Restart the managed server.

Calling business service fails from WebLogic Server - "Hostname Verification Exception"

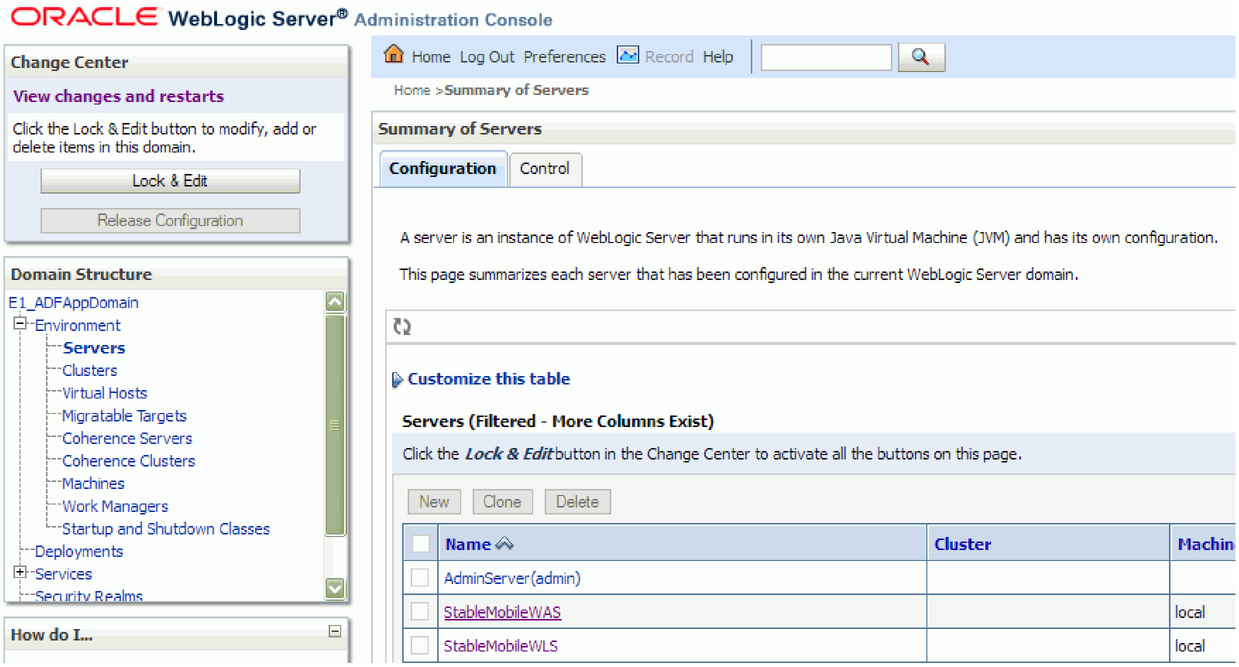
When the application fails to call a business service, check the log file for the following error:

- HOSTNAME VERIFICATION EXCEPTION

  ```
  [Security:090504]Certificate chain received from
  host3933-domain.name.com - 10.111.222.166 failed hostname verification
  check. Certificate contained host3933 but check expected
  host3933-domain.name.com
  ```

To resolve this issue:

1. Log in to WebLogic Server Administration Console.



ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Home >Summary of Servers

Change Center

View changes and restarts

Click the Lock & Edit button to modify, add or delete items in this domain.

Lock & Edit

Release Configuration

Domain Structure

E1_ADFAppDomain
- Environment
  - **Servers**
  - Clusters
  - Virtual Hosts
  - Migratable Targets
  - Coherence Servers
  - Coherence Clusters
  - Machines
  - Work Managers
  - Startup and Shutdown Classes
- Deployments
- Services
- Security Realms

How do I...

Summary of Servers

Configuration | Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.

This page summarizes each server that has been configured in the current WebLogic Server domain.

Customize this table

Servers (Filtered - More Columns Exist)

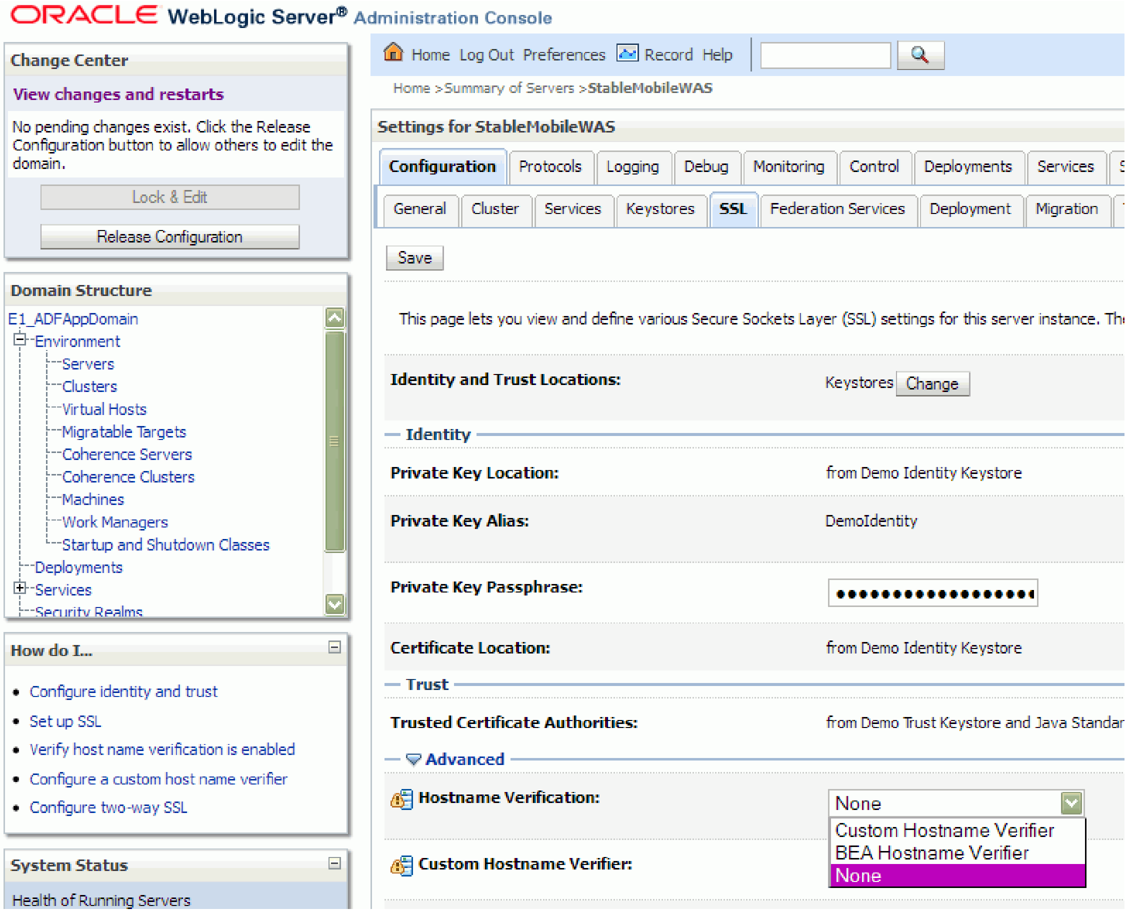
Click the ***Lock & Edit*** button in the Change Center to activate all the buttons on this page.

New | Clone | Delete

□	Name	Cluster	Machin
□	AdminServer(admin)		
□	StableMobileWAS		local
□	StableMobileWLS		local

2. Click Servers in the Environment node, and then select the specific WebLogic managed server for which you want to configure the hostname verification.

3. Click the Lock and Edit button to allow changes.



ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help

Home >Summary of Servers >StableMobileWAS

Change Center

View changes and restarts

No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Lock & Edit

Release Configuration

Domain Structure

E1_ADFAppDomain
- Environment
  - Servers
  - Clusters
  - Virtual Hosts
  - Migratable Targets
  - Coherence Servers
  - Coherence Clusters
  - Machines
  - Work Managers
  - Startup and Shutdown Classes
- Deployments
- Services
- Security Realms

How do I...

- Configure identity and trust
- Set up SSL
- Verify host name verification is enabled
- Configure a custom host name verifier
- Configure two-way SSL

System Status

Health of Running Servers

Settings for StableMobileWAS

Configuration | Protocols | Logging | Debug | Monitoring | Control | Deployments | Services

General | Cluster | Services | Keystores | SSL | Federation Services | Deployment | Migration

Save

This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. Th

Identity and Trust Locations: Keystores Change

Identity

Private Key Location: from Demo Identity Keystore

Private Key Alias: DemoIdentity

Private Key Passphrase: ••••••••••••••••••

Certificate Location: from Demo Identity Keystore

Trust

Trusted Certificate Authorities: from Demo Trust Keystore and Java Standar

Advanced

Hostname Verification: None

Custom Hostname Verifier
BEA Hostname Verifier
None

Custom Hostname Verifier:

4. Click the SSL tab, and then open the Advanced area.
5. In the Hostname Verification drop-down menu, select None.
6. Save the changes and restart the specific WebLogic managed server.

Calling business service fails from WebLogic Server - "Clock Skew or Delay Exception"

When the application fails to call a business service, check the log file for the following errors:

- CLOCK SKEW OR DELAY EXCEPTION

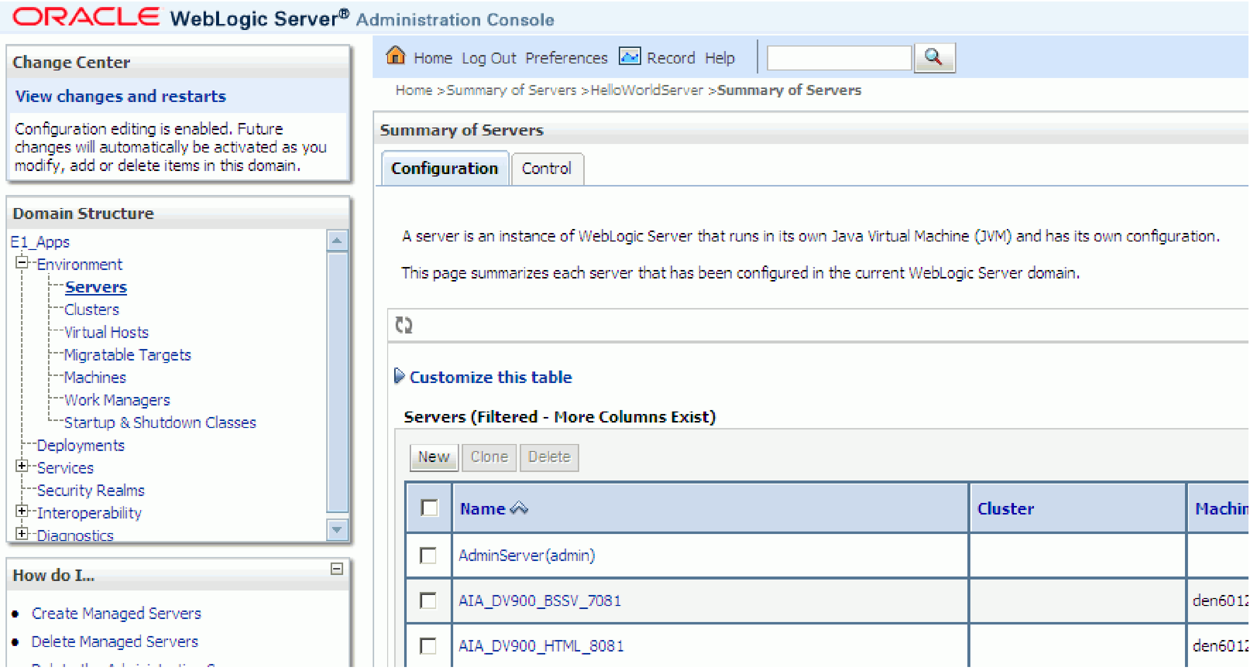
```
FaultString [Message Created time past the current time even accounting
for set clock skew] FaultActor [null]No Detail; nested exception is:
javax.xml.rpc.soap.SOAPFaultException: Message Created time past the
current time even accounting for set clock skew
```

or

```
FaultString [Security token failed to validate.
weblogic.xml.crypto.wss.SecurityTokenValidateResult@9bd3ce8[status:
false][msg UNT Error:Message older than allowed MessageAge]] FaultActor
[null]No Detail; nested exception is:
weblogic.wsee.jaxrpc.soapfault.WLSOAPFaultException: Security token
failed to validate.
```

To resolve this issue:

1. Log into the WebLogic Server Administration Console.



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

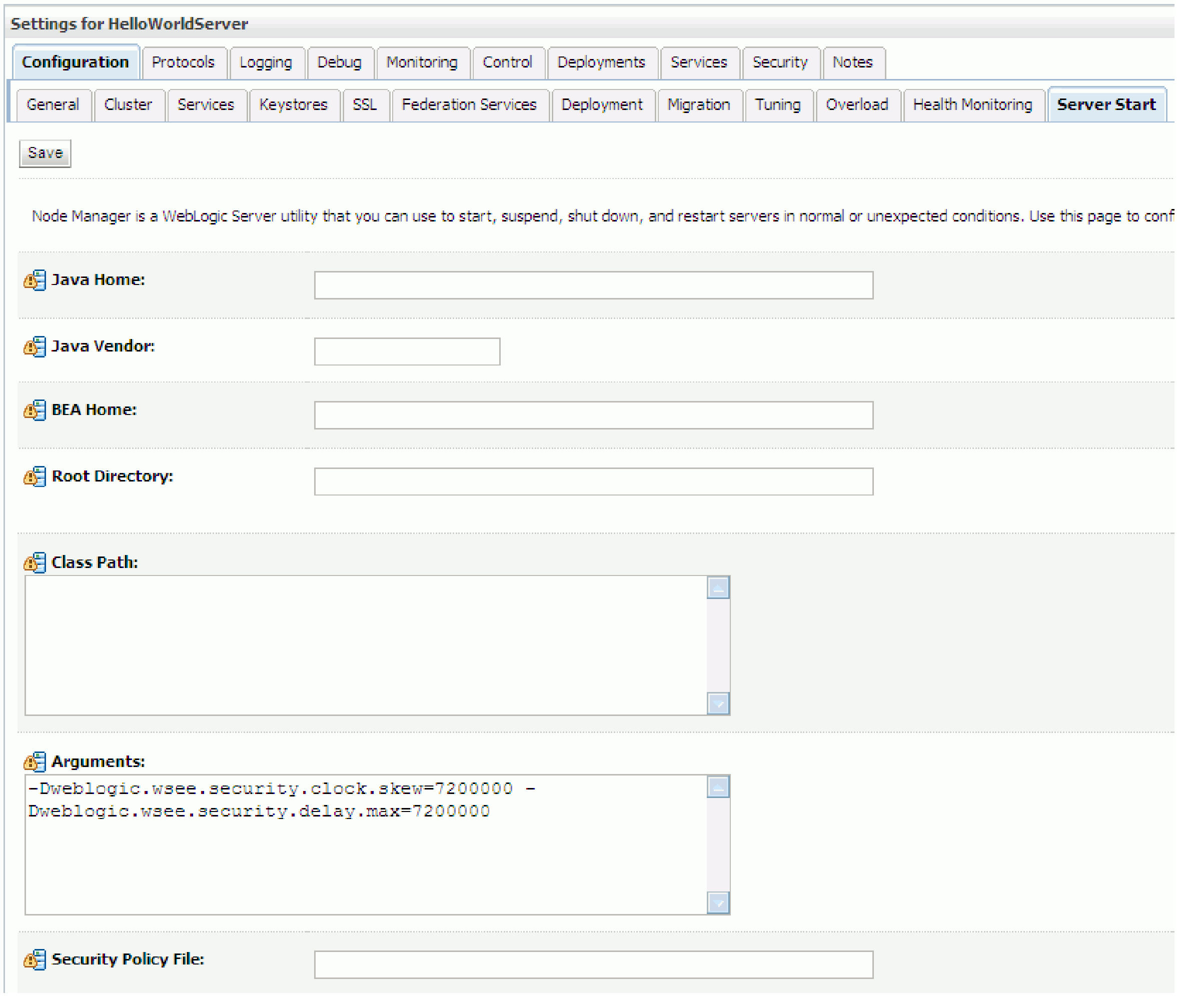
A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.

This page summarizes each server that has been configured in the current WebLogic Server domain.

Servers (Filtered - More Columns Exist)

□	Name	Cluster	Machin
□	AdminServer(admin)		
□	AIA_DV900_BSSV_7081		den601:
□	AIA_DV900_HTML_8081		den601:

2. Click Servers in the Environment node, and then select the specific WebLogic managed server for which you want to set system level properties.



Settings for HelloWorldServer

Node Manager is a WebLogic Server utility that you can use to start, suspend, shut down, and restart servers in normal or unexpected conditions. Use this page to conf

Java Home:

Java Vendor:

BEA Home:

Root Directory:

Class Path:

Arguments:

```
-Dweblogic.wsee.security.clock.skew=7200000 -
Dweblogic.wsee.security.delay.max=7200000
```

Security Policy File:

3. On the Configuration tab, click the Server Start tab.
4. In the Arguments field on the Server Start tab, enter the properties for the clock skew and delay. Separate the two properties with a space, for example:

   ```
   -Dweblogic.wsee.security.clock.skew=72000000
   -Dweblogic.wsee.security.delay.max=72000000
   ```

5. Save the changes and restart the specific WebLogic managed server.

Viewing photos in Expense Management shows X11 error

When attempting to view photo attachments in the Expense Management mobile application, an error message displays with one of these two possible errors:

```
sun/awt/X11GraphicsEnvironment
```

or

```
Can't connect to X11 window server using 'localhost:10.0' as the value of
the DISPLAY variable.
```

Cause: If the machine where the Business Services Server is running does not have a monitor or proper setting for the DISPLAY variable, the graphics environment (awt) needed to process photo attachments is not loaded and one of the X11 related exceptions is thrown.

To resolve this issue on the Business Services Server on WebLogic Server:

1. In the WebLogic Server Administration Console of the Business Services Server, click Environment/Servers.
2. Click the server on which the business services are deployed.
3. Click the Server Start tab.
4. Click the Lock & Edit button.
5. In the Arguments text box, append the following text:

   ```
   -Djava.awt.headless=true
   ```

6. Click Save.
7. Click Activate Changes.
8. Restart the managed server.

To resolve this issue on the Business Services Server on IBM WebSphere Application Server:

1. If it is not already running, start the WebSphere Application Server service.
2. Browse to the WebSphere Application Server Administrative Console.
3. Authenticate with the server as the admin resource.
4. After authentication, click Servers, Application Servers, and then the name of your Business Service Server.
5. Locate the Server Infrastructure section of your Business Services Server configuration page, expand Java and Process Management, and click Process Definition.
6. On the Process Definition page, go to the Additional Properties section and click Java Virtual Machine.
7. In the Generic JVM arguments section on the Java Virtual Machine page, append the following JVM arguments. Be sure to add the JVM arguments on one line:

   ```
   -Djava.awt.headless=true
   ```

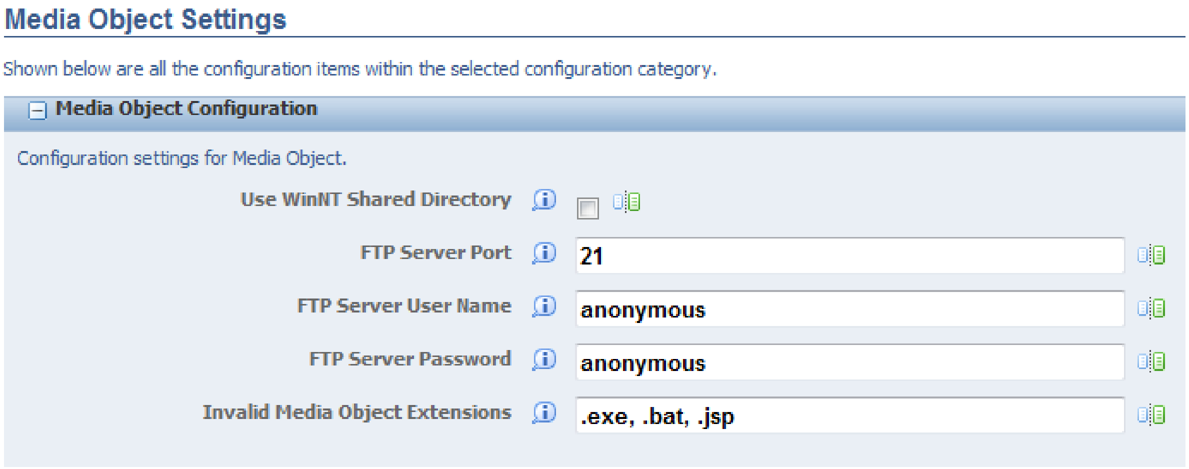
8. Shut down and restart the WebSphere Application Server.

Users cannot view attached images uploaded in Mobile Expense Management

If users cannot view images in the EnterpriseOne web client that were uploaded from the mobile application, then the media object settings for the Business Services Server are not configured correctly. Typically, this issue occurs if you are using an FTP server for the media object file transfer.

To fix this issue:

1. In Server Manager, access the Media Object Settings for the Business Services Server.



Media Object Settings

Shown below are all the configuration items within the selected configuration category.

Media Object Configuration

Configuration settings for Media Object.

Use WinNT Shared Directory ☐

FTP Server Port: 21

FTP Server User Name: anonymous

FTP Server Password: anonymous

Invalid Media Object Extensions: .exe, .bat, .jsp

2. If using an FTP server for the media object server, clear the Use WinNT Shared Directory setting.

   See "Configuring the Business Services Server for Media Object Operations" in the *JD Edwards EnterpriseOne Tools Business Services Server Reference Guide* for more information about these settings.

Mobile Menu application error

If users receive an error when using the Mobile Menu, then one or both of the following issues might exist:

- The menu cannot be displayed because the java property DEPLOYED_APPS is not configured properly.
- Application configured in java properties is not deployed.

See Configuring and Deploying the JDEADFMobileLoginModule.jar in this guide for instructions on how to set the parameter for DEPLOYED_APPS.

Blank screen appears in the mobile application after accessing a feature from the spring board (Release 9.1 Update 4)

Note: This issue can occur when all of the following criteria is met:

- The Business Services Server is on Oracle WebLogic Server 12.1.2, which is supported beginning with EnterpriseOne Tools release 9.1 Update 4.
- A JAX-RPC business services package is deployed on the Business Services Server.
- The Mobile Applications Server (ADF Server) is on Oracle WebLogic Server 10.3.5.

If a blank screen appears, look in the WebLogic Server Container logs on the Mobile Applications Server (ADF Server):

```
java.rmi.RemoteException: SOAPFaultException - FaultCode
[{http://schemas.xmlsoap.org/soap/envelope/}Server] FaultString [] FaultActor
[null] Detail [<detail><java:string
xmlns:java="java.io">java.lang.NullPointerException
</java:string></detail>]; nested exception is:
```

```
weblogic.wsee.jaxrpc.soapfault.WLSOAPFaultException:
at foundation.Oracle_E1_SBF_JWS_PkgBldFile_FoundationEnvironmentManager_
Stub.getUserProfile(Unknown Source)
at foundation.Oracle_E1_SBF_JWS_PkgBldFile_
FoundationEnvironmentManagerPortClient.getUserProfile(Unknown Source)
```

Also, look in the Container logs on the Business Services Server for the following exception:

```
java.lang.NullPointerException
at weblogic.servlet.internal.PostInputStream.complain(PostInputStream.java:83)
at weblogic.servlet.internal.PostInputStream.read(PostInputStream.java:188)
at
weblogic.servlet.internal.ServletInputStreamImpl.read(ServletInputStreamImpl.java:
236)
at weblogic.xml.babel.reader.XmlReader$Utf8Reader.read(XmlReader.java:660)
at weblogic.xml.babel.scanner.ScannerState.read(ScannerState.java:404)
at weblogic.xml.babel.scanner.ScannerState.checkedRead(ScannerState.java:631)
at weblogic.xml.babel.scanner.CharData.read(CharData.java:55)
at
weblogic.xml.babel.scanner.AttributeValue.readDoubleQuote(AttributeValue.java:55)
at weblogic.xml.babel.scanner.AttributeValue.read(AttributeValue.java:78)
at weblogic.xml.babel.scanner.OpenTag.read(OpenTag.java:64)
at weblogic.xml.babel.scanner.Scanner.startState(Scanner.java:250)
at weblogic.xml.babel.scanner.Scanner.scan(Scanner.java:177)
.... MORE STACKTRACE...
```

To resolve this issue:

1. In the WebLogic Server Administration Console, click Environments/Servers.
2. Click the server on which the mobile application has been deployed.
3. Click the Server Start tab.
4. Click the Lock & Edit button.
5. In the Arguments text box, append the following text:

   ```
   -Dweblogic.wsee.workarea.skipWorkAreaHeader=true
   ```

6. Click Save.
7. Click Activate Changes.
8. Restart the managed server.