

JD Edwards World

Service Enablement Installation and Configuration Guide for
A9.3

Release A9.3

E21965-04

March 2018

E21965-04

Copyright © 2013, 2018, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	v
Audience.....	v
Documentation Accessibility	v
Related Documents	v
Conventions	v
 1 Install Service Enablement	
1.1 Overview	1-1
1.2 Installing Service Enablement.....	1-1
 2 WebLogic Application Server	
2.1 Web Services Overview	2-1
2.2 WebLogic Application Server	2-1
2.2.1 Before You Begin.....	2-1
2.2.2 Configuring the WebLogic Application Server.....	2-1
 3 WebSphere Application Server	
3.1 Installing the WebSphere Application Server	3-1
 A Install WebLogic Application Server	
A.1 Installing WebLogic Application Server	A-1
 B Create WebSphere Application Server	
B.1 Creating Application Servers in WebSphere	B-1
 C Code and Deploy your own Web Services	
C.1 Coding and Deploying Your Own Web Services.....	C-1
 D Add Web Services to Oracle Enterprise Repository	
D.1 Web Services Deployment and Java Documents Location Update.....	D-1
D.2 CAR XML Documents Builder.....	D-3

E Uninstall Service Enablement

E.1	Uninstalling Service Enablement.....	E-1
E.1.1	Oracle Universal Installer (OUI).....	E-1

Preface

Welcome to the JD Edwards World Service Enablement Installation and Configuration Guide.

Audience

This guide is intended for implementers and end users of JD Edwards World Service Enablement Installation and Configuration.

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

You can access related documents from the JD Edwards World Release Documentation Overview pages on My Oracle Support. Access the main documentation overview page by searching for the document ID, which is 1362397.1, or by using this link:

- <https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1362397.1>

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Install Service Enablement

This chapter contains these topics:

- [Section 1.1, "Overview,"](#)
- [Section 1.2, "Installing Service Enablement."](#)

1.1 Overview

Thank you for ordering JD Edwards World A9.2.1 Service Enablement. This Java-based service enablement product is a statement of Oracle's continued commitment to the JD Edwards World product family. Service Enablement allows you to integrate your JD Edwards World Software with other software packages through the use of Java-based Web services.

This guide explains installation and configuration options and steps for JD Edwards World Service Enablement. The *JD Edwards World Web Enablement Installation and Configuration Guide* has general information about JD Edwards World Service Enablement.

Note: In this guide, the name System i includes IBM servers named AS/400, eServer iSeries, System i5, System i or Power Servers running the IBM i for Business operating system.

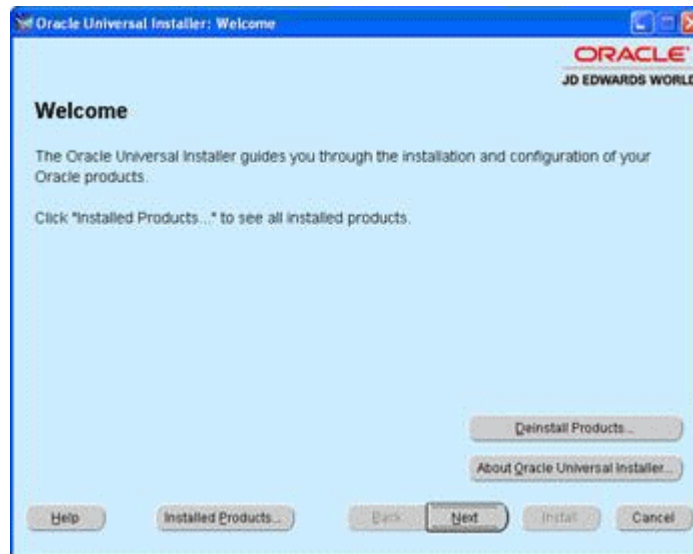
1.2 Installing Service Enablement

To install Service Enablement

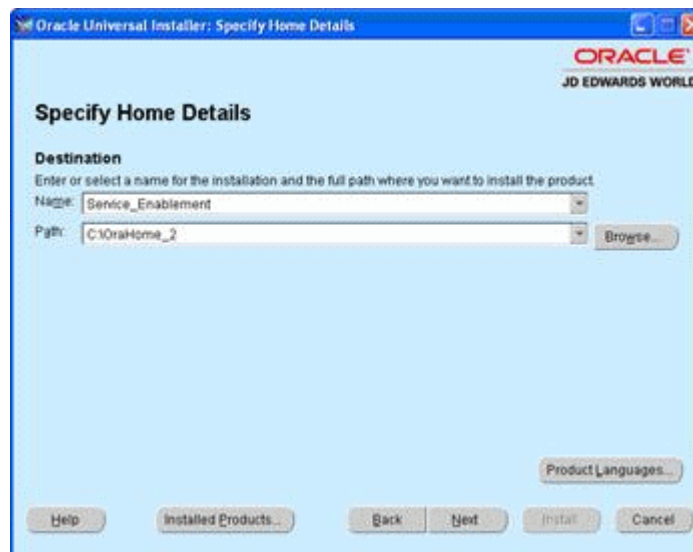
1. Download and unzip the service enablement archive file.

Start the Oracle Universal Installer (OUI).

Run Disk1\oui\bin\setup.exe from your extract to location.

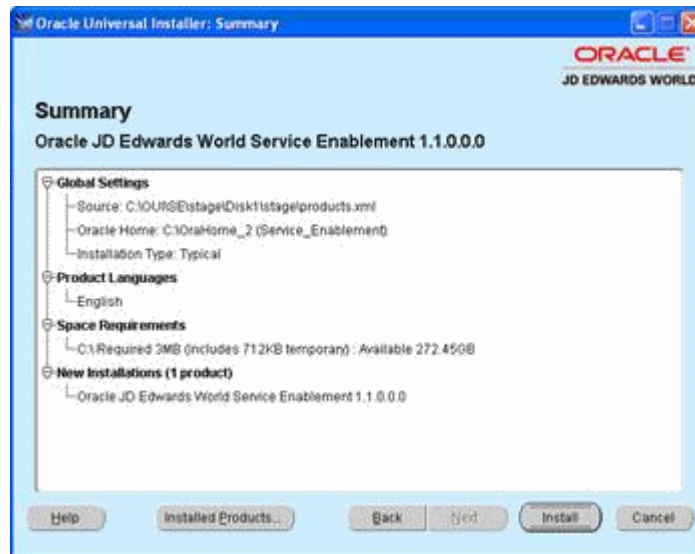
Figure 1–1 Oracle Universal Installer Welcome screen

2. On the Welcome screen, click Next.

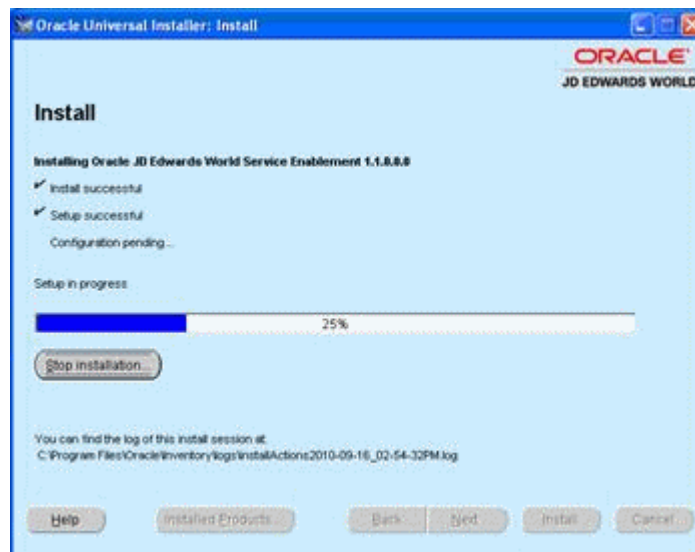
Figure 1–2 OUI Specify Home Details screen

3. On the Specify Home Details screen, enter a folder Name and Path for your installation. JD Edwards World recommends that you retain the OraHome name in some form for your path directory.

Using the OraHome name is an Oracle convention that facilitates consistent directory names among Oracle product installations.

Figure 1–3 OUI Summary screen

4. On the Summary screen, click Install.

Figure 1–4 OUI Install screen

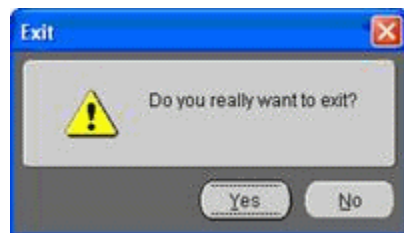
The Install screen displays the Setup in progress.

Figure 1–5 OUI End of Installation screen



5. On the End of Installation screen, click Exit.

Figure 1–6 Exit window



6. On the Exit screen, click Yes.

WebLogic Application Server

This chapter contains these topics:

- [Section 2.1, "Web Services Overview,"](#)
- [Section 2.2, "WebLogic Application Server."](#)

2.1 Web Services Overview

You must deploy the World Web Service EAR file to an Oracle WebLogic or IBM WebSphere application server. For more information about release requirements, see the *JD Edwards World Minimum Technical Requirements Guide* and A9.2.1. All necessary Java security setup occurs after deployment. This guide contains specific deployment and security setup instructions for both application servers. Make sure you have installed and configured the application server before deploying the EAR file.

2.2 WebLogic Application Server

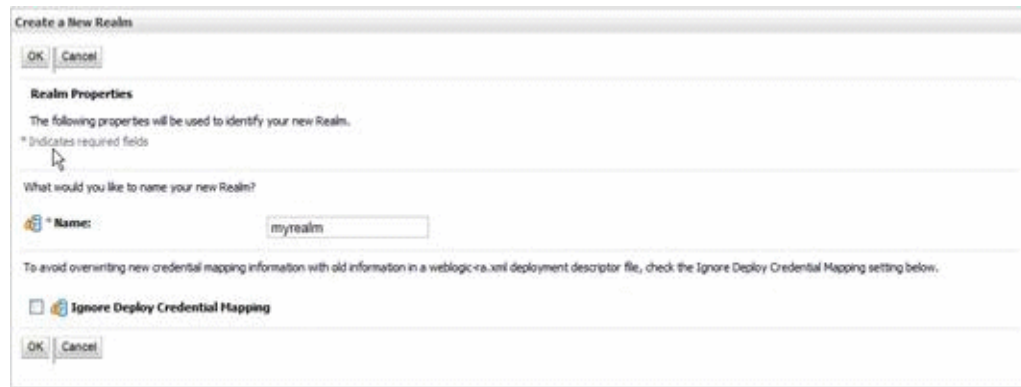
2.2.1 Before You Begin

You need to configure an appropriate WebLogic Application Server using the procedure in [Appendix A, "Install WebLogic Application Server"](#) in this guide.

2.2.2 Configuring the WebLogic Application Server

To configure the WebLogic Application Server

1. Start the WebLogic Admin Server:
`%SystemRoot%\system32\cmd.exe /k"C:\Oracle\Middleware\user_projects\domains\base_domain\bin\startWebLogic.cmd"`
2. Launch the application server console:
`http://localhost:7001/console`
3. From WebLogic console select Security Realms to create a Security Realm.
Click New.

Figure 2–1 Create a New Realm screen


Create a New Realm


OK Cancel

Realm Properties

The following properties will be used to identify your new Realm.

* Indicates required fields

What would you like to name your new Realm?

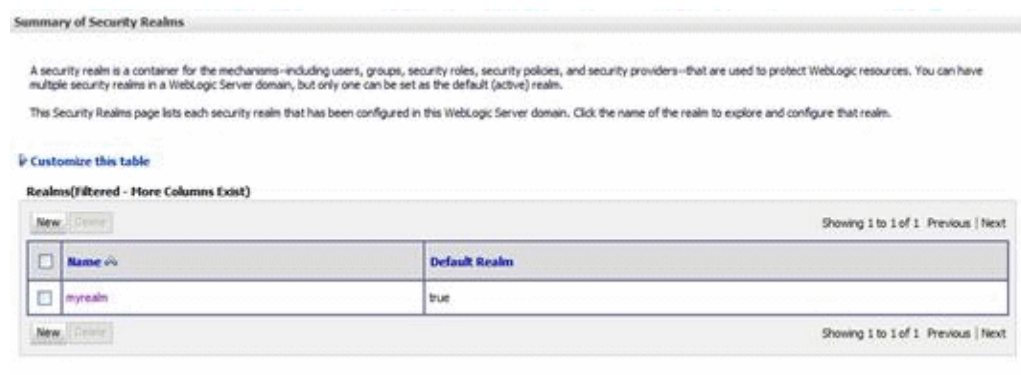
 **Name:**

To avoid overwriting new credential mapping information with old information in a weblogic-ra.xml deployment descriptor file, check the Ignore Deploy Credential Mapping setting below.

☐ **Ignore Deploy Credential Mapping**

OK Cancel

4. Enter a Realm Name and then click OK.

Figure 2–2 Summary of Security Realms screen


Summary of Security Realms

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

[Customize this table](#)

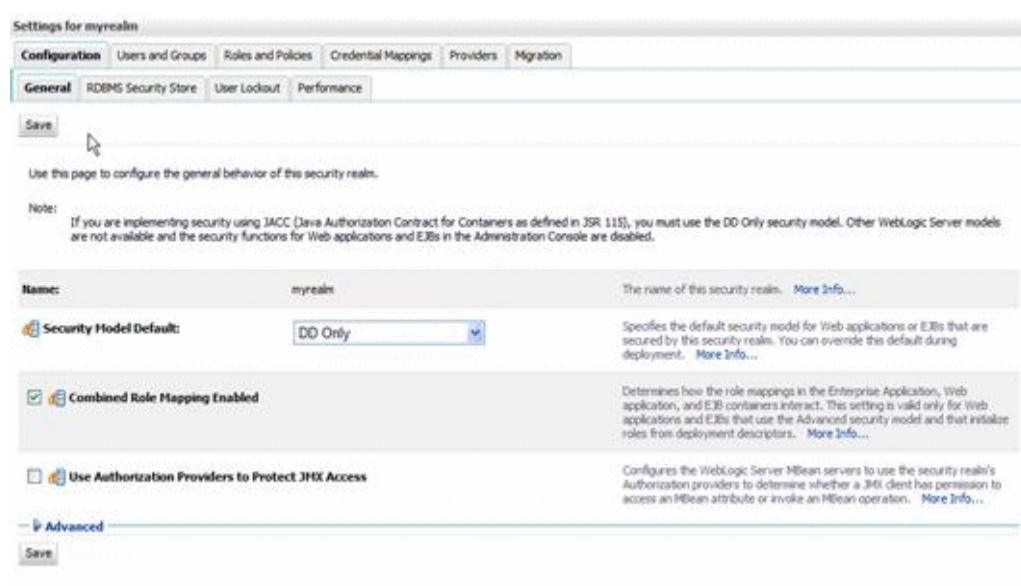
Realms (Filtered - More Columns Exist)

New Delete Showing 1 to 1 of 1 Previous Next

<input type="checkbox"/>	Name	Default Realm
<input type="checkbox"/>	myrealm	true

New Delete Showing 1 to 1 of 1 Previous Next

5. Click New to create a realm.

Figure 2–3 Settings for MyRealms (General Tab) screen


Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings Providers Migration


General RDBMS Security Store User Logout Performance

Save

Use this page to configure the general behavior of this security realm.

Note:
If you are implementing security using JAAS (Java Authorization Contract for Containers as defined in JSR 115), you must use the DO Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

Name: myrealm The name of this security realm. [More Info...](#)

 **Security Model Default:** Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. [More Info...](#)

☒ **Combined Role Mapping Enabled** Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. [More Info...](#)

☐ **Use Authorization Providers to Protect JMX Access** Configures the WebLogic Server MBean servers to use the security realm's Authorization providers to determine whether a JMX client has permission to access an MBean attribute or invoke an MBean operation. [More Info...](#)

[Advanced](#)

Save

6. Select the Providers tab and then click New.

Figure 2–4 Create a New Authentication Provider screen

7. Enter the Name and select the Type WorldAuthenticator from the dropdown list.
Click OK.

The WorldAuthenticator displays as one of the Authentication Providers.

Figure 2–5 Settings for MyRealm (Authentication Tab) screen

Name	Description	Version
DefaultAuthenticator	WebLogic Authentication Provider	1.0
DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
WorldAuthenticator	World Authentication Provider	1.0

Make sure the WLS DefaultAuthenticator is before the WorldAuthenticator.

8. Click the WorldAuthenticator link.

Figure 2–6 Settings for WorldAuthenticator (Common Tab) screen

Home Log Out Preferences Record Help Welcome, weblogic Connected to: base_domain

Home > Summary of Deployments > BankAccountImpl_v4Service > Summary of Deployments > AccountValidationImpl_v4Service > Summary of Security
 RASite > myrealm > Providers > WorldAuthenticator > Providers > WorldAuthenticator

Settings for WorldAuthenticator

Configuration

Common Provider Specific

Save

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

Name: WorldAuthenticator

Description: World Authentication Provider

Version: 1.0

Control Flag: REQUIRED

Save

9. Set the Control Flag to REQUIRED and then click Save.

Figure 2–7 Settings for Default Authenticator (Common Tab) screen

Settings for DefaultAuthenticator

Configuration Performance Migration

Common Provider Specific

Save

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

Name: DefaultAuthenticator The name of this WebLogic Authentication provider. [More Info...](#)

Description: WebLogic Authentication Provider A short description of the Authentication provider. [More Info...](#)

Version: 1.0 The version number of the Authentication provider. [More Info...](#)

Control Flag: SUFFICIENT Returns how the login sequence uses the Authentication provider. [More Info...](#)

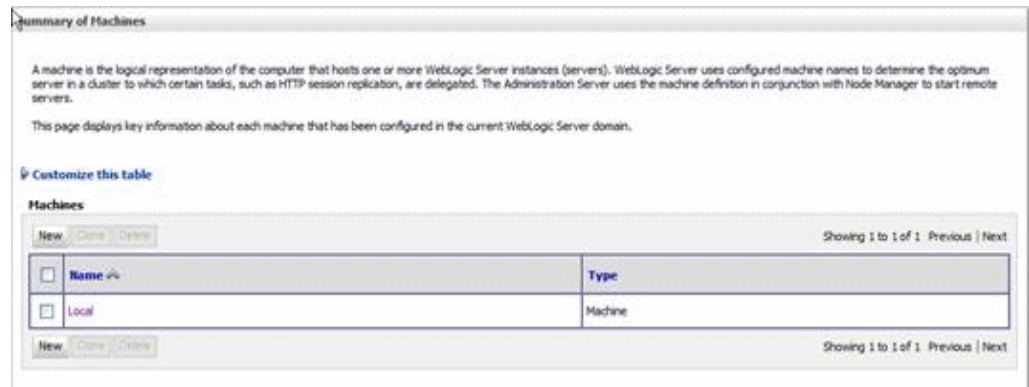
Save

10. Select the DefaultAuthenticator link and Change the Control Flag of the DefaultAuthenticator to SUFFICIENT.

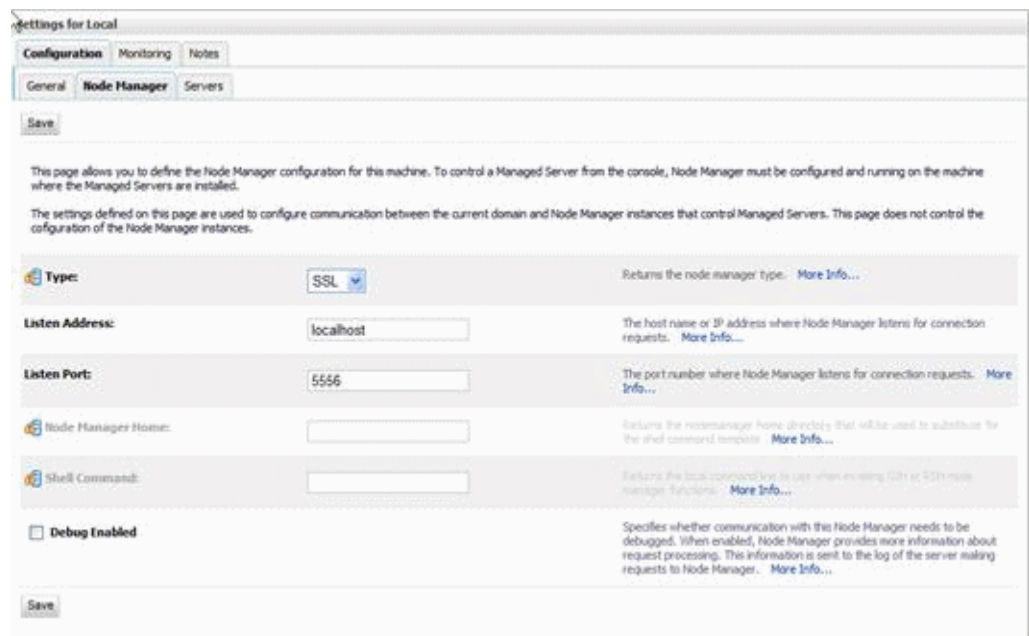
Click Save.

11. Create a machine. Use the default values.

http://localhost:7001/consolehelp/console-help.portal?_nfpb=true&_pageLabel=page&helpId=machines.ConfigureMachines

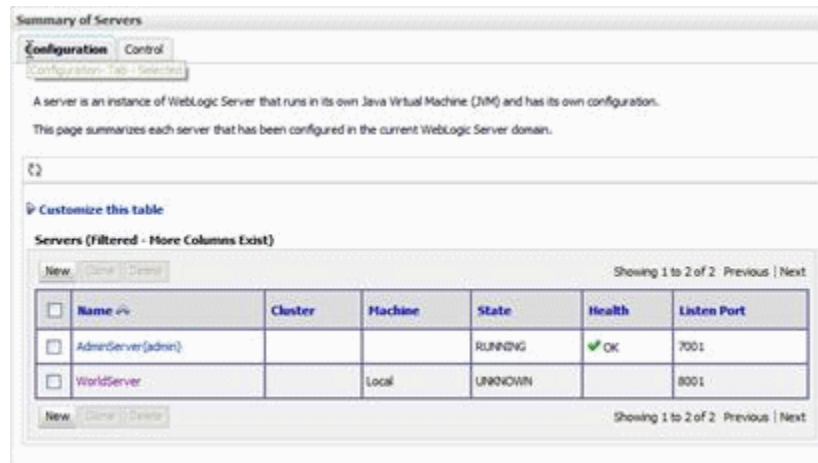
Figure 2–8 Summary of Machines screen

12. Select Local Machine.

Figure 2–9 Settings for Local (Mode Manager Tab) screen

13. Create a managed server for the Web Services.

`http://localhost:7001/consolehelp/console-help.portal?_nfpb=true&_pageLabel=page&helpId=domainconfig.CreateManagedServers`

Figure 2–10 Summary of Servers (Configuration Tab) screen

14. Select WorldServer.

Set Machine to machine configured in step 12.

Figure 2–11 Configuration (General tab) screen

Use this page to configure general features of this server such as default network communications.

Name: WorldServer

Machine: Local

Cluster: (Stand-Alone)

Listen Address:

☒ **Listen Port Enabled**

Listen Port: 8001

☒ **SSL Listen Port Enabled**

SSL Listen Port: 8002

☐ **Client Cert Proxy Enabled**

Java Compiler: javac

Services use the SSL port (https://). Make sure to verify that the SSL Listen Port is Enabled.

If using NodeManager to start and stop the managed server, select the Server Start tab and configure as the following graphic displays:

Figure 2–12 Settings for WorldServer (Configuration Tab) screen

Settings for WorldServer

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

General | Cluster | Services | KeyStores | SSL | Federation Services | Deployment | Migration | Tuning | Overload | Health Monitoring | **Server Start**

Save

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 configure the startup settings that Node Manager will use to start this server on a remote machine.

Java Home: C:\Oracle\Middleware\jdk160_14_R27 6 5-32 The Java home directory (path on the machine running Node Manager) to use when starting this server. [More Info...](#)

Java Vendor: Sun The Java vendor value to use when starting this server. For example, BEA, Sun, HP, etc. [More Info...](#)

BEA Home: C:\Oracle\Middleware\wlserver_10.3 The BEA home directory (path on the machine running Node Manager) to use when starting this server. [More Info...](#)

Root Directory: The directory that this server uses as its root directory. This directory must be on the computer that hosts the Node Manager. If you do not specify a Root Directory value, the domain directory is used by default. [More Info...](#)

Class Path: The classpath (path on the machine running Node Manager) to use when starting this server. [More Info...](#)

```
ins\base_domain\lib\j400.jar;\Oracle\Middleware\user_projects\domains\base_domain\lib\log4j-1.2.14.jar;\Oracle\Middleware\wlserver_10.3\server\lib\weblogic.jar;\Oracle\Middleware\wlserver_10.3\server\lib\weblogic_sp.jar;
```

Arguments: The arguments to use when starting this server. [More Info...](#)

```
-Xms256m -Xmx512m -XX:CompileThreshold=8000 -XX:PermSize=256m -XX:MaxPermSize=128m
```

Security Policy File: The security policy file (directory and filename on the machine running Node Manager) to use when starting this server. [More Info...](#)

User Name: weblogic The user name to use when loading this server. [More Info...](#)

Password: The password of the username used to boot the server and perform server health monitoring. [More Info...](#)

Confirm Password: [More Info...](#)

Save

- Class Path:

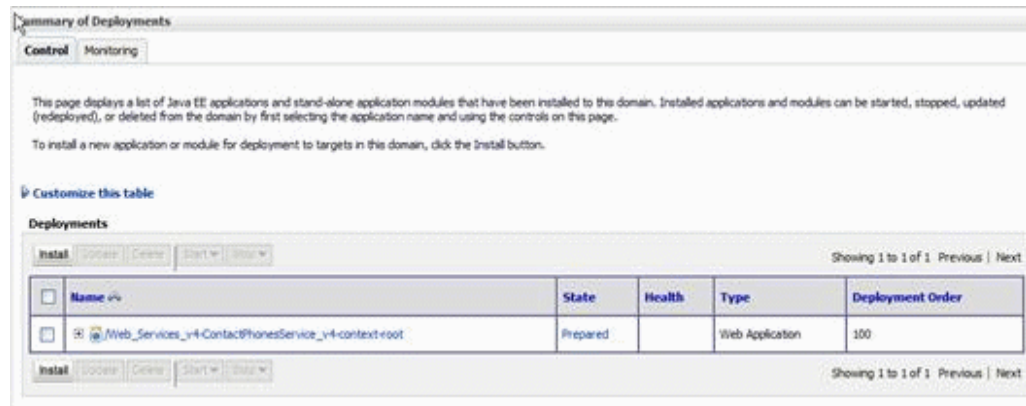
```
\Oracle\Middleware\user_projects\domains\base_
domain\lib\BaseJar.jar;\Oracle\Middleware\user_projects\domains\base_
domain\lib\JDEWorldJDBC.jar;\Oracle\Middleware\user_
projects\domains\base_domain\lib\jt400.jar;\Oracle\Middleware\user_
projects\domains\base_
domain\lib\log4j-1.2.14.jar;\Oracle\Middleware\wlserver_
10.3\server\lib\weblogic.jar;\Oracle\Middleware\wlserver_
10.3\server\lib\weblogic_sp.jar;
```

Note: For details about the latest version supported for log4j, see Doc ID 2318897.1 in My Oracle Support. (WS: Instructions to Address JD Edwards World Security Vulnerabilities (Doc ID 2318897.1)(Release A9.3 Update)

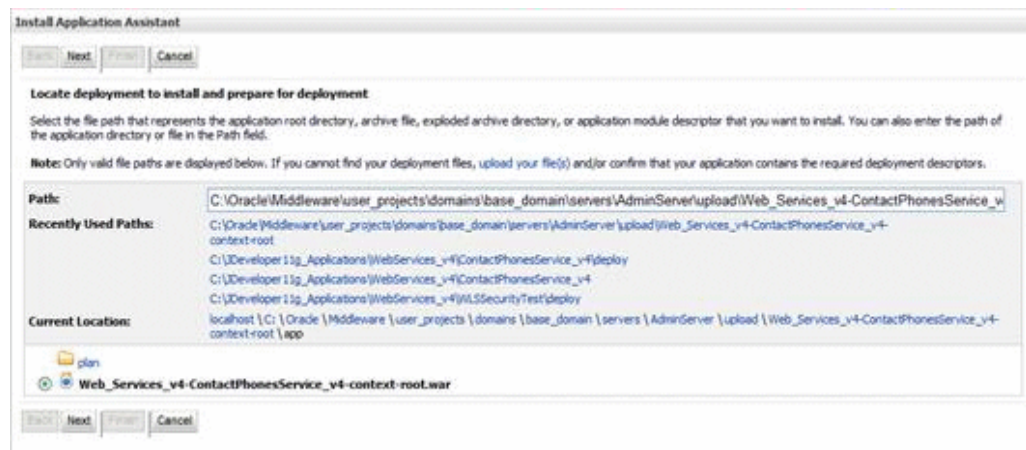
- Arguments:

```
-Xms256m -Xmx512m -XX:CompileThreshold=8000 -XX:PermSize=256m
-XX:MaxPermSize=128m
```

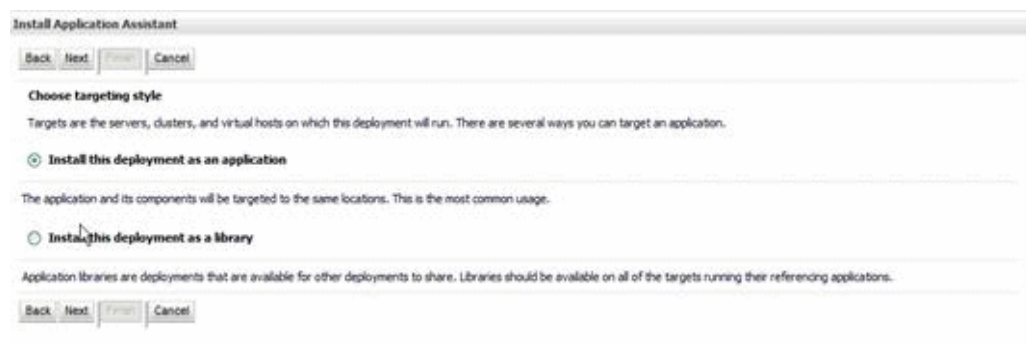
15. Deploy Services to managed server On Server Console, select Deployments.

Figure 2–13 Summary of Deployments (Control Tab) screen

16. Click Install.

Figure 2–14 Install Application Assistant (Locate Deployment Tab) screen

17. Locate service WAR file and then click Next.

Figure 2–15 Install Application Assistant (Choose Targeting Style Tab) screen

18. Select Install this deployment as an application and then click Next.

Figure 2–16 Install Application Assistant (Select Deployment Targets Tab) screen

Install Application Assistant

Back Next Finish Cancel

Select deployment targets

Select the servers and/or clusters to which you want to deploy this application. (You can reconfigure deployment targets later).

Available targets for Web_Services_v4-ContactPhonesService_v4-context-root :

Servers	
<input type="checkbox"/>	AdminServer
<input checked="" type="checkbox"/>	WorldServer

Back Next Finish Cancel

19. Verify the managed server you created earlier, and click Next.

Figure 2–17 Install Application Assistant (Optional Settings Tab) screen

Install Application Assistant

Back Next Finish Cancel

Optional Settings

You can modify these settings or accept the defaults

General

What do you want to name this deployment?

Name: Web_Services_v4-ContactPhonesSe

Security

What security model do you want to use with this application?

☒ DD Only: Use only roles and policies that are defined in the deployment descriptors.

☐ Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.

☐ Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.

☐ Advanced: Use a custom model that you have configured on the realm's configuration page.

Source accessibility

How should the source files be made accessible?

☒ Use the defaults defined by the deployment's targets

Recommended selection.

☐ Copy this application onto every target for me

During deployment, the files will be copied automatically to the managed servers to which the application is targeted.

☐ I will make the deployment accessible from the following location

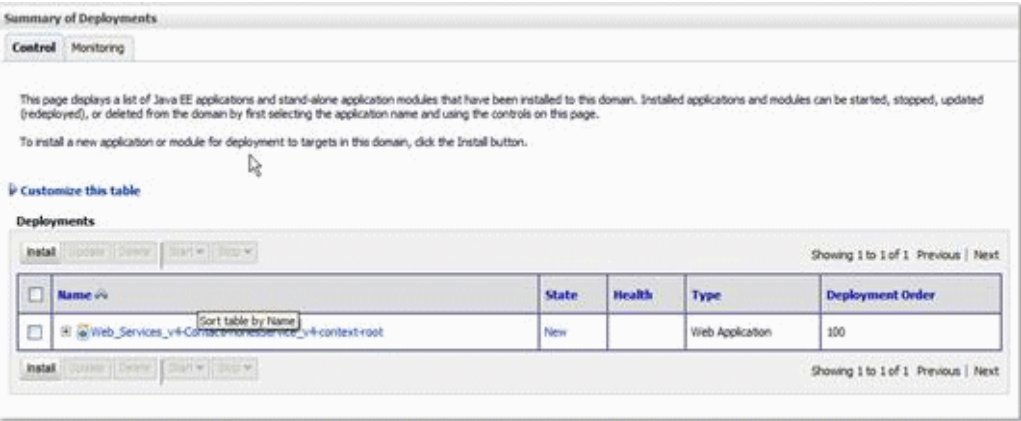
Location: C:\Oracle\Middleware\user_projects\domains\base_doma

Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.

Back Next Finish Cancel

20. Click Finish.

Figure 2–18 Summary of Deployments (Control Tab) screen



The Summary of Deployments displays your service.

- 21. Configure security for service (the service must be started).
- 22. From the Deployments screen, expand the service you want to secure.

Figure 2–19 Expanded Service Deployment (Name) screen

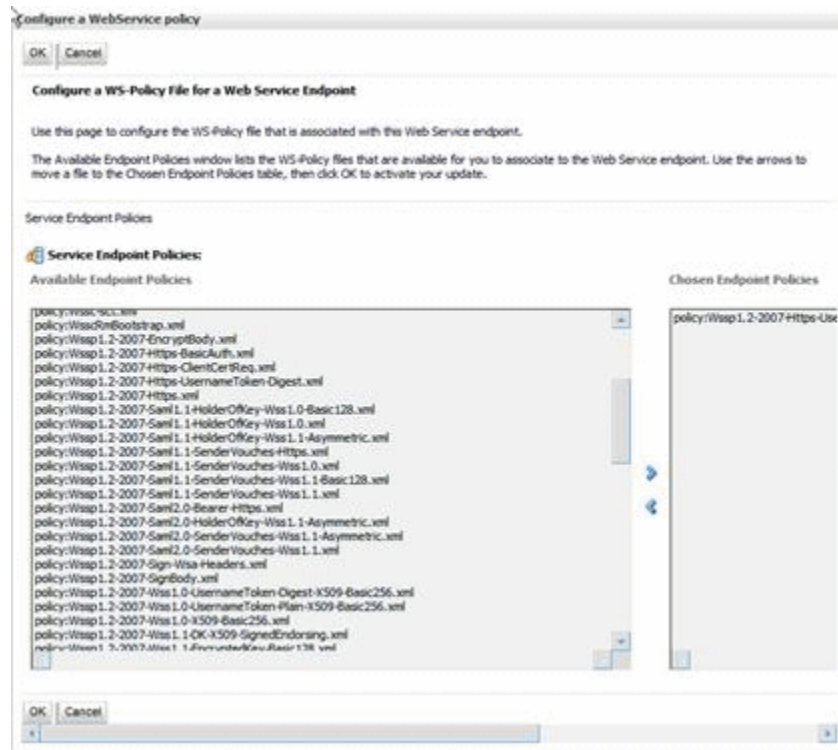


- 23. Select the web service and then select the Configuration-> WS-Policy tab.

Figure 2–20 Settings for Contact Phones Implemented Service (Configuration Tab, WS-Policy Subtab) screen



- 24. Select the service.

Figure 2–21 Configure a Web Service Policy screen

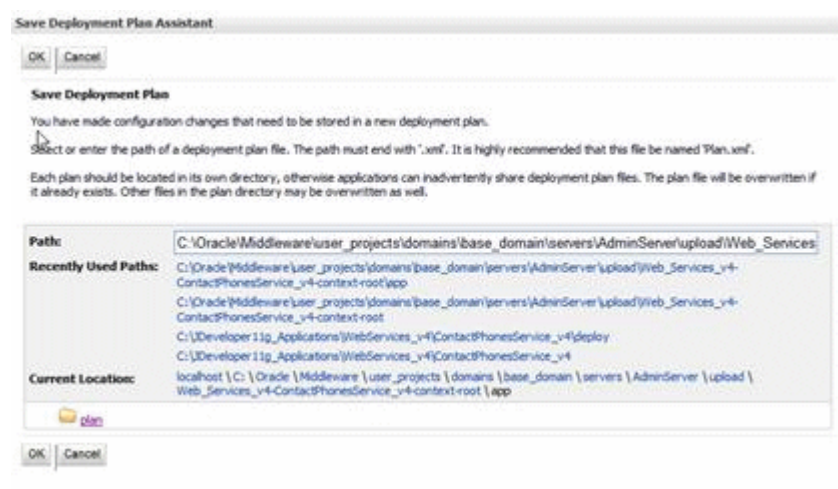
25. Select:

policy:Wssp1.2-2007-Https-UsernameToken-Plain.xml

Click the right arrow to move it from the Available Endpoint Policies to the Chosen Endpoint Policies area.

Click OK.

Save the deployment plan.

Figure 2–22 Save Deployment Plan Assistant screen

26. Click OK and then restart the server.

All web services need to specify a security string as part of the SOAP Header in the format DN=username, ADR=machineName, ENV=environment, for example:

```
<soapenv:Header>
  <wsse:Security
    xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
    xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"
    soapenv:mustUnderstand="1">
    <wsse:UsernameToken
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
      xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <Username>DN=SOAPROXY,ADR=JDED, ENV=A93TS</Username>
      <wsse:Password
        Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">edduser93</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
  </soapenv:Header>
```


WebSphere Application Server

This chapter contains the topic:

- [Section 3.1, "Installing the WebSphere Application Server."](#)

If you do not already have an appropriate WebSphere Application Server, create an application server. Refer to [Appendix B, "Create WebSphere Application Server"](#) in this guide.

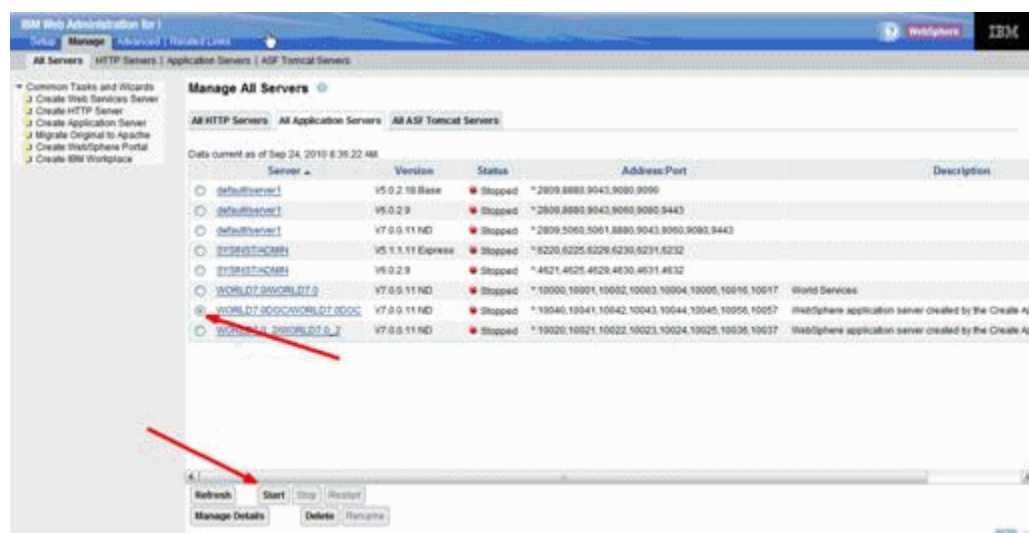
3.1 Installing the WebSphere Application Server

To install the WebSphere Application Server

1. Start Application Server.

Launch the IBM Web Administrator for i: <http://localhost:2001/HTTPAdmin>

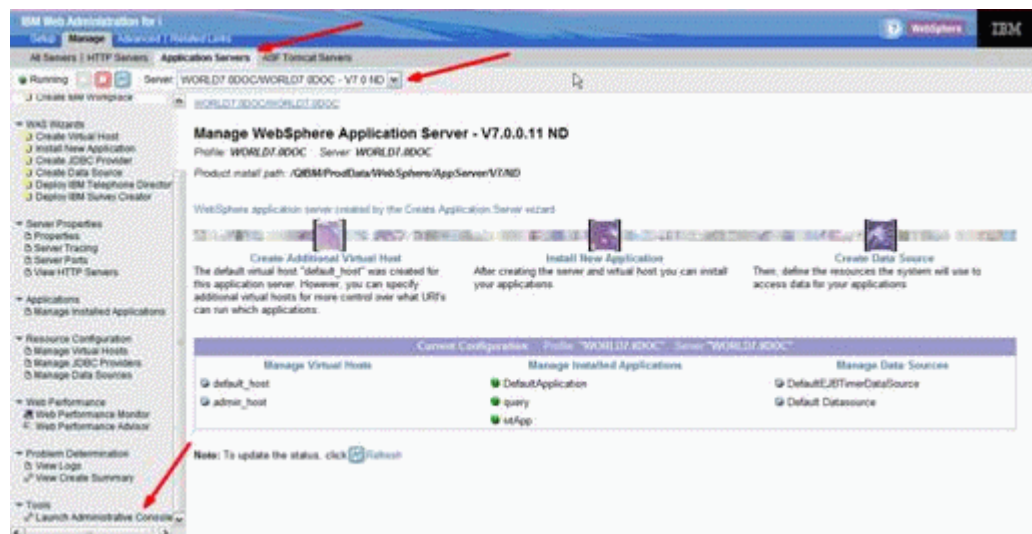
Figure 3–1 IBM Web Administrator (Manage All Servers Tab) screen



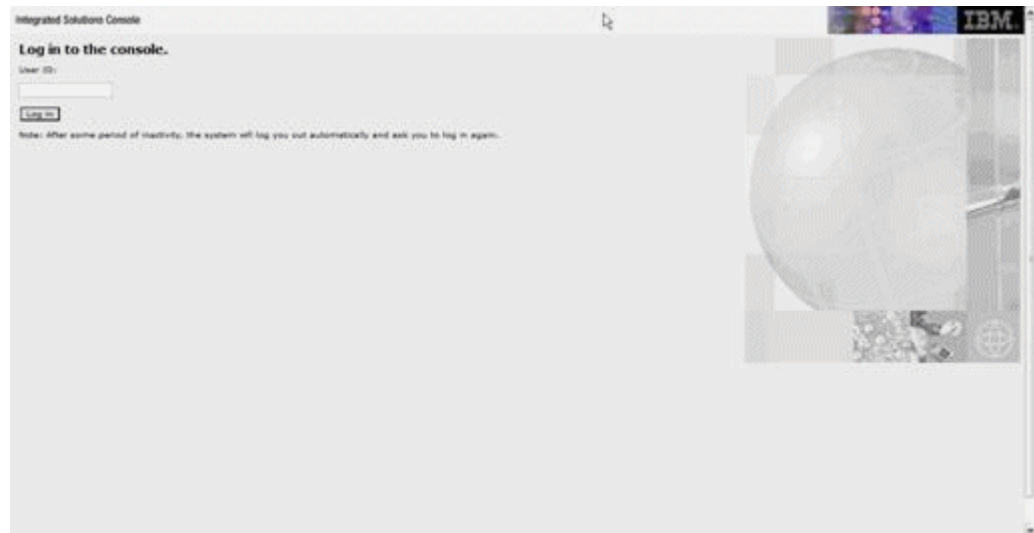
2. Select the appropriate Application Server and then click Start.

Figure 3–2 Start Page on the IBM Web Administrator screen

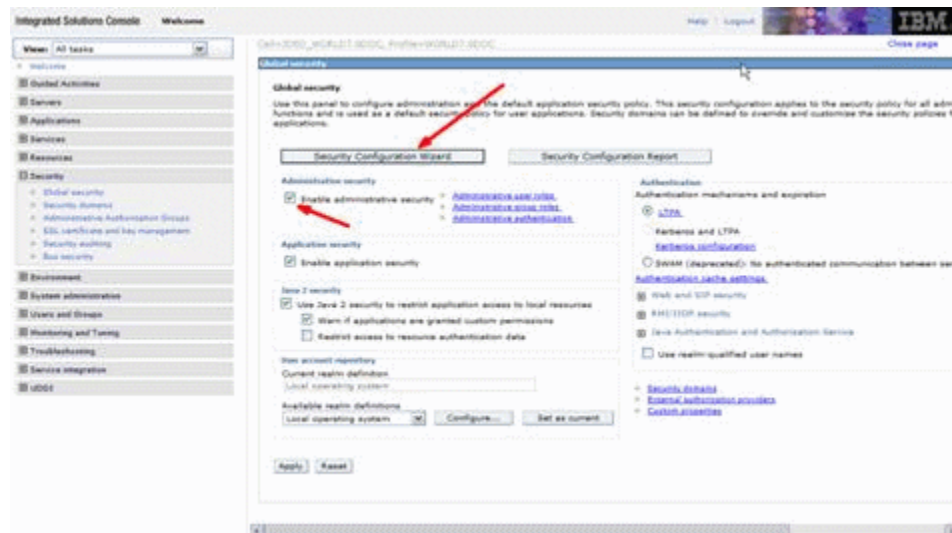
3. Click Start.
Launch Administrative Console.

Figure 3–3 Manage WebSphere Application Server screen

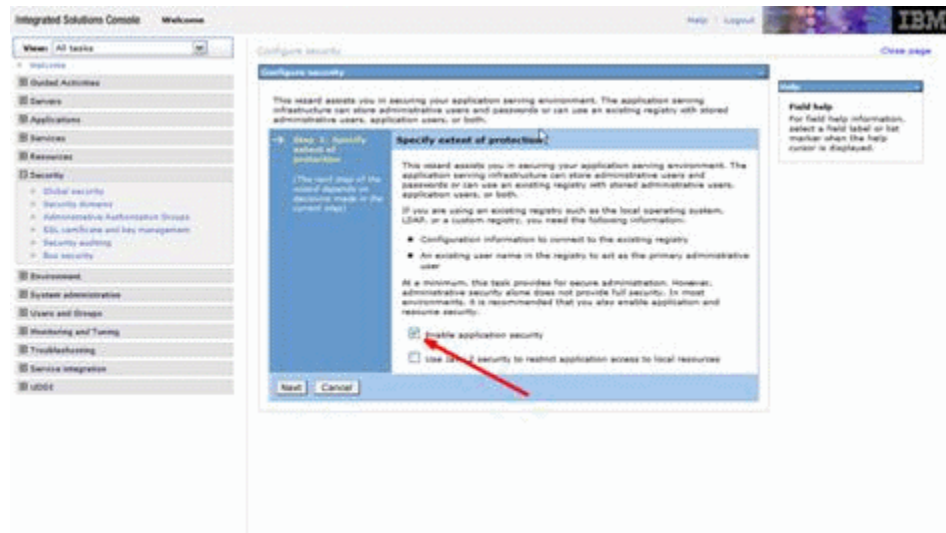
4. Select the Application Servers Tab then select the appropriate server from the Server dropdown box.
Click the Launch Administrative Console link.

Figure 3–4 Log in to the Console screen

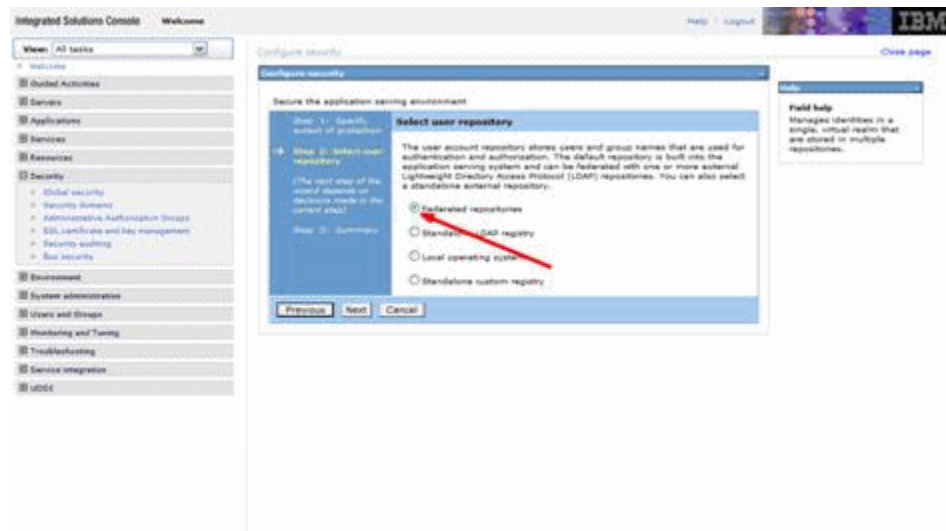
5. Leave the User ID blank and click Log in.

Figure 3–5 Global Security (Wizard Button) screen

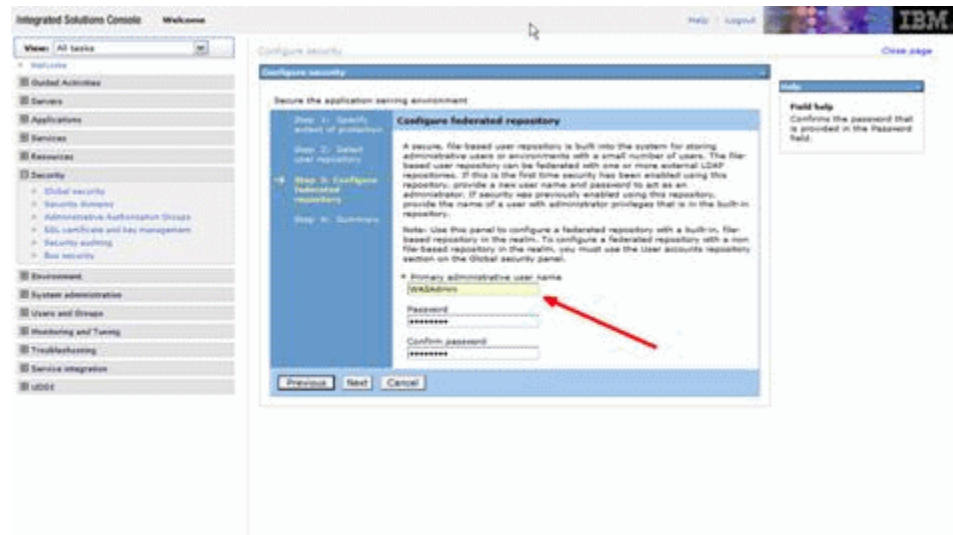
6. Configure security for JAAS.
 Open: Security - Global Security.
 Select the Enable administrative security checkbox.
 Click Security Configuration Wizard.

Figure 3–6 Specify Extent of Protection (Enable Application Security Button) screen

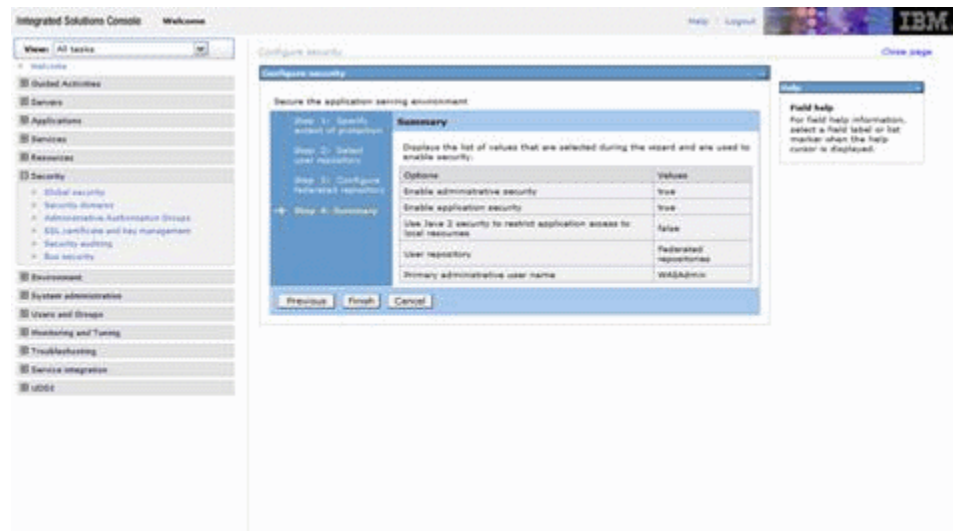
7. Select Enable application security and then click Next.

Figure 3–7 Federated Repositories Button

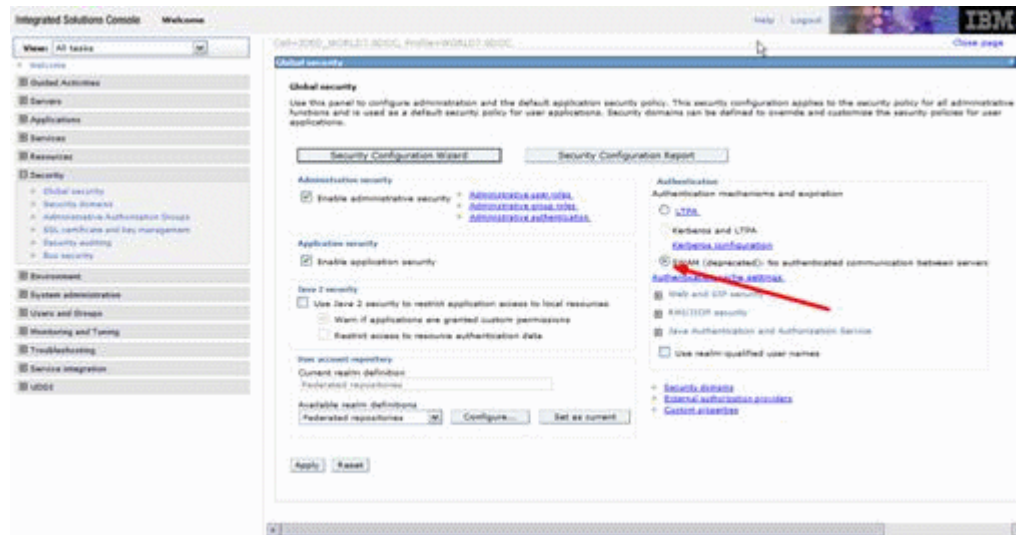
8. Select Federated repositories and then click Next.

Figure 3–8 Primary Administrative User Name field

9. Enter Primary administrative user name and Password and then click Next.

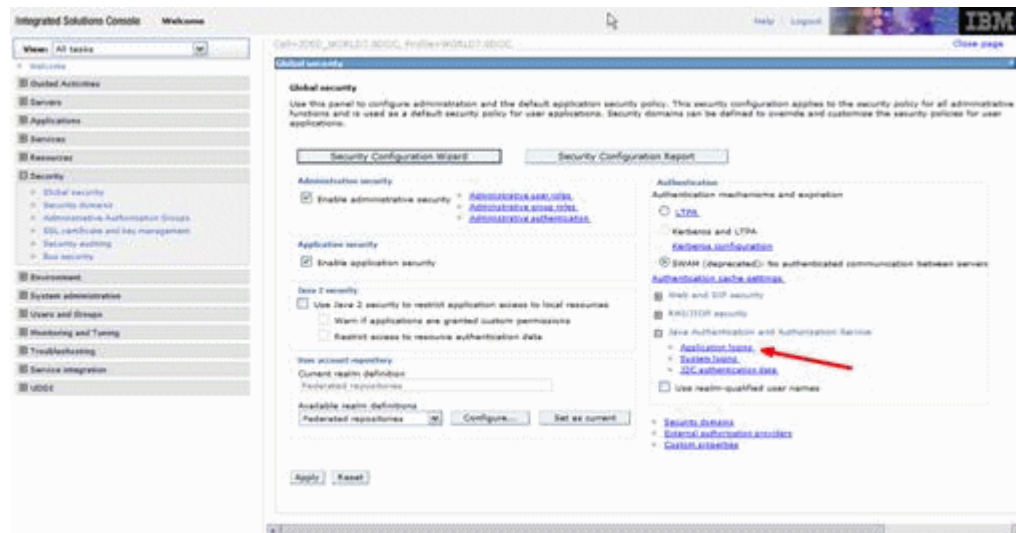
Figure 3–9 Summary screen

10. Review settings and then click Finish.

Figure 3–10 SWAM Button on the Global Security screen

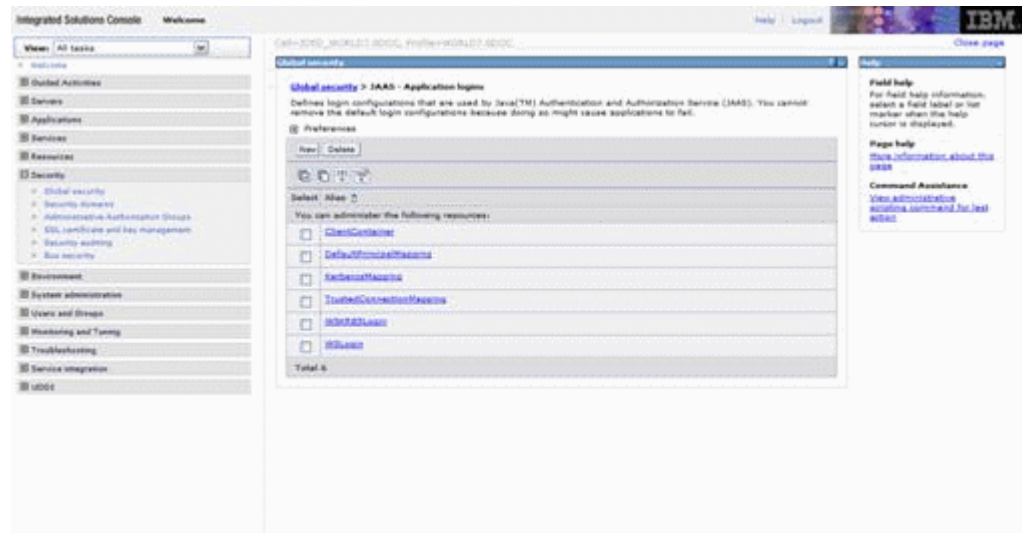
11. Select the Use SWAM -no authenticated communication between servers checkbox.

Click Apply and then click Save.

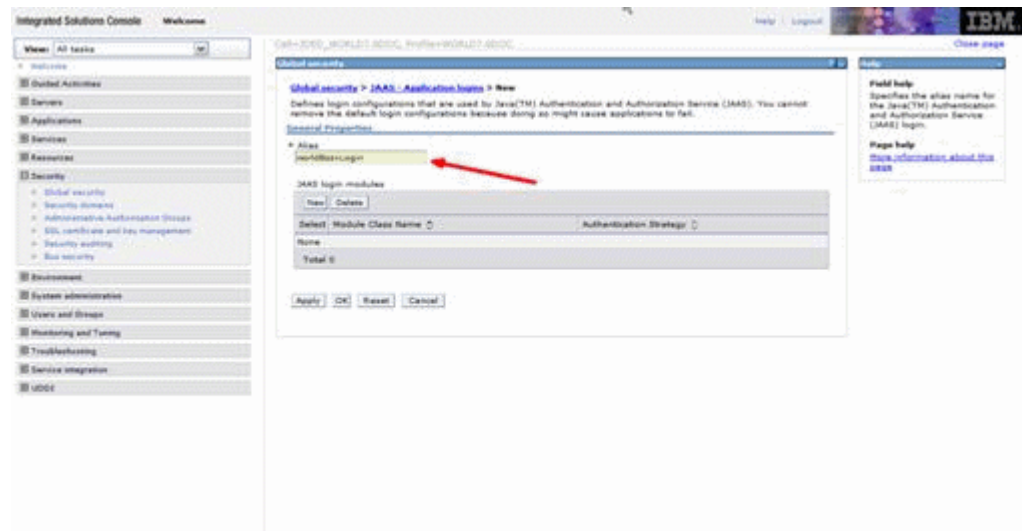
Figure 3–11 Global Security screen with Selection Noted

12. Add World Application login and configure custom login module.

Open Security - Global Security - Java Authentication and Authorization Service - Application Logins.

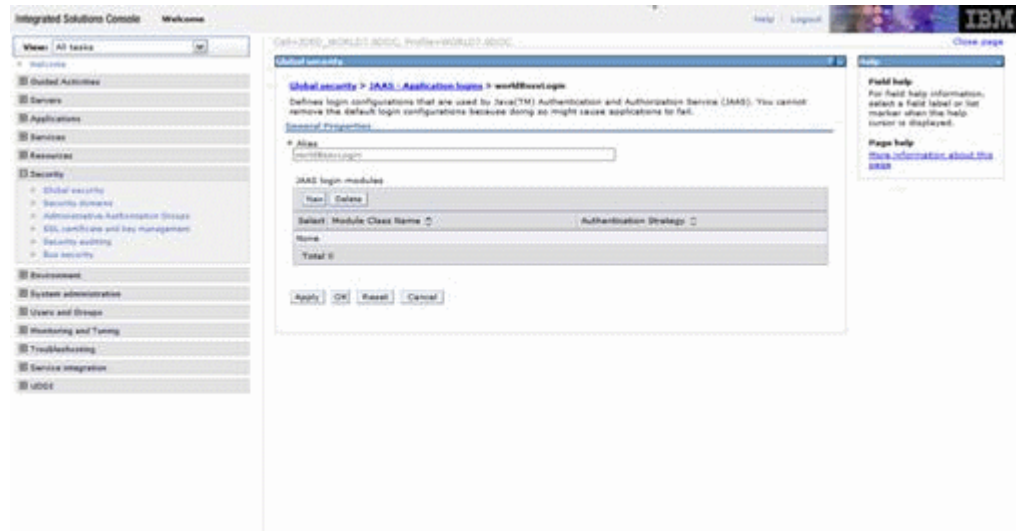
Figure 3–12 Global Security JAAS Application Login screen

13. Click New.

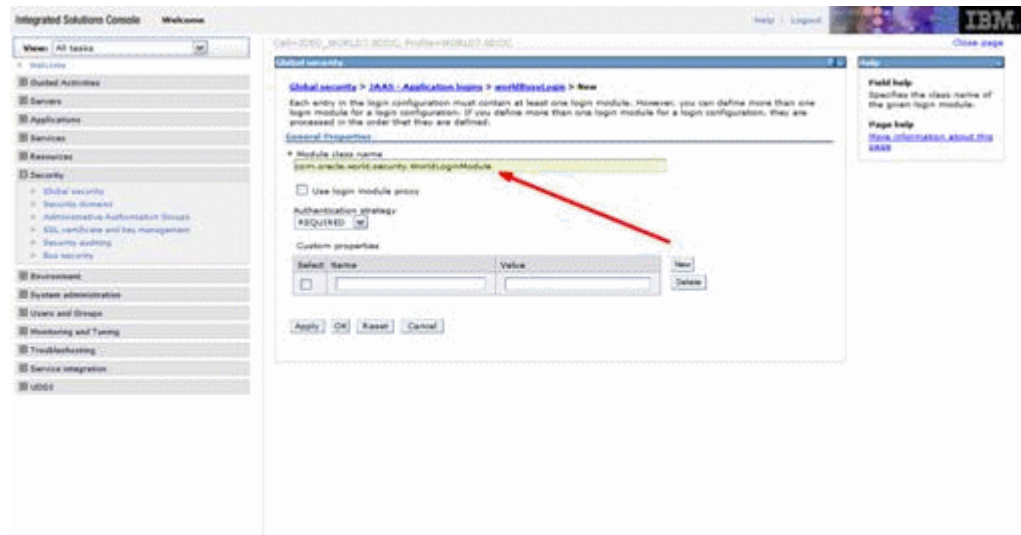
Figure 3–13 Alias Field

14. Enter the Alias:
worldBssvLogin
Click Apply.

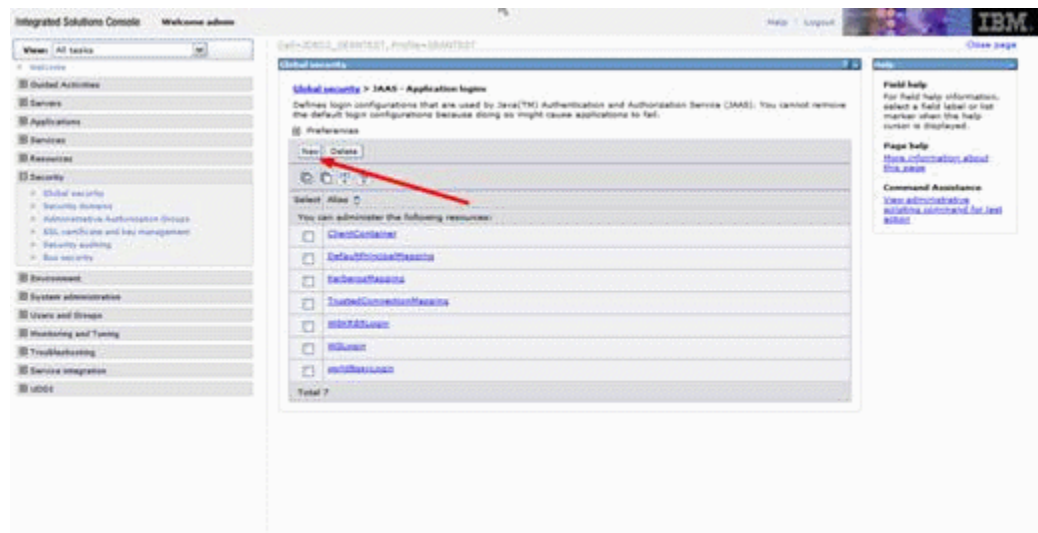
Figure 3–15 *WorldBssvLogin screen*



16. Click New.

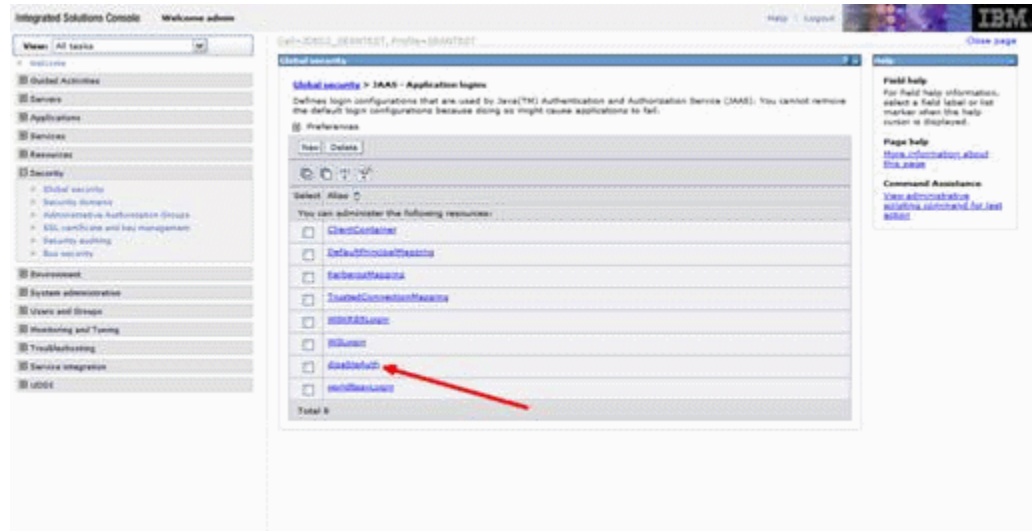
Figure 3–16 Module Class Name field

17. Enter full pathname for custom login module in the Module class name field.
 com.oracle.world.security.WorldLoginModule
 Click Apply.

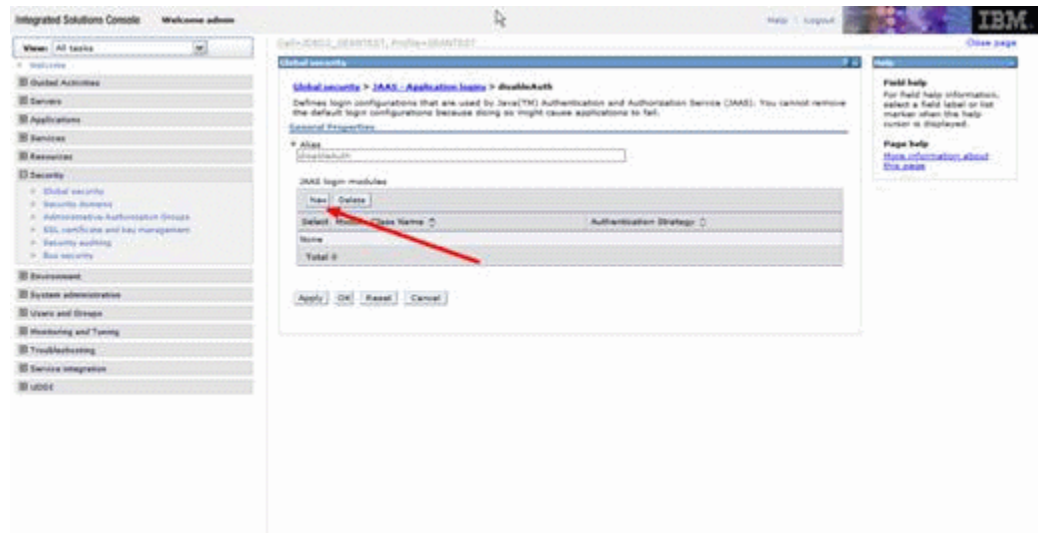
Figure 3–17 New Button on the JAAS Application Login screen

18. Navigate back to the JAAS - Application logins screen and then click New.

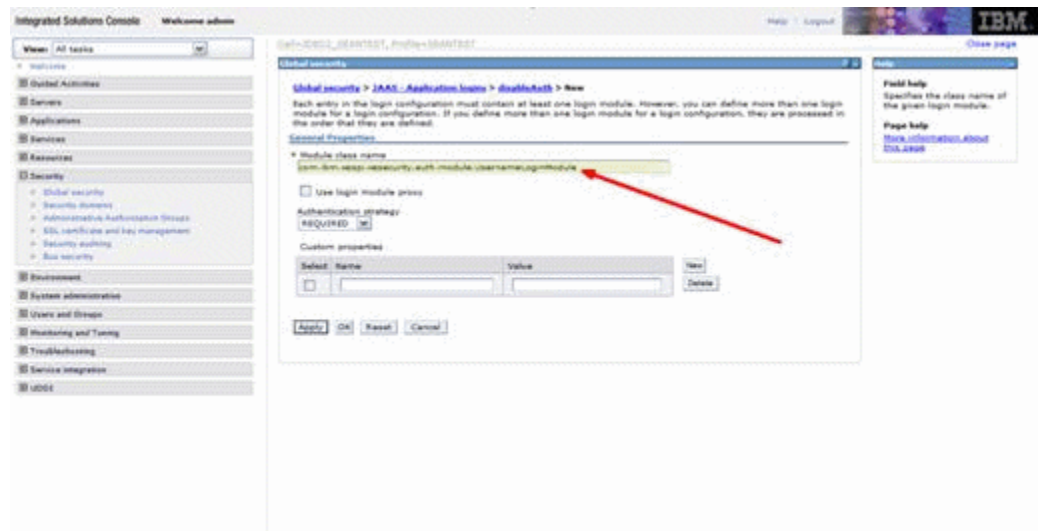
Figure 3–19 Global Security screen with Selection Noted



20. Click the `disableAuth` link.

Figure 3–20 New button on the Global Security JAAS Authorization Login screen

21. Click New.

Figure 3–21 Module Class Name field

22. Enter full pathname for custom login module in the Module class name field.

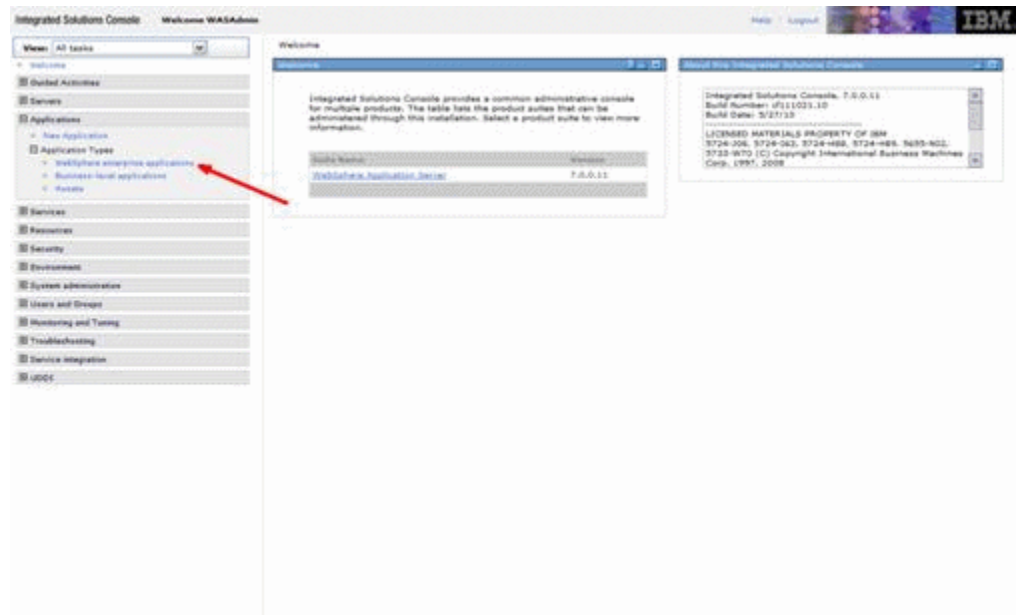
com.ibm.ws.security.auth.module.UsernameLoginModule

Click Apply.

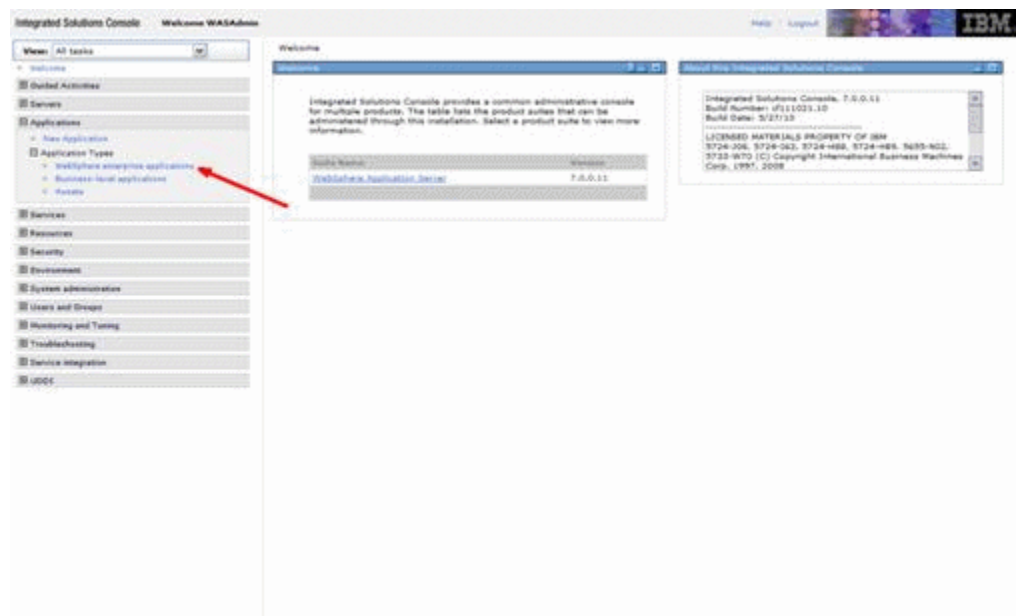
You must logout of the Console and restart the server for these changes to take effect.

Click the Logout link in the upper right-hand corner of the Console.

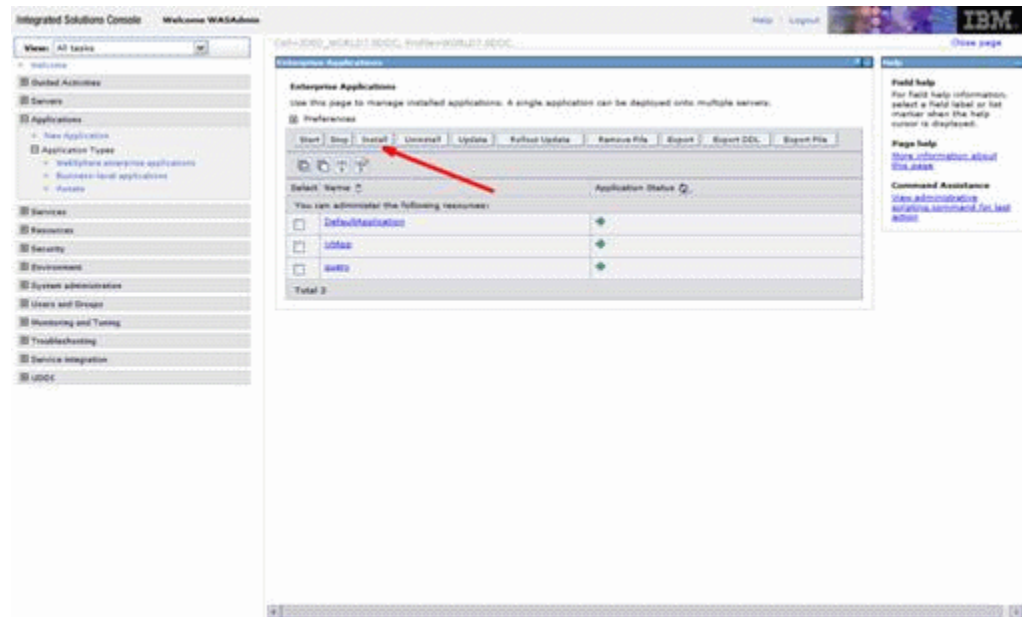
Restart the server. Refer to Step 1, Start Application Server section of this document. Use the User name and Password you created when logging in after restarting the server.

Figure 3–22 Correct Application (Type Noted) screen

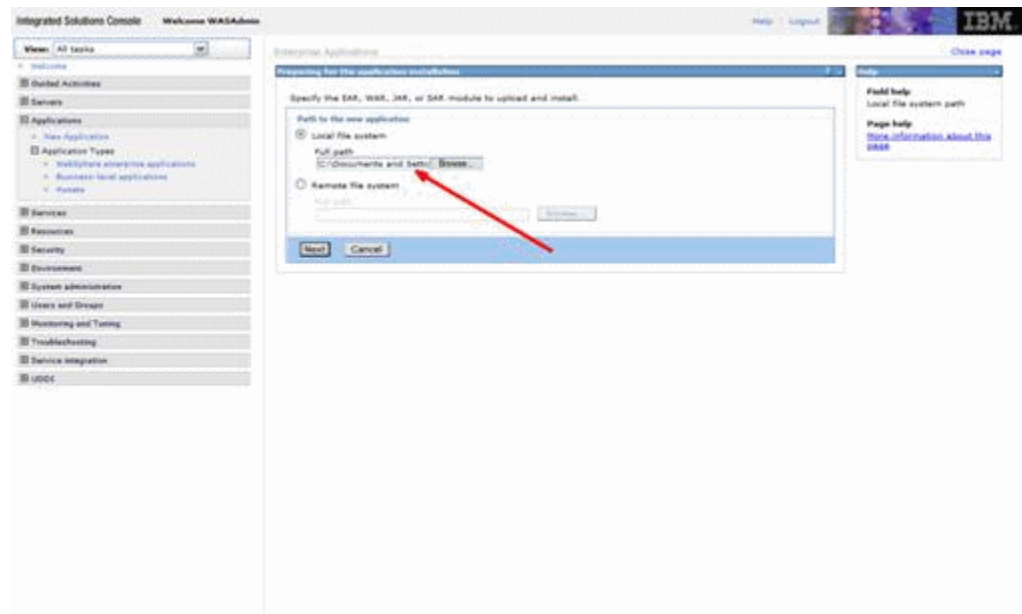
23. Deploy Web Services EAR file.

Figure 3–23 Correct Application (Type Noted) screen

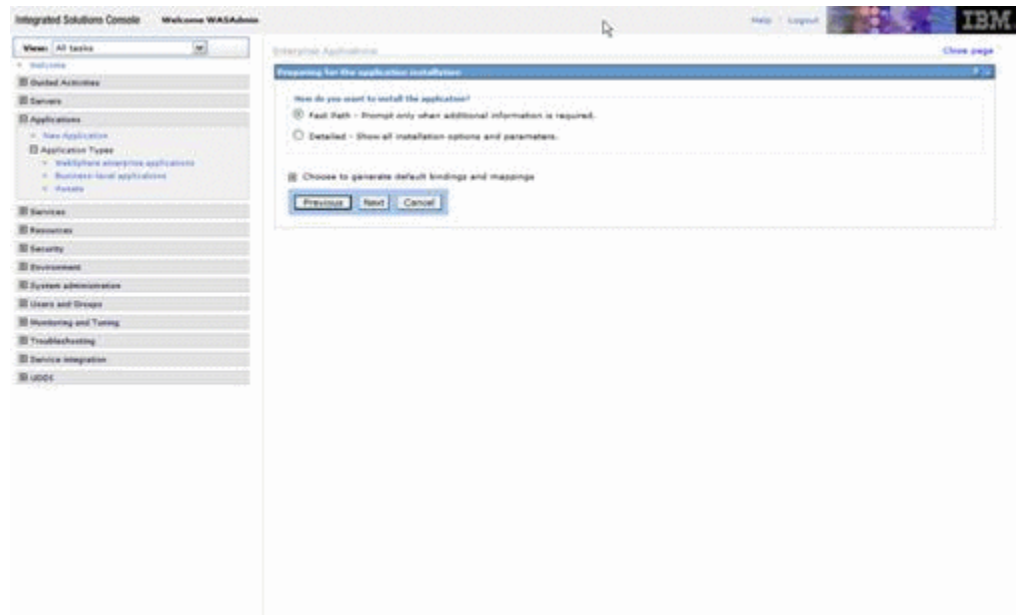
24. Open the Applications then click the WebSphere enterprise applications link.

Figure 3–24 Enterprise Applications screen

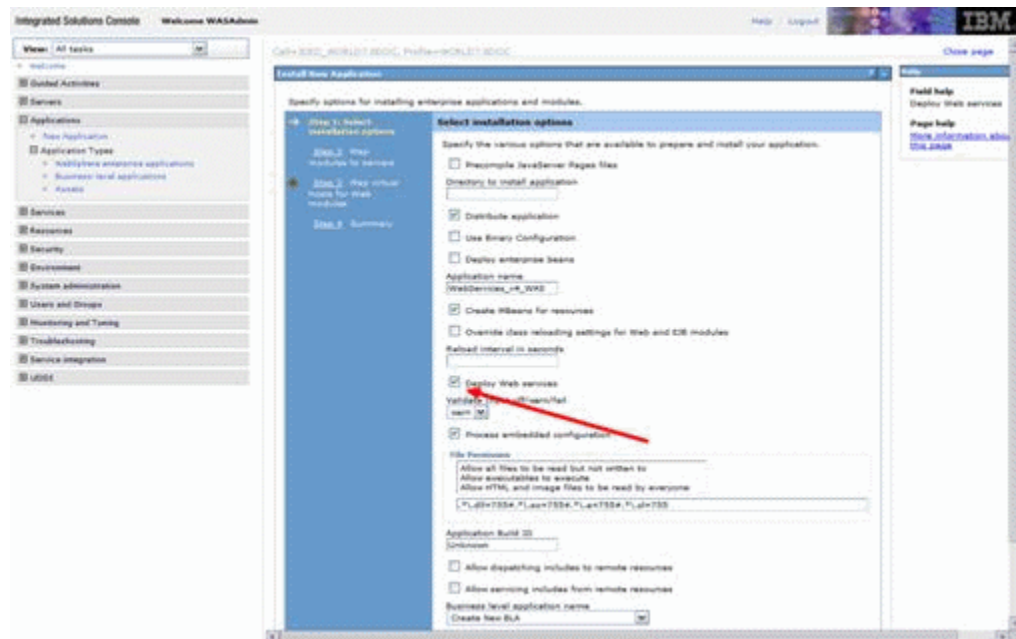
25. Click Install.

Figure 3–25 Full Path field

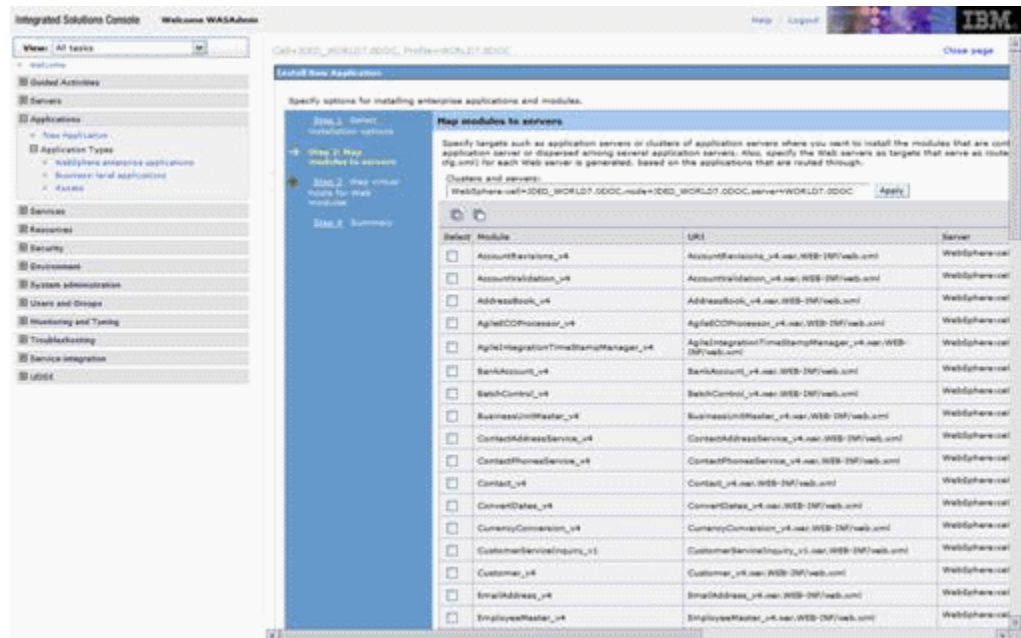
26. Enter the Full path to WebServices_v4_WAS.ear file and then click Next.

Figure 3-26 Next button

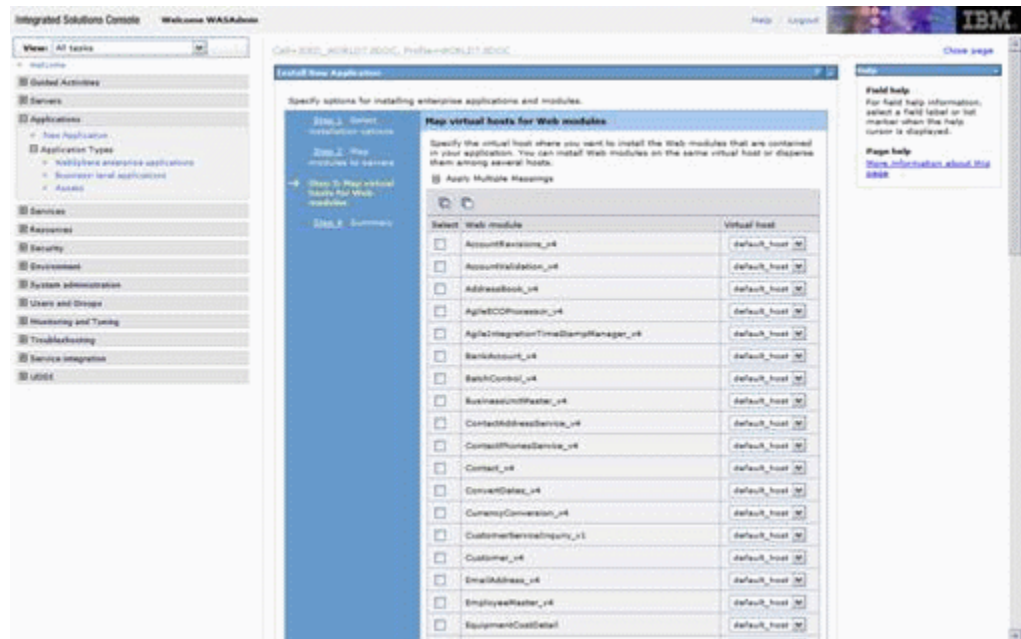
27. Click Next.

Figure 3-27 Deploy Web Services checkbox

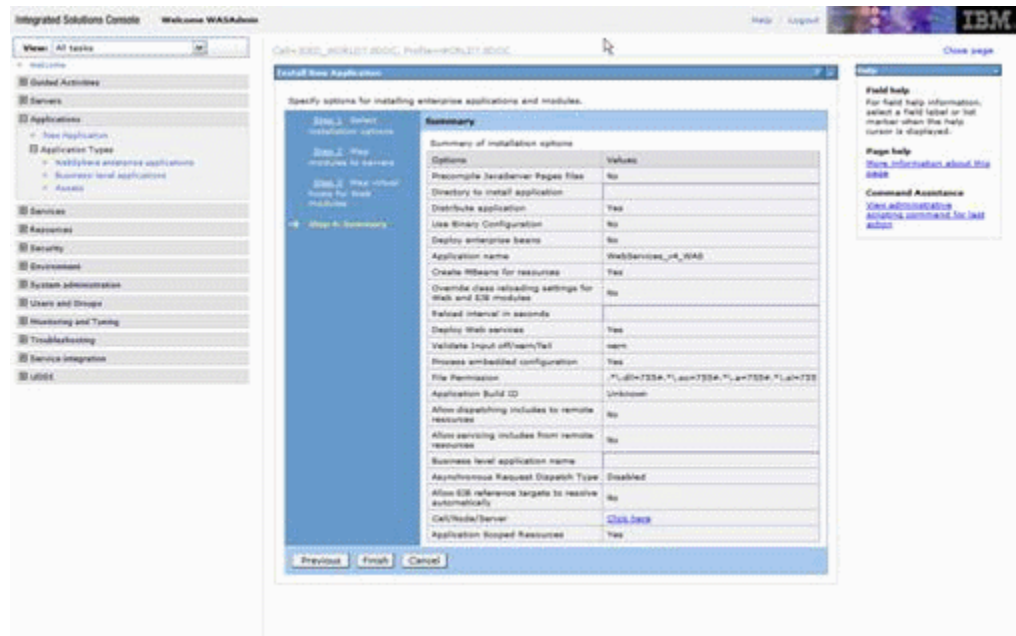
28. Select Deploy Web services and then click Next.

Figure 3–28 Map Modules to Servers screen

29. Click Next.

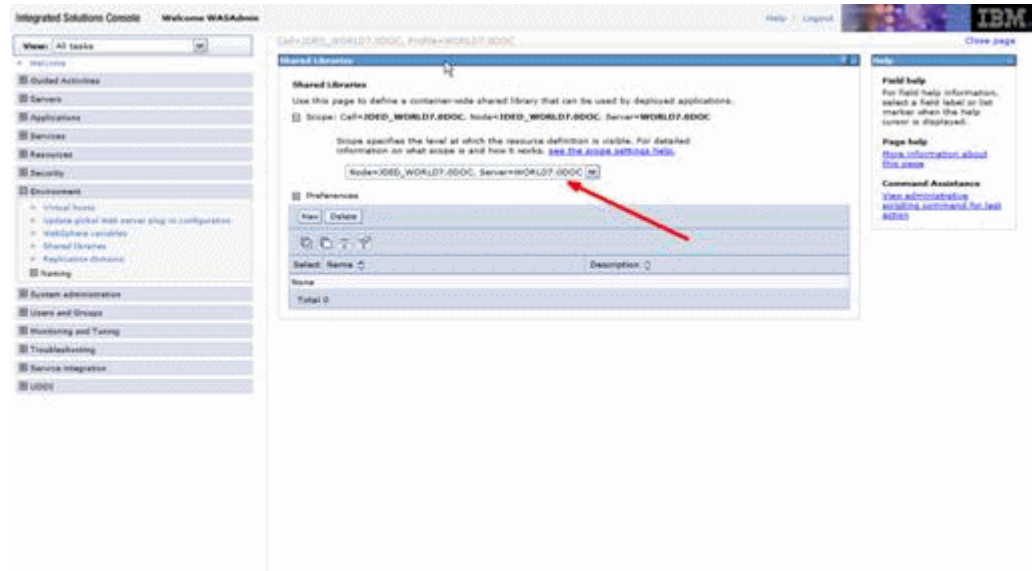
Figure 3–29 Next screen

30. Click Next.

Figure 3–30 Summary screen with Finish button

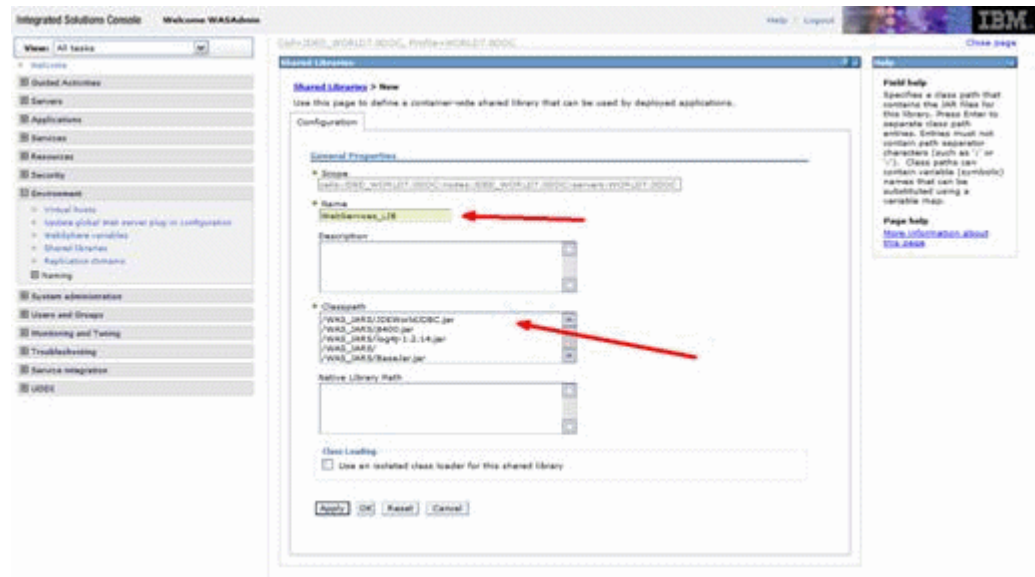
31. Click Finish.

32. Create Shared Libraries.

Figure 3–31 Dropdown List

33. Open the Environment and then click the Shared Libraries link.

Select the appropriate Scope from the dropdown list and then click New.

Figure 3–32 Shared Libraries screen

- 34.** Enter `WebServices_LIB` in the Name field.

Enter the location of the `JDEWorldJDBC.jar`, `jt400.jar`, `log4j.jar`, and the `BaseJar.jar` in the Classpath field.

Click OK.

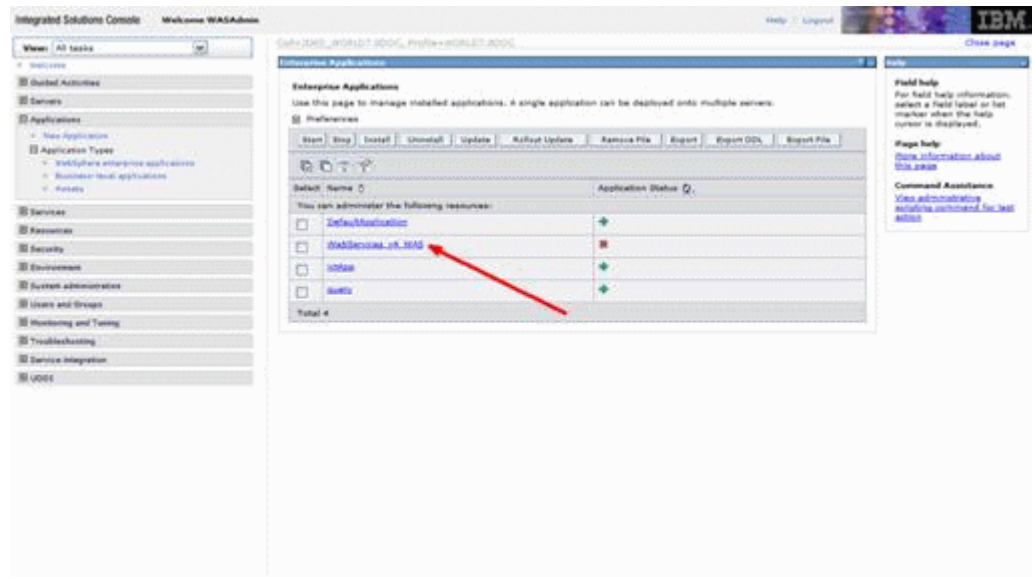
For details about the latest version supported for `log4j`, see Doc ID 2318897.1 in My Oracle Support. (WS: Instructions to Address JD Edwards World Security Vulnerabilities (Doc ID 2318897.1)(Release A9.3 Update)

- 35.** Copy `jt400.jar`, `JDEWorldJDBC.jar`, `log4j.jar`, and `BaseJar.jar` to the IFS.

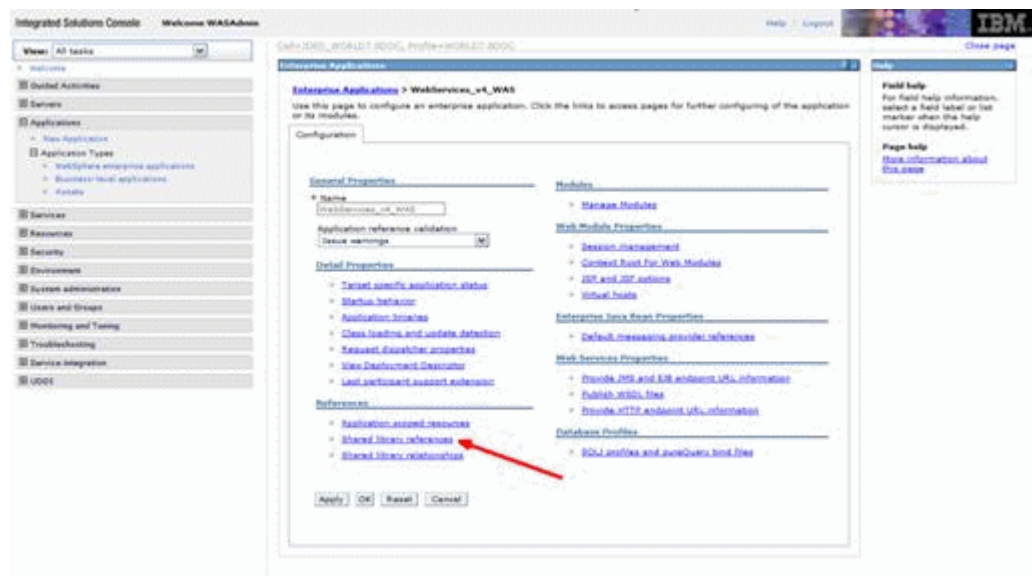
Copy all four files to the directory you specified in the Classpath field.

The `JDEWorldJDBC.jar` and the `BaseJar.jar` are included in the Web Services .zip file downloaded from the MyOracleSupport Web site.

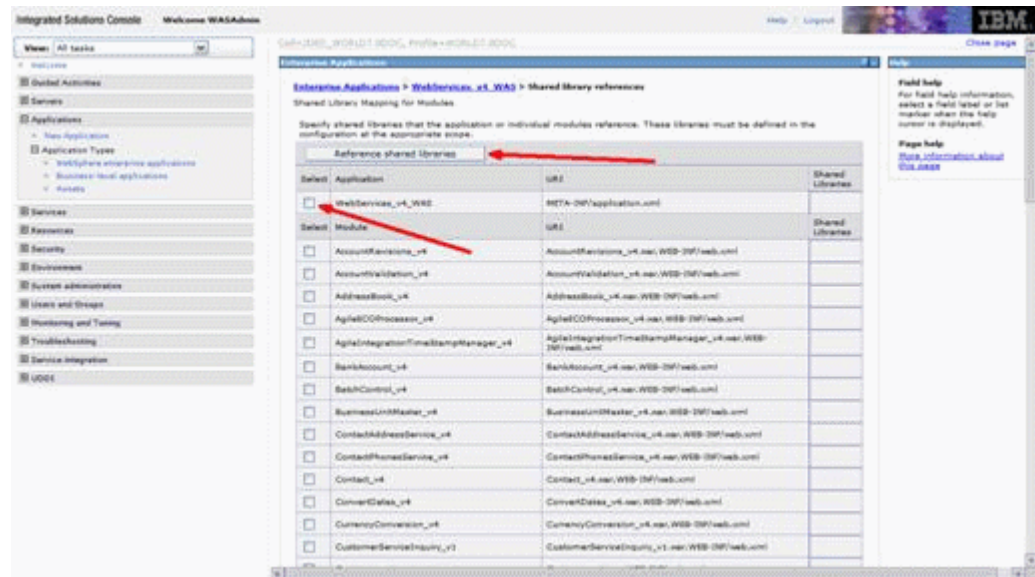
- 36.** Associate `WebSeverices_LIB` Shared Library with the `WebServices_v4_WAS` Application.

Figure 3–33 Enterprise Applications screen

37. Open the Applications and then select the WebSphere enterprise applications link. Click the WebServices_v4_WAS link.

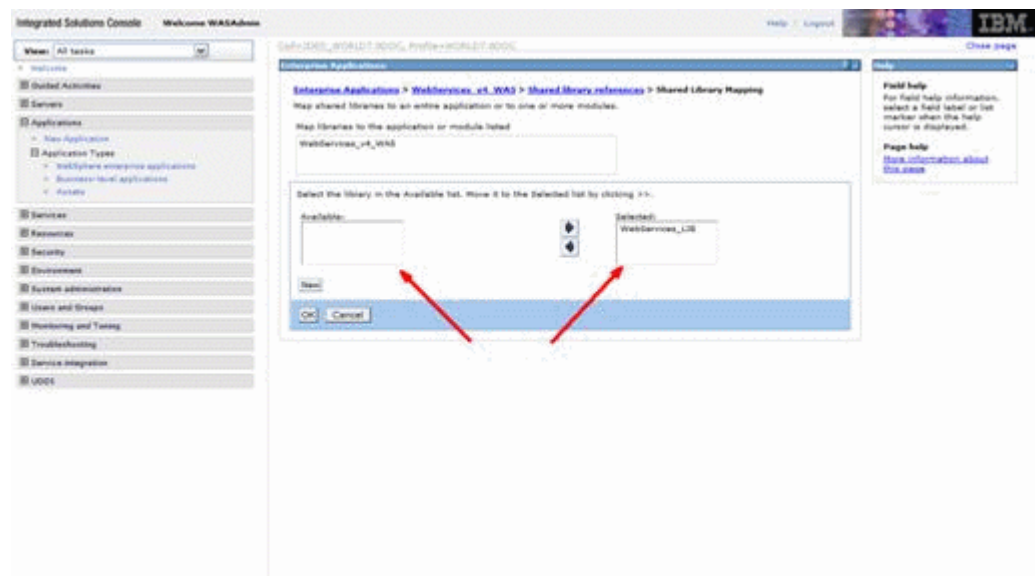
Figure 3–34 Enterprise Applications WebServices_v4_WAS screen

38. Click the Shared Library References link under References.

Figure 3–35 Reference Shared Libraries button

39. Select the WebServices_v4_WAS application box.

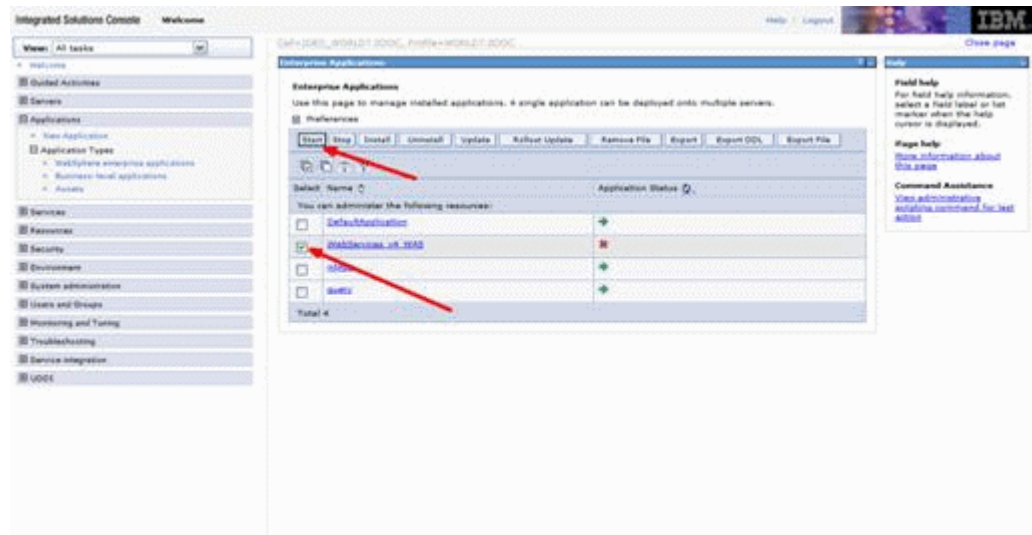
Click Reference Shared Libraries.

Figure 3–36 WebServices_LIB menu item

40. Select the WebServices_LIB Shared Library Reference using the arrow button

Click OK.

41. Start WebServices_v4_WAS application

Figure 3–37 Start button

42. Open Applications and then select the WebSphere enterprise applications link.
Select the WebServices_v4_WAS application.
Click Start.

Install WebLogic Application Server

This appendix contains the topic:

- [Section A.1, "Installing WebLogic Application Server."](#)

A.1 Installing WebLogic Application Server

To install WebLogic Application Server

1. Download Required Jars:

jt400.jar - retrieve from: <http://jt400.sourceforge.net/>

log4j - for details about the latest version supported for log4j, see Doc ID 2318897.1 in My Oracle Support. Use the following URL to access and sign in to My Oracle Support:

<https://support.oracle.com>

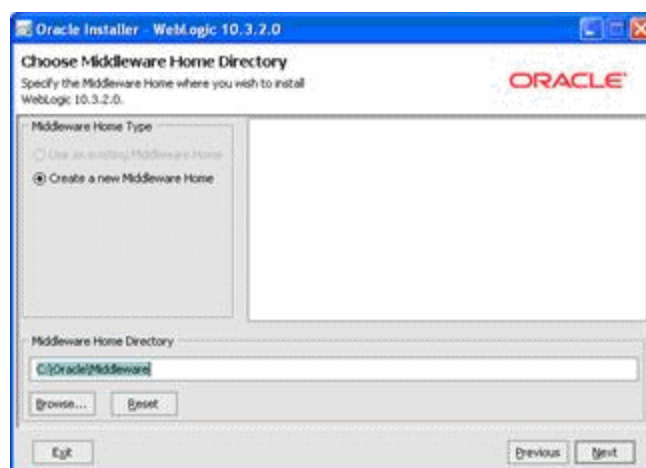
(WS: Instructions to Address JD Edwards World Security Vulnerabilities (Doc ID 2318897.1) (Release A9.3 Update)

WebLogic Installation Instructions

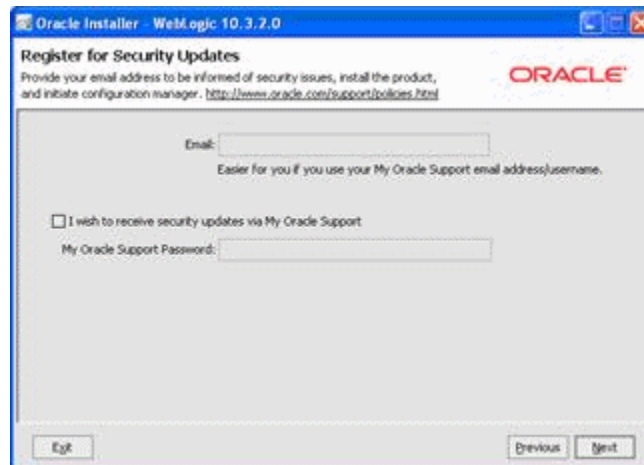
1. Download the WLS server installation file from OTN and install.

Use the default values.

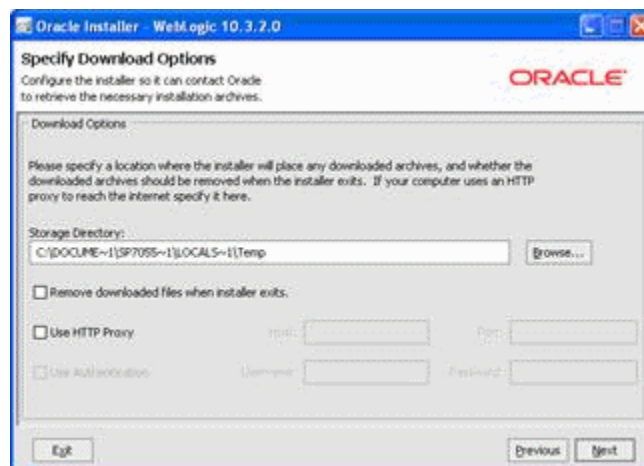
Figure A–1 Choose Middleware Home Directory screen



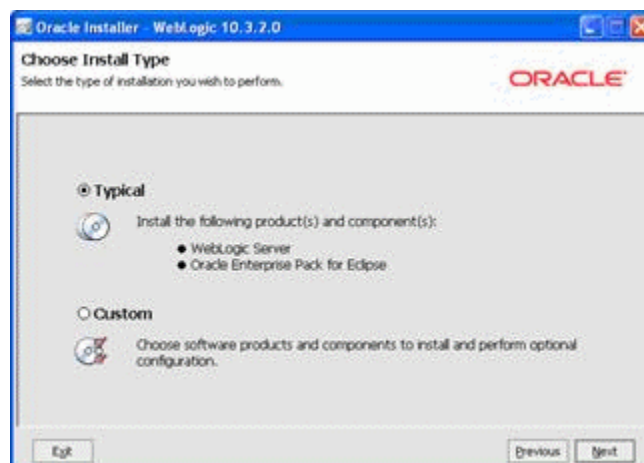
2. Click Next.

Figure A–2 Register for Security Updates screen

3. Click Next.

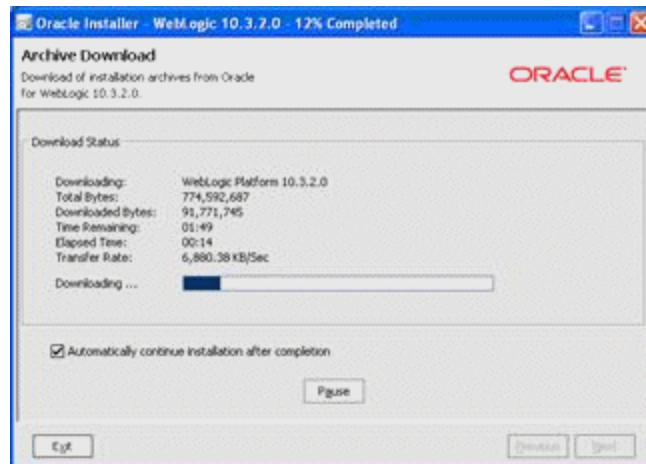
Figure A–3 Specify Download Options screen

4. Click Next.

Figure A–4 Choose Install Type screen

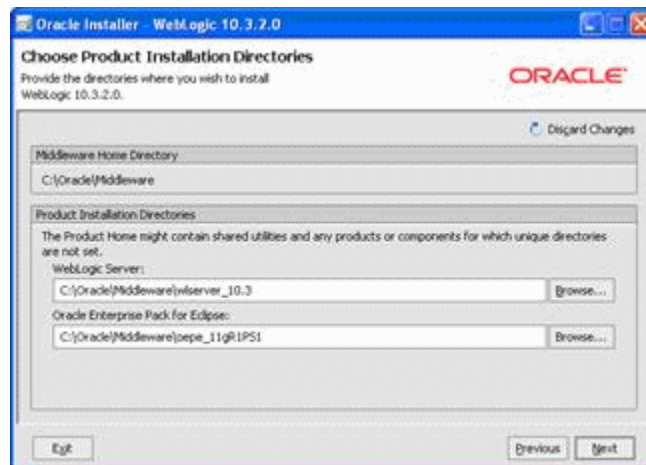
5. Select Typical and then click Next.

Figure A–5 Archive Download screen

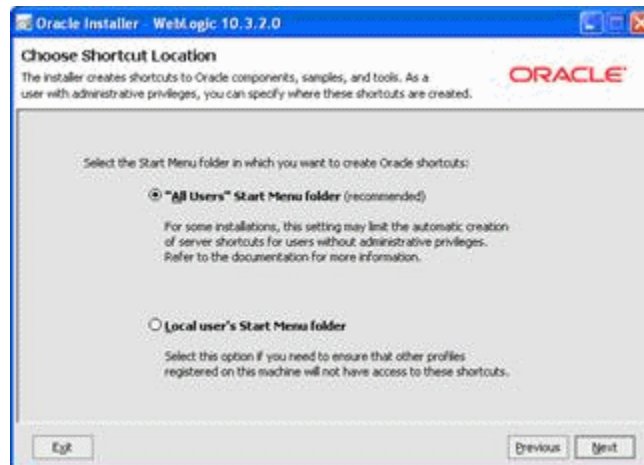


6. Click Next.

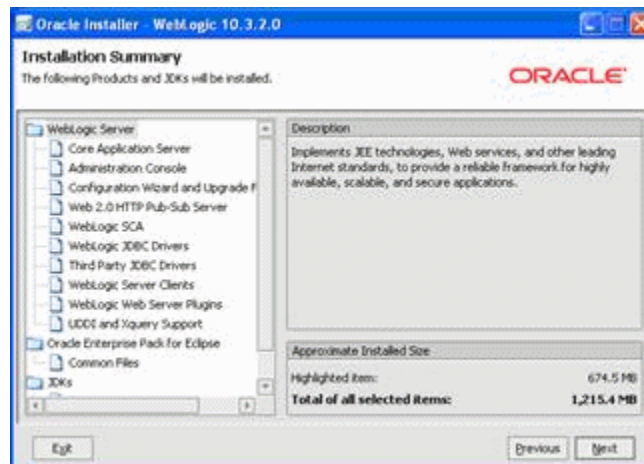
Figure A–6 Choose Product Installation Directories screen



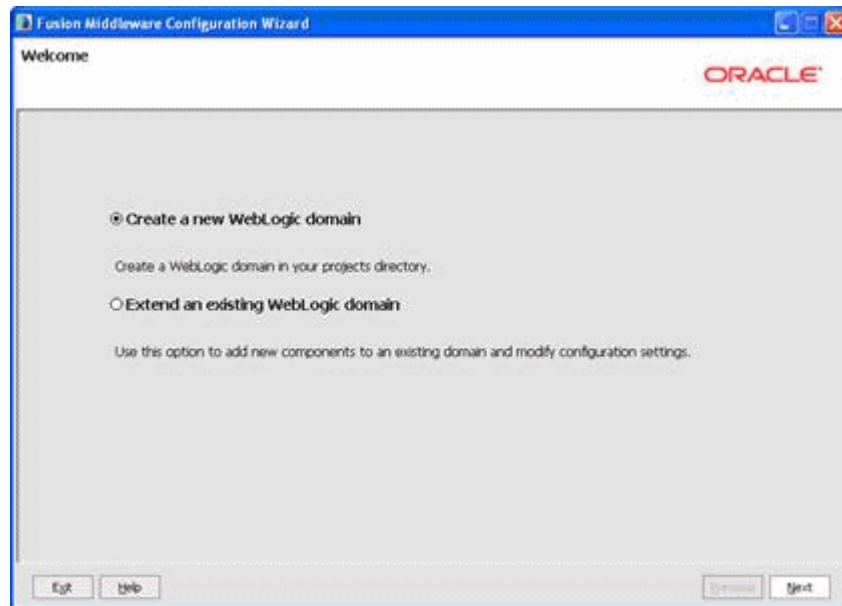
7. Click Next.

Figure A-7 Choose Shortcut Location screen

8. Click Next.

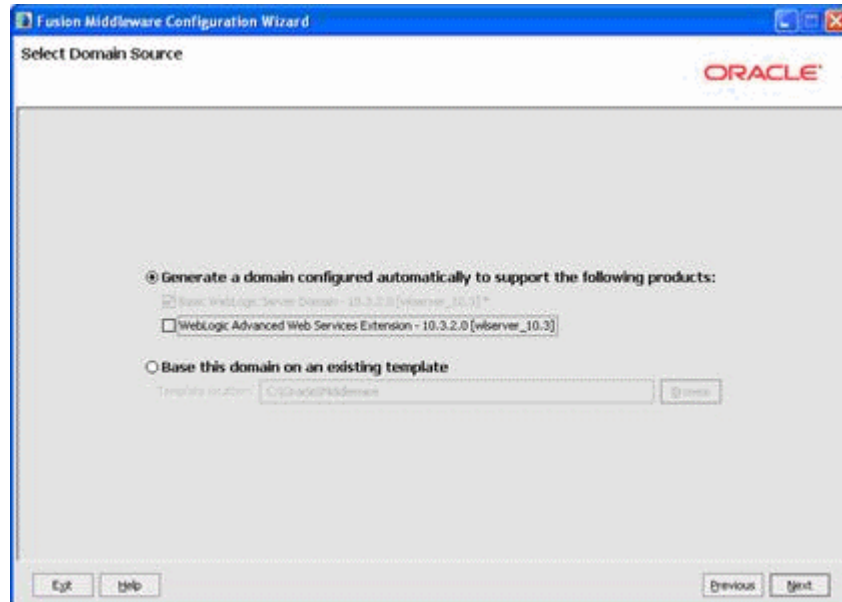
Figure A-8 Installation Summary screen

9. Configure the base_domain.

Figure A–9 Fusion Middleware Configuration Wizard Welcome screen

Start > Programs > Oracle Fusion Middleware 11.1.1.2.0 > WebLogic Server
11gR1 > Tools > Configuration Wizard

Click Next.

Figure A–10 Select Domain Source screen

10. Click Next.

Figure A–11 Specify Domain Name and Location screen

The screenshot shows the 'Specify Domain Name and Location' screen of the Fusion Middleware Configuration Wizard. The window title is 'Fusion Middleware Configuration Wizard'. The main heading is 'Specify Domain Name and Location'. Below the heading, it says 'Enter the name and location for the domain:'. There are two input fields: 'Domain name:' with the text 'base_domain' and 'Domain location:' with the text 'C:\Oracle\Middleware\user_projects\domains'. A 'Browse...' button is next to the 'Domain location:' field. At the bottom, there are 'Exit', 'Help', 'Previous', and 'Next' buttons.

11. Click Next.

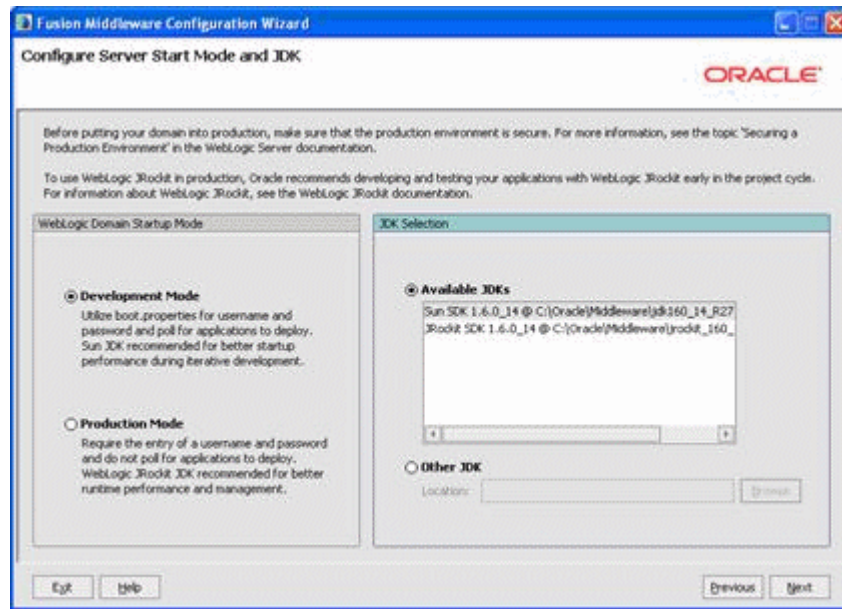
Figure A–12 Configure Administrator User Name and Password screen

The screenshot shows the 'Configure Administrator User Name and Password' screen of the Fusion Middleware Configuration Wizard. The window title is 'Fusion Middleware Configuration Wizard'. The main heading is 'Configure Administrator User Name and Password'. Below the heading, there is a 'Discard Changes' checkbox. There are four input fields: '*User name:' with the text 'weblogic', '*User password:' with masked text '*****', '*Confirm user password:' with masked text '*****', and 'Description:' with the text 'This user is the default administrator.'. At the bottom, there are 'Exit', 'Help', 'Previous', and 'Next' buttons.

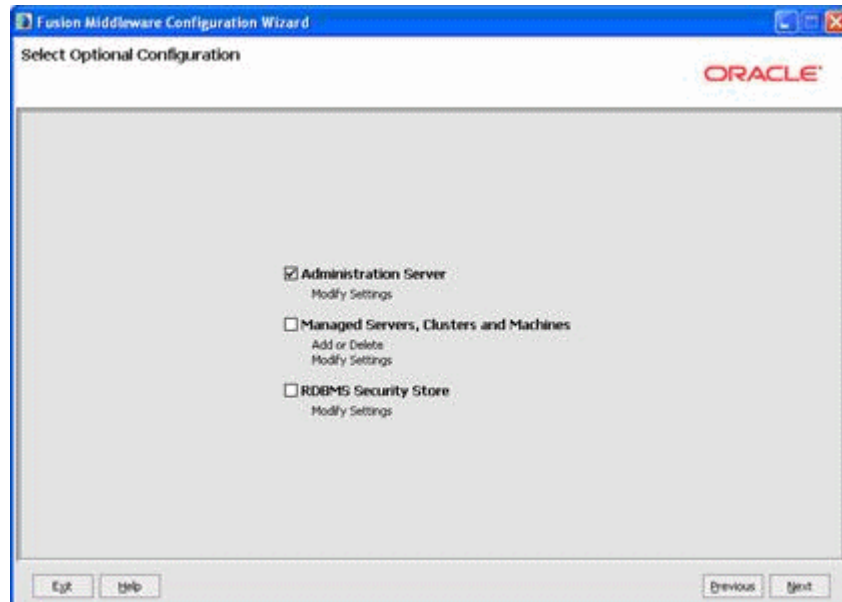
User Password:

"welcome1"

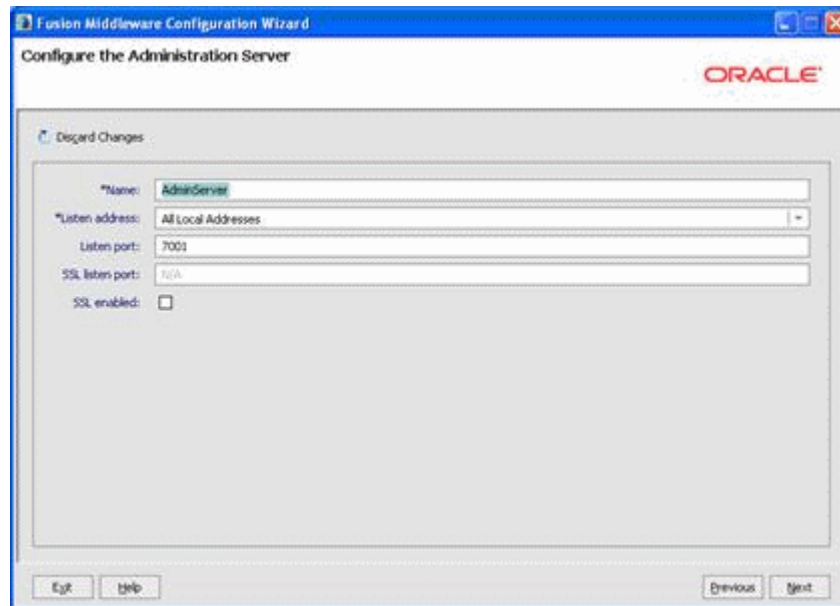
12. Click Next.

Figure A-13 Configure Server Start Mode and JDK screen

13. Click Next.

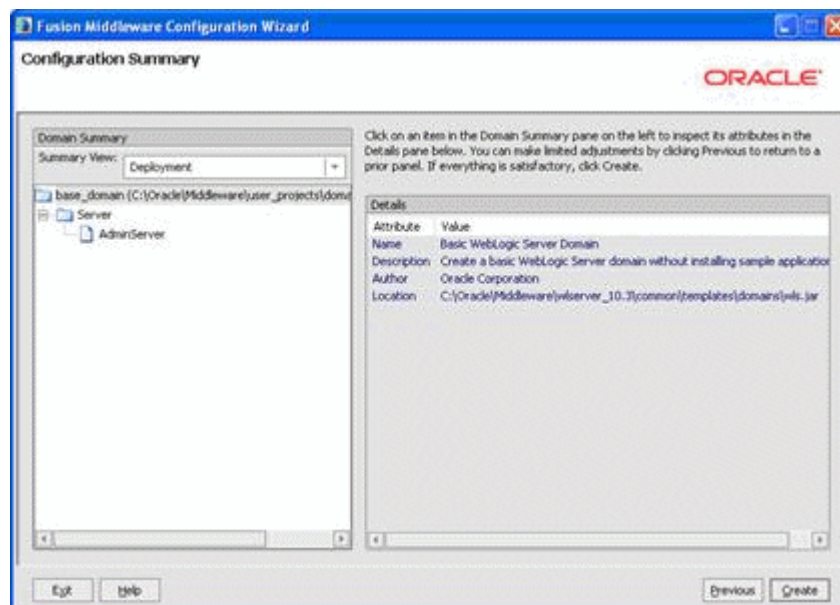
Figure A-14 Select Optional Configuration screen

14. Select:
 Administration Server
 Click Next.

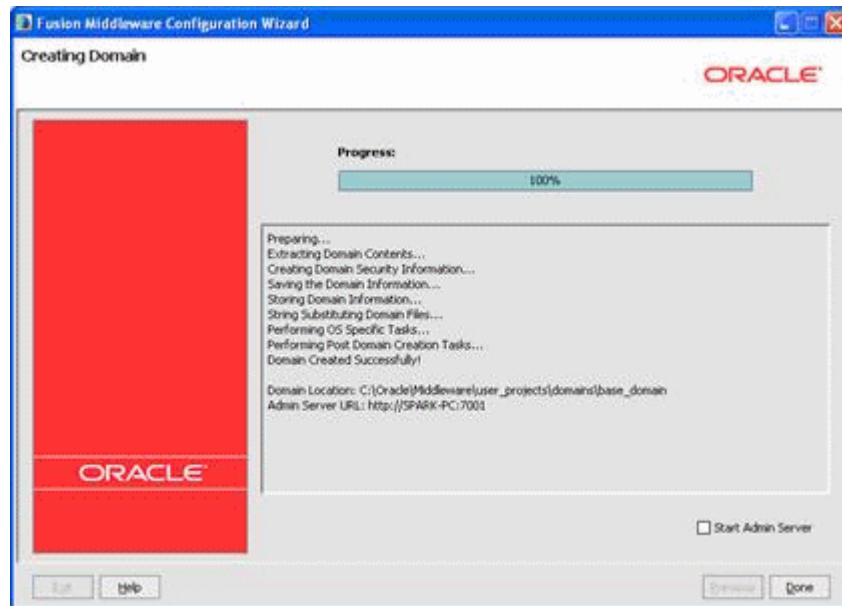
Figure A-15 *Configure the Administration Server screen*

15. Use defaults.

Click Next.

Figure A-16 *Configuration Summary screen*

16. Click Create.

Figure A-17 Creating Domain screen

17. Copy jt400.jar, JDEWorldJDBC.jar, log4j.jar, and BaseJar.jar to WebLogic server library.

(WLS_Home\Middleware\user_projects\domains\base_domain\lib

The JDEWorldJDBC.jar and the BaseJar.jar are included in the Web Services .zip file downloaded from the MyOracleSupport website.

For details about the latest version supported for log4j, see Doc ID 2318897.1 in My Oracle Support. (WS: Instructions to Address JD Edwards World Security Vulnerabilities (Doc ID 2318897.1)(Release A9.3 Update)

18. Install the custom security authenticator into WebLogic server environment.

Copy the MJF (e.g. WorldAuthenticator.jar) to <WL_HOME>/server/lib/mbeantypes.

The WorldAuthenticator.jar file is included in the Web Services .zip file downloaded from the MyOracleSupport website.

Create WebSphere Application Server

This appendix contains the topic:

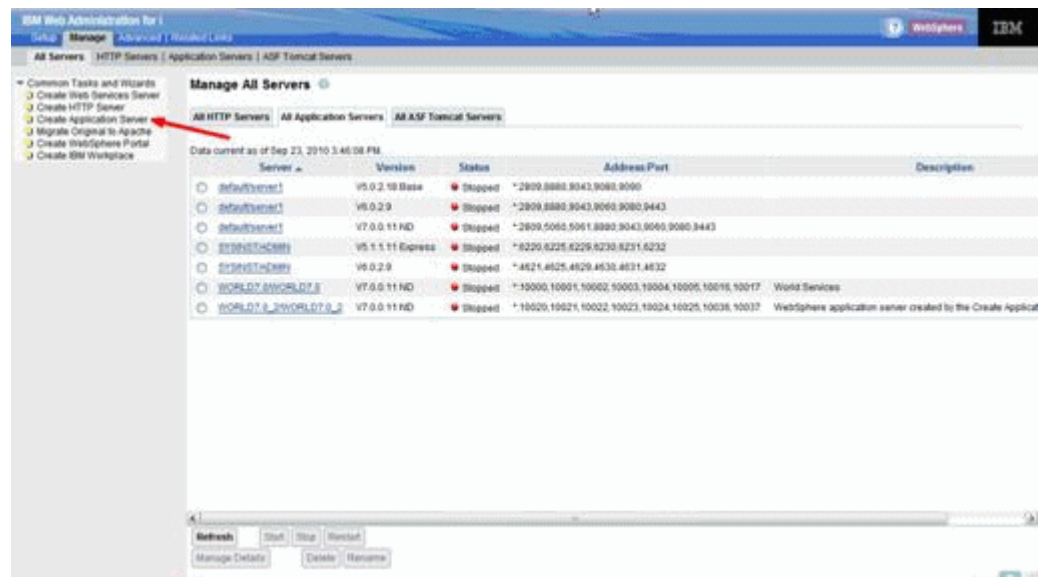
- [Section B.1, "Creating Application Servers in WebSphere."](#)

B.1 Creating Application Servers in WebSphere

To create Application Servers in WebSphere

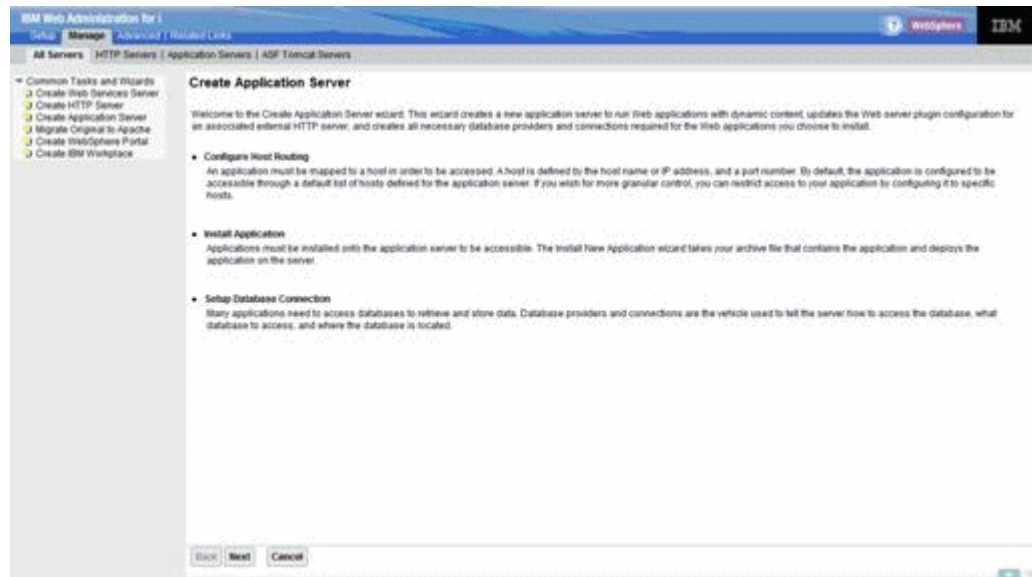
1. Launch the IBM Web Administrator for i: <http://localhost:2001/HTTPAdmin>

Figure B–1 Manage All Servers screen



2. Click Create Application Server.

Figure B–2 Create Application Server screen



3. Click Next.

Figure B–3 Create Application Server screen, Select Application Server and Type page



4. Select V7.0 ND and then click Next.

Figure B–4 *Create WebSphere Application Server screen, Specify Application Server Name page*

IBM Web Administration for i
Setup Manage Advanced Related Links
All Servers HTTP Servers Application Servers ADF Tomcat Servers

Common Tasks and Wizards
 Create Web Services Server
 Create HTTP Server
 Create Application Server
 Migrate Original to Apache
 Create WebSphere Portal
 Create IBM Workplace

Create WebSphere Application Server 7.0.0.11 ND
Specify Application Server Name

Specify a unique name for the application server.

Application server name: WORLDIT 8000

Server description: WebSphere application server created by the C...

Back Next Cancel

5. Enter Application Server Name and Description and then click Next.

Figure B–5 *Do Not Associate an External HTTP server ... Radio button*

IBM Web Administration for i
Setup Manage Advanced Related Links
All Servers HTTP Servers Application Servers ADF Tomcat Servers

Common Tasks and Wizards
 Create Web Services Server
 Create HTTP Server
 Create Application Server
 Migrate Original to Apache
 Create WebSphere Portal
 Create IBM Workplace

Create WebSphere Application Server 7.0.0.11 ND
Select HTTP Server Type

The application server may be associated with an external HTTP server. If selected, the wizard will set up the external HTTP server with the necessary information to route incoming URL requests to this application server.

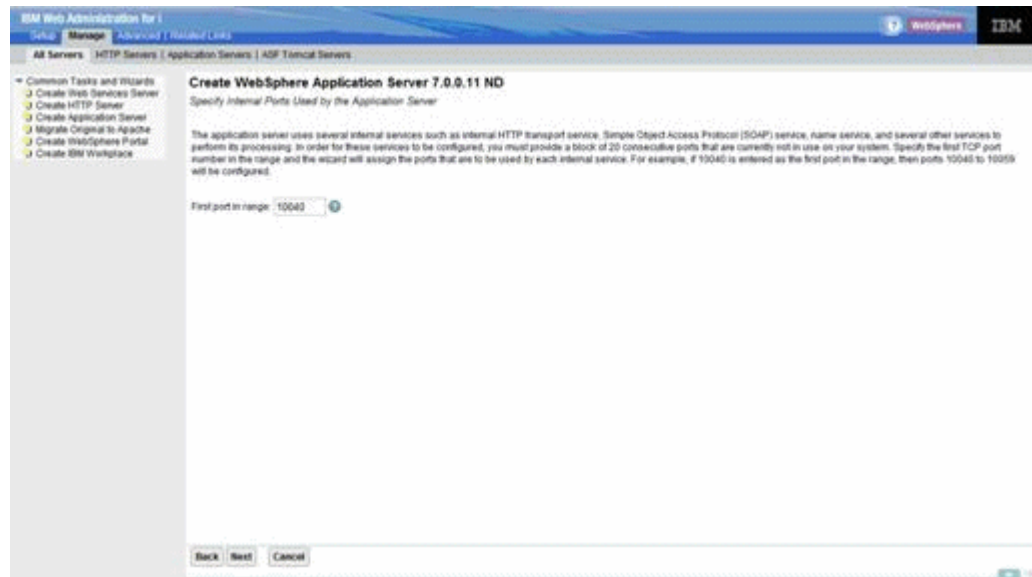
Choose the HTTP server type.

☐ Create a new HTTP server (powered by Apache)
☐ Select an existing HTTP server (powered by Apache)
☒ Do not associate an external HTTP server with this application server

Back Next Cancel

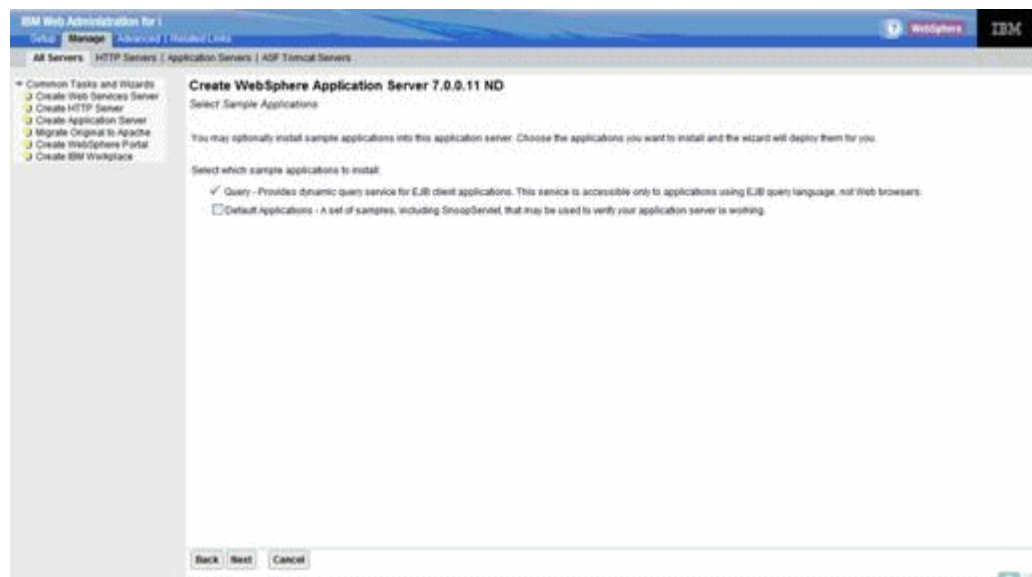
6. Select Do not associate an external HTTP server with this application server and then click Next.

Figure B–6 *Create WebSphere Application Server screen*



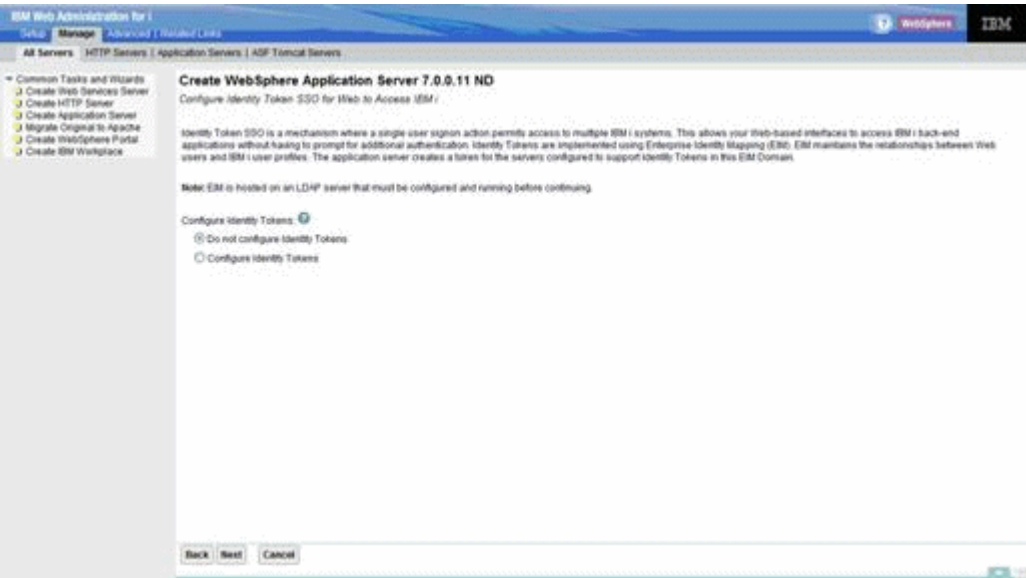
7. Click Next.

Figure B–7 *Create WebSphere Application Server screen, Sample Applications page*



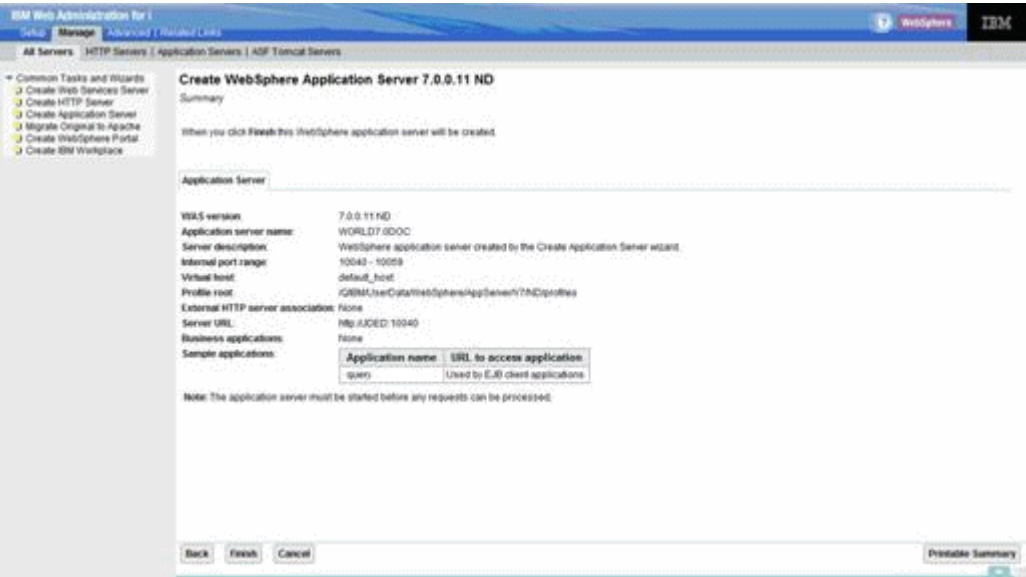
8. Click Next.

Figure B–8 Create WebSphere Application Server screen, Configure Identity Tokens page



9. Click Next.

Figure B–9 Create WebSphere Application Server screen, Summary page



10. Click Finish.

Code and Deploy your own Web Services

This appendix contains the topic:

- [Section C.1, "Coding and Deploying Your Own Web Services."](#)

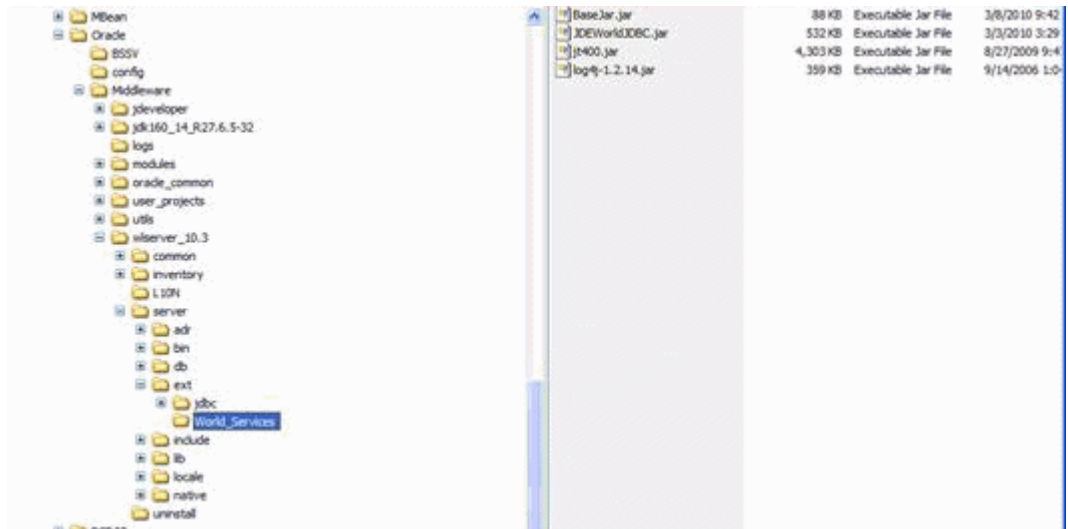
C.1 Coding and Deploying Your Own Web Services

To code and deploy your own Web Services

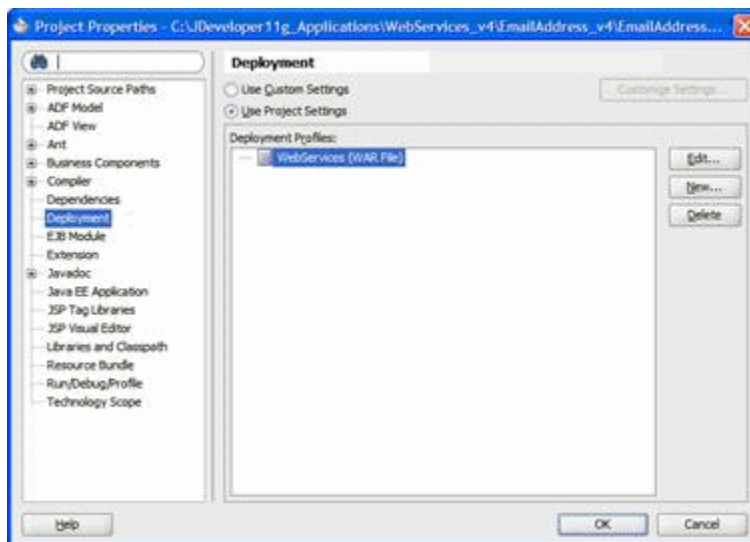
- Use the WebServiceBase_v4 and WebServiceBaseImpl_v4 classes to create custom web services
- Both classes exist in the BaseJar.jar file
- Extending one of the base classes (WebServiceBase_v4 and WebServiceBaseImpl_v4) gives you an RPGInvoke and Connection
- Use the RPGInvoke to call an RPG program on the JDEdwards World system
- Use the Connection to access the JDEdwards World database
- Extend WebServiceBase_v4 when creating services that only require executing a JD Edwards World program
- Extend WebServiceBaseImpl_v4 when creating a web service that requires database access
- Refer to the source zip file for examples on how to create web services using the BaseJar.jar file

Deployment Profiles

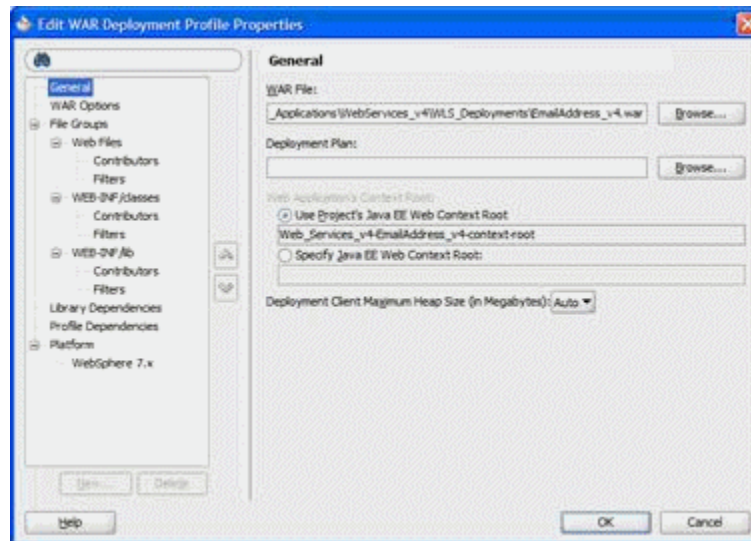
The jar files required for the Web Services were configured in the previous procedure by adding the jar files to the World_Services folder and setting the server classpath to include these jars.

Figure C–1 Location of World Services folder

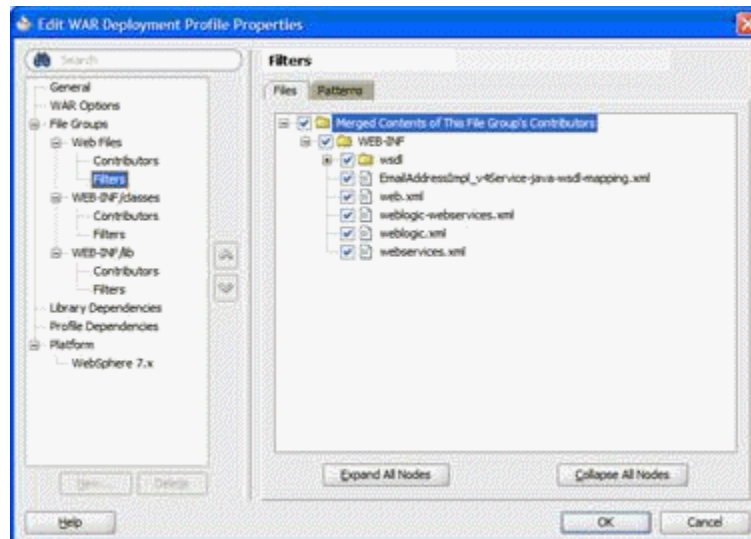
In JDeveloper, the individual projects only need to deploy those files that are required by the web service.

Figure C–2 Project Properties screen

1. Highlight WebServices(WAR File) and then click Edit.

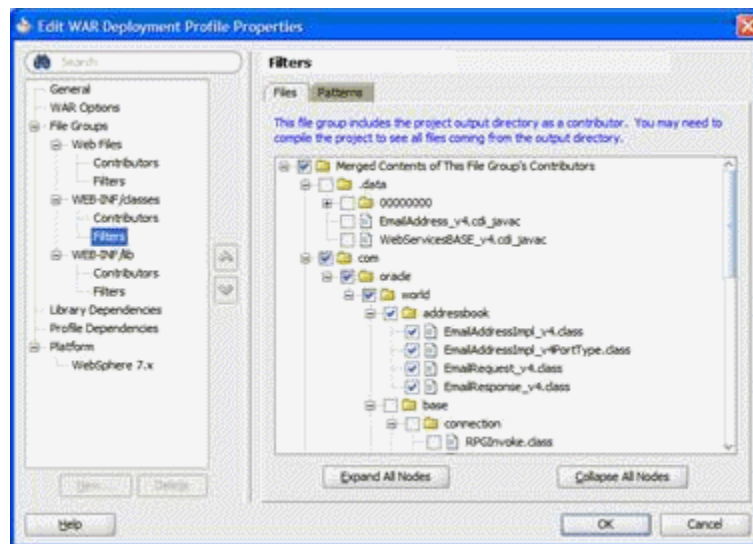
Figure C–3 Edit WAR Deployment Profile Properties screen, General page

2. Enter a path where you want your WAR file created.

Figure C–4 Edit WAR Deployment Profile Properties screen, Filtering tab

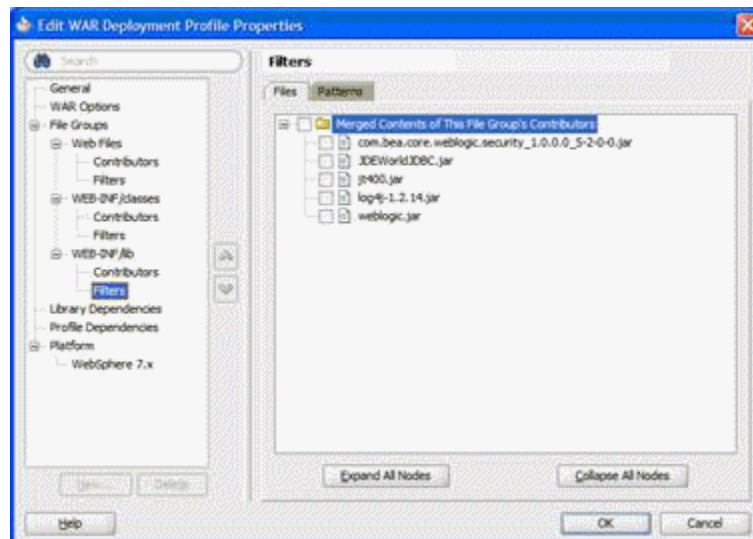
3. Under Web Files > Filters, select all files.

Figure C–5 *Edit WAR Deployment Profile Properties screen, Filter location in file structure*



4. Under WEB-INF/classes, only select the files specific to this service. The files under base are included in the BaseJar.jar, so they do not need to be included here.

Figure C–6 *Edit WAR Deployment Profile Properties screen Showing Merged Contents of the File folder*



5. Under WEB-INF/lib no classes should be selected, these jars are either part of the WLS install or were included in the server classpath in the installation instructions above.

Add Web Services to Oracle Enterprise Repository

This appendix contains these topics:

- [Section D.1, "Web Services Deployment and Java Documents Location Update,"](#)
- [Section D.2, "CAR XML Documents Builder."](#)

Follow the procedures in this appendix if you have purchased Oracle Enterprise Repository (OER) and you want to register your JD Edwards World Web Services in your OER instance. A batch import facility, Converged Application Repository (CAR), is provided in the JD Edwards World Service Enablement Software Update for importing the services into OER. See the *JD Edwards World Service Enablement Guide* for more information.

After you run the Software Update self-extracting archive file, you can access the WorldCARV1.zip file from the extract to location. The .zip file contains the CARv1 objects.

Unzip WorldCARV1.zip into the root directory, which creates the folder WorldCARV1. This folder contains the following objects:

- 58 xml documents contained in WorldCARv1.xml
- Source for the Java programs
- Commands and Java classes

To prepare the supplied xmls for the OER Harvester, refer to Web Services Deployment and Java Documents Location Update in this guide.

To register your own Web Services into OER:

- CAR XML documents builder
- Web Services deployment and java Documents location update

JD Edwards World Converged Application Repository (CAR) - Service Enablement XML documents.

D.1 Web Services Deployment and Java Documents Location Update

JD Edwards World CAR XML documents must be updated with the Web Services deployment and Java Documents location before being harvested by OER (Oracle Enterprise Repository).

CAR XML documents are updated through the execution (from MS Windows Command Prompt) of WorldCARLoc.bat command.

The system updates the following CAR XML document elements:

- Service location:

```
<LocationURL>#wsdeployment#/WorldServices-ServiceName_  
v4-context-root/ServiceNameImplPort?WSDL</LocationURL>
```

- Java Document location:

```
<Value>#javadocdeployment#\com\oracle\world\application\ServiceNameImpl.ht  
ml</Value>
```

Each token (Service: #wsdeployment# and Java Document: #javadocdeployment#) are replaced by the corresponding root location value.

Service root location

Replaced by the http address and port where the Services were deployed. For example:

```
http://localhost:7101
```

- XML <LocationURL> element after update:

```
<LocationURL>http://localhost:7101/WorldServices-ServiceName_  
v4-context-root/ServiceNameImplPort?WSDL</LocationURL>
```

Java Documents root location

Replaced by the directory path where the Java Documents were created. For example:

```
C:\JDeveloper11g_Applications\JavaDocTest\Javadoc
```

- XML <Value> element after update:

```
<Value>C:\JDeveloper11g_  
Applications\JavaDocTest\Javadoc\com\oracle\world\utilities\BatchCtrlImpl.html  
</Value>
```

WorldCARLoc.bat command execution

Note: Java Runtime Environment (JRE) 1.6 or higher is required. You can download the latest JRE version from:
<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

1. Create a backup copy of the CAR XML documents in a new directory/folder outside of the current CAR XML directory.
Use the backup in case the XML documents are updated with the wrong values.
2. Open MS Windows Command Prompt.
3. Access the WorldCARV1 directory:
CD\WorldCARV1 <Enter>
4. Execute WorldCARLoc.bat command:
WorldCARLoc "Drive:\CAR_XML_Documents_Directory" "Services_
Deployment_Address:Port" "Drive:\Java_Documents_Root_Path"
Where:

Drive:\CAR_XML_Documents_Directory: drive and directory where the CAR XML documents have been deployed.

Services_Deployment_Address:Port: http address where the Services have been deployed.

Drive:\Java_Documents_Root_Path: drive and directory path where the Java Documents have been created.

Note: Enter each one of the three parameters required separated by a blank character. For example: WorldCARLoc "C:\CARv1xml" "http://localhost:7001" "C:\JDeveloper11g_Applications\JavaDocTest\Javadoc"

5. Verify that all World CAR XML documents were properly updated. Execute the OER Harvester following OER Service Registry instructions.

D.2 CAR XML Documents Builder

You use the CAR XML documents builder to generate CAR XML documents to register customers Web Services (as part of JD Edwards World Service Enablement) in OER.

The Web Services information, contained in the CAR XML documents required by OER, is collected from custom Java Doc tags that need to be added to each Web Service that will be registered in OER.

Java Doc custom tags description

Note: The CAR XML documents builder collects information from Implementations and Managers classes. ("Impl" and "Manager" texts must be part of the source class name. For example, AddressBookImpl_v4.java

Update the Impl/Manager class with the following tags:

Web Service tags - must be entered before the class declaration statement.

@wsname: Web Service name.

@wsdesc: Web Service description.

@version: Web Service version.

@applname: Application name.

@prodcode: JD Edwards product code.

@applrelease: JD Edwards application release

@prodcodedesc: JD Edwards product code description

@wsdlurl: #wsdeployment# + deployment location

Note: #wsdeployment# token is not required if the deployment http address is entered as part of the URL.

Example:

```
/**
 * Description of AddressBook Impl Class
 *
 * @wsname Address Book
 * @wsdesc Web service for maintaining Address Book information.<BR>
 * @version v4
 * @applname JD Edwards World
 * @applrelease A9.2
 * @prodcode 01
 * @prodcodedesc Address Book
 * @wsdlurl #wsdeployment#/Web_Services_v4-AddressBook_
v4-context-root/AddressBookImpl_v4Port?WSDL
 */
```

Exposed/public methods tags must be entered before each exposed/public method declaration:

@pubmethodname: public method name

@pubmethoddesc: public method description

Example:

```
/**
 * This method retrieves Address Book records by querying the Address Book
 * Master (F0101) and related files.
 * @param getRequest - Structure containing input values.
 * @return AddressBookResponse_v4 - Structure containing output values.
 * @pubmethodname getAddressBook
 * @pubmethoddesc This method retrieves Address Book records by
 * querying the Address Book Master(F0101) and related files.<BR>
 */
```

General Rules

- Enter the text associated to each tag leaving two blank characters, between the tag and the text.
- Java Doc custom tags can be used together with Java standard Java Doc tags as for example @param.
- Description tags (@wsdesc and @pubmethoddesc) require "
" (break a line) tag at the end of the entire description. If more the one line of text is needed, the text can be wrapped in the next line(s).
- Execute CAR XML Builder:

After all custom tags have been added to the Web Services execute WorldCARXMLB.bat command to build CAR XML documents. This process generates

one XML document for each Web Service (Impl/Manager class) to be registered in OER.

- Open MS Windows Command Prompt.
- Access the WorldCARV1 directory:

CD\WorldCARV1 <Enter>

- Execute WorldCARXMLB.bat command:

```
WorldCARXMLB "Drive:\Web_Services_Source_Directory" "Drive:\CAR_XML_Documents_Directory"
```

Where:

Drive:\Web_Service_Source_Directory: drive and directory location of Web Services sources. Only the parent directory needs to be specified. For example specifying "C:\Services" will traverse all subdirectories to retrieve source files.

Drive:\CAR_XML_Documents_Directory: drive and directory where the XML documents will be created. If the directory doesn't exist it will be created.

Note: Enter both parameters required separated by a blank character.

After, you verify that all XML documents were properly created, execute the command described in the Web Services deployment and Java Documents location update section of this document.

Uninstall Service Enablement

This appendix contains the topic:

- [Section E.1, "Uninstalling Service Enablement."](#)

E.1 Uninstalling Service Enablement

E.1.1 Oracle Universal Installer (OUI)

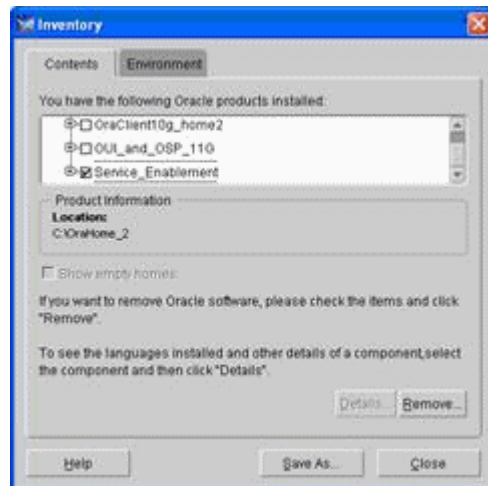
If you need to uninstall JD Edwards World Service Enablement, use the OUI installer.

Figure E–1 Oracle Universal Installer Welcome screen

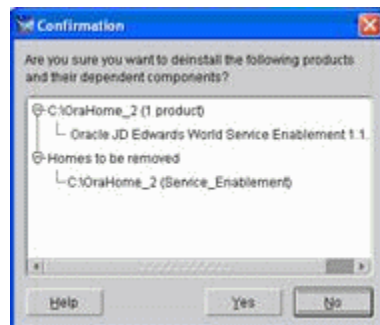


1. Start the OUI installer.

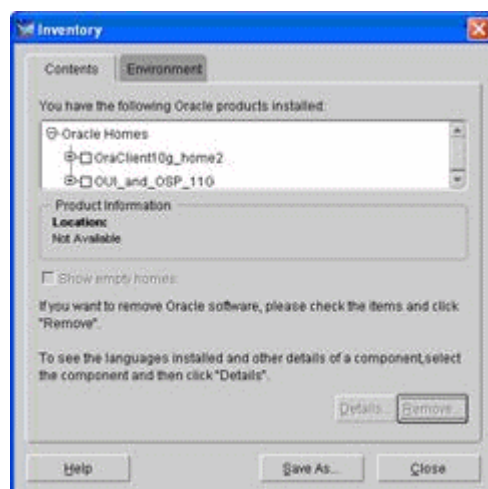
Run `Disk1\oui\bin\setup.exe` and click **Deinstall Products** on the Welcome screen.

Figure E–2 Inventory window

2. Select the checkbox of the Service Enablement folder name you created and then click Remove.

Figure E–3 Confirmation screen

3. On the Confirmation screen, click Yes.

Figure E–4 Inventory screen

4. On the Inventory screen, click Close.

Figure E-5 End of Installation screen

5. On the End of Installation screen, click Exit.

Figure E-6 Exit window

6. On the Exit screen, click Yes.

