JD Edwards World

Service Enablement Installation and Configuration Guide

Release A9.4

E58797-03

April 2021

Describes how to install and configure JD Edwards World Service Enablement.

ORACLE

JD Edwards World Service Enablement Installation and Configuration Guide, Release A9.4

E58797-03

Copyright © 2015, 2021, Oracle and/or its affiliates.

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 embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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 Inside 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, Epyc, and the AMD 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 Information v
Conventions v

Part I Overview and Service Enablement Installation

1 Overview

2 Install Service Enablement

2.1 Installing Service Enablement 2-1

Part II Deploy and Configure Web Services

3 About Deploying and Configuring Web Services

4 Configure the WebLogic Application Server

4.1 Configuring the WebLogic Application Server 4-1

5 Configure the WebSphere Application Server

5.1 Configuring the WebSphere Application Server for World JAX-WS Web Services 5-1
5.2 Create an Application Server 5-1
5.3 Set Up a Shared Library 5-1
5.4 Set Server Heap Size 5-3
5.5 Configure Application Security 5-6
5.6 Set Up Policies and Bindings 5-12
5.7 Deploy Services 5-23

A Install WebLogic Application Server

A.1 Installing the WebLogic Application Server A-1

B Create WebSphere Application Server

B.1 Creating the WebSphere Application Server B-1

C Code and Deploy Your Own Web Services

C.1 Coding and Deploying Your Own Web Services C-1
C.2 Deployment Profiles C-1

D Uninstall Service Enablement

D.1 Uninstalling Service Enablement D-1

Preface

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

Audience

This document is intended for implementers and end users of JD Edwards World Web Enablement Services.

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 Information

For additional information about JD Edwards World applications, features, content, and training, visit the JD Edwards World pages on the JD Edwards Resource Library located at:

http://learnjde.com

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Indicates cautionary information or terms defined in the glossary.
italic	Indicates book titles or emphasis.

Part I

Overview and Service Enablement Installation

This part contains these chapters:

- Chapter 1, "Overview,"
- Chapter 2, "Install Service Enablement."

1

Overview

Thank you for ordering JD Edwards World 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.

See the *JD Edwards World Service Enablement Guide* for 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.

2

Install Service Enablement

This chapter contains the topic:

- Section 2.1, "Installing Service Enablement."

2.1 Installing Service Enablement

To install Service Enablement

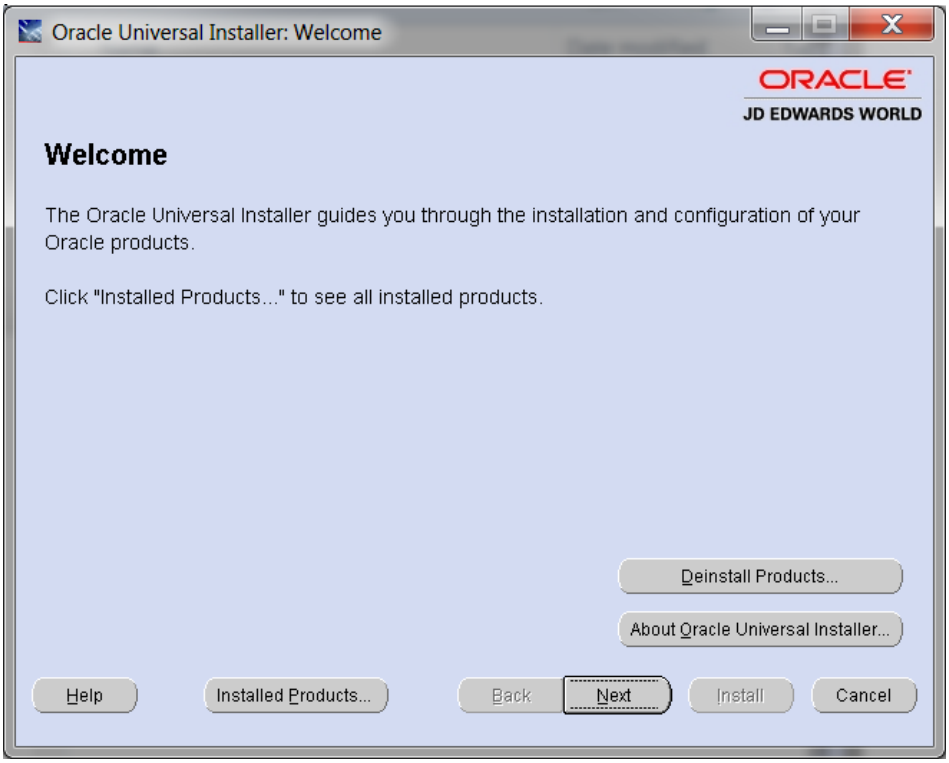
1. Download and unzip the service enablement archive file.

   The download is available via the Update Center.

   Start the Oracle Universal Installer (OUI) by running:

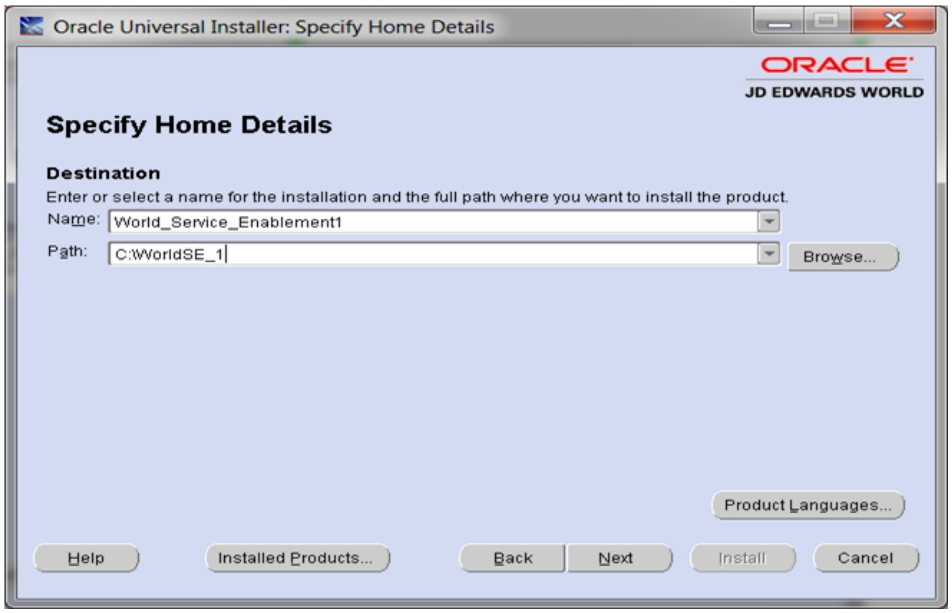
   Disk1\oui\bin\setup.exe from the extract location

Figure 2–1 Oracle Universal Installer: Welcome screen



2. On the Welcome screen, click Next.

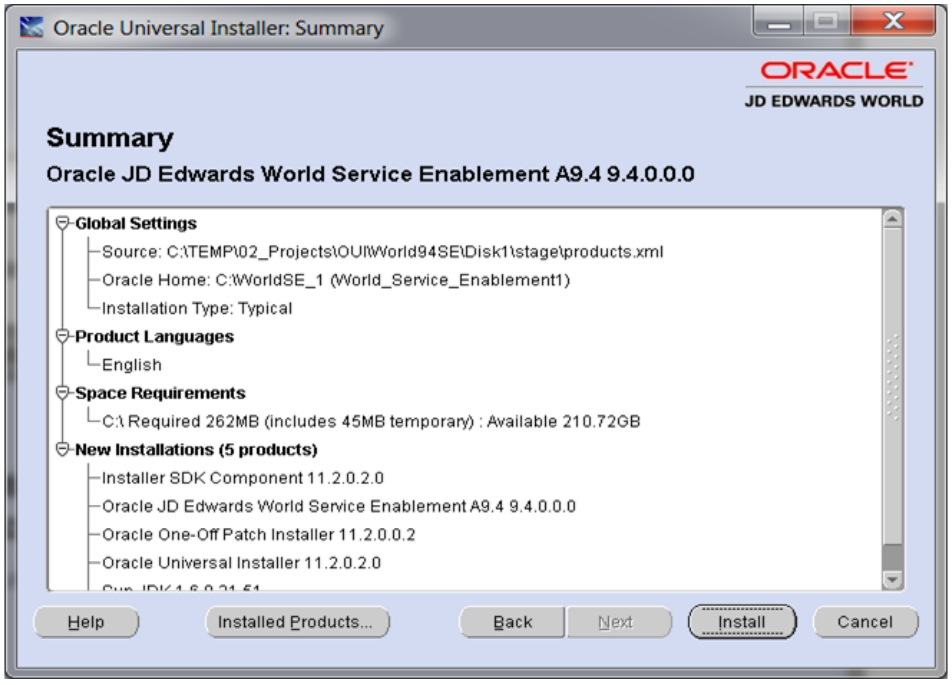
Figure 2–2 Specify Home Details screen



3. On the Specify Home Details screen, enter a folder Name and Path for your installation.

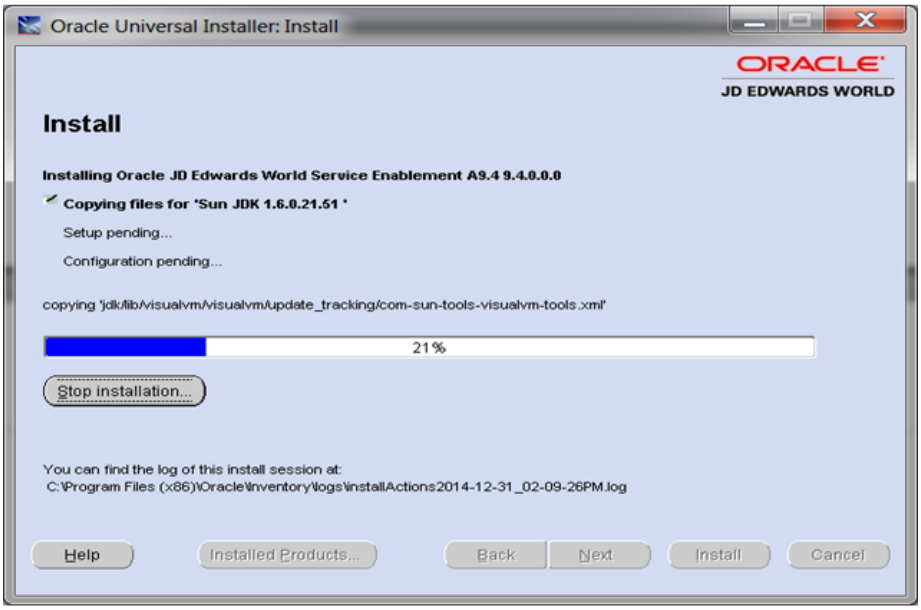
   JD Edwards World recommends that you retain the OraHome name in some form for your path directory. Using the OraHome name is an Oracle convention that facilitates consistent directory names among Oracle product installations.

Figure 2–3 Summary screen



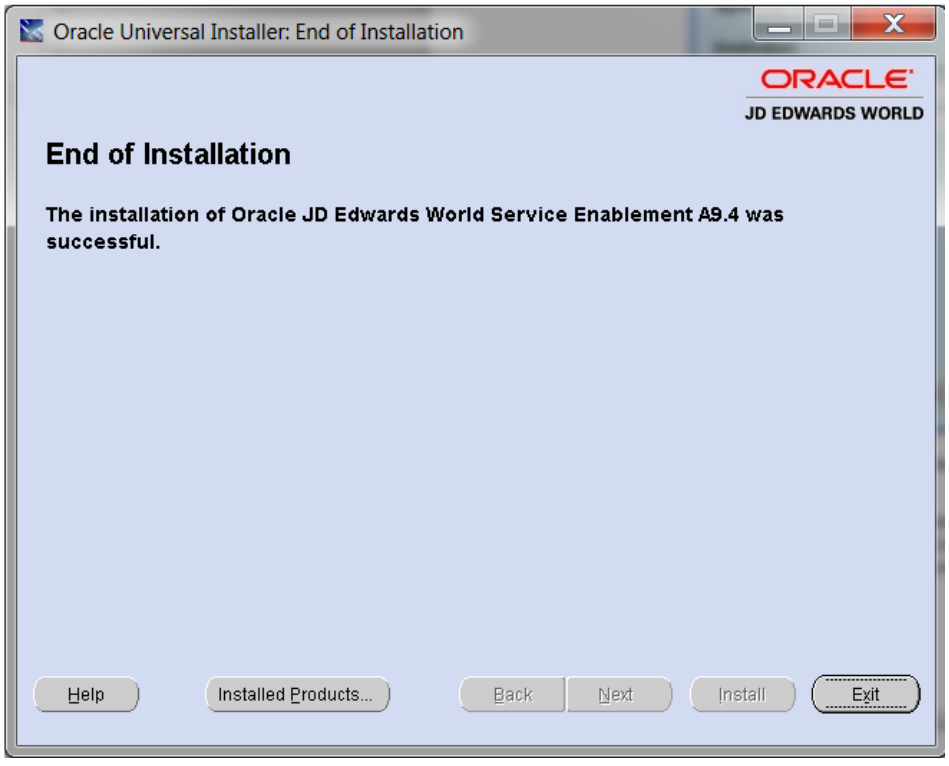
4. On the Summary screen, click Install.

Figure 2–4 Install screen



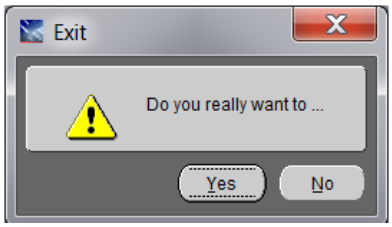
The Install screen displays the Setup in progress.

Figure 2–5 End of Installation screen



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

Figure 2–6 Exit screen



6. On the Exit screen, click Yes.

Part II

Deploy and Configure Web Services

This part contains these chapters:

- Chapter 3, "About Deploying and Configuring Web Services,"
- Chapter 4, "Configure the WebLogic Application Server,"
- Chapter 5, "Configure the WebSphere Application Server."

3

About Deploying and Configuring Web Services

You must deploy the World Web Service EAR file to a WebLogic or WebSphere application server. All necessary Java security setup occurs after deployment.

The following chapters contain specific deployment and security setup instructions for:

- WebLogic Application Server
- WebSphere Application Server

> **Note:** Make sure you have installed and configured the application server before deploying the EAR file.

4

Configure the WebLogic Application Server

This chapter contains the topic:

- Section 4.1, "Configuring the WebLogic Application Server."

4.1 Configuring the WebLogic Application Server

Before you begin, see the World specific steps outlined in Appendix A, "Install 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"

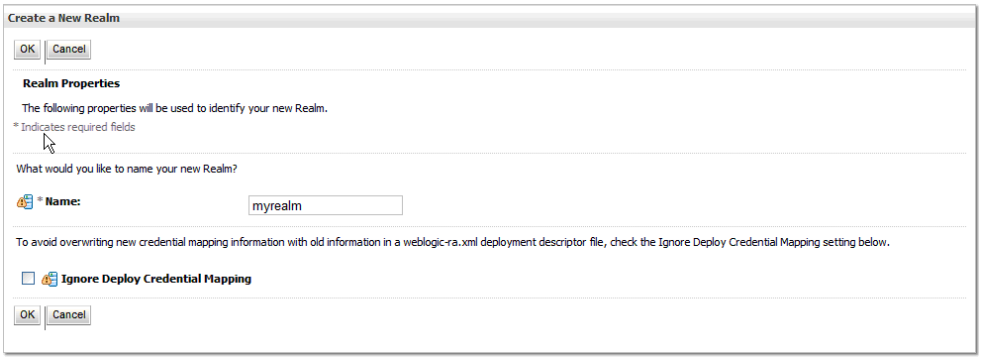
2. Launch the application server console.

   http://localhost:7001/console

3. From WebLogic console select Security Realms to create a Security Realm.

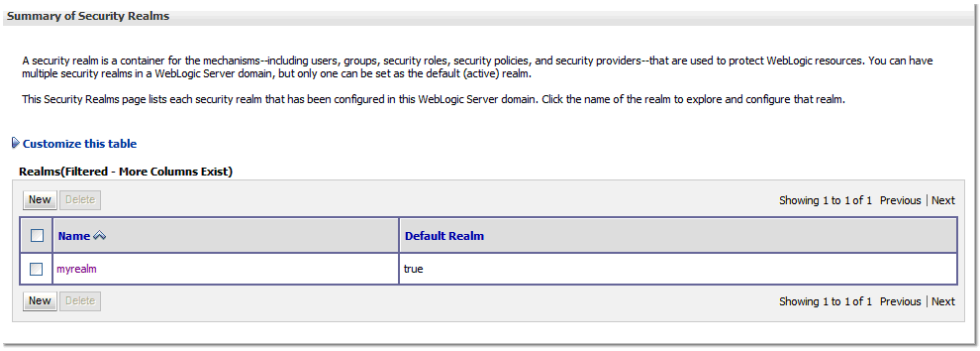
   Click New.

Figure 4–1 Create New Realm screen



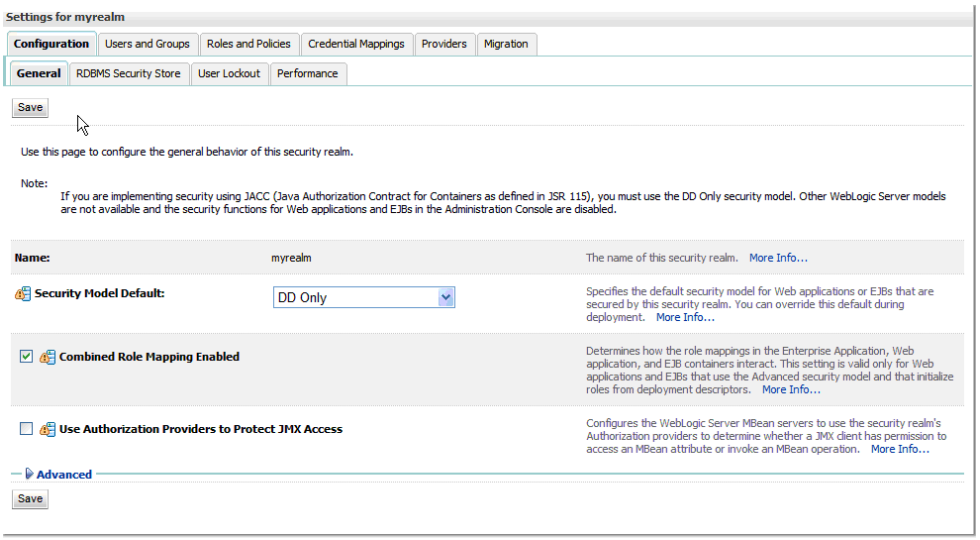
4. Enter a Realm Name and then click OK.

Figure 4–2 Summary of Security Realms screen



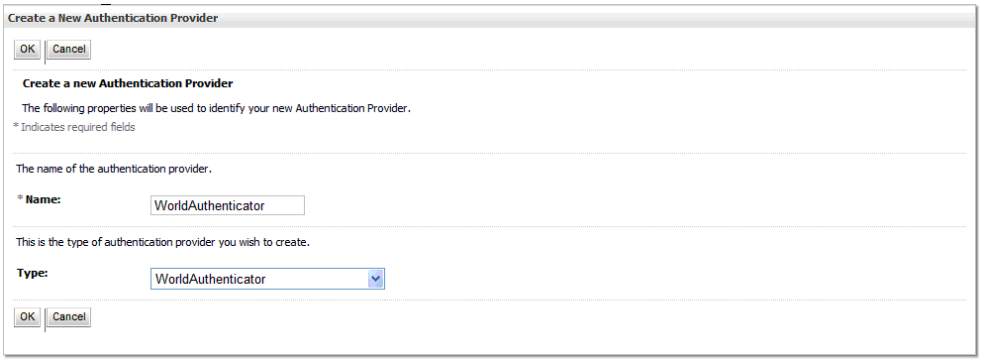
5. Click New to create a realm.

Figure 4–3 Settings for myrealm screen



6. Select the Providers tab and then click New.

Figure 4–4 Create a New Authentication Provider screen

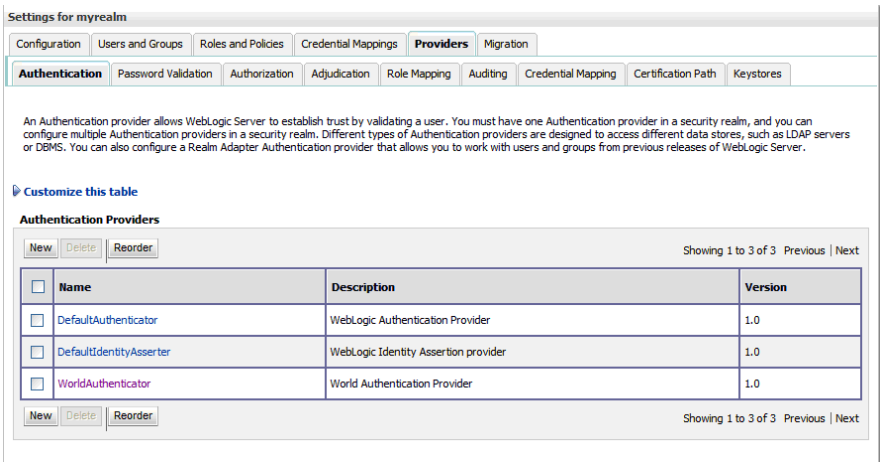


7. Enter the Name and select the Type WorldAuthenticator from the dropdown list. (If the WorldAuthenticator is not listed, review steps 18 and 19 of Appendix A, "Install WebLogic Application Server.")

Click OK.

The WorldAuthenticator displays as one of the Authentication Providers.

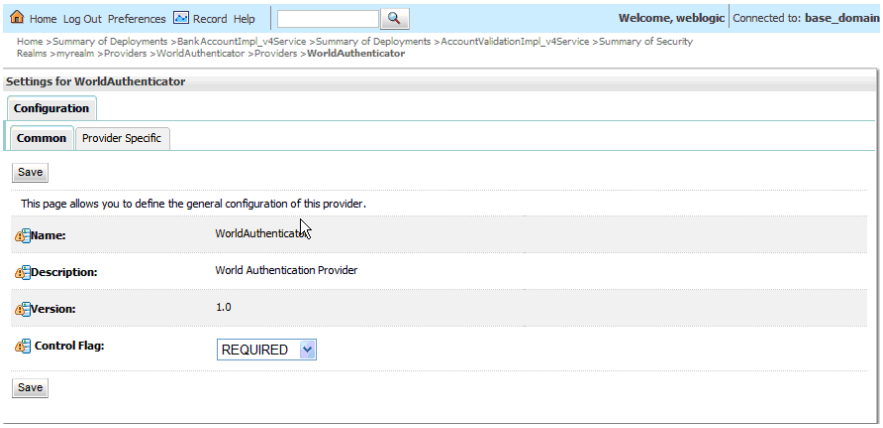
Figure 4–5 Settings for myrealm screen



Make sure the WLS DefaultAuthenticator is before the WorldAuthenticator.

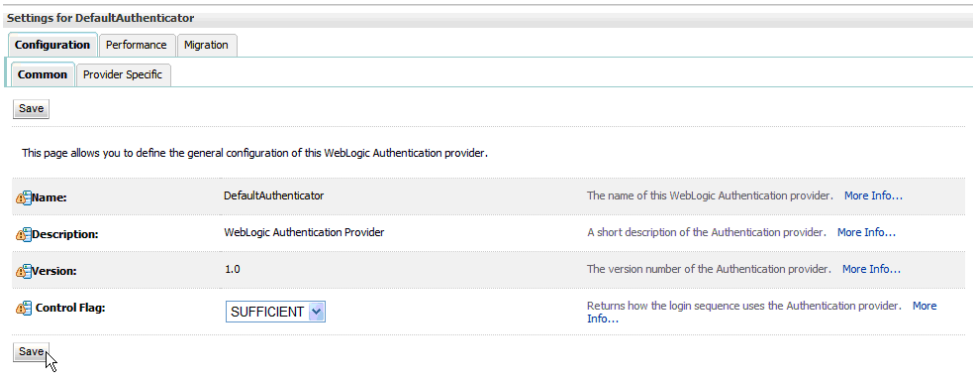
8. Click the WorldAuthenticator link.

Figure 4–6 Settings for World Authenticator screen



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

Figure 4–7 Settings for Default Authenticator screen



From WebLogic console select Security Realms. Then select the Security Realm (the exsisting or created one), and then select Providers.

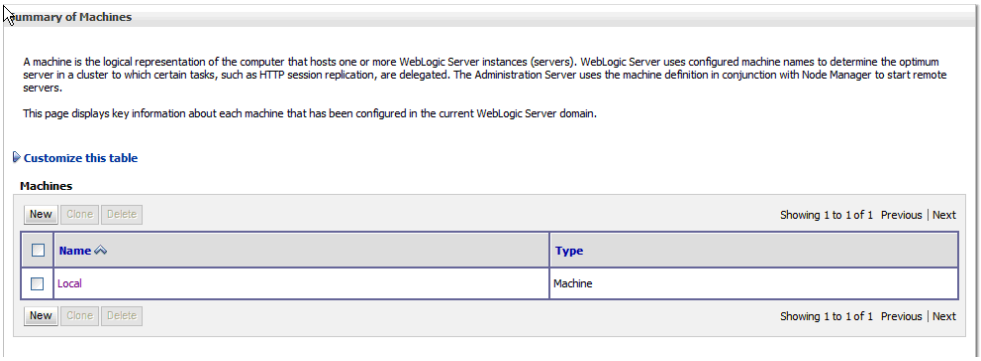
10. Select the DefaultAuthenticator link, and change the Control Flag of the DefaultAuthenticator to SUFFICIENT.

    Click Save.

11. Create a machine using default values.

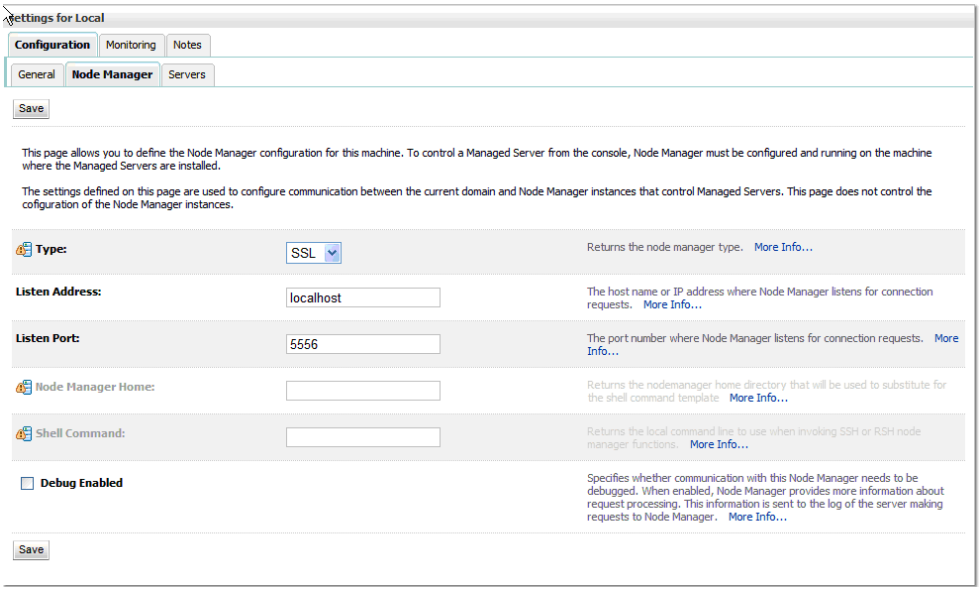
    http://localhost:7001/consolehelp/console-help.portal?_nfpb=true&_pageLabel=page&helpId=machines.ConfigureMachines

Figure 4–8 Summary of Machines screen



12. Select Local Machine.

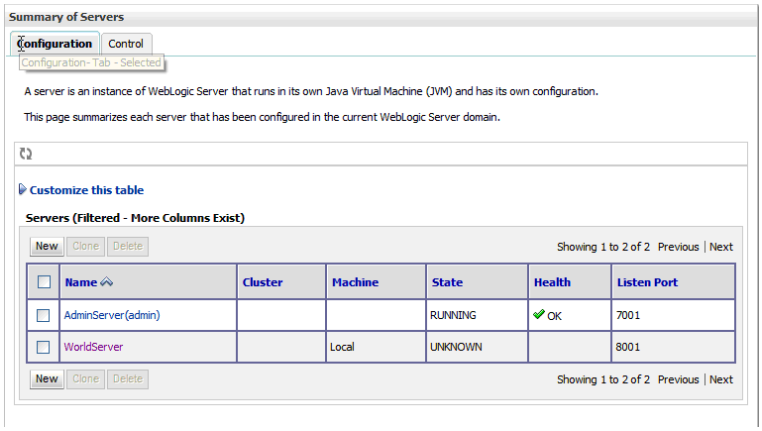
Figure 4–9 Settings for Local screen



13. Create a managed server for the Web Services.

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

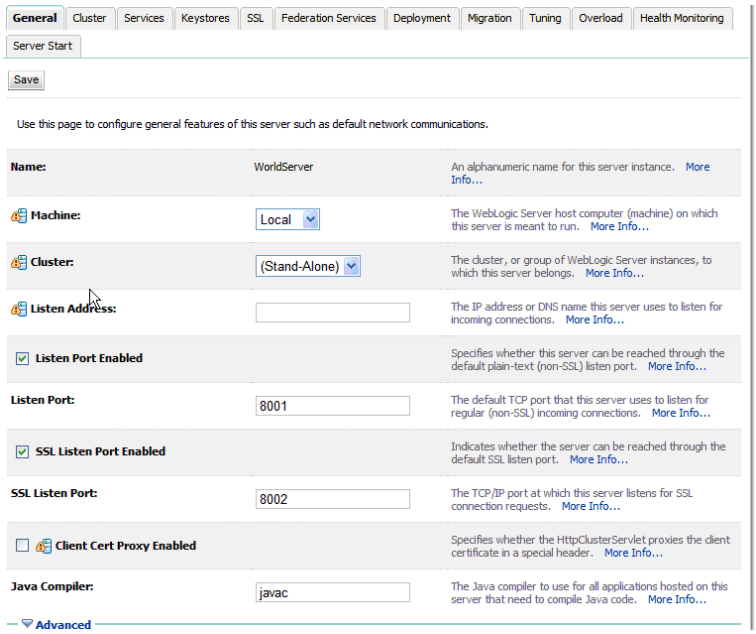
Figure 4–10 Summary of Servers screen



14. Select WorldServer.

Set Machine to machine configured in step 12.

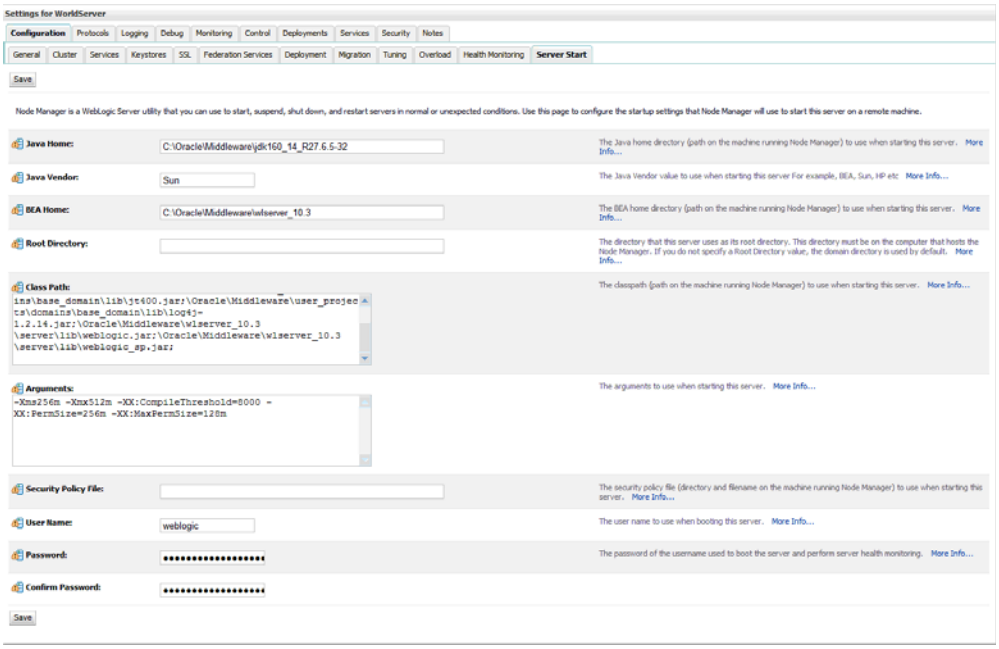
Figure 4–11 Server Start screen



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 4–12 Settings for World Server screen



- 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;

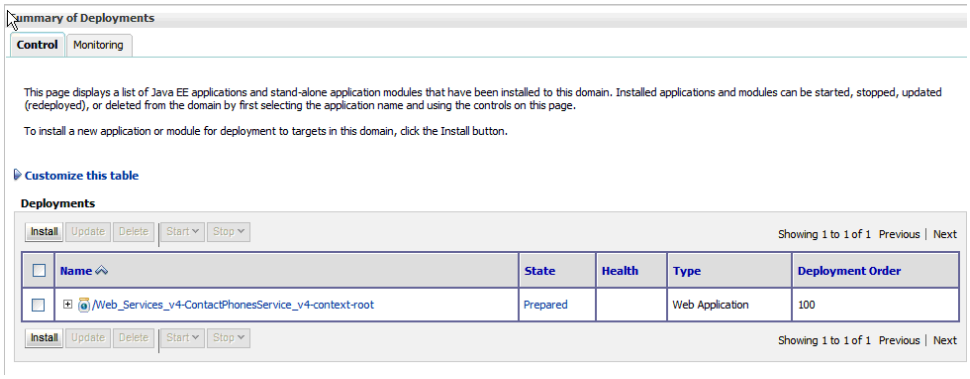
  Note: For details about the latest version supported for log4j, see Doc ID 2318897.1 in My Oracle Support. (WS: Instructions to Address JD Edwards World Security Vulnerabilities (Doc ID 2318897.1) (Release A9.4 Update)

- Arguments:

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

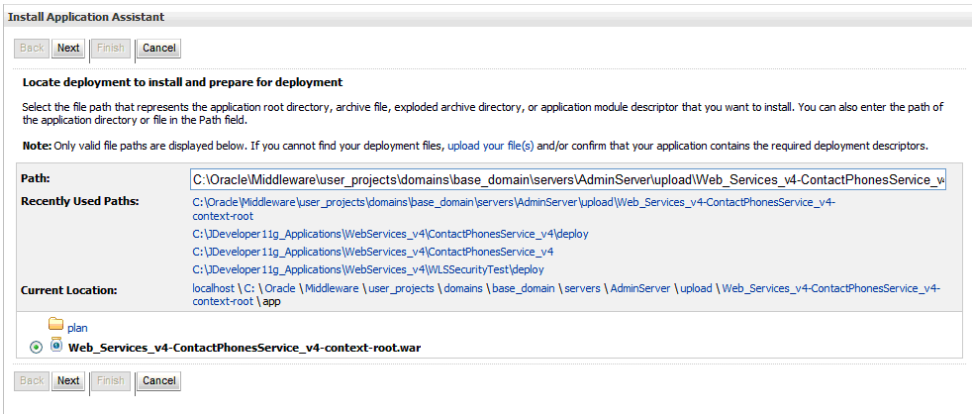
15. Deploy Services to managed server On Server Console, select Deployments.

Figure 4–13 Summary of Deployments screen



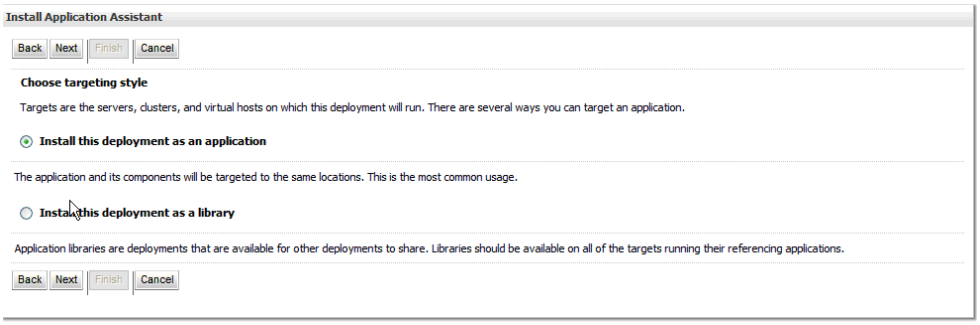
16. Click Install.

Figure 4–14 Install Application Assistant screen



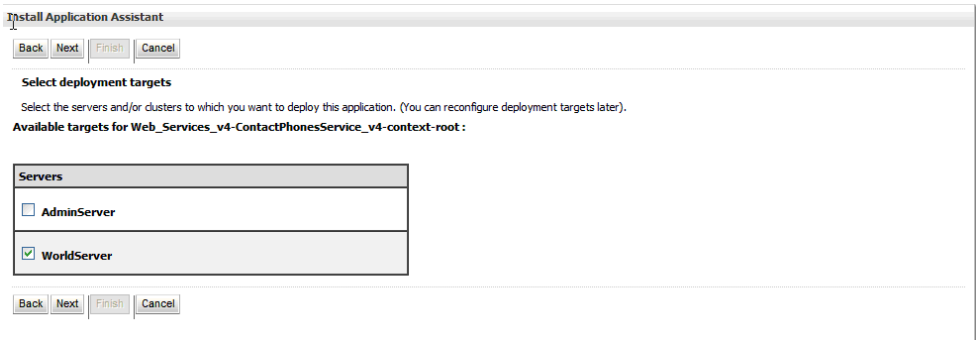
17. Locate service WAR file (WebServices_xx_WLS.ear) and then click Next.

Figure 4–15 Install Application Assistant screen



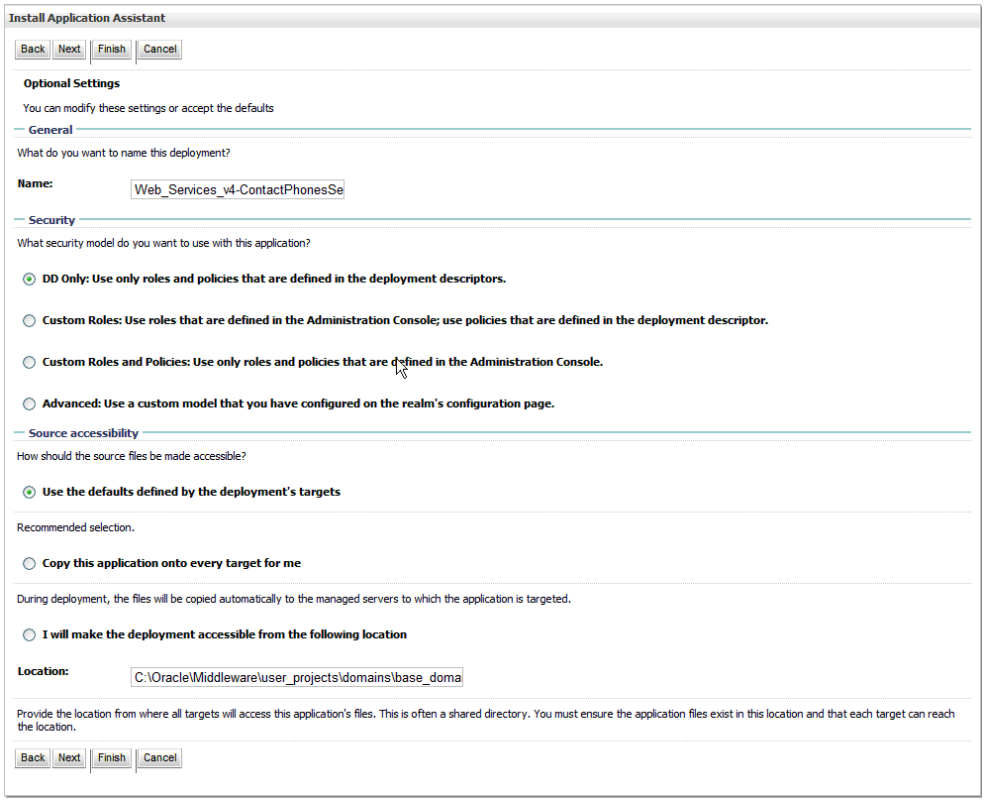
18. Select Install this deployment as an application and then click Next.

Figure 4–16 Install Application Assistant screen



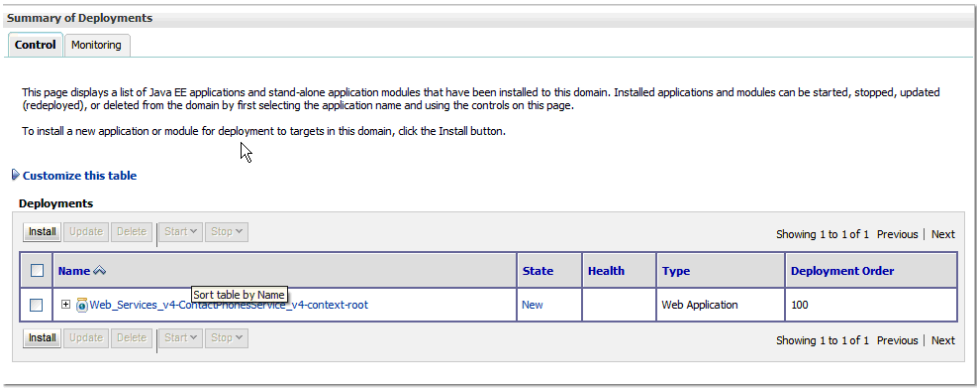
19. Verify the managed server you created earlier, and click Next.

Figure 4–17 Install Application Assistant screen



20. Click Finish.

Figure 4–18 Summary of Deployments screen



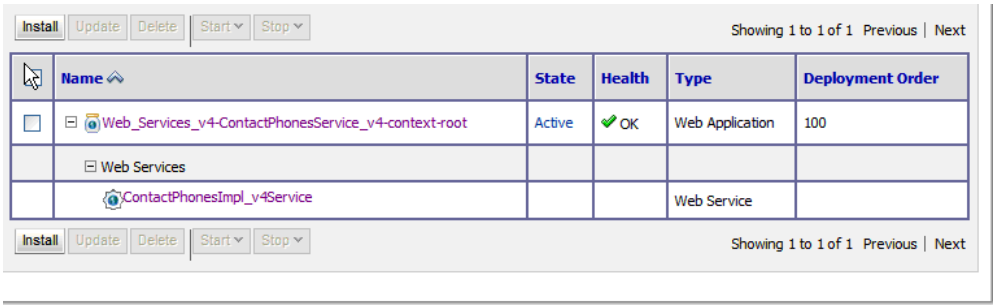
The Summary of Deployments displays your service.

21. Configure security for service (the service must be Active/Started).

22. From the Deployments screen, expand the service you want to secure.

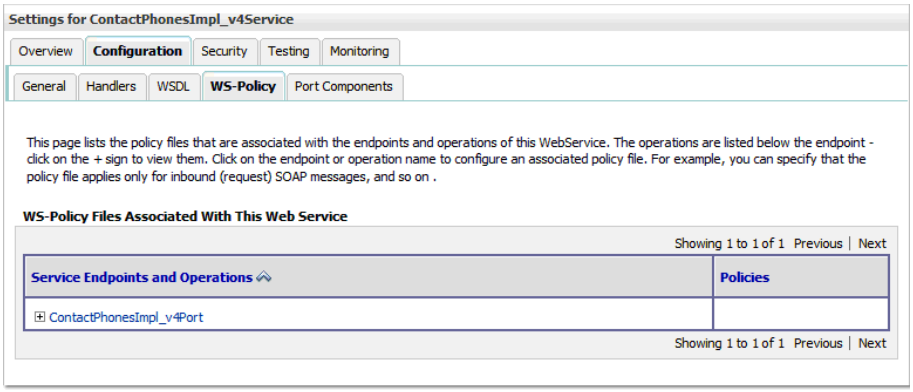
Collapse the Modules and EJBs nodes and then select the service you want to secure (for example: AddressBookImpl_v4Service).

Figure 4–19 Summary of Deployments screen



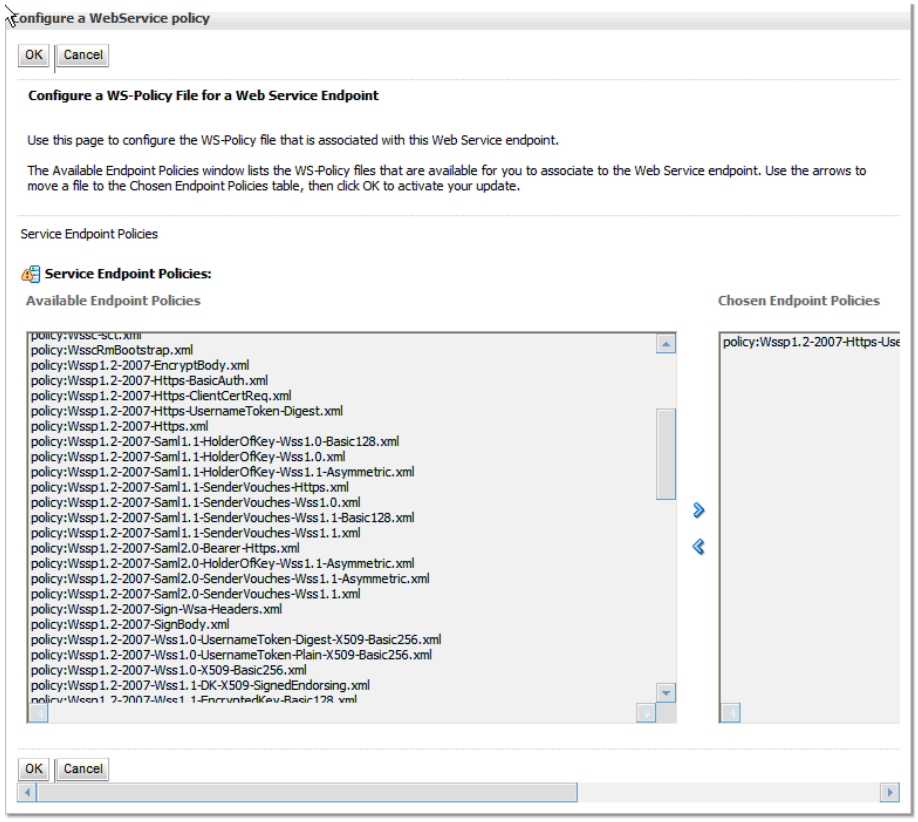
23. Select the web service and then select the Configuration-> WS-Policy tab.

Figure 4–20 Settings for WS-Policy tab



24. Select the option **WebLogic** on the **Configure the Policy Type for a Web Service** screen and select Next.

Figure 4–21 Configure a WebService policy screen



25. Select:

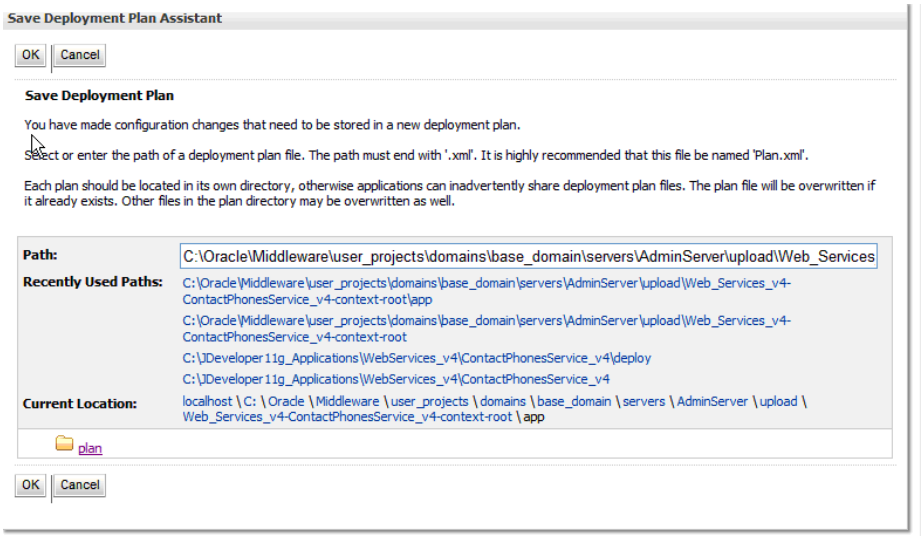
policy:Wssp1.2-2007-Https-UsernameToken-Plain.xml

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 4–22 Save Deployment Plan Assistant screen



Restart the server.

Access the WSDL.

From the Home Weblogic screen, select Deployments, then Expand Web Services. Select the Web Service Secured in Step 23. Select the Testing tab then Expand the service. Select ?WSDL under Test Point. The service WSDL will open in a browser window. Copy the URL (WSDL) and paste into testing application. Remember to use SSL and the Secure port (listed in Step 14).

26. Test services.

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; replace <soapenv:Header/> with the following lines:

```
<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>
```

5

Configure the WebSphere Application Server

This chapter contains these topics:

- Section 5.1, "Configuring the WebSphere Application Server for World JAX-WS Web Services,"
- Section 5.2, "Create an Application Server,"
- Section 5.3, "Set Up a Shared Library,"
- Section 5.4, "Set Server Heap Size,"
- Section 5.5, "Configure Application Security,"
- Section 5.6, "Set Up Policies and Bindings,"
- Section 5.7, "Deploy Services."

5.1 Configuring the WebSphere Application Server for World JAX-WS Web Services

Since Release A.9.3.1, the World Web Services were updated to use the Java API for XML Web Services (JAX_WS). In order to run these services on WebSphere Application Server, there are specific release levels and configuration steps that need to be used.

The functionality for the JAX-WS services requires PM70894, which ships in versions 7.0.0.27, 8.0.0.6, and 8.5.0.2 of WebSphere. If this functionality is required for a earlier release of WebSphere, you will need to contact your IBM representative to check on the availability of an ifix for your specific version.

Please refer to the certification information on myoraclesupport.com to determine the versions of WebSphere currently certified.

5.2 Create an Application Server

- See Appendix B, "Create WebSphere Application Server" in this guide.

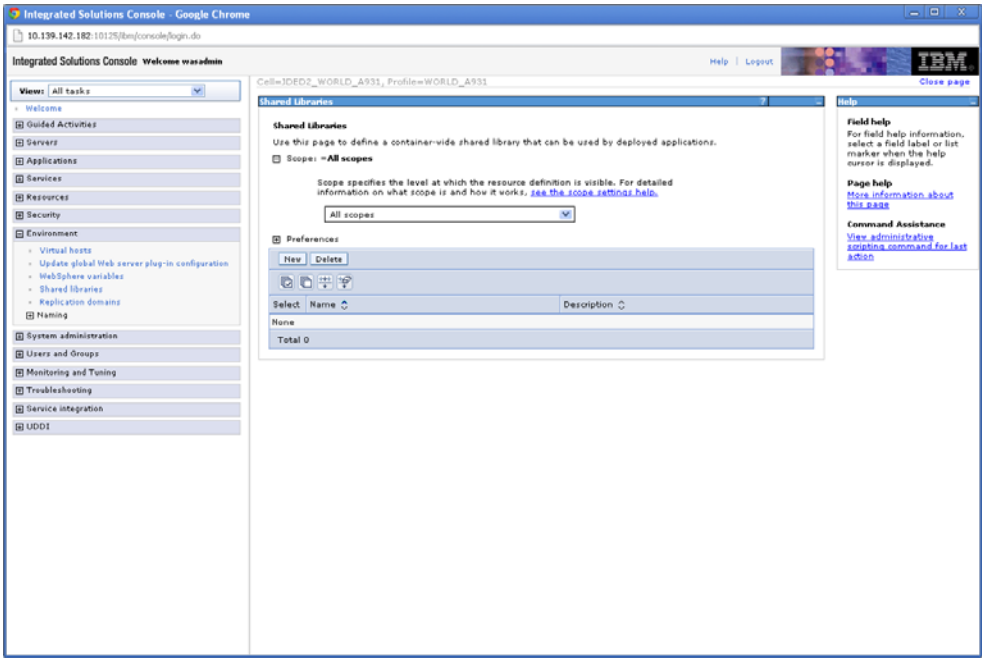
5.3 Set Up a Shared Library

The jt400.jar file needs to be set up in a shared library so that the web services process can authenticate a user. The jt400.jar can be downloaded and saved to an IFS folder.

To set up a shared library

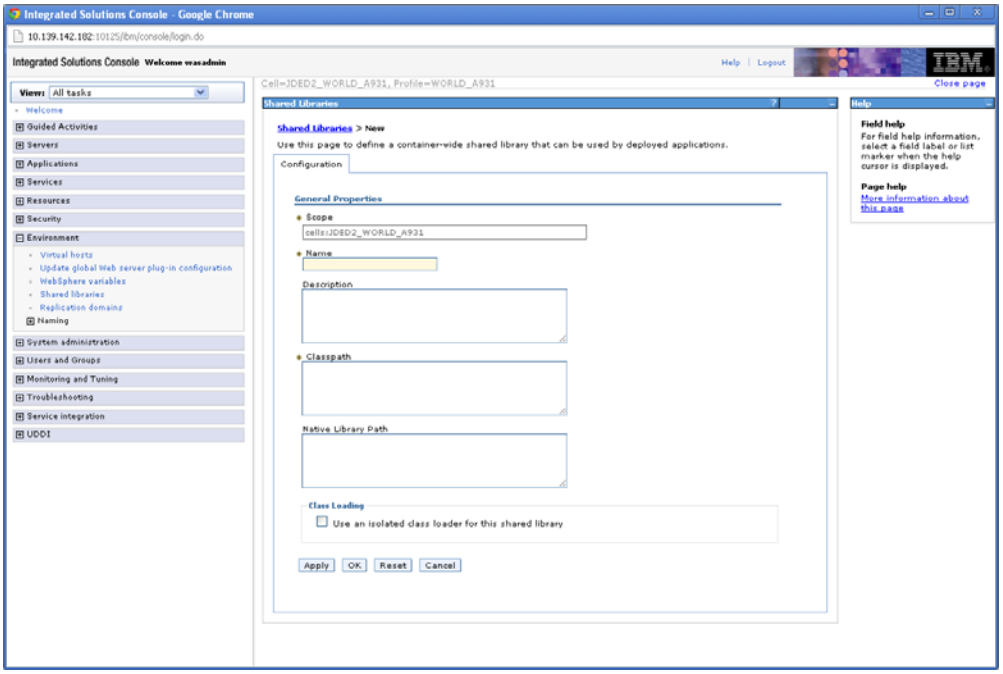
1. Access the WebSphere Integrated Solutions Console and select **Environment->Shared libraries**.

Figure 5–1 Shared Libraries screen



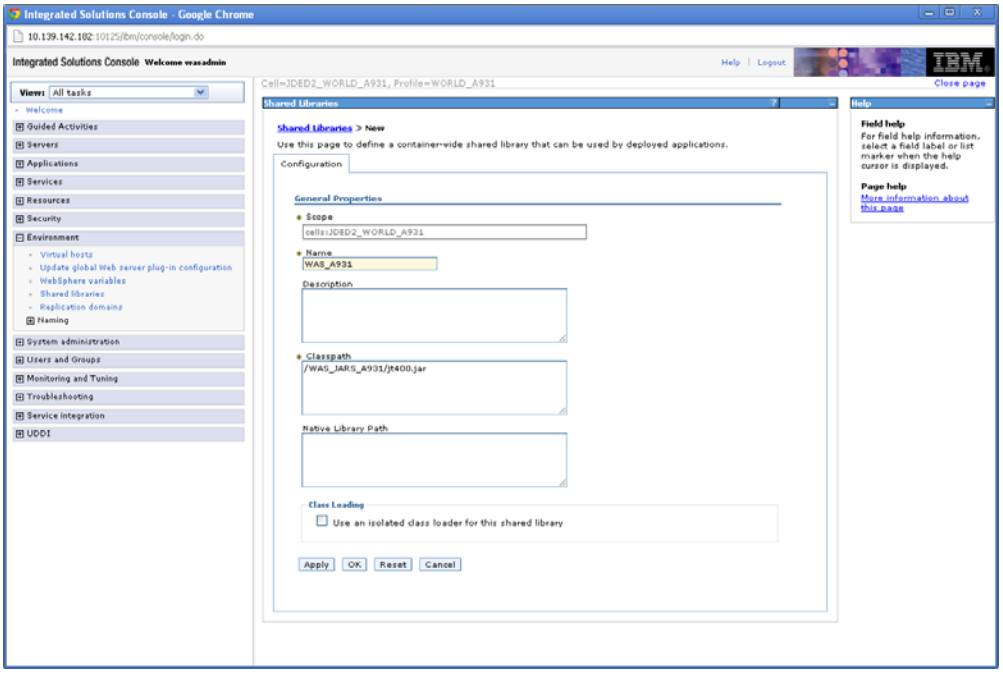
2. Select a scope from the drop-down and then click New.

Figure 5–2 Shared Libraries screen



Enter "WAS_A931" in the Name field, and for the classpath, enter "/path," where jt400 is saved as "/jt400.jar."

Figure 5–3 Shared Libraries screen



Click OK.

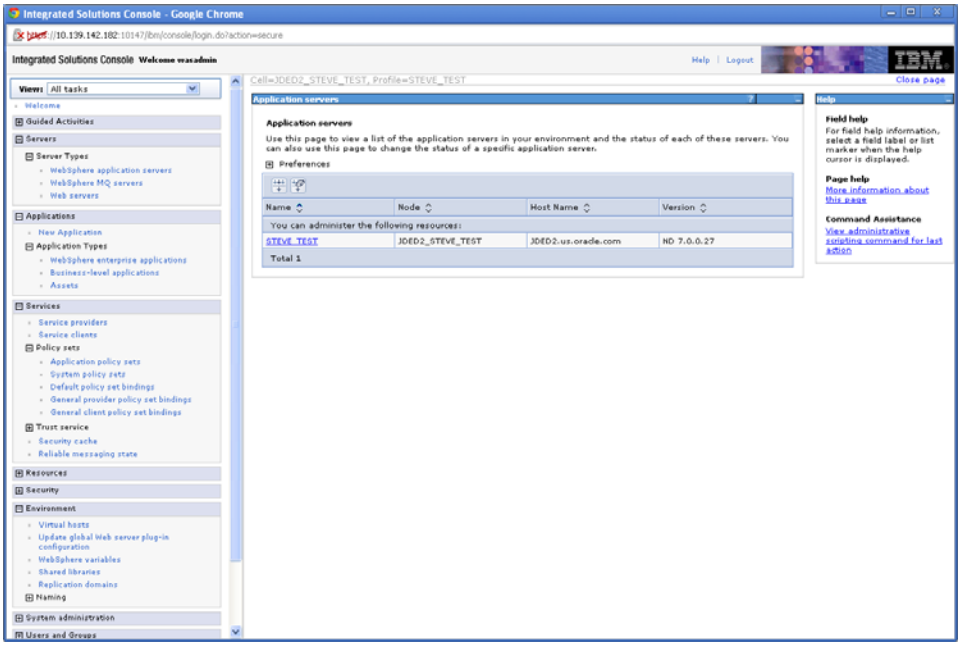
Click Save.

5.4 Set Server Heap Size

To set server heap size

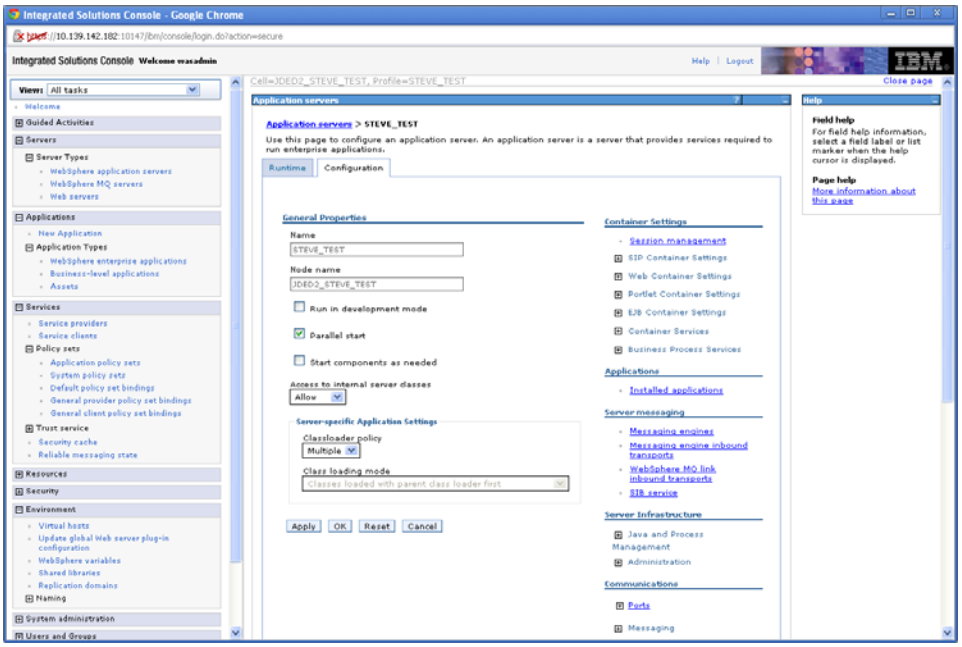
1. From the WebSphere Integrated Solutions Console, select **Servers_>Server Types_ >WebSphere application servers**.

Figure 5–4 WebSphere Application Servers screen



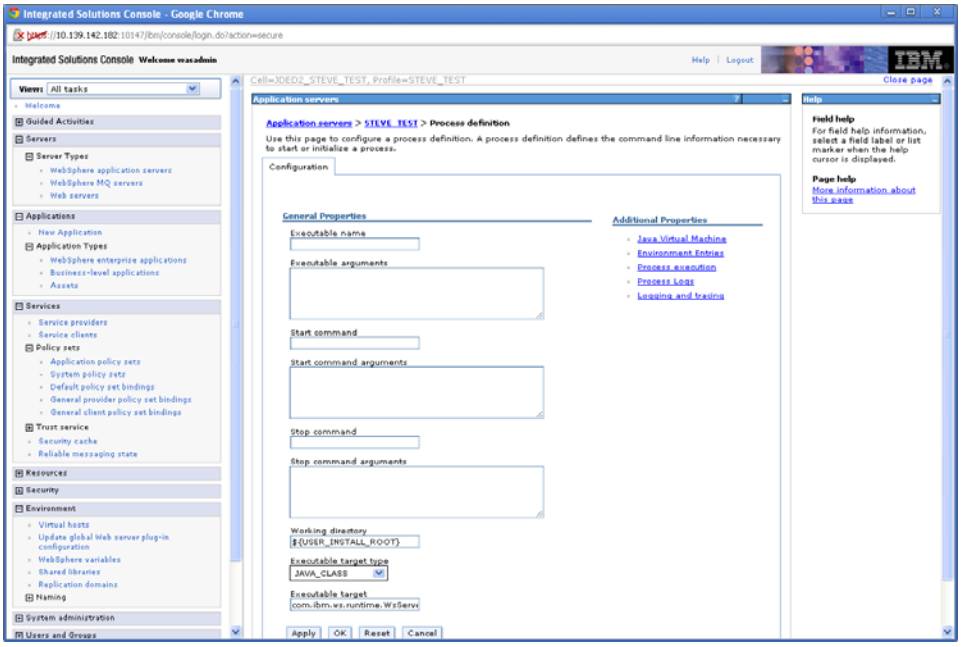
2. Select your server.

Figure 5–5 WebSphere Application Servers screen



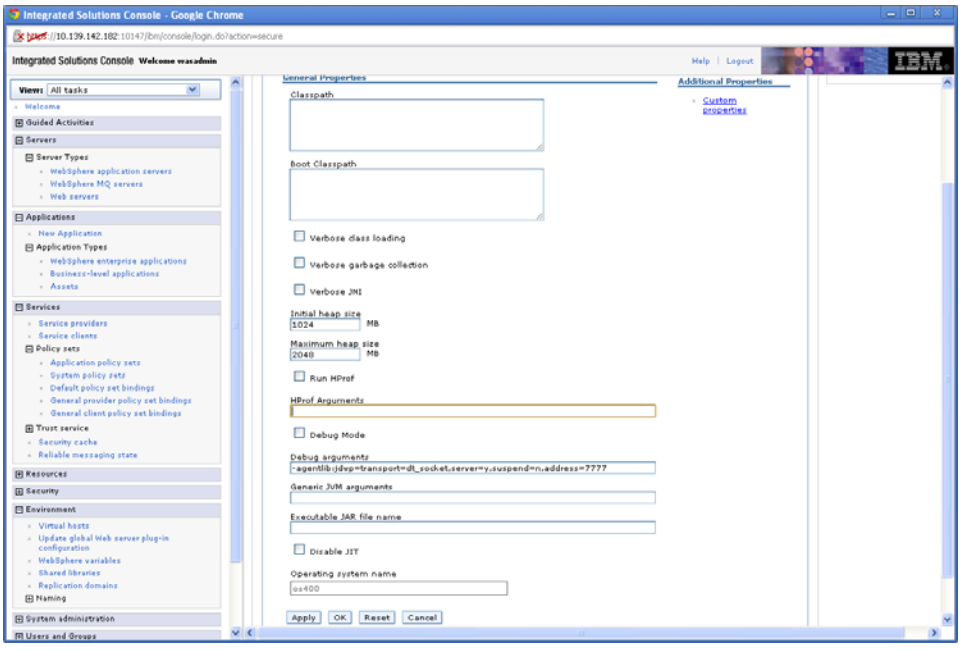
3. Select **Java and Process Management_>Process definition**.

Figure 5–6 WebSphere Application Servers screen



4. Select **Java Virtual Machine**.

Figure 5–7 WebSphere Application Server screen



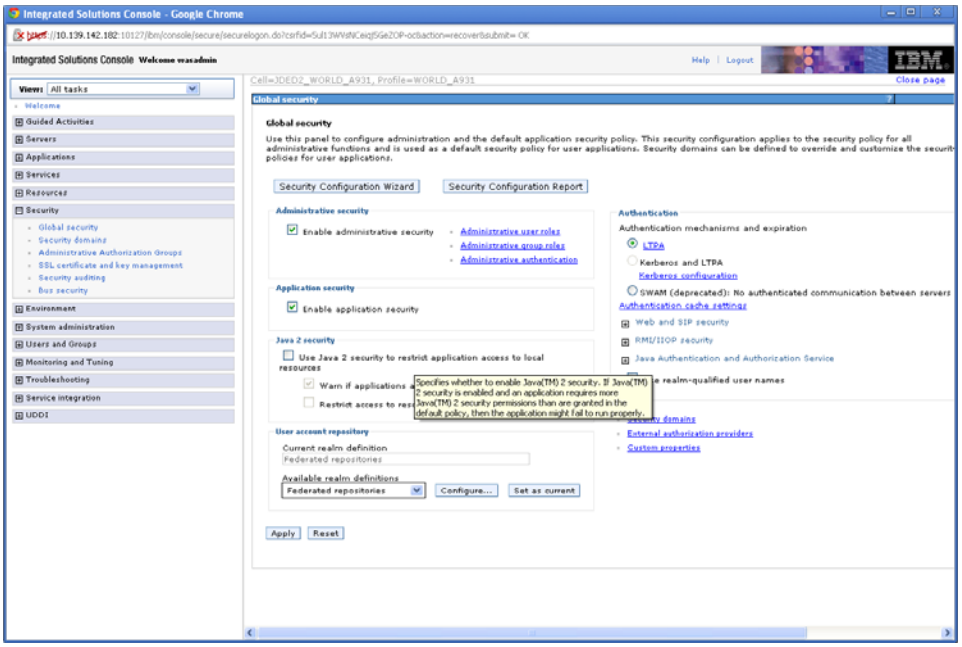
5. For the Initial heap size, enter 1024.
6. For the Maximum heap size, enter 2048.
7. Click OK.
8. Click Save.
9. Restart the server.

5.5 Configure Application Security

To configure application security

1. From the WebSphere Integrated Solutions Console, select the **Security->Global Security** option.

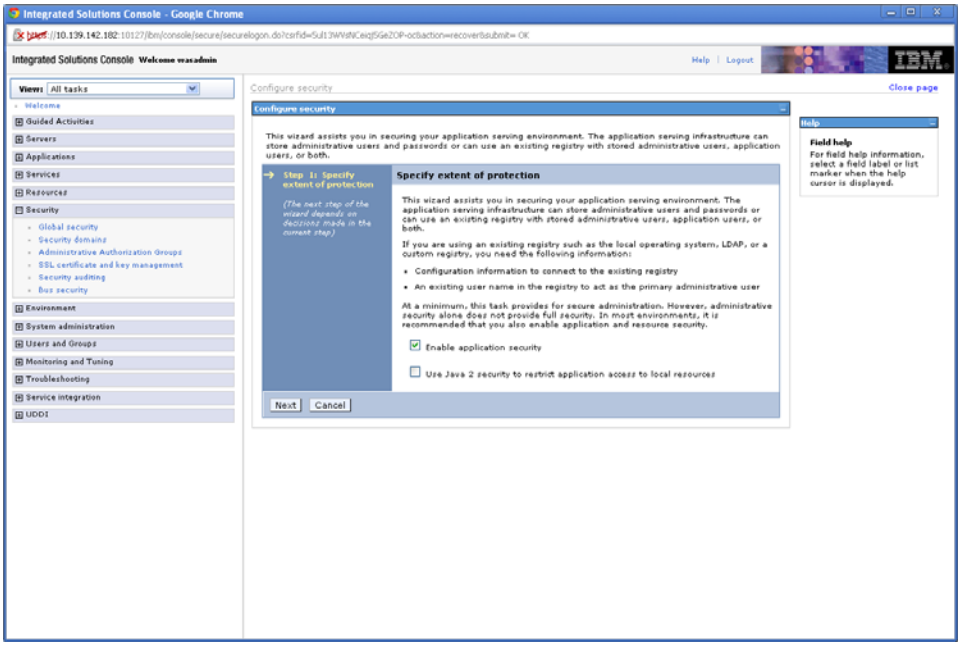
Figure 5–8 Global Security screen



2. Check the **Enable administrative security** checkbox and uncheck **Use Java 2 security to restrict application access to local resources**.

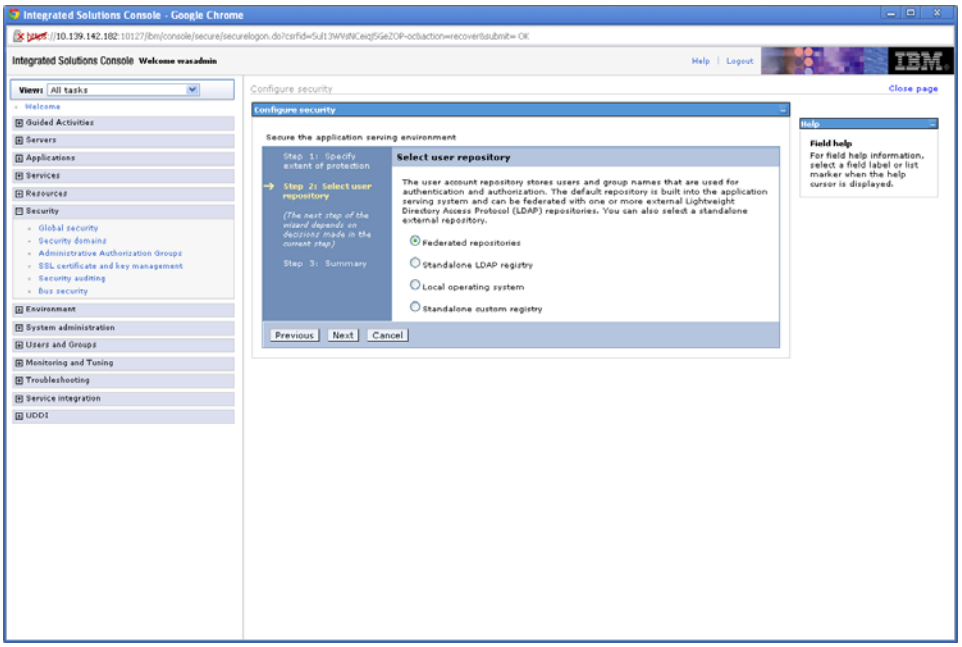
3. Select the **Security Configuration Wizard** button.

Figure 5–9 Configure Security screen



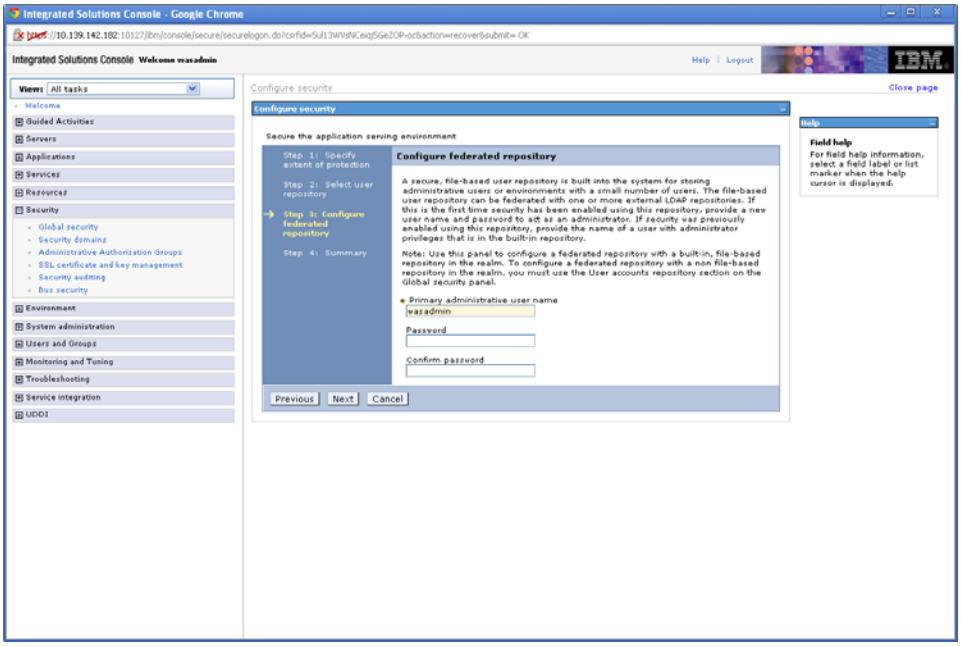
4. Click Next.

Figure 5–10 Configure Security screen



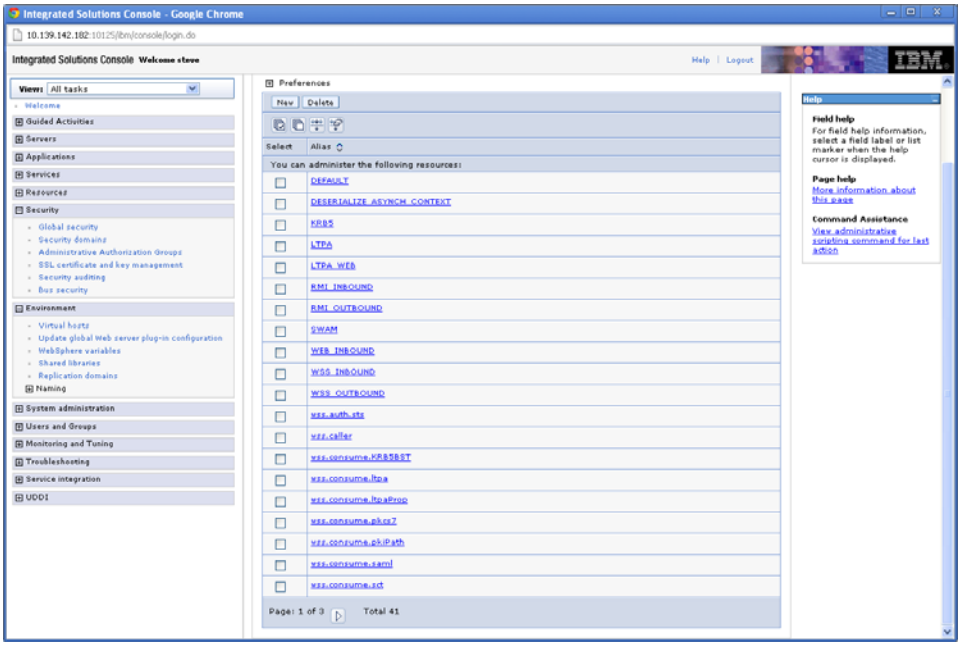
5. Select **Federated repositories**. Click Next.

Figure 5–11 Configure Security screen



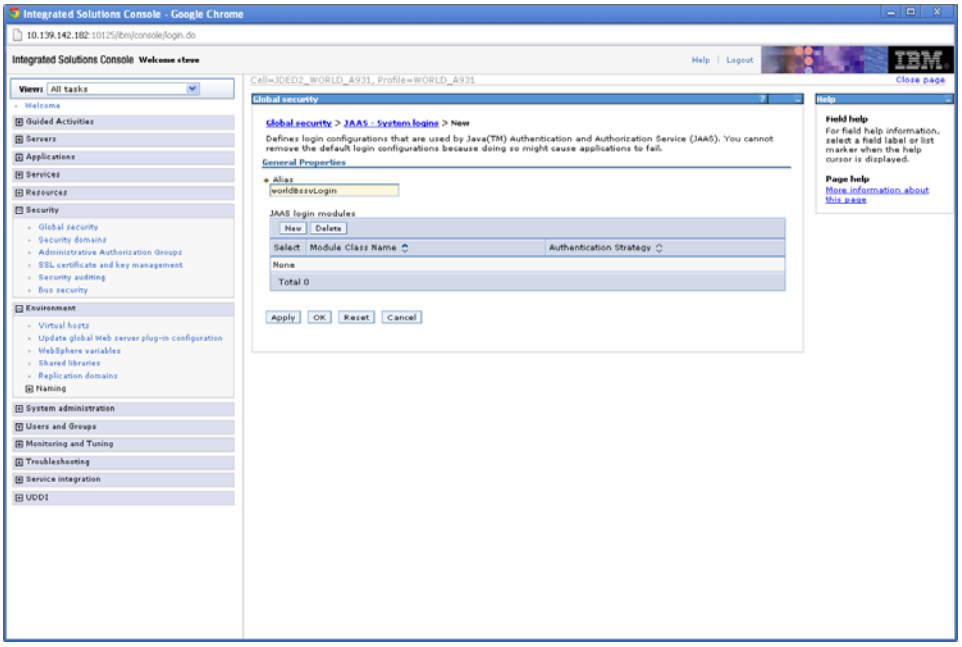
6. Enter a user name and password to be used to administer this server.
7. Click Next, and click Finish.
8. Expand the **Java Authentication** and **Authorization Service**, and select **System logins**.

Figure 5–12 Configure Security screen



9. Click New.

Figure 5–13 Global Security screen



10. Enter "worldBssvAuth" for the Alias, and click New under JAAS login modules.

11. Enter "com.ibm.ws.wssecurity.impl.auth.module.PreCallerLoginModule" and click OK.

12. Click New under JAAS login modules to add the following modules:

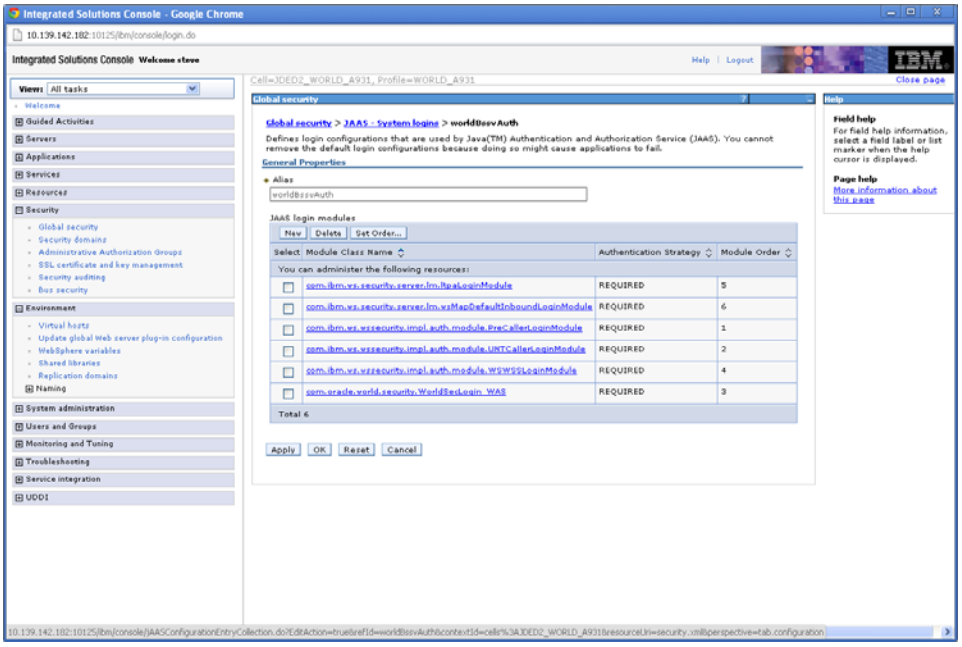
- com.ibm.ws.wssecurity.impl.auth.module.UNTCallerLoginModule
- com.oracle.world.security.WorldSecLogin_WAS

  (Check the Use login module proxy box when adding this class name)
- com.ibm.ws.wssecurity.impl.auth.module.WSWSSLoginModule
- com.ibm.ws.security.server.lm.ltpaLoginModule
- com.ibm.ws.security.server.lm.wsMapDefaultInboundLoginModule

13. Click Save.

The worldBssvAuth system login should look like the screen shot below:

Figure 5–14 Global Security screen



14. From the System logins screen click New.

Figure 5–15 Global Security screen

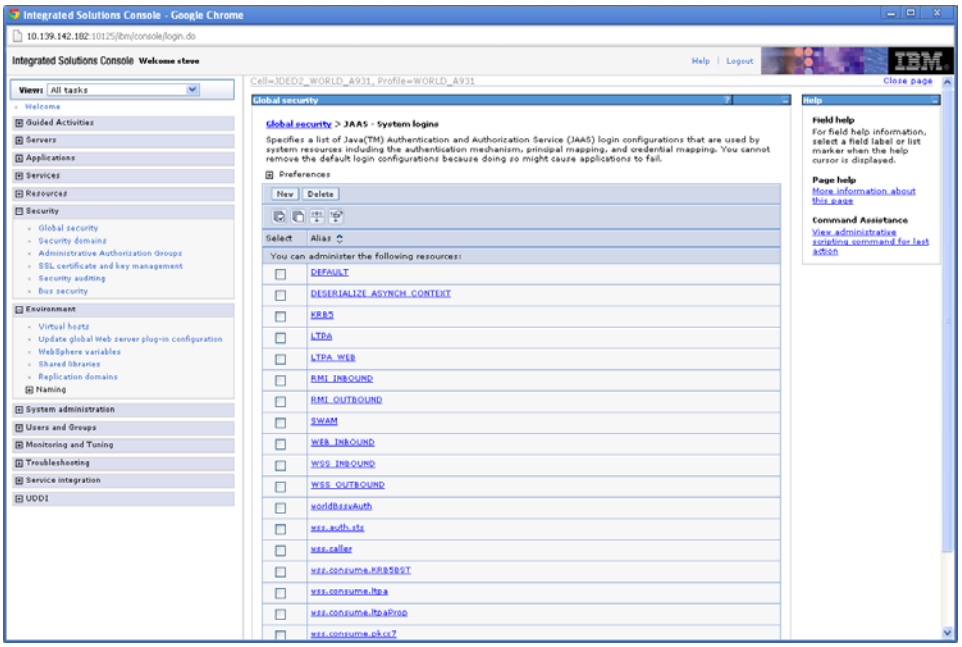
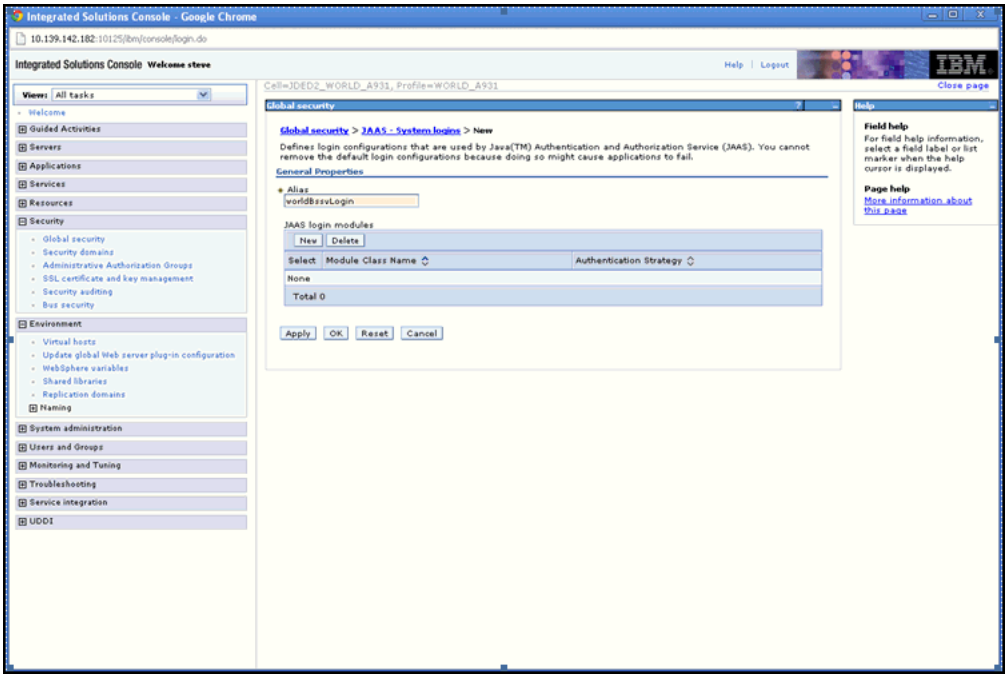
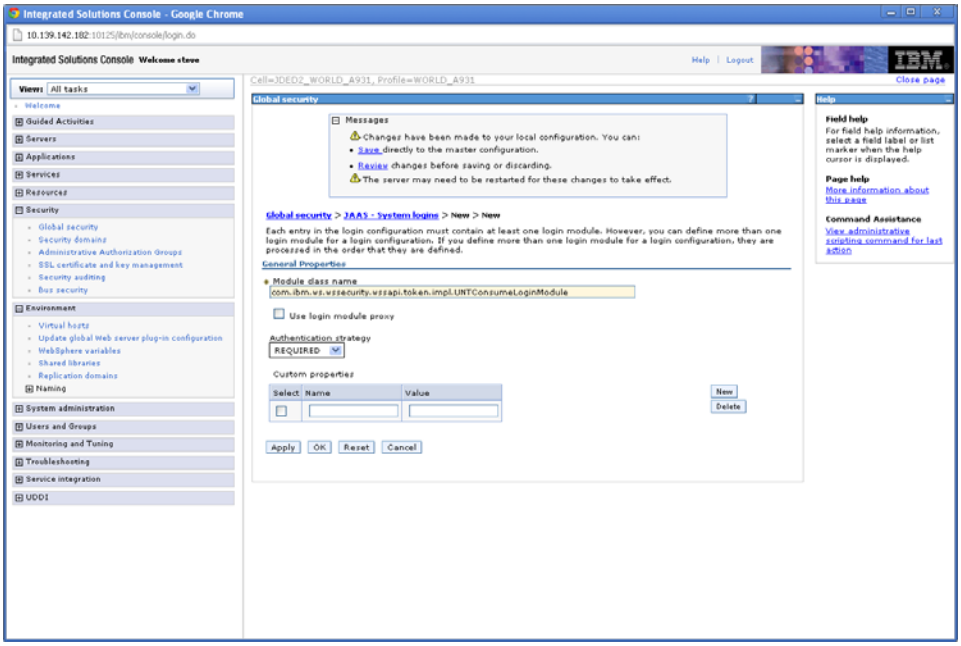


Figure 5–16 Global Security screen



15. Enter "worldBssvLogin" for the Alias and click New under JAAS login modules.

Figure 5–17 Global Security screen



16. Enter "com.ibm.ws.wssecurity.wssapi.token.impl.UNTConsumeLoginModule" for the Module class name, and click OK.

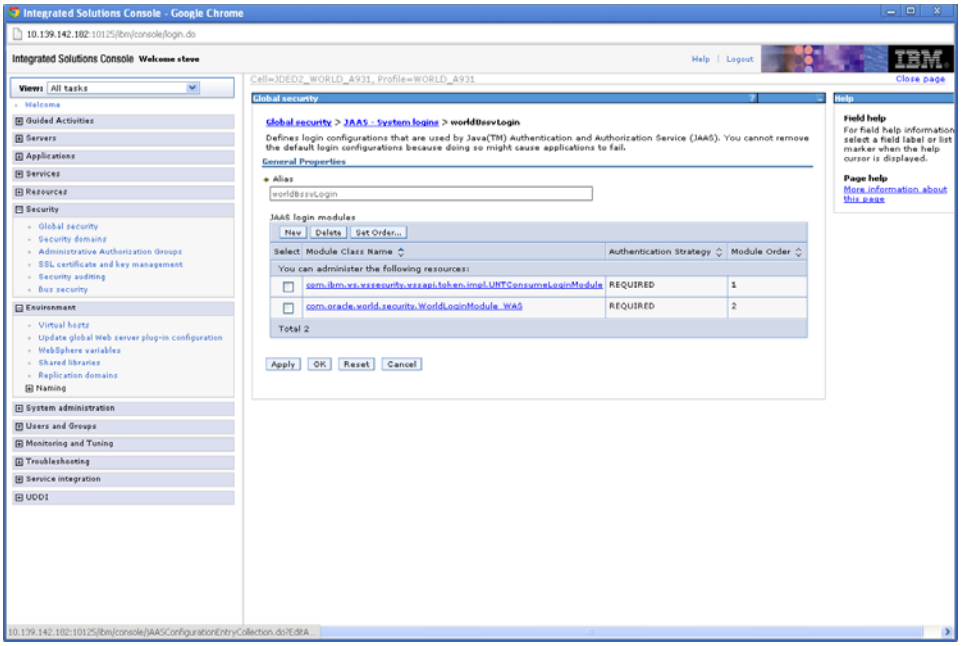
17. Click New and enter "com.oracle.world.security.WorldLoginModule_WAS" for the Module class name.

18. Click the **Use login module proxy** checkbox and click OK.

19. Click Save.

The worldBssvLogin system login should look like the screen shot below:

Figure 5–18 Global Security screen

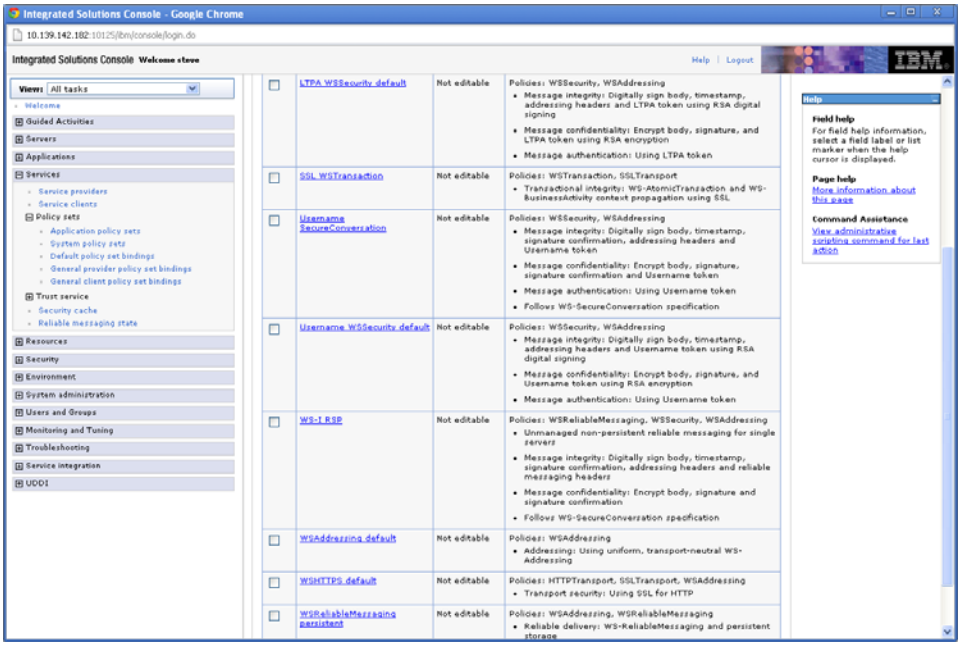


5.6 Set Up Policies and Bindings

To set up policies and bindings

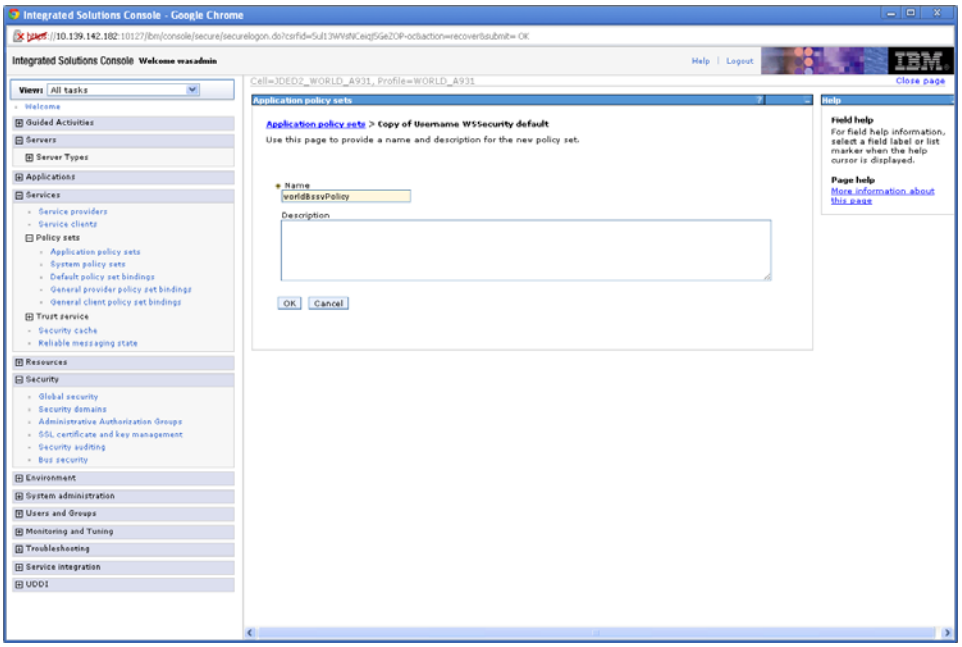
1. From the Integrated Solutions Console, select **Services->Policy sets->Application policy sets**.

Figure 5–19 Application Policy Sets screen



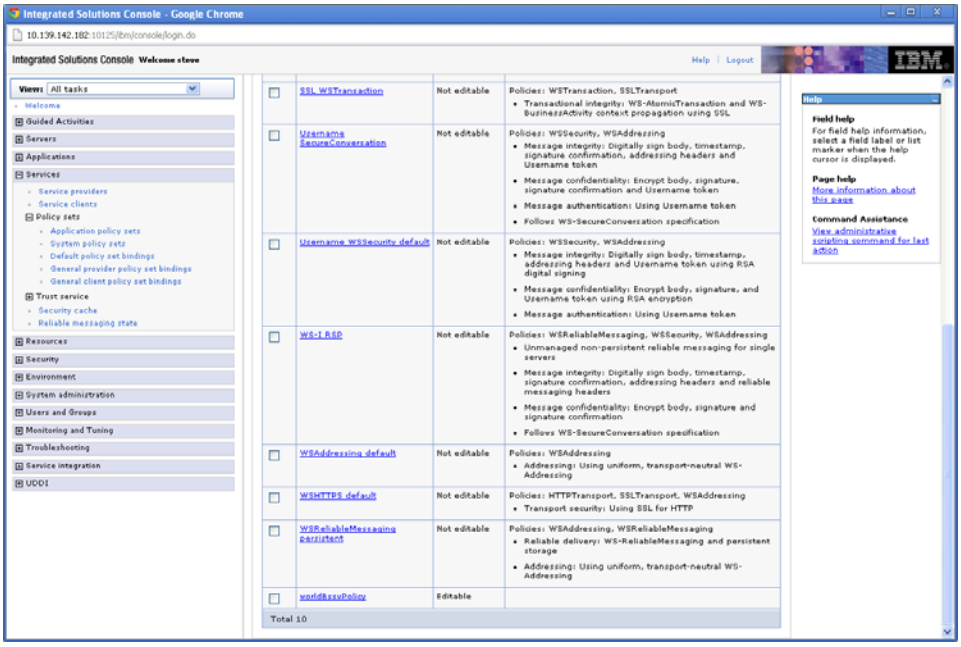
2. Select the box next to **Username WSSecurity default** and click Copy.

Figure 5–20 Application Policy Sets screen



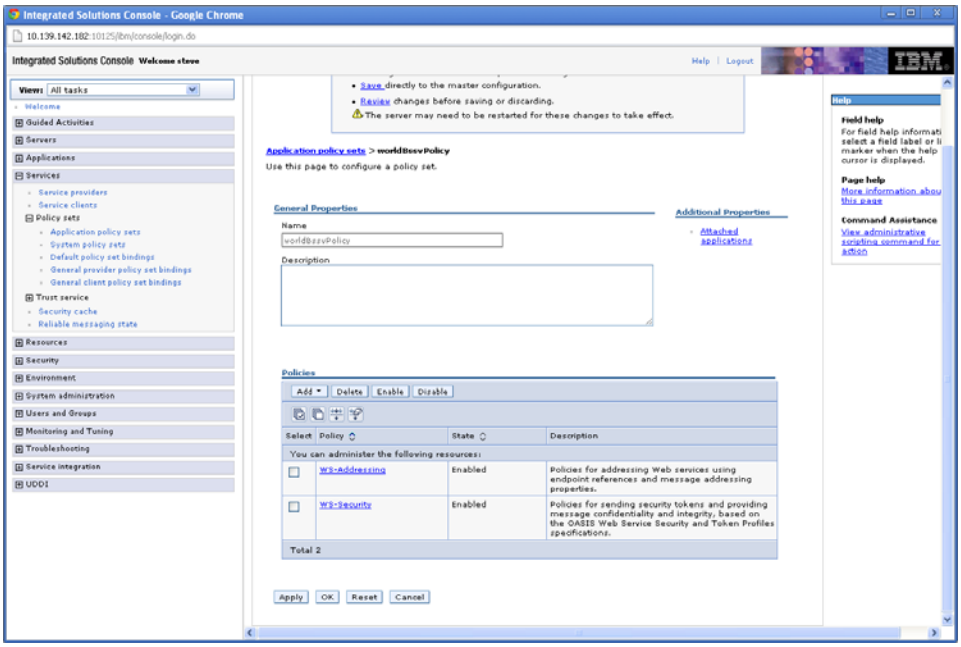
3. Enter "worldBssvPolicy" for the Name and click OK.

Figure 5–21 Application Policy Sets screen



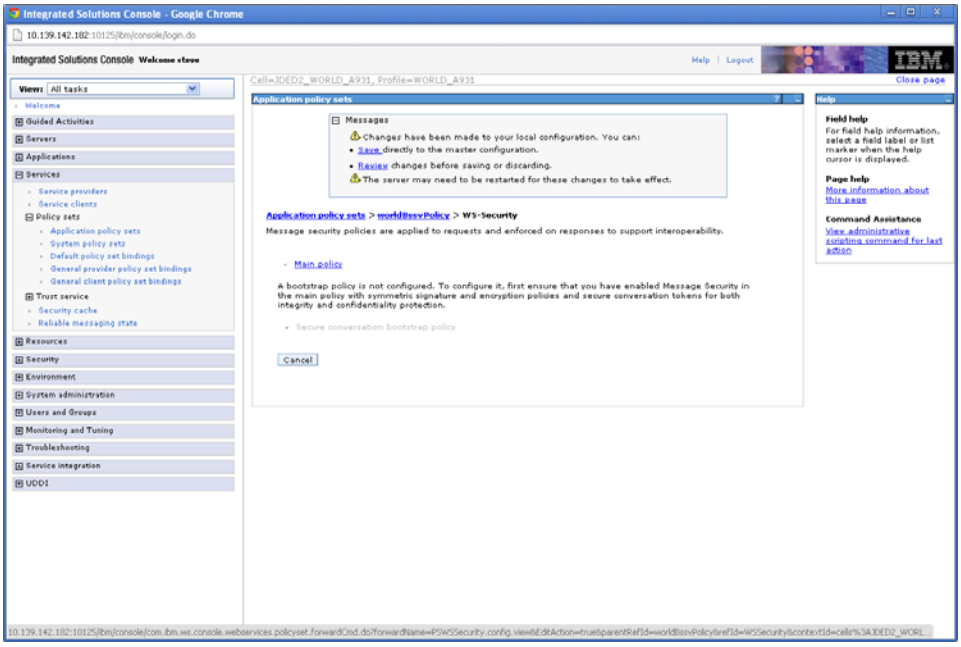
4. Select **worldBssvPolicy**.

Figure 5–22 Application Policy Sets screen



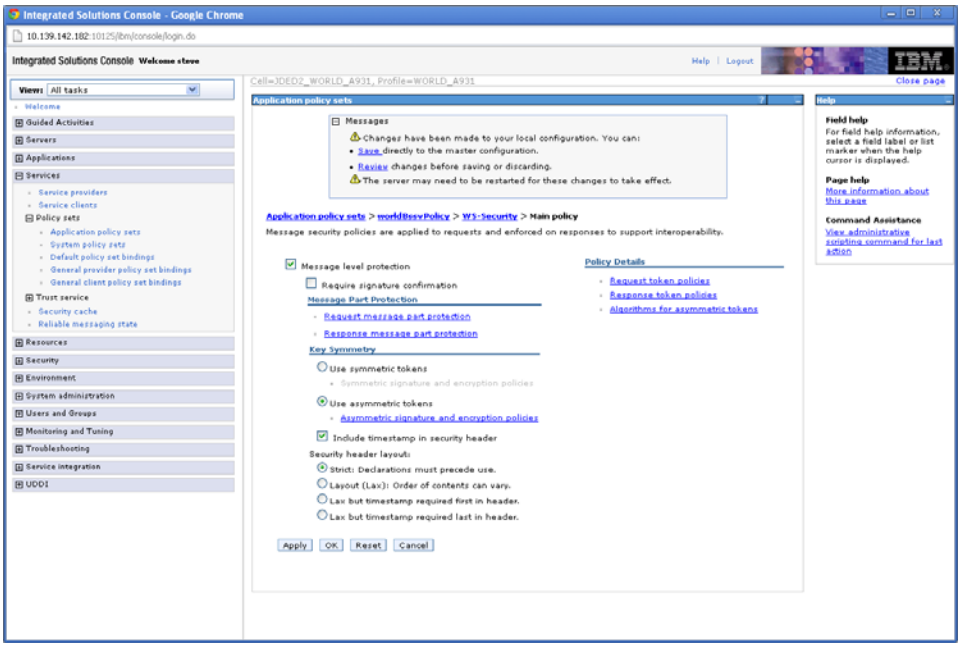
5. Check the box next to **WS-Addressing** and click Delete.
6. Click on **WS-Security**.

Figure 5–23 Application Policy Sets screen



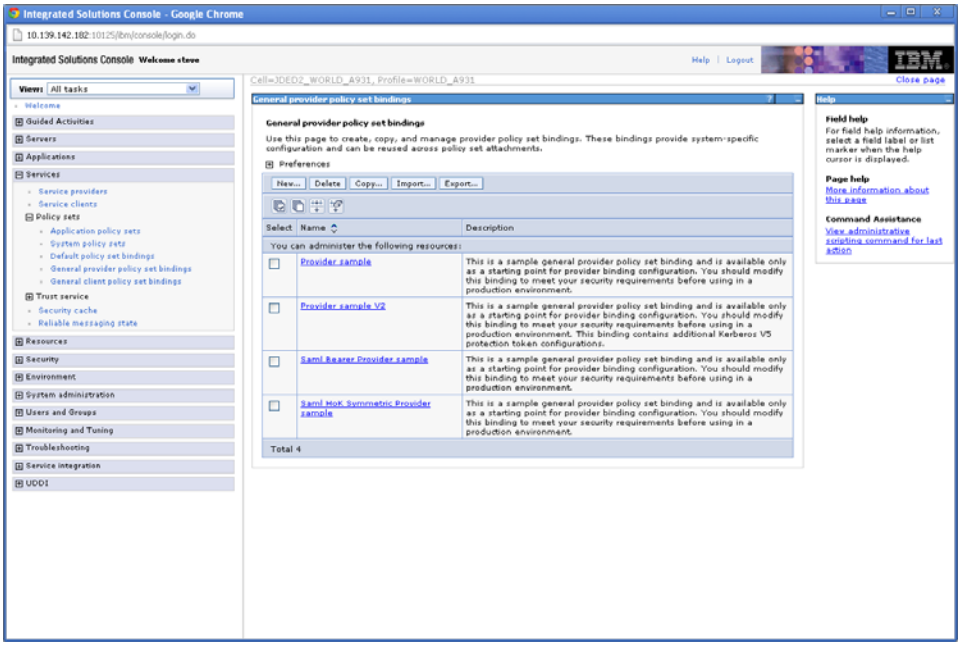
7. Click on **Main policy**.

Figure 5–24 Application Policy Sets screen



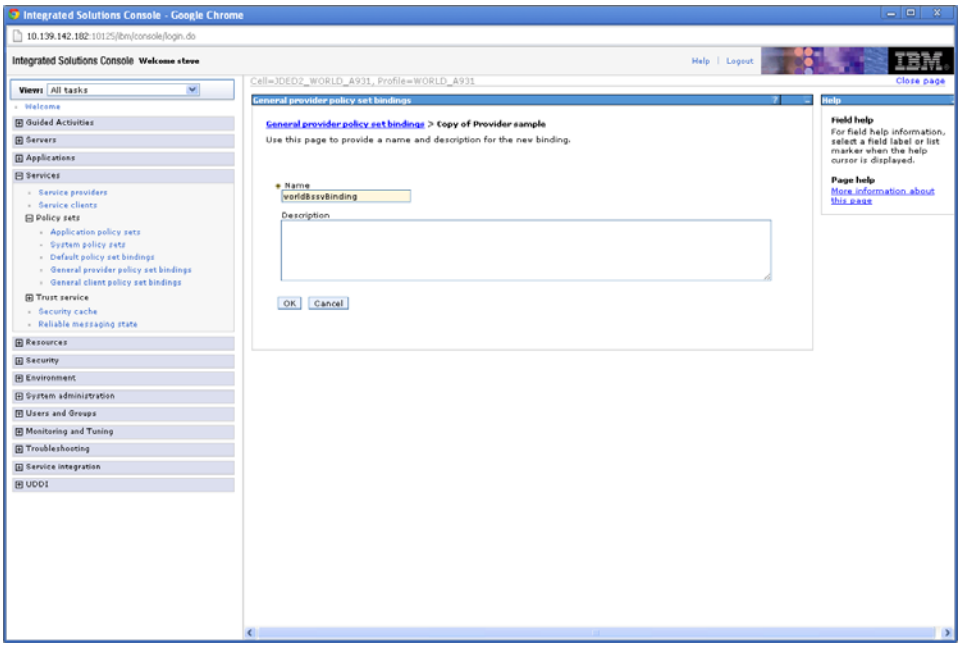
8. Uncheck the box next to **Message level protection**.
9. Click OK.
10. Click Save.
11. On the left hand menu, select **General provider policy set bindings**.

Figure 5–25 General Provider Policy Set Bindings screen



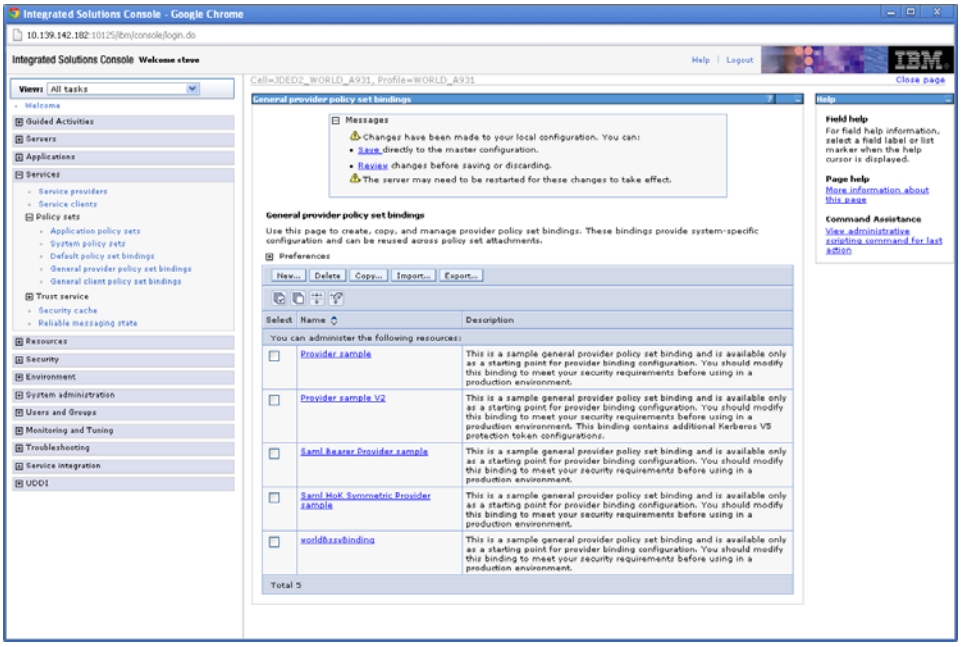
12. Check the box next to **Provider sample** and click Copy.

Figure 5–26 General Provider Policy Set Bindings screen



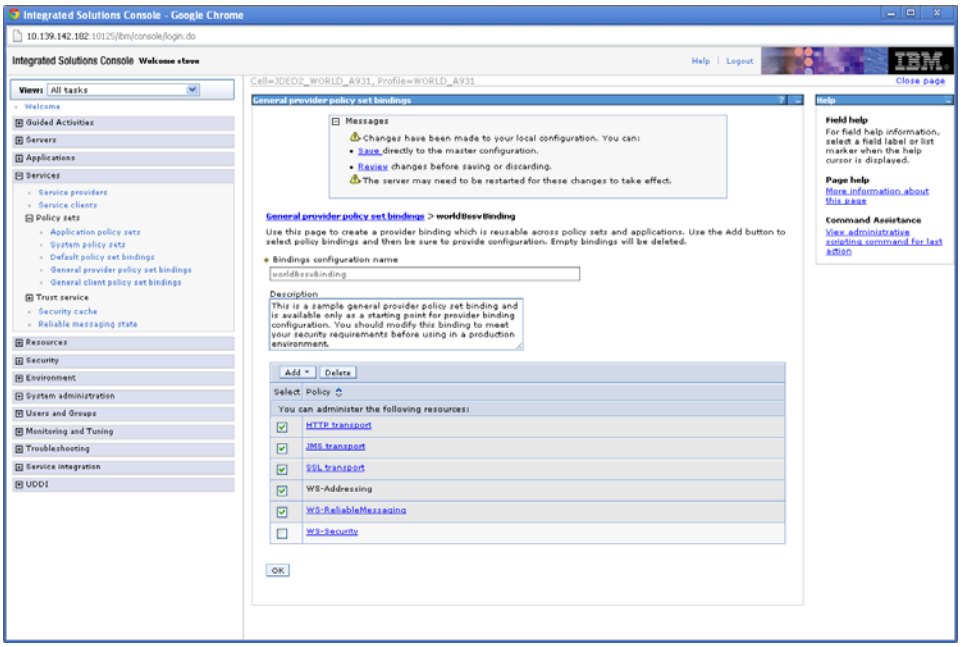
13. Enter "worldBssvBinding" in the Name field and click OK.

Figure 5–27 General Provider Policy Set Bindings screen



14. Select **worldBssvBinding**.

Figure 5–28 General Provider Policy Set Bindings screen



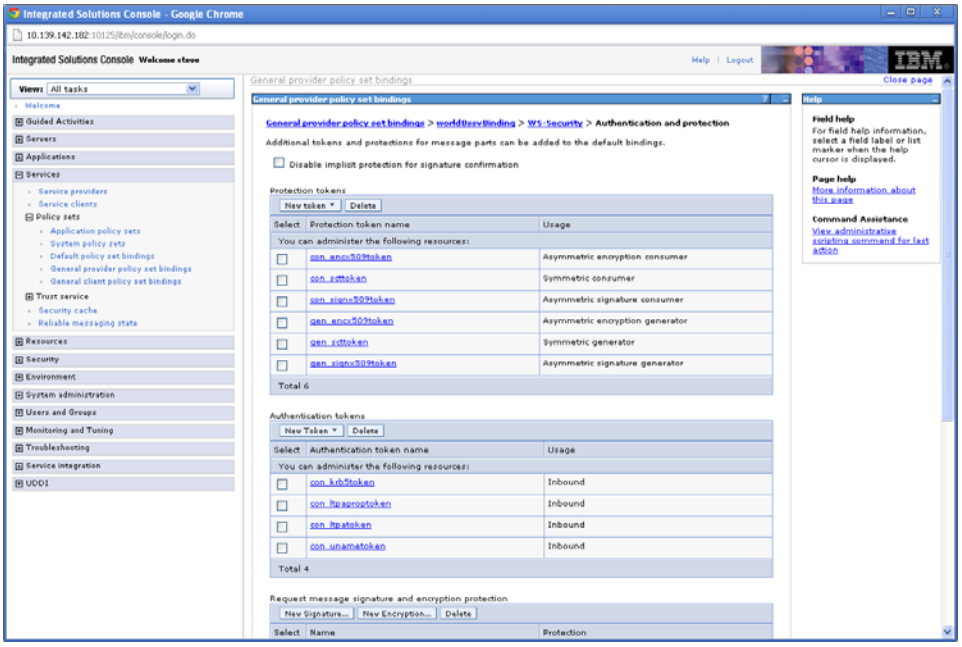
15. Check all the boxes EXCEPT WS-Security and click Delete.

16. Click OK.

17. Click Save.

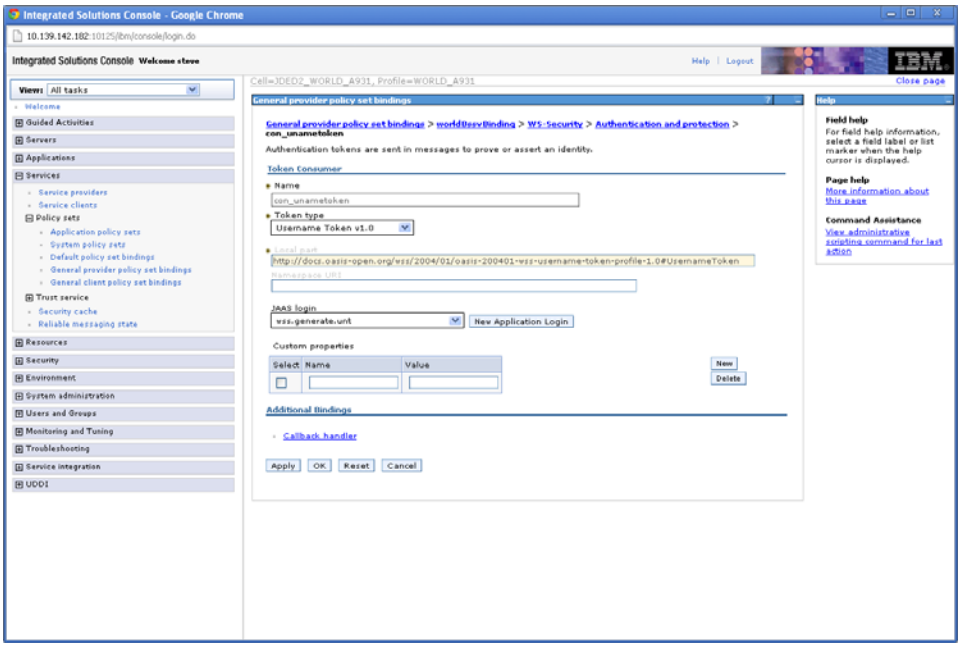
18. Select **worldBssvBinding->WS-Security->Authentication and protection**.

Figure 5–29 General Provider Policy Set Bindings screen



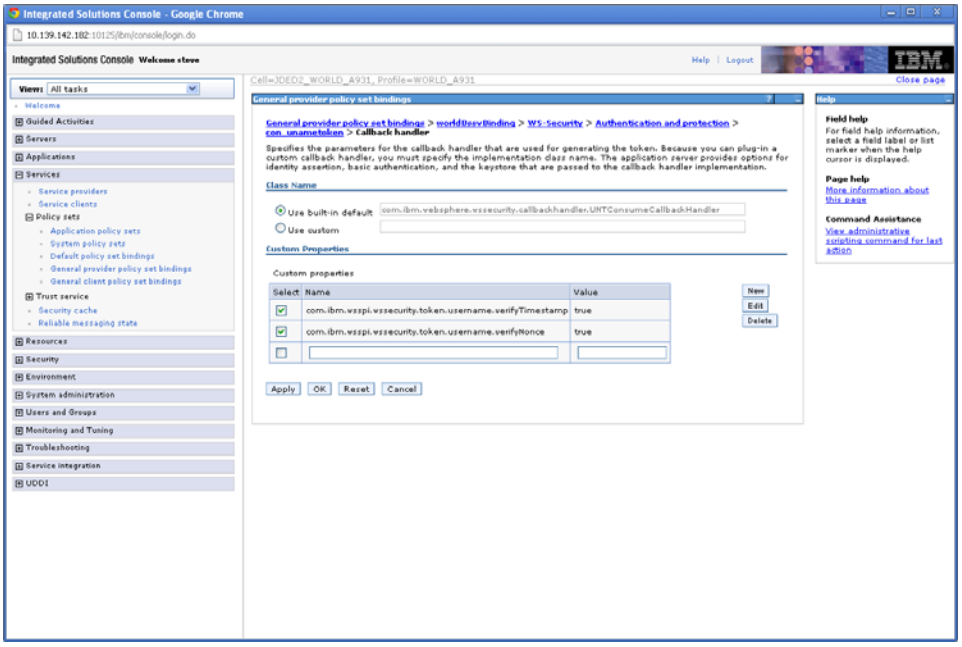
19. Under **Authentication tokens** select **con_unametoken**.

Figure 5–30 General Provider Policy Set Bindings screen



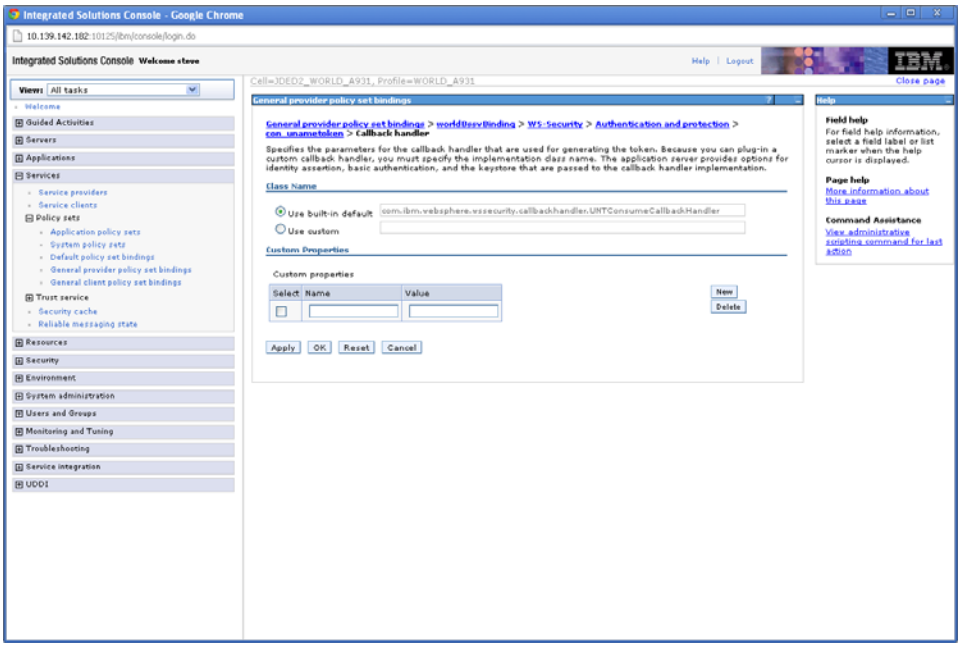
20. Select **Callback handler**.

Figure 5–31 General Provider Policy Set Bindings screen



21. Check the boxes next to the two **Custom properties** and click Delete.

Figure 5–32 General Provider Policy Set Bindings screen

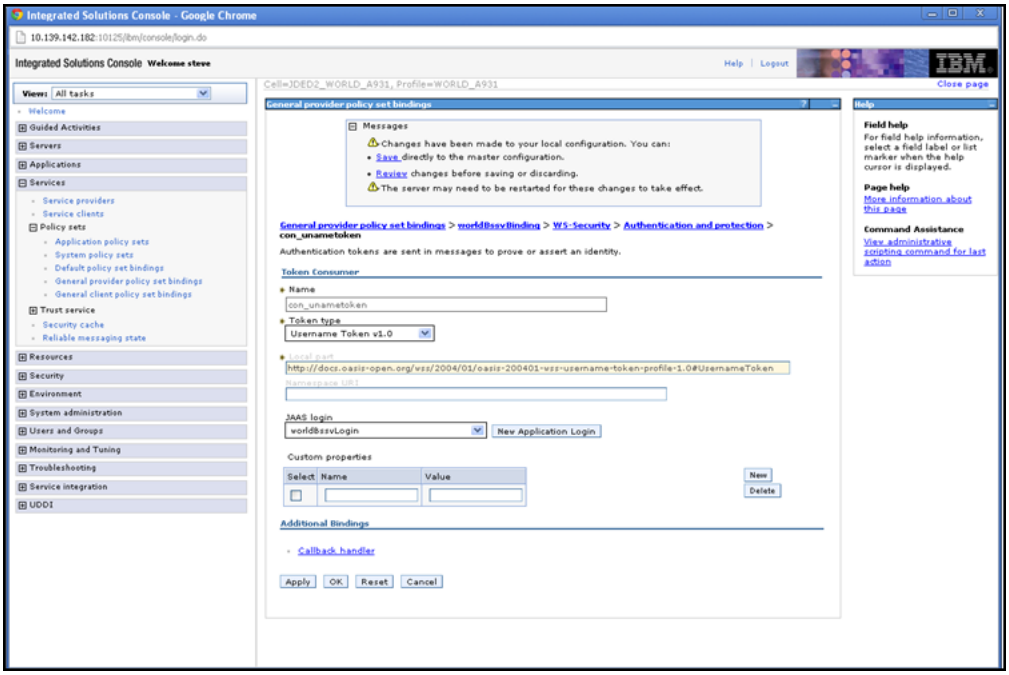


22. Under Custom properties, enter" com.ibm.wsspi.wssecurity.token.UsernameToken.authDeferred" in the Name field.

23. Enter "true" in the Value field.

24. Click OK.

Figure 5–33 General Provider Policy Set Bindings screen

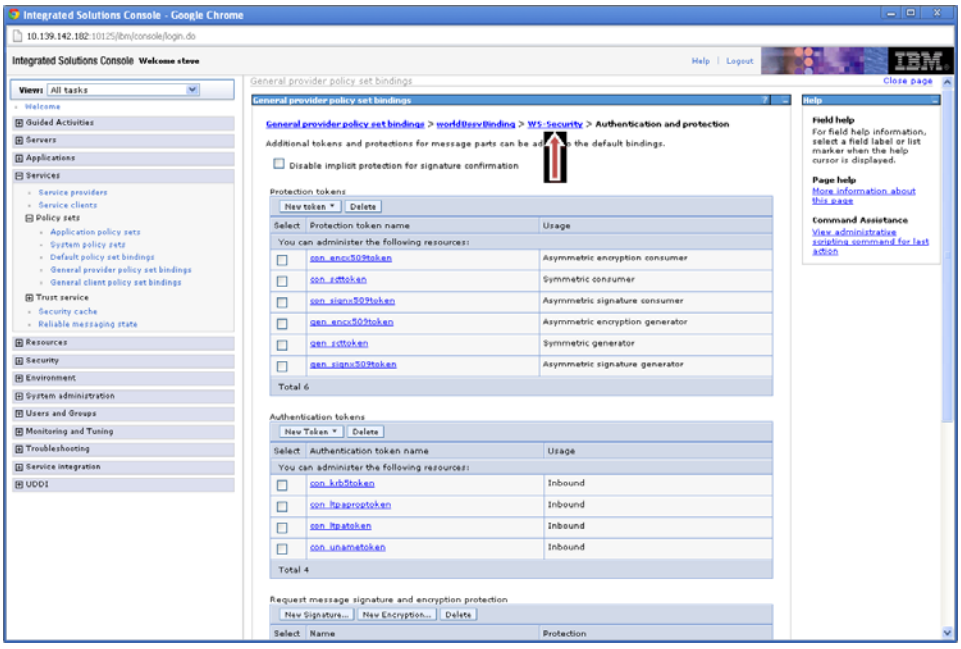


25. In the **JAAS login dropdown** box, select **worldBssvLogin**.

26. Click OK.

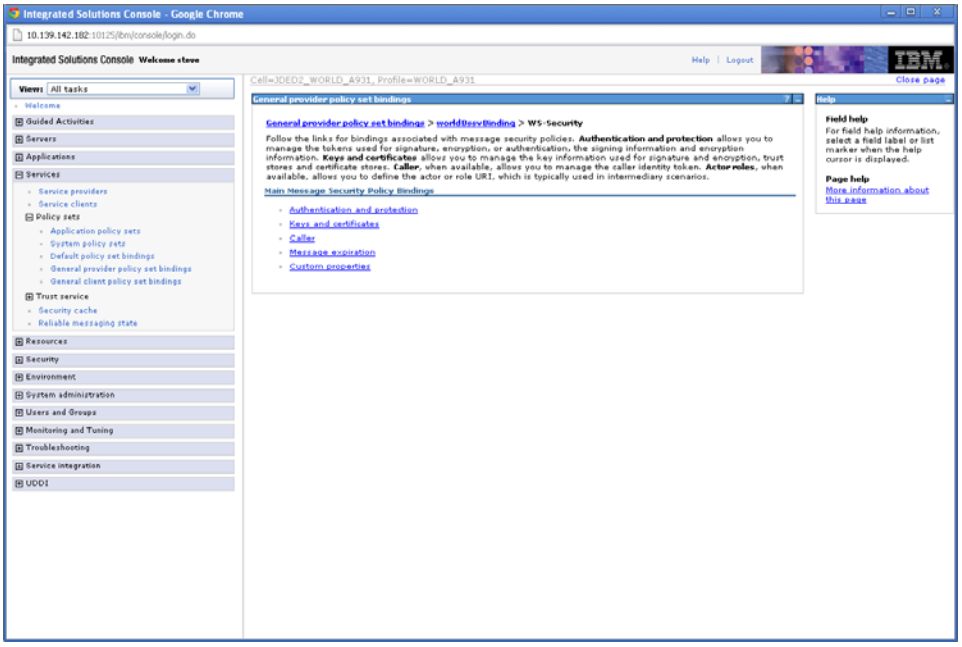
27. Click Save.

Figure 5–34 General Provider Policy Set Bindings screen



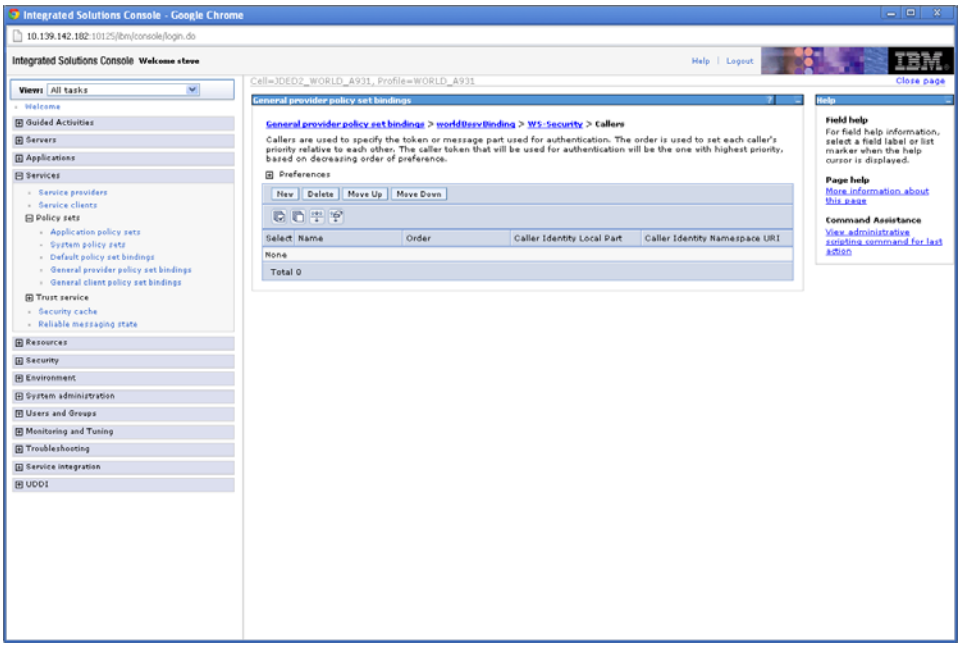
28. In the breadcrumb menu, select **WS-Security**.

Figure 5–35 General Provider Policy Set Bindings screen



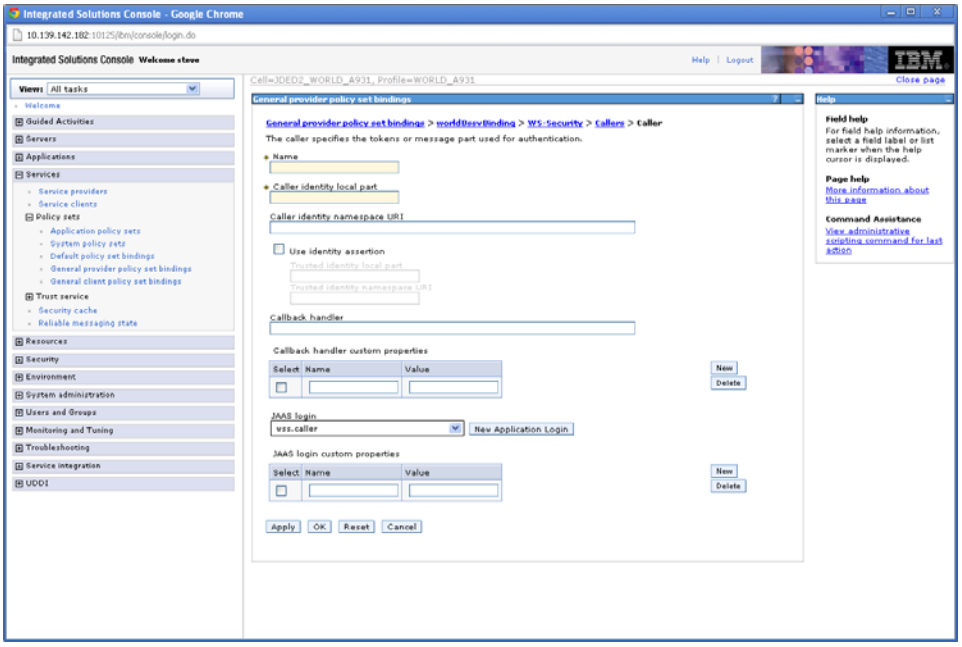
29. Select **Caller**.

Figure 5–36 General Provider Policy Set Bindings screen



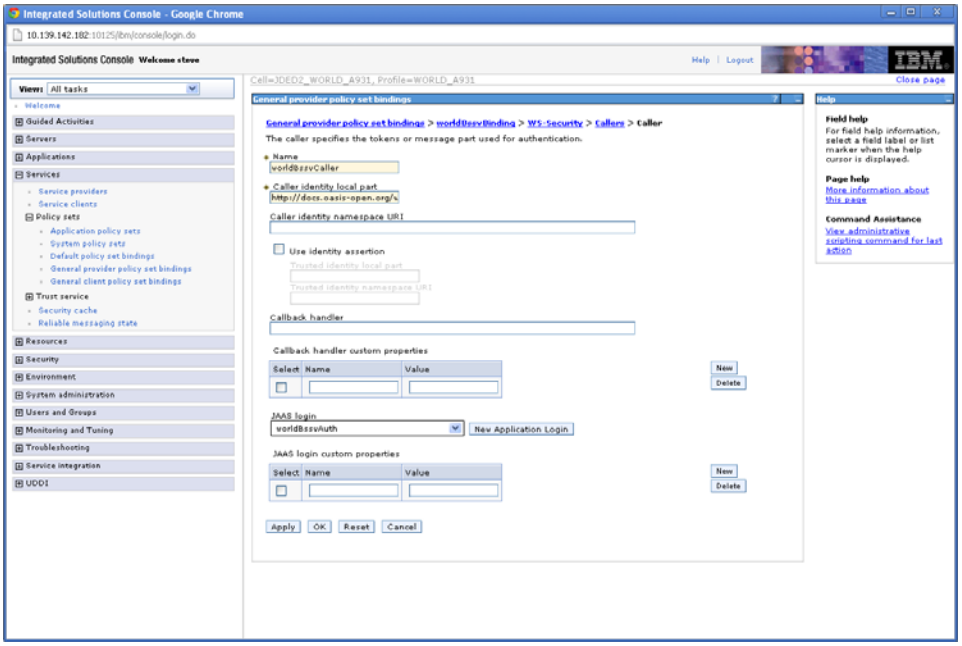
30. Click New.

Figure 5–37 General Provider Policy Set Bindings screen



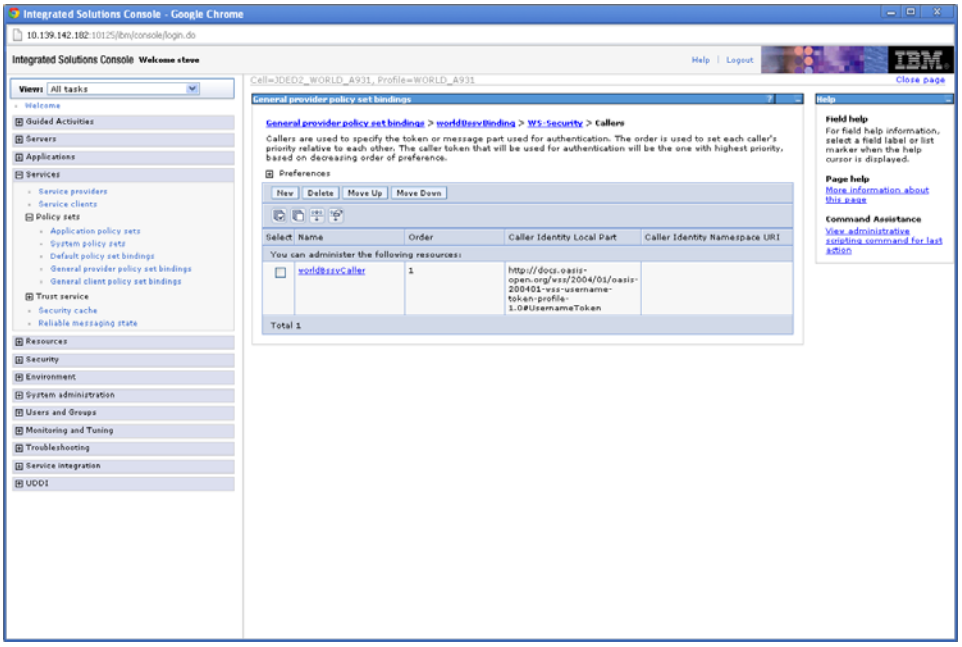
31. Enter "worldBssvCaller" in the Name field.
32. Enter "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#UsernameToken" in the Caller identity local part field.
33. In the **JAAS login dropdown**, select **worldBssvAuth**.

Figure 5–38 General Provider Policy Set Bindings screen



34. Click OK.
35. Click Save.

Figure 5–39 General Provider Policy Set Bindings screen



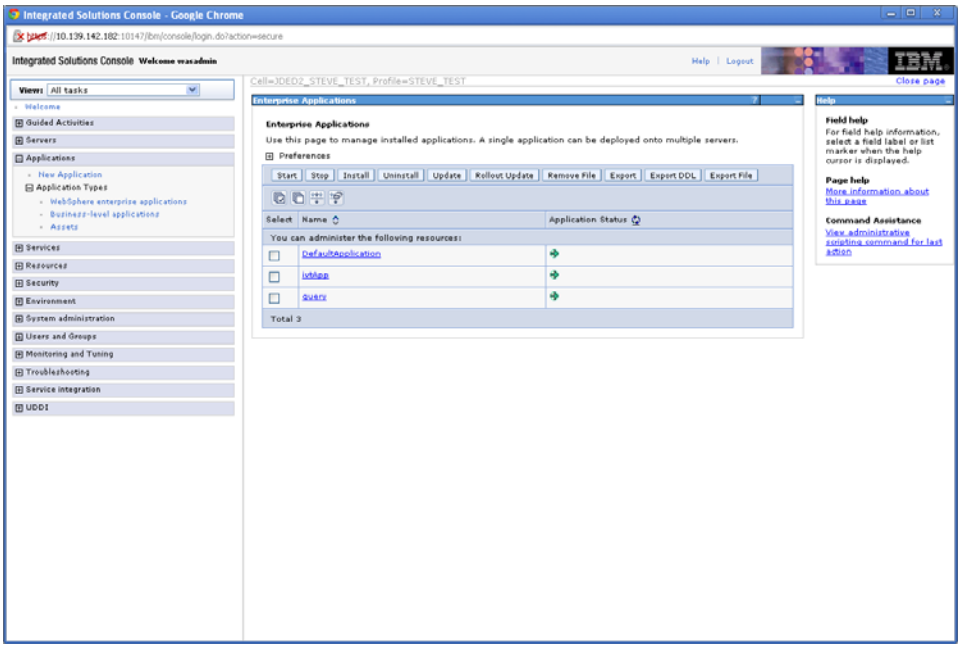
36. Restart the server.

5.7 Deploy Services

To deploy services

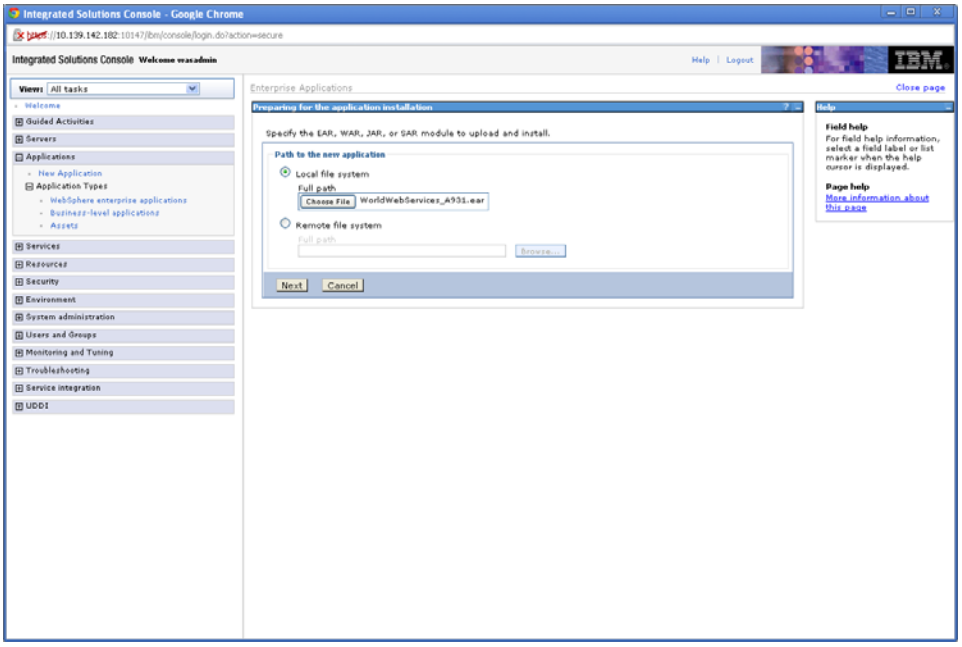
1. From the Integrated Solutions Console, select **Applications->Application Types->WebSphere enterprise applications**.

Figure 5–40 Enterprise Applications screen



2. Click Install.

Figure 5–41 Preparing for the Application Installation screen

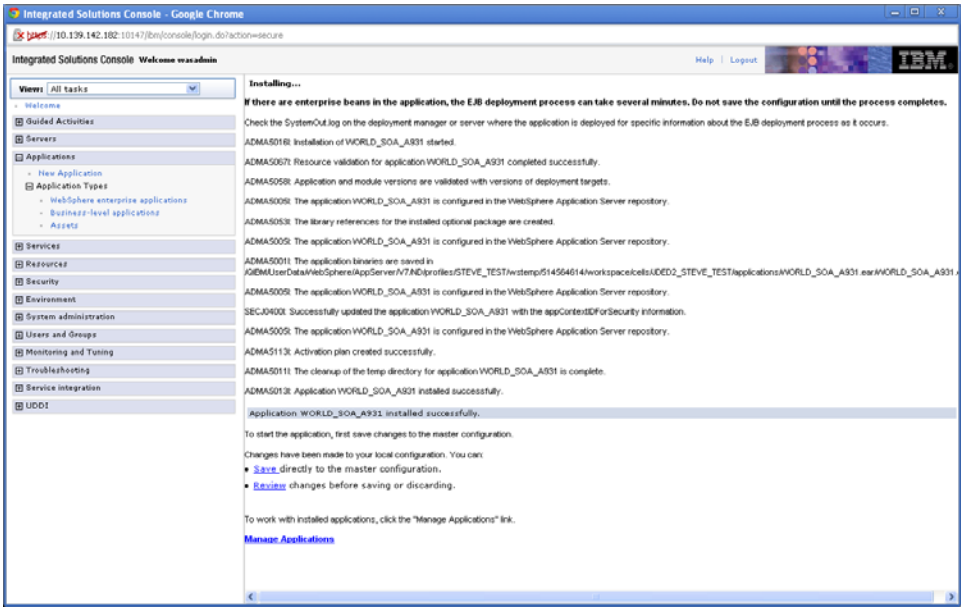


3. Click **Choose File**, navigate to folder where the .ear file was downloaded, and select the **WorldWebServices_A931.ear** file.
4. On the **Preparing for the application installation** screen, click Next.
5. On the **Select installation options** screen, click Next.
6. On the **Map modules to servers** screen, click Next.
7. On the **Map virtual hosts for Web modules** screen, click Next.
8. On the **Summary** screen, click Finish.

   The following screen should be displayed:

Note: This can take several minutes.

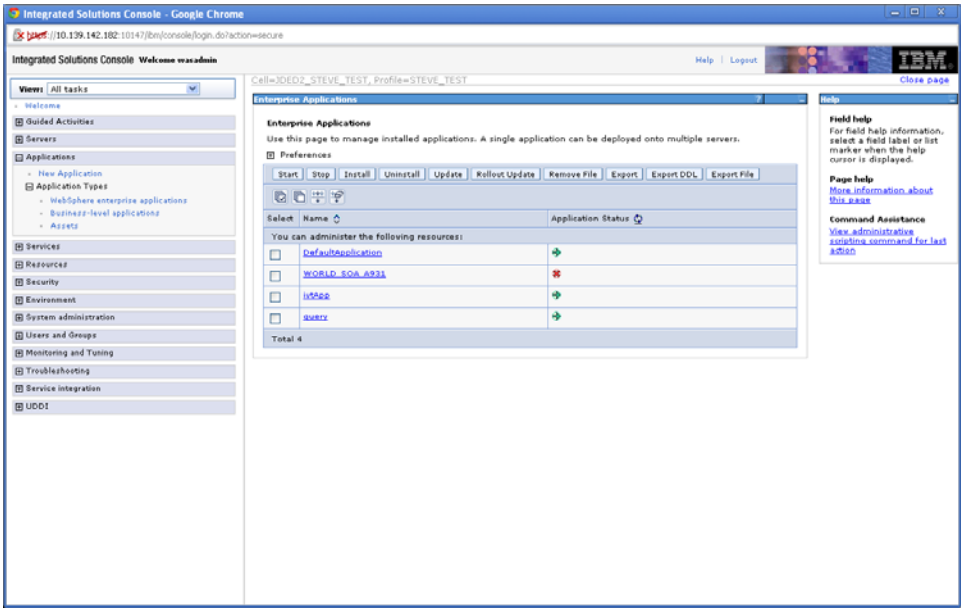
Figure 5–42 Installation screen



9. Click Save.

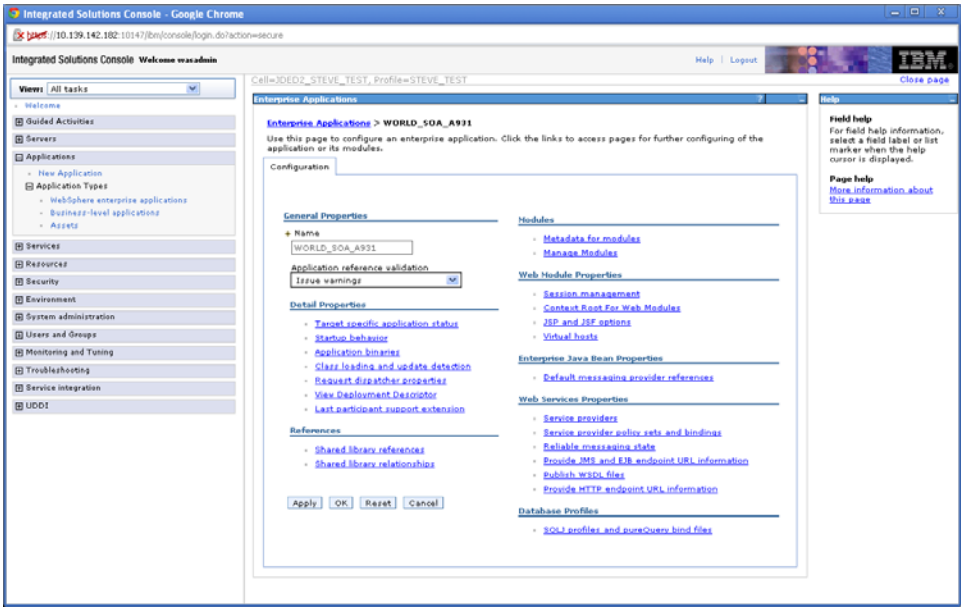
> **Note:** This can take several minutes.

Figure 5–43 Enterprise Applications screen



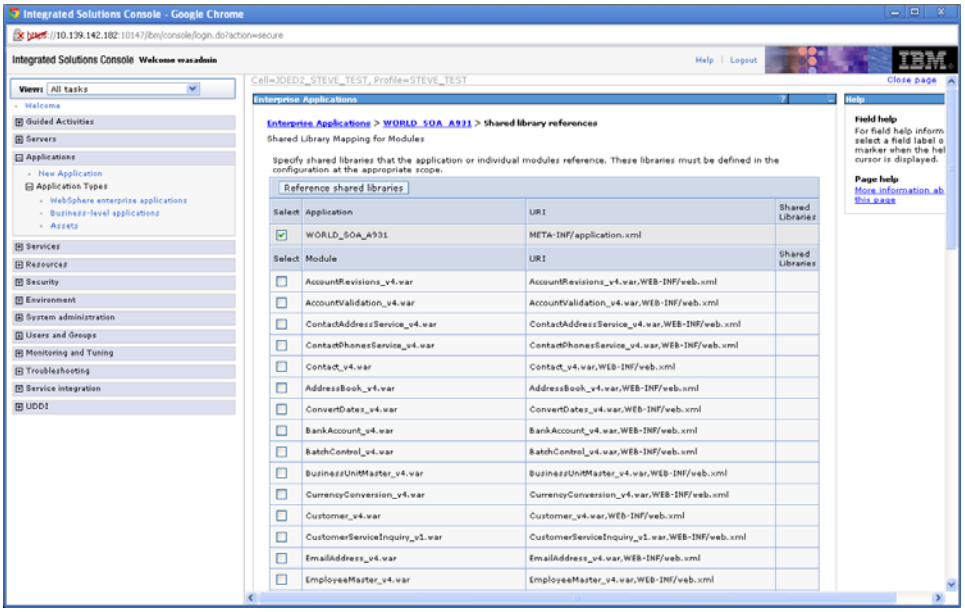
10. Click **WORLD_SOA_A931**.

Figure 5–44 Enterprise Applications screen



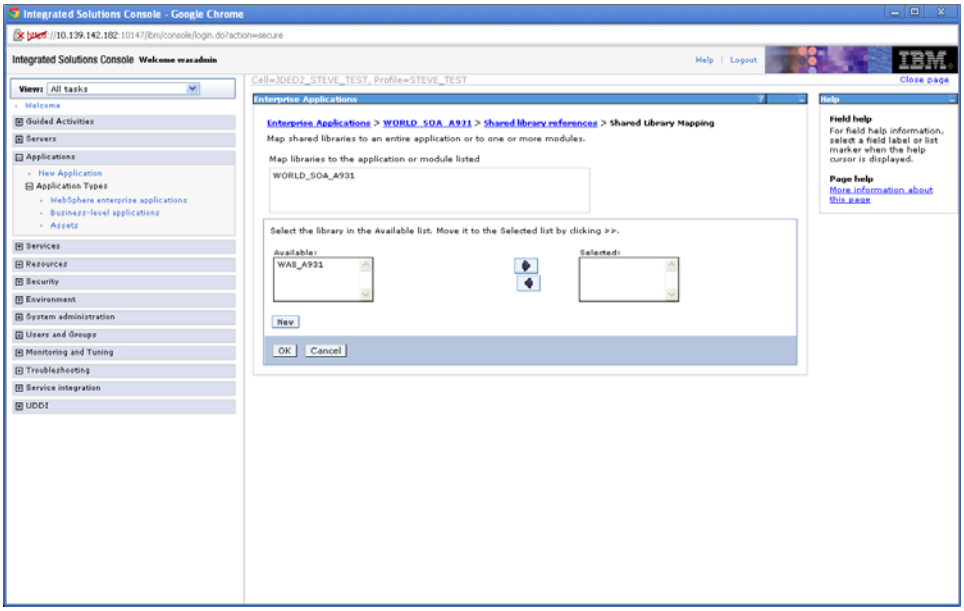
11. Click **Shared library references**.

Figure 5–45 Enterprise Applications screen



12. Check **WORLD_SOA_A931**, and click **Reference shared libraries**.

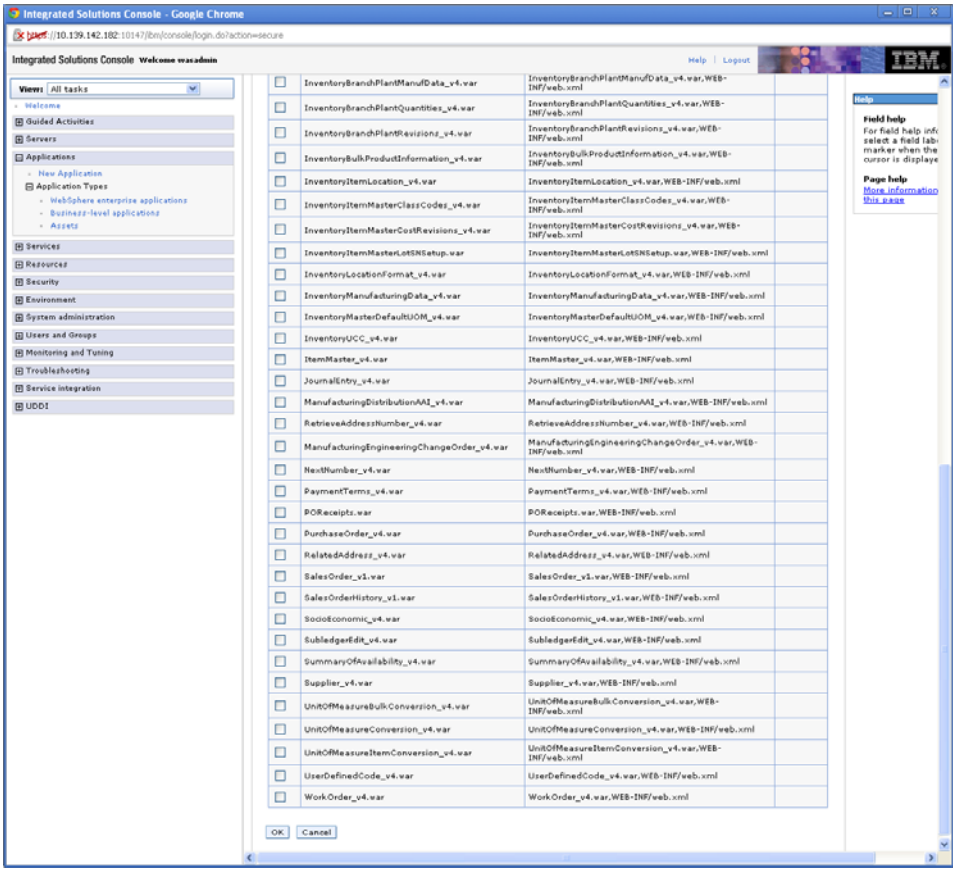
Figure 5–46 Enterprise Applications screen



13. In the Available box, select **WAS_A931**, and click the arrow key to move the library to the Selected box.

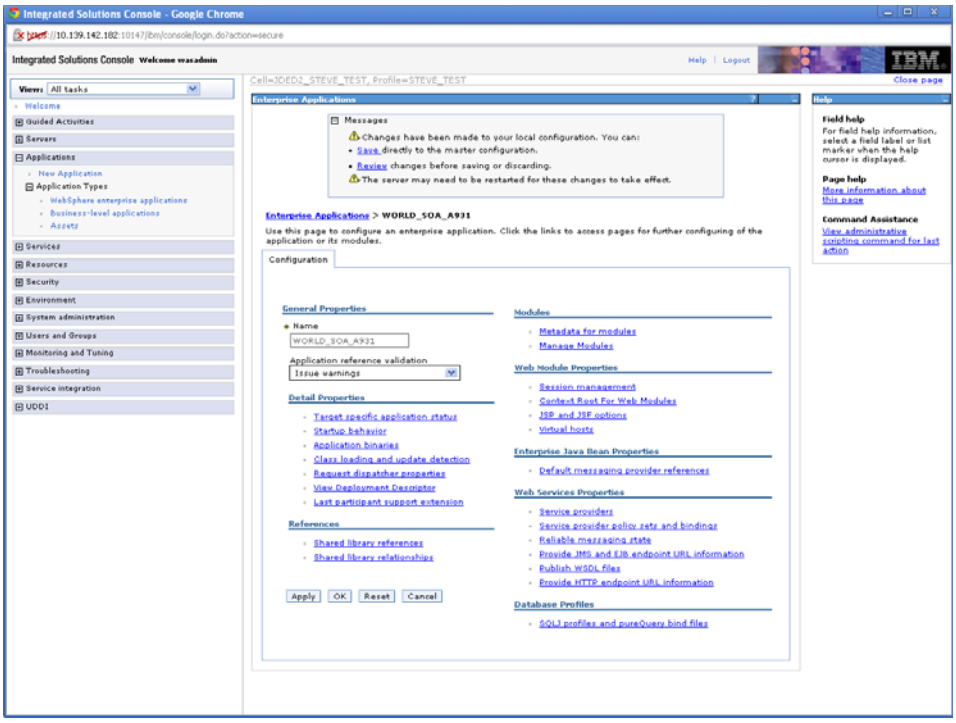
14. Click OK.

Figure 5–47 Enterprise Applications screen



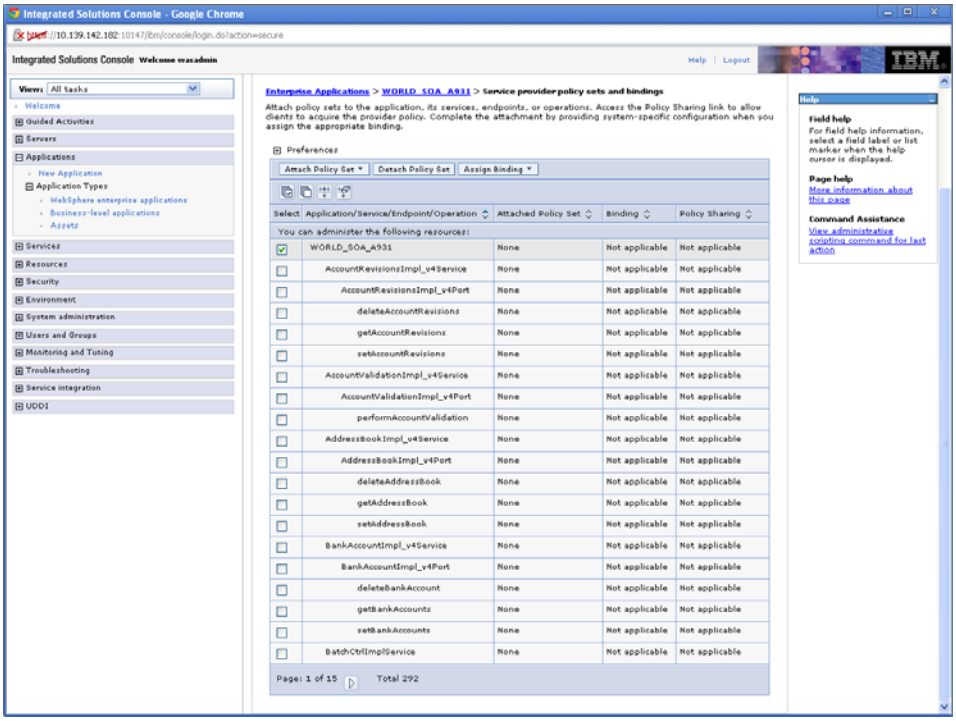
15. Click OK.

Figure 5–48 Enterprise Applications screen



16. Click Service provider policy sets and bindings.

Figure 5–49 Enterprise Applications screen

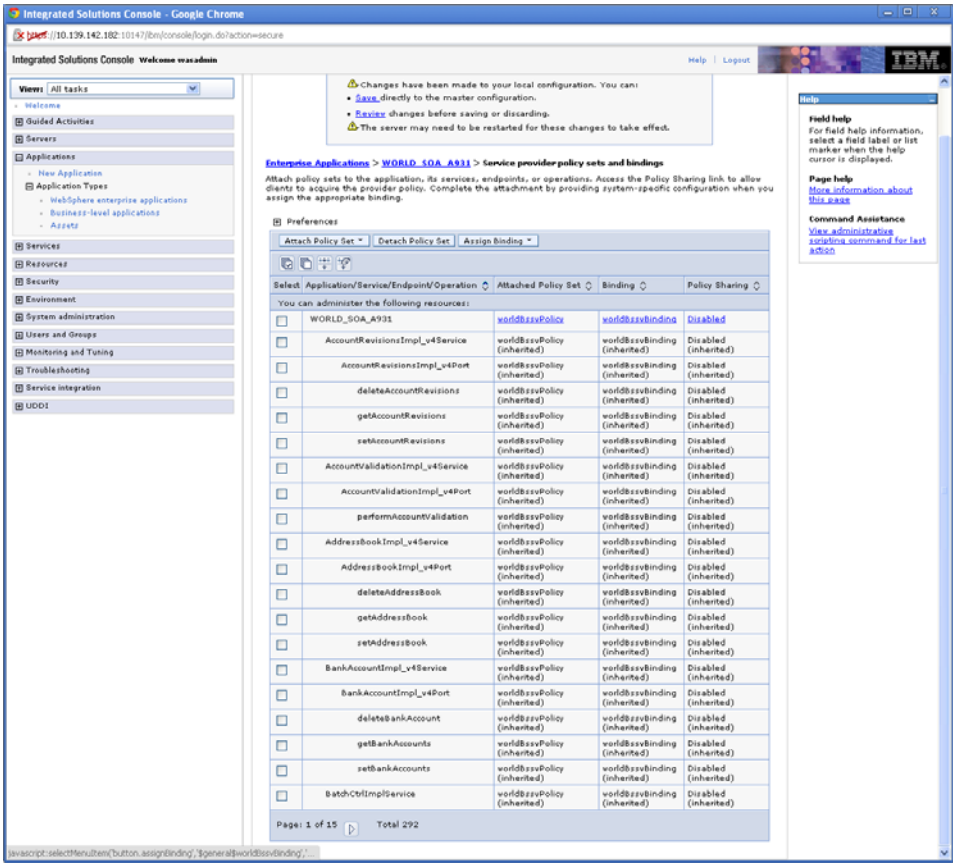


17. Check the box next to WORLD_SOA_A931, and click **Attach Policy Set->worldBssvPolicy**.

> **Note:** This can take several minutes.

18. Check the box next to WORLD_SOA_A931, and click **Assign Binding->worldBssvBinding**.

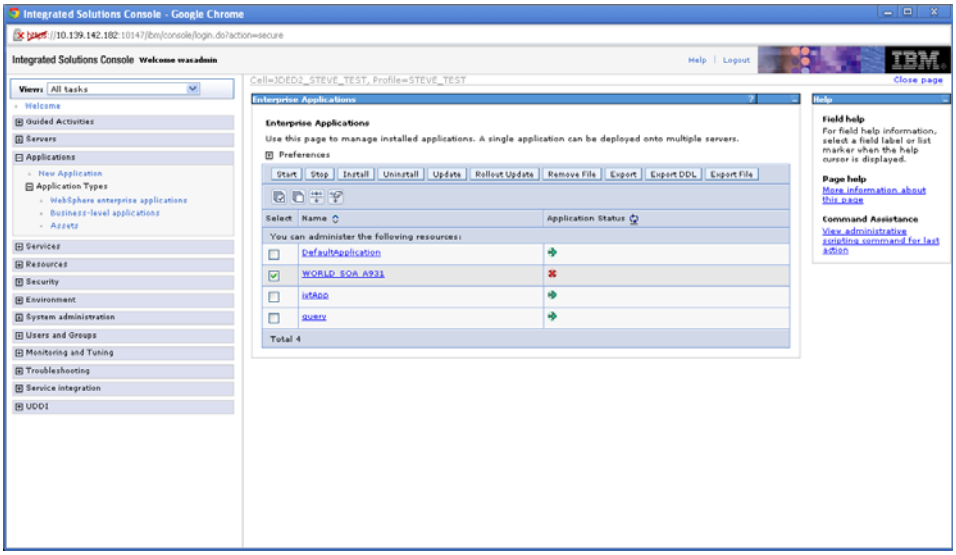
Figure 5–50 Enterprise Applications screen



19. Click Save.

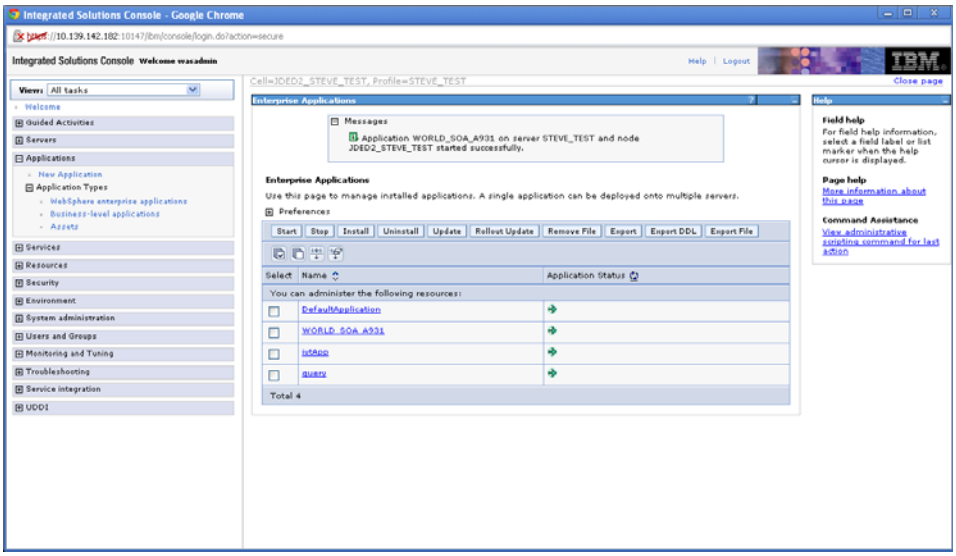
20. On the left hand menu, select **WebSphere enterprise applications**.

Figure 5–51 Enterprise Applications screen



21. Check the box next to WORLD_SOA_A931 and click Start.

Figure 5–52 Enterprise Applications screen



A

Install WebLogic Application Server

This appendix contains the topic:

- Section A.1, "Installing the WebLogic Application Server"

A.1 Installing the WebLogic Application Server

To install the WebLogic Application Server

1. Download Required Jars:

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

   log4j jar- for details about the latest version supported for log4j, see Doc ID 2763469.1 in My Oracle Support. Use the following URL to access and sign in to My Oracle Support:

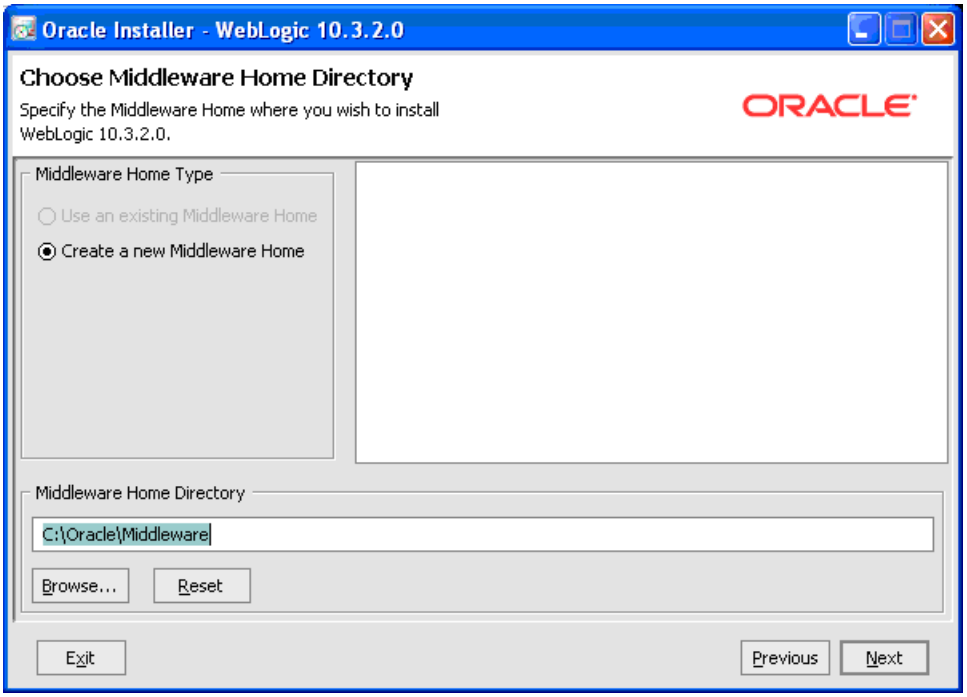
   https://support.oracle.com

   (WS: Instructions to Address JD Edwards World Security Vulnerabilities (Doc ID 2763469.1) (Release A9.4 Update)

WebLogic Installation Instructions

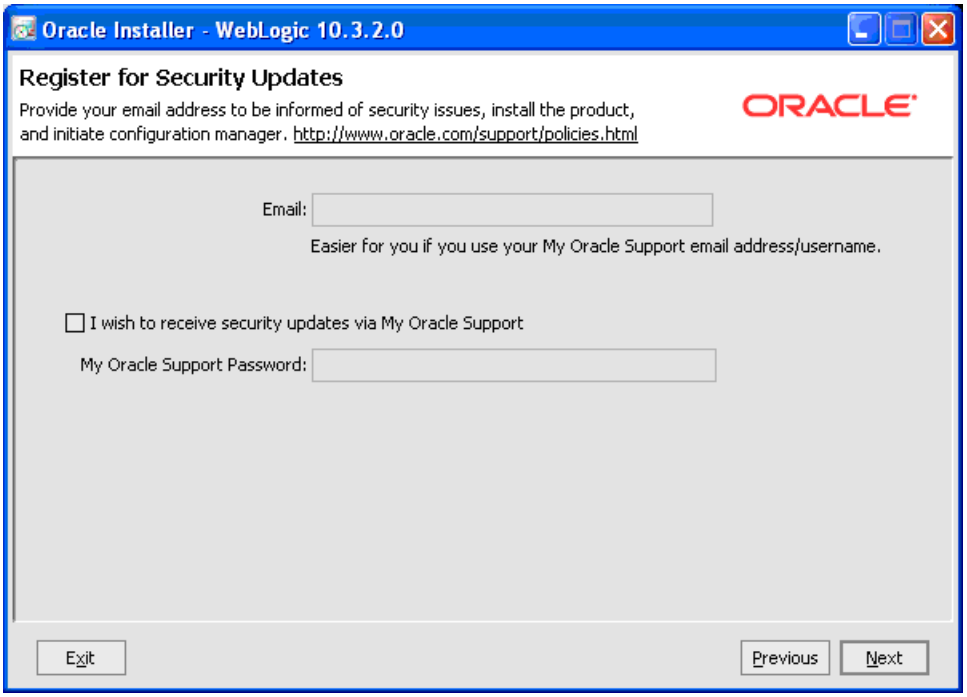
1. Download the WLS server installation file from OTN and install. Use the default values.

Figure A–1 Choose Middleware Home Directory screen



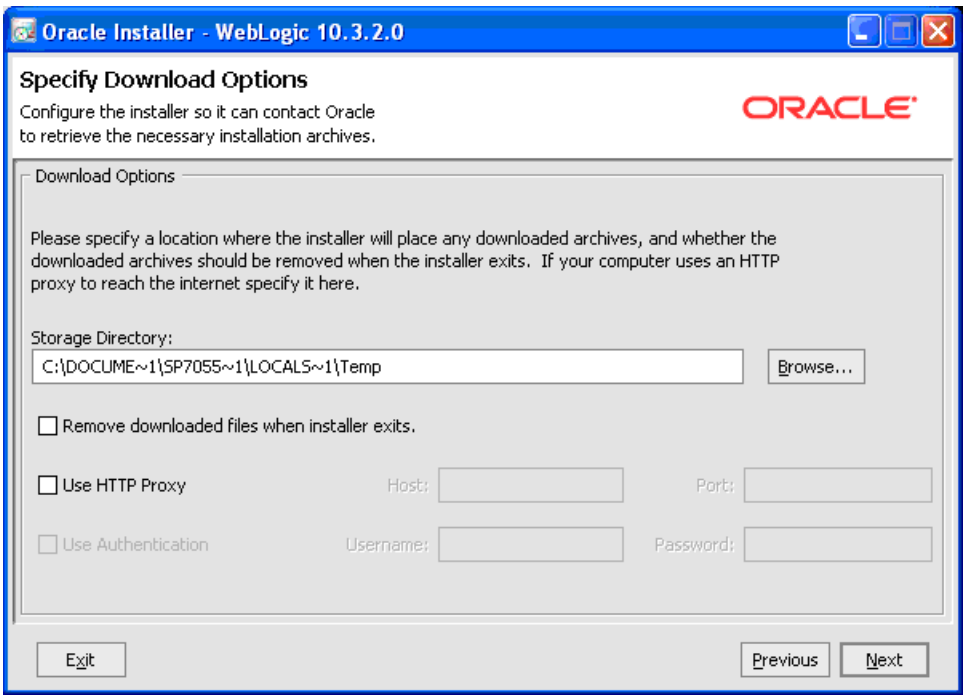
2. Click Next.

Figure A–2 Register for Security Updates screen



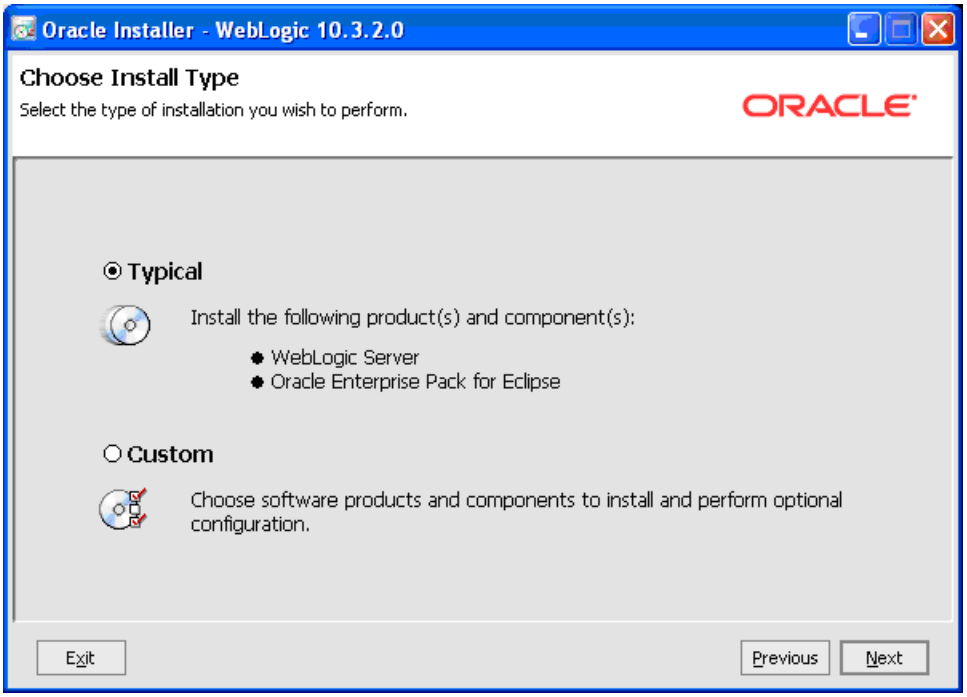
3. Click Next.

Figure A–3 Specify Download Options screen



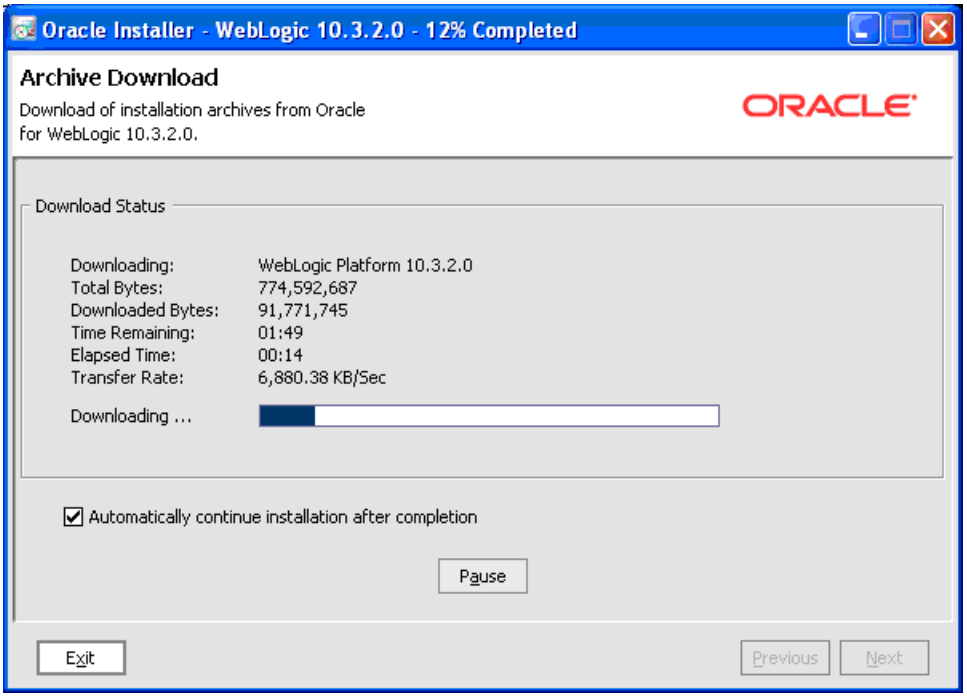
4. Click Next.

Figure A–4 Choose Install Type screen



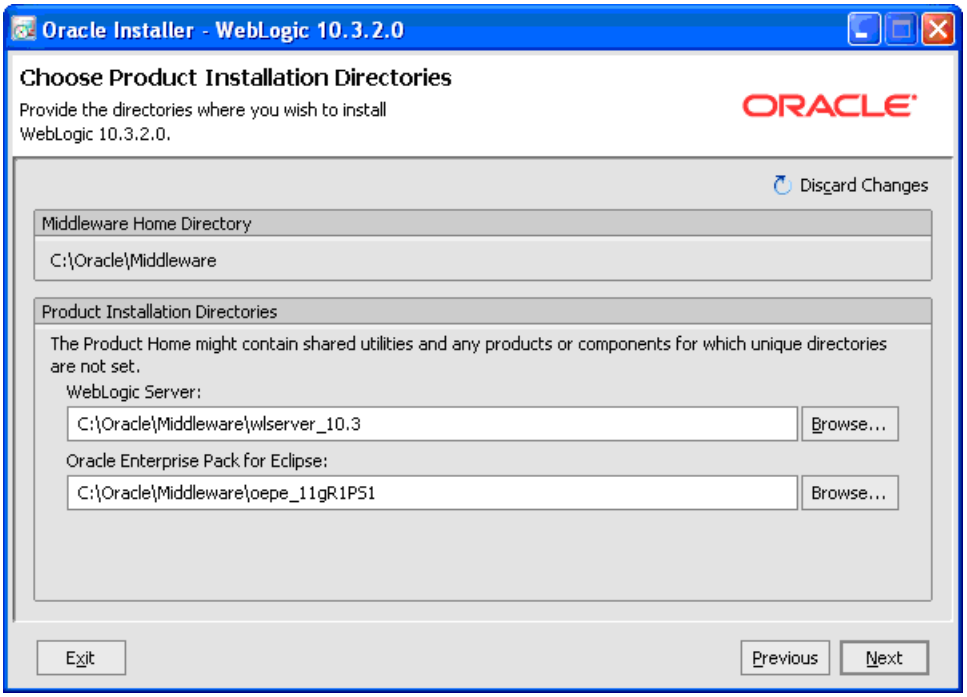
5. Select Typical and then click Next.

Figure A–5 Archive Download screen



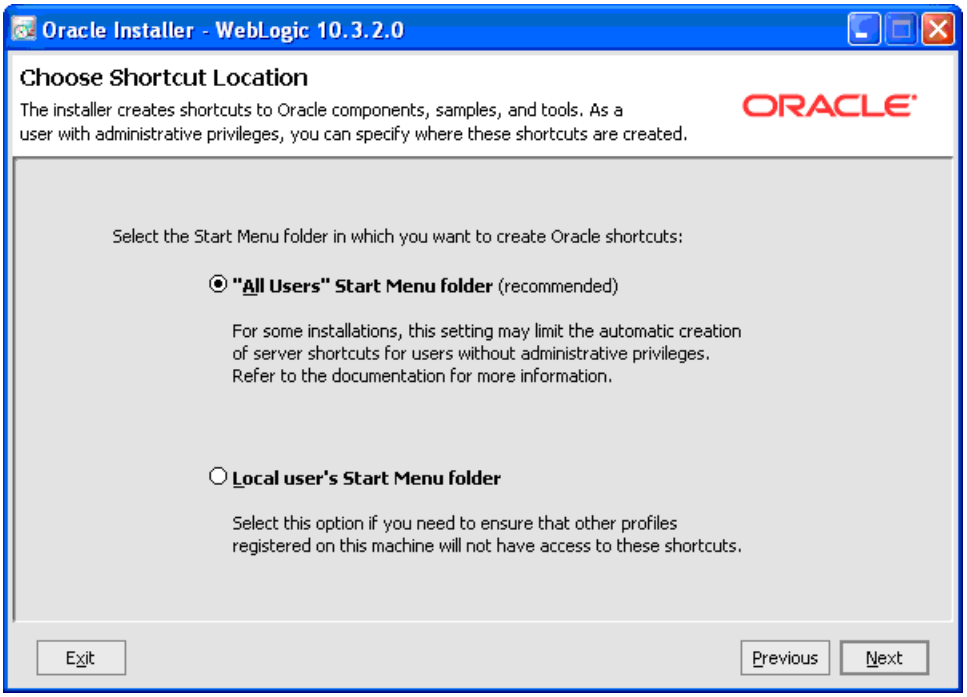
6. Click Next.

Figure A–6 Choose Product Installation Directories screen



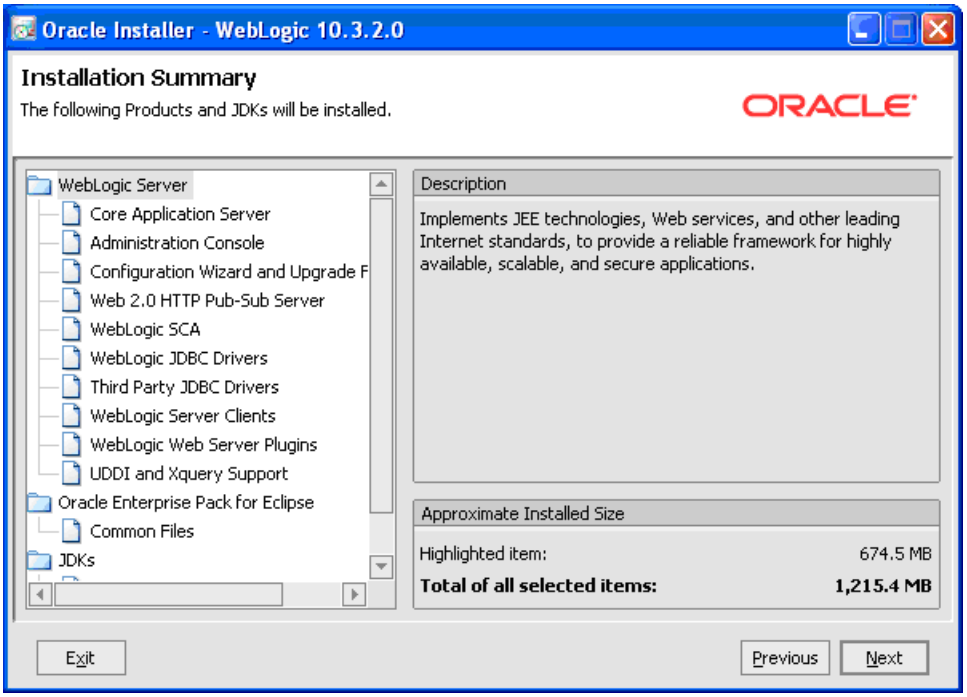
7. Click Next.

Figure A–7 Choose Shortcut Location screen



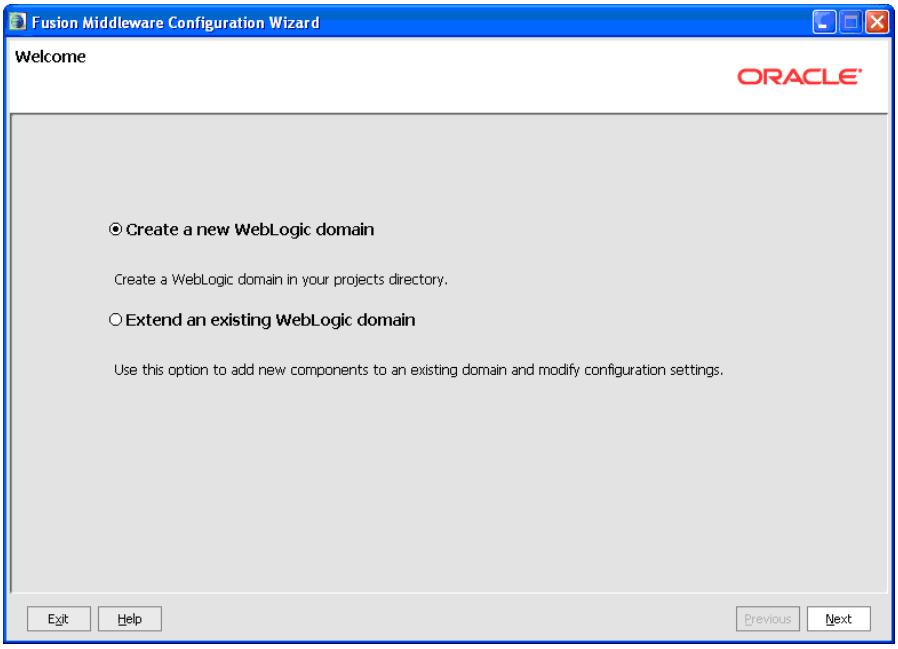
8. Click Next.

Figure A–8 Installation Summary screen



9. Configure the base_domain.

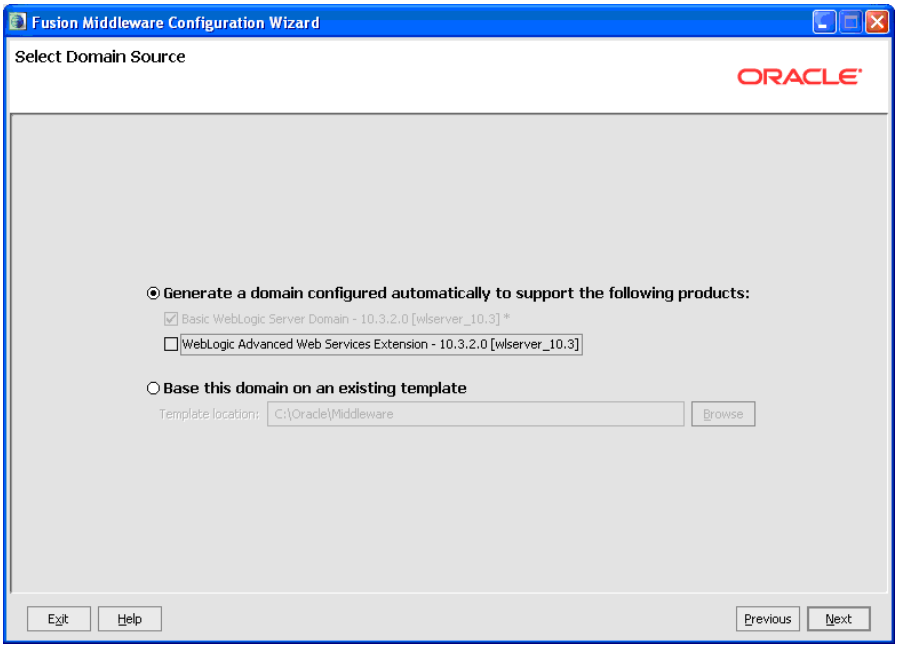
Figure A–9 Create a New WebLogic Domain screen



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

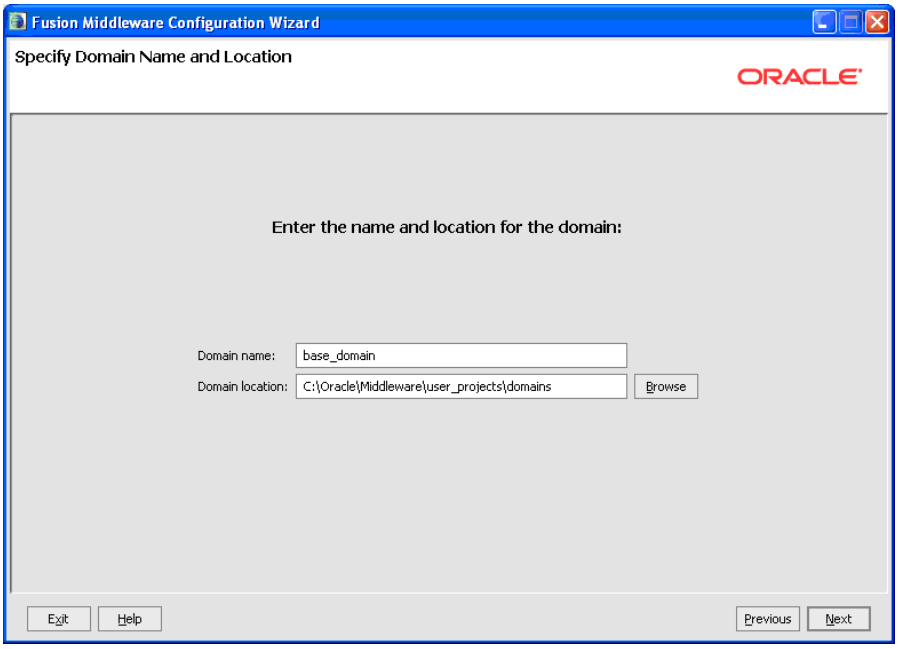
Click Next.

Figure A–10 Select a Domain Source screen



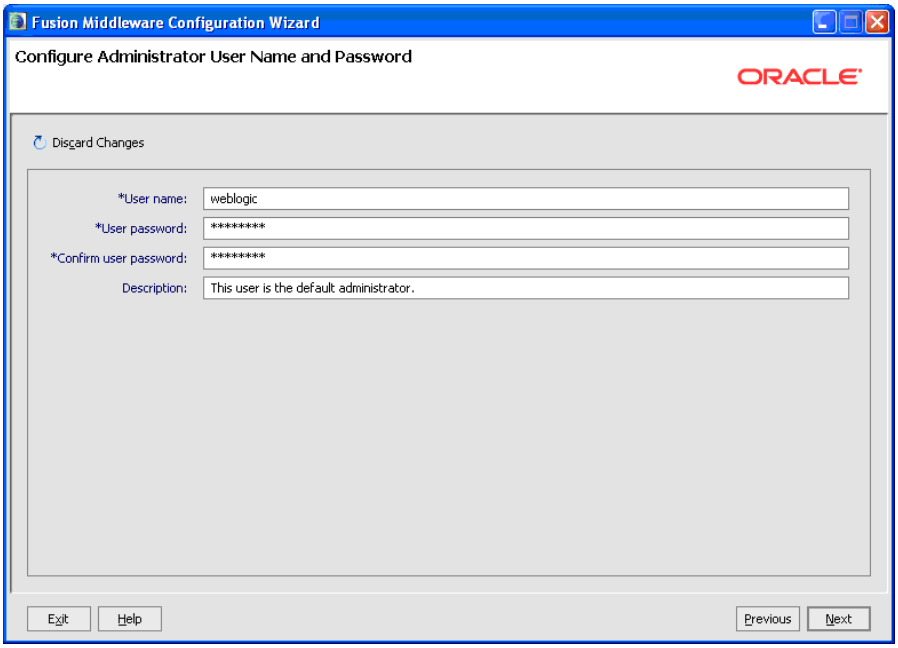
10. Click Next.

Figure A–11 Specify Domain Name and Location screen



11. Click Next.

Figure A–12 Configure Administrator User Name and Password screen

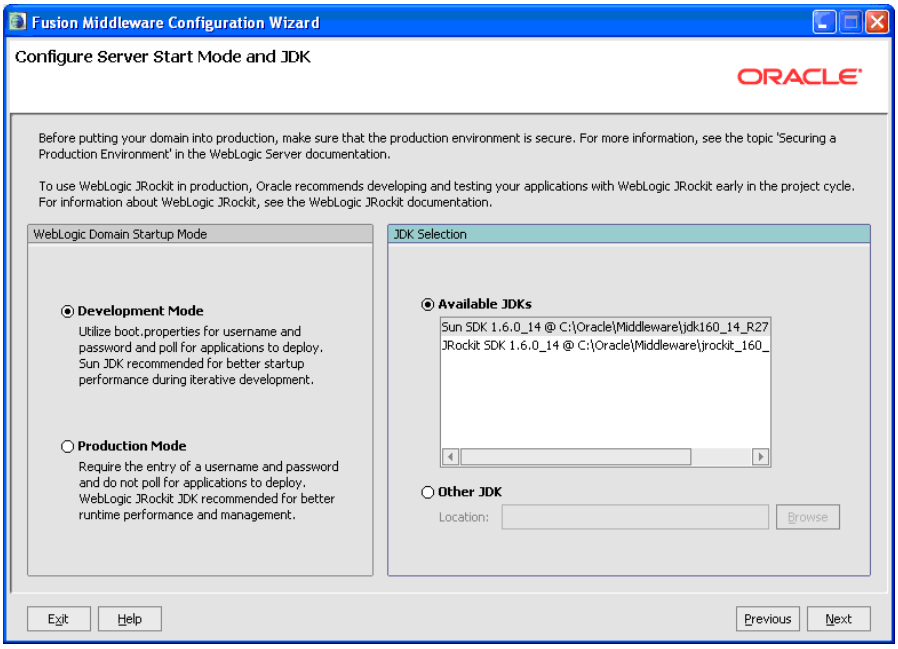


User Password:

"welcome1"

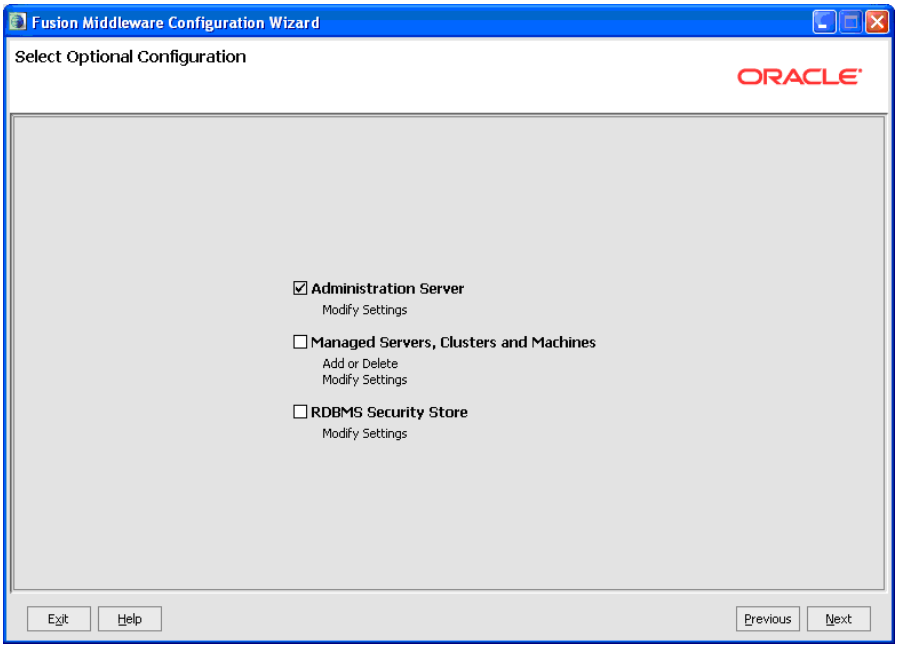
12. Click Next.

Figure A–13 Configure Server Start Mode JDK screen



13. Click Next.

Figure A–14 Select Optional Configuration screen

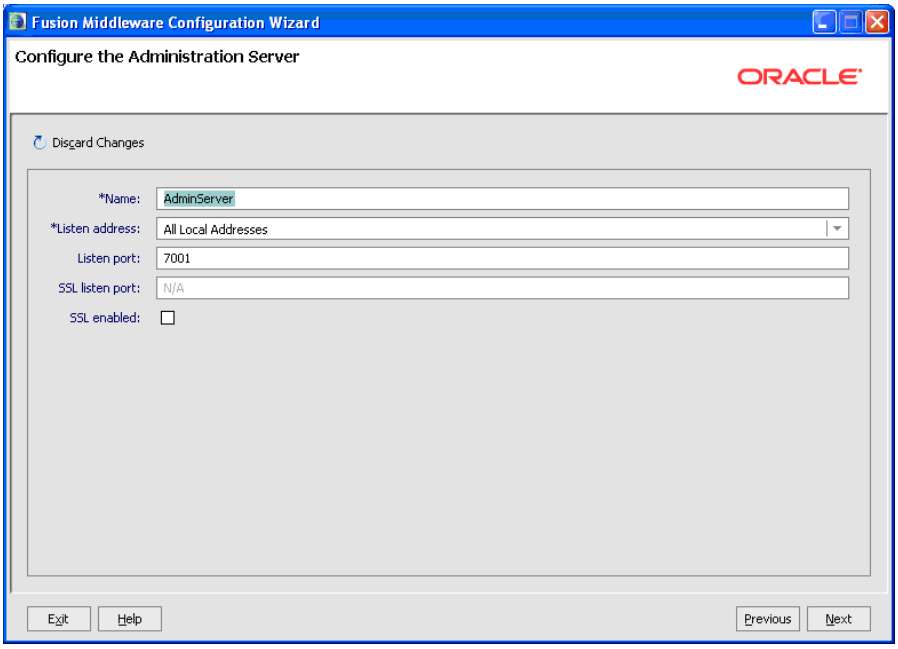


Select:

- Administration Server

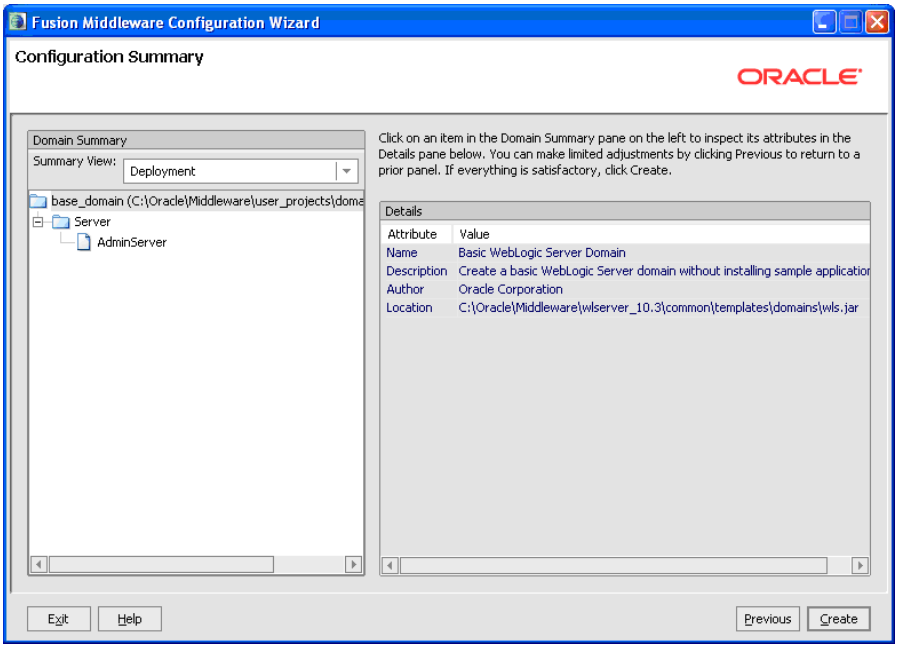
Click Next.

Figure A–15 Configure the Administrator Server screen



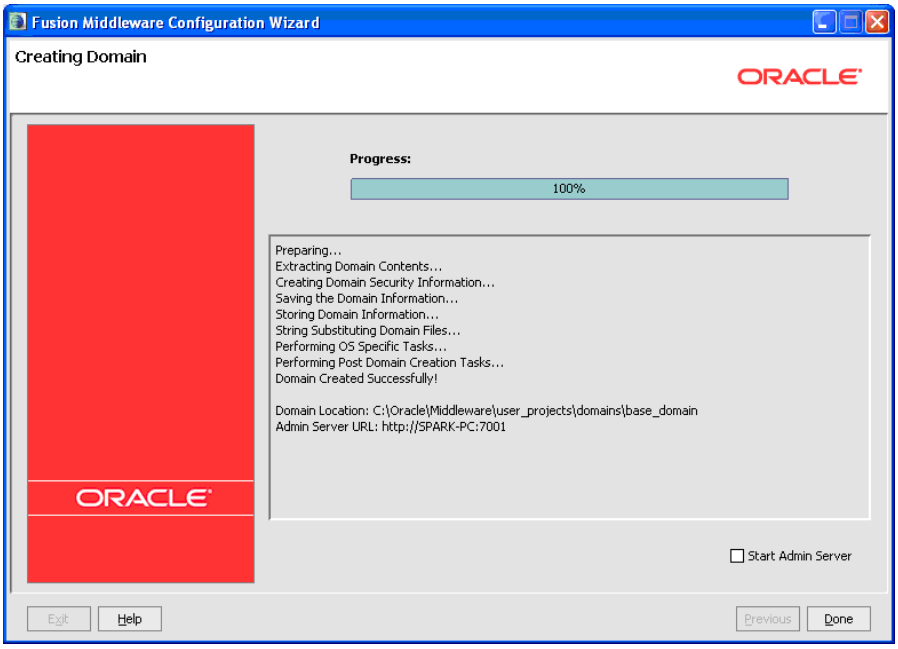
14. Use defaults and click Next.

Figure A–16 Configuration Summary screen



15. Click Create.

Figure A–17 Creating Domain screen



16. 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 A9.4 Update)

17. 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.

B

Create WebSphere Application Server

This appendix contains the topic:

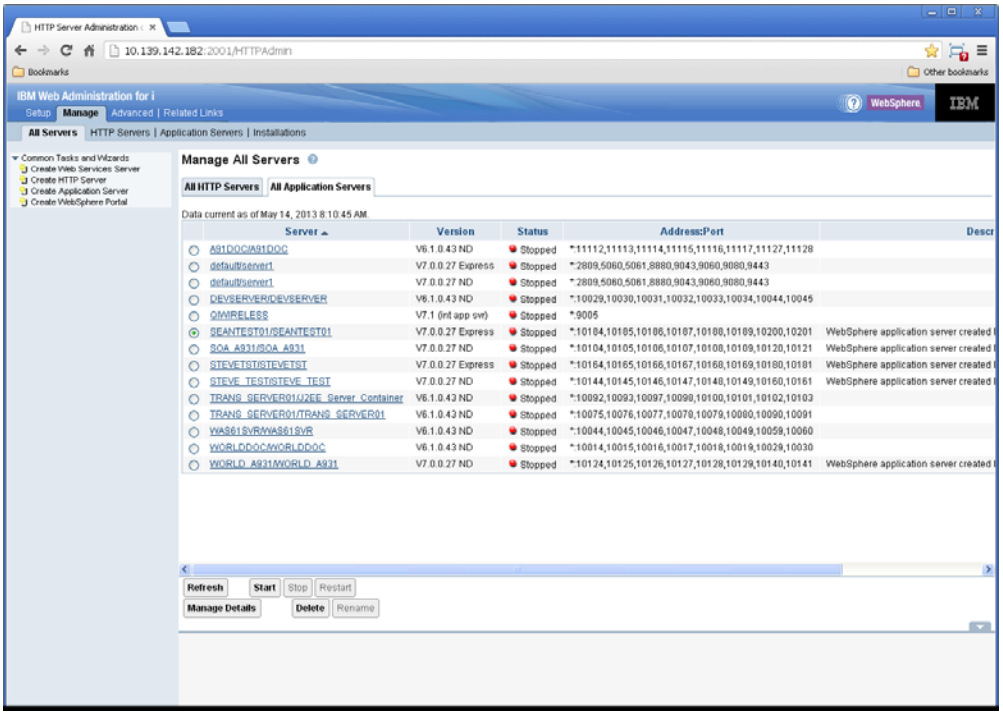
- Section B.1, "Creating the WebSphere Application Server."

B.1 Creating the WebSphere Application Server

To create Application Servers in WebSphere

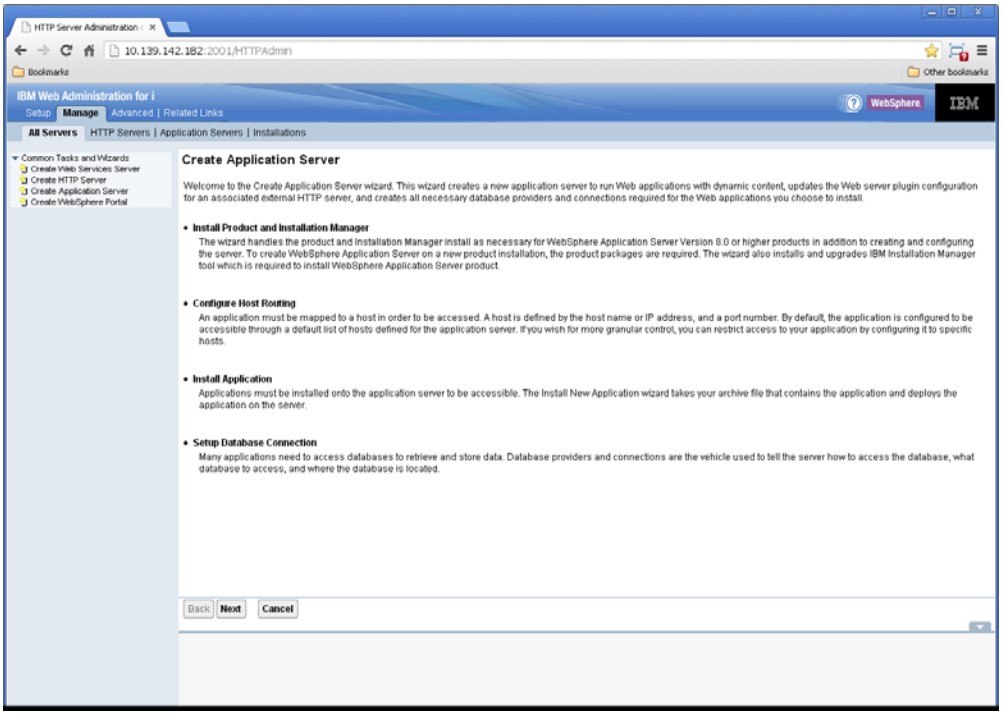
1. Launch the IBM Web Administrator for i: http://localhost:2001/HTTPAdmin.

Figure B–1 IBM Web Administrator screen



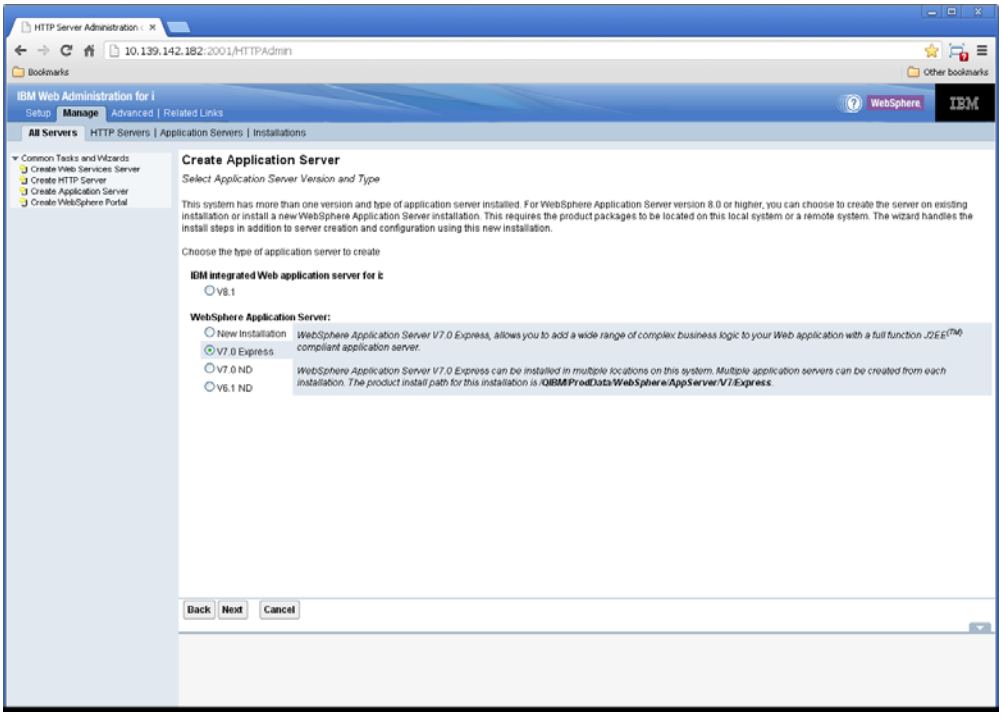
2. Click Create Application Server.

Figure B–2 Create Application Server screen



3. Click Next.

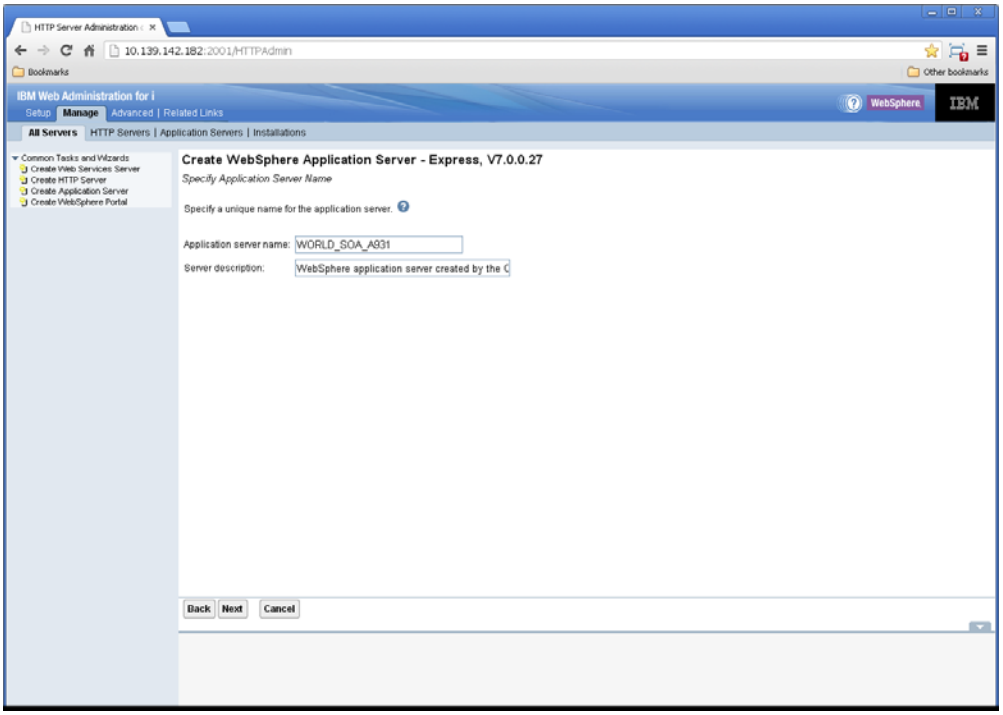
Figure B–3 Create Application Server screen



4. Select the desired WebSphere Application Server version, and Click Next.

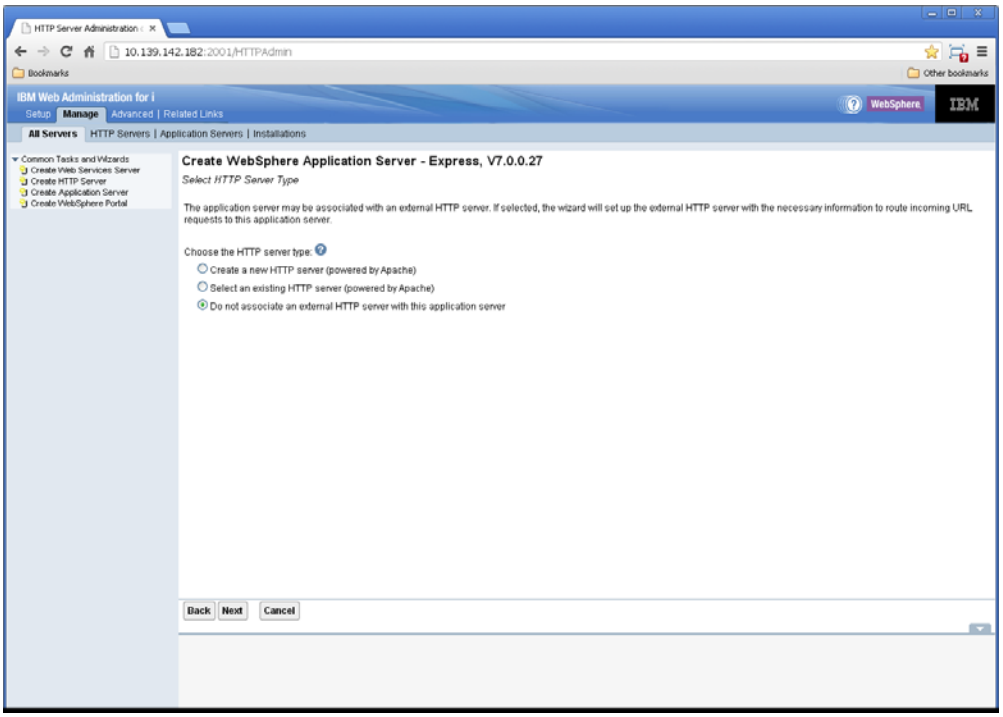
Note: Please refer to the certification information on myoraclesupport.com to determine the certified versions of WebSphere.

Figure B–4 Create WebSphere Application Server screen



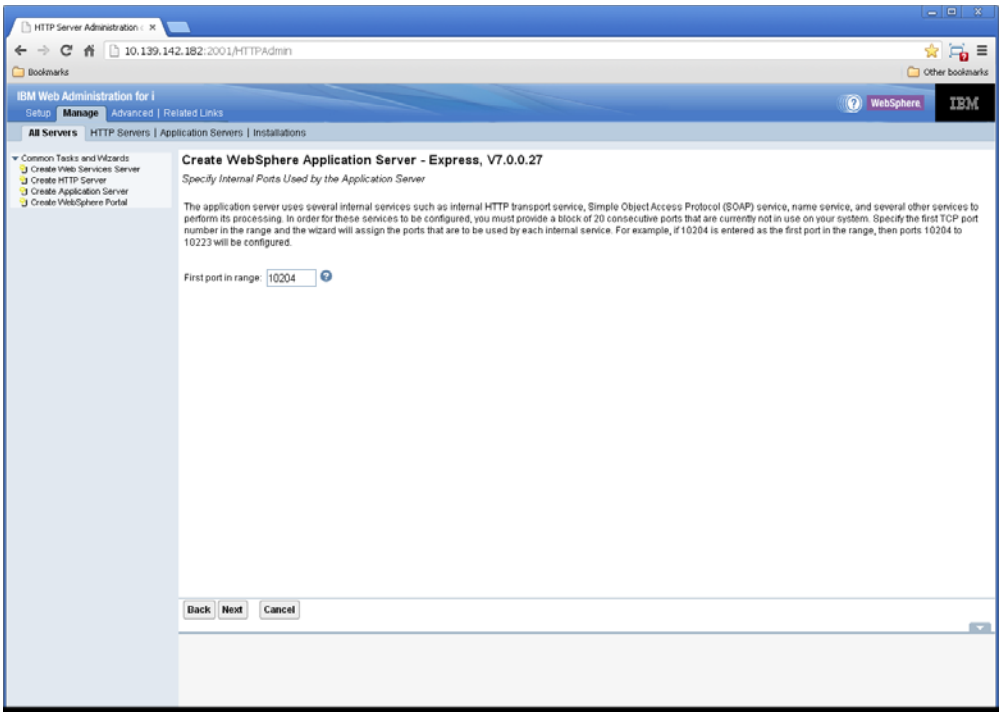
5. Enter Application Server Name and Description and then click Next.

Figure B–5 Create WebSphere Application Server screen



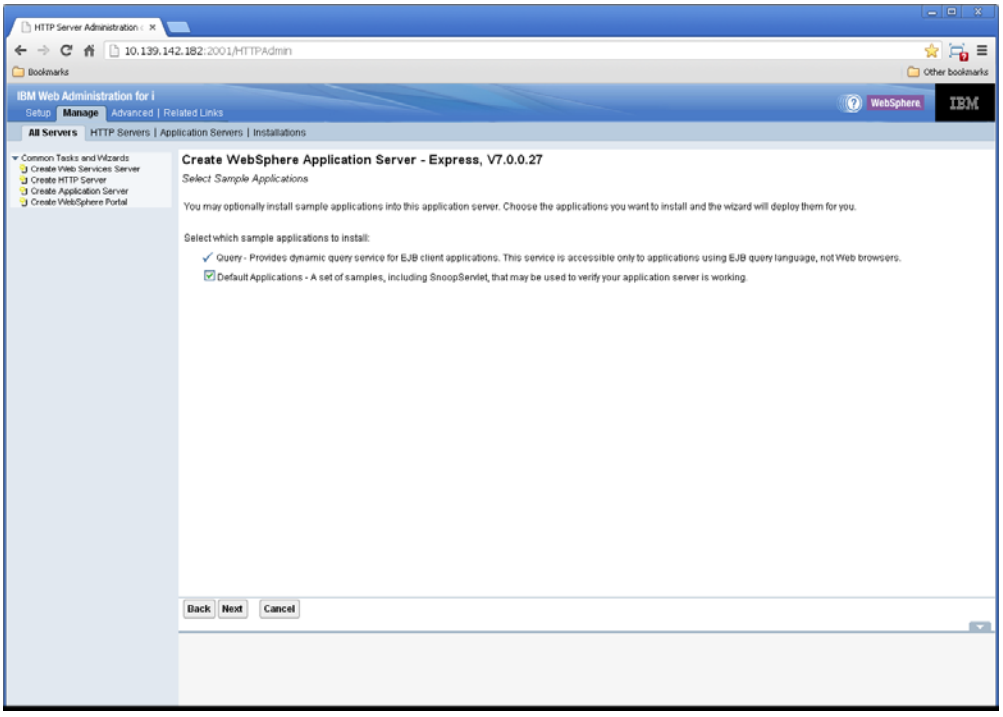
6. Select **Do not associate an external HTTP server with this application server** and then click Next.

Figure B–6 Create WebSphere Application Server screen



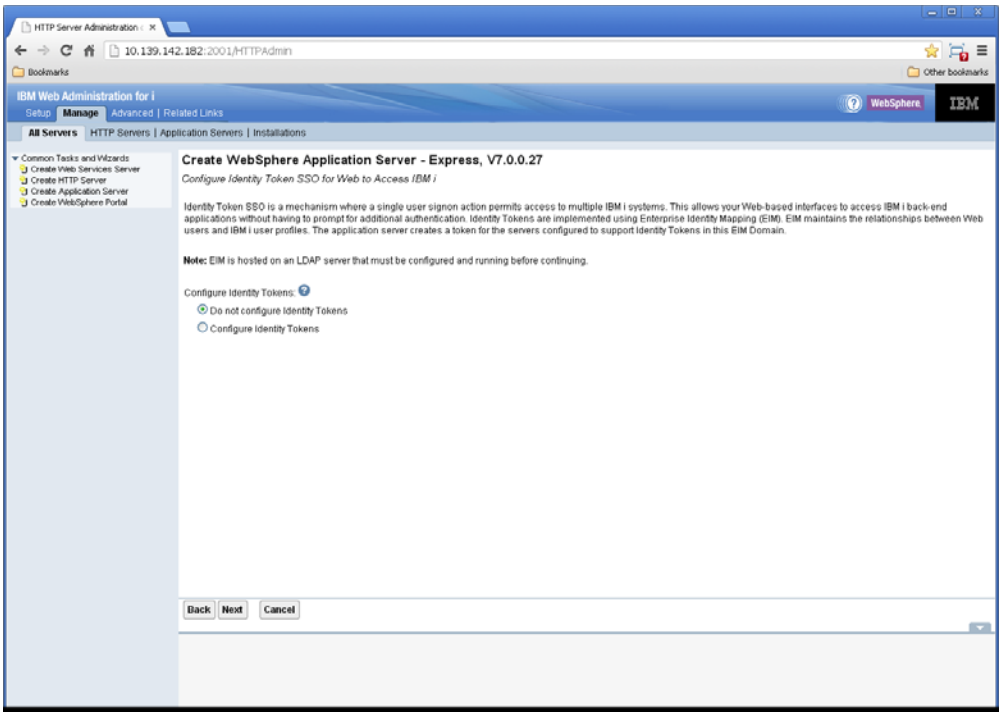
7. Click Next.

Figure B–7 Create WebSphere Application Server screen



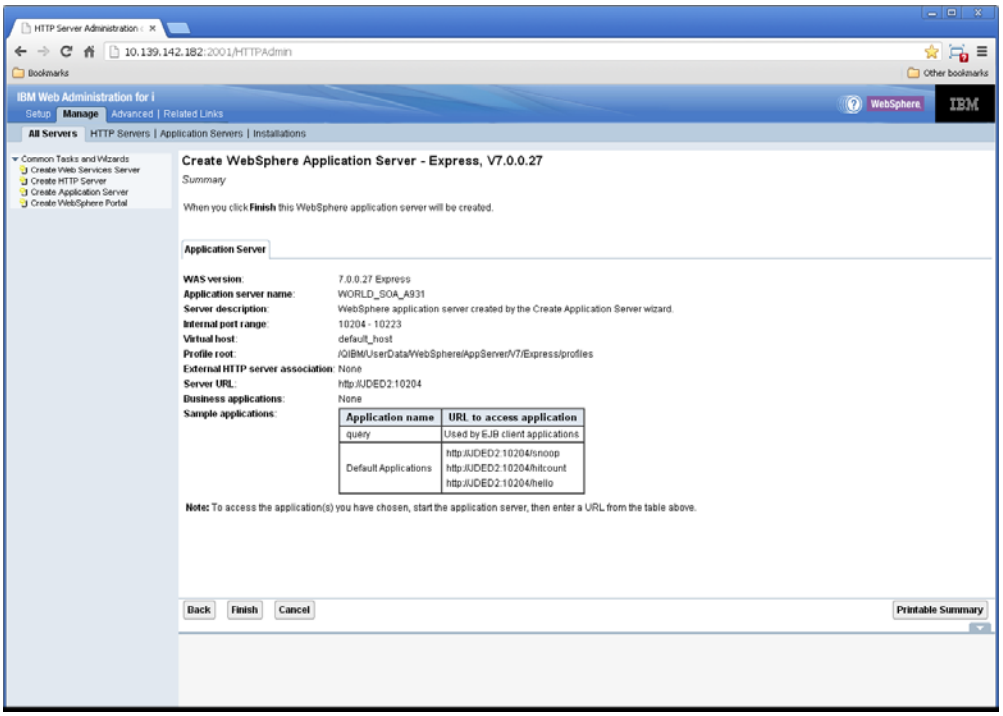
8. Click Next.

Figure B–8 Create WebSphere Application Server screen



9. Click Next.

Figure B–9 Create WebSphere Application Server screen



10. Click Finish.

C

Code and Deploy Your Own Web Services

This appendix contains these topics:

- Section C.1, "Coding and Deploying Your Own Web Services,"
- Section C.2, "Deployment Profiles."

C.1 Coding and Deploying Your Own Web Services

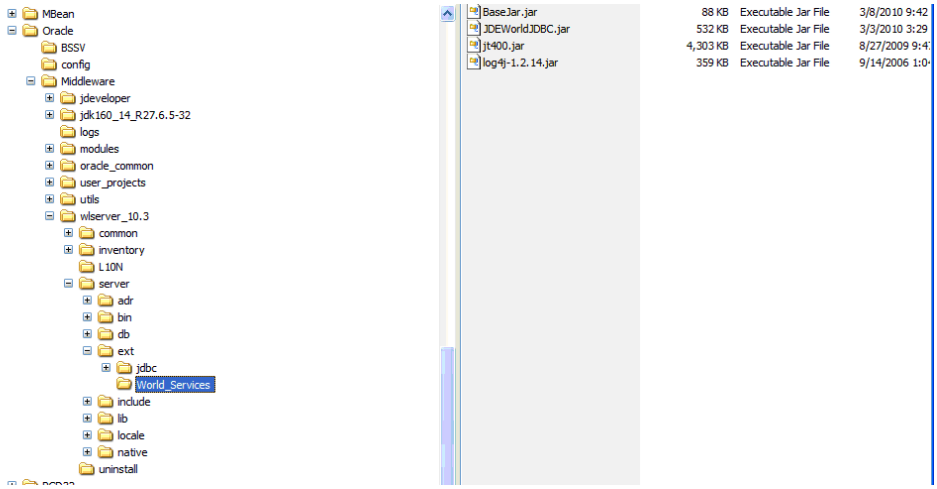
To code and deploy your own Web Services

- 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 JD Edwards World system.
- Use the Connection to access the JD Edwards 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.

C.2 Deployment Profiles

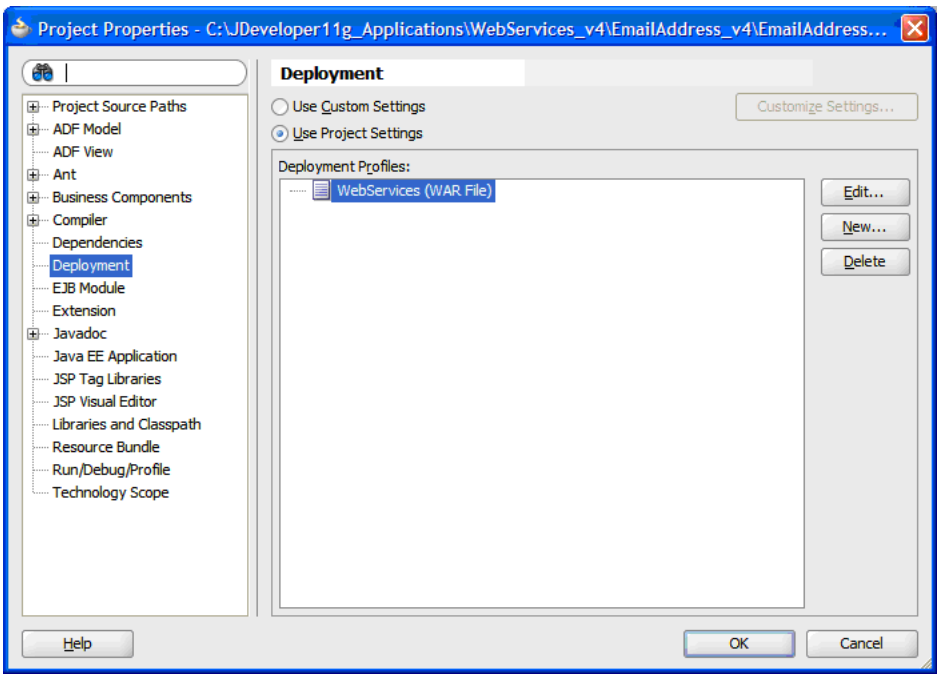
The jar files required for the Web Services were configured in the previous procedure by adding the jar files to the World_Services folder and setting the server classpath to include these jars.

Figure C–1 World_Services Folder



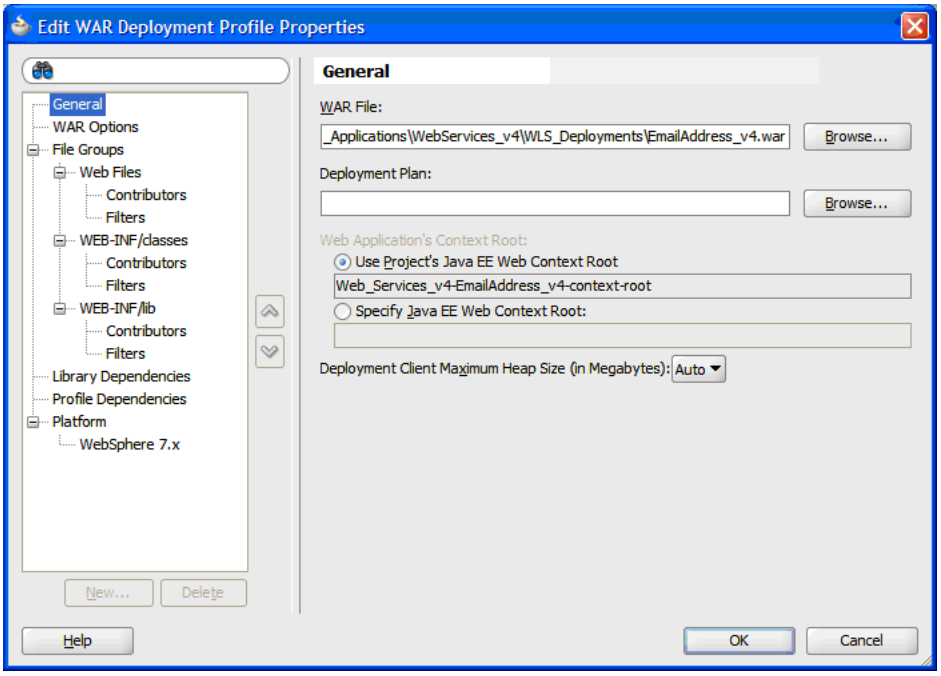
In Jdeveloper, the individual projects only need to deploy those files that are required by the web service.

Figure C–2 Project Properties screen



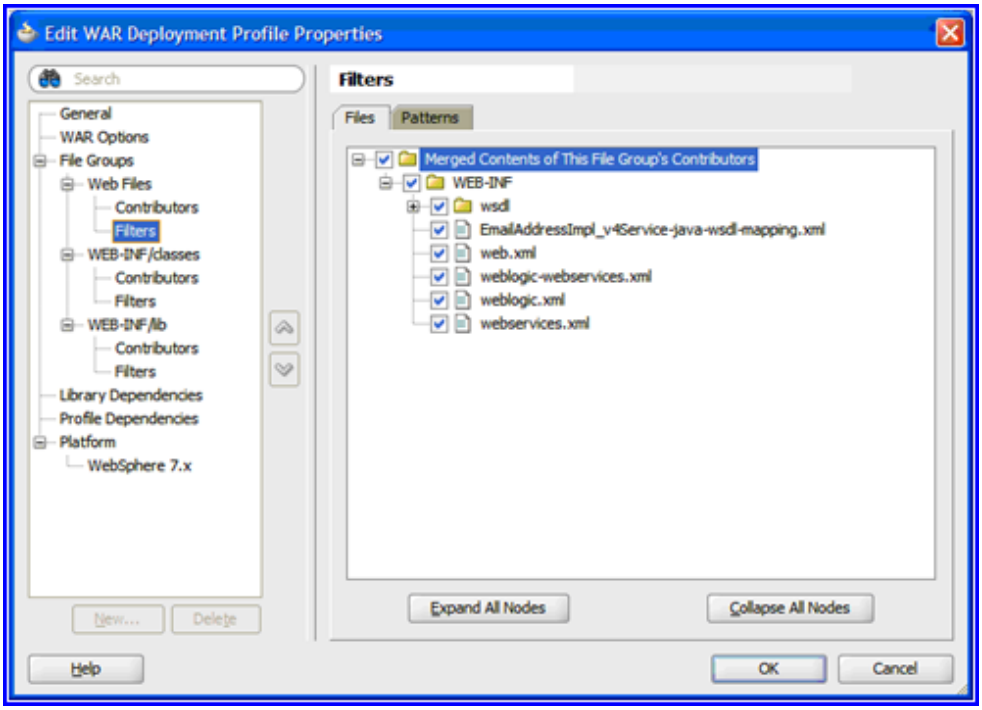
1. Highlight WebServices(WAR File) and then click Edit.

Figure C–3 Edit WAR Deployment Profile Properties screen



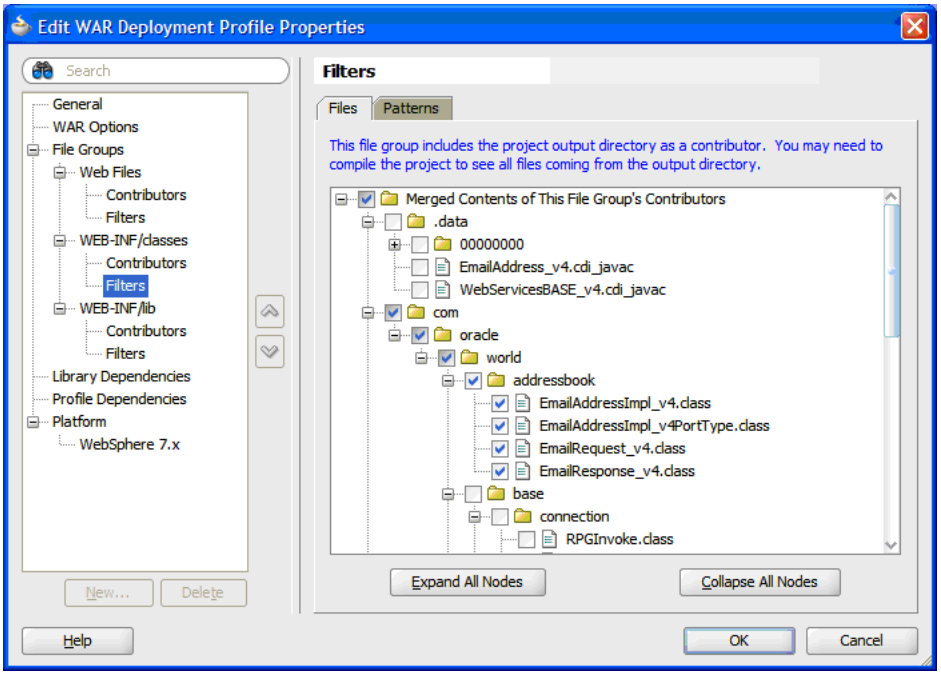
2. Enter a path where you want your WAR file created.

Figure C–4 Edit WAR Deployment Profile Properties screen



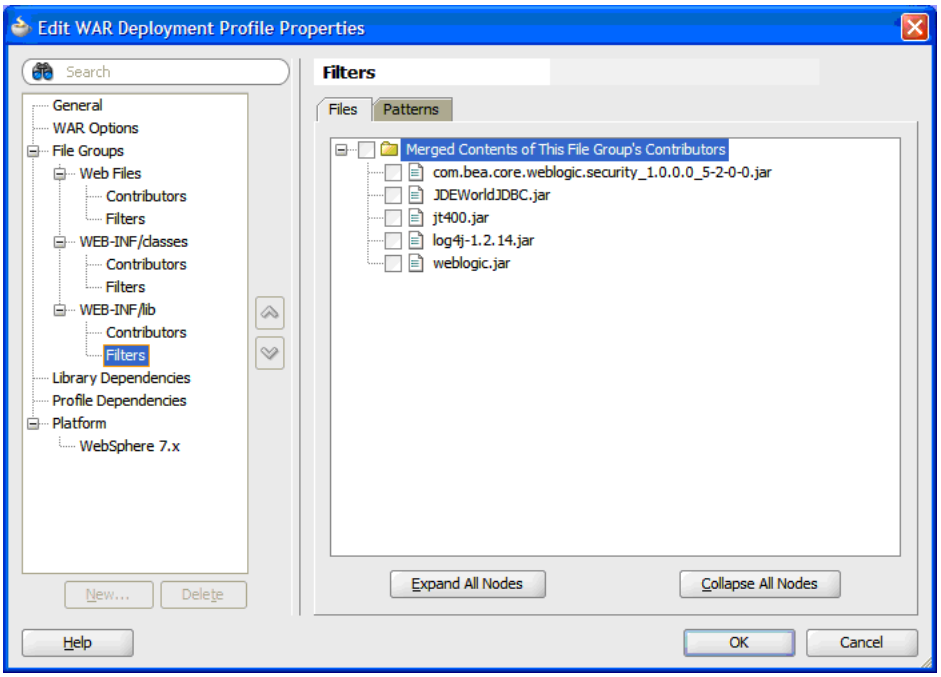
3. Under Web Files > Filters, select all files.

Figure C–5 Edit WAR Deployment Profile Properties screen



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



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.

D

Uninstall Service Enablement

This appendix contains the topic:

- Section D.1, "Uninstalling Service Enablement."

D.1 Uninstalling Service Enablement

To uninstall Service Enablement

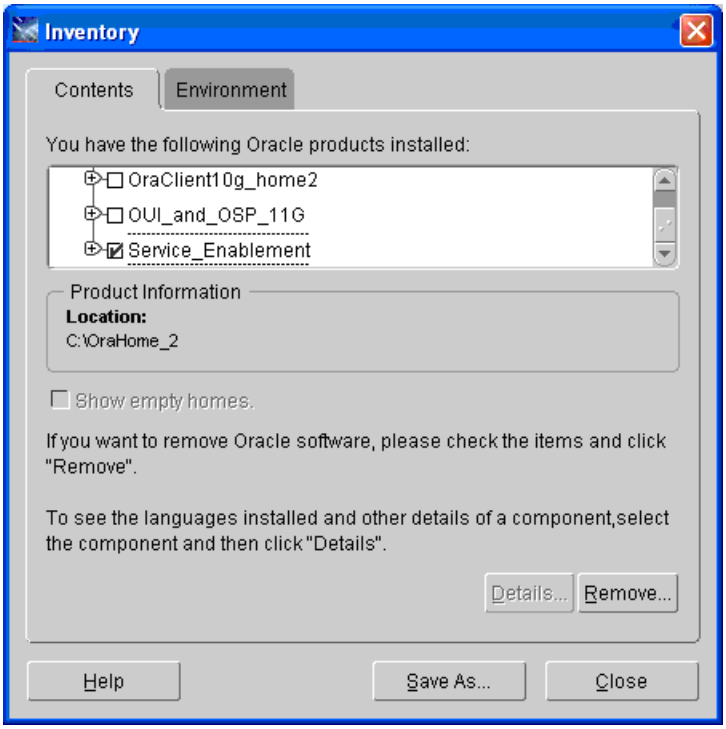
If you need to uninstall JD Edwards World Service Enablement, use the OUI installer.

Figure D–1 OUI Installer Welcome screen

1. Start the OUI installer:

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

Figure D–2 Inventory screen

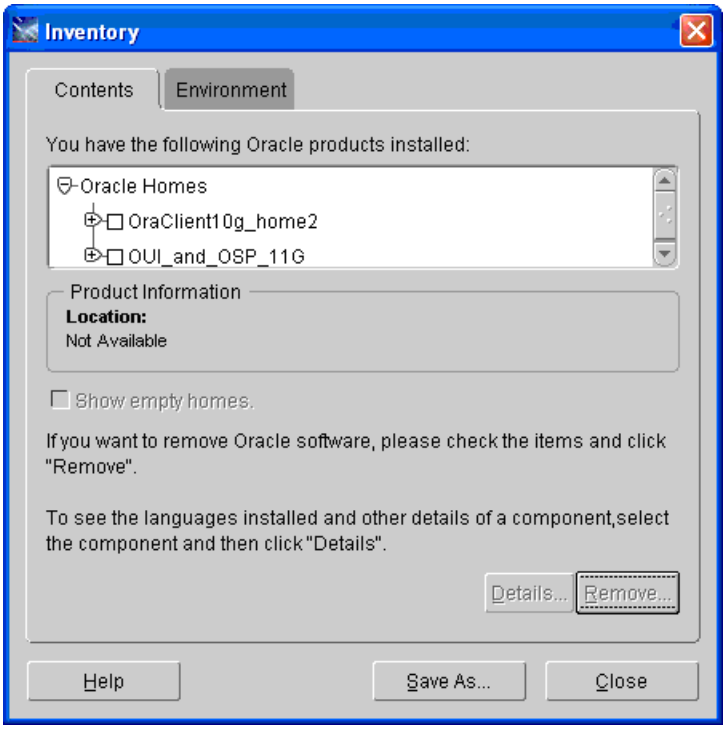


2. Select the checkbox of the Service Enablement folder name you created and then click Remove.

Figure D–3 Confirmation screen

3. On the Confirmation screen, click Yes.

Figure D–4 Inventory screen

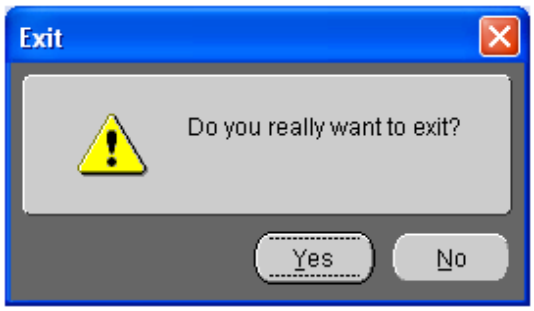


4. On the Inventory screen, click Close.

Figure D–5 End of Installation screen

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

Figure D–6 Exit screen



6. On the Exit screen, click Yes.