JD Edwards EnterpriseOne Tools

IBM WebSphere Portal for Microsoft Windows Guide

9.2

JD Edwards EnterpriseOne Tools
IBM WebSphere Portal for Microsoft Windows Guide

9.2

Part Number: E53530-05

Contents

Preface i

1 Overview 1

Overview 1

2 Installing the WebSphere Portal Server 3

Prerequisites 3

Preparing the Microsoft Windows Operating System 4

Installing the Portal Server 4

Registering the WSRP Provider 38

3 Using the Migration Wizard 63

Using the Migration Wizard 63

Using the Migration Wizard 64

4 Database Configuration for WebSphere Portal 101

Database Configuration for WebSphere Portal 101

5 Configuring IBM WebSphere Portal Server v8.5 to use Oracle Database 103

Configuring IBM WebSphere Portal Server v8.5 to use Oracle Database 103

Before You Begin 103

Creating the Oracle Database for IBM WebSphere Portal Server v8.5 104

Oracle Database Setup Considerations 121

6 Verifying Database Connections 125

Verifying Database Connections 125

Verifying Database Connections 125

7 Configuring the Microsoft Active Directory for Portal 127

Installing Microsoft Active Directory for Microsoft Windows 200x 127

Working with LDAP Attributes 137
Configuring LDAP Server for Dynamic Group Queries 141
Configuring a Portal to Use LDAP Referrals 142
Enabling Security with the LDAP Directory 142
Configuring an External HTTP Server for WebSphere Portal v8.5 143
Installing the JD Edwards Collaborative Portal 150

8 Appendix A - Start and Stop Portal Servers 151
Start and Stop Portal Servers 151
Starting and Stopping the WebSphere Portal Administration Server (server1) 151
Starting server1 (Portal Administration Server) 151
Stopping server1 (Portal Administration Server) 152
Starting and Stopping the WebSphere Portal Server 152
Starting the WebSphere Portal Server 152
Stopping WebSphere Portal Server 152

9 Appendix B - Example of a PortalUsers.ldif File 155
Example of a PortalUsers.ldif File 155

10 Glossary 157
DBCA 157
JAR file 157
JDBC 157
LDAP directory 157
MTR 157
WAR file 157
WAS 158

Preface

Welcome to the JD Edwards EnterpriseOne documentation.

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 EnterpriseOne applications, features, content, and training, visit the JD Edwards EnterpriseOne pages on the JD Edwards Resource Library located at:

http://learnjde.com

Conventions

The following text conventions are used in this document:

Convention	Meaning
Bold	Boldface type indicates graphical user interface elements associated with an action or terms defined in text or the glossary.
Italics	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`Monospace`	Monospace type indicates commands within a paragraph, URLs, code examples, text that appears on a screen, or text that you enter.
> Oracle by Example	Indicates a link to an Oracle by Example (OBE). OBEs provide hands-on, step- by-step instructions, including screen captures that guide you through a process using your own environment. Access to OBEs requires a valid Oracle account.

1 Overview

Overview

This document describes the process of installing and configuring WebSphere Portal Server v8.5. Before beginning the installation, verify that your environment meets the requirements by referring to the Minimum Technical Requirements document for Collaborative Portal 8.5, which is referenced in this section of this guide: Minimum Technical Requirements.

This document steps the installer through the installation, upgrade, and configuration of the WebSphere Portal Server environment and its related components. The document includes sections on databases transfer, security, and LDAP. WebSphere Portal v8.5 includes an install wizard that eases the entire installation process.

WebSphere Portal v8.5 includes an install wizard to make the overall installation process friendlier. The installation wizard can be used for post installation processes such as database transfer, disable and enable security and configure LDAP server.

2 Installing the WebSphere Portal Server

Prerequisites

The following sections discuss the prerequisites for installing the Websphere portal server.

Minimum Technical Requirements

Before you install Portal v8.5, you must first install WebSphere Application Server 8.5.5.6 and the latest supported fix pack listed in the JD Edwards EnterpriseOne HTML Web Server Minimum Technical Requirements (MTRs). These MTRs are available on My Oracle Support in document ID 705409.1 and can be accessed at this link:

https://metalink3.oracle.com/od/faces/secure/km/DocumentDisplay.jspx?id=705409.1

Installing WebSphere Application Server 8.5.5.6

To install WebSphere Application Server 8.5.5.6, refer to Chapter 3: Installing and Configuring WebSphere Application Server 8.5.5.6 in the JD Edwards EnterpriseOne HTML Web Server Reference Guide for Microsoft Windows-Based Systems and WebSphere Application Server 8.5.5.6. This document is available on My Oracle Support in document ID 705495.1 and can be accessed at this link:

https://metalink3-dr.oracle.com/od/faces/secure/km/DocumentDisplay.jspx?id=705495.1

If you are using same single physical machine for both the Portal and the HTML Server, you cannot install the JD Edwards EnterpriseOne HTML Web Server (also called JAS) to the same profile as that of Portal. By default, WebSphere Portal v8.5 creates a separate profile called wp_profile.

References

IBM product documentation for Portal v8.5:

http://www.ibm.com/developerworks/websphere/zones/portal/proddoc/index.html

http://www-10.lotus.com/ldd/portalwiki.nsf/xpViewCategories.xsp?lookupName=IBM%20WebSphere%20Portal%207%20Product%20Documentation&SessionID=CWFHNIG8CY

IBM WebSphere Application Server 8.5.5.6 Info Center:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

IBM Portal v8.5 Hardware and Software Requirements:

http://www-01.ibm.com/support/docview.wss?uid=swg27007791

Preparing the Microsoft Windows Operating System

Use these steps to prepare your Microsoft Windows operating system for the installation of Portal 8.5 components:

1. Check that the system logon user ID you will use during installation has the following permissions and rights:
   - The user ID must already exist prior to installation.
   - The user ID must belong to the Administrators group.
2. Perform these steps to determine if a user account is a member of the Administrators group:
   a. Click Start > Programs > Administrative Tools > Computer Management.
   b. Expand Local Users and Groups and select Groups.
   c. Open the Administrators group to see what members belong to it.
   d. Add the user to the Administrators group if necessary.
3. Consider these recommendations when installing to avoid excessively long path names:
   - Specify short cell and node names; do not use names longer than 5 characters. For example, you might use scell instead of stonemillNode01cell.
   - Ensure there are no special characters in the node and/or cell names as they are known to cause problems during install.
   - Name WAR files with less than 21 characters. If necessary, modify the file name before installing.
   - Refer to the following tech note for additional information: WKSP0016E - 'Filename is too long error' in Microsoft Windows..

     > **Note:** If you exceed the 259 maximum character length, you may receive one of these error messages during configuration or in the wpinstalllog.txt file: · The input line is too long. · The syntax of the command is incorrect. · The filename is too long.
4. If you are installing on a server with a firewall enabled, disable the firewall before installing. If you do not disable the firewall and the installation program detects it, a warning message might be displayed during the installation.

Installing the Portal Server

To begin the installation

1. Download the WebSphere Portal 8.5 software from the IBM support site.
2. From either the Setup CD or directory, you can use various methods to launch the installer, as shown in this table (it is recommended to use Graphical user interface for installation):

Installation Method	Command and Description
Graphical user interface	install
Console mode	install -console

Installation Method	Command and Description
Silent install	install -options “path_to_file\response_filename" where path_to_file is the full path to the response file, and where response_filename is the name of the file. A sample install response file (installresponse.txt) and a sample uninstall response file (uninstallresponse.txt) are located in the root directory of the Setup CD. Important: Do not place the response file in a path that contains a space and do not put a space in the file name.

Installation Method	Command and Description

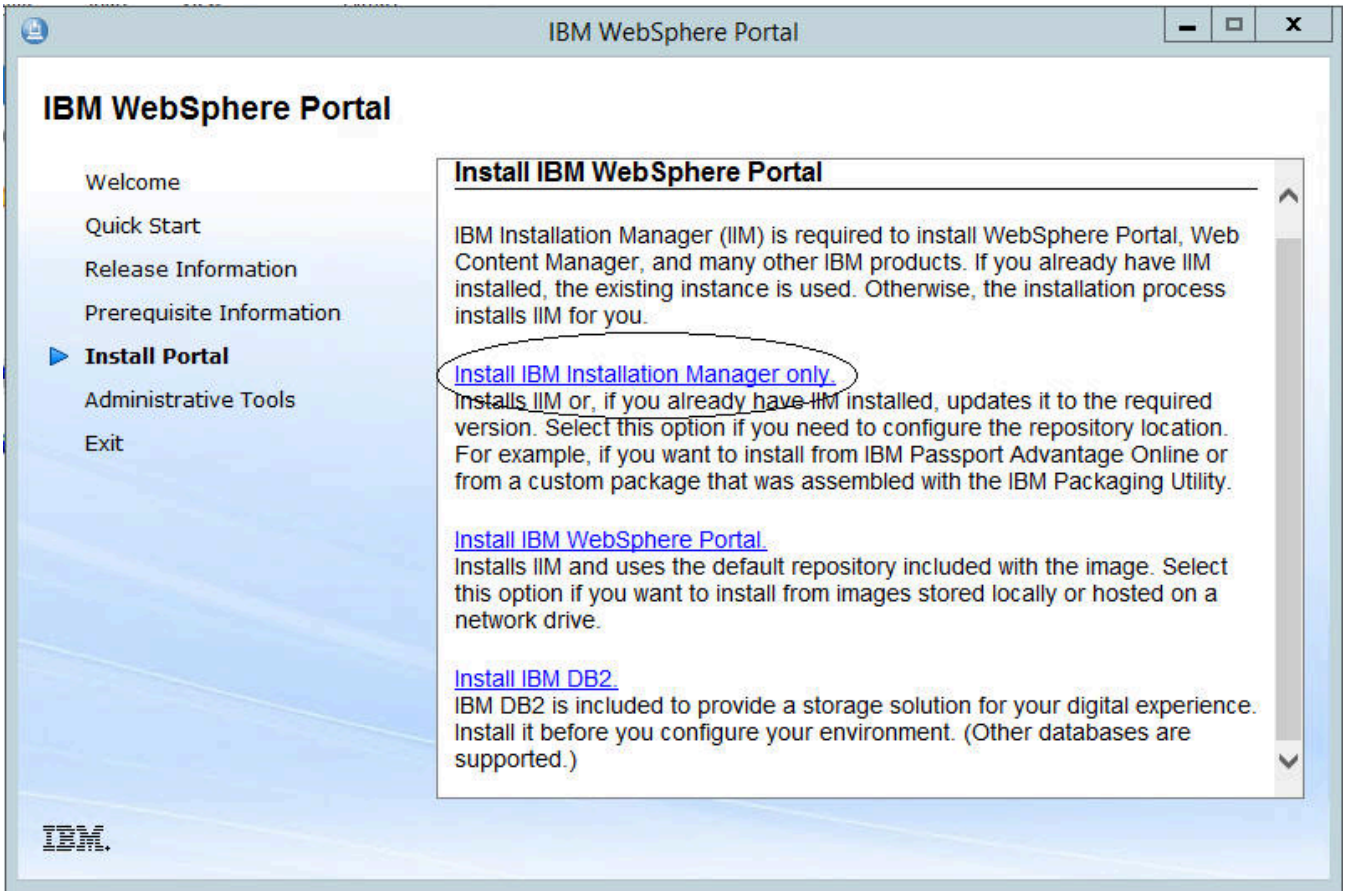
Note:

If the installation program does not detect a WebSphere Application Server instance that you know exists, exit the installation program and re-run it using command line options to specify the WebSphere Application Server instance location.

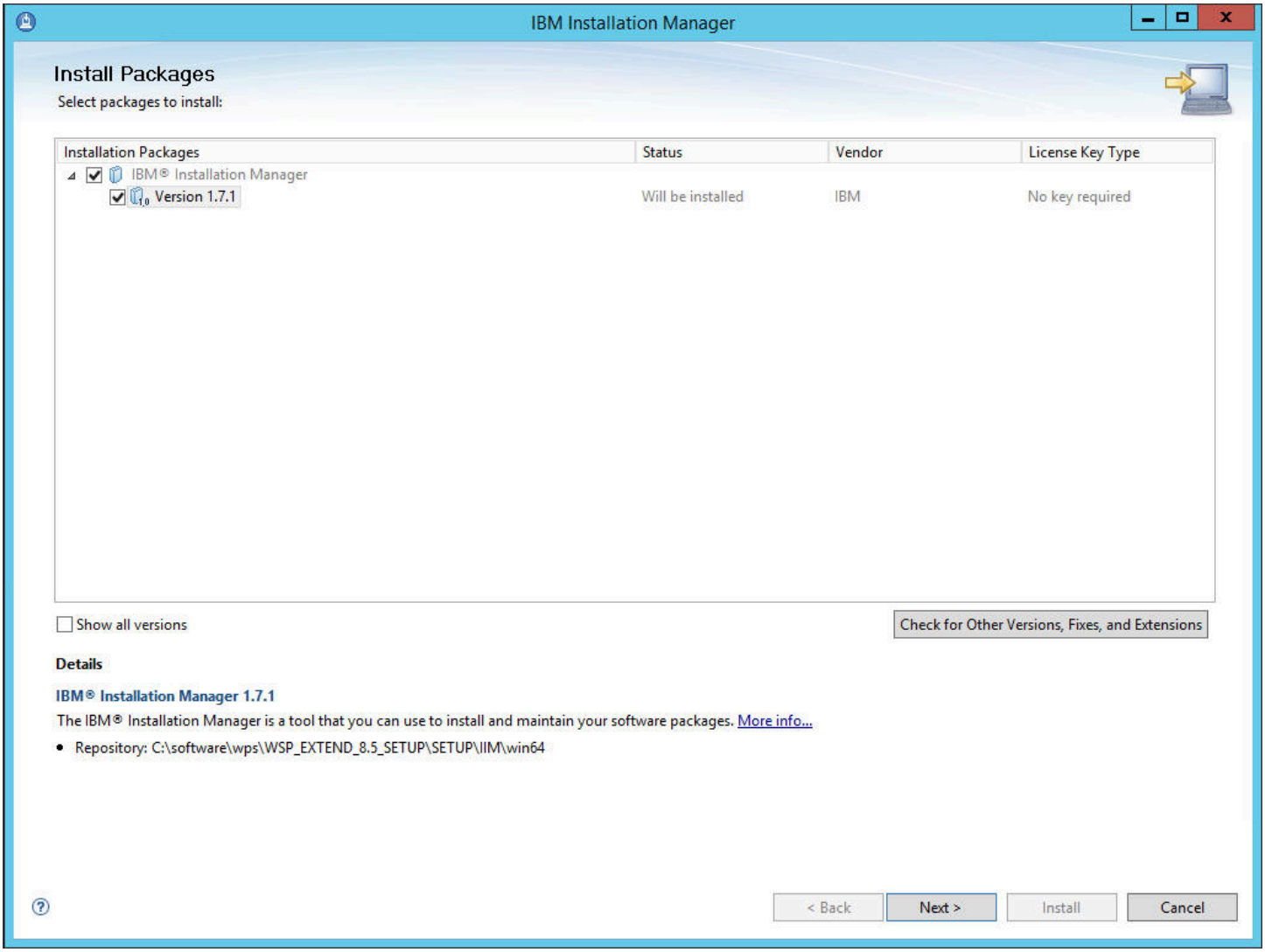
For example:

```
install -W was.undetectedWas="\my\WAS\location"
```

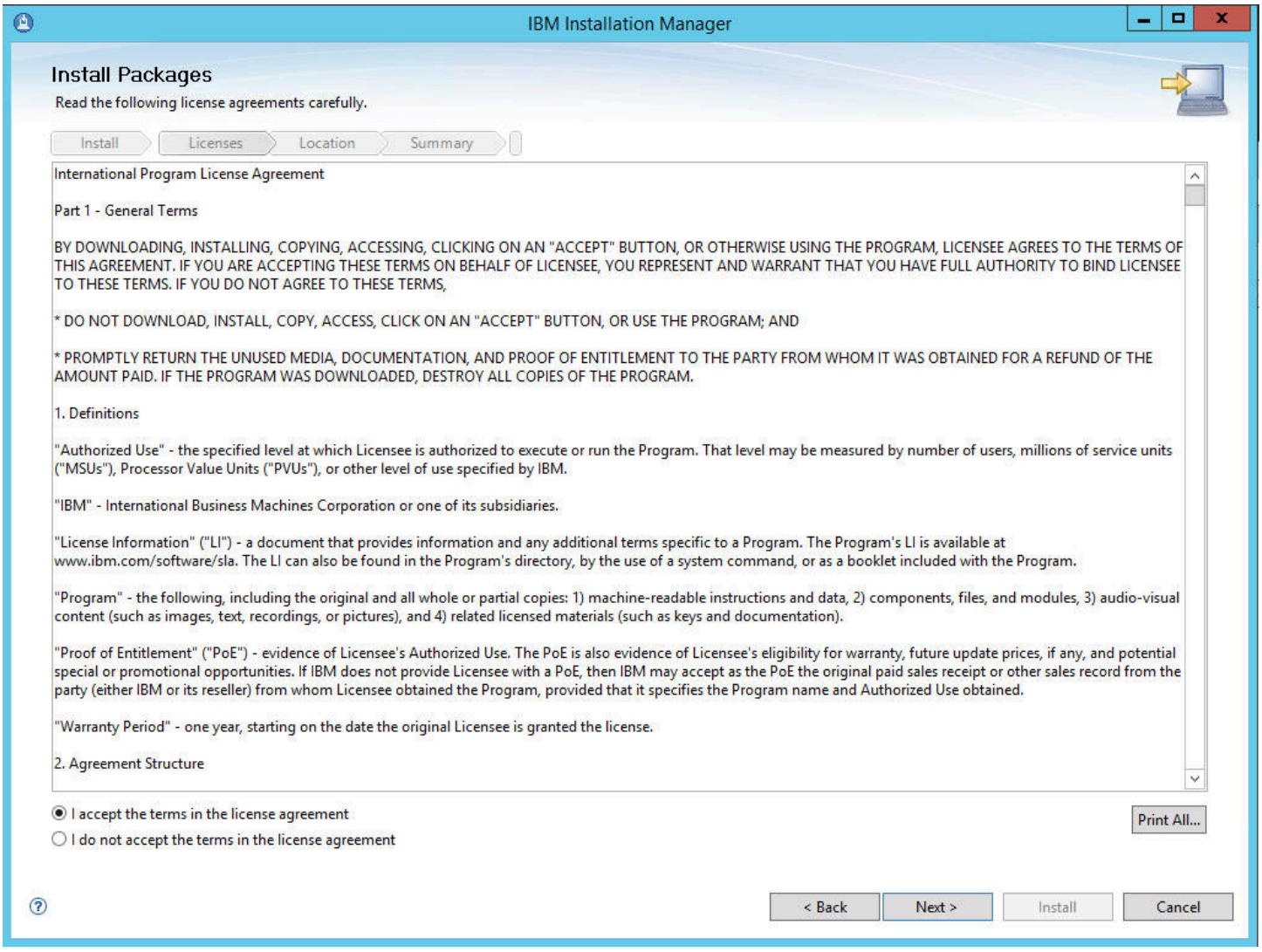
Upon execution, by default the installer creates a separate profile called wp_profile. This profile is used to host the Portal contents. Therefore, you should not install Portal into an existing profile with other applications installed.



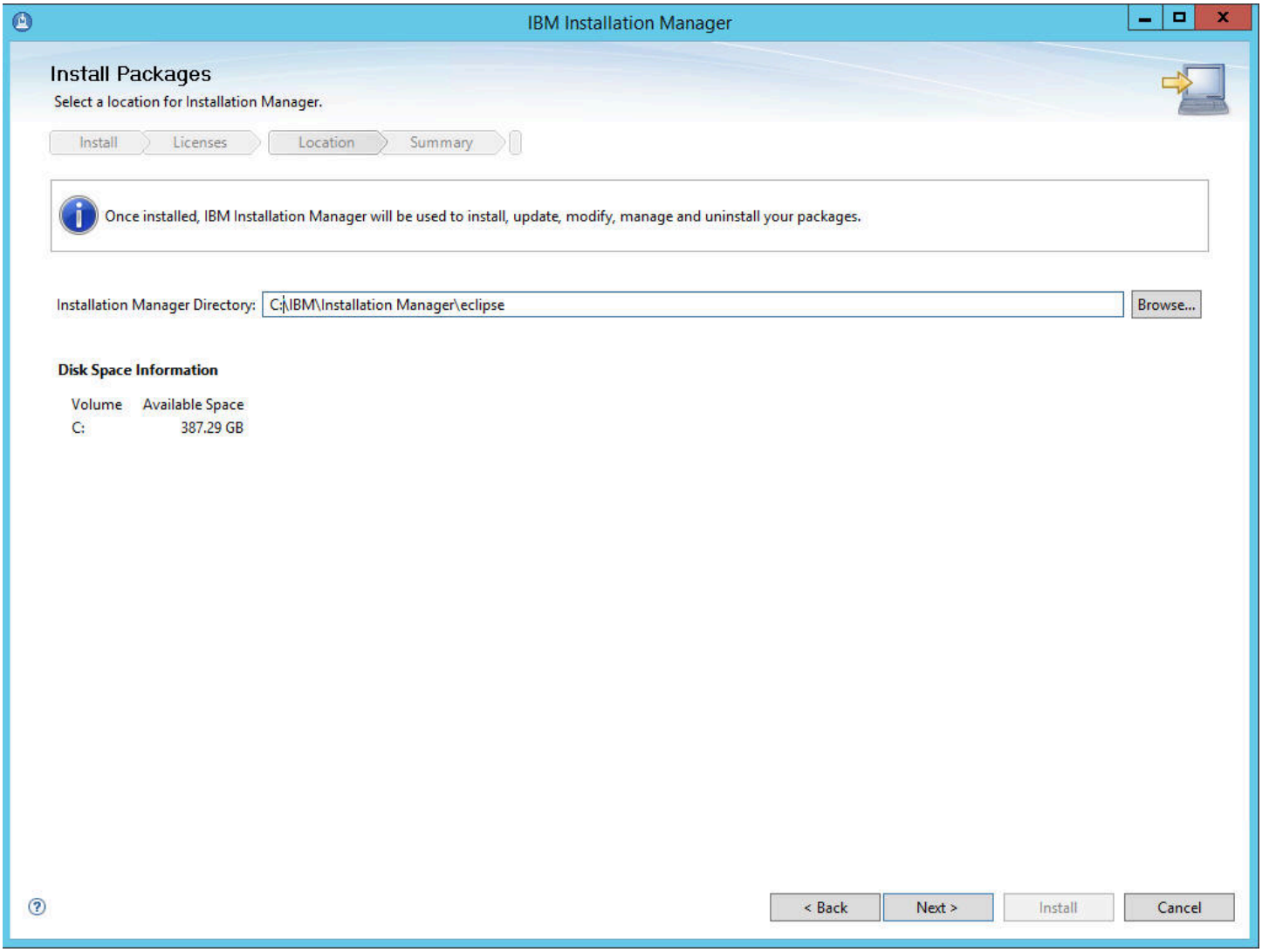
3. After launching the IBM WebSphere Portal wizard, select Install Portal in the left window pane, and then click on the hyperlink for Install IBM Installation Manager only.


IBM Installation Manager
Install Packages
Select packages to install:
Installation Packages
Status
Vendor
License Key Type
IBM® Installation Manager
Version 1.7.1
Will be installed
IBM
No key required
Show all versions
Check for Other Versions, Fixes, and Extensions
Details
IBM® Installation Manager 1.7.1
The IBM® Installation Manager is a tool that you can use to install and maintain your software packages. More info...
Repository: C:\software\wps\WSP_EXTEND_8.5_SETUP\SETUP\IIM\win64
< Back
Next >
Install
Cancel

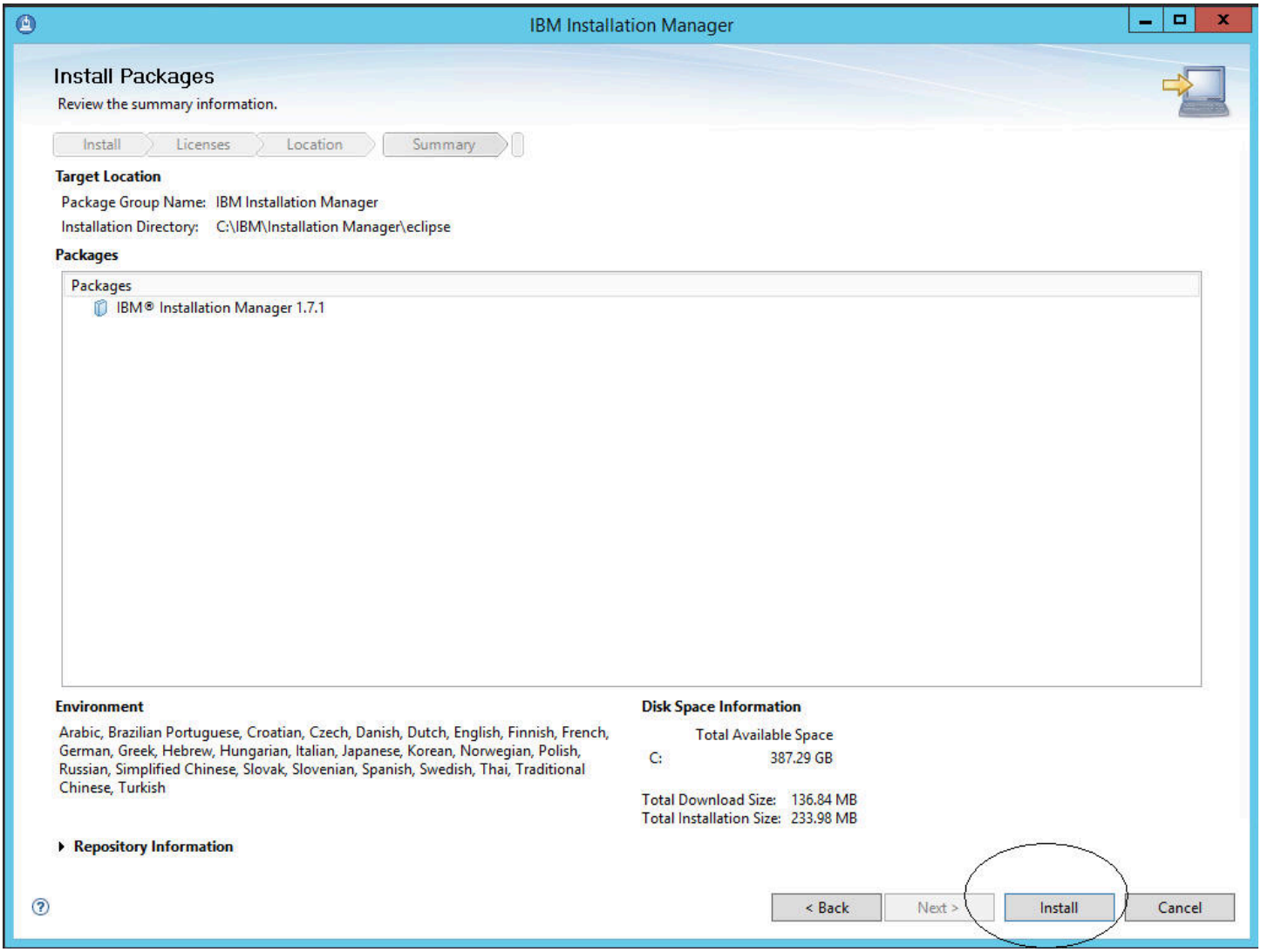
4. On the Install Packages window, make sure that the IBM Installation Manager and the version have been selected. Click the Next button.



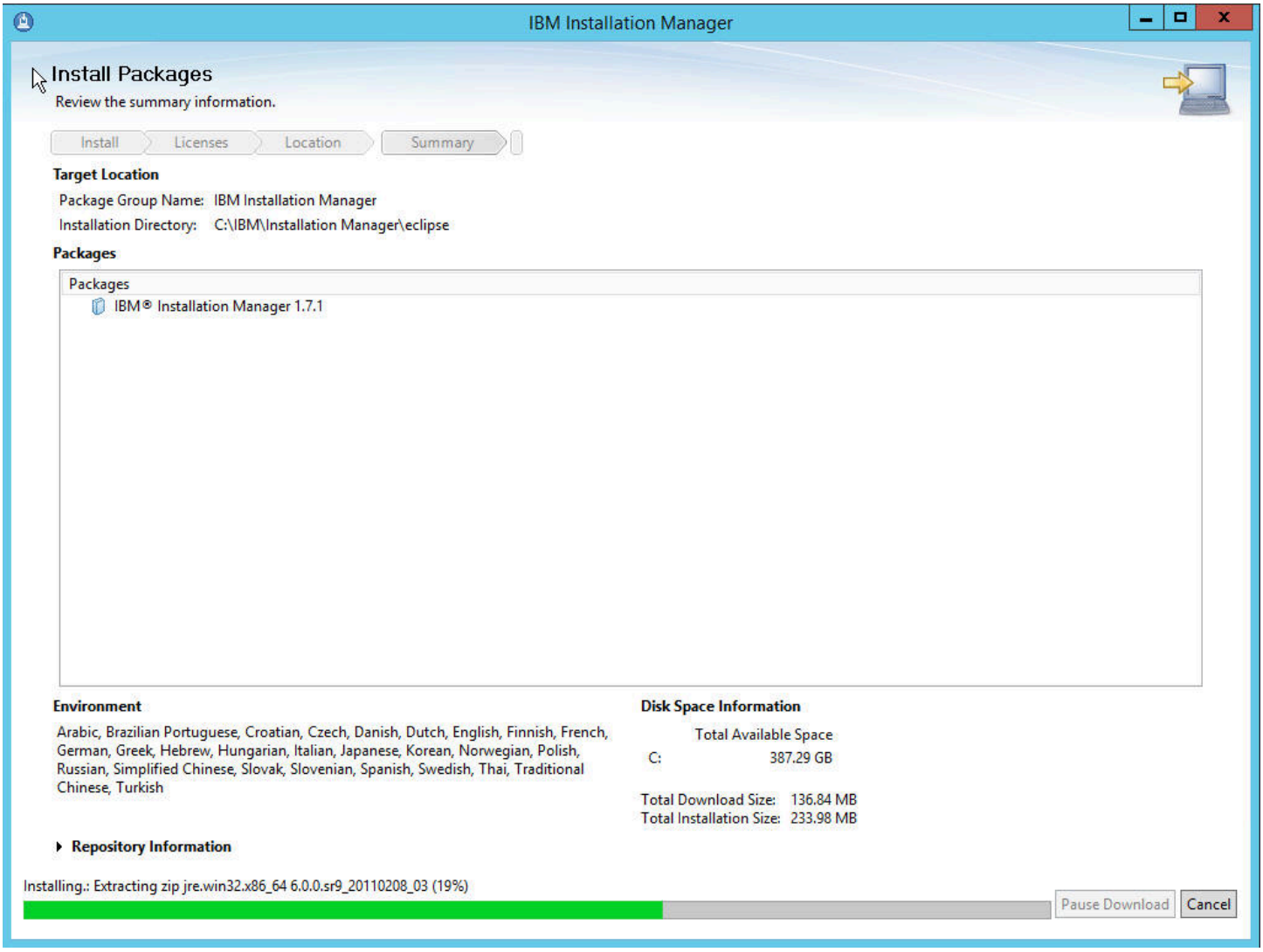
5. Accept the license agreement terms and click the Next button.



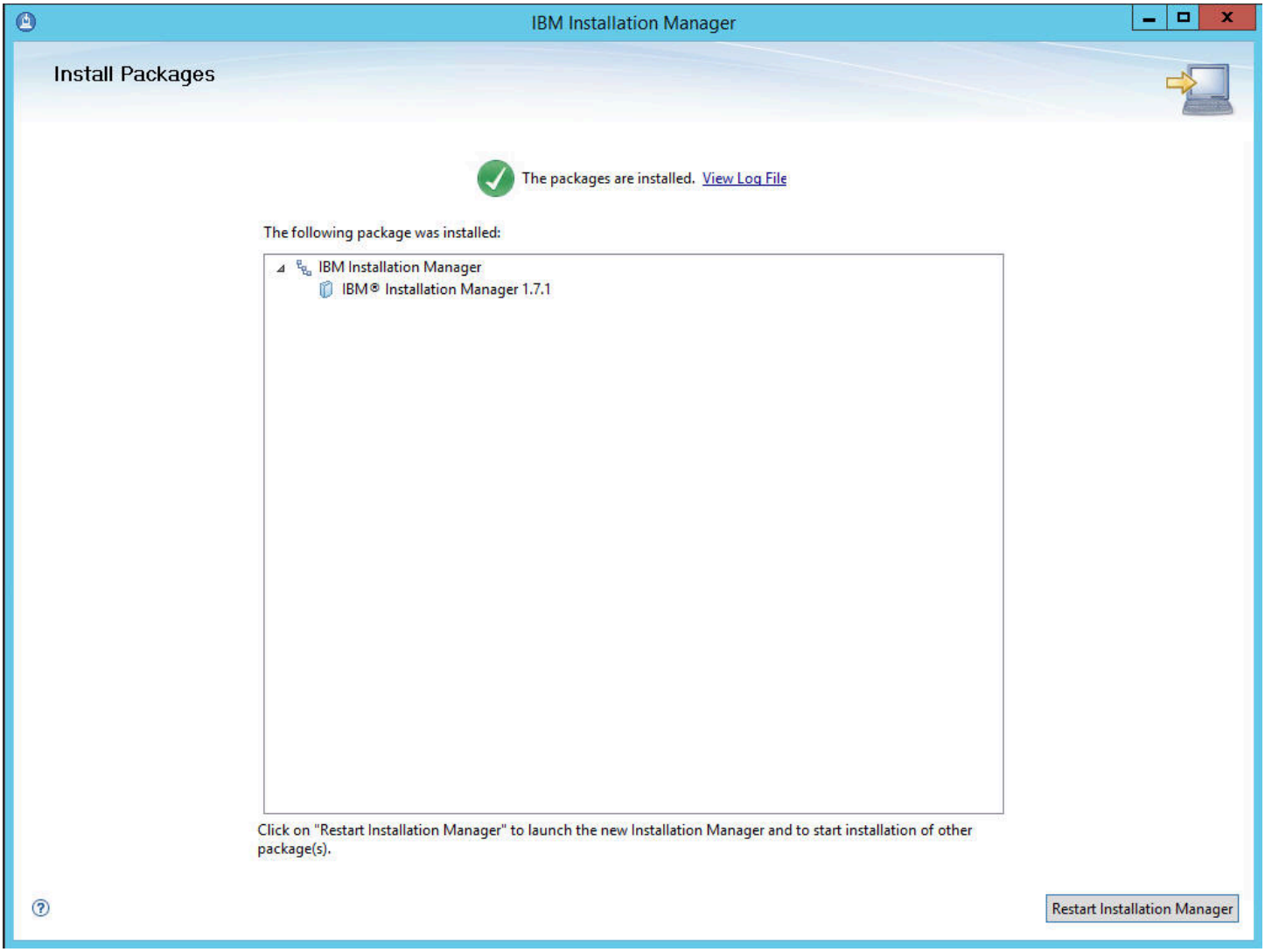
6. Select a location for Installation manager and click Next.



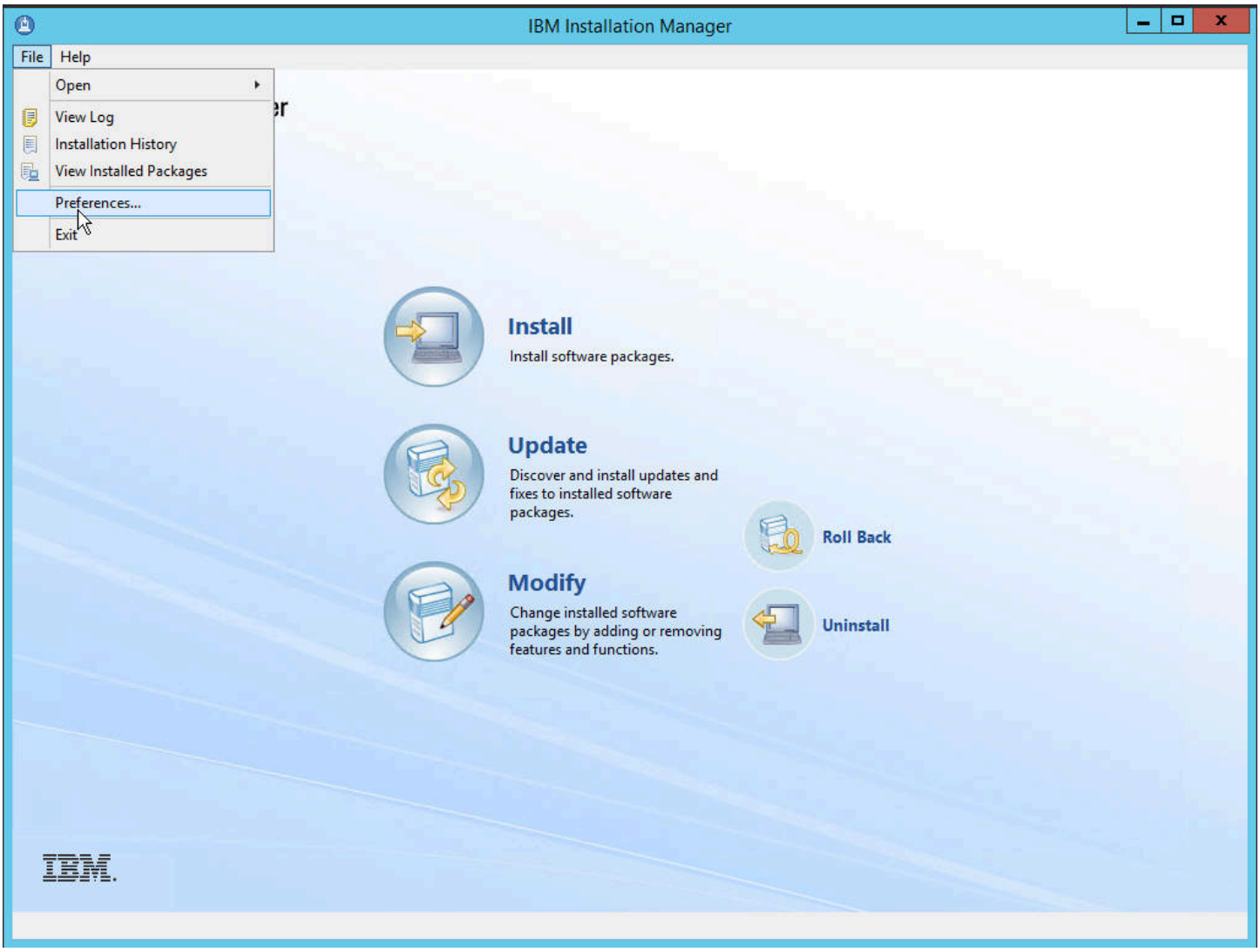
7. Review the summary information and click Install.



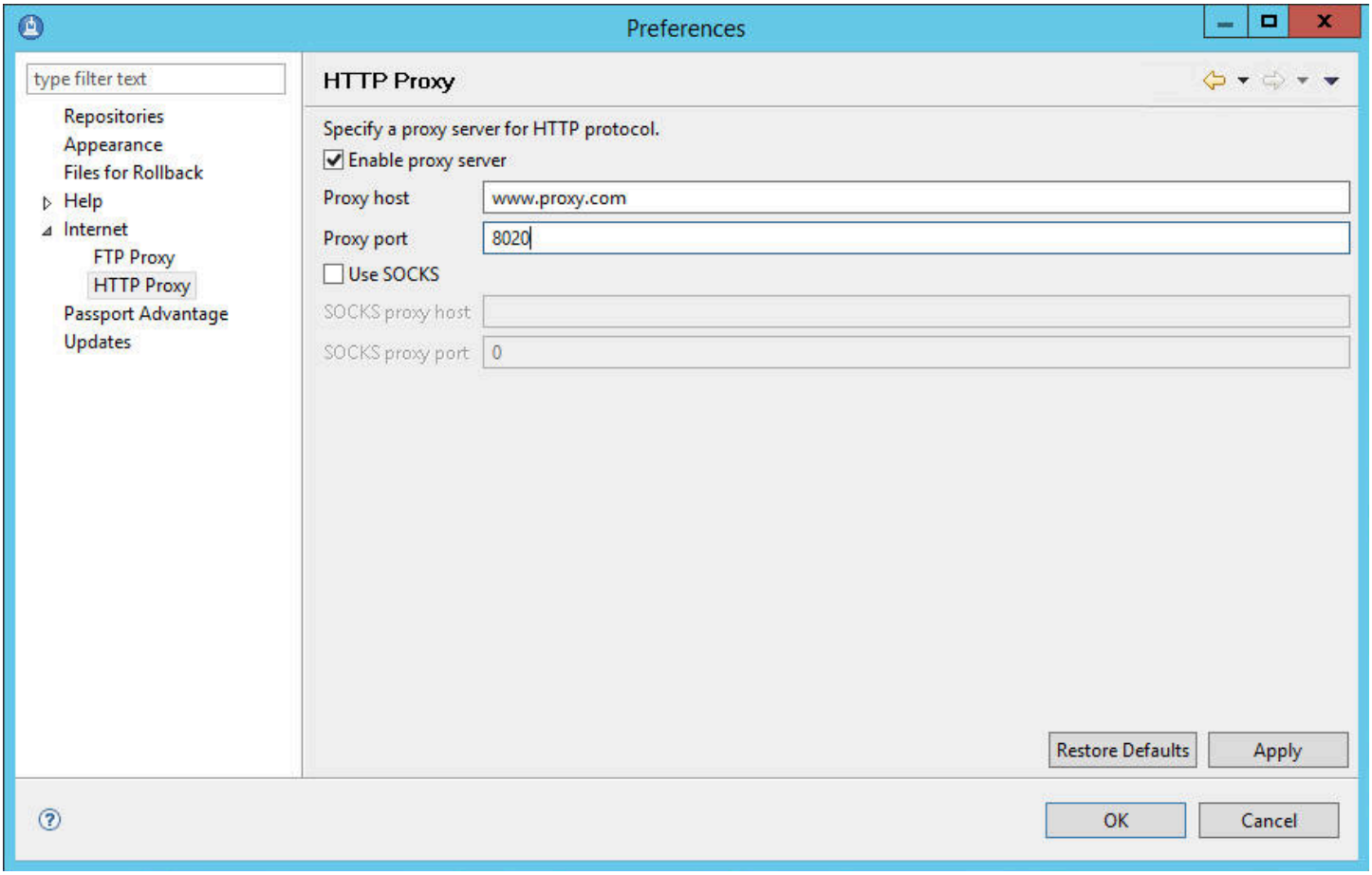
8. The progress of the install will be displayed in the bar along the bottom of the screen.



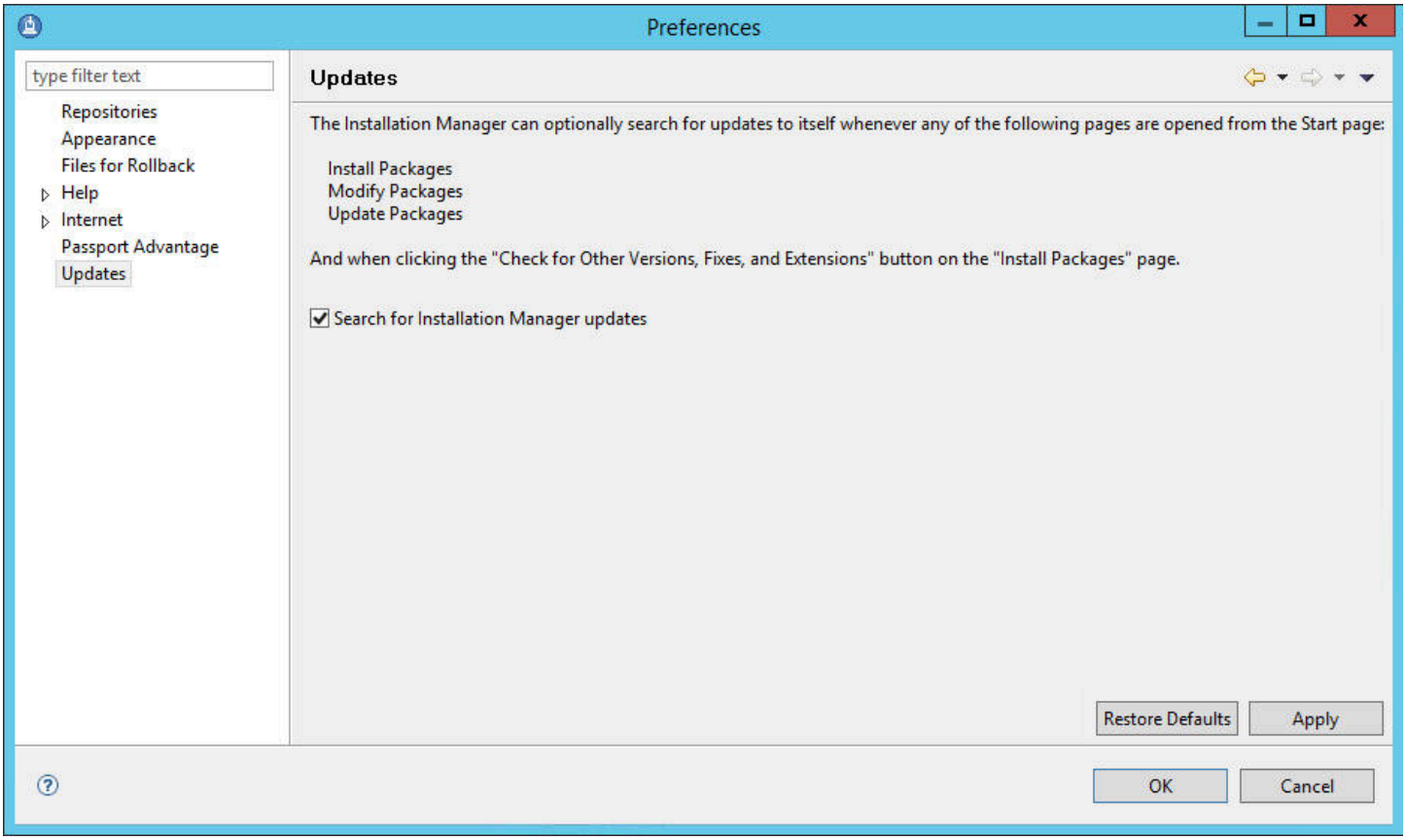
9. When the install of Installation Manager completes successfully, this screen will appear. Click on Restart Installation Manager to launch the new Installation Manager and to start installation of other packages.



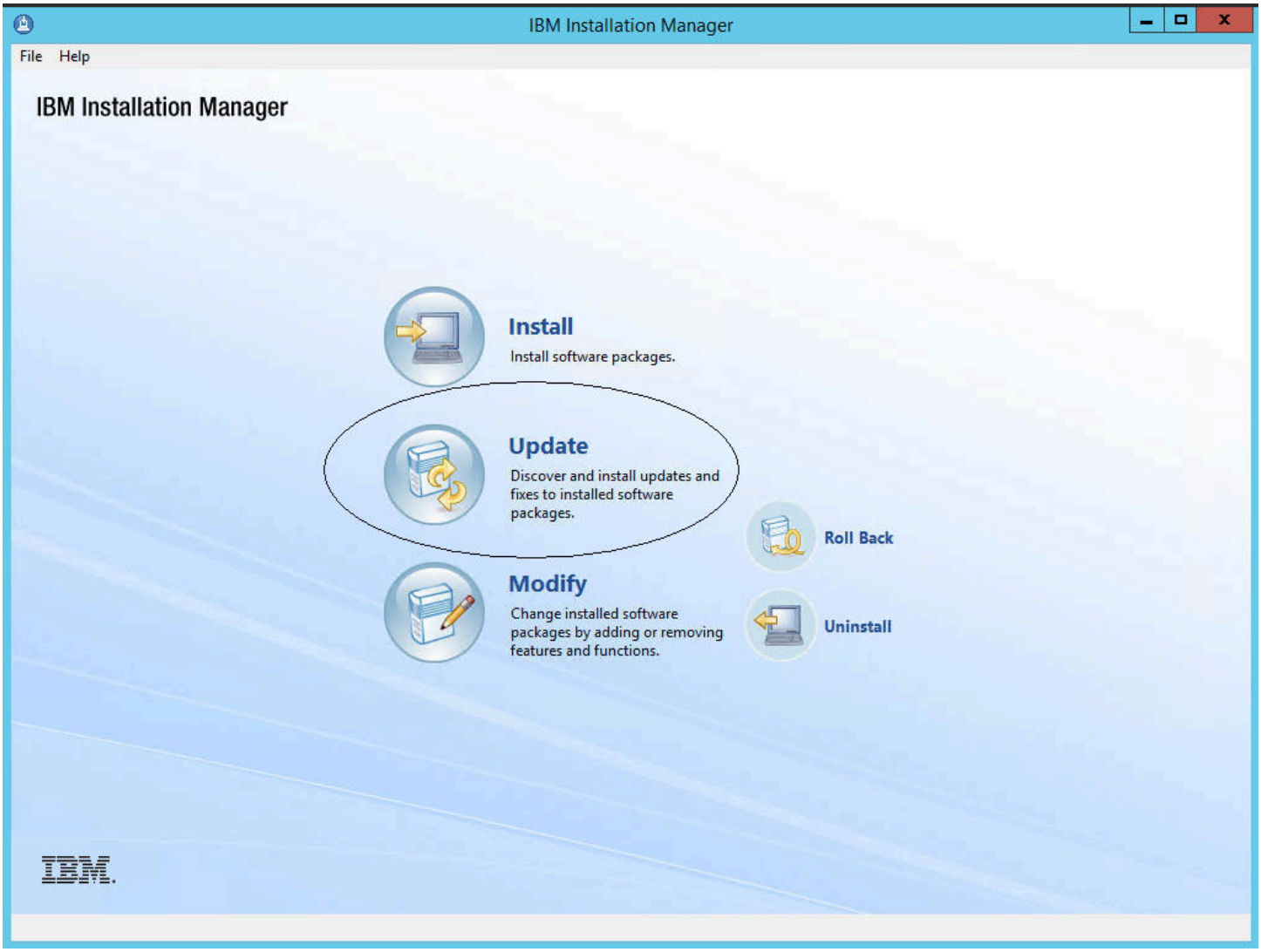
10. After Installation Manager is launched, select File|Preferences.



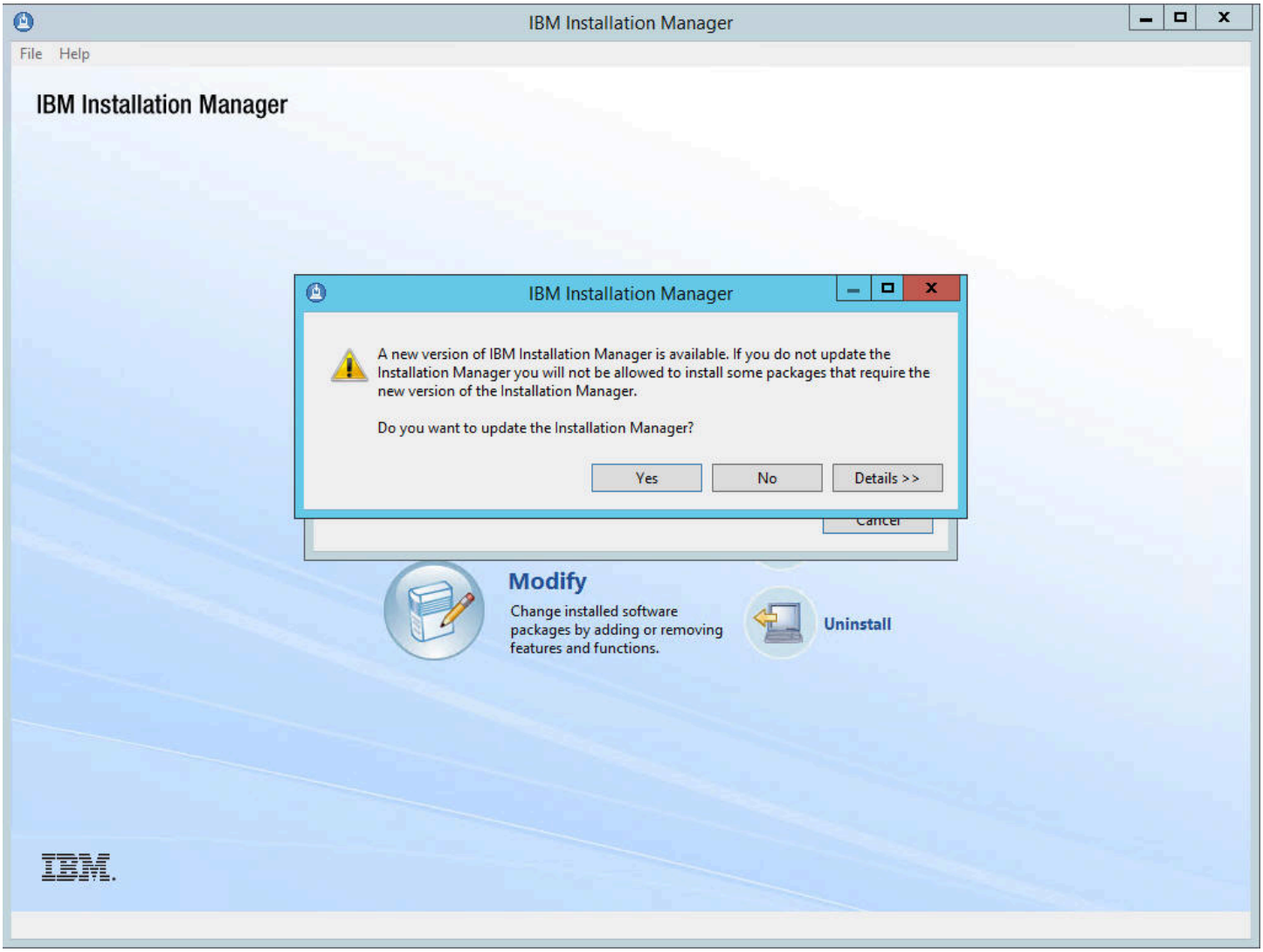
11. Make sure that the correct information is provided for the Proxy host and Proxy port. Click OK.



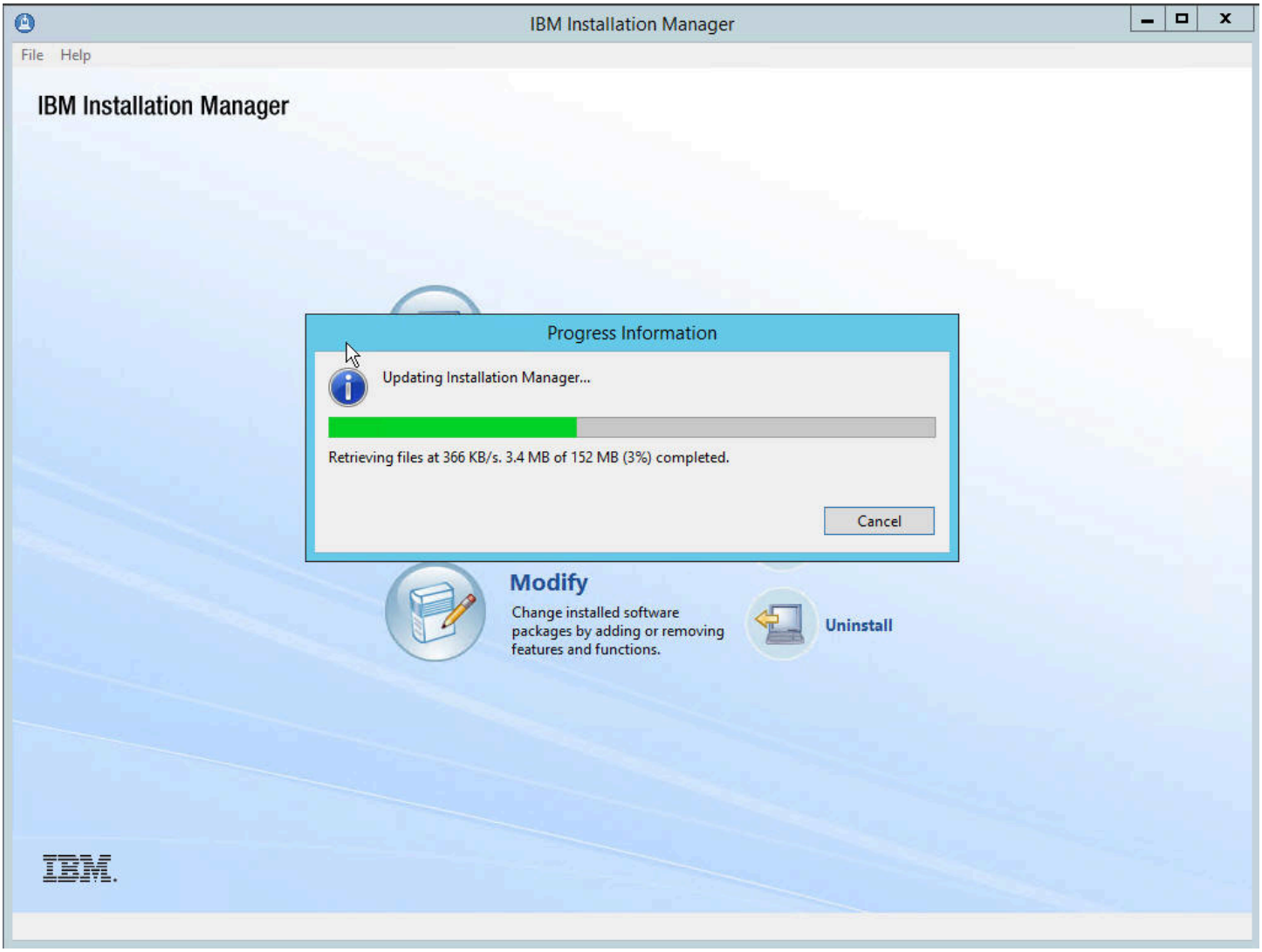
12. If you want to search for Installation Manager updates, then select the checkbox. Click OK.



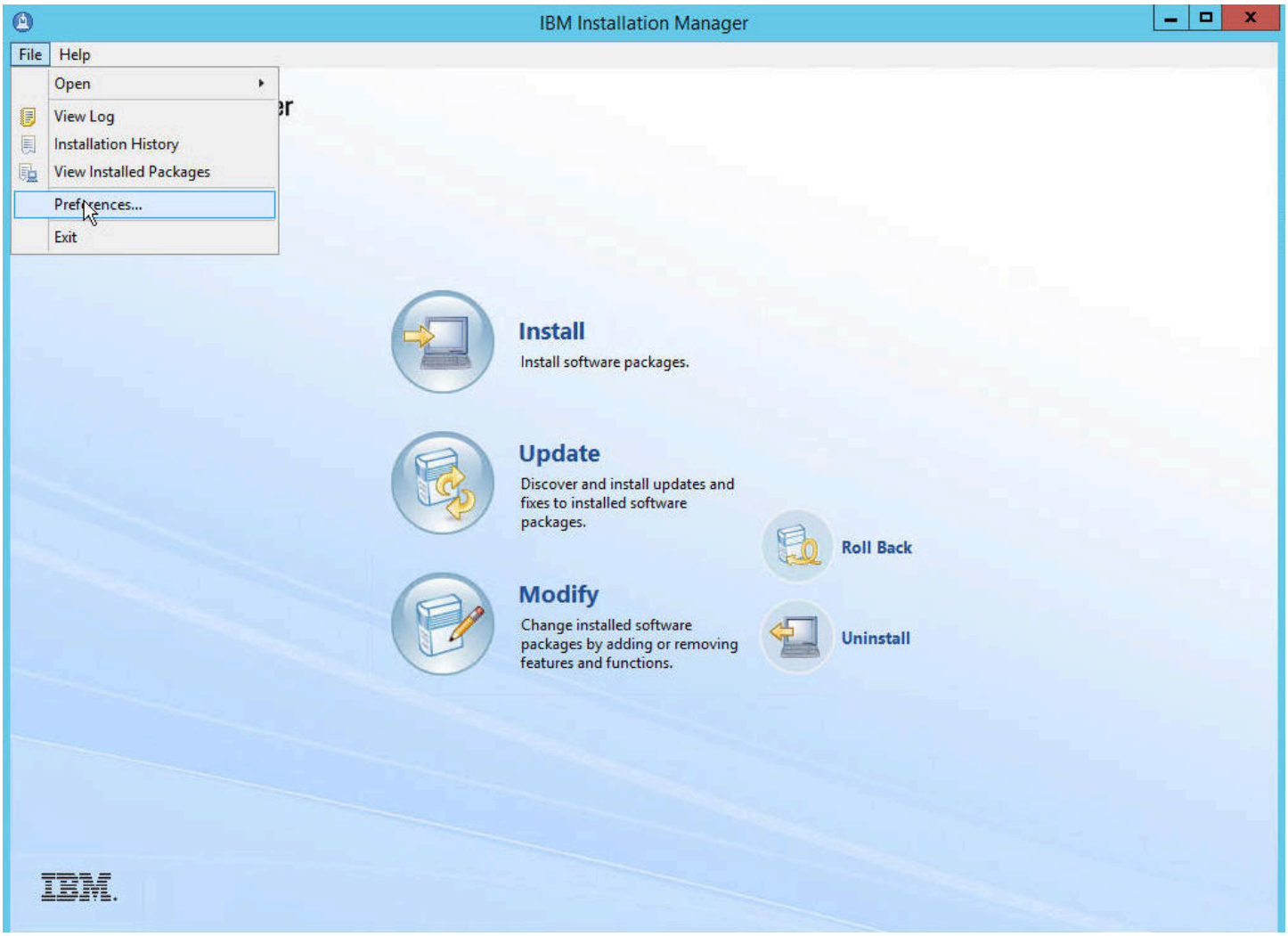
13. To discover and install updates and fixes to installed software packages, click Update.



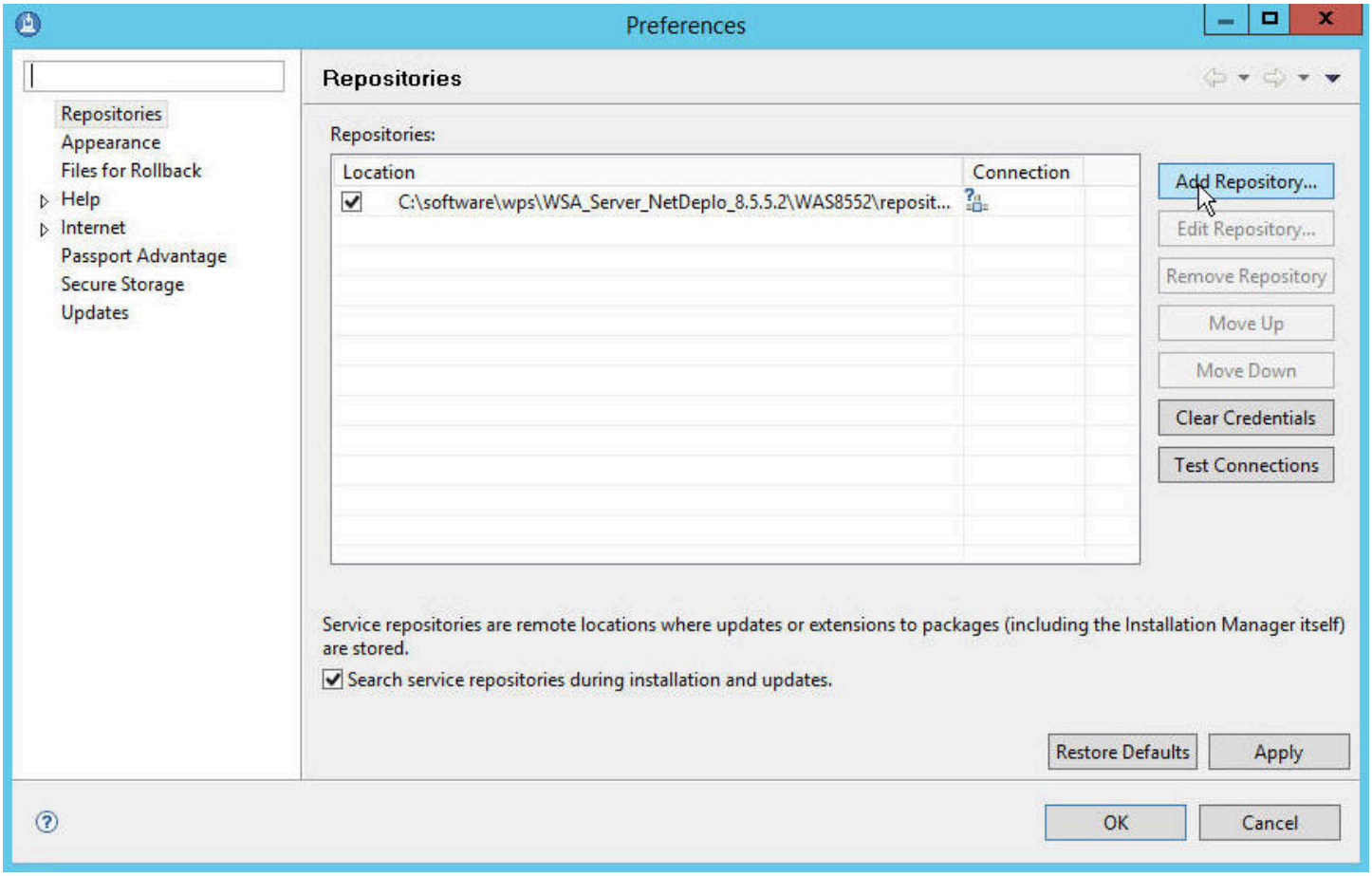
14. A popup window will notify you if there are updates available.



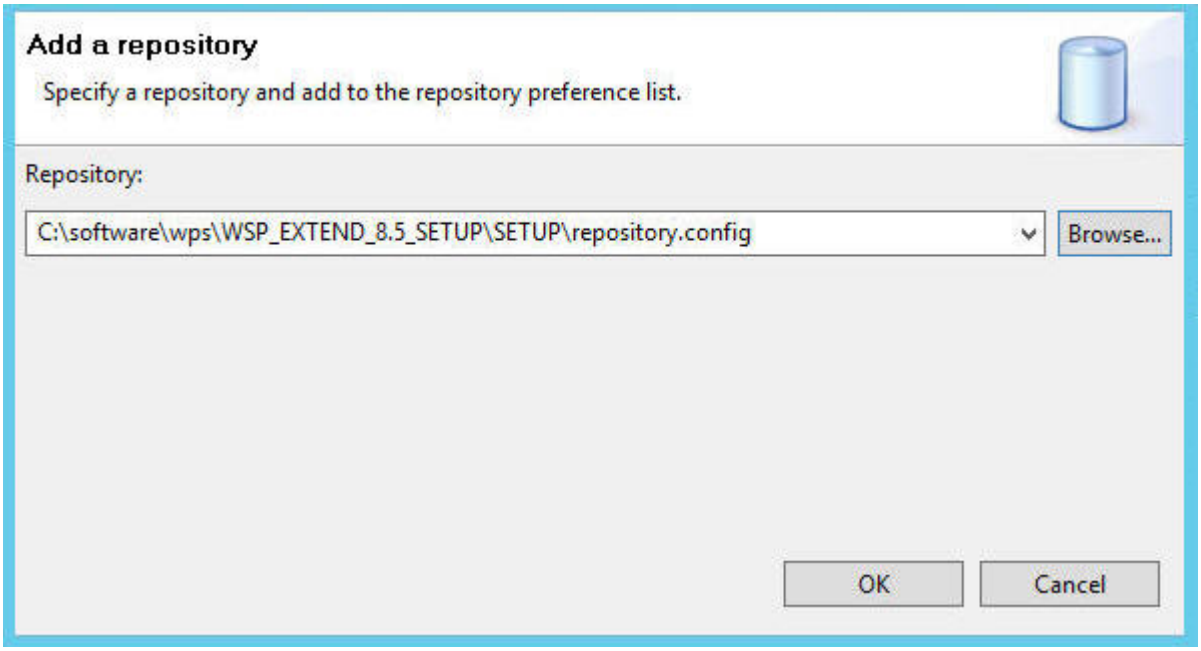
15. If Yes has been selected, a Progress Information popup window will appear displaying the progress of the update being installed.



16. Once the update is installed, the IBM Installation Manager home screen will appear. Select File|Preferences.

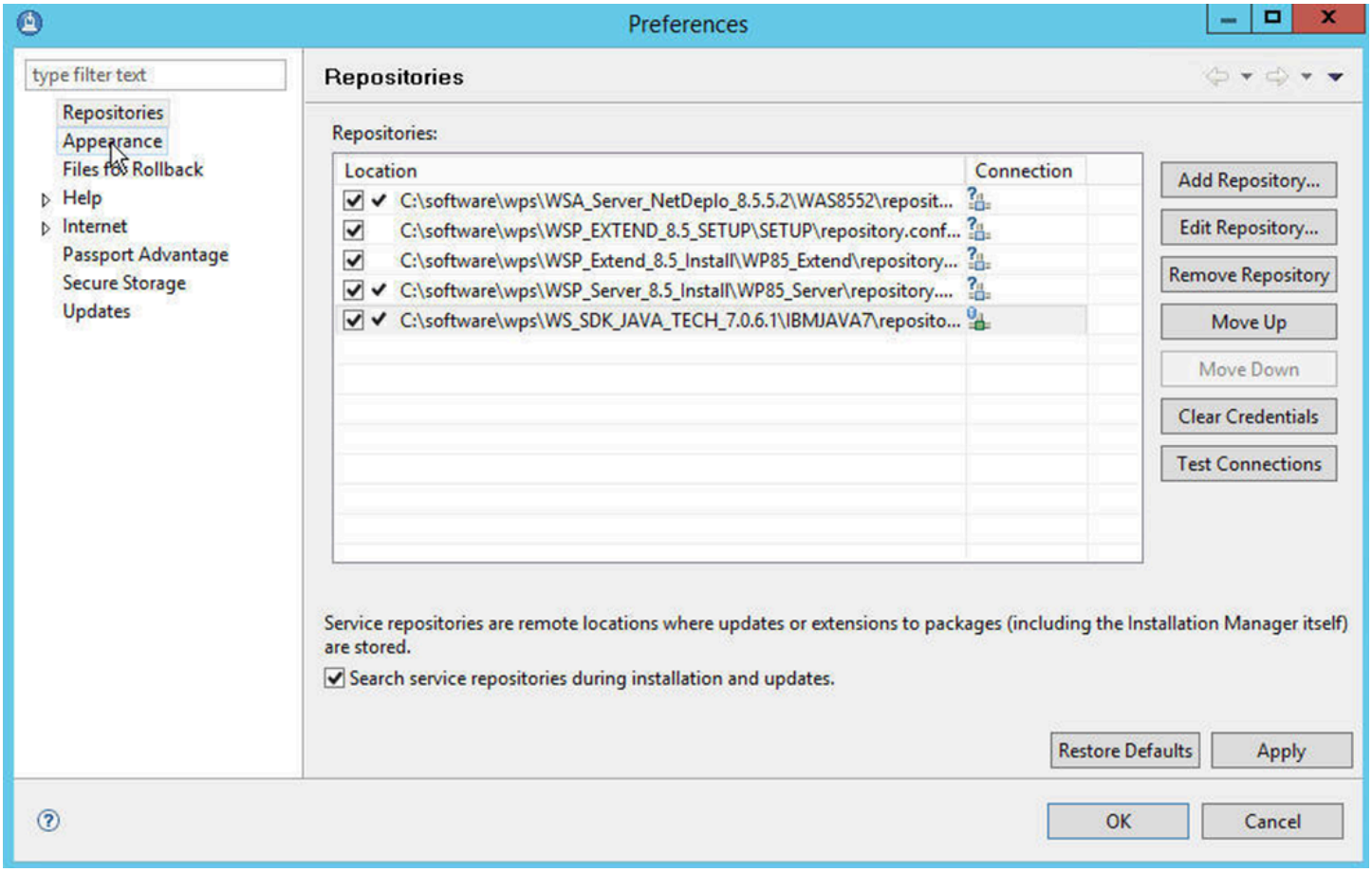


17. Within Preferences, select Repositories in the left window pane. Click on the Add Repository button.



18. In the Add a repository popup window, add WSA_Server_NetDeplo_8.5.5.2 and then click OK.

    Not all users may use WSP Extend but WSA_Server_NetDeploy, WSA Srvr 8.5.

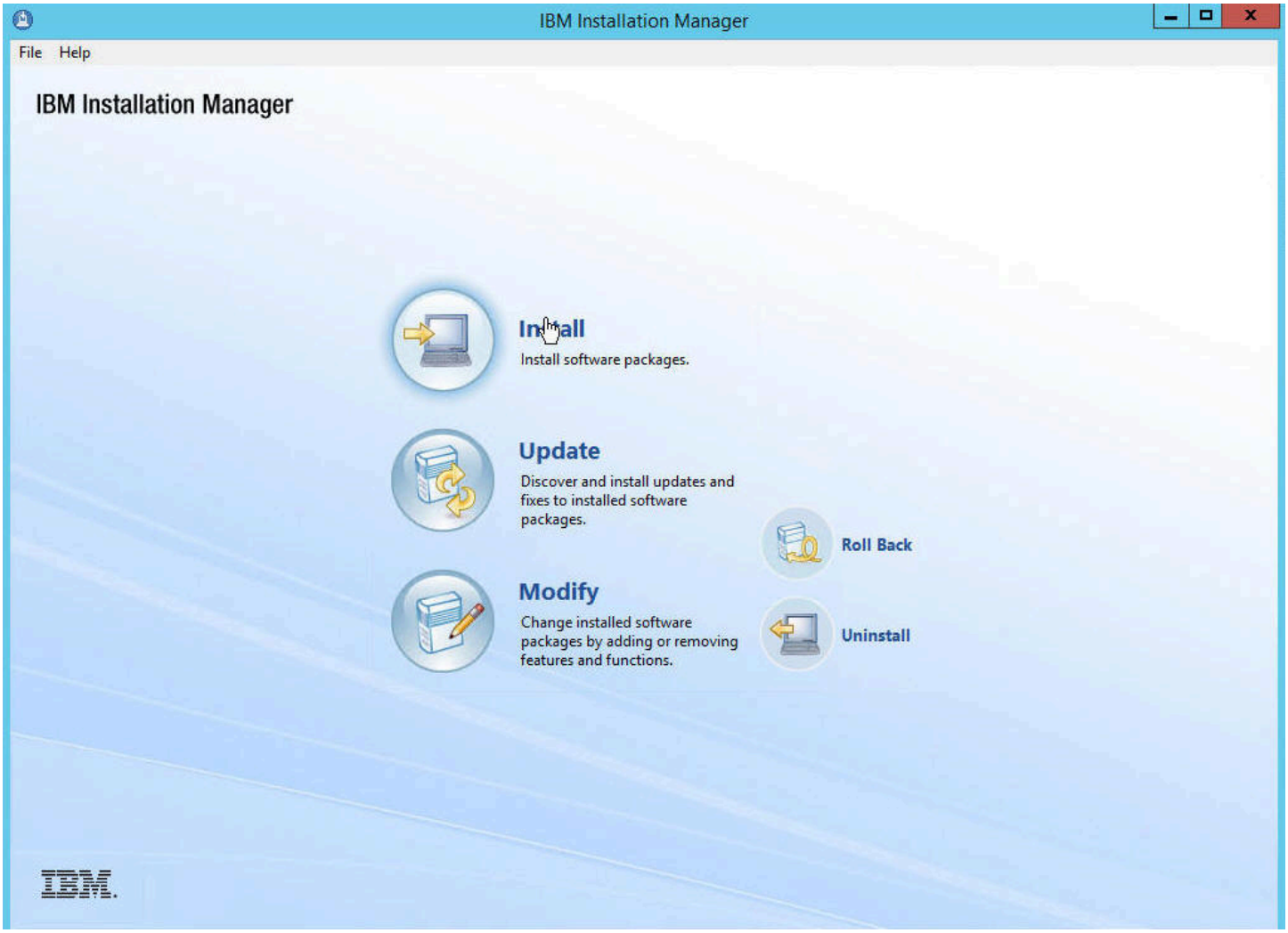

Preferences
type filter text
Repositories
Appearance
Files for Rollback
Help
Internet
Passport Advantage
Secure Storage
Updates
Repositories
Repositories:
Location
Connection
C:\software\wps\WSA_Server_NetDeplo_8.5.5.2\WAS8552\reposit...
C:\software\wps\WSP_EXTEND_8.5_SETUP\SETUP\repository.conf...
C:\software\wps\WSP_Extend_8.5_Install\WP85_Extend\repository...
C:\software\wps\WSP_Server_8.5_Install\WP85_Server\repository....
C:\software\wps\WS_SDK_JAVA_TECH_7.0.6.1\IBMJAVA7\reposito...
Add Repository...
Edit Repository...
Remove Repository
Move Up
Move Down
Clear Credentials
Test Connections
Service repositories are remote locations where updates or extensions to packages (including the Installation Manager itself) are stored.
Search service repositories during installation and updates.
Restore Defaults
Apply
OK
Cancel

19. Add these repositories, and then click OK:

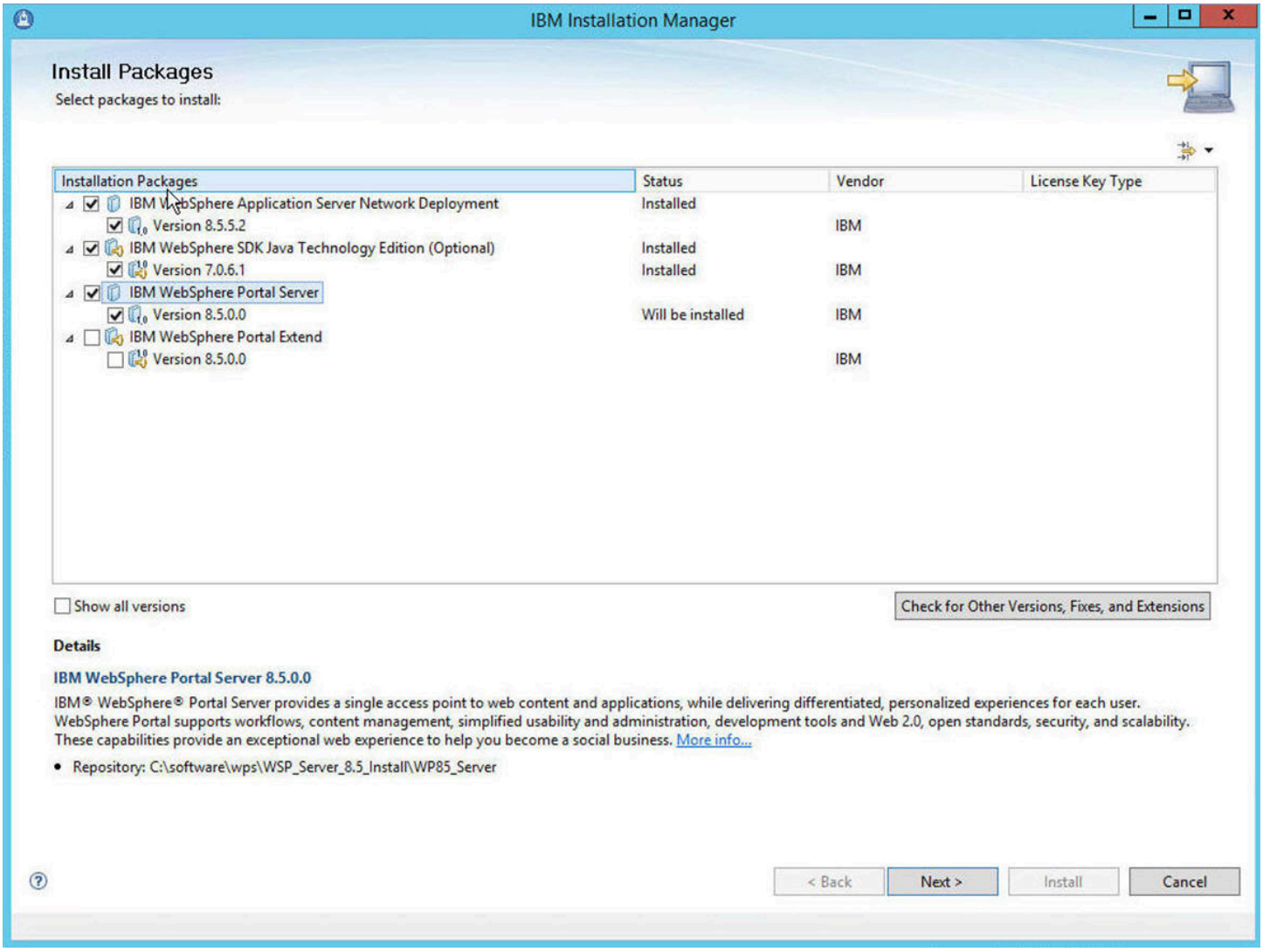
    WSA_Server_NetDeplo_8.5.5.2

    WSP_Server_8.5_Install

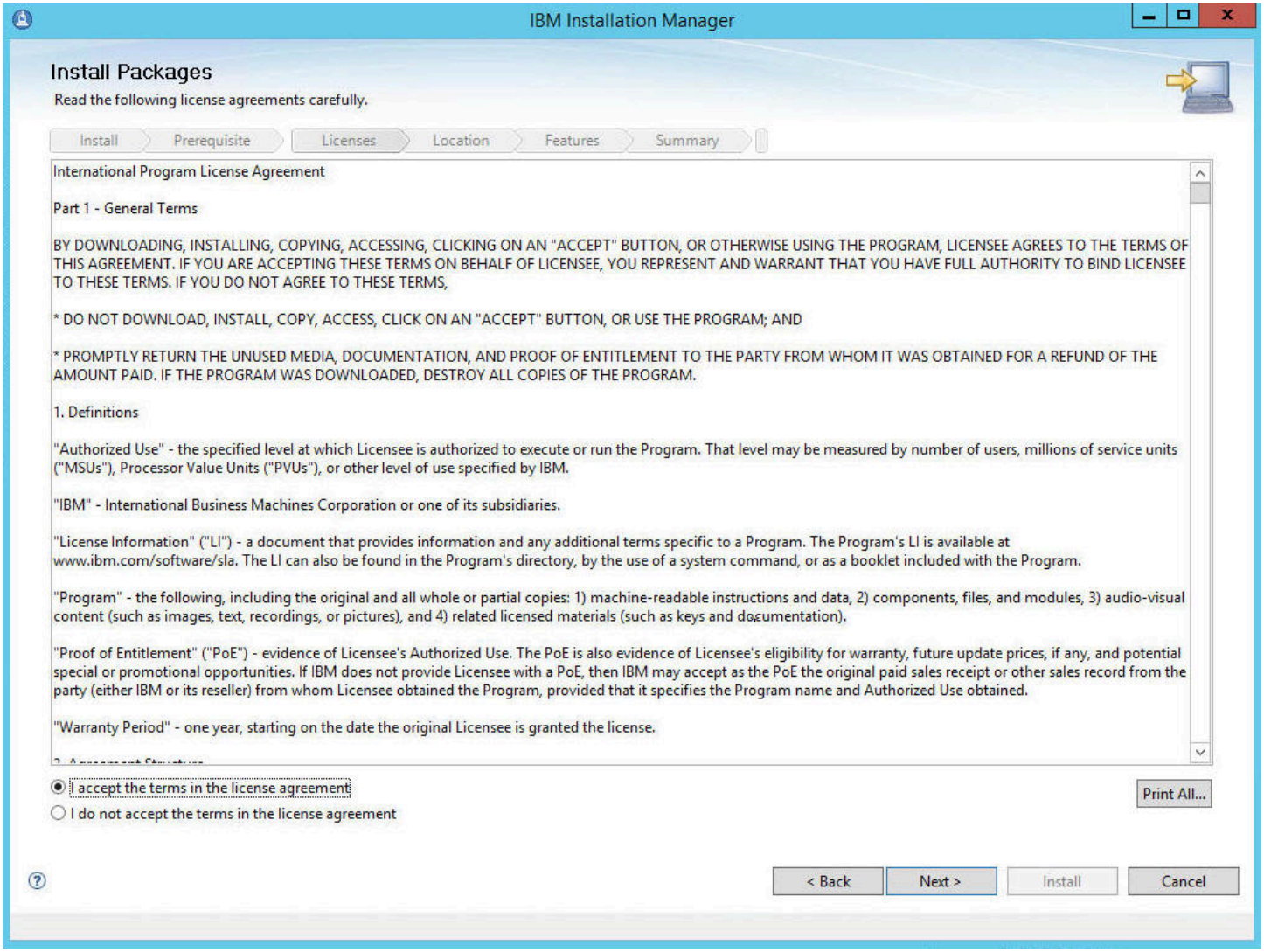
    WS_SDK_JAVA_TECH_7.0.6.1


IBM Installation Manager
File Help
IBM Installation Manager
Install
Install software packages.
Update
Discover and install updates and fixes to installed software packages.
Roll Back
Modify
Change installed software packages by adding or removing features and functions.
Uninstall
IBM.

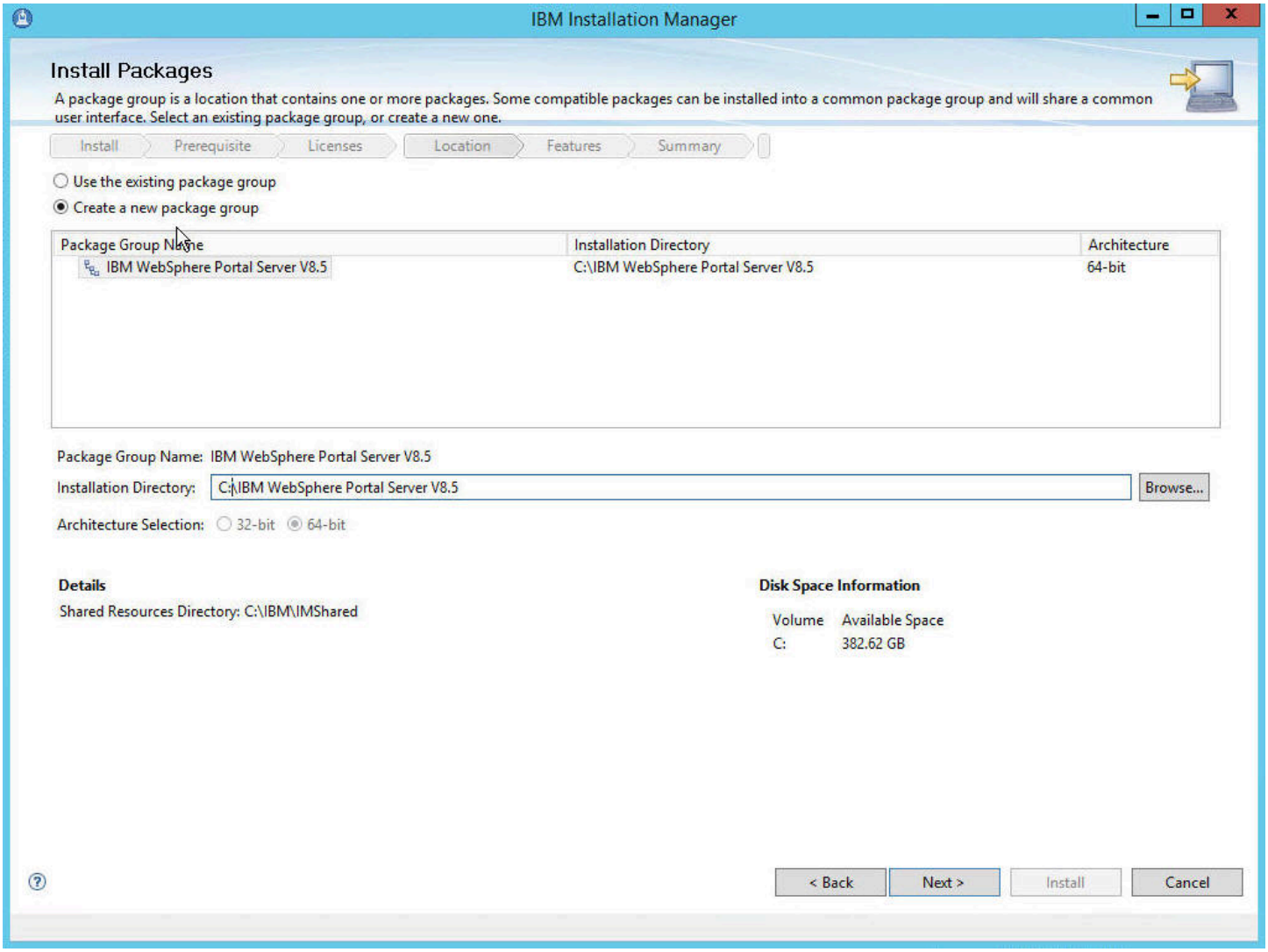
20. Click Install.


IBM Installation Manager
Install Packages
Select packages to install:
Installation Packages
Status
Vendor
License Key Type
IBM WebSphere Application Server Network Deployment
Installed
Version 8.5.5.2
IBM
IBM WebSphere SDK Java Technology Edition (Optional)
Installed
Version 7.0.6.1
Installed
IBM
IBM WebSphere Portal Server
Version 8.5.0.0
Will be installed
IBM
IBM WebSphere Portal Extend
Version 8.5.0.0
IBM
Show all versions
Check for Other Versions, Fixes, and Extensions
Details
IBM WebSphere Portal Server 8.5.0.0
IBM® WebSphere® Portal Server provides a single access point to web content and applications, while delivering differentiated, personalized experiences for each user. WebSphere Portal supports workflows, content management, simplified usability and administration, development tools and Web 2.0, open standards, security, and scalability. These capabilities provide an exceptional web experience to help you become a social business. More info...
Repository: C:\software\wps\WSP_Server_8.5_Install\WP85_Server
< Back
Next >
Install
Cancel

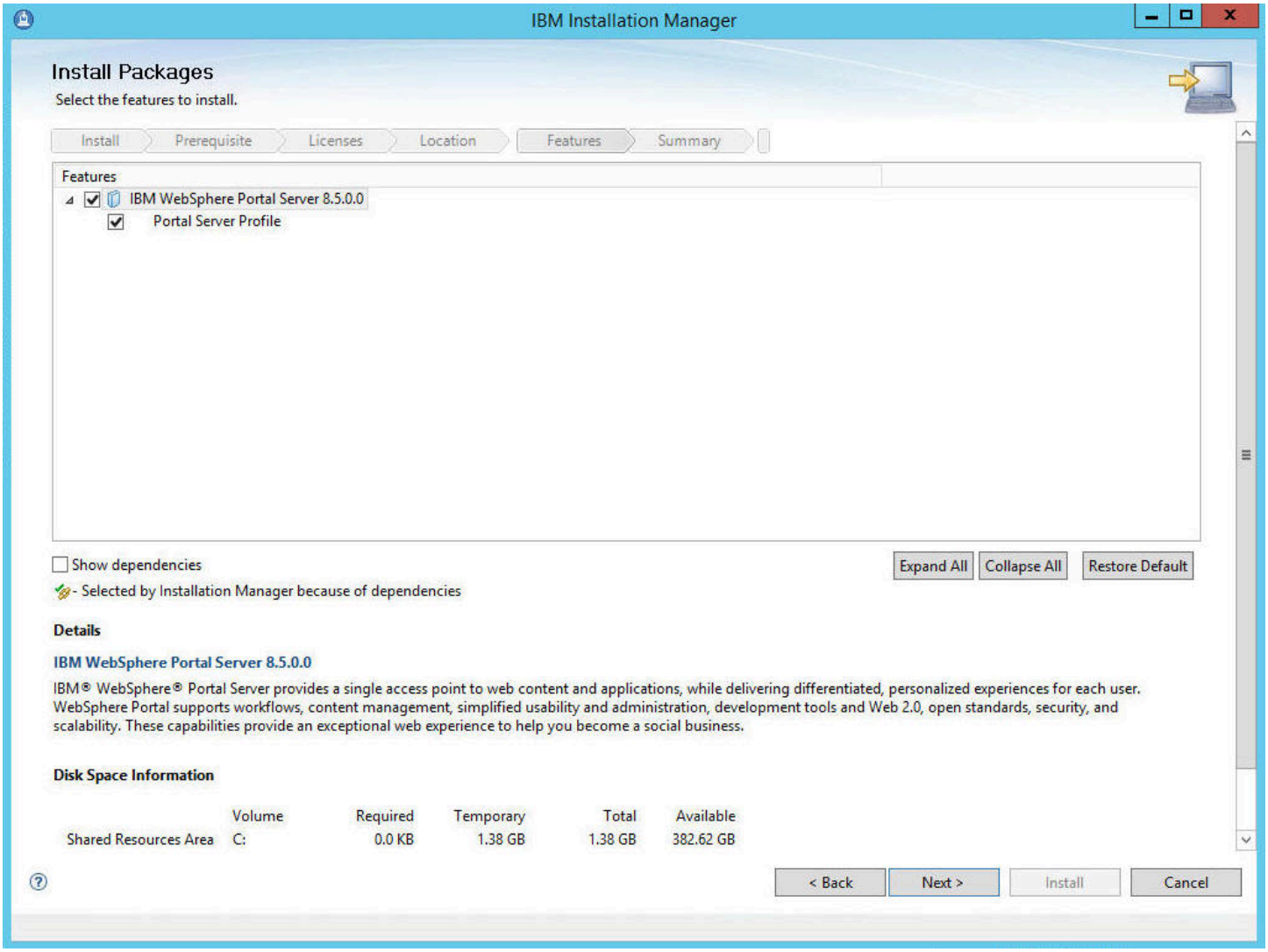
21. Select IBM WebSphere Portal Server and click Next.



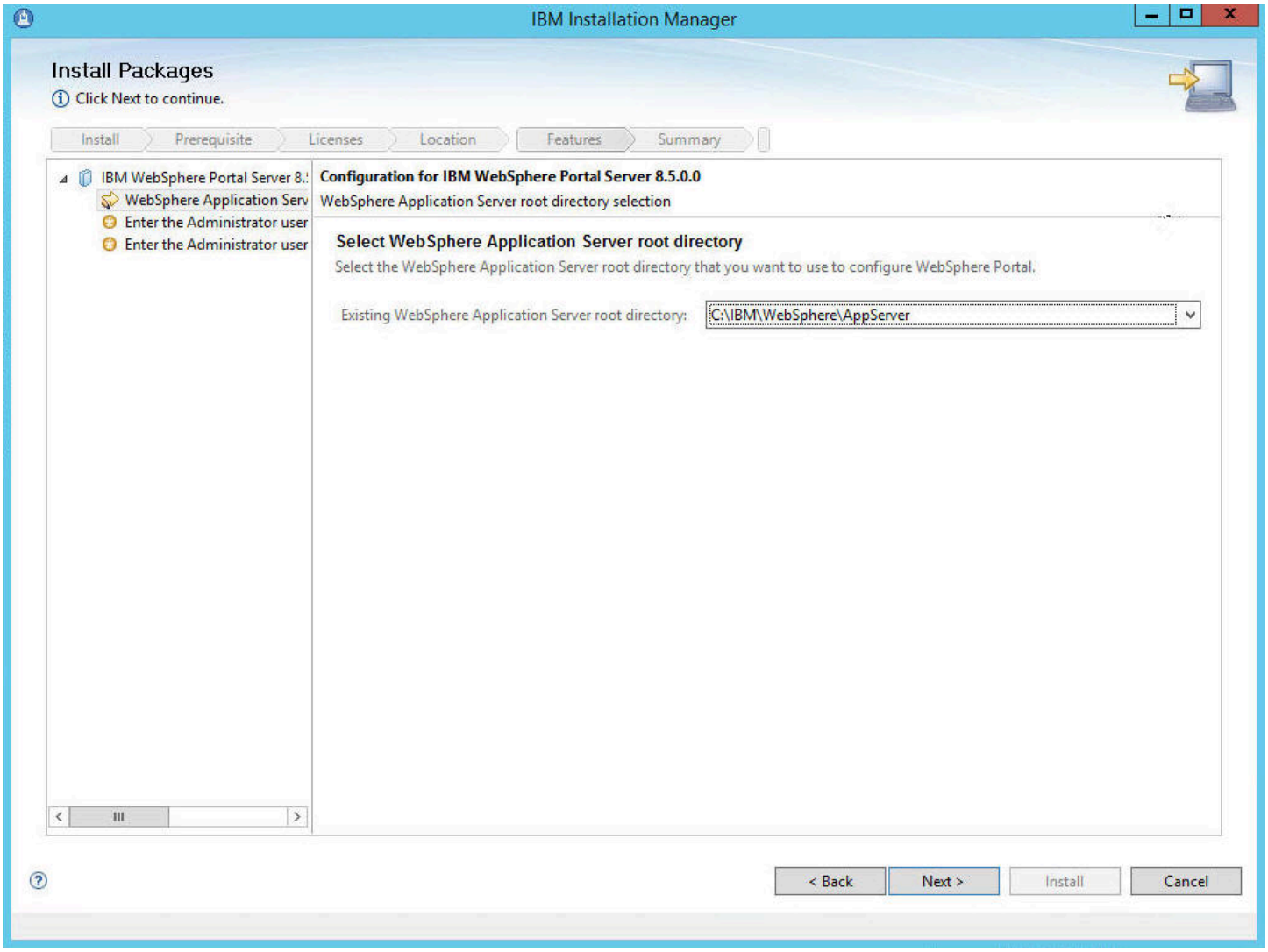
22. Accept the license agreement terms and click Next.



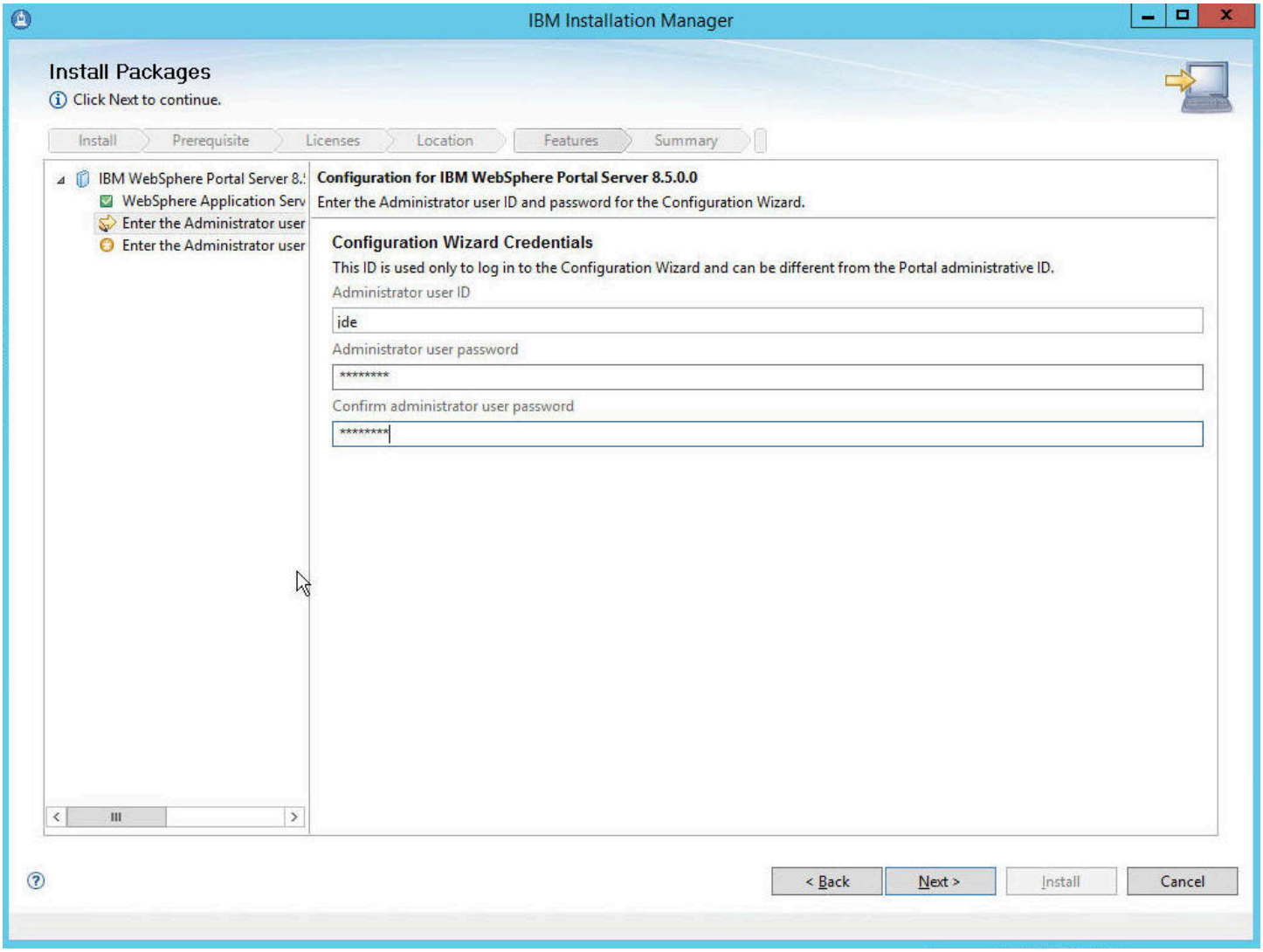
23. Select Create a new package group and click Next.



24. Select the features to install and click Next.



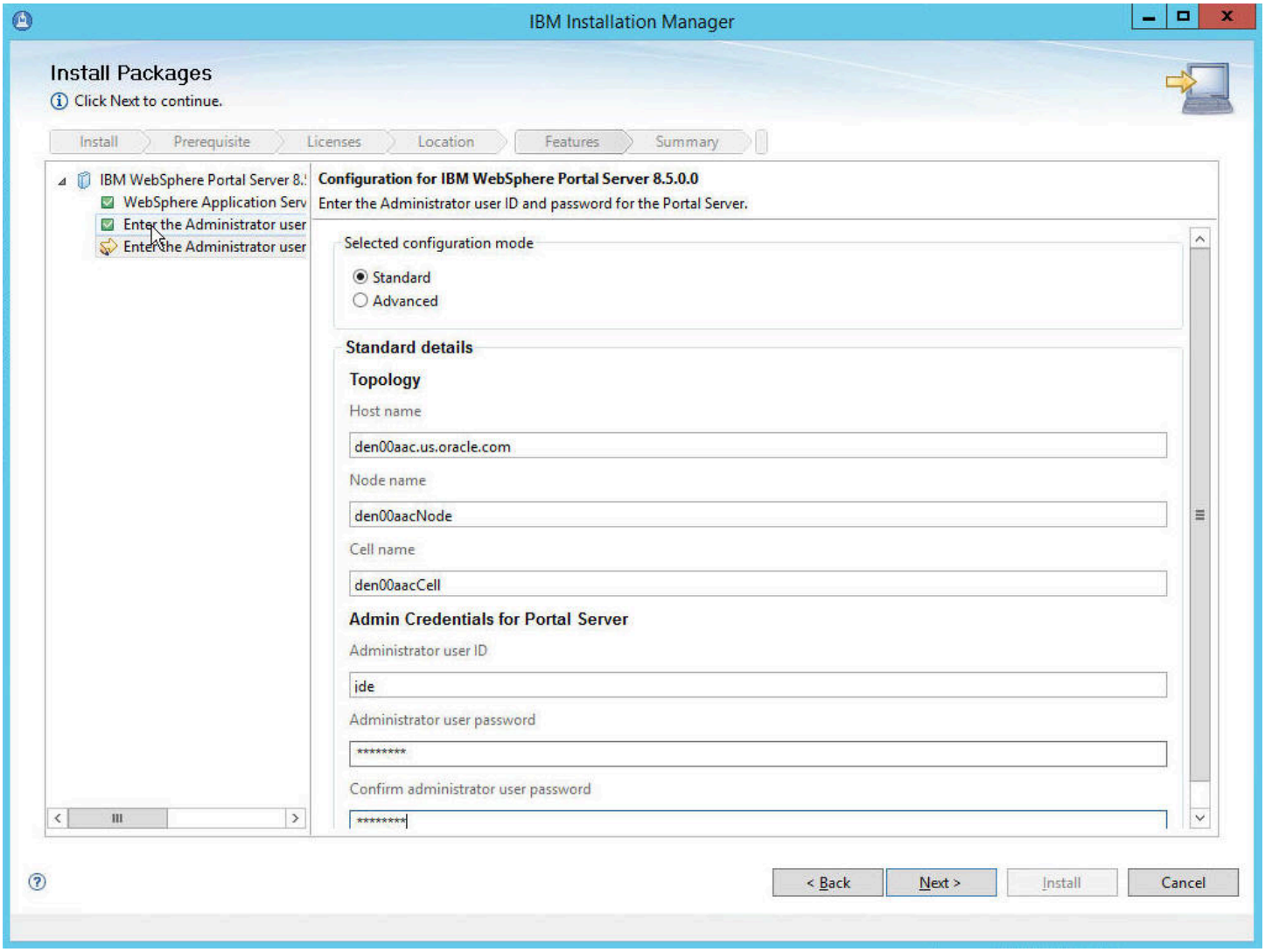
25. Verify the existing WebSphere Application Server root directory and click Next.



26. On the security screen for the administration user ID and password, WebSphere Portal enables security by default. It is not possible and/or recommended to disable security. Complete these fields:

Field	Description
Administrative User ID	Enter the user ID that you assign for the Portal administrator. For example: wpsadmin This user is used for Stopping Services after the Portal installation is completed. It is not related to any user IDs used to access the operating system.
Administrative Password	Enter the password for the Administrative User defined in the previous field.
Confirm Password	Confirm the password you entered in the previous field.

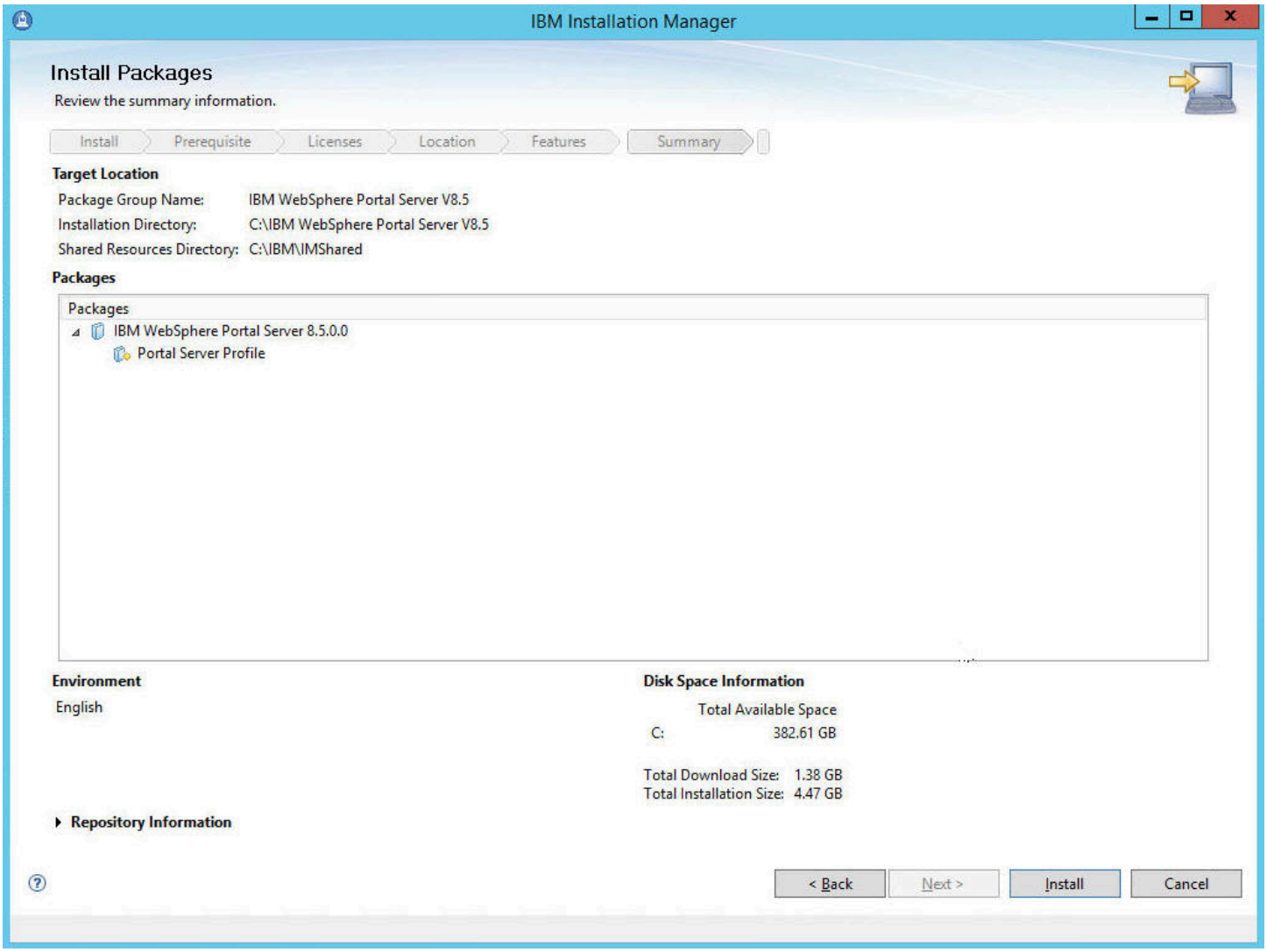
Field	Description



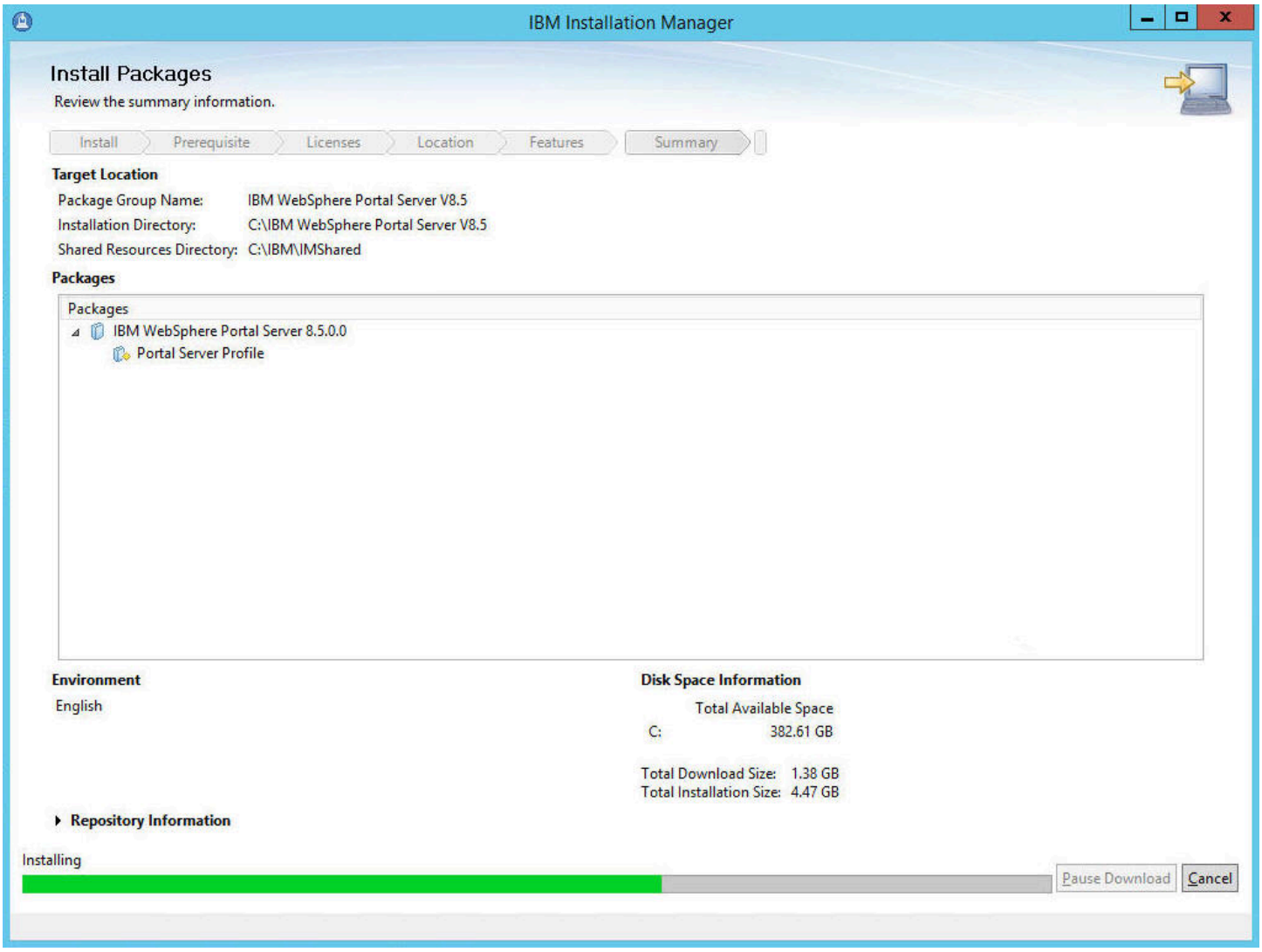
27. On the instance properties screen, complete these fields:

Field	Description
Node name	Enter a unique Node name for this installation of WebSphere Portal and Lotus Web Content Management. The Node name is used to identify the server. Having a unique node name is important when configuring a federated, production environment. Do not use names that contain special characters (i.e _ underscore..etc.).
Host name	Enter the fully-qualified Host name for this installation of WebSphere Portal and Lotus Web Content Management. The Host name must include the fully-qualified domain name (for example, hostname.example.com). Do not use a local host or a loopback address

Field	Description



28. Review the summary information. Click Install.



29. A progress bar will appear at the bottom of the screen.
30. Select Use the existing package group and click Next.
31. The progress of the install will be displayed in the bar along the bottom of the screen.

32. When the install completes successfully, this screen will appear.

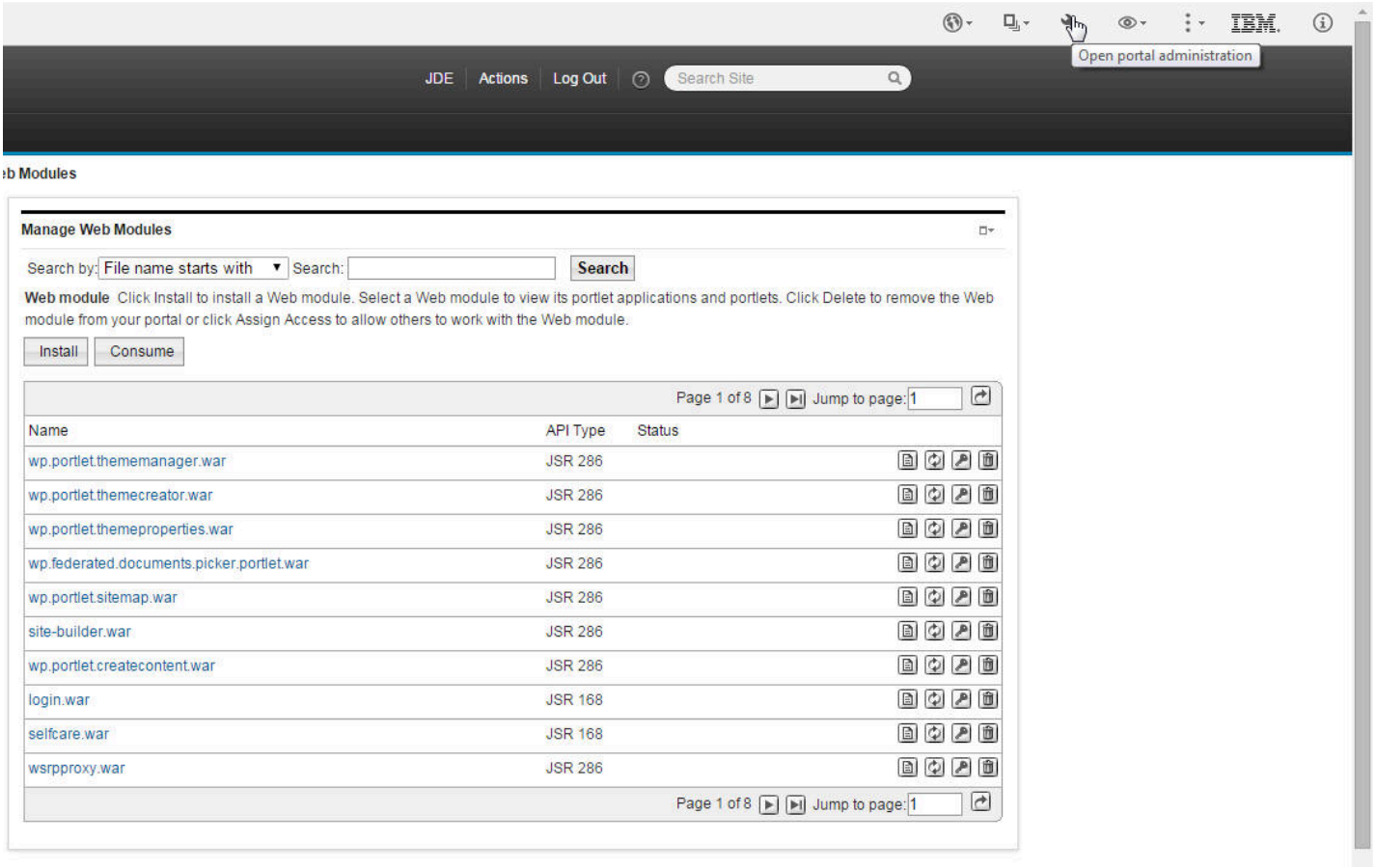
This completes the installation of WebSphere Portal 8.5.

Registering the WSRP Provider

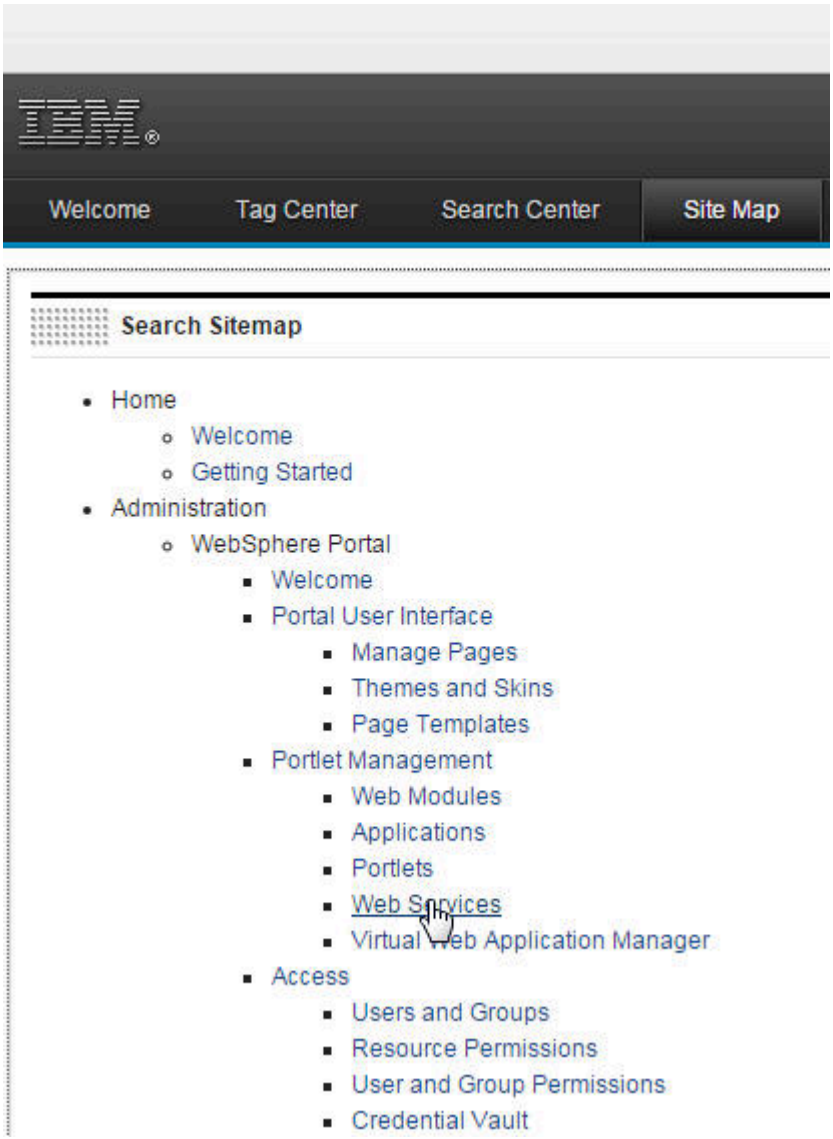
To register the WSRP Producer:


IBM
Welcome
Tag Center
Search Center
Site Map
Search Sitemap
Home
Welcome
Getting Started
Administration
WebSphere Portal
Welcome
Portal User Interface
Manage Pages
Themes and Skins
Page Templates
Portlet Management
Web Modules
Applications
Portlets
Web Services
Virtual Web Application Manager
Access
Users and Groups
Resource Permissions
User and Group Permissions
Credential Vault
Portal Settings
Global Settings
Custom Unique Names
Supported Markups
Supported Clients
Import XML
Portal Content
Web Content Libraries
Syndicators
Subscribers
Feed Configurations
Feed Jobs
Search Administration
Manage Search
Portal Analysis
Theme Analyzer
Frequent Users
Enable Tracing
About IBM WebSphere Portal

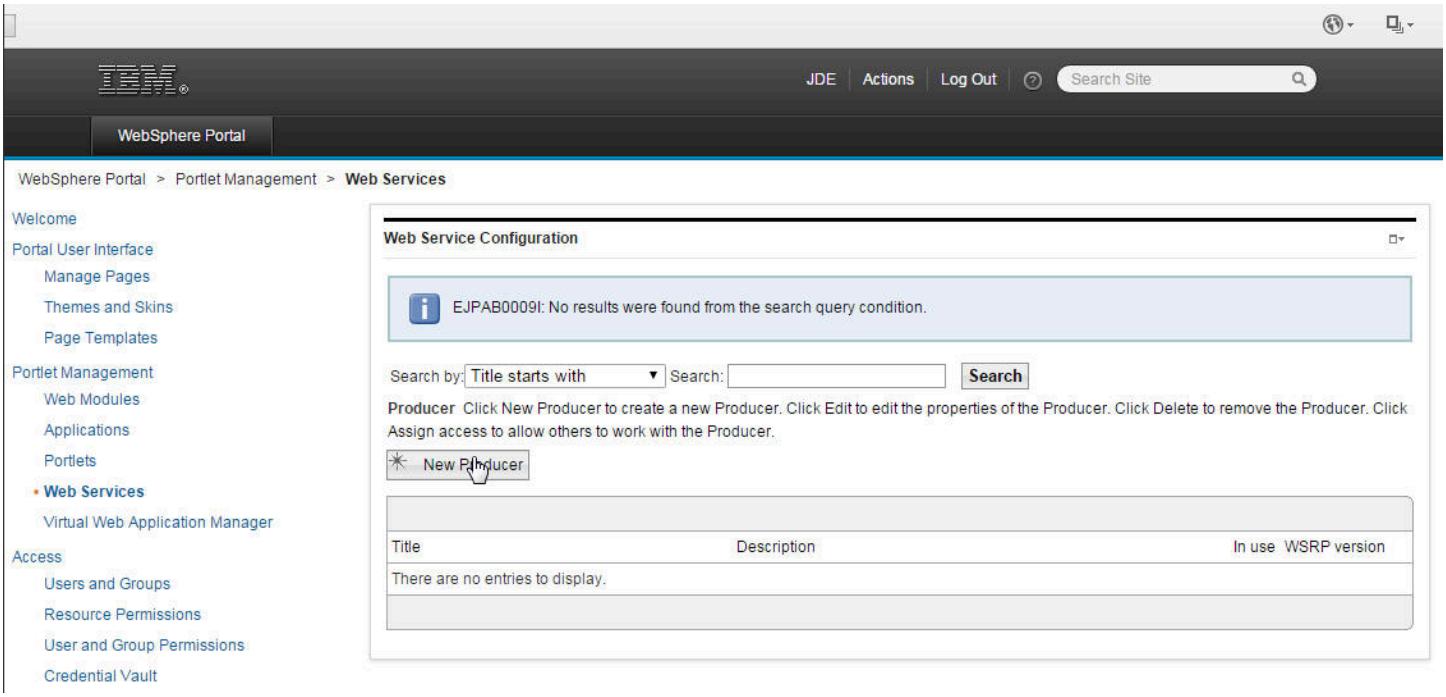
1. When the IBM WebSphere Portal is launched a Site Map will be available. Select WebSphere Portal located below Administration.



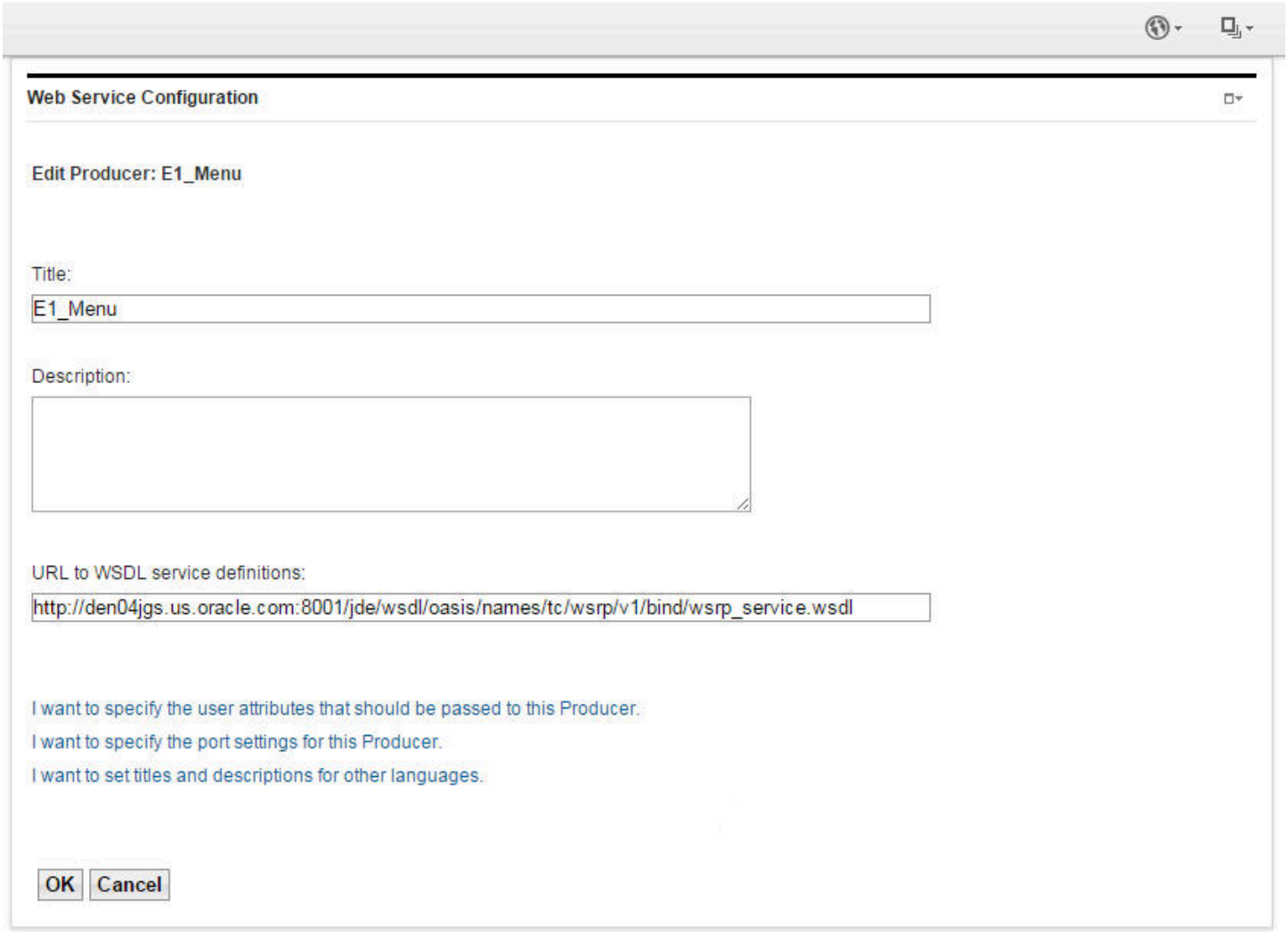
2. Select the Open portal administration icon located in the upper right side of the toolbar.



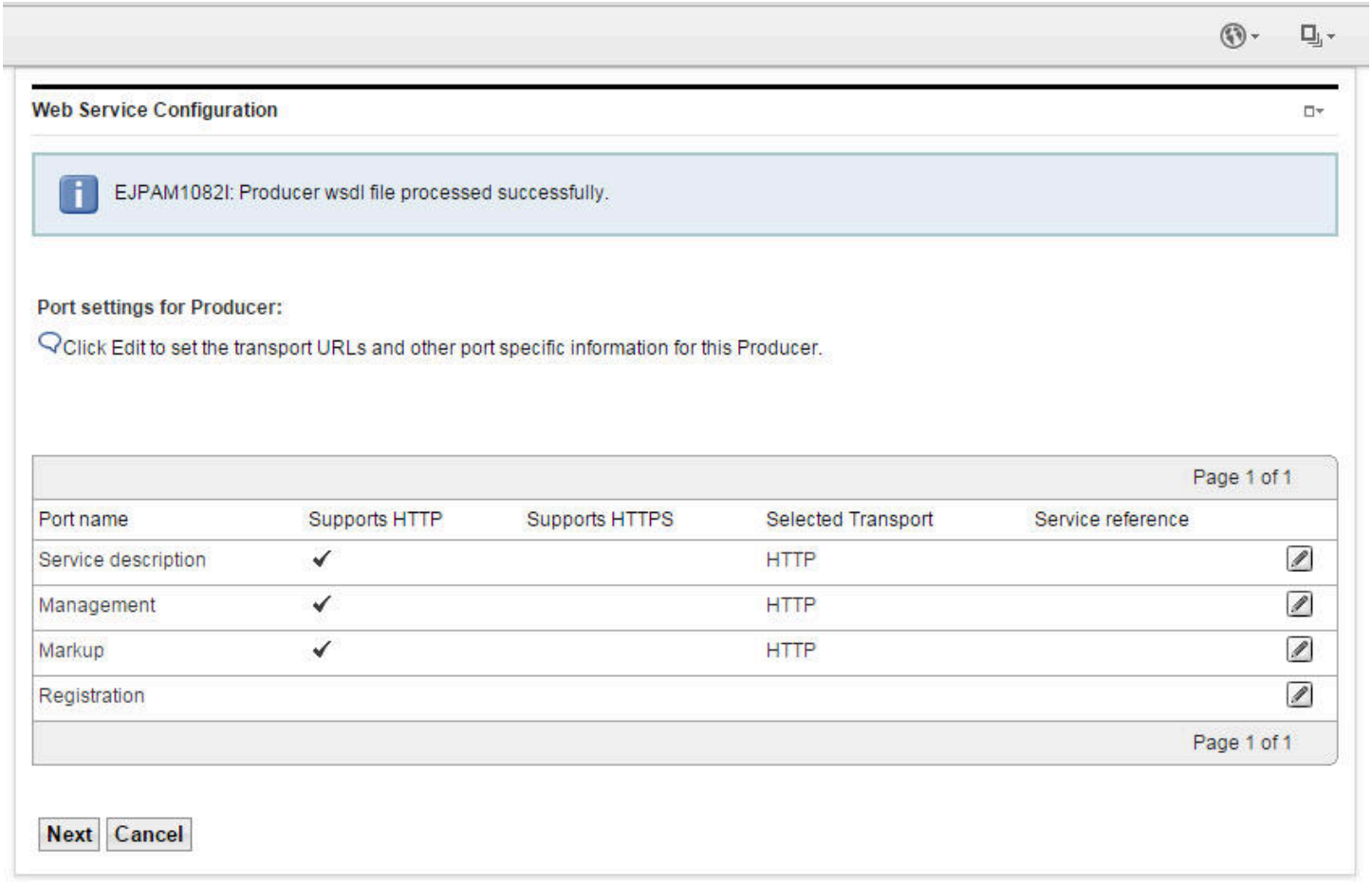
3. Next, click on Web Services located below Portlet Management.



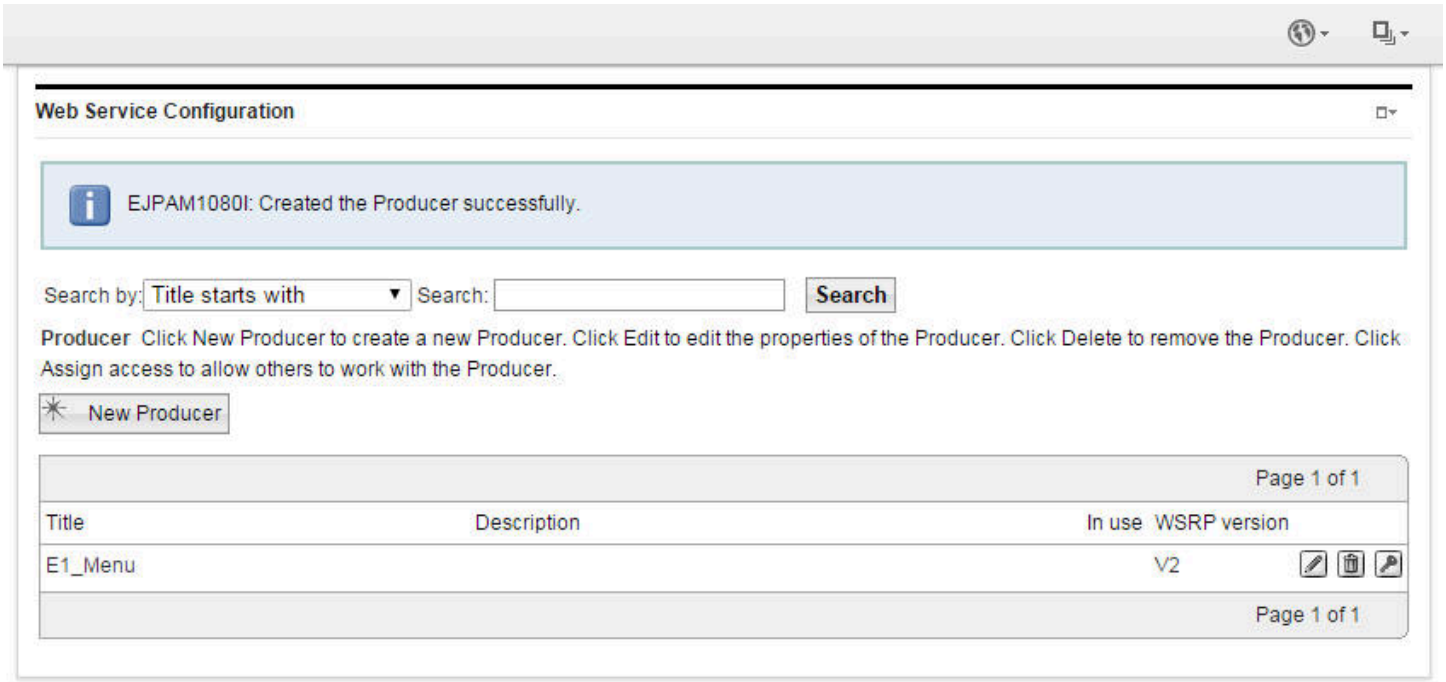
4. Click the New Producer button.



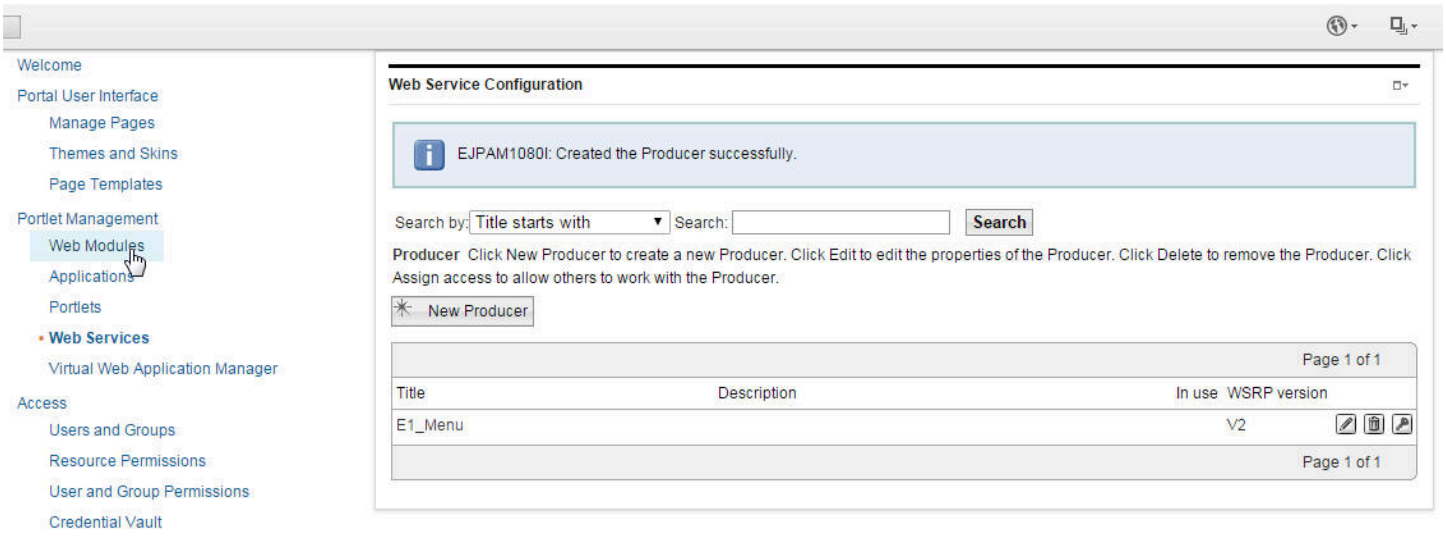
5. Verify or enter the Edit Producer URL. Click OK.



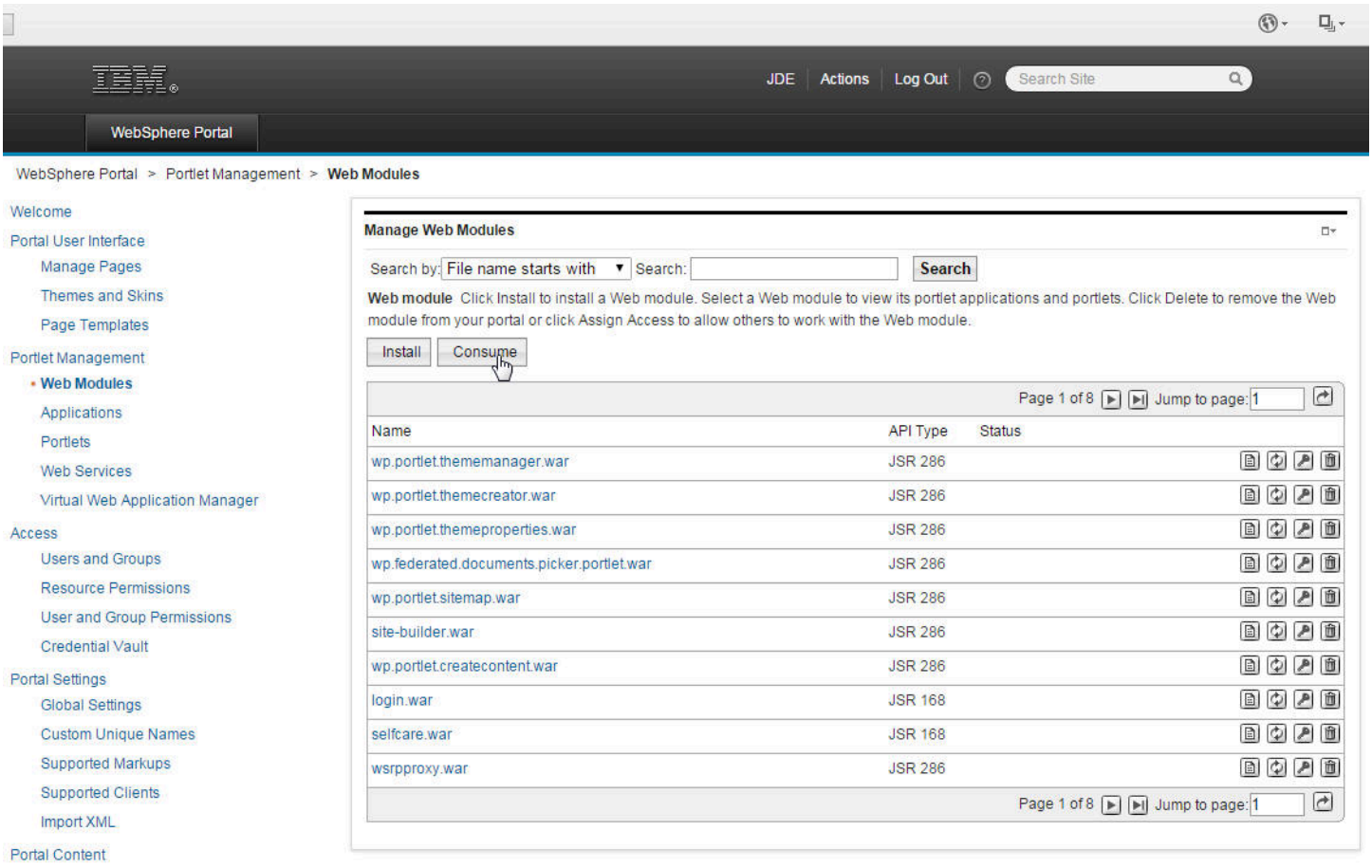
6. Click Edit to set the transport URLs and other port specific information for this Producer. Click Next.



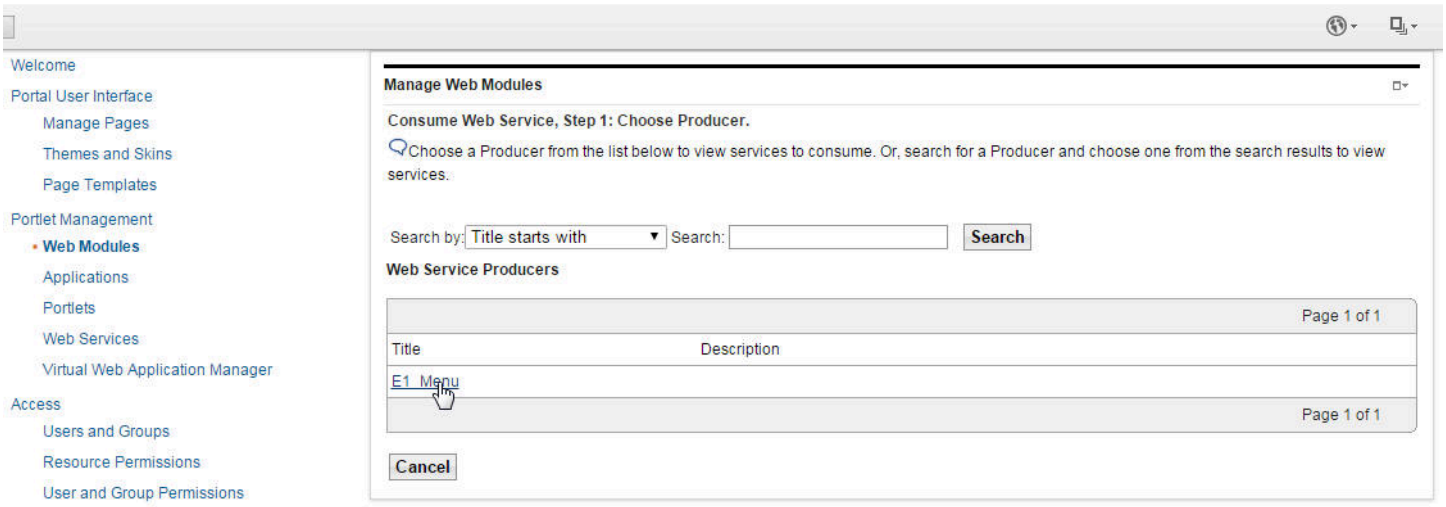
7. Add a New Producer if needed.



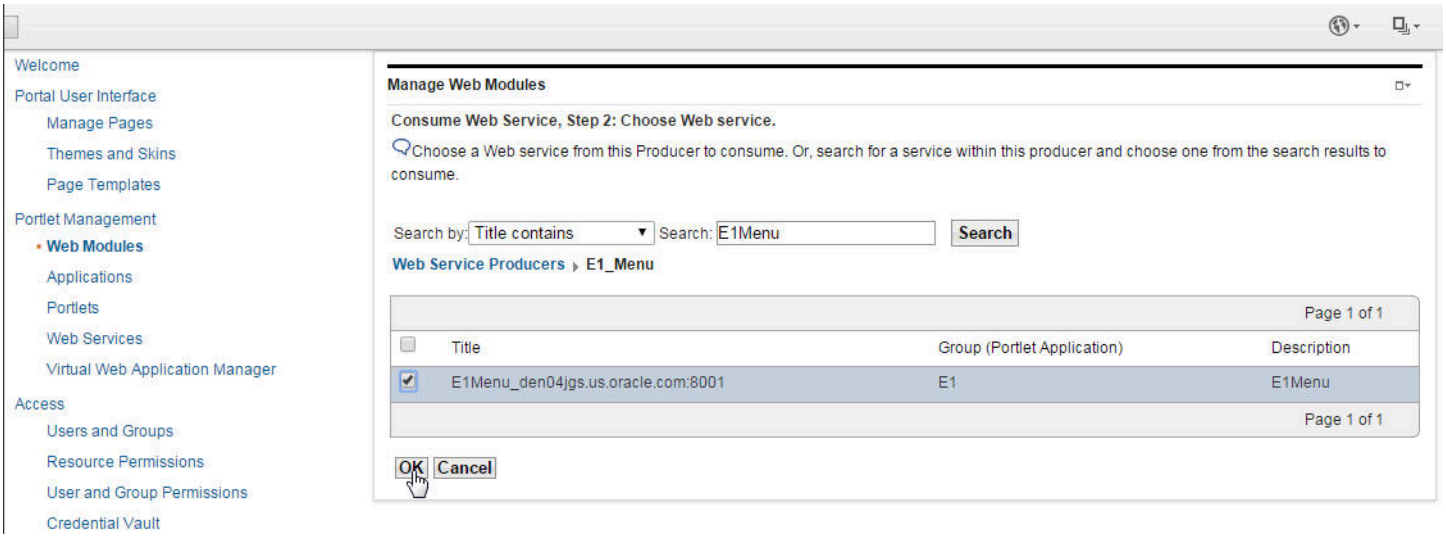
8. Select Web Modules below Portlet Management.



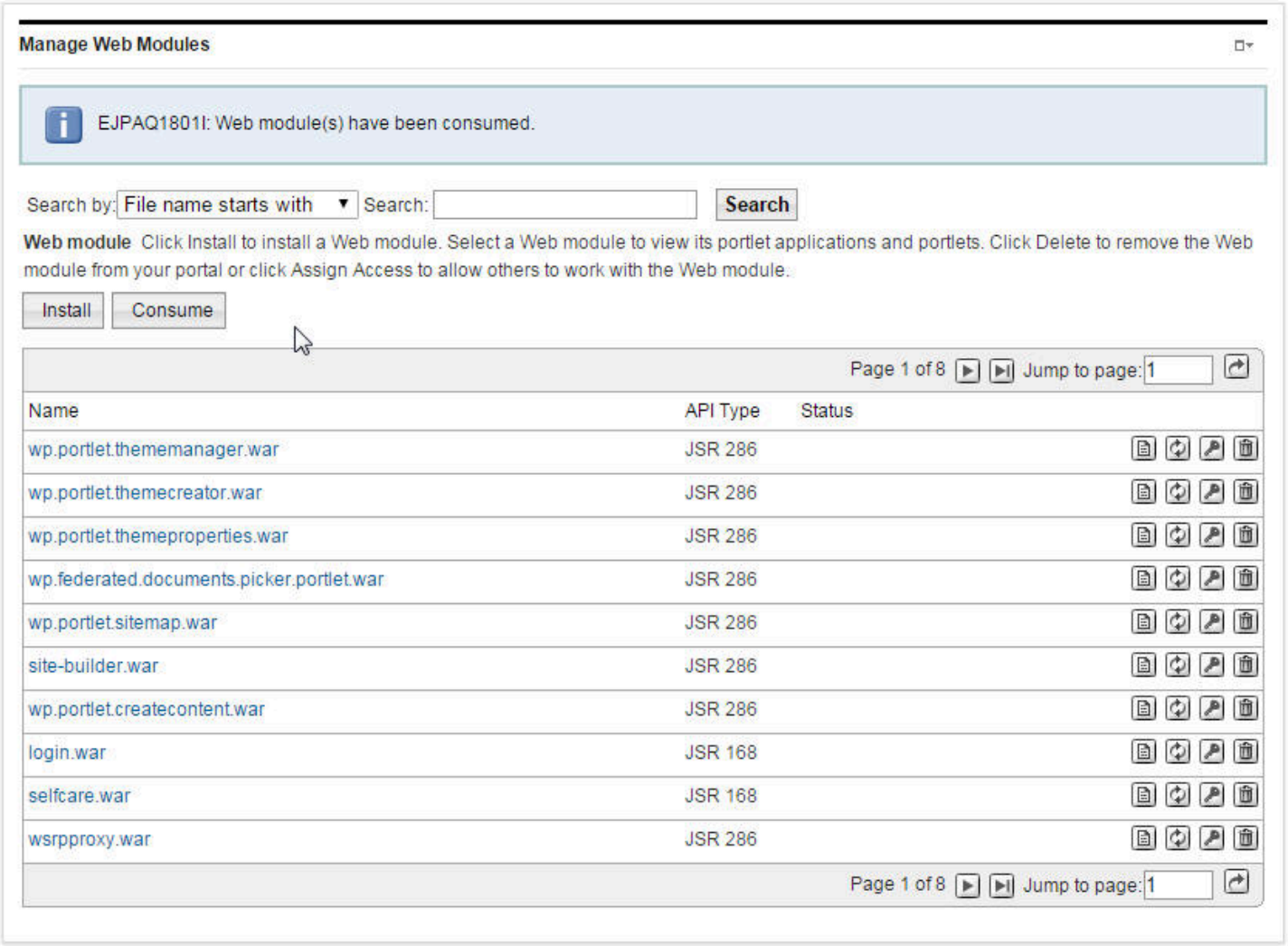
9. Click the Consume button.



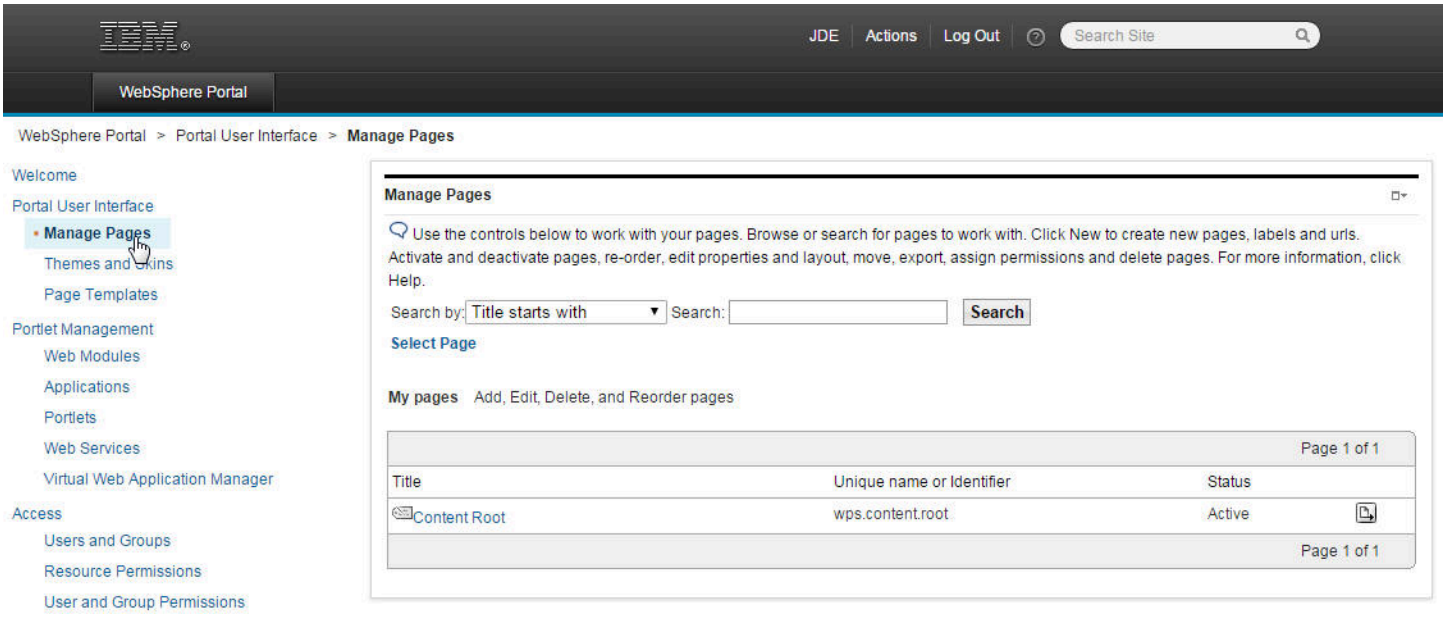
10. Click the E1_Menu hyperlink.



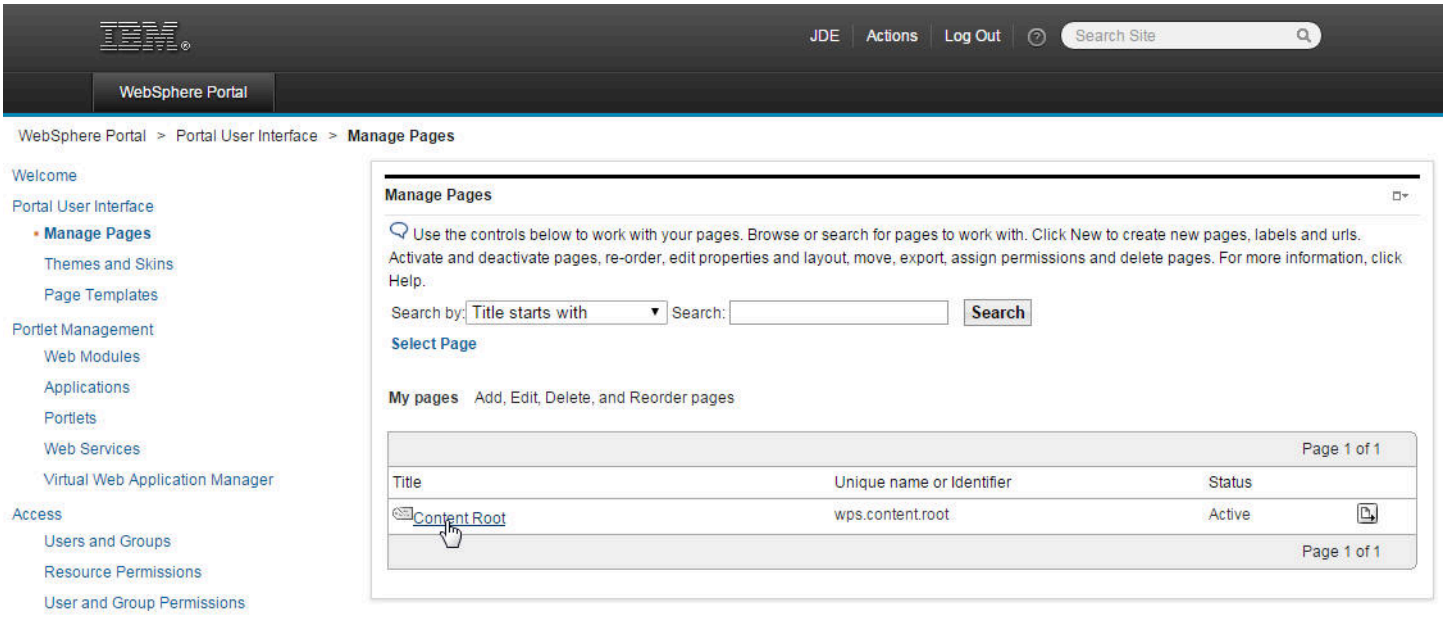
11. Click OK.


Manage Web Modules
EJPAQ1801I: Web module(s) have been consumed.
Search by: File name starts with
Search:
Search
Web module Click Install to install a Web module. Select a Web module to view its portlet applications and portlets. Click Delete to remove the Web module from your portal or click Assign Access to allow others to work with the Web module.
Install
Consume
Page 1 of 8
Jump to page: 1
Name
API Type
Status
wp.portlet.thememanager.war JSR 286
wp.portlet.themecreator.war JSR 286
wp.portlet.themeproperties.war JSR 286
wp.federated.documents.picker.portlet.war JSR 286
wp.portlet.sitemap.war JSR 286
site-builder.war JSR 286
wp.portlet.createcontent.war JSR 286
login.war JSR 168
selfcare.war JSR 168
wsrpproxy.war JSR 286
Page 1 of 8
Jump to page: 1

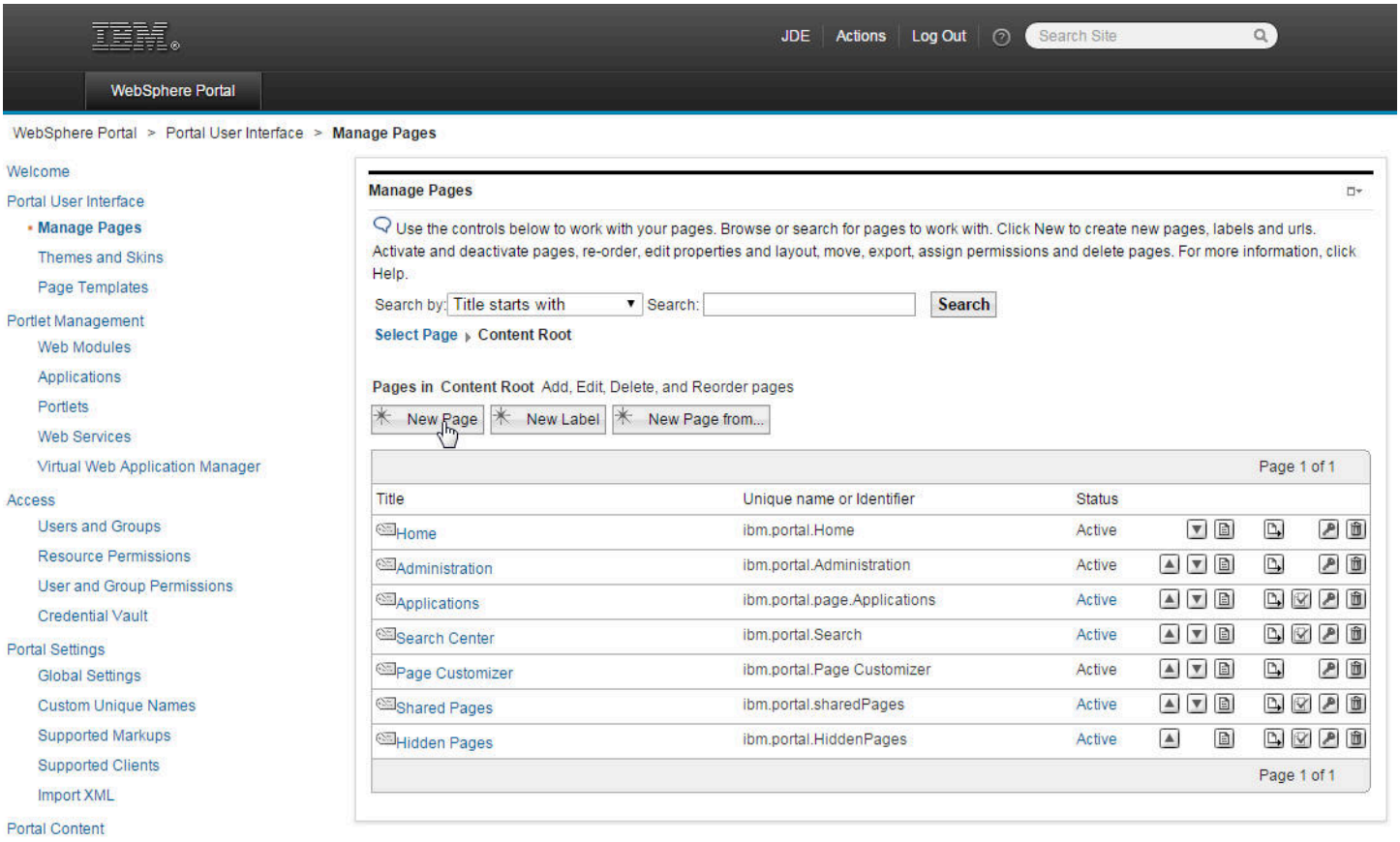
12. Click the Install icon to install a Web module. select a Web module to view its portlet applications and portlets. Click Delete to remove the Web module from your portal or click Assign Access to allow others to work with the Web module.



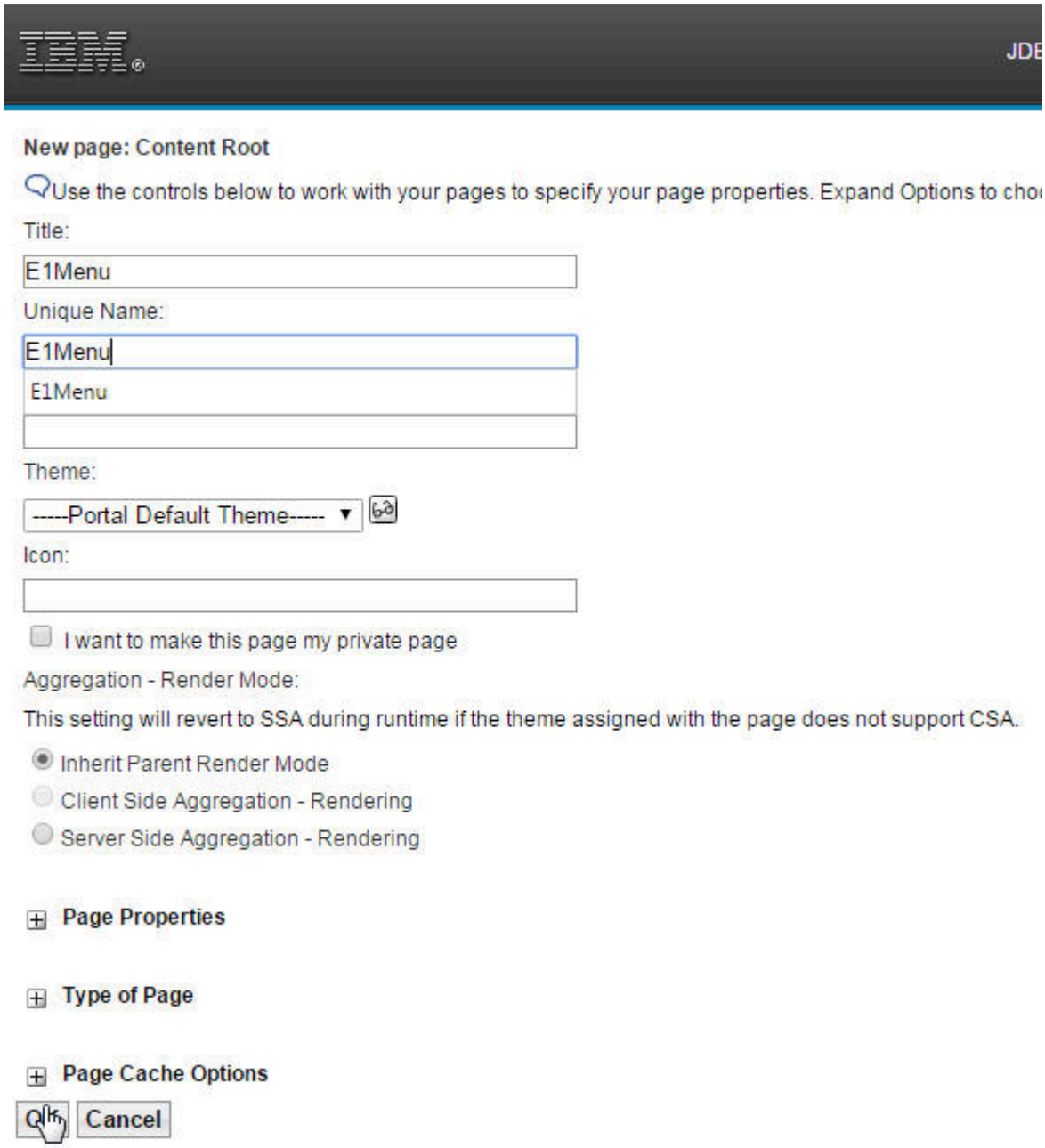
13. Click Manage Pages.



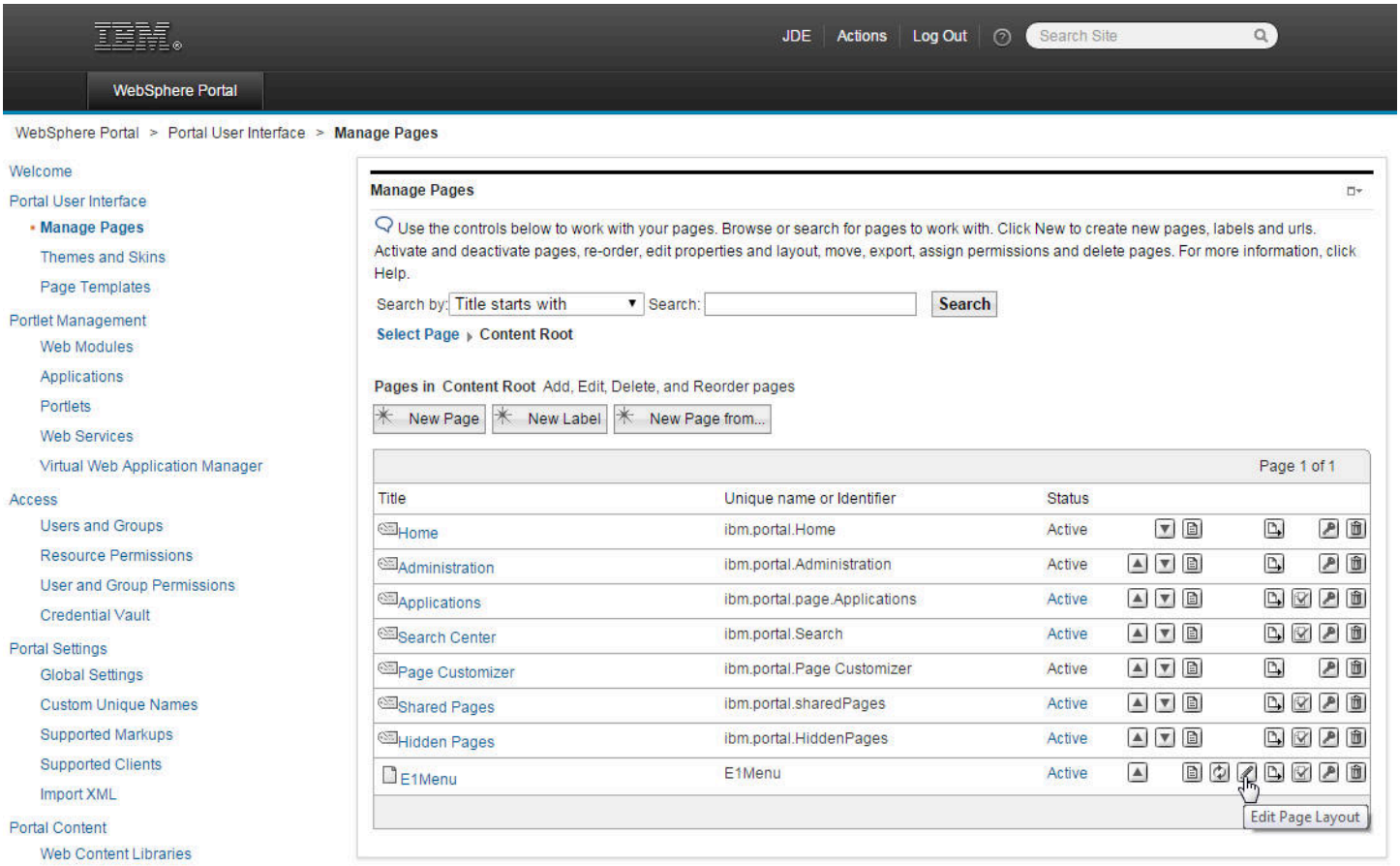
14. Click the Content Root Hyperlink.



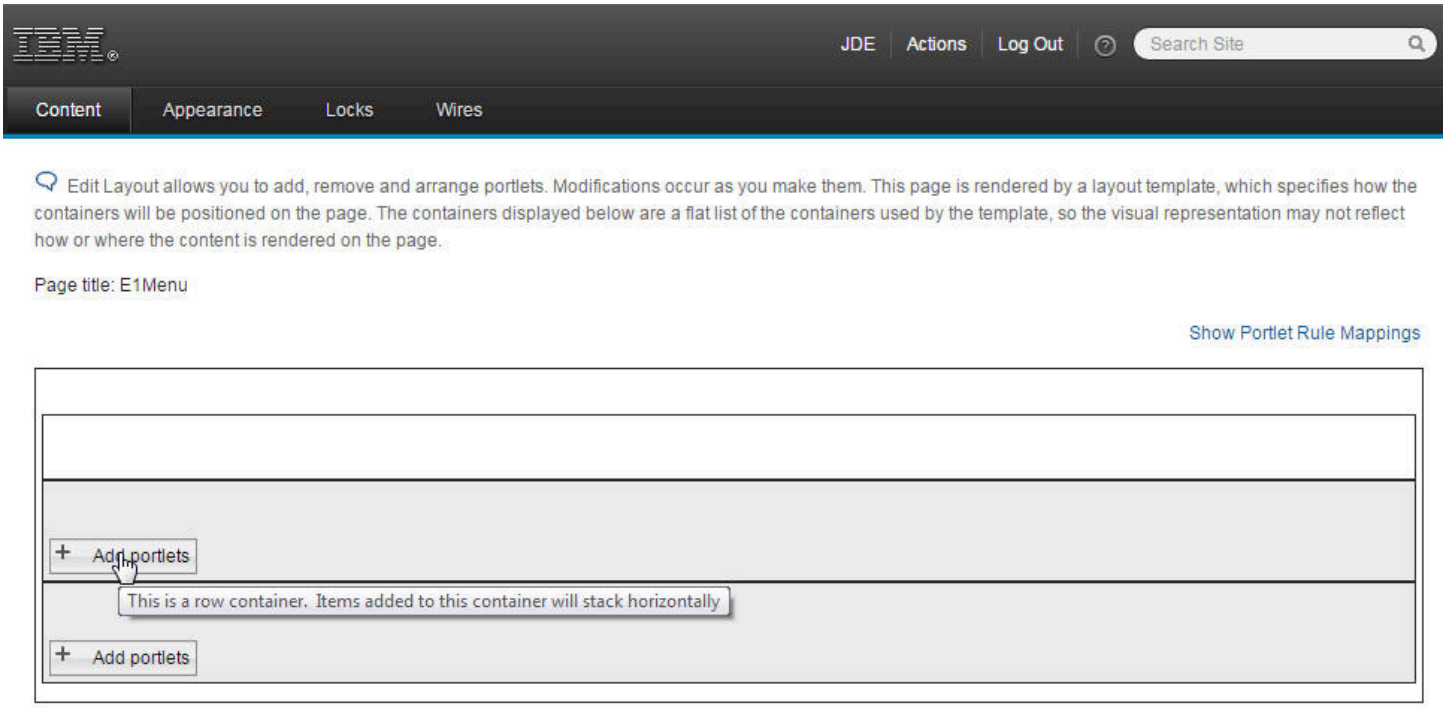
15. Click the New Page button.



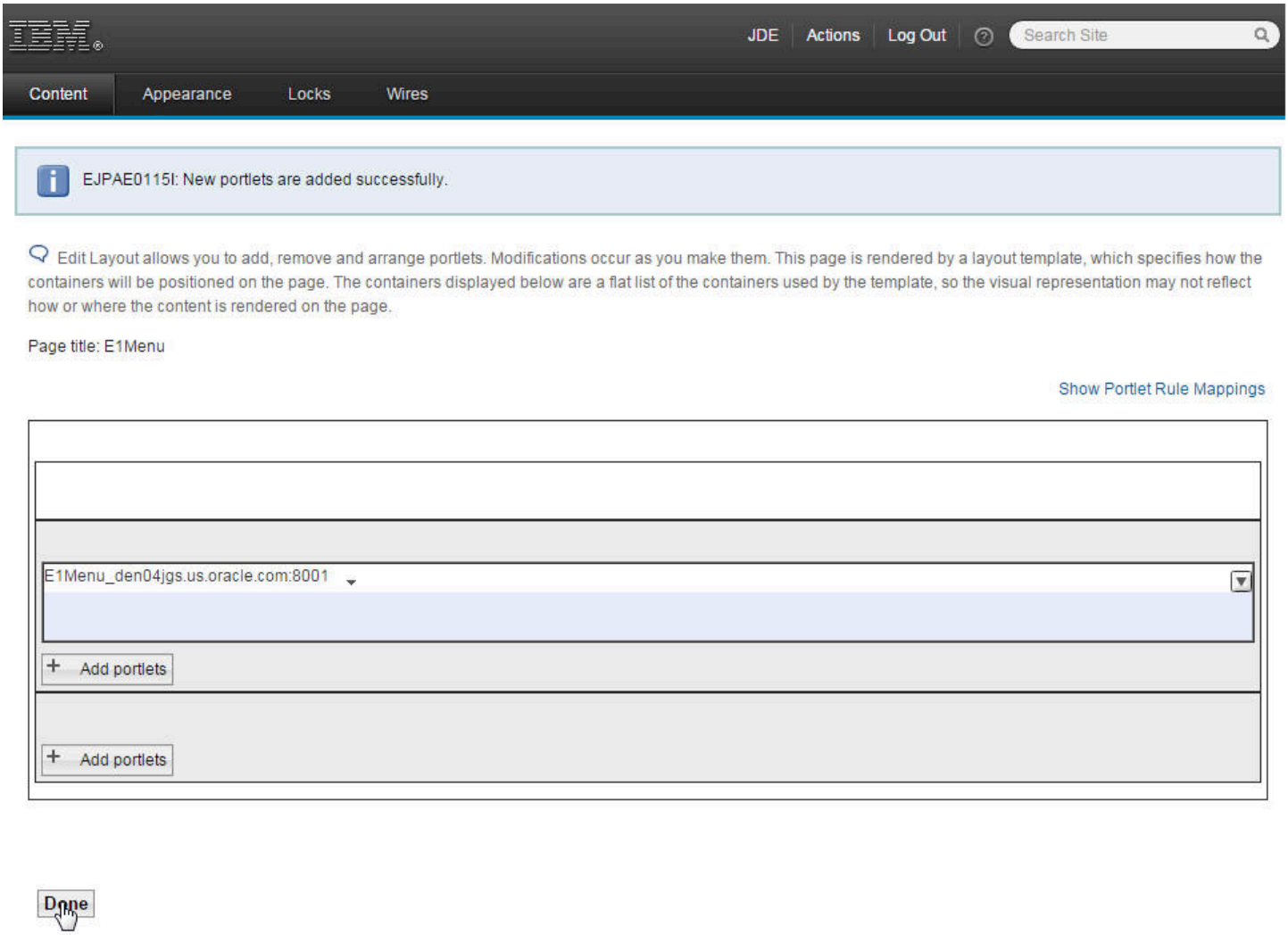
16. Fill in the Title and a Unique Name fields and then click the OK button.



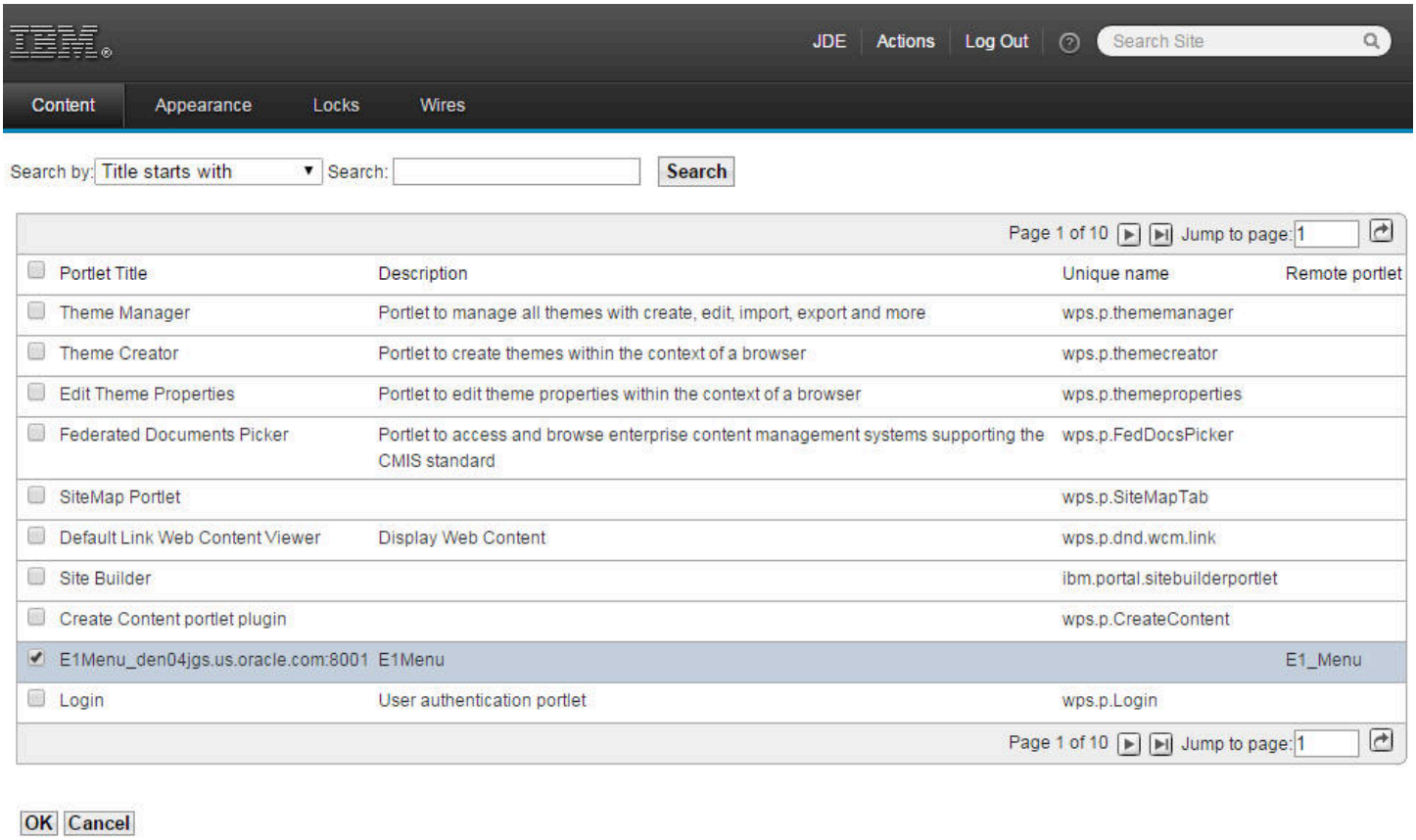
17. Click the Edit Page Layout icon.



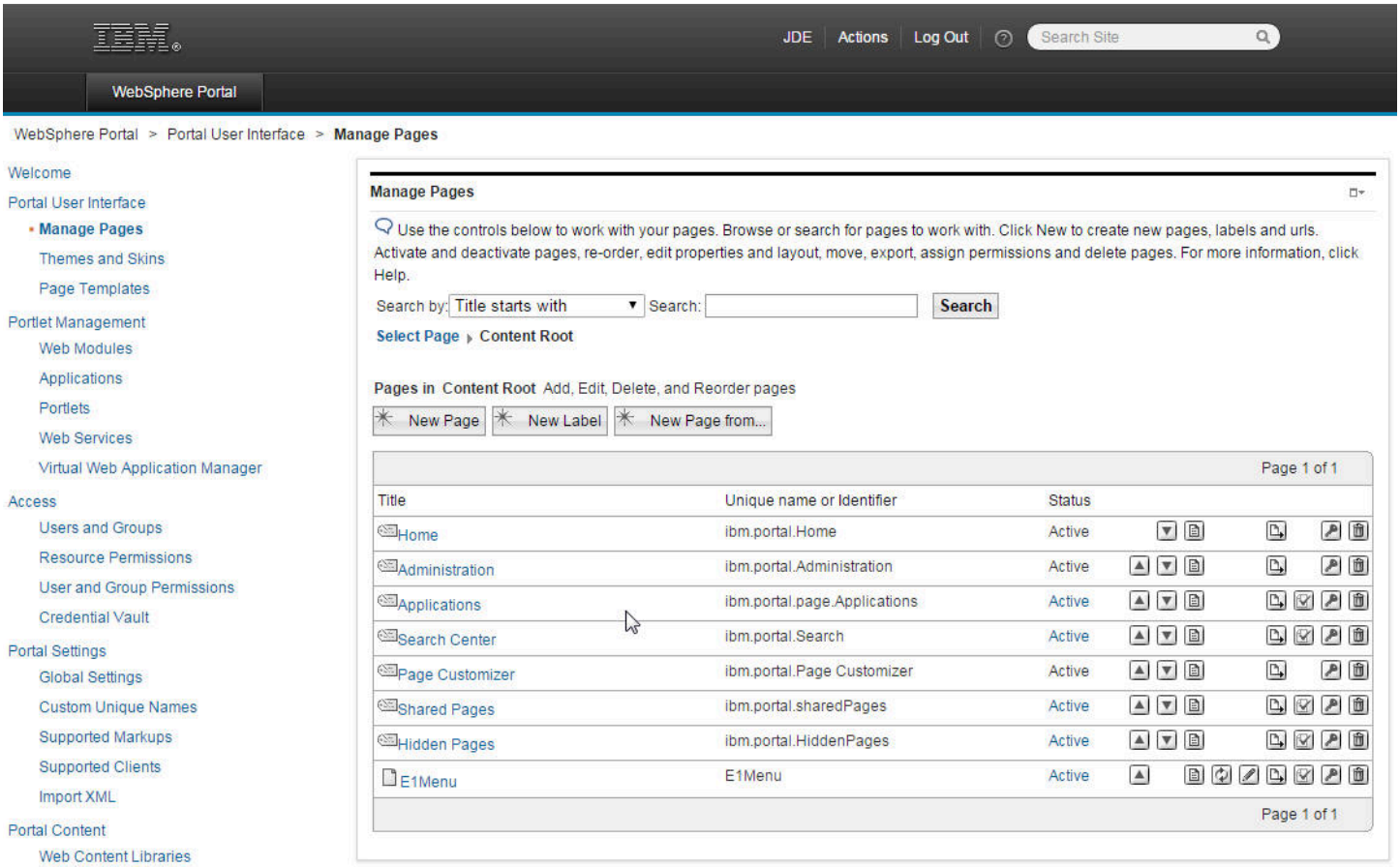
18. Click the Add Portlets button.



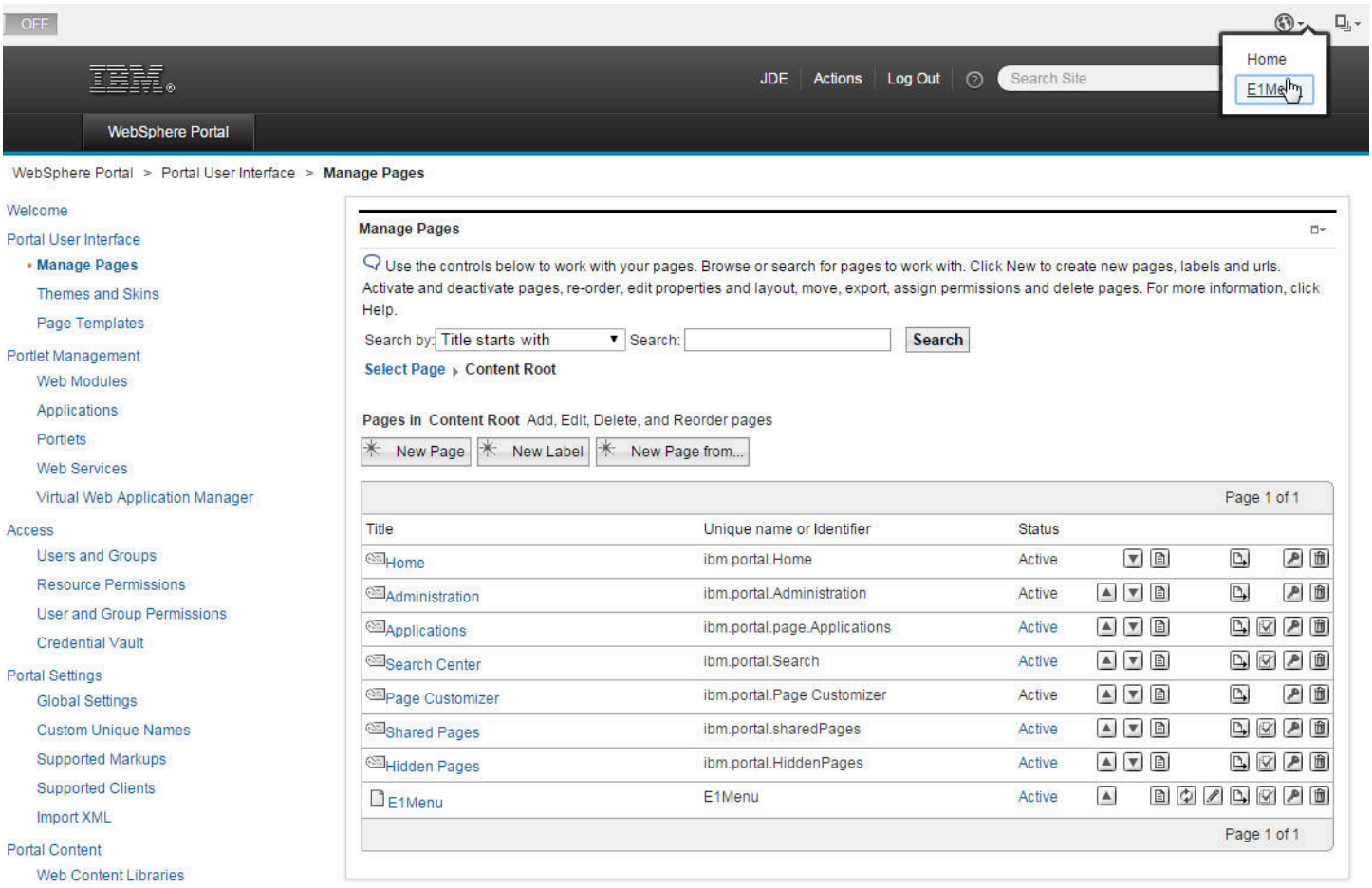
19. When you have added the portlets that you need, click the Done button.



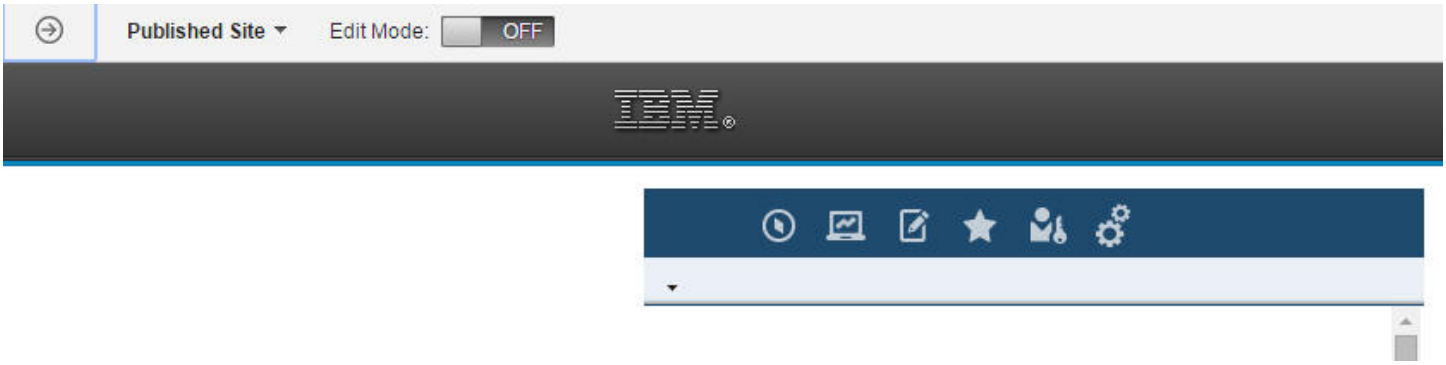
20. Select the E1 Menu and click OK.



21. The Manage Pages screen will display.



22. Select E1 Menu from the dropdown menu in the upper right area of the toolbar.



23. The E1 Menu icons will display.

This completes the successful registration of the WSRP Producer.

3 Using the Migration Wizard

Using the Migration Wizard

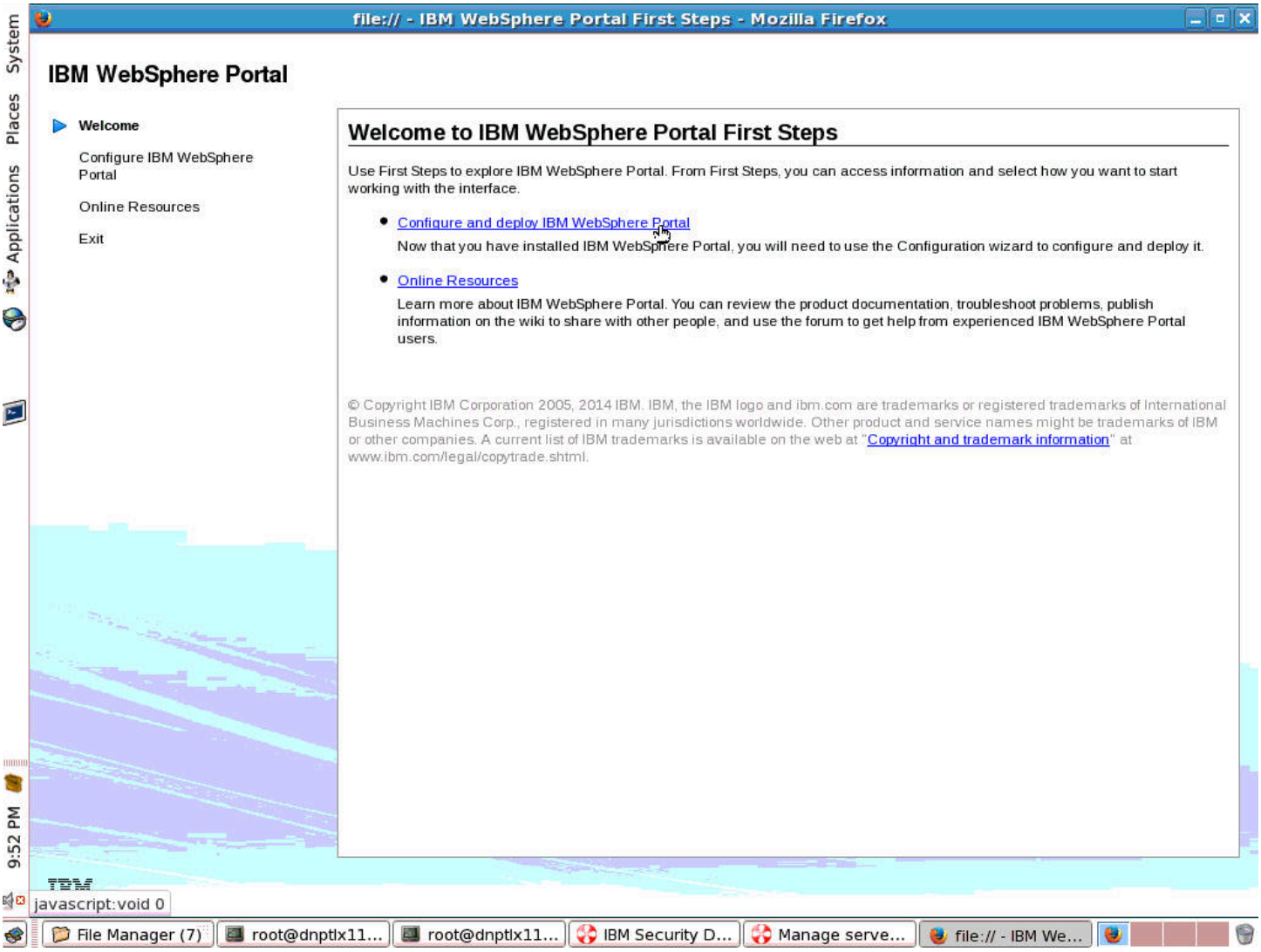
Note: This chapter replaces content from previous guides related to:

- Working with the properties file for the Oracle, DB2 for i, and SQL Server 200x databases
- Transferring WebSphere Portal and Java Content Repository Databases to DB2 for i
- Configuring IBM WebSphere Portal Server v8.5 to use SQL Server 200x Database

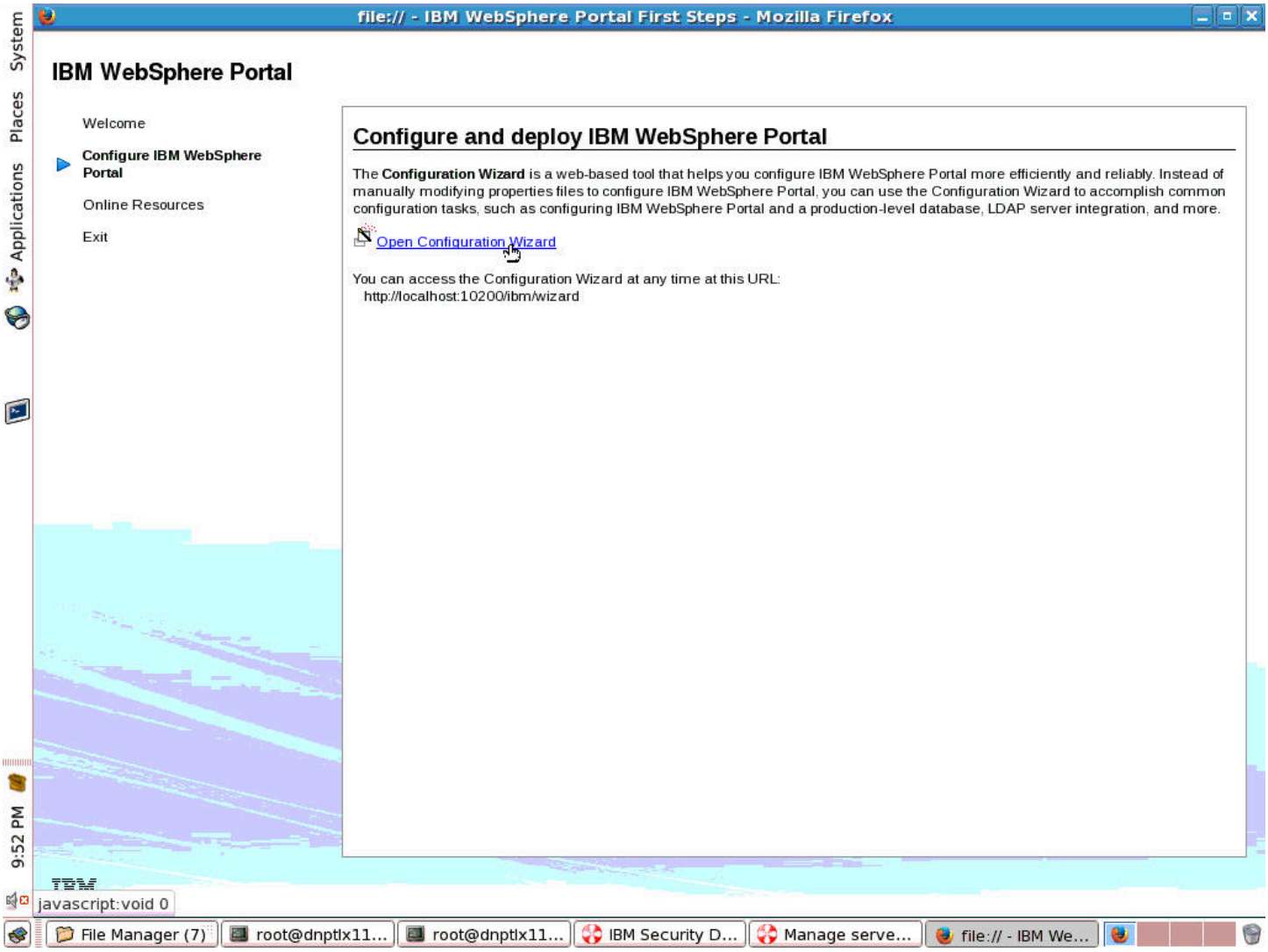
Using the Migration Wizard

To use the Migration Wizard:

1. On the Manage server state tab, select IBM WebSphere | IBM WebSphere Portal Server V8.5 | First Steps to launch the Portal Server First Steps application.

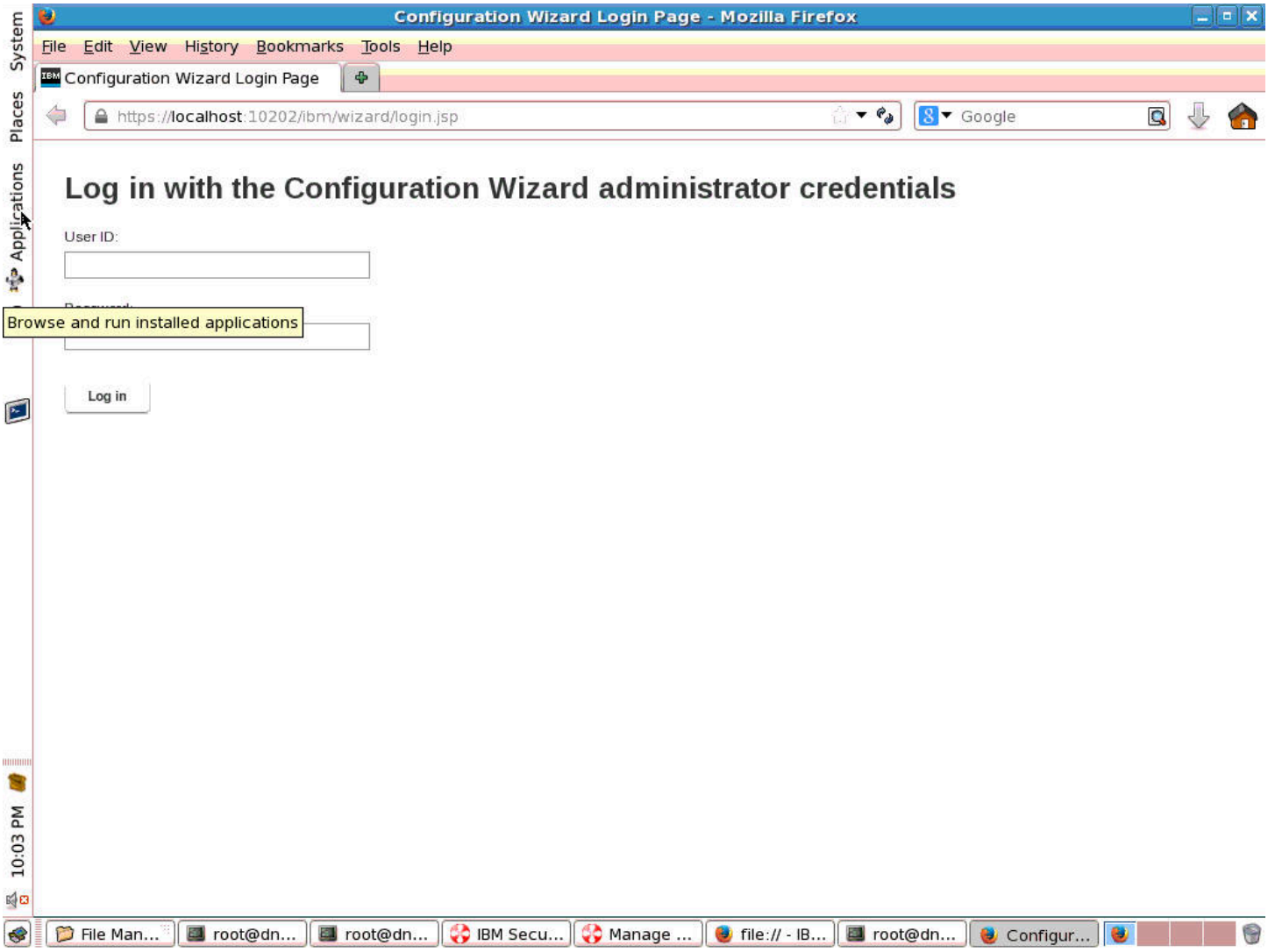

file:// - IBM WebSphere Portal First Steps - Mozilla Firefox
IBM WebSphere Portal
Welcome
Configure IBM WebSphere Portal
Online Resources
Exit
Welcome to IBM WebSphere Portal First Steps
Use First Steps to explore IBM WebSphere Portal. From First Steps, you can access information and select how you want to start working with the interface.
Configure and deploy IBM WebSphere Portal
Now that you have installed IBM WebSphere Portal, you will need to use the Configuration wizard to configure and deploy it.
Online Resources
Learn more about IBM WebSphere Portal. You can review the product documentation, troubleshoot problems, publish information on the wiki to share with other people, and use the forum to get help from experienced IBM WebSphere Portal users.
© Copyright IBM Corporation 2005, 2014 IBM. IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.
javascript:void 0
System
Places
Applications
9:52 PM
File Manager (7)
root@dnptlx11...
root@dnptlx11...
IBM Security D...
Manage serve...
file:// - IBM We...

2. Select the **Configure and deploy IBM WebSphere Portal Server** hyperlink.

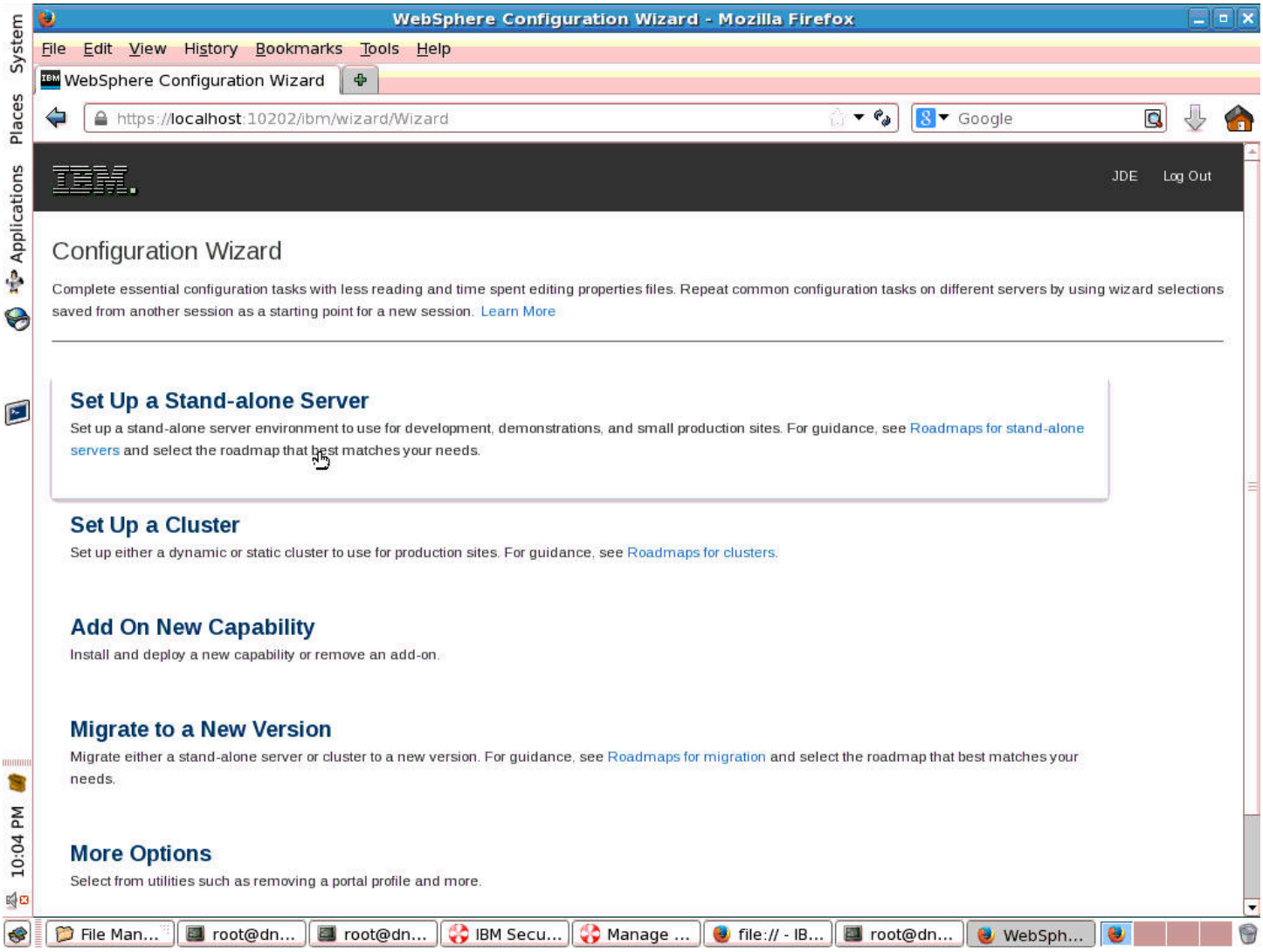


3. Select the Open Configuration Wizard hyperlink.

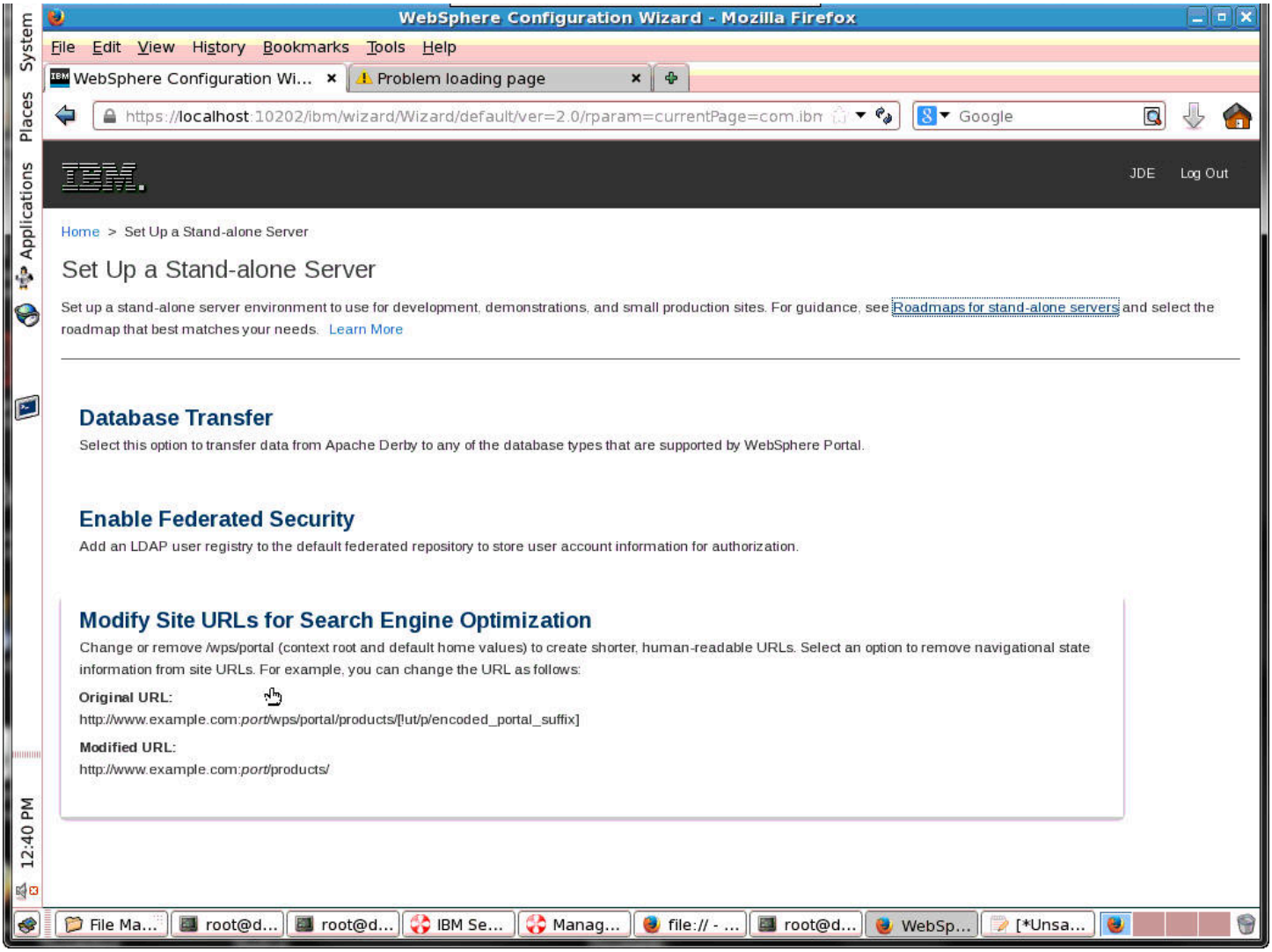
4. Select IBM WebSphere | Start the server.



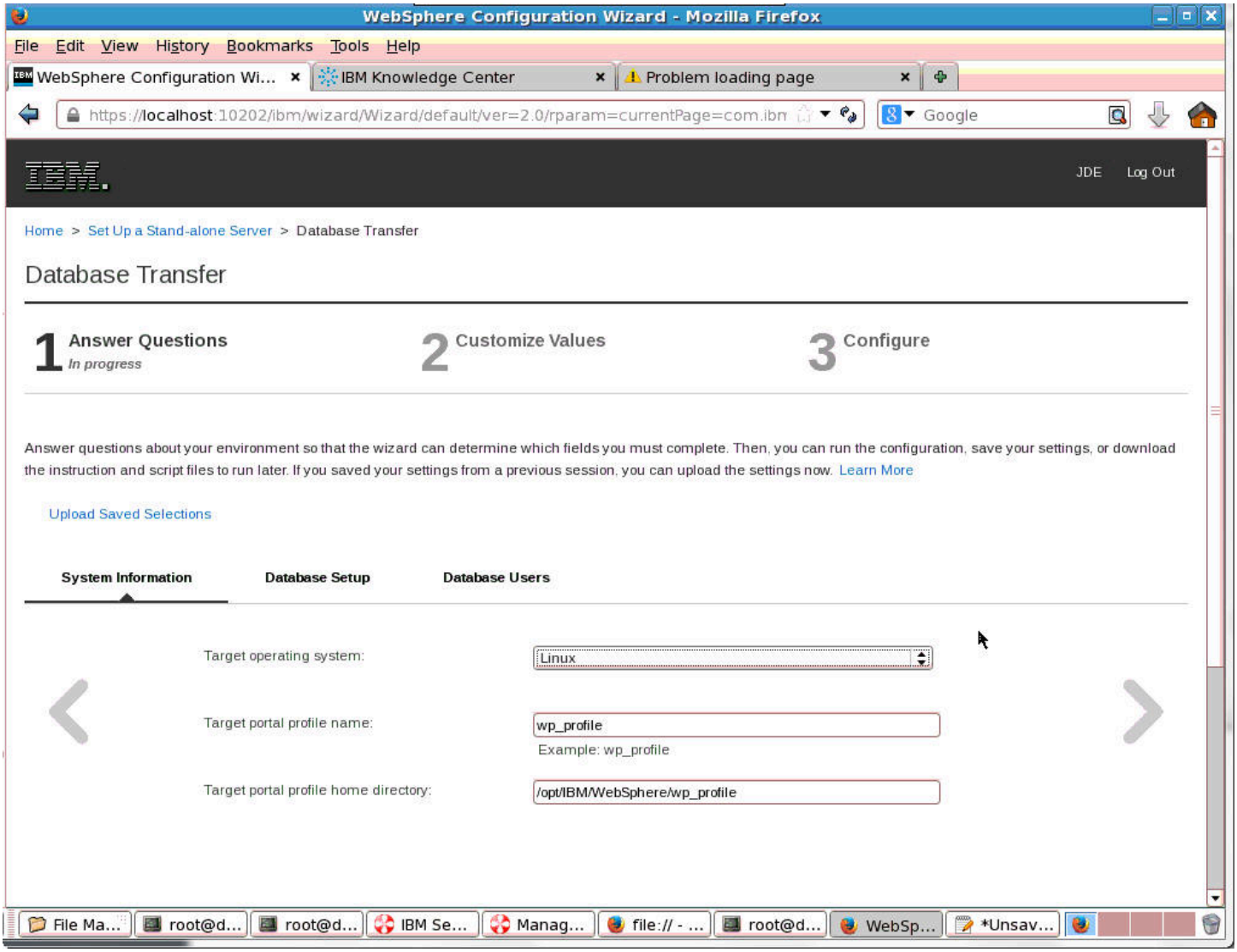
5. Enter User ID and Password to login.



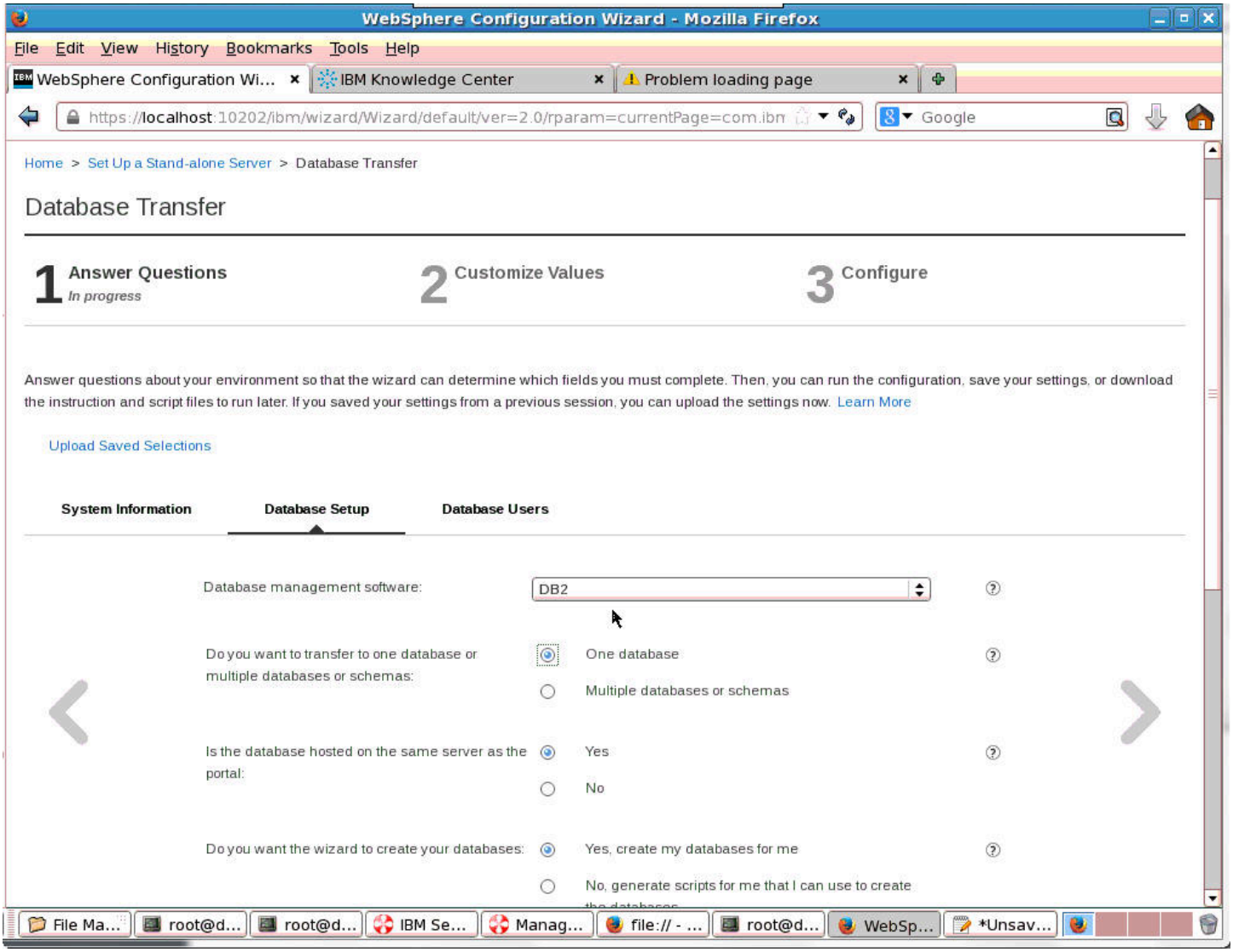
6. Select Set Up a Stand-alone Server.



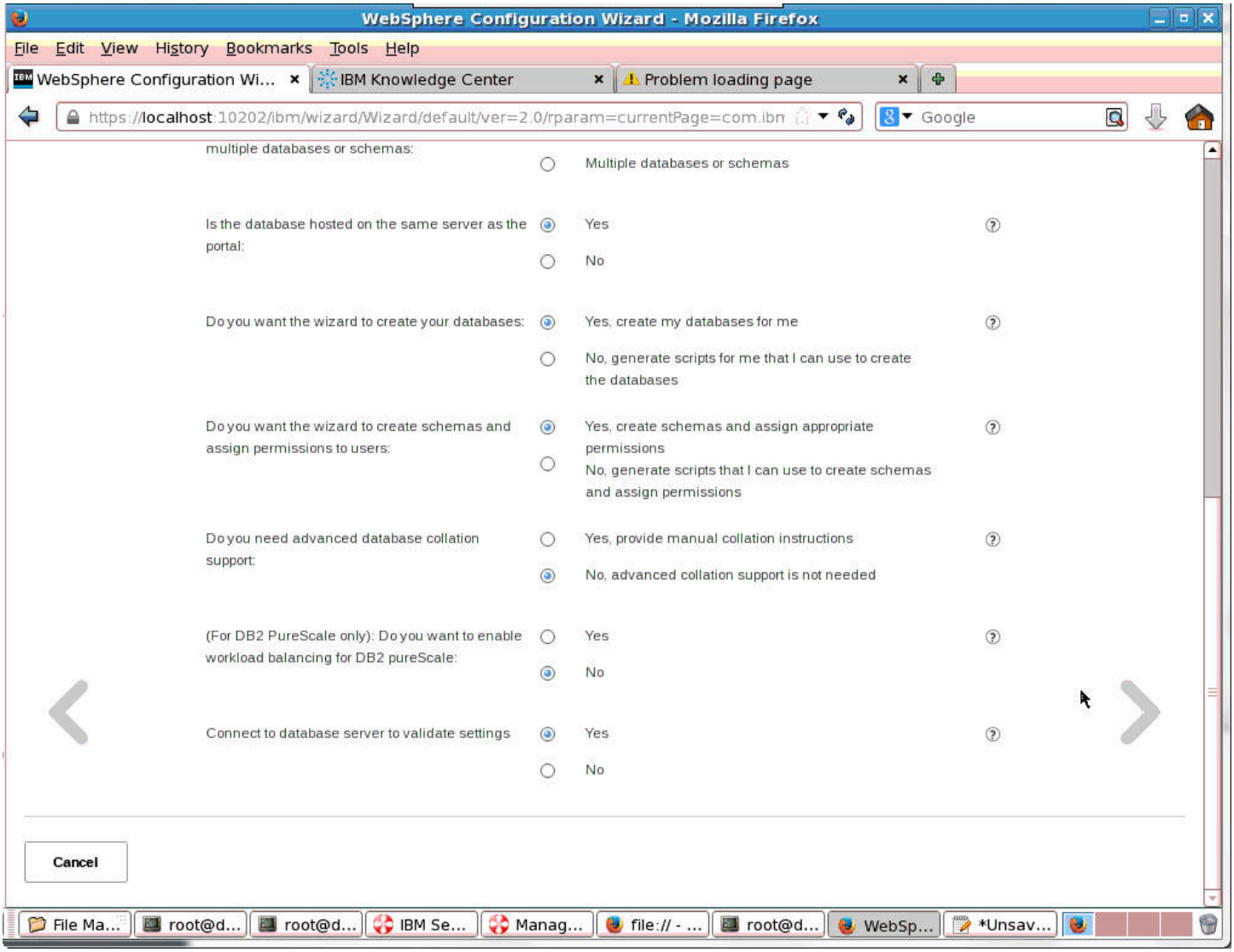
7. Select Database Transfer.



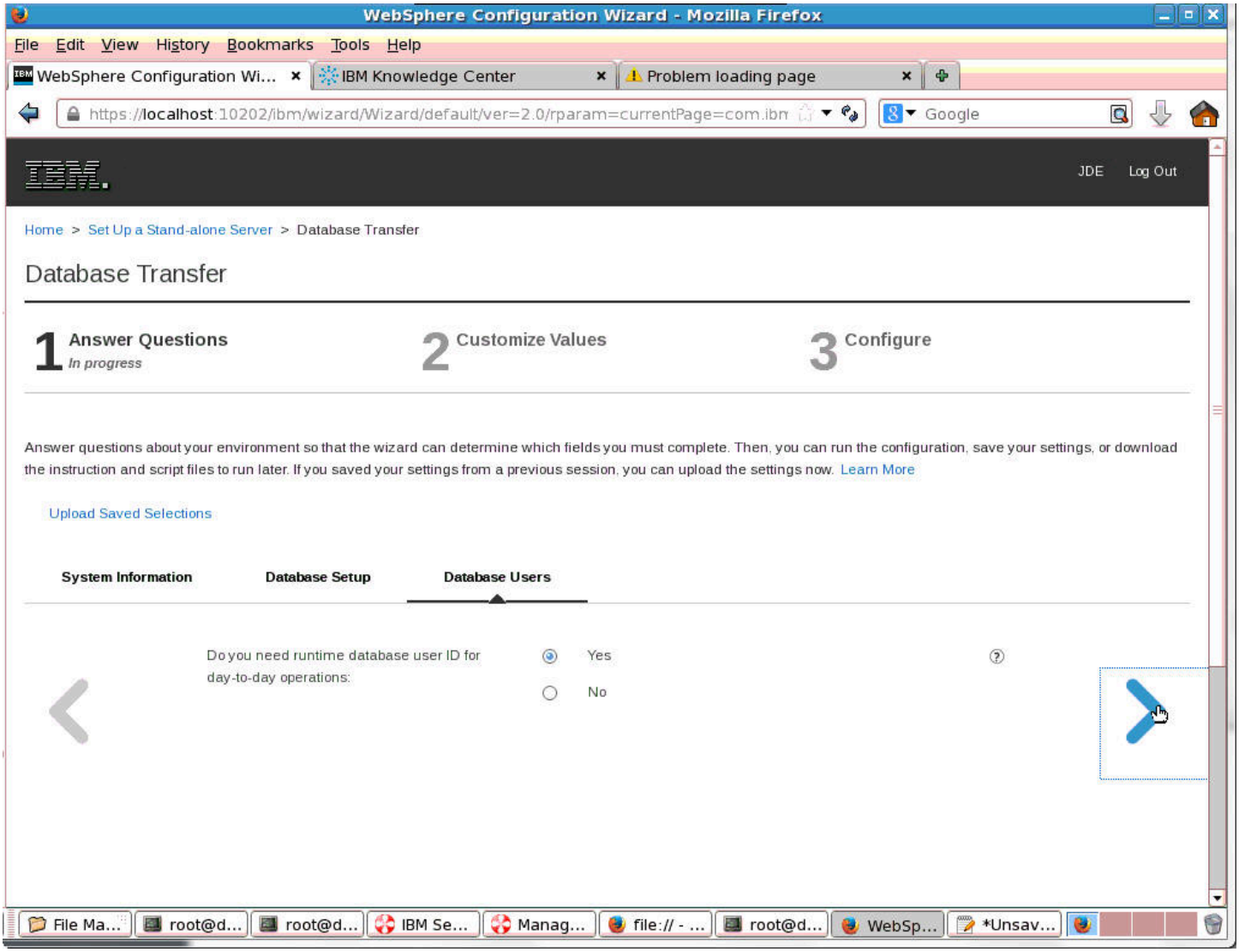
8. Answer the questions for Database Transfer.



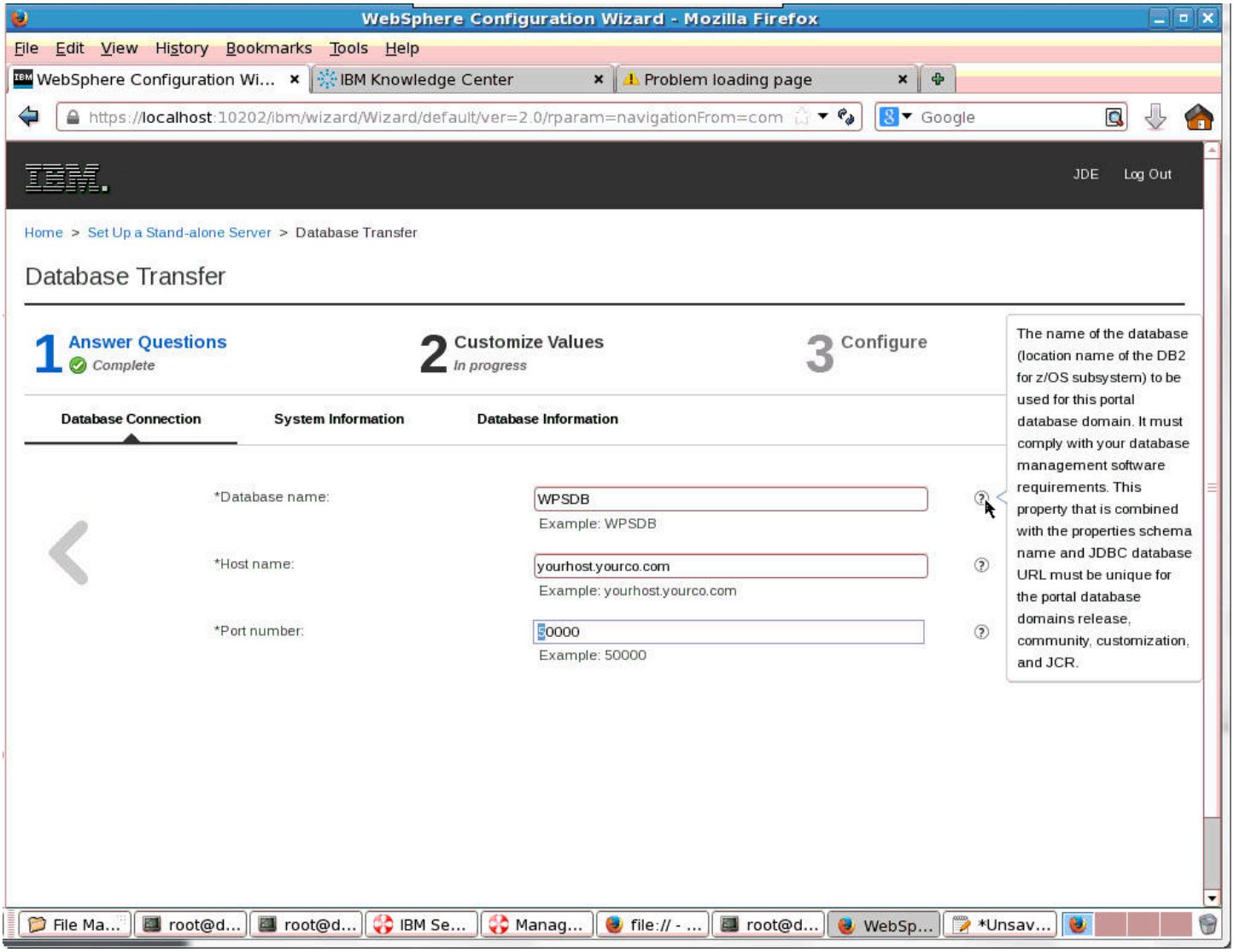
9. Scroll down for more questions.



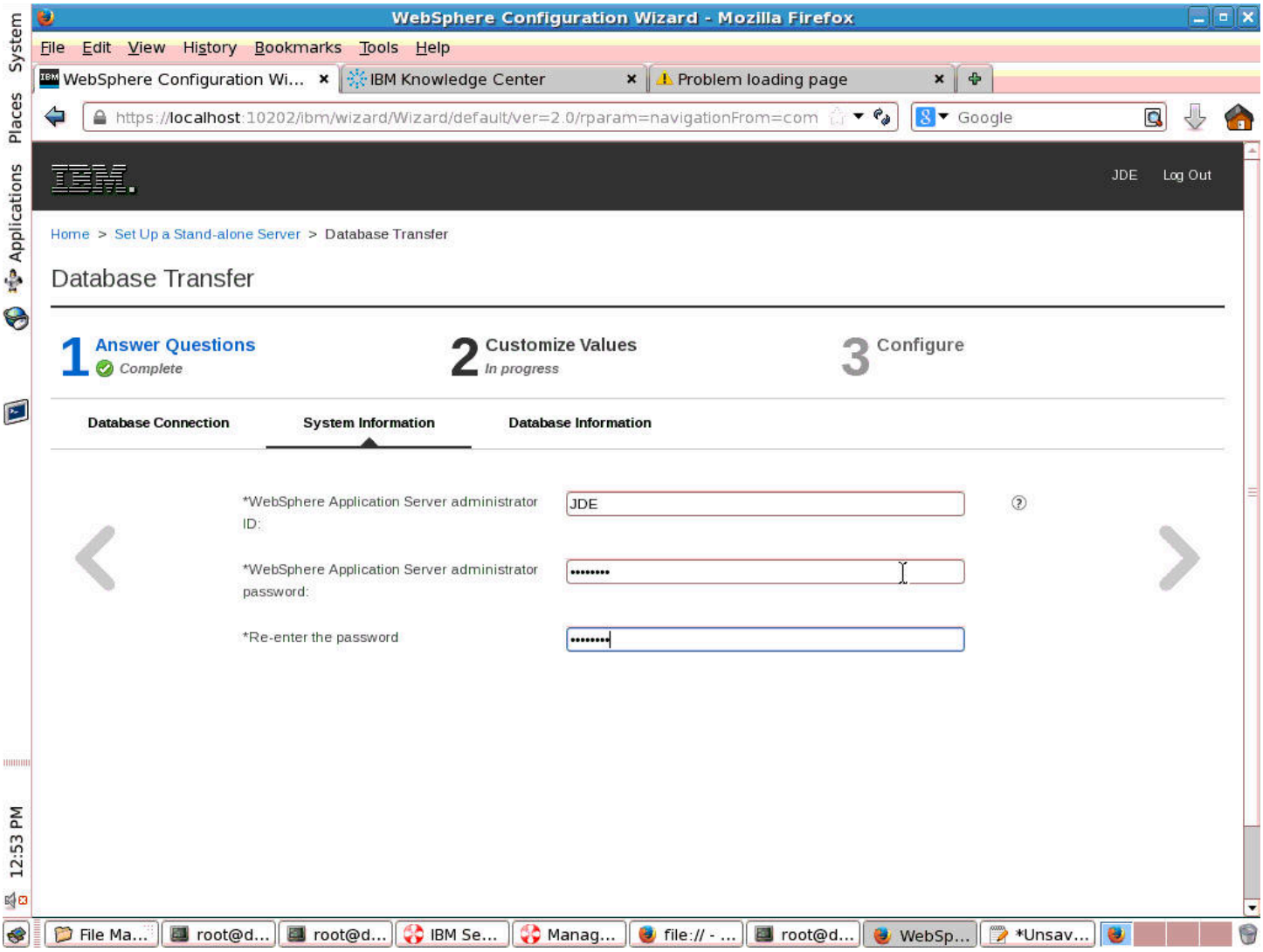
10. Scroll down for more questions.



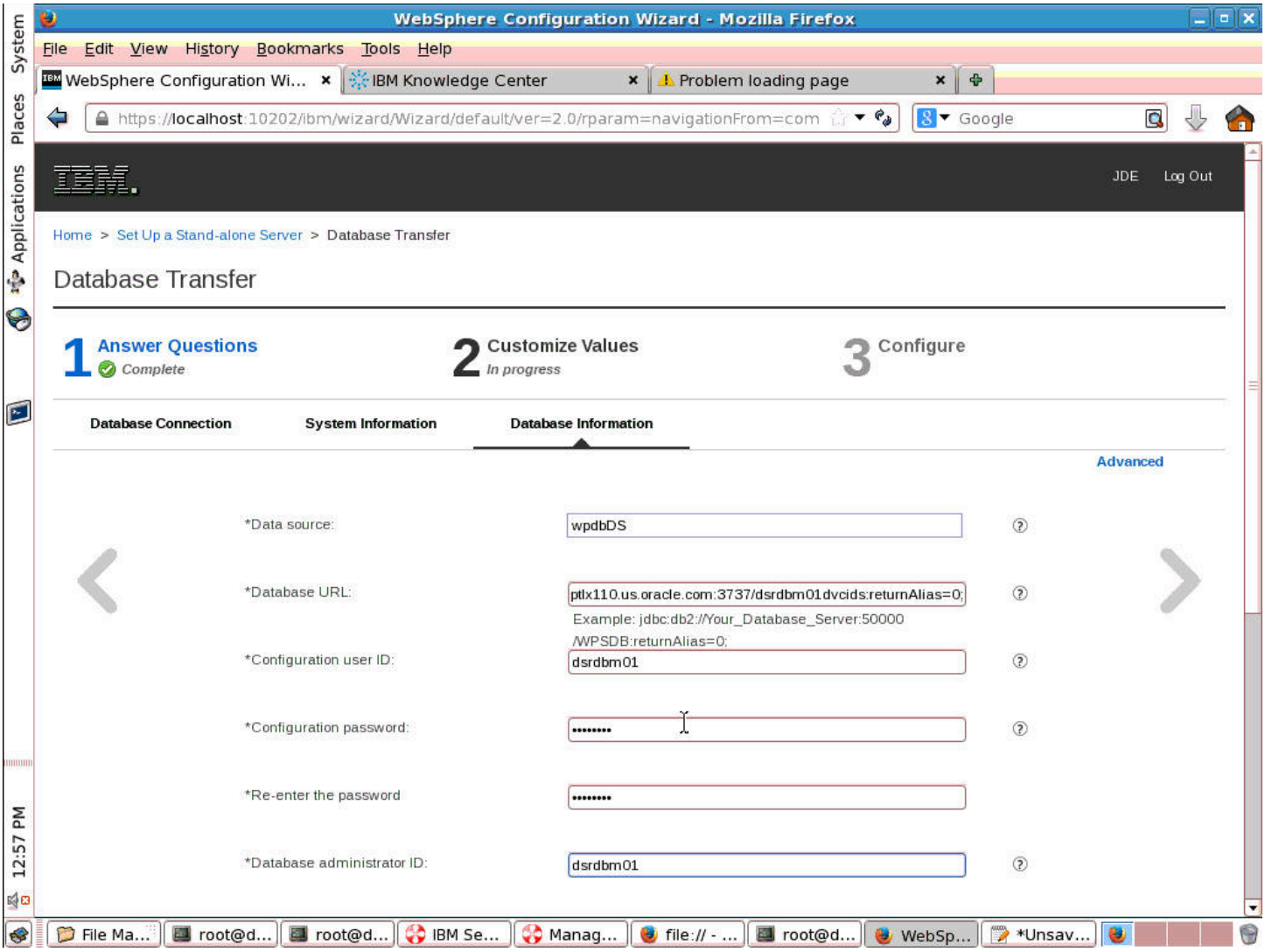
11. Click the right arrow when finished to proceed.



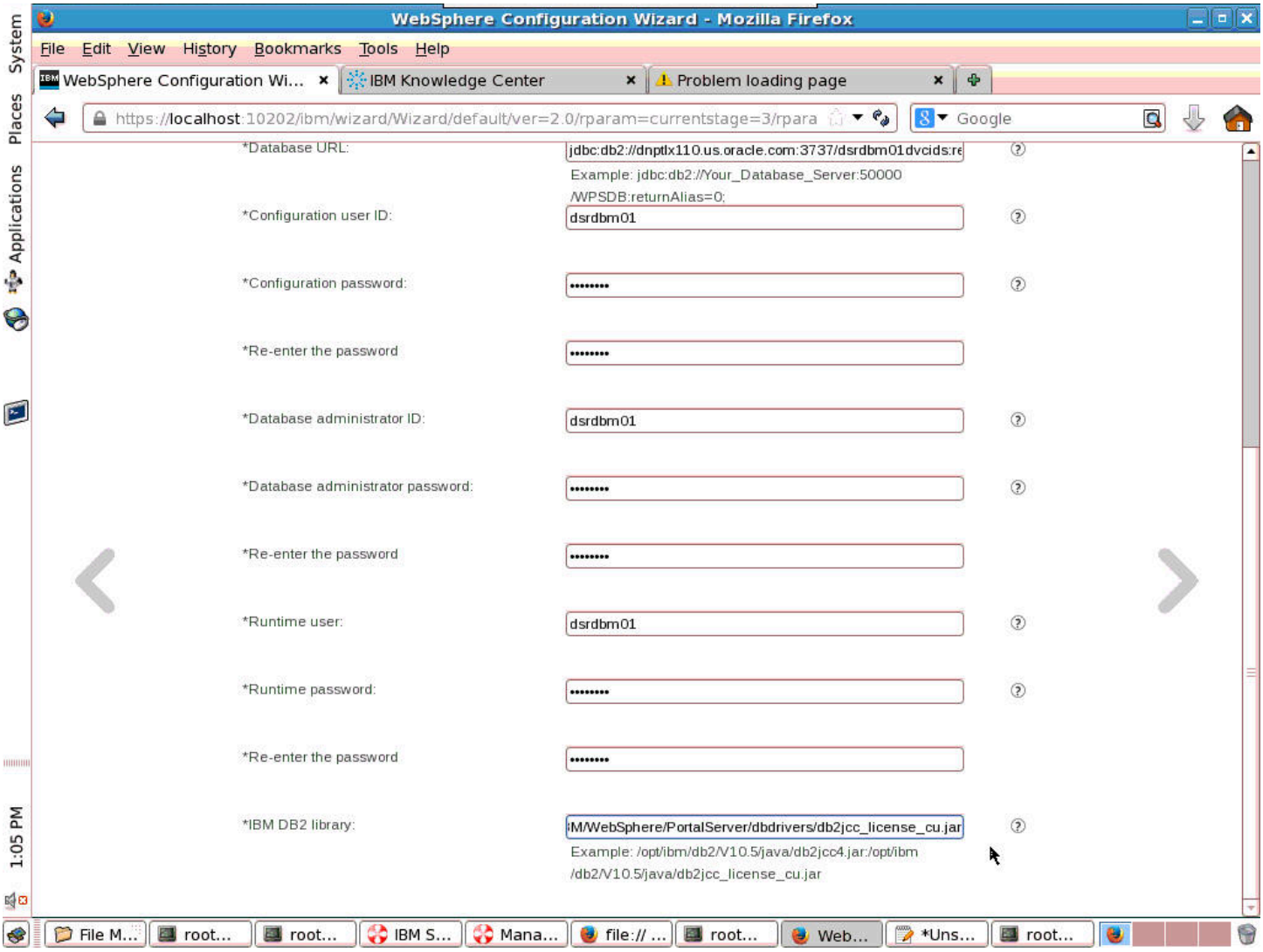
12. Enter the database connection information.



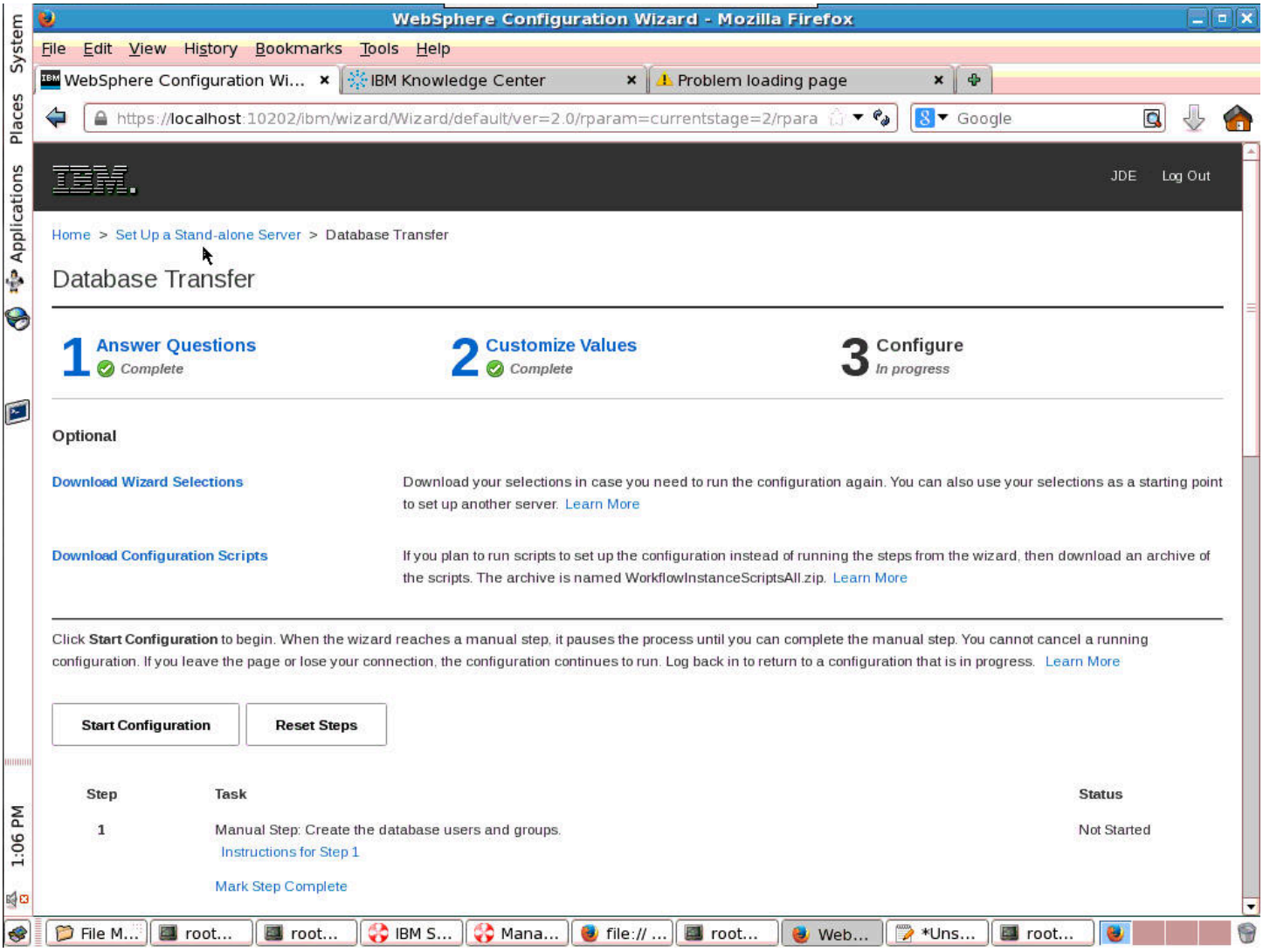
13. Enter the administrative ID and password.



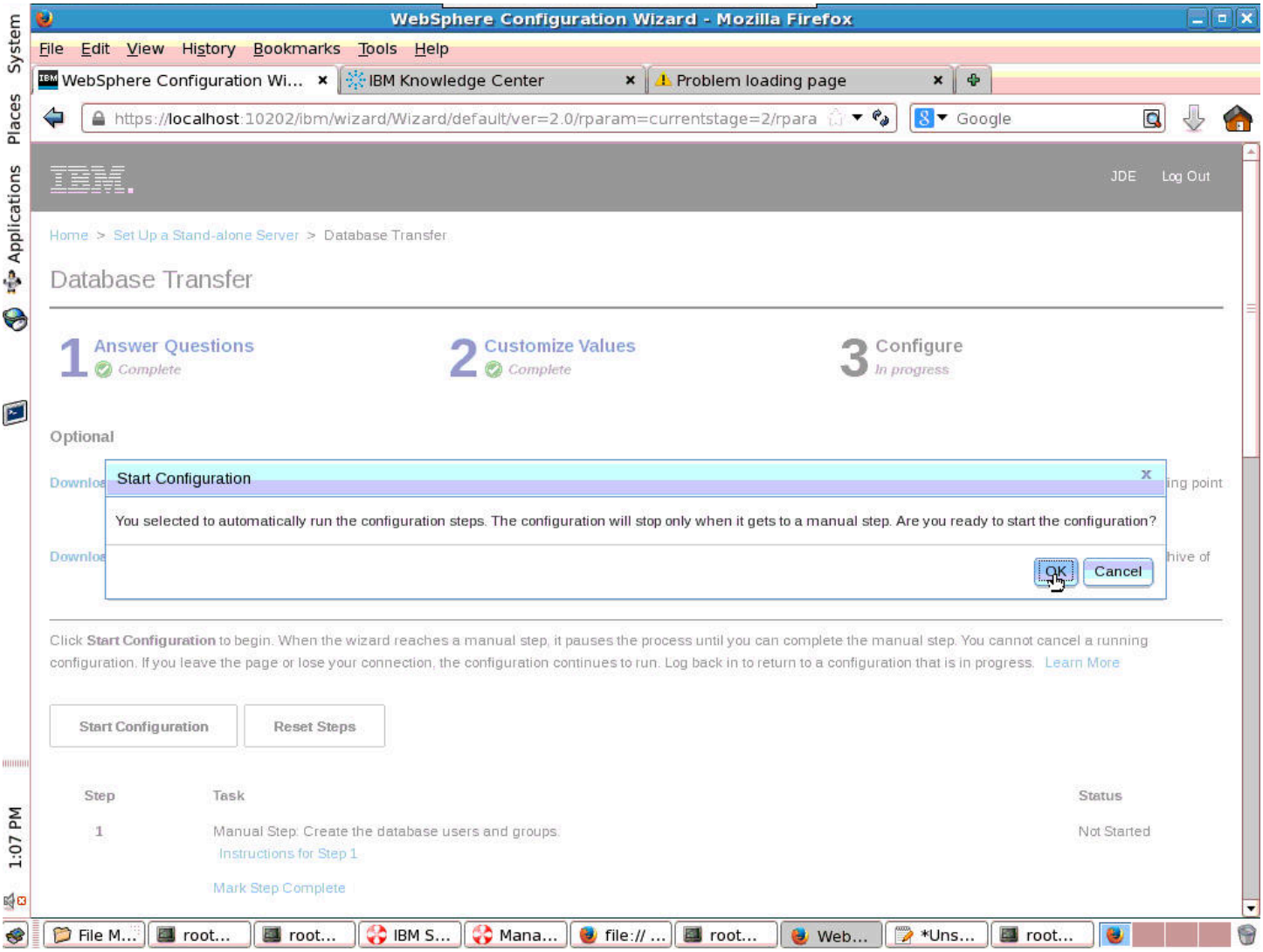
14. Enter the database connection parameters.



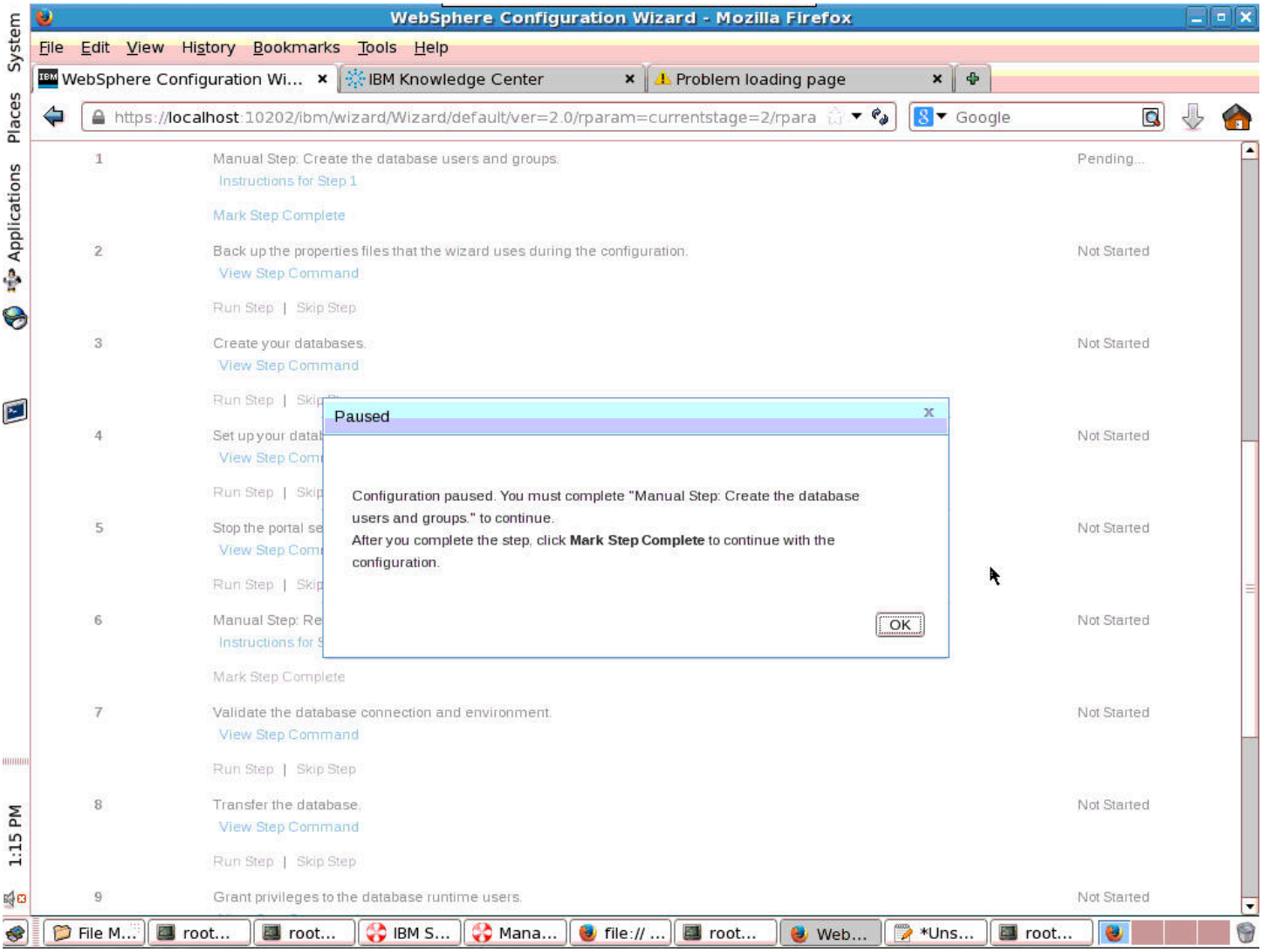
15. Scroll down for more parameters.



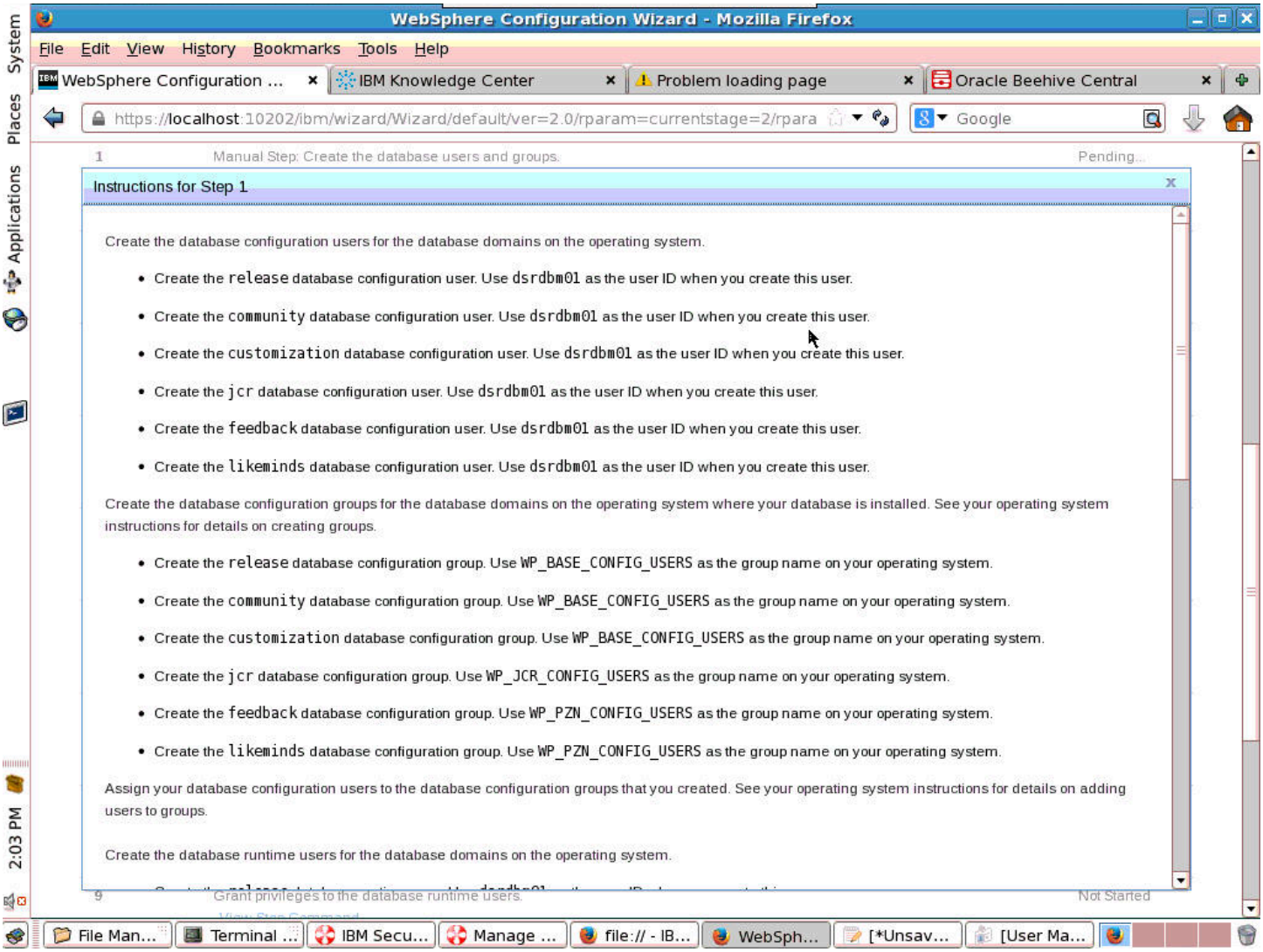
16. Configure the Database Transfer by clicking the Start Configuration button.



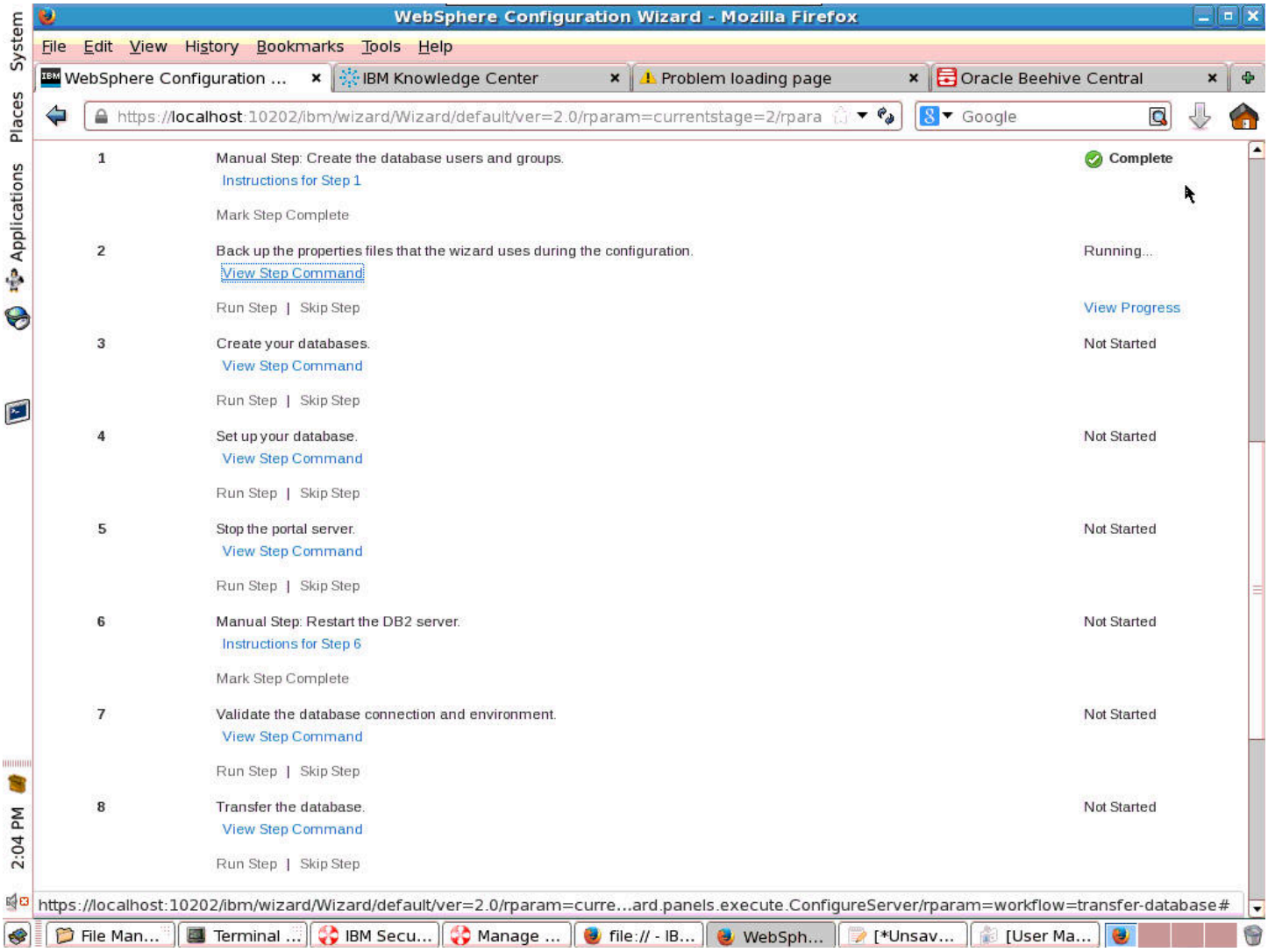
17. Click OK to confirm that you are ready to start the configuration.



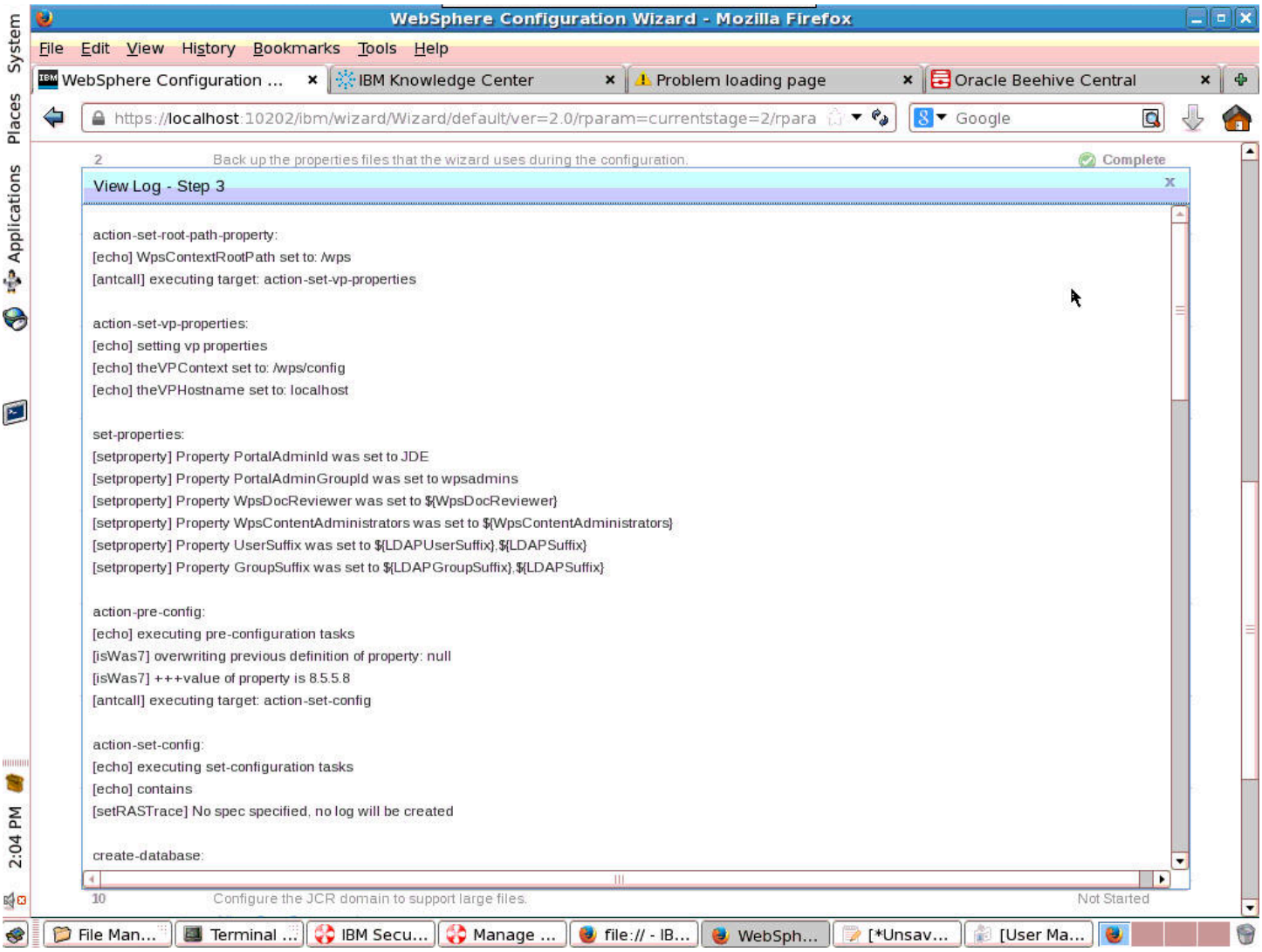
18. The configuration will pause with a notice to complete manual steps. Click OK.



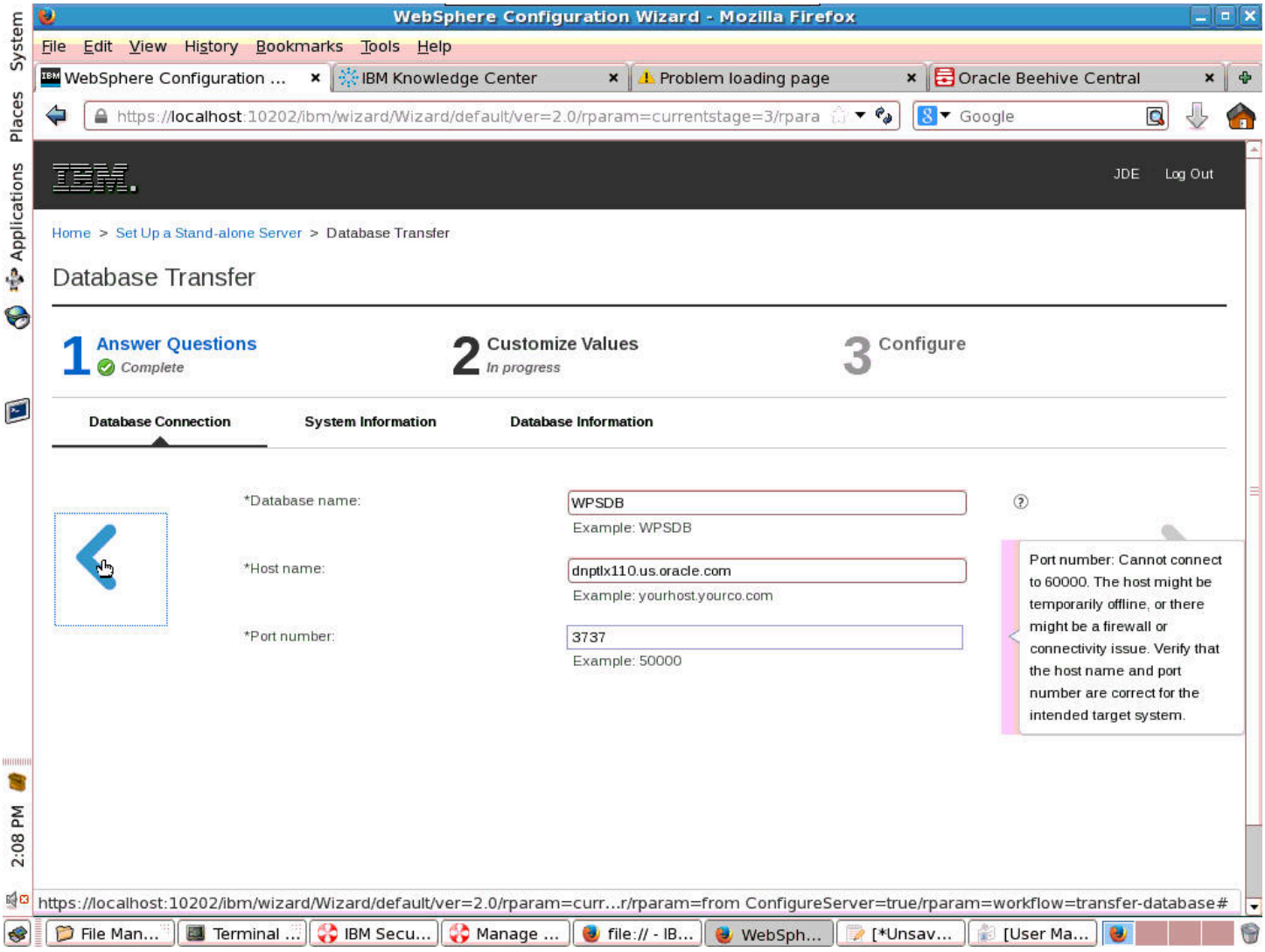
19. A list of instructions will appear for creating the database users and groups.



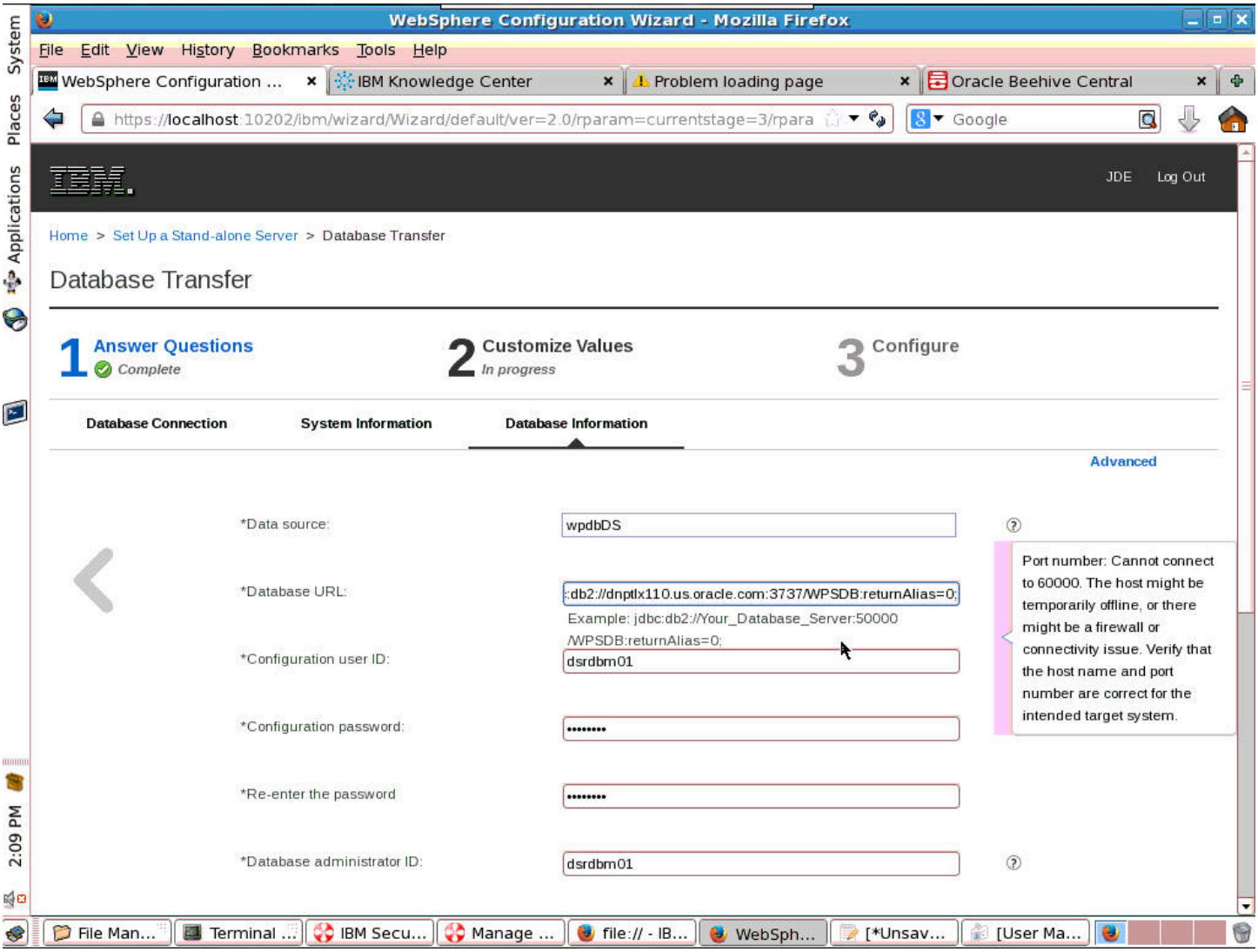
20. When the instructions have been completed the step will be marked Complete and the automated part of the configuration process start again.



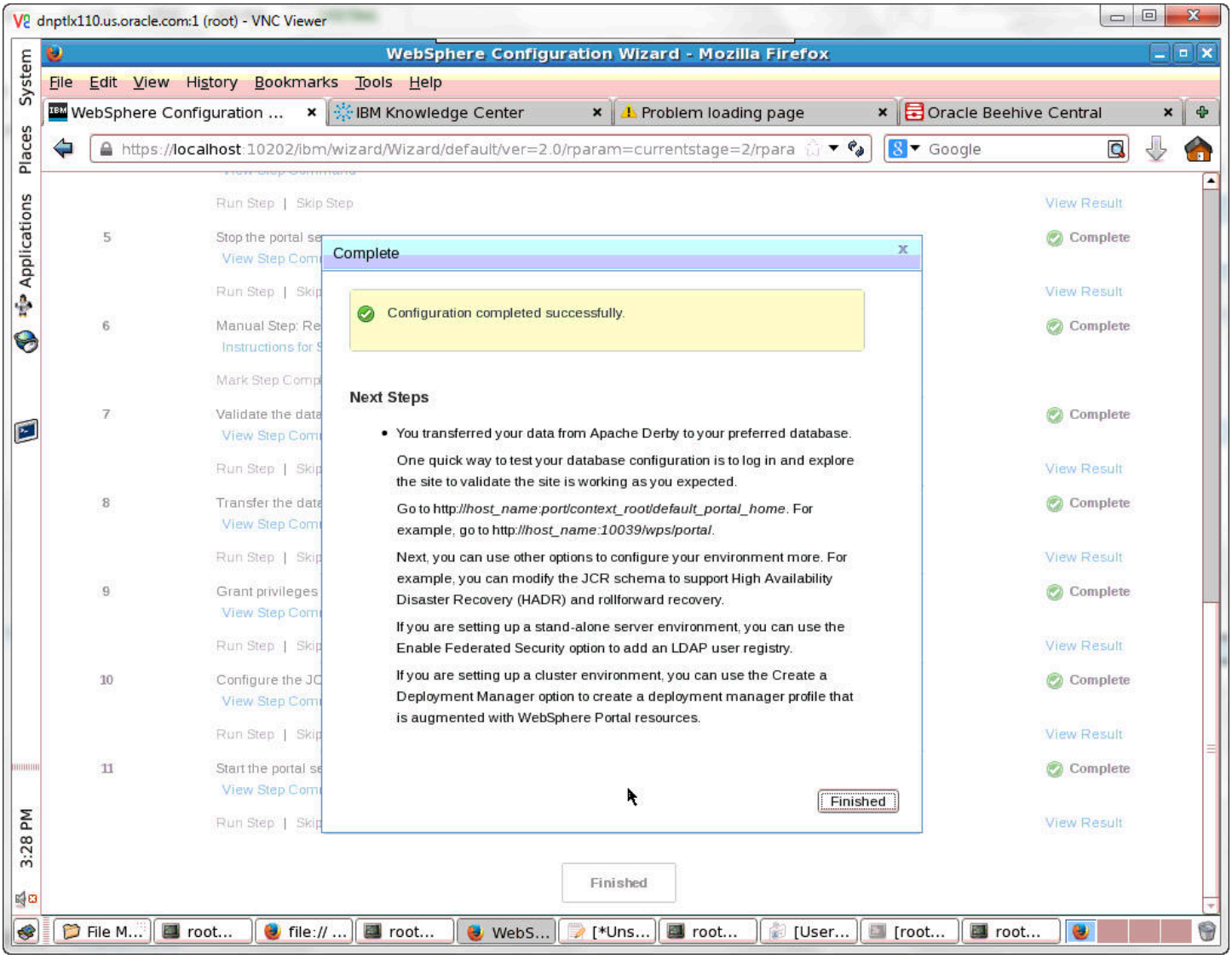
21. A View Log will appear.



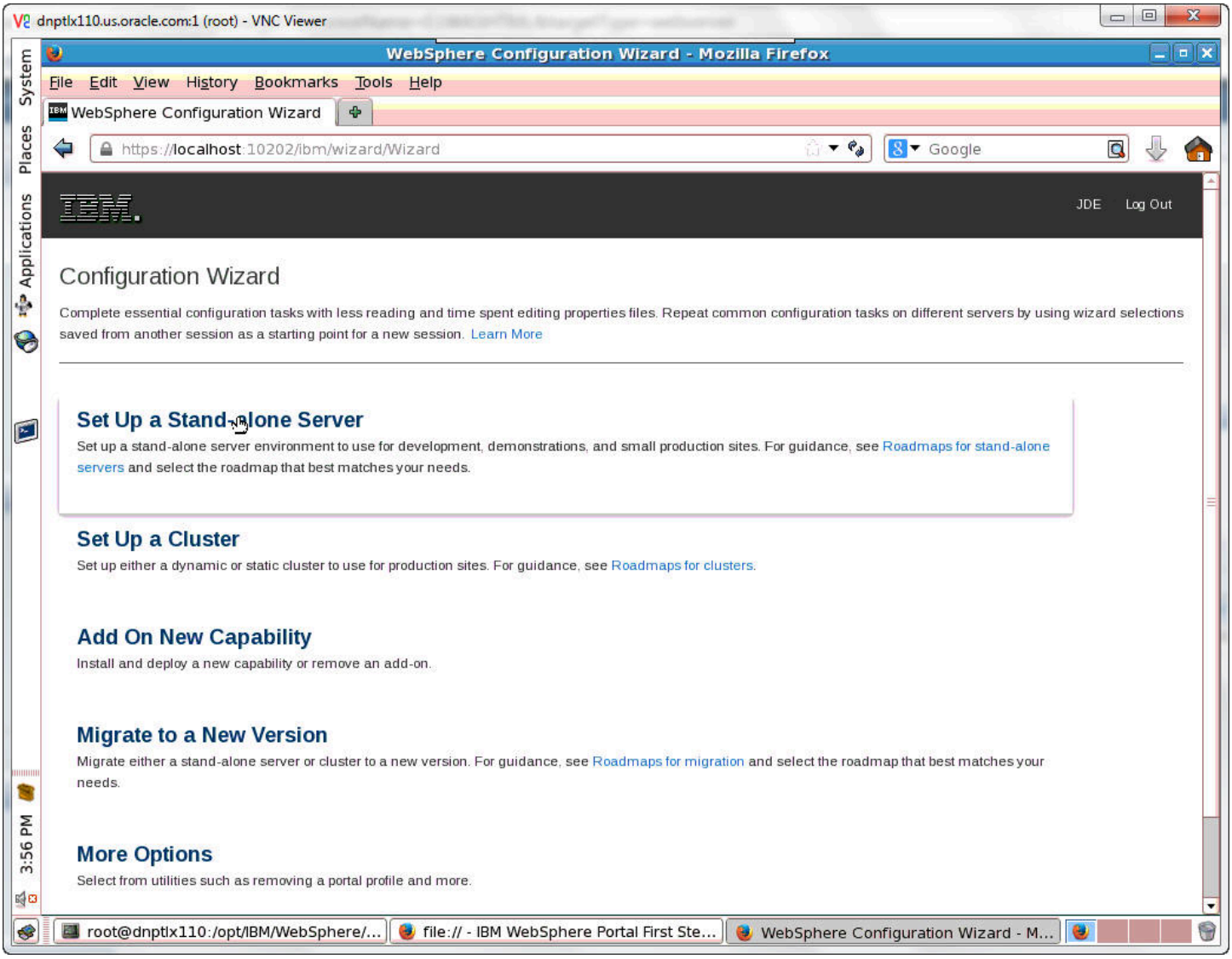
22. The Database Transfer screen will appear with any information that needs to be corrected.



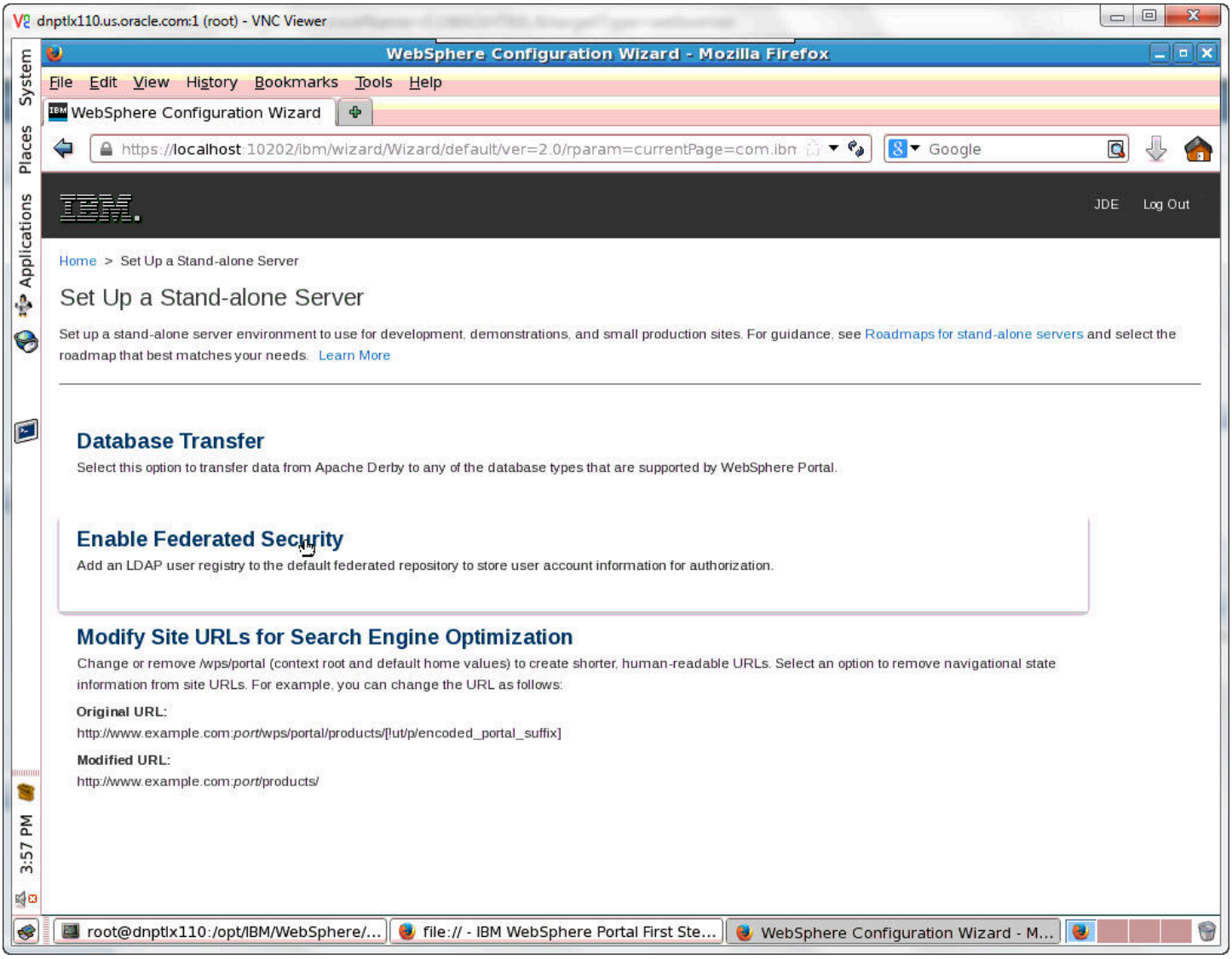
23. Correct the information to proceed.



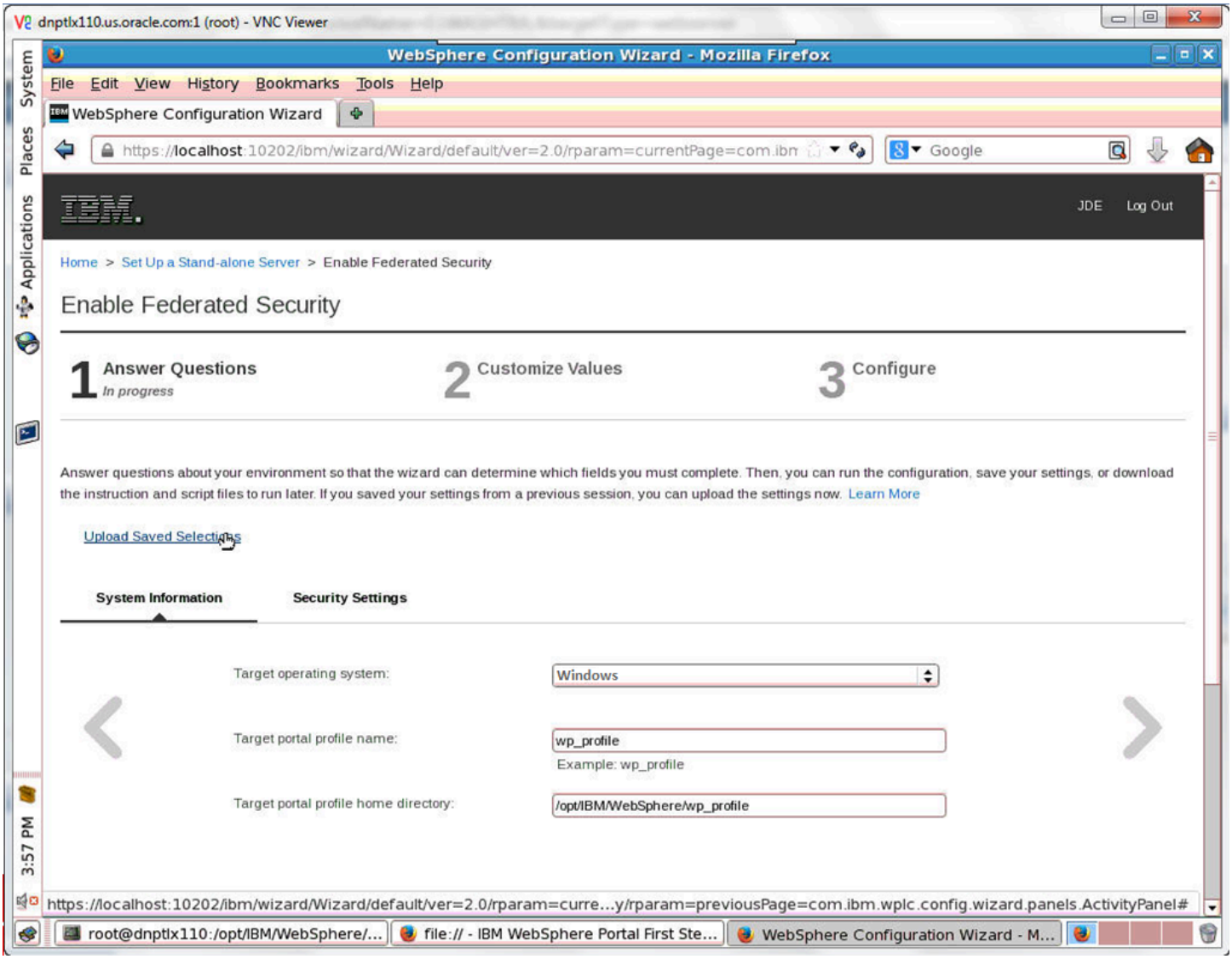
24. When the configuration has completed successfully, a confirmation screen will appear.



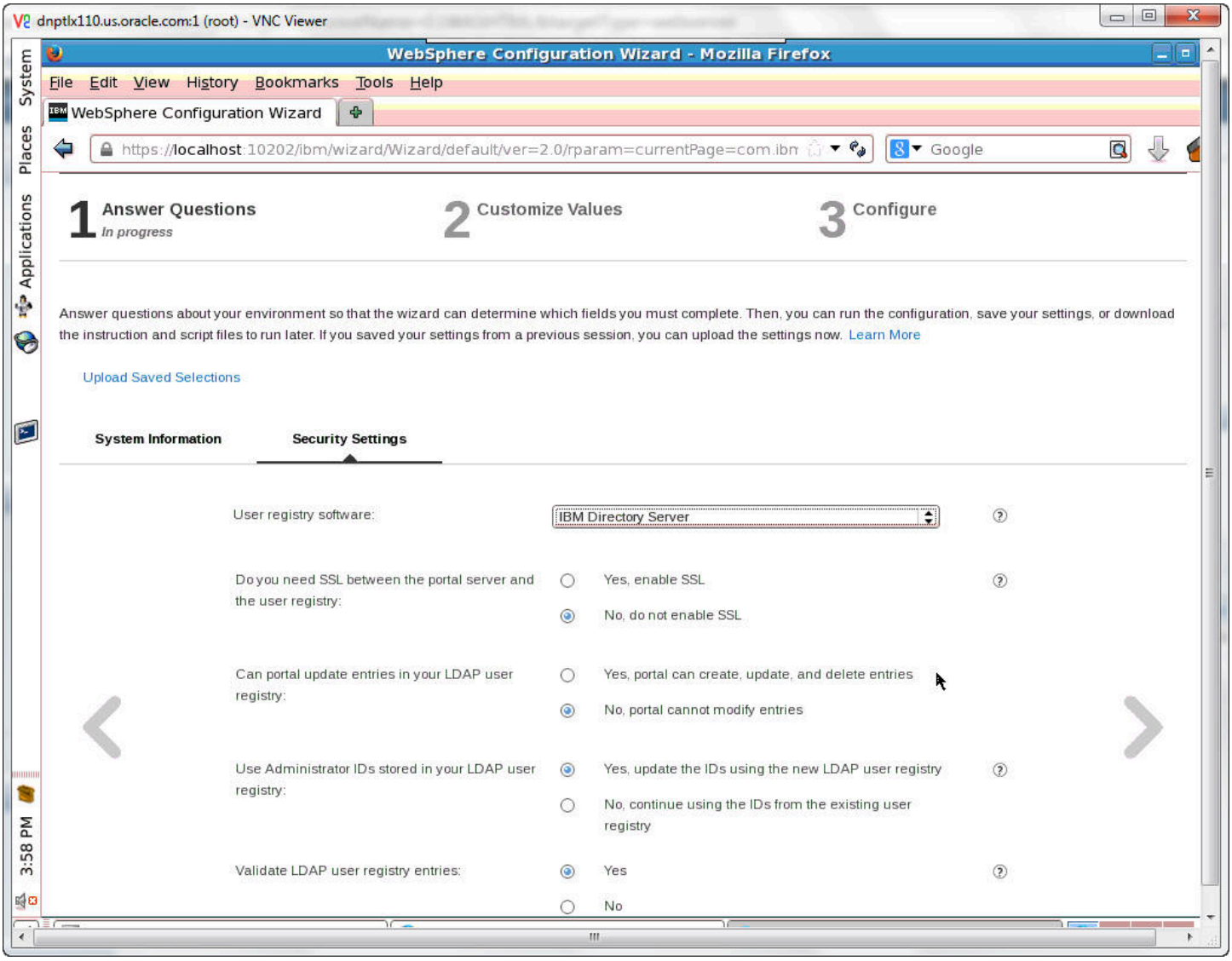
25. Select Set Up a Stand-alone Server.



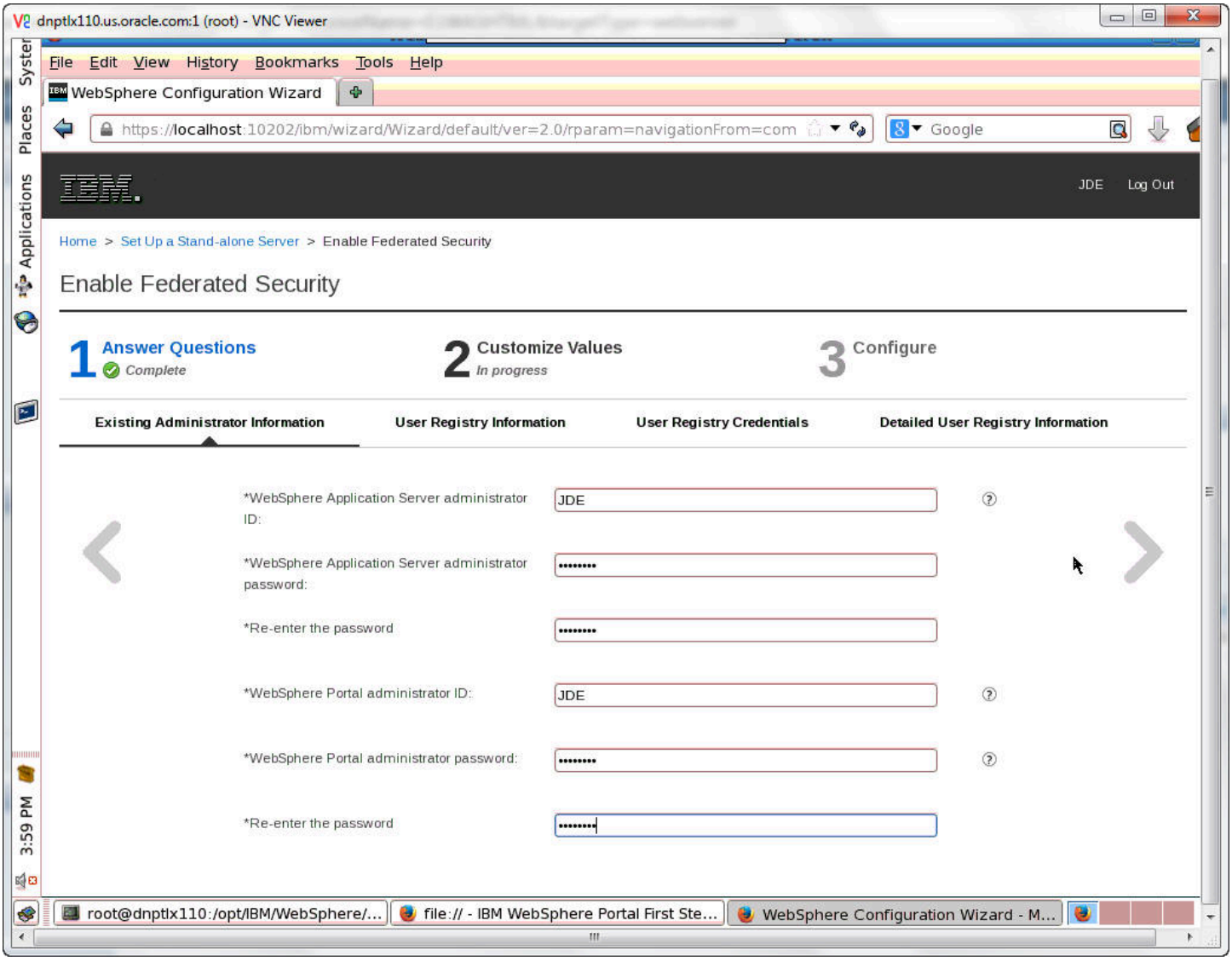
26. Select Enable Federated Security.


dnptlx110.us.oracle.com:1 (root) - VNC Viewer
WebSphere Configuration Wizard - Mozilla Firefox
File Edit View History Bookmarks Tools Help
WebSphere Configuration Wizard
https://localhost:10202/ibm/wizard/Wizard/default/ver=2.0/rparam=currentPage=com.ibm
Google
JDE Log Out
Home > Set Up a Stand-alone Server > Enable Federated Security
Enable Federated Security
1 Answer Questions
In progress
2 Customize Values
3 Configure
Answer questions about your environment so that the wizard can determine which fields you must complete. Then, you can run the configuration, save your settings, or download the instruction and script files to run later. If you saved your settings from a previous session, you can upload the settings now. Learn More
Upload Saved Selections
System Information
Security Settings
Target operating system:
Windows
Target portal profile name:
wp_profile
Example: wp_profile
Target portal profile home directory:
/opt/IBM/WebSphere/wp_profile
https://localhost:10202/ibm/wizard/Wizard/default/ver=2.0/rparam=curre...y/rparam=previousPage=com.ibm.wplc.config.wizard.panels.ActivityPanel#
root@dnptlx110:/opt/IBM/WebSphere/...
file:// - IBM WebSphere Portal First Ste...
WebSphere Configuration Wizard - M...
3:57 PM

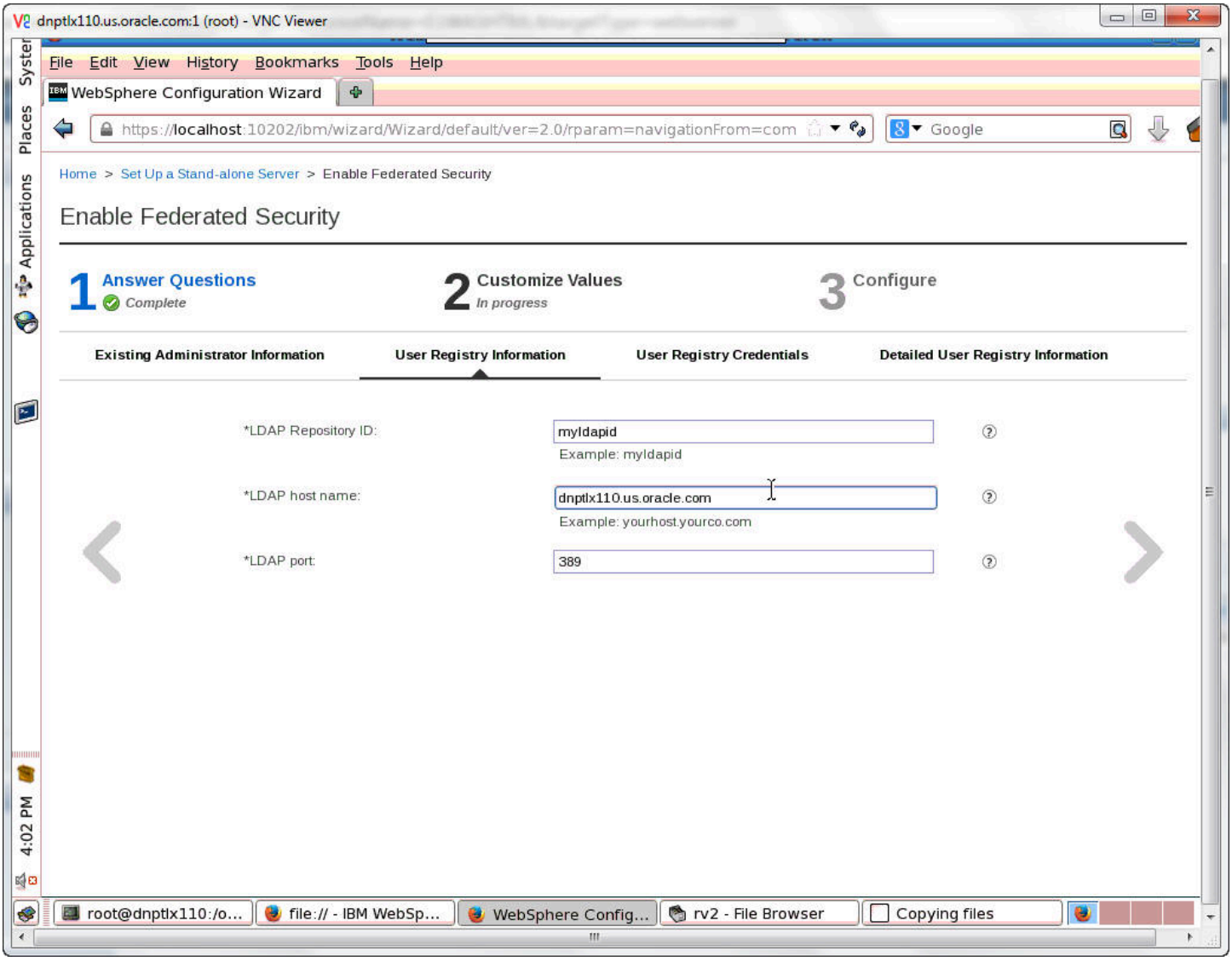
27. Click on the Upload Saved Selections hyperlink.



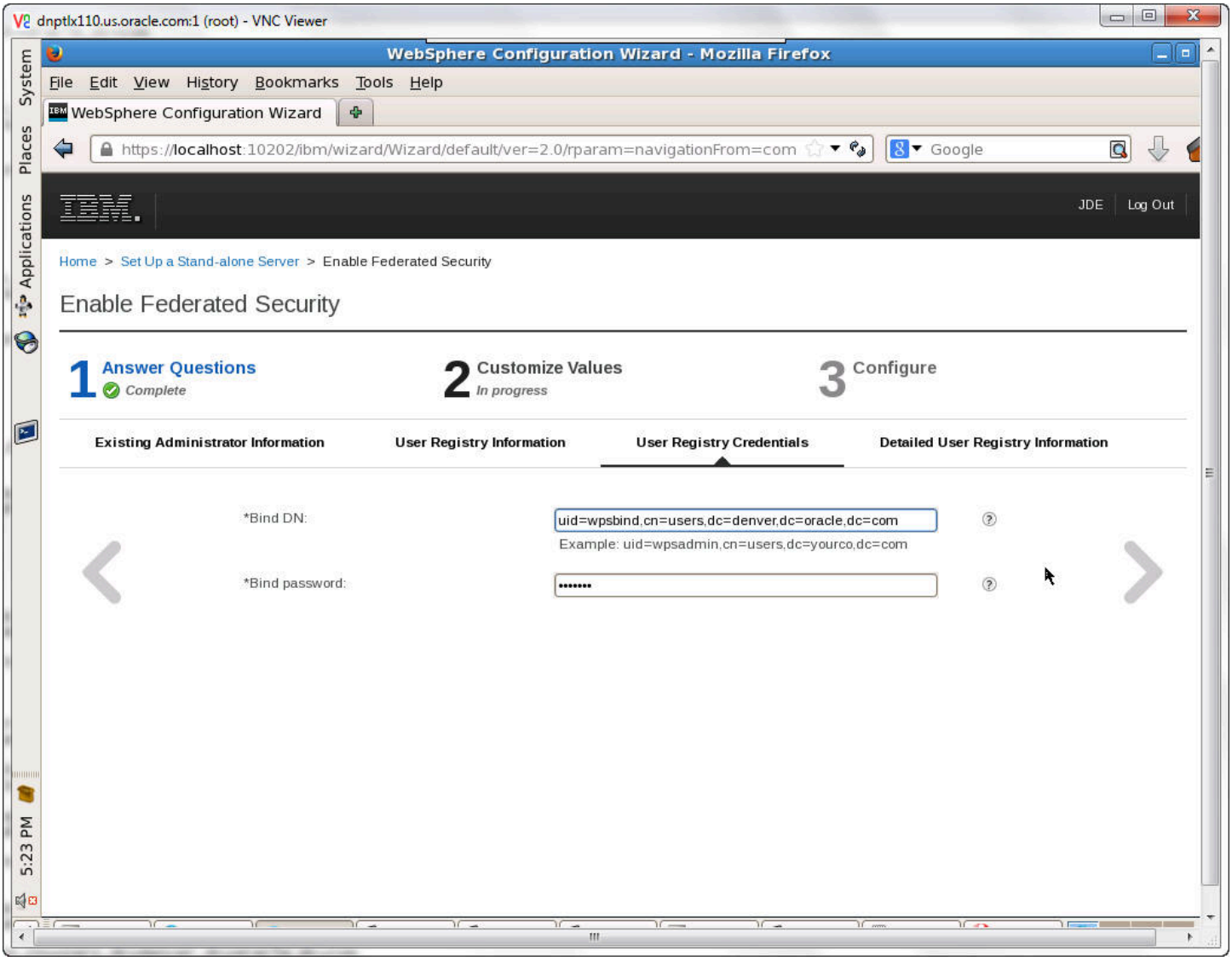
28. Answer the Security Settings questions.



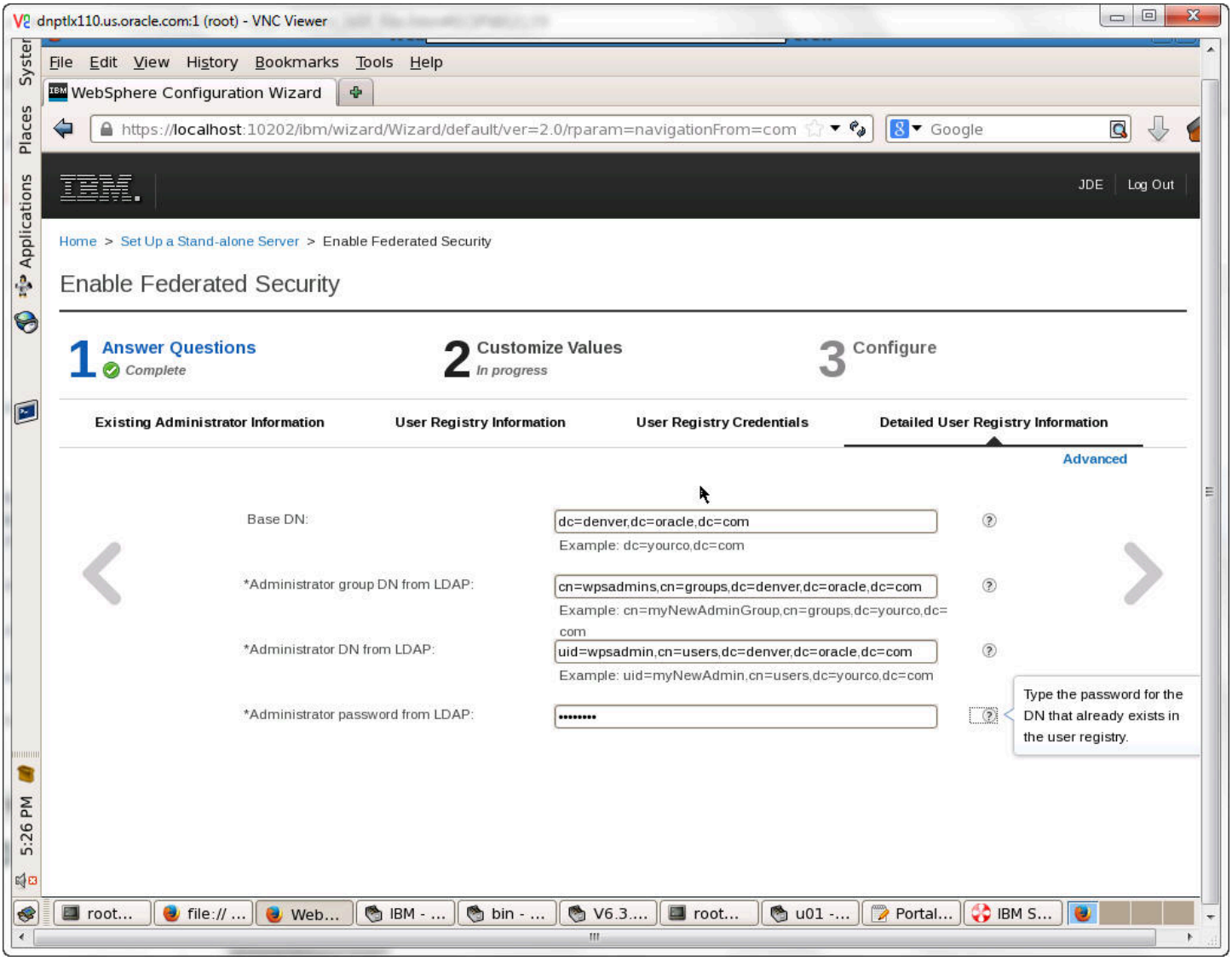
29. Enter the values for Existing Administrator Information.



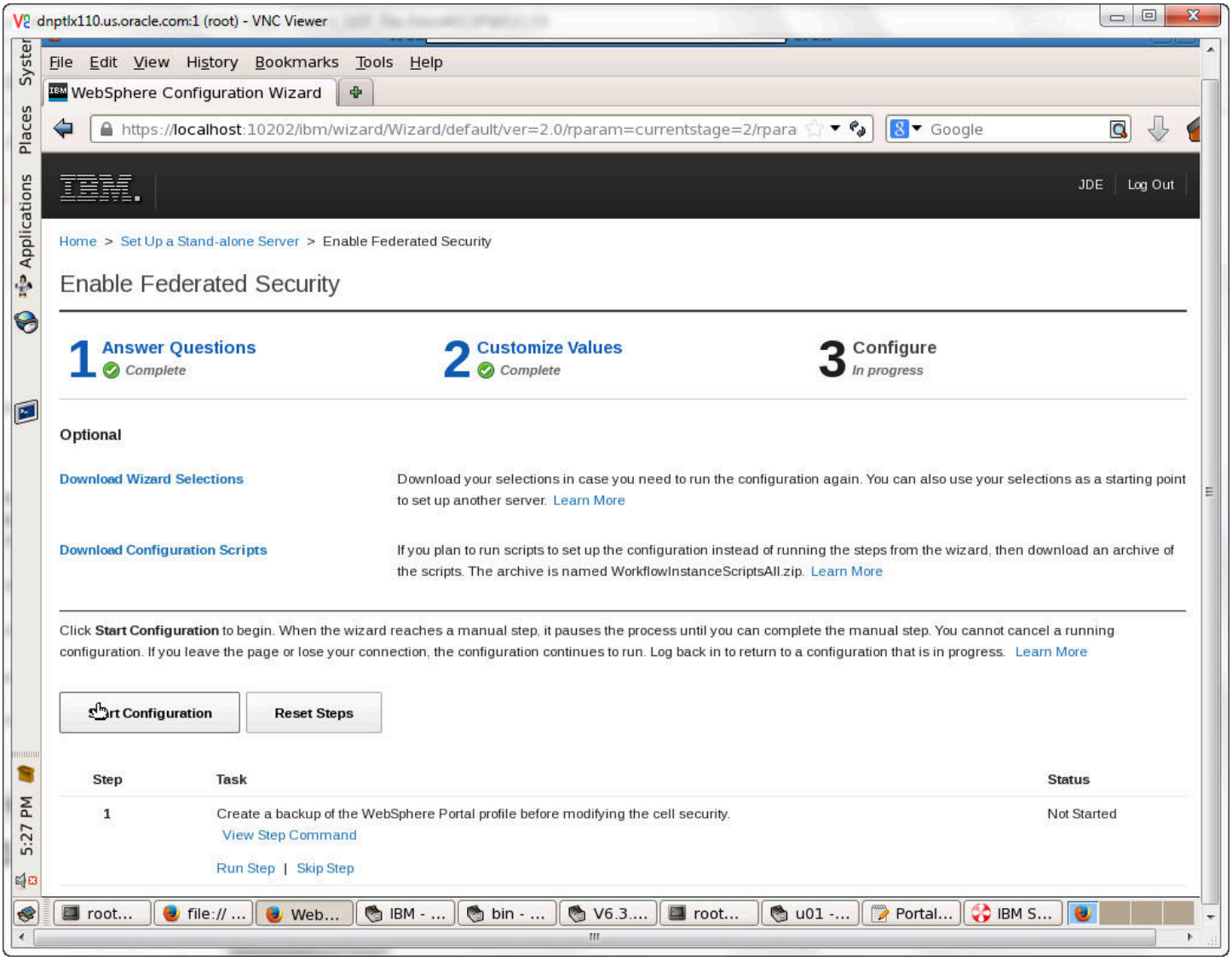
30. Enter the values for User Registry Information.



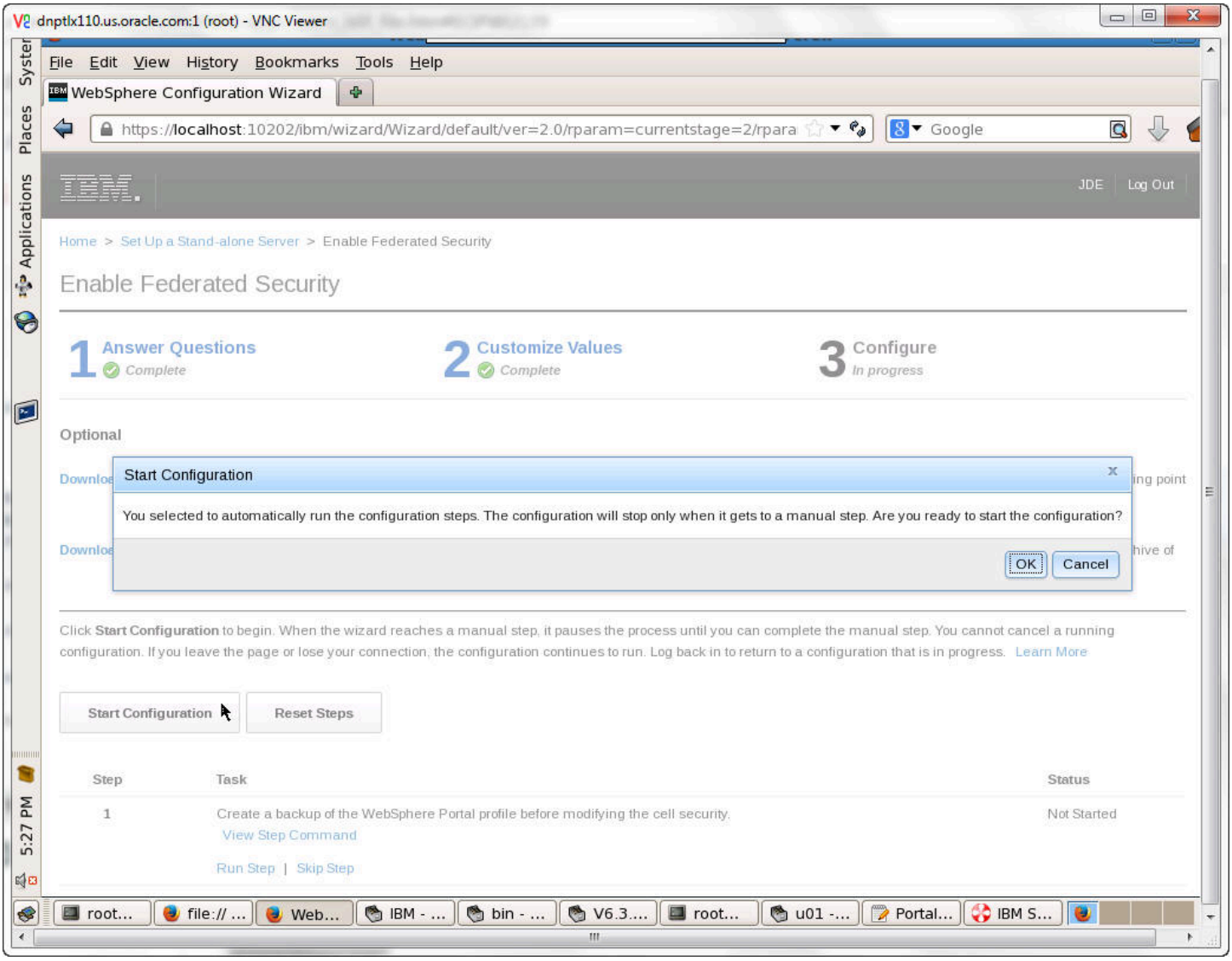
31. Enter the values for User Registry Information.



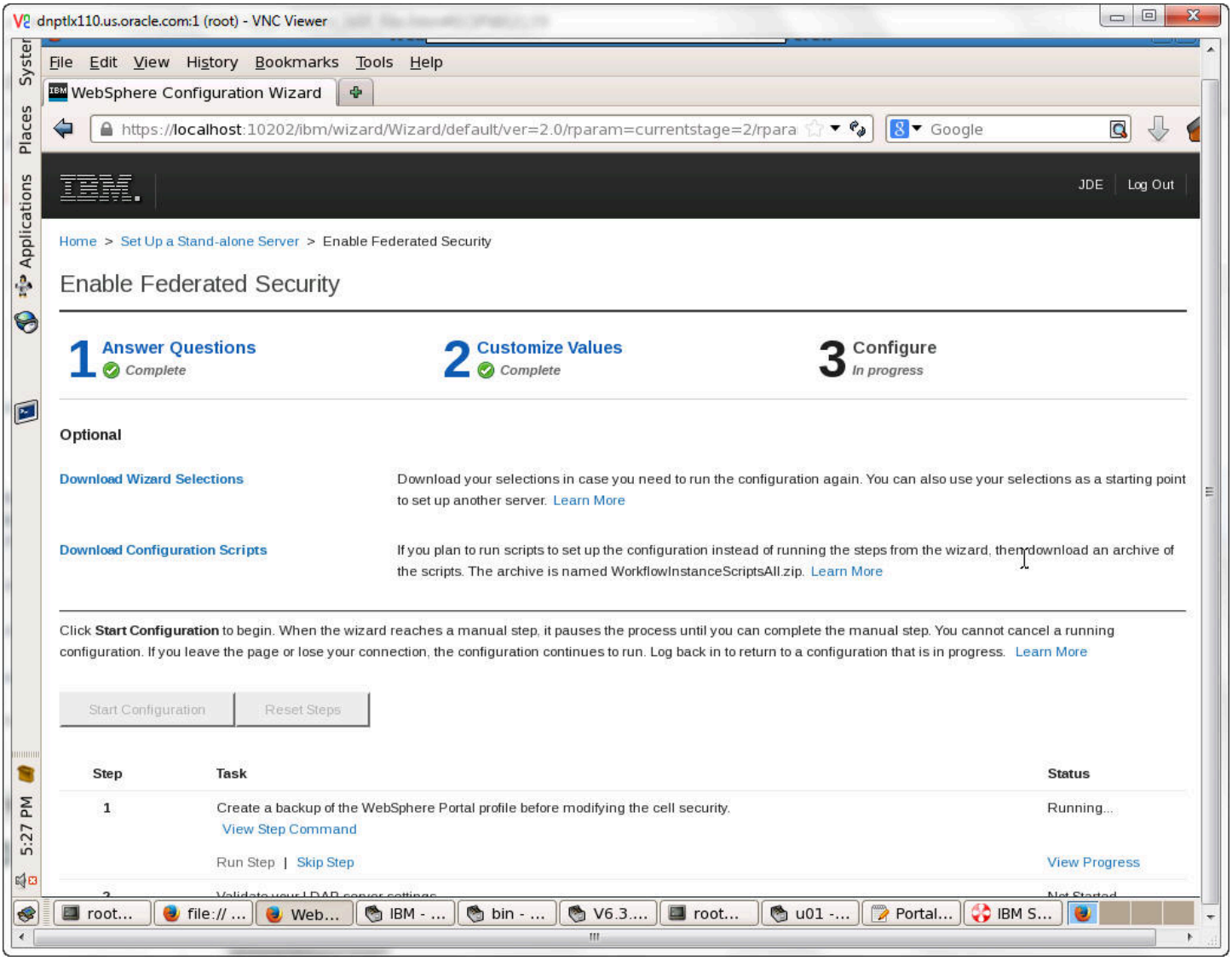
32. Enter the values for Detailed User Registry Information.



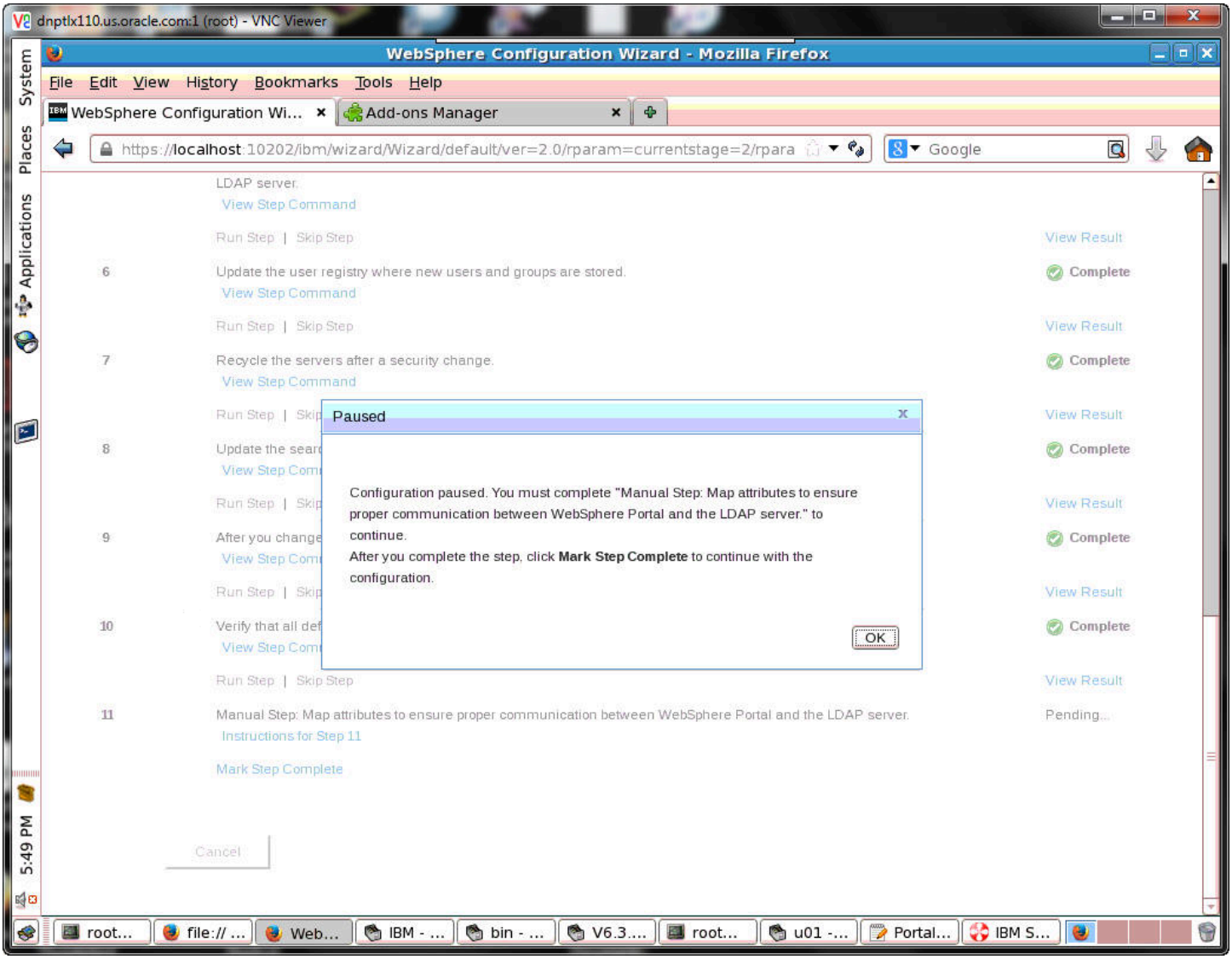
33. Click on the Start Configuration button.



34. Click OK to confirm that you are ready to start the configuration.



35. The configuration steps and status will appear at the bottom of the screen.



36. The configuration will pause with a notice to complete manual steps. Click OK.

    Once the manual steps are completed and all steps have been marked complete, you will receive a screen a final screen indicating that the installation has finished.

4 Database Configuration for WebSphere Portal

Database Configuration for WebSphere Portal

This chapter discusses the database configuration for the Websphere portal.

By default, IBM WebSphere Portal v8.5 installs and uses an Apache Derby database. Installing with Apache Derby lets you quickly get WebSphere Portal installed and running in a proof-of-concept environment. Before using the product extensively, you should visit the IBM Information Center for Portal v8.5 to learn the advantages and disadvantages of using Apache Derby and determine how transferring to another database affects the capacity and scalability of a production environment. Please refer to the following link from IBM: ***https://www-304.ibm.com/support/docview.wss?uid=swg27019558#Databases_C-worksWith***

The Apache Derby database that is installed by default is not intended for use in a production environment or for authoring Web content. Derby does not support clustered environments, enabling security in a database-only mode, or vertical cloned environments in which multiple application servers are configured on a single server. Use one of the other supported databases in a production environment or when authoring Web content because they are better able to handle large amounts of data and can be tuned for performance.

When you choose to transfer data to another supported database such as Oracle or SQL Server or *DB2 for Linux, UNIX, and Windows database* or *DB2 for i* , perform the database transfer before you use the portal extensively. Large amounts of data in the databases can cause the database transfer to fail if your Java heap size is not large enough. Because information is added to the databases as you use the Portal, perform the database transfer as soon as it is practical to avoid problems in a production environment.

Data can be transferred from a Derby database, but cannot be transferred to a Derby database. If you are transferring from a database other than the default database, you will need to edit the wkplc.properties, wkplc_dbdomain.properties and wkplc_dbtype.properties files to update the source and target database information.

You can install the database server on the same system as WebSphere Portal, or you can install the database server on a different, also referred to as a remote system.

Using a remote database can have performance benefits. When you are deploying a large scale environment, you can dedicate a server specifically to your database. As more users are accessing the portal, the portal application becomes database intensive. Database activity can take up CPU utilization and disk I/O time. You can increase capacity by separating the database from the server that the Portal is running on increases capacity.

If you install the database server on a remote system, you may be required to install database client software on the WebSphere Portal system so the Portal can communicate with the remote database server.

Documentation in this section is taken directly from the IBM WebSphere Portal v8.5 Infocenter.

5 Configuring IBM WebSphere Portal Server v8.5 to use Oracle Database

Configuring IBM WebSphere Portal Server v8.5 to use Oracle Database

This chapter discusses configuring the IBM Websphere Portal Server v8.5 to use the Oracle database.

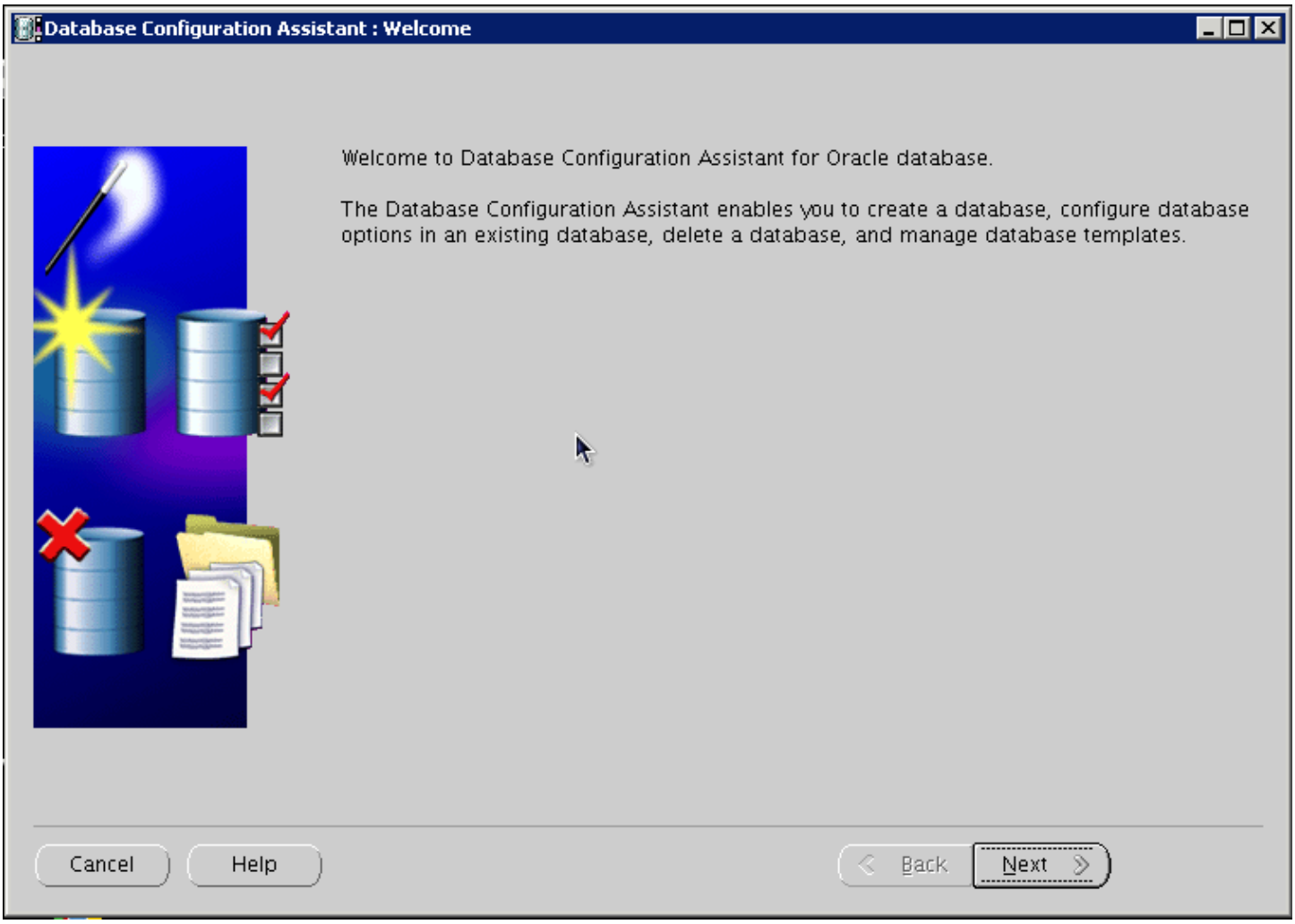
Before You Begin

Before beginning the database configuration, verify that a supported version of Oracle Database software is installed. Refer to the Minimum Technical Requirements for this information. In addition, we strongly recommend you visit the IBM WebSphere Portal Version v8.5 Information Center and review the “Configuring WebSphere Portal to use a database" section: ***http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Windows_standalone_Configuring_WebSphere_Portal_to_use_a_database_wp7***.

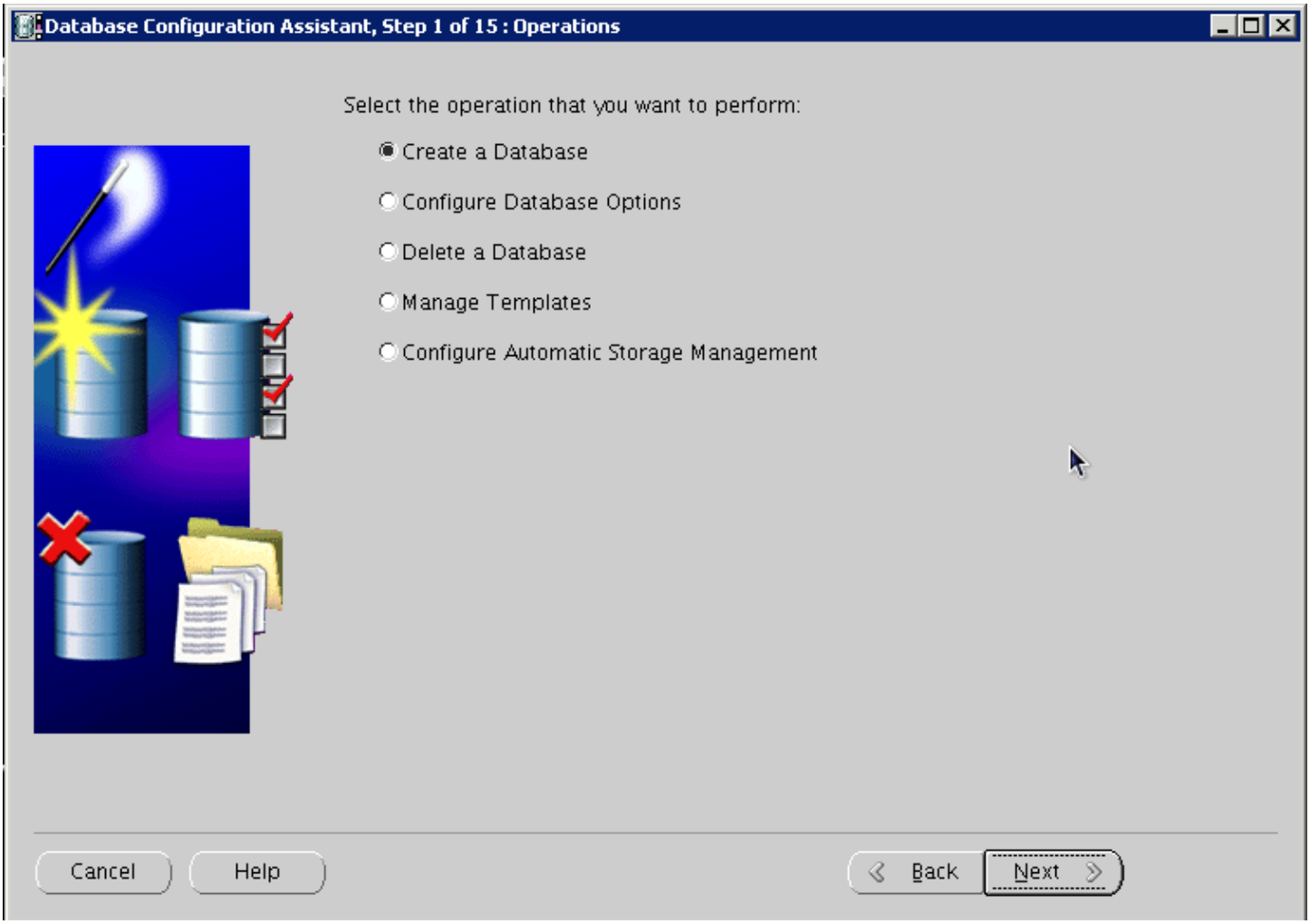
For advanced configurations, refer to the IBM WebSphere Portal Version v8.5 Information Center.

Creating the Oracle Database for IBM WebSphere Portal Server v8.5

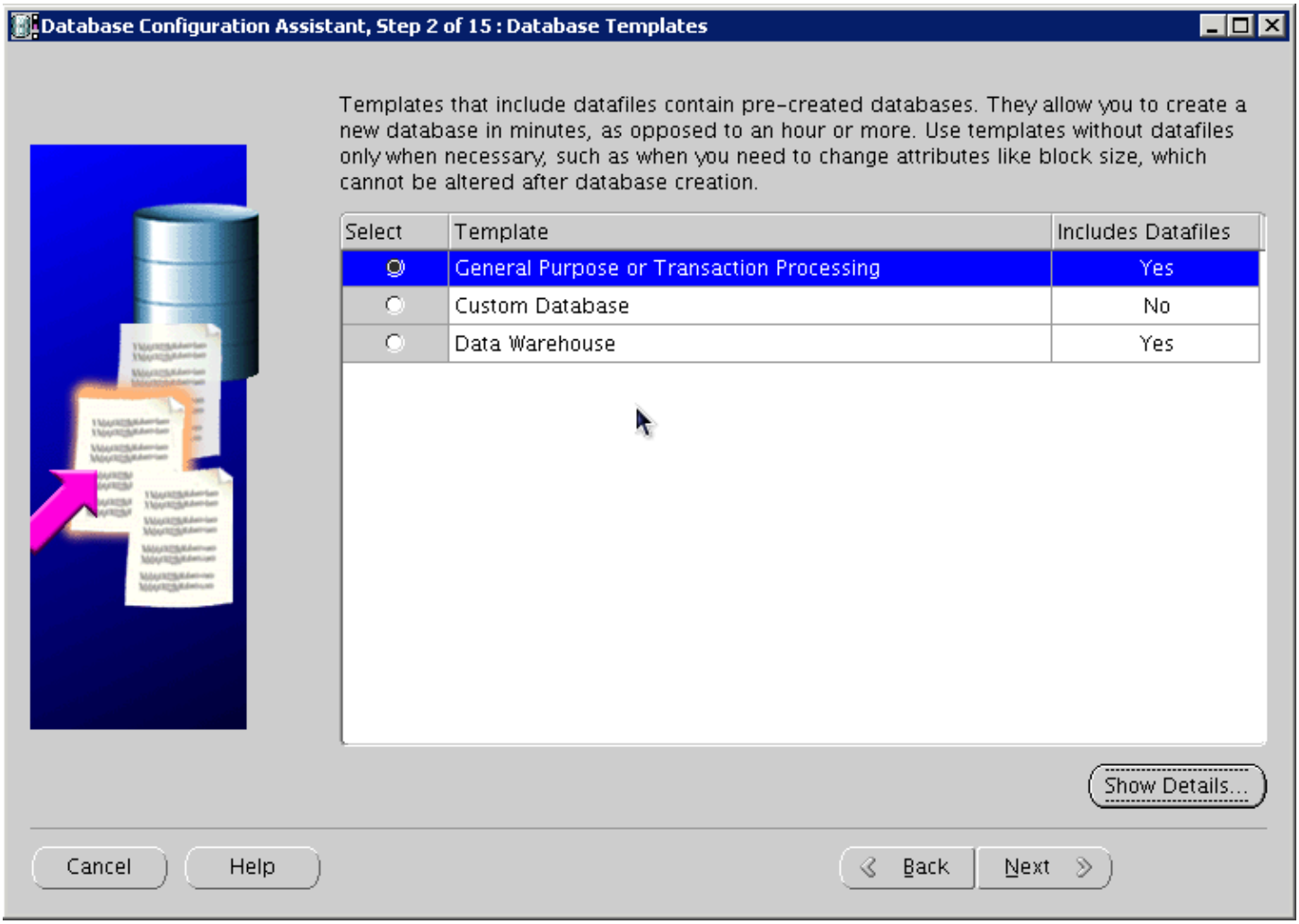
1. Launch Database Configuration Assistant (dbca), click Next:



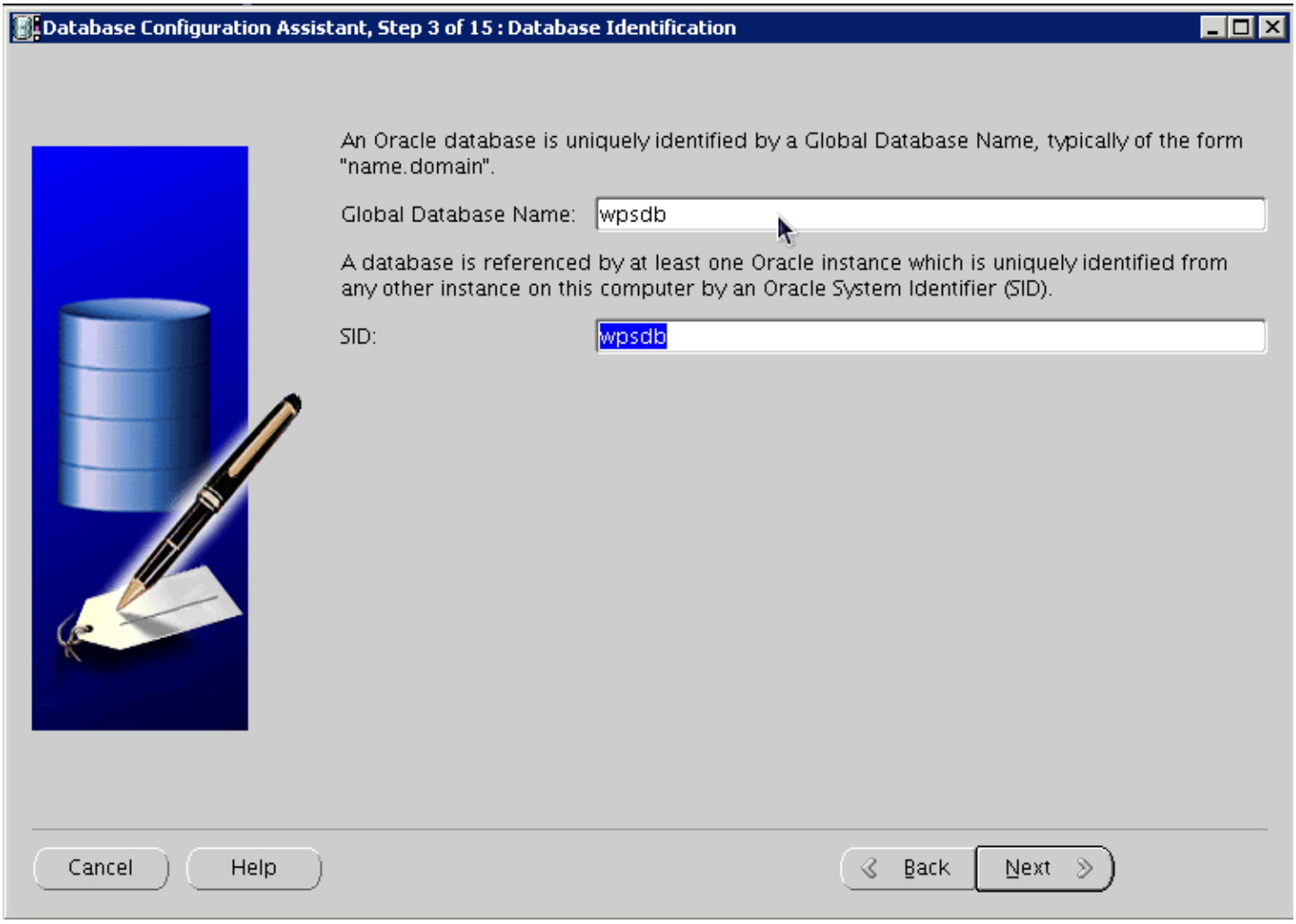
2. Select create database, click next:



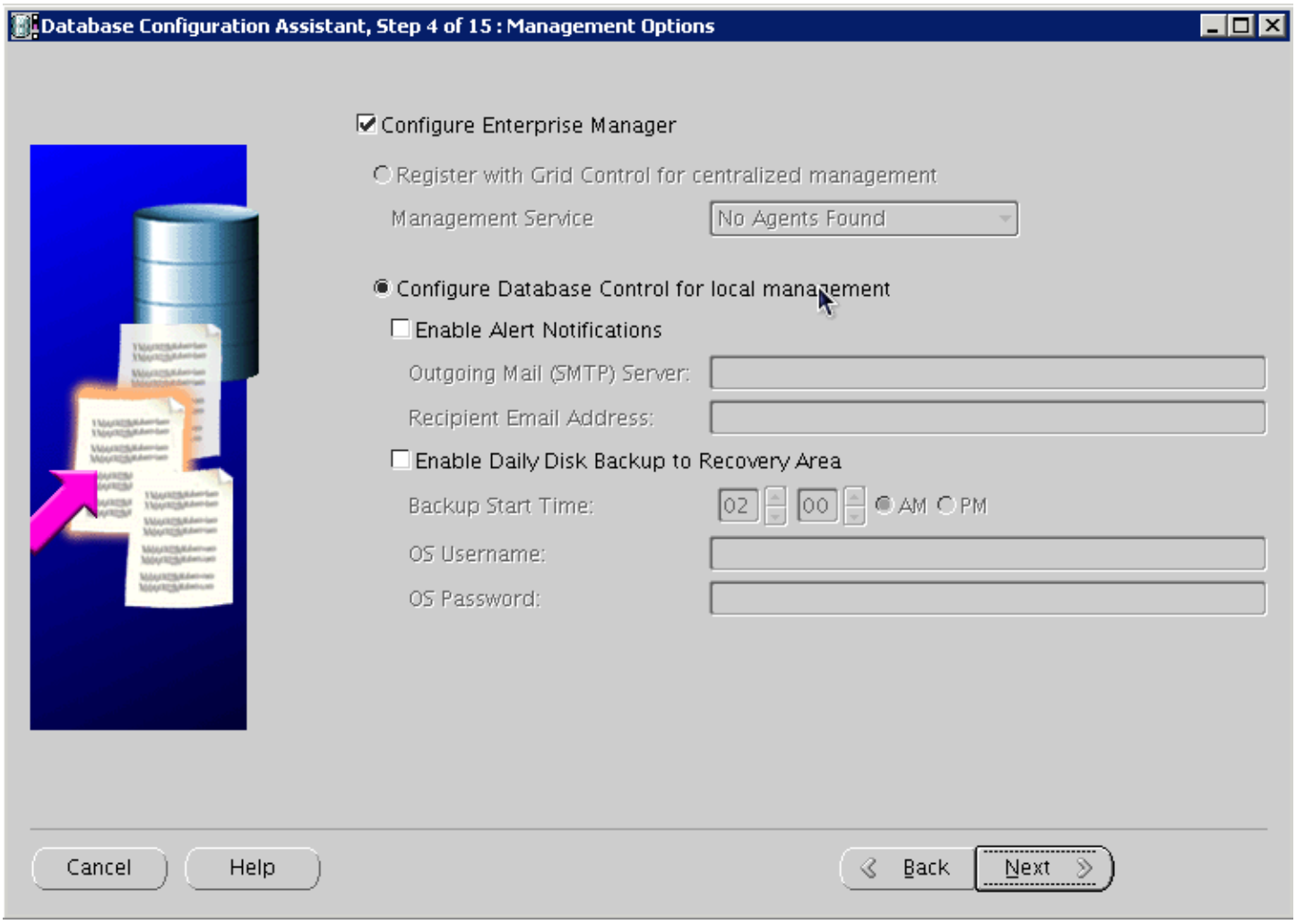
3. Select General Purpose or Transaction Processing, click next:



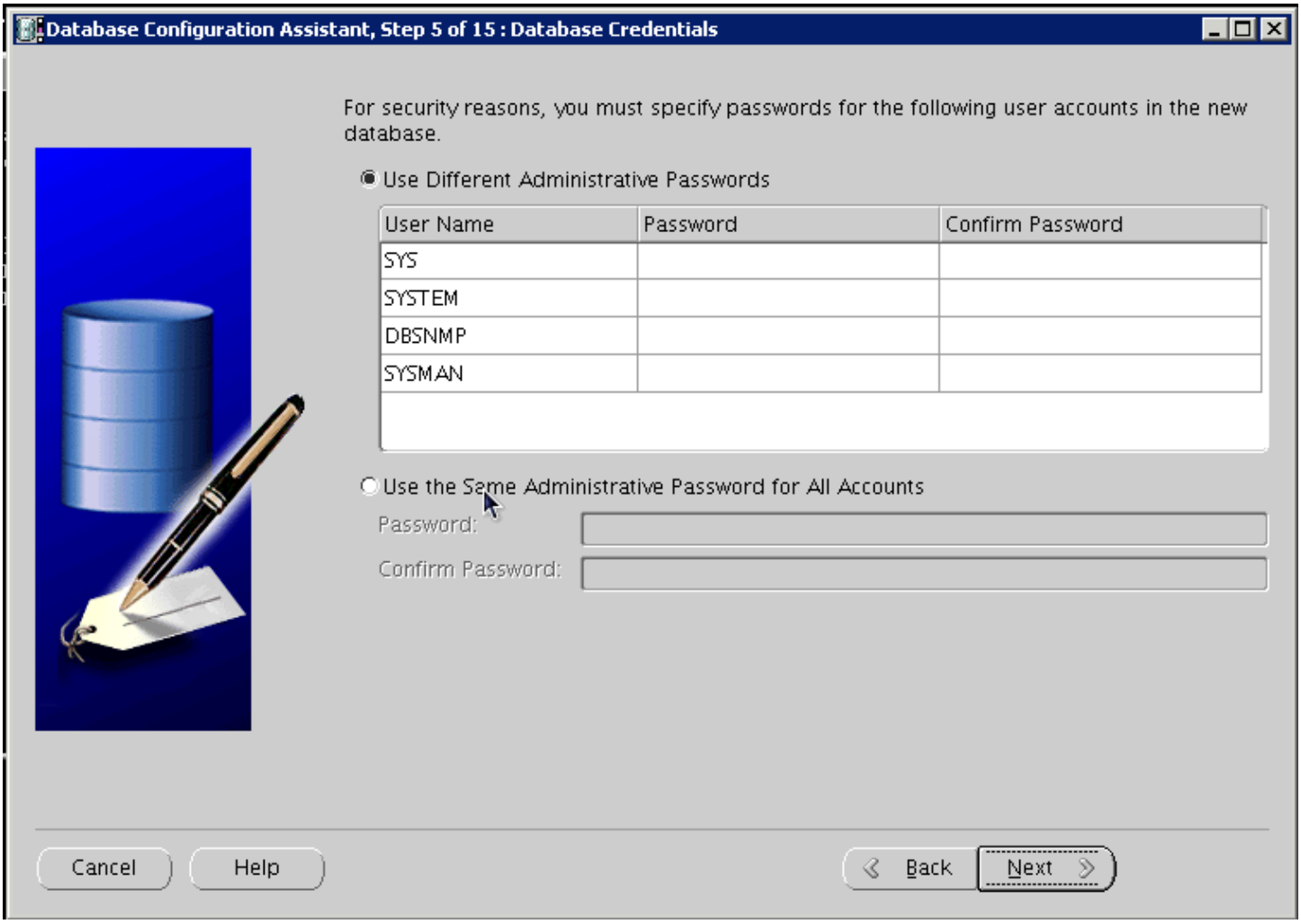
4. Provide the SID, click next:



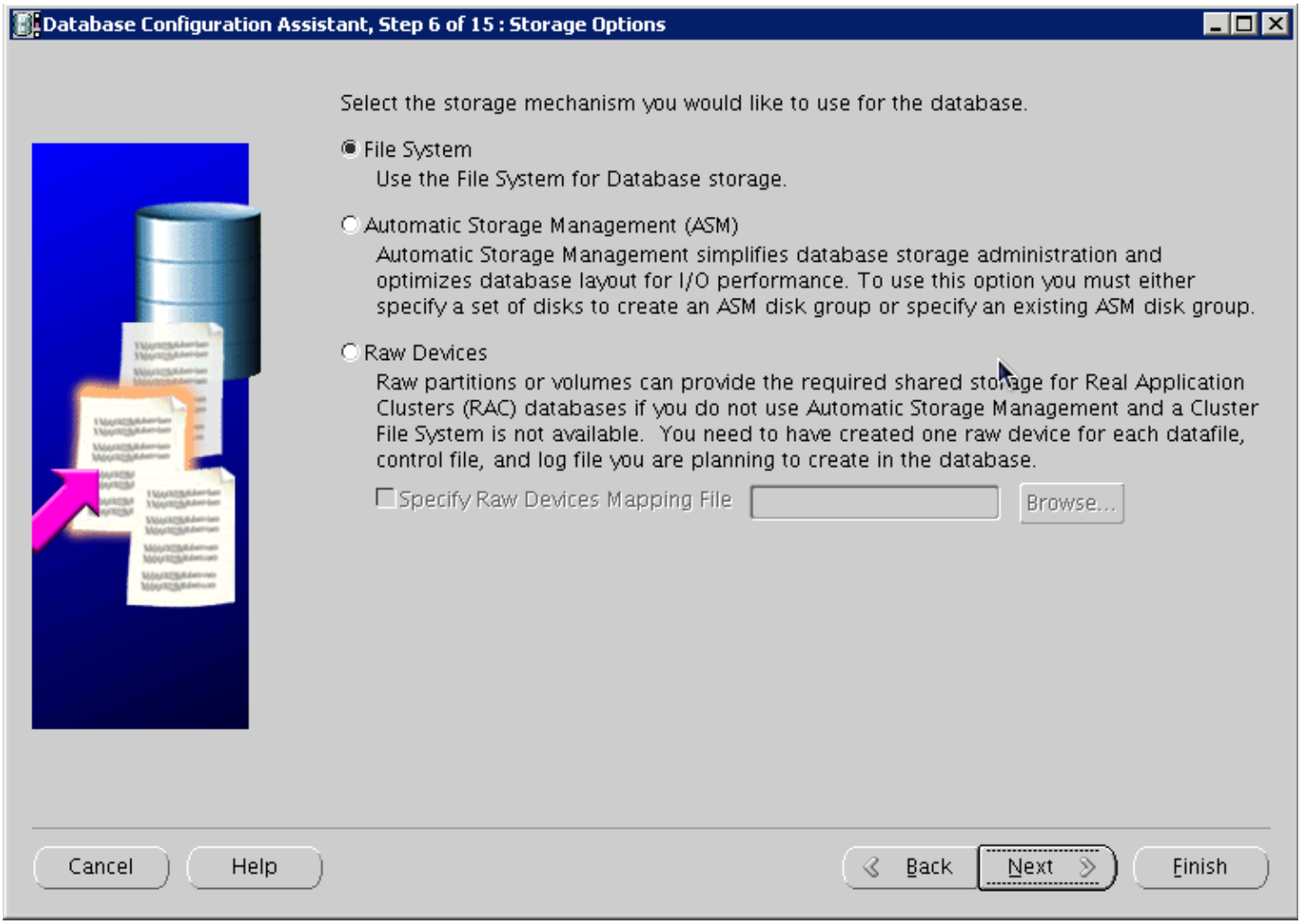
5. Select Configure with EnterpriseManager, click next:



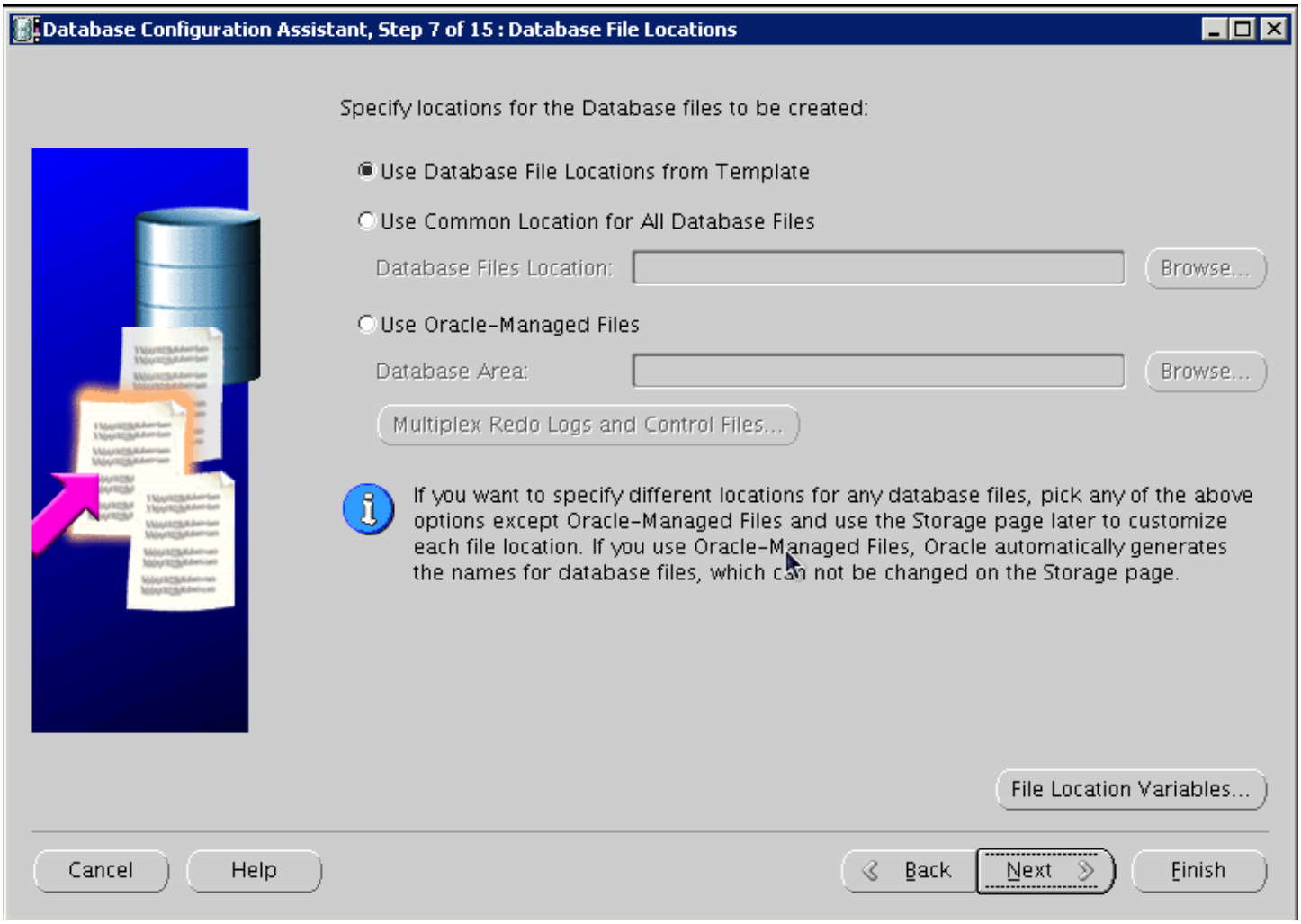
6. Provide account and password details, click next:



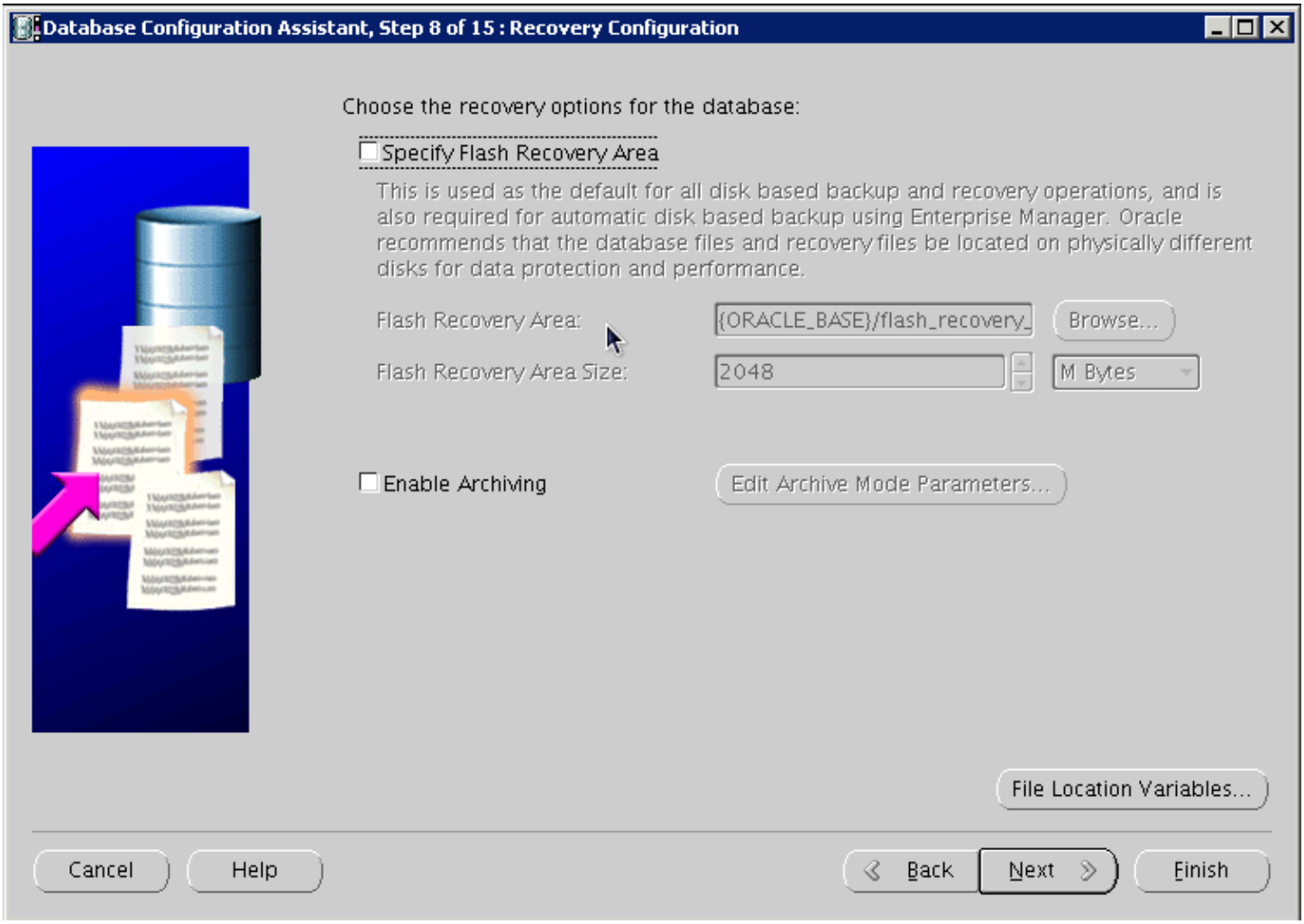
7. Configure the storage options, and then click next:



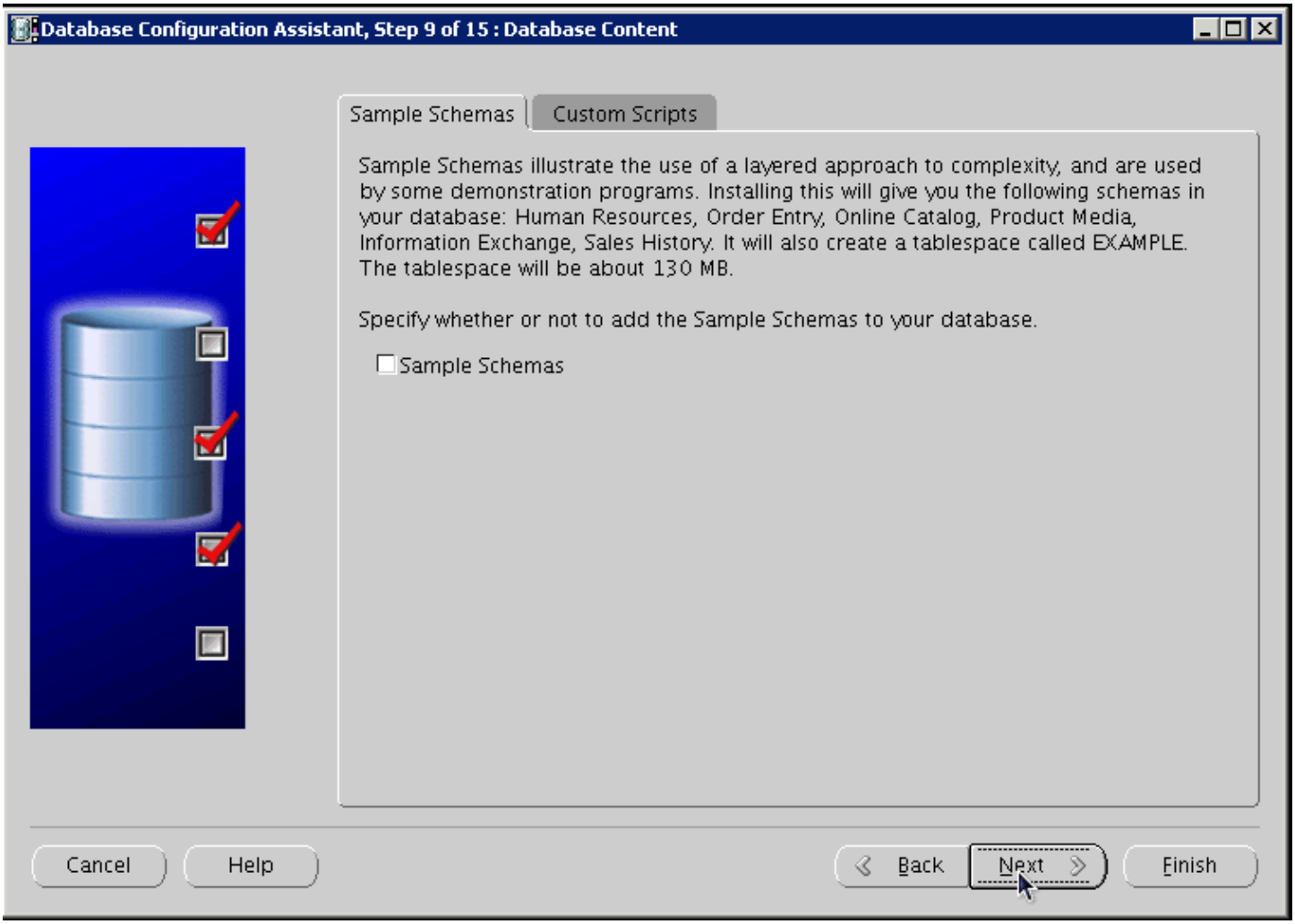
8. Configure file locations, click Next:



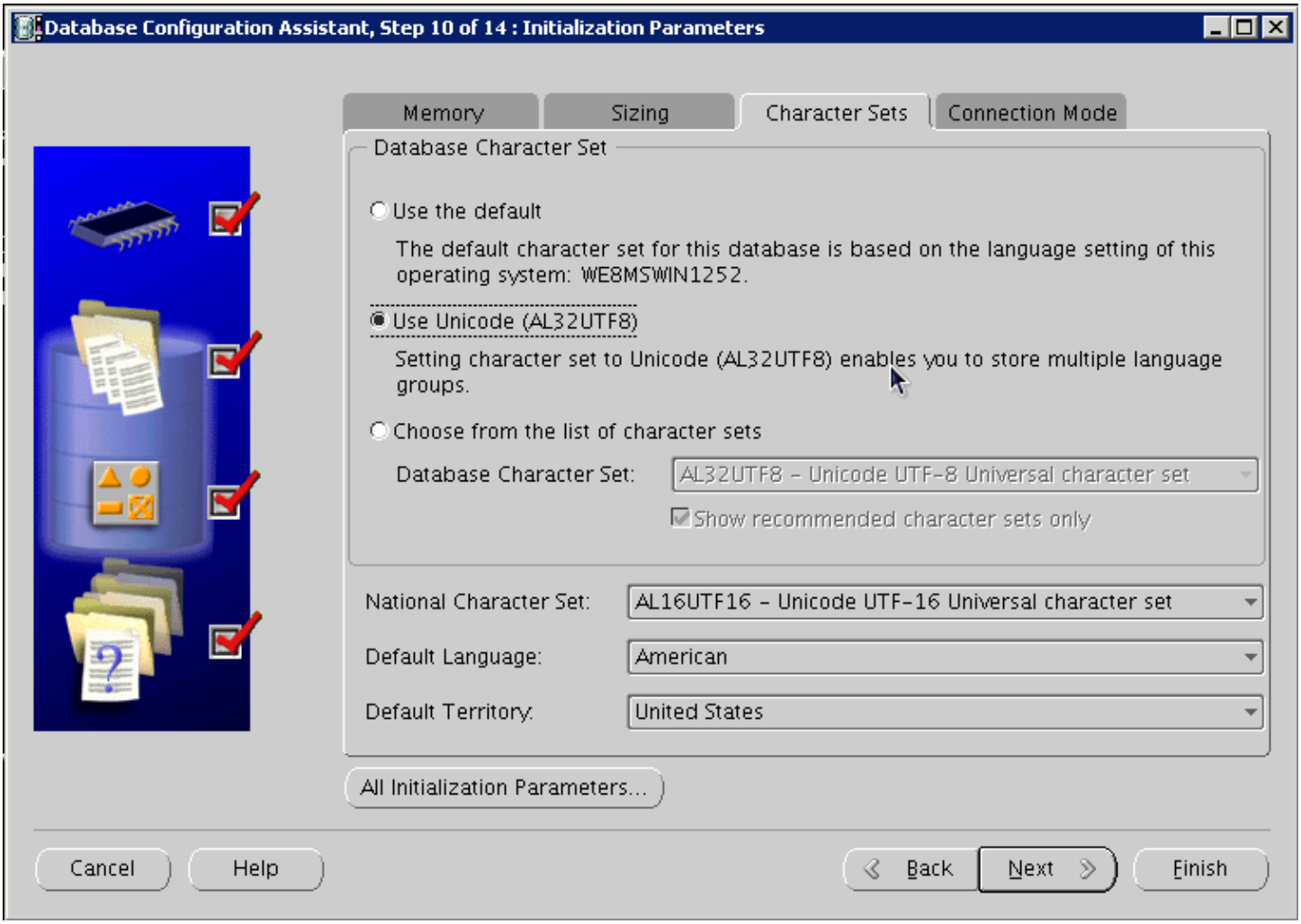
9. Configure recovery options, click next:



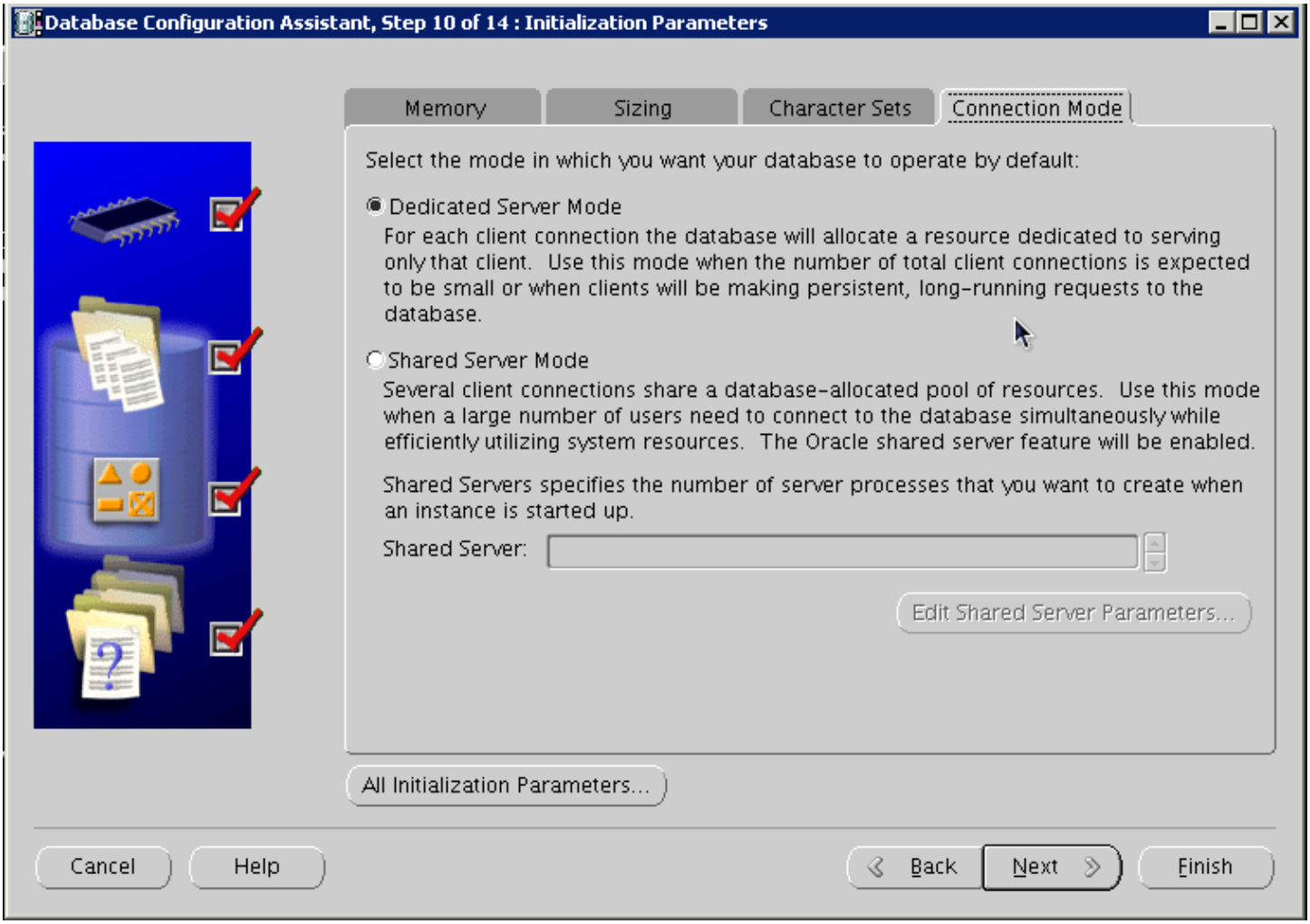
10. Do Not install sample schemas, click next:



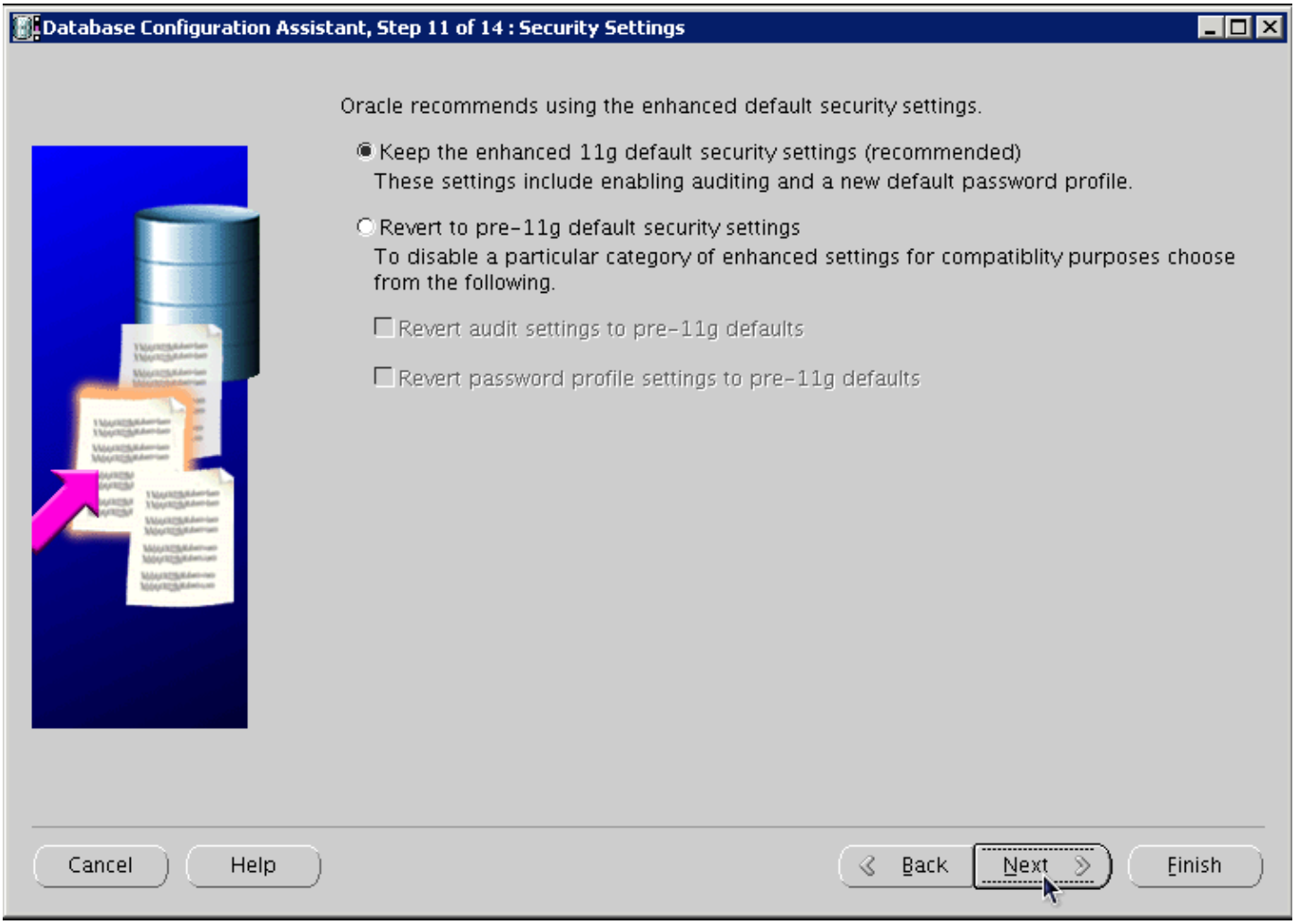
11. Configure UNICODE Character Set:



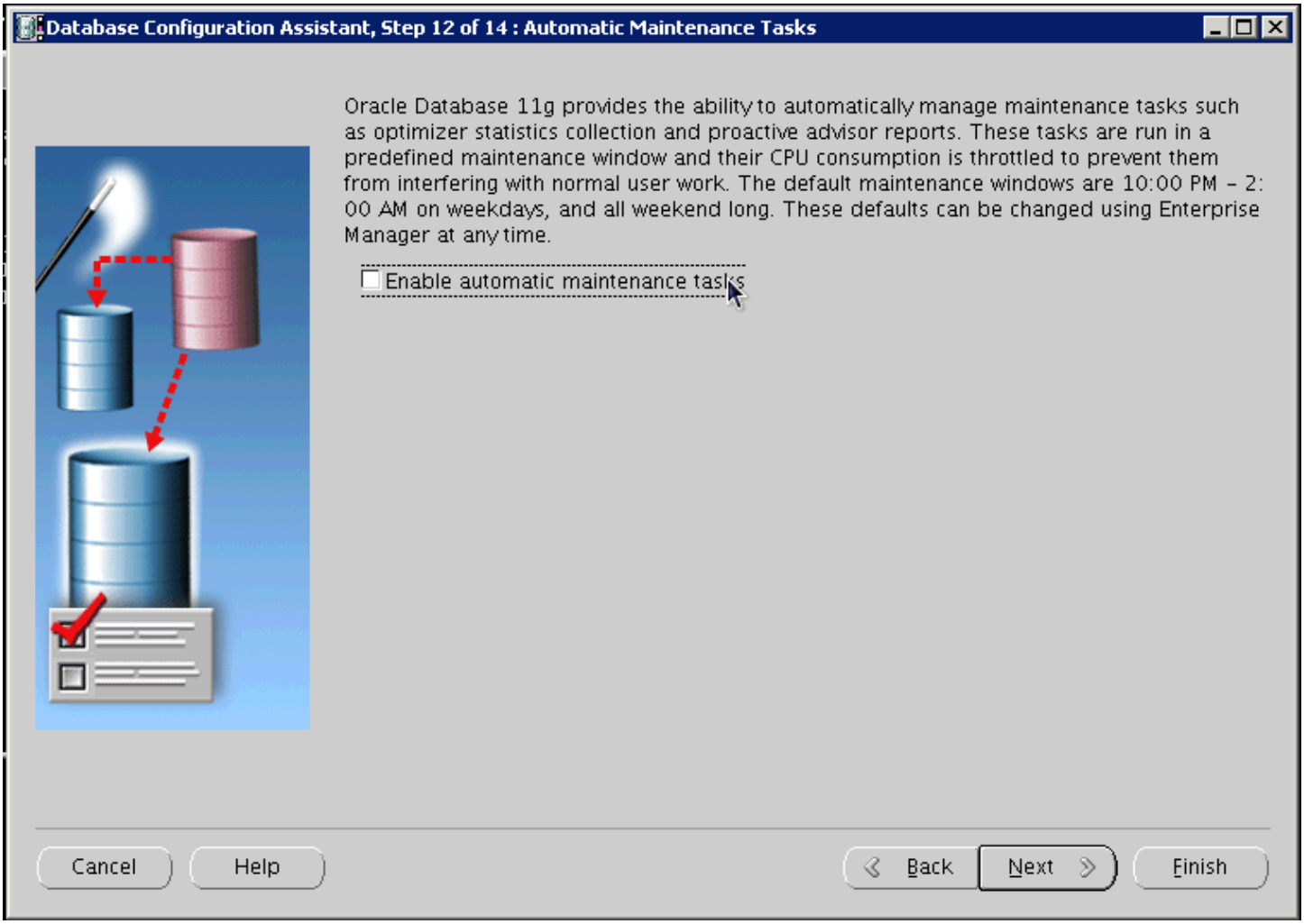
12. Configure Connection Mode, click next:



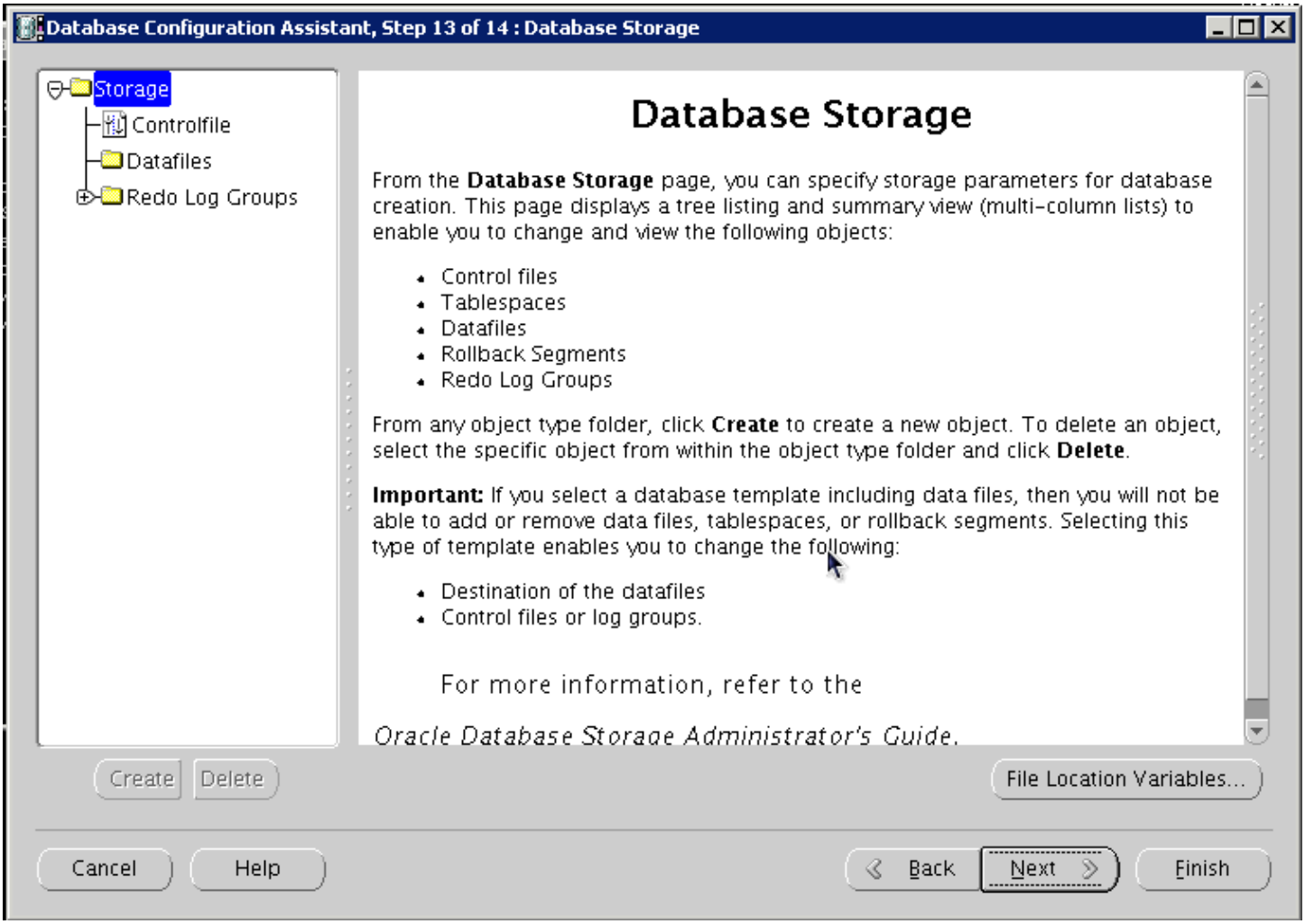
13. Configure Security settings, click next:



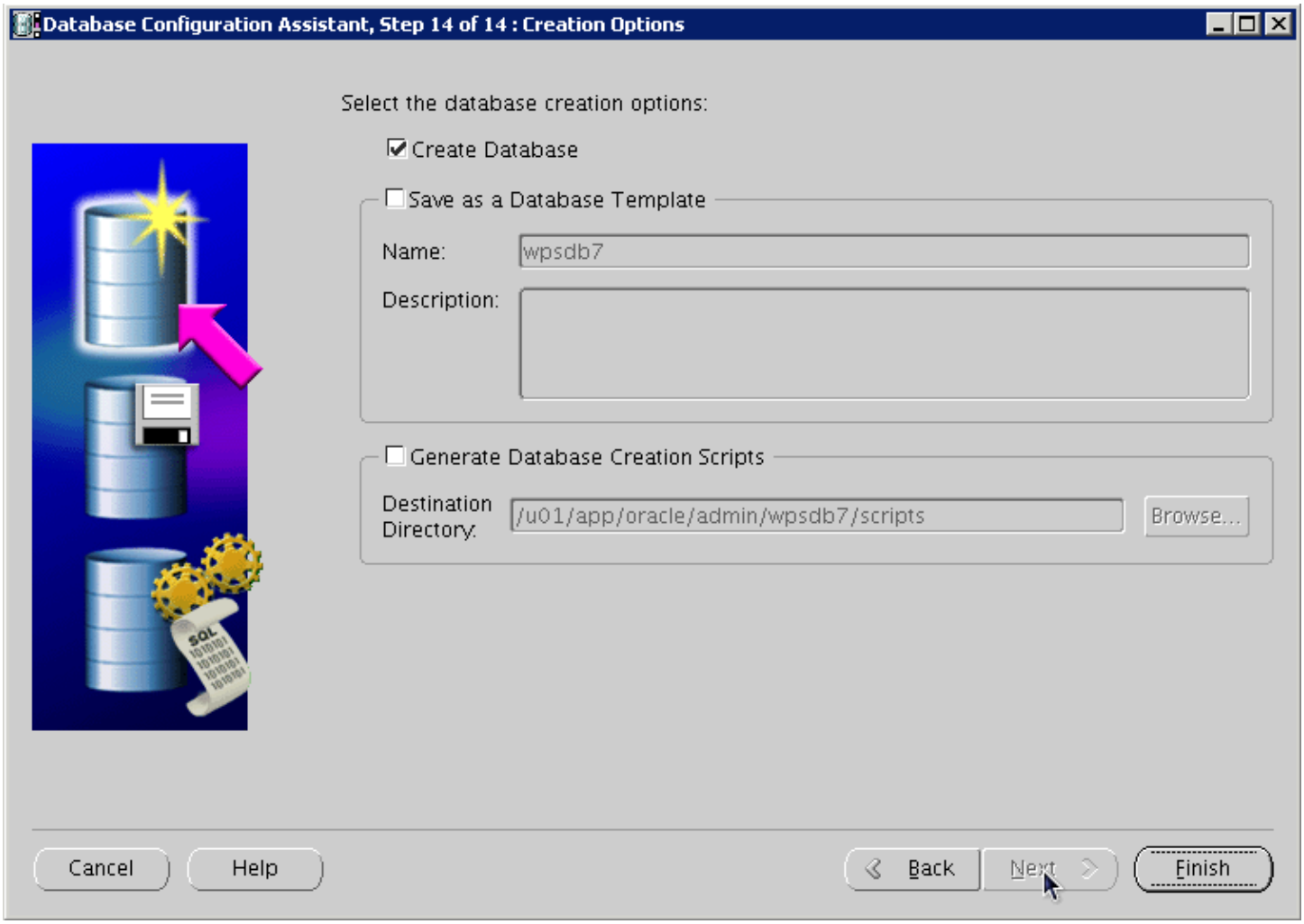
14. Configure maintenance task, click next:



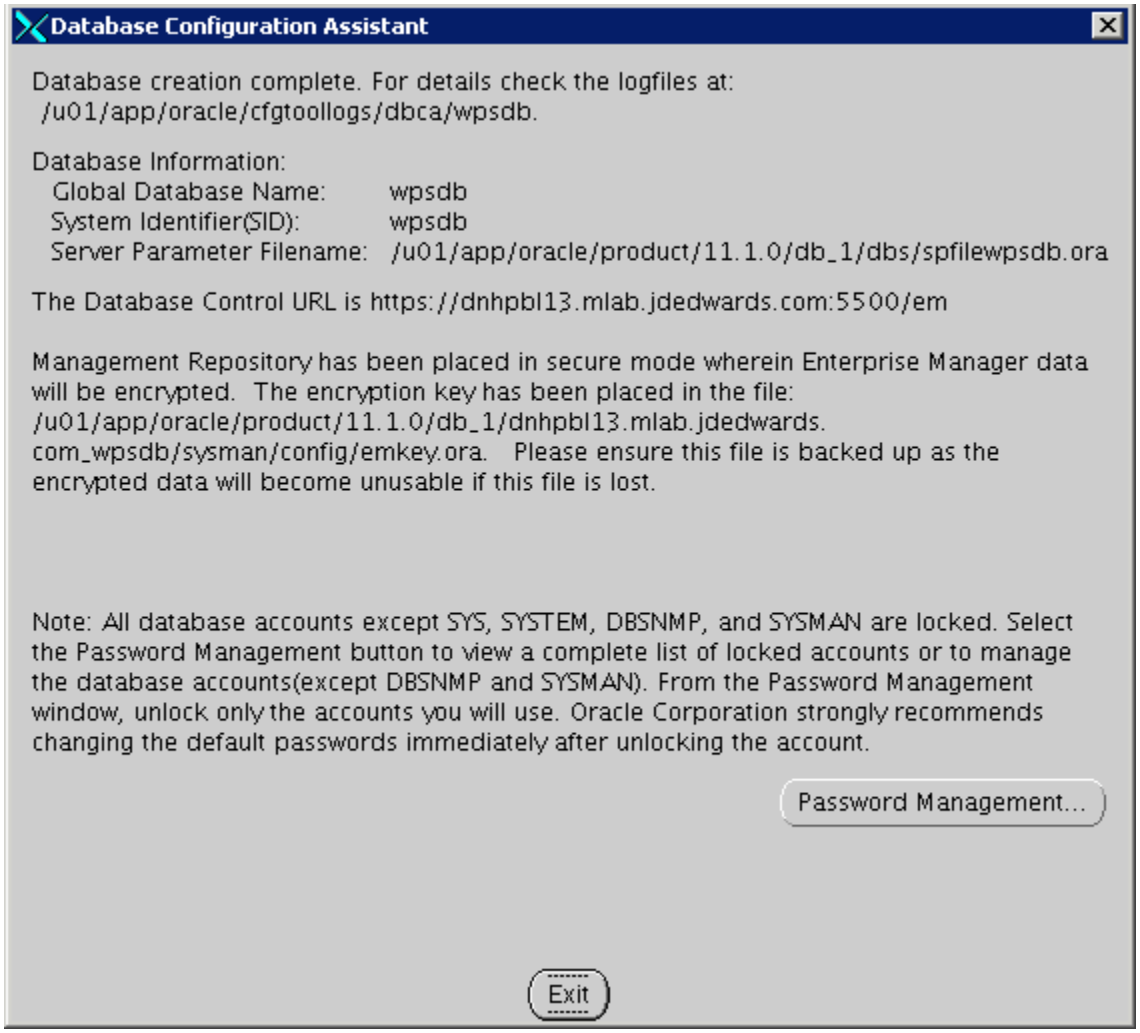
15. Review storage information, click next:



16. Review information, click finish:



17. Once the installation completes review the installation summary information:



18. From sqlplus command line perform the following select query:

```
SQL> select * from NLS_DATABASE_PARAMETERS;
```

```
[oracle@dnhpbl13 bin]$ sqlplus sys/oracle@wpsdb as sysdba

SQL*Plus: Release 11.1.0.6.0 - Production on Mon Aug 8 00:05:59 2011

Copyright (c) 1982, 2007, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.1.0.6.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> select * from NLS_DATABASE_PARAMETERS;

PARAMETER
------------------------------
VALUE
--------------------------------------------------------------------------------
NLS_NCHAR_CHARACTERSET
AL16UTF16

NLS_RDBMS_VERSION
11.1.0.6.0


20 rows selected.
```

Oracle Database Setup Considerations

Listed below are some important considerations before setting up Oracle databases to work with WebSphere Portal.

For information about creating databases, refer to the Oracle product documentation. For information on the recommended database architecture and the databases you will need to create, see the Planning for Oracle topic. Be sure that all databases to be used with WebSphere Portal are created as UNICODE character set databases.

If you are using Oracle 10g databases, you must also obtain a copy of the ojdbc6.jar file from the Oracle JDBC driver download site, copy it to the WebSphere Portal machine, and update the wkplc_dbtype.properties file with oracle.DbLibrary=(the path to the local ojdbc6.jar). If you are using Oracle 11g databases, you must also copy the ojdbc6.jar file from the Oracle server to the WebSphere Portal machine and update the wkplc_dbtype.properties file with oracle.DbLibrary=(the path to the local ojdbc6.jar). The typical location is the oracle_home/sqldeveloper/jdbc/lib directory. Record the copy location on your local machine for future reference.

When creating Oracle databases for use with WebSphere Portal, you should consider the following information:

- The Oracle databases must be created manually before configuring WebSphere Portal.
- All databases must be created using UNICODE Database and National character sets such as UTF8, AL32UTF8, or AL16UTF16.

- It is recommended that all databases to be used with WebSphere Portal are configured in Dedicated Server Mode.
- Determine if your Oracle server will be remote or local to the WebSphere Portal installation.
- After installing the database software for WebSphere Portal, you will need to set the buffer pools allocated to the Oracle database in order for WebSphere Portal to communicate with the Java Content Repository database. Use the following recommended values as a guide. Refer to the Oracle product documentation for information on how to set the buffer pools. Recommended initial buffer pool sizes:

  db_block_size = 8192 bytes

  db_cache_size = 307,200 bytes

  db_files = 1024 files

  log_buffer = 65536 bytes

  open_cursors = 1500 cursors

  pga_aggregate_target = 204,800 bytes

  pre_page_sga = true

  processes = 300 processes

  shared_pool_size = 204,800 bytes

  > **Note:** If you are using IBM Java Content Repository, the open_cursors value may need to be increased based on the table count in the Java Content Repository schema.

- Raise the number of parallel servers as appropriate. For example, if you have more than 875 parallel servers, you should set the parallel_max_serversto 1200.
- The Oracle parameter CURSOR_SHARING allows similar SQL Statements to be shared when possible, which prevents parsing and establishing a new execution plan. The execution plan is used by Oracle to gather the data needed to satisfy a request. There are two options for CURSOR_SHARING, which are as follows:
  - FORCE

    When you select this option, Oracle uses the same execution plan for all SQLs that are similar in value even if the values are different. When you use this option, the execution plan may not provide optimum performance. For example, similar SQLs with different values may behave differently when executed running the same plan.
  - EXACT

    When you select this option, Oracle only shares the same execution plan for SQLs that are identical and use the same values. This option removes the risk of a SQL statement being executed when optimum performance conditions do not exist.
- WebSphere Portal supports both options. Regardless of the option selected, portlet applications should not be affected. Contact your database administrator for further assistance on these options.

Refer to the following instructions for creating tablespaces:

1. In the database directory, create the data directory data and the index directoryindex.

2. Create tablespaces using the following commands as examples:

   a. Substitute the values of your environment for the following variables:

      - &jcrdb. is the name of the database you created to store user data.
      - &dbpath. is the directory where you created the database; the default path is /oracle/oradata.

   b. Ensure that the '.' is included in the variables when you substitute the values of your environment with these variables.

      > **Note:** You must use the same table space names listed in the commands. The table space names cannot be customized or modified.

      ```
      create tablespace ICMLFQ32 datafile '&dbpath./&jcrdb./data/
      &jcrdb._ICMLFQ32_01.dbf' size 300M reuse autoextend on next 10M
       maxsizeUNLIMITED extent management local autoallocate;

      create tablespace ICMLNF32 datafile '&dbpath./&jcrdb./data/
      &jcrdb._ICMLNF32_01.dbf' size 25M reuse autoextend on next 10M maxsizeUNLIMITED
       extent management local autoallocate;

      create tablespace ICMVFQ04 datafile '&dbpath./&jcrdb./data/
      &jcrdb._ICMVFQ04_01.dbf' size 25M reuse autoextend on next 10M maxsizeUNLIMITED
       extent management local autoallocate;

      create tablespace ICMSFQ04 datafile '&dbpath./&jcrdb./data/
      &jcrdb._ICMSFQ04_01.dbf' size 150M reuse autoextend on next 10M
       maxsizeUNLIMITED extent management local autoallocate;

      create tablespace ICMLSNDX datafile '&dbpath./&jcrdb./index/
      &jcrdb._ICMLSNDX_01.dbf' size 10M reuse autoextend on next 10M maxsizeUNLIMITED
       extent management local autoallocate;
      ```

   c. Set the size, autoextend, and maxsize values according to your environment. For example, you may want to change the maxsize to a set value rather than UNLIMITED.

   d. Consult your Database Administrator for specific guidance about creating tablespaces for your environment.

   e. Refer to the Oracle command reference for more information about using the create tablespaces command.

This topic provides instructions on automatically setting up your database using the ConfigEngine task to create users, grant permissions, and create Java Content Repository table spaces.

1. On the database server, make sure the subfolders your_oracle_instance/data and your_oracle_instance/index exist. If this folder hierarchy does not exist, create it manually before you run the setup-database task.

   The setup-database task requires these folders to create table spaces. If these folders do not exist, the setup-database task will fail. Note: The setup-database task creates the table spaces, index spaces, and the database users as specified in the properties files.

2. Complete these steps to manually grant database user privileges:

   a. Copy the appropriate template files to a work directory. Choose one of the following template files:

      - createRuntimeRoleForDifferentSchema.sql if the name of the database user and the schema name are not the same.
      - createRuntimeRoleForSameSchema.sql if the name of the database user and the schema name are the same.
      - JCR database domain: For the JCR database domain, you must also copy grantExtendedPermissionsToRuntimeRole.sql.

   b. Locate these files in the following directories:

      PortalServer_root\\base\\wp.db.impl\\config\\templates\\setupdb\\dbms\\domain PortalServer_root\\pzn\\prereq.pzn\\config\\templates\\setupdb\\dbms\\domain

   c. Replace all placeholder values with the values as defined in wkplc_dbdomain.properties. Placeholder values are surrounded by the character @.

   d. Run these statements.

      Complete these steps to grant database user privileges with the ConfigEngine task:

      Ensure the database administrator user ID is specified for domain.DBA.DbUser in wp_profile_root\\ConfigEngine\\properties\\wkplc_dbdomain.properties. For example, domain.DBA.DbUser=dbadmin.

   e. Run the following task: ./ConfigEngine.sh grant-runtime-db-user-privileges -DTransferDomainList=comma_separated_list_of_domains

3. After transferring the database tables, run the dbms_stats.gather_schema_stats command to update the database statistics.

   For example:

   ```
   SQL> execute dbms_stats.gather_schema_stats(ownname=> 'jcr', cascade=> TRUE);
   ```

4. Run the ./ConfigEngine.sh create-jcr-jms-resources-post-dbxfer -DWasPassword=password command to create JMS resources in the new database.

   > **Note:** Regardless of the method used to transfer data (configuration wizard or the steps in this topic), you must run this task to create JMS resources.

5. Change to the directory wp_profile_root\\bin.
6. Start the Administrative server (server1) and WebSphere Portal server.

6 Verifying Database Connections

Verifying Database Connections

This section provides information on verifying database connections.

Verifying Database Connections

After you configure IBM® WebSphere® Portal to work with your database, test the database connection to ensure that it operates correctly. Then verify that all database transactions work properly within the WebSphere Portal environment. For example, all portal pages should display without HTTP 404 errors, and there should be no database layer-related exceptions in the SystemOut.log and SystemErr.log files.

You can verify the database connection using IBM WebSphere Application Server or by opening WebSphere Portal in a browser.

To verify that the WebSphere Portal application server is running by using WebSphere Application Server, complete these steps:

1. Open the WebSphere Application Server administrative console by entering the following address in a browser:

   http://hostname.example.com:10001/ibm/console

   where hostname.example.com is the fully qualified host name of the machine where WebSphere Portal is running and 10042 is the default transport port that is created by WebSphere Application Server.
2. Log into the administrative console.
3. Click Resources, JDBC, JDBC Providers.
4. Select all scopes (the default setting) or select a specific cell, node, or node/server.

   Select the scope that corresponds to your instance of WebSphere Portal.

   The view refreshes.
5. Select the name of the data source that is defined in wkplc_dbdomain.properties.

   The default data source is wpdbDS.
6. Select the name of the JDBC provider that is specified in wkplc_dbtype.properties.

   The default JDBC provider is wpdbJDBC_dbtype, where dbtype is replaced by the value that matches your environment.
7. Click Test Connection to verify the database connection.

   If configuration parameters have been changed, you might need to restart WebSphere Application Server for the test to complete.

To verify that the WebSphere Portal application server is running by opening WebSphere Portal in a browser, enter the following URL in a supported browser:

http://hostname.example.com:10039/wps/portal

where hostname.example.com is the fully qualified host name of the machine, where WebSphere Portal is running and 10039 is the default transport port that is created by WebSphere Application Server.

7 Configuring the Microsoft Active Directory for Portal

Installing Microsoft Active Directory for Microsoft Windows 200x

If you plan to use Active Directory as an LDAP user registry, you must install and set up the server so that it will communicate with IBM® WebSphere® Portal.

Preparing Active Directory

Perform the following steps to install and configure Active Directory:

1. Install required Service Packs.
2. Perform the following steps to install Internet Information Services (IIS), which is required to export server certificates and must be installed before installing Certificate Services:
    a. Open the Control Panel and select Add/Remove Programs.
    b. Choose Add/Remove Windows Components.
    c. Choose the Internet Information Services (IIS) component and then click Next.
    d. Follow the instruction of the Windows Components Wizard. The Windows Server CD is needed.
3. Use the following steps to install Certificate Services if you plan on using Active Directory over SSL:
    a. Open the Control Panel and select Add/Remove Programs.
    b. Choose Add/Remove Windows Components.
    c. Select Certificate Services and then click Next.
    d. Select Stand-alone root CA and then click Next. You can also choose other options depends on you needs.
    e. Fill in CA identifying information and then click Next.
    f. Follow the instruction of the Windows Components Wizard. The Windows Server CD is needed.

Perform the following steps as a guide to create the WebSphere Portal administrative user:

1. Create a new user with the Windows administrative tools.

    Note: There is a 20 character limitation for the user account name.

2. Set the password for the new user.
3. Activate the new user with the Windows administrative tools. Set the msDS-UserAccountDisabled attribute to false.

Perform the following steps to enable SSL for Active Directory; this step is required to set passwords during sign up and user creation:

1. Install an Enterprise Certificate Authority on a Windows 2000 Domain Controller, which installs a certificate on a server or install a third-party certificate on the Domain Controller.
2. Click Start -> All Programs -> Administrative Tools -> Active Directory Users and Computer.

3. In the Active Directory Users and Computers window, right-click on your domain name and select Properties.
4. In the Domain Properties dialog box, select the Group Policy tab.
5. Select the Default Domain Policy group policy and then click Edit.
6. Select Windows Settings under Computer Configuration.
7. Select Security Settings and then select Public Key Policies.
8. Select Automatic Certificate Request Settings.
9. Use the wizard to add a policy for Domain Controllers.

Note: When these requirements are complete, all domain controllers request a certificate and support LDAP over SSL using port 636.

LDAP User Registry without SSL

Configure IBM® WebSphere® Portal to use a standalone LDAP user registry to store all user account information for authorization.

If you need to rerun the wp-modify-ldap-security task to change the LDAP repositories or because the task failed, you must choose a new name for the realm using the standalone.ldap.realm parameter or you can set ignoreDuplicateIDs=true in the wklpc.properties file, before rerunning the task.

Perform the following steps to configure a standalone LDAP user registry:

Note: Use the wp_security_xxx.properties helper file, located in the wp_profile_root/ConfigEngine/config/helpersdirectory, when performing this task to ensure the correct properties are entered. In the instructions below, when the step refers to thewkplc.properties file, you will use your wp_security_xxx.properties helper file.

1. Use a text editor to open the wkplc.properties file, located in the wp_profile_root\\ConfigEngine\\properties directory.
2. Required: Enter a value for the following required parameters in the wkplc.properties file under the Stand-alone security heading:

   Note: See the properties file for specific information about the required parameters and for advanced parameters.

   standalone.ldap.id
   standalone.ldap.host
   standalone.ldap.port
   standalone.ldap.bindDN
   standalone.ldap.bindPassword
   standalone.ldap.ldapServerType
   standalone.ldap.userIdMap
   standalone.ldap.groupIdMap
   standalone.ldap.groupMemberIdMap

standalone.ldap.userFilter

standalone.ldap.groupFilter

standalone.ldap.serverId

standalone.ldap.serverPassword

standalone.ldap.realm

standalone.ldap.primaryAdminId

standalone.ldap.primaryAdminPassword

standalone.ldap.primaryPortalAdminId

standalone.ldap.primaryPortalAdminPassword

standalone.ldap.primaryPortalAdminGroup

standalone.ldap.baseDN

3. Required: Enter a value for the following required entity types parameters in the wkplc.properties file under the LDAP entity types heading:

> **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

standalone.ldap.et.group.objectClasses

standalone.ldap.et.group.objectClassesForCreate

standalone.ldap.et.group.searchBases

standalone.ldap.et.personaccount.objectClasses

standalone.ldap.et.personaccount.objectClassesForCreate

standalone.ldap.et.personaccount.searchBases

4. Required: Enter a value for the following required group member parameters in the wkplc.properties file under the Group member attributes heading:

> **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

standalone.ldap.gm.groupMemberName

standalone.ldap.gm.objectClass

standalone.ldap.gm.scope

standalone.ldap.gm.dummyMember

5. Required: Enter a value for the following required relative distinguished name (RDN®) parameters in the wkplc.propertiesfile under the Default parent, RDN attribute heading:

   > **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

   standalone.ldap.personAccountParent

   standalone.ldap.groupParent

   standalone.ldap.personAccountRdnProperties

   standalone.ldap.groupRdnProperties
6. Save your changes to the wkplc.properties file.
7. Run the ./ConfigEngine.sh validate-standalone-ldap -DWasPassword=password task to validate your LDAP server settings.

   > **Note:** If you have not deleted the default file repository, WasPassword is the value entered during installation and not a value found in your LDAP user registry.

   > **Note:** During the validation task, you may receive the following prompt: Add signer to the trust store now? Press y and Enter.
8. Run the ./ConfigEngine.sh wp-modify-ldap-security -DWasPassword=password task, from thewp_profile_root\\ConfigEngine directory, to set the stand-alone LDAP user registry.
9. Stop and restart the appropriate servers to propagate the changes. For specific instructions, see the following link under Related tasks: Starting and stopping servers, deployment managers, and node agents.
10. Run the ./ConfigEngine.sh wp-validate-standalone-ldap-attribute-config -DWasPassword=password task, from the wp_profile_root\\ConfigEngine directory, to check that all defined attributes are available in the configured LDAP user registry.

    > **Note:** When you finish configuring your LDAP user registry, see "Adapting the attribute configuration" for information about adding and mapping attributes to ensure proper communication between WebSphere Portal and the LDAP server.
11. Optional: Run the Member Fixer task to update the member names used by Web Content Management with the corresponding members in the LDAP directory. This step ensures that access to the Web content libraries for

the Intranet and Internet Site Templates for the contentAuthors group is correctly mapped to the appropriate group in the LDAP directory.

> **Note:** This step is only needed if you have installed the product with Web Content Management and intend to use the Intranet and Internet Site Templates that were optionally installed with the product by running the configure-express task.

a. Edit the wp_profile_root\\PortalServer\\wcm\\shared\\app\\config\\wcmservices\ \MemberFixerModule.properties file.
b. Add the following lines to the file:

```
uid=xyzadmin,o=defaultWIMFileBasedRealm -> portal_admin_DN

cn=contentauthors,o=defaultWIMFileBasedRealm -> content_authors_group_DN
```

Where portal_admin_DN is the distinguished name of the portal administrator and content_authors_group_DN is the distinguished name of the content authors group used during LDAP configuration.

> **Note:**
>
> - Ensure the portal administrator you specify for portal_admin_DN is a member of the group you specify forcontent_authors_group_DN, otherwise the portal administrator cannot access the Web content libraries for the Intranet and Internet Site Templates.
> - If you plan to run the express-memberfixer task in an environment with multiple realms, remove thecn=contentauthors,o=defaultWIMFileBasedRealm group if it exists. If this group exists in an environment with multiple realms, the Member Fixer task does not have any effect.

c. Save your changes and close the file.
d. Run the ./ConfigEngine.sh express-memberfixer -DmemberfixerRealm=realm_name -DPortalAdminPwd=password-DWasPassword=password task, located in the wp_profile_root\ \ConfigEngine directory.

> **Note:** Choose the appropriate value to enter for realm_name depending on the type of LDAP user registry you configured:

The following table contains the value for realm_name when running the Member Fixer task to update the member names used by Web Content Management:

Type of LDAP	Value
Standalone LDAP	The value specified for realm_name should match the value forstandalone.ldap.realm in the wkplc.properties file.
Federated LDAP	The value specified for realm_name should match the value forfederated.realm in the wkplc.properties file. If the value forfederated.realm is empty, use defaultWIMFileBasedRealmas the default value.

12. Optional: Assign access to the Web content libraries.

    a. Log in as a portal administrator.
    b. Navigate to Administration -> Portal Content -> Web Content Libraries.
    c. Click the Set permissions icon for the Web library.
    d. Click the Edit Role icon for Editor.
    e. Add the group you specified for content_authors_group_DN as an Editor for the Intranet and Internet libraries.
    f. Click Apply then Done.
    g. If you have created any additional Web Content Management libraries, run the Web content member fixer task to update the member names used by the libraries.

LDAP User Registry over SSL

Configure IBM® WebSphere® Portal to use a standalone LDAP user registry over SSL to store all user account information for secure authorization.

Perform the following steps to configure a standalone LDAP user registry over SSL:

> **Note:** Use the wp_security_xxx.properties helper file, located in the wp_profile_root/ConfigEngine/config/helpersdirectory, when performing this task to ensure the correct properties are entered. In the instructions below, when the step refers to thewkplc.properties file, you will use your wp_security_xxx.properties helper file.

1. Choose one of the following options to specify the LDAP server's SSL certificate in either the server trust store or the default client trust store:

    a. Choose one of the following to add the certificate to the server trust store:

    The following table contains the options for adding the SSL certificate to the server trust store:

Option	Steps
Add the certificate to the server trust store	i. Log in to the WebSphere Application Server Administrative Console. ii. Navigate to Security, SSL certificate and key management, SSL configurations. iii. Click the appropriate SSL configuration from the list. For example, Stand-alone environments:NodeDefaultSSLSettings Clustered environments: CellDefaultSSLSettings iv. Click Key stores and certificates. v. Click the appropriate trust store from the list. For example, Stand-alone environments: NodeDefaultTrustStore Clustered environments: CellDefaultTrustStore vi. Click Signer certificates, click Add, and then enter the following information: Type the Alias the key store uses for the signer certificate. Type the File name where the signer certificate is located. vii. Click OK and then click Save to save the changes to the master configuration.

Option	Steps
Retrieve the certificate from the port	i. Log in to the WebSphere Application Server Administrative Console. ii. Navigate to Security, SSL certificate and key management, SSL configurations. iii. Click the appropriate SSL configuration from the list. For example, Stand-alone environments:NodeDefaultSSLSettings Clustered environments: CellDefaultSSLSettings iv. Click Key stores and certificates. v. Click the appropriate trust store from the list. For example, Stand-alone environments: NodeDefaultTrustStore Clustered environments: CellDefaultTrustStore vi. Click Signer certificates, click Retrieve from port, and then enter the following information: Type the Host name used when attempting to retrieve the signer certificate from the SSL port. Type the SSL Port used when attempting to retrieve the signer certificate. Type the Alias the key store uses for the signer certificate. Clustered environments: Ensure the setting for SSL configuration for outbound connection matches your SSL settings. vii. Click Retrieve signer information to retrieve the certificate from the port.

Option	Steps
	viii. Click OK and then click Save to save the changes to the master configuration.

b. Add the certificate to the client trust store:

- See Secure installation for client signer retrieval.
- Run the retrieveSigners task from the wp_profile_root/bin directory; see retrieveSigners command for information. In a deployed environment, you will need to run the retrieveSigners task, for any federated node, against the Deployment Manager.

> **Note:** This task might report an error, but it does successfully update the trust store. You can ignore the error message. Example task: Stand-alone environments

Example task:

For stand-alone environments:

```
retrieveSigners.bat NodeDefaultTrustStore ClientDefaultTrustStore -autoAcceptBootstrapSigner
-conntype SOAP -port port_number
```

For clustered environments

```
retrieveSigners.bat CellDefaultTrustStore ClientDefaultTrustStore -autoAcceptBootstrapSigner
-conntype SOAP -port port_number
```

When prompted, enter the following:

Realm/Cell Name: name

Username: user_ID

Password: password

The following message displays:

CWPKI0308I: Adding signer alias "alias_name" to local keystore "ClientDefaultTrustStore" with the following SHA digest: ssl_certificate_fingerprint

- Update the trust store properties file.

2. Use a text editor to open the wkplc.properties file, located in the wp_profile_root\\ConfigEngine\\properties directory.

3. Required: Enter a value for the following required parameters in the wkplc.properties file under the VMM Stand-alone LDAP configuration heading:

   > **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

   standalone.ldap.id

   standalone.ldap.host

   standalone.ldap.port

   standalone.ldap.bindDN

   standalone.ldap.bindPassword

   standalone.ldap.ldapServerType

   standalone.ldap.userIdMap

   standalone.ldap.groupIdMap

   standalone.ldap.groupMemberIdMap

   standalone.ldap.userFilter

   standalone.ldap.groupFilter

   standalone.ldap.serverId

   standalone.ldap.serverPassword

   standalone.ldap.realm

   standalone.ldap.primaryAdminId

   standalone.ldap.primaryAdminPassword

   standalone.ldap.primaryPortalAdminId

   standalone.ldap.primaryPortalAdminPassword

   standalone.ldap.primaryPortalAdminGroup

   standalone.ldap.baseDN

4. Required: Enter a value for the following required entity types parameters in the wkplc.properties file under the LDAP entity types heading:

   > **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

   standalone.ldap.et.group.objectClasses

   standalone.ldap.et.group.objectClassesForCreate

   standalone.ldap.et.group.searchBases

   standalone.ldap.et.personaccount.objectClasses

   standalone.ldap.et.personaccount.objectClassesForCreate

   standalone.ldap.et.personaccount.searchBases

5. Required: Enter a value for the following required group member parameters in the wkplc.properties file under the Group member attributes heading:

   > **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

   standalone.ldap.gm.groupMemberName

   standalone.ldap.gm.objectClass

   standalone.ldap.gm.scope

   standalone.ldap.gm.dummyMember

6. Required: Enter a value for the following required relative distinguished name (RDN®) parameters in the wkplc.properties file under the Default parent, RDN attribute heading:

   > **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

   standalone.ldap.personAccountParent

   standalone.ldap.groupParent

   standalone.ldap.personAccountRdnProperties

   standalone.ldap.groupRdnProperties

7. Enter a value for the following parameters to enable Secure Socket Layers (SSL):

   > **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

   Required parameters:

   standalone.ldap.sslEnabled

   standalone.ldap.sslConfiguration

Optional parameters:

standalone.ldap.certificateMapMode

standalone.ldap.certificateFilter

8. Save your changes to the wkplc.properties file.
9. Run the ./ConfigEngine.sh validate-standalone-ldap -DWasPassword=password task to validate your LDAP server settings.

> **Note:** If you have not deleted the default file repository, WasPassword is the value entered during installation and not a value found in your LDAP user registry.

> **Note:** During the validation task, you may receive the following prompt: Add signer to the trust store now? Press y and then Enter.

10. Run the ./ConfigEngine.sh wp-modify-ldap-security -DWasPassword=password task, from thewp_profile_root\\ConfigEngine directory, to set the stand-alone LDAP user registry.
11. Stop and restart the appropriate servers to propagate the changes. For specific instructions, see the following link under Related tasks: Starting and stopping servers, deployment managers, and node agents.
12. Run the ./ConfigEngine.sh wp-validate-standalone-ldap-attribute-config -DWasPassword=password task, from the wp_profile_root\\ConfigEngine directory, to check that all defined attributes are available in the configured LDAP user registry.

> **Note:** When you finish configuring your LDAP user registry, see "Adapting the attribute configuration" for information about adding and mapping attributes to ensure proper communication between WebSphere Portal and the LDAP server.

Working with LDAP Attributes

This section describes how to:

- Perform a query on attributes.
- Add new attributes to your user registry.
- Map attributes between WebSphere Portal and your LDAP server.
- Remove attributes from your database.

After installing IBM® WebSphere® Portal and configuring your LDAP user registries, you can query the defined attributes to see what attributes are flagged as unsupported or if the attribute is mapped to a different LDAP attribute.

To perform a query:

Run the ./ConfigEngine.sh wp-query-attribute-config -DWasPassword=password task, from thewp_profile_root/ConfigEngine directory, any time during the configuration process or at runtime to query an overview of the currently defined attributes.

This task creates the availableAttributes.html report, located in the wp_profile_root/ConfigEngine/logdirectory. The report contains one table that lists the available attributes for Users (PersonAccount) and one table that lists the available attributes for Groups. For each configured repository, there is a column that indicates if the attribute is flagged as unsupported or if the attribute is mapped to a different LDAP attribute.

Note: This task does not validate the existence of attributes in the LDAP schema.

The VMM is configured with a default attribute schema that might not be compatible with your LDAP server. If this is the case, extend the VMM attribute schema by adding new attributes that you can map between IBM® WebSphere® Portal and your user registry.

Perform the following steps to add new attributes to your user registry:

1. Install the required Enterprise Archive (.ear) file on WebSphere Application Server.
    a. Open a command prompt.
    b. Navigate to the wp_profile_root\\ConfigEngine directory.
    c. Run the ./ConfigEngine.sh wp-la-install-ear -DWasPassword=password task.
2. Stop and restart the appropriate servers to propagate the changes. For specific instructions, see the following link under Related tasks: Starting and stopping servers, deployment managers, and node agents.
3. Use a text editor to open the wkplc.properties file, located in the wp_profile_root\\ConfigEngine\\properties directory.
4. Enter a value for the following required parameters in the wkplc.properties file under the VMM Property Extension Properties heading:

    Note: See the properties file for specific information about the required parameters and for advanced parameters.

    la.providerURL

    la.propertyName

    la.entityTypes

    la.dataType

    la.multiValued
5. Save your changes to the wkplc.properties file.
6. Run the ConfigEngine.sh wp-add-property -DWasPassword=password task to add the attribute to the user registry.

    Note: This task performs an EJB call to WebSphere Application Server, which must authenticate against WebSphere Application Server. Depending on the configuration in the sas.client.props file, you may receive a popup window or a command line prompt asking for user identity and password. Enter the WebSphere Application Server user ID and password.

    Note: If you have multiple properties to add, repeat all steps, except for the wp-la-install-ear task, until all new attributes are added.
7. Stop and restart the appropriate servers to propagate the changes.

After you install and configure your LDAP user registry and after you query the defined attributes, you can map the attributes so they match the configured LDAP servers and your business needs.

Perform the following steps to map attributes between WebSphere Portal and your LDAP server; if you have multiple LDAP servers, you will need to perform these steps for each LDAP server:

1. Use a text editor to open the wkplc.properties file, located in the wp_profile_root\\ConfigEngine\\properties directory.

2. For a stand-alone repository, enter a value for the following sets of parameters in the wkplc.properties file to identify your LDAP server. The parameters are found under the LDAP attribute configuration heading:

   > **Note:** Make sure you use the same values you used to configure your LDAP server.

   standalone.ldap.id

   standalone.ldap.host

   standalone.ldap.port

   standalone.ldap.sslEnabled

   standalone.ldap.bindDN

   standalone.ldap.bindPassword

   standalone.ldap.baseDN

   > **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

3. For a stand-alone repository, run the following task from the wp_profile_root\\ConfigEngine directory. This task checks that all defined attributes are available in the configured LDAP user registry:

   ```
   ConfigEngine.sh wp-validate-standalone-ldap-attribute-config -DWasPassword=password
   ```

4. Open the ConfigTrace.log file, located in the wp_profile_root\\ConfigEngine\\log directory, to review the following output for the PersonAccount and Group entity type:

   The following attributes are defined in WebSphere Portal but not in the LDAP server

   This list contains all attributes that are defined in WebSphere Portal but not available in the LDAP. Flag attributes that you do not plan to use in WebSphere Portal as unsupported. Map the attributes that you plan to use to the attributes that exist in the LDAP; you must also map the uid, cn, firstName, sn, preferredLanguage, and ibm-primaryEmail attributes if they are contained in the list.

   The following attributes are flagged as required in the LDAP server but not in WebSphere Portal

   This list contains all attributes that are defined as "MUST" in the LDAP server but not as required in WebSphere Portal. You should flag these attributes as required within WebSphere Portal; see the step below about flagging an attribute as either unsupported or required.

   The following attributes have a different type in WebSphere Portal and in the LDAP server

   This list contains all attributes that WebSphere Portal might ignore because the data type within WebSphere Portal and within the LDAP server do not match.

5. Use a text editor to open the wkplc.properties file, located in the wp_profile_root\\ConfigEngine\\properties directory.
6. For a stand-alone repository, enter a value for the following sets of parameters in the wkplc.properties file to correct any issues found in the config trace file. The following parameters are found under the LDAP attribute configuration heading:

   > **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

standalone.ldap.id

standalone.ldap.attributes.nonSupported

standalone.ldap.attributes.nonSupported.delete

standalone.ldap.attributes.mapping.ldapName

standalone.ldap.attributes.mapping.portalName

standalone.ldap.attributes.mapping.entityTypes

For example, the following values will flag certificate and members as unsupported attributes and will map ibm-primaryEmail to mail and ibm-jobTitle to title for both the PersonAccount andGroup entityTypes:

standalone.ldap.attributes.nonSupported=certificate, members

standalone.ldap.attributes.nonSupported.delete=

standalone.ldap.attributes.mapping.ldapName=mail, title

standalone.ldap.attributes.mapping.portalName=ibm-primaryEmail, ibm-jobTitle

standalone.ldap.attributes.mapping.entityTypes=PersonAccount, Group

7. Save your changes to the wkplc.properties file.
8. For a stand-alone repository, run the following task from the wp_profile_root\\ConfigEngine directory. This tasks updates the LDAP user registry configuration with the list of unsupported attributes and the proper mapping between WebSphere Portal and the LDAP user registry:

```
./ConfigEngine.sh wp-update-standalone-ldap-attribute-config -DWasPassword=password
```

9. Stop and restart the appropriate servers to propagate the changes. For specific instructions, see the following link under Related tasks: Starting and stopping servers, deployment managers, and node agents.
10. Optional: Perform the following steps to flag an attribute as either unsupported or required for the entire WebSphere Portal environment instead of just for the specified LDAP:

    a. Enter a value for the following required parameters in the wkplc.properties file:

    > **Note:** See the properties file for specific information about the required parameters and for advanced parameters.

    user.attributes.required

    user.attributes.nonsupported

    b. Save your changes to the wkplc.properties file.
    c. Run the following task from the wp_profile_root\\ConfigEngine directory:

    ```
    ./ConfigEngine.sh wp-update-attribute-config -DWasPassword=password
    ```

    d. Stop and restart all necessary servers to propagate your changes.

Due to a Virtual Member Manager (VMM) limitation, there is currently no task to update an attribute. Therefore, if you added an attribute to your property extension database or when adapting attributes to match your LDAP server that were spelled incorrectly or already added due to migration, you must remove the attribute from the database. Use caution when performing these steps.

Perform the following steps to remove an attribute from your database:

Note: Do not remove attributes that have already been populated with user values because this can cause database inconsistencies.

Note: In a clustered environment, perform the following steps on the deployment manager and then resynch the nodes.

1. Open the tool you use to edit your database.
2. Verify that your attribute name is available in the LAPROP table.
3. Delete the required attributes from the LAPROP table.
4. Open the wimxmlextension.xml file, located in the wp_profile_root/config/cells/cellname/wim/model directory.
5. Locate and delete the propertySchema definition for the attributes that you deleted from the LAPROP table; for example:

```
<wim:propertySchema nsURI="http://www.ibm.com/websphere/wim" dataType="String"
    multiValued="true" propertyName="attribute_name">
  <wim:applicableEntityTypeNames>PersonAccount</wim:applicableEntityTypeNames>
</wim:propertySchema>
```

6. Save your changes to the wimxmlextension.xml file.
7. Open the wimconfig.xml file, located in the wp_profile_root/config/cells/cellname/wim/config directory.
8. Locate and delete the propertiesNotSupported definitions for the attributes that you deleted from the LAPROP table; for example:

```
<config:propertiesNotSupported name="attribute_name">
```

9. Save your changes to the wimconfig.xml file.
10. Stop and restart the server1 and WebSphere_Portal servers from the wp_profile_root/bin directory.

Configuring LDAP Server for Dynamic Group Queries

By default, WebSphere Portal is enabled for static groups. However, the Virtual Member Manager (VMM) allows users to be members of either static or dynamic groups. Static groups are those where a persistent binding exists between a group and its members. Dynamic groups are those where a search query is defined to retrieve the members of a group. If you have your LDAP server configured to use dynamic groups, complete the steps in this task for WebSphere Portal to use dynamic group queries when you setup your LDAP server.

Perform the required tasks to configure either a stand-alone or federated LDAP server security.

The steps in this task use groupOfURLs as the object class for dynamic groups and memberURL as the dynamic membership attribute. The actual values for object classes and dynamic membership attributes can vary depending on your LDAP server. For this reason, you should export an LDIF file to verify the object classes and dynamic membership attributes. Either refer to your LDAP documentation or ask your LDAP administrator for instructions on exporting an LDIF file.

Note: Perform the following steps on the Deployment Manager then synchronize the nodes.

To configure WebSphere Portal to use dynamic groups, do the following:

1. For stand-alone LDAP server or federated LDAP server(s), perform these steps:

a. Navigate to the following directory: wp_profile_root/cells/cell_name/wim/config.
b. Locate and open wimconfig.xml with any text editor.
c. Add the following line to the <config:groupConfiguration> tag:

```
<config:dynamicMemberAttributes name="memberurl" objectClass="groupofurls"/>
```

d. Save and close wimconfig.xml.

2. Stop and restart the appropriate servers to propagate the changes.

Configuring a Portal to Use LDAP Referrals

Referrals redirect object requests from one LDAP server to another when objects do not exist or cannot be located in a particular directory tree. You should enable referrals if your environment has more than one user registry existing on multiple servers or domains.

To configure your portal to use LDAP referrals, do the following:

1. Use any text editor to open the wkplc.properties file in the following directory: wp_profile_root/ConfigEngine/properties.
2. Specify values for the following parameters:
   - et.ldap.id=ID_of_your_LDAP_server
   - et.ldap.host=hostname_of_your_LDAP_server
   - et.ldap.referral=follow
3. Save and close wkplc.properties.
4. Run the following task from the wp_profile_root/ConfigEngine directory to create an LDAP entity type:

```
./ConfigEngine.bat wp-update-et-ldap -DWasPassword=password
Windows: ./ConfigEngine.sh wp-update-et-ldap -DWasPassword=password
i: ./ConfigEngine.sh wp-update-et-ldap -DWasPassword=password
```

5. Stop and restart the appropriate servers to propagate the changes.

Enabling Security with the LDAP Directory

Once you have enabled security with your LDAP directory, you must provide the user ID and password required for security authentication on WebSphere Application Server when you perform certain administrative tasks with WebSphere Application Server.

For example, to stop the WebSphere Portal application server, you would issue this command:

```
stopServer WebSphere_Portal -user admin_userid -password admin_password
```

Configuring an External HTTP Server for WebSphere Portal v8.5

By default, the installation configures the WebSphere Portal v8.5 to use the internal HTTP transport within the WebSphere Application Server to handle requests (port 10030). Portal also supports the use of an external Web server which is the recommended configuration for production Portals.

This section explains how you can configure an external web server port to communicate with the WebSphere Portal, which includes these tasks:

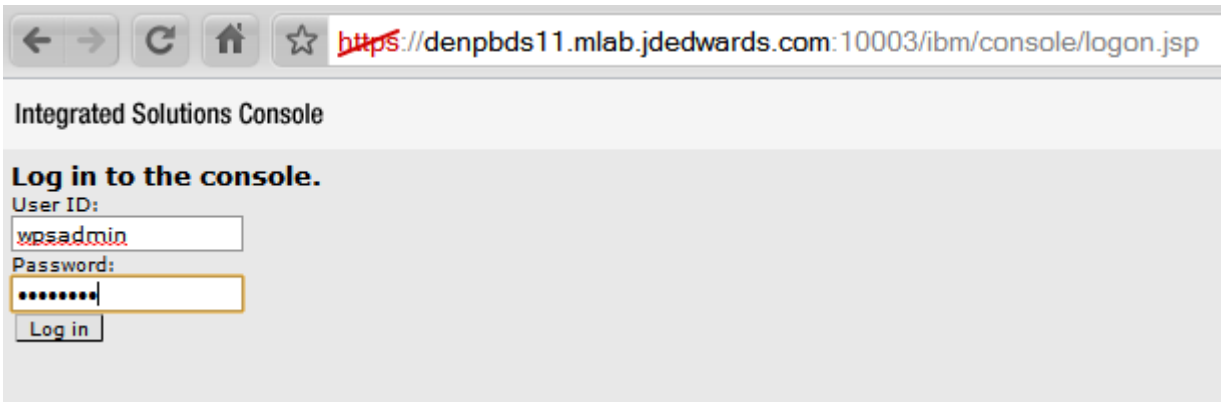
- Creating a webserver definition for the wp_profile
- Remapping the WebSphere portal to the external web server
- Modifying the wpconfig.properties file
- Adding the external port
- Generating the webserver plugin for the wp_profile
- Propagating webserver plugin

Creating a Webserver Definition

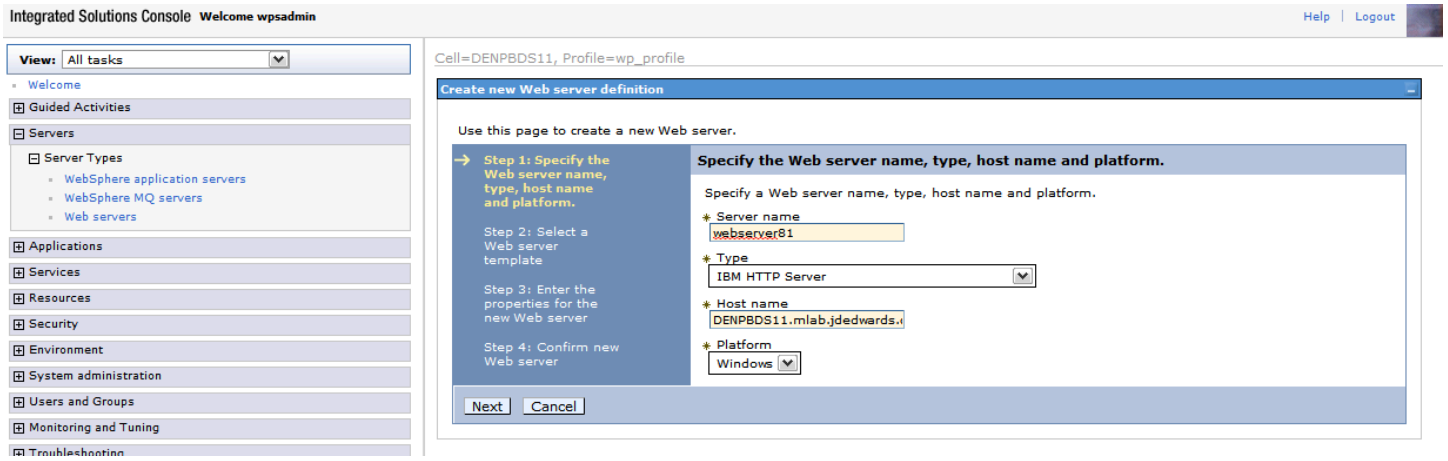
When WebSphere Application Server was initially installed, a webserver definition was created for the WebSphere Application Server profile, known as the default profile. The installation of the WebSphere Portal Server creates a new profile, wp_profile. This profile is a non-default profile. Non-default profiles do not have web server definitions or plugin files created for them at the time of install. To use an external http server with portal, a second webserver definition and its corresponding plugin-cfg.xml file must be created manually for the wp_profile.

To create the new definition:

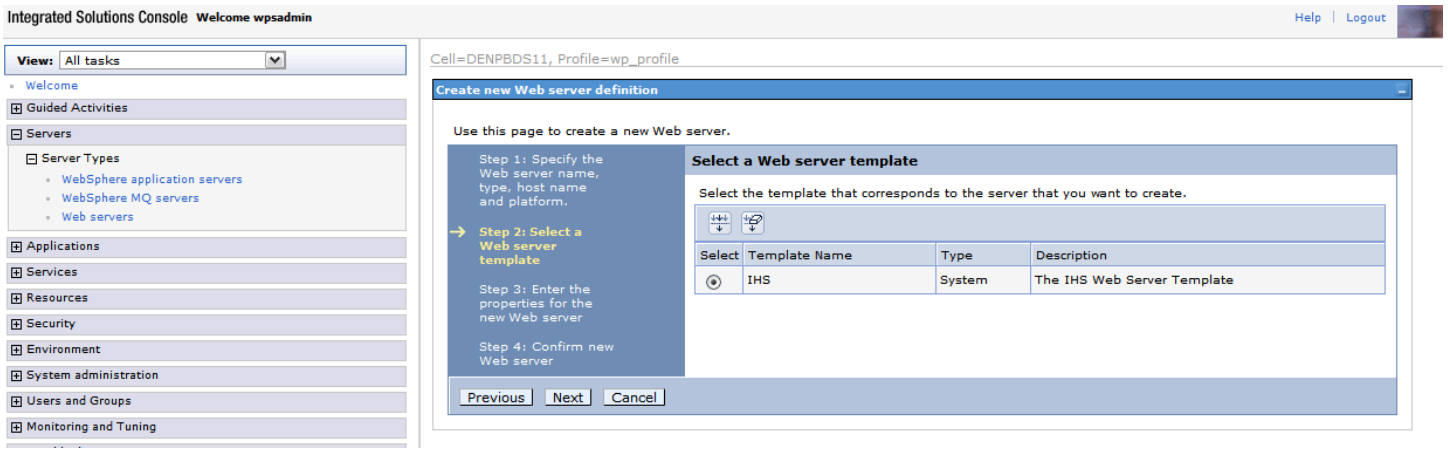
1. Log in to the server1 admin console of the wp_profile, Navigate to servers, webservers, and then click New.



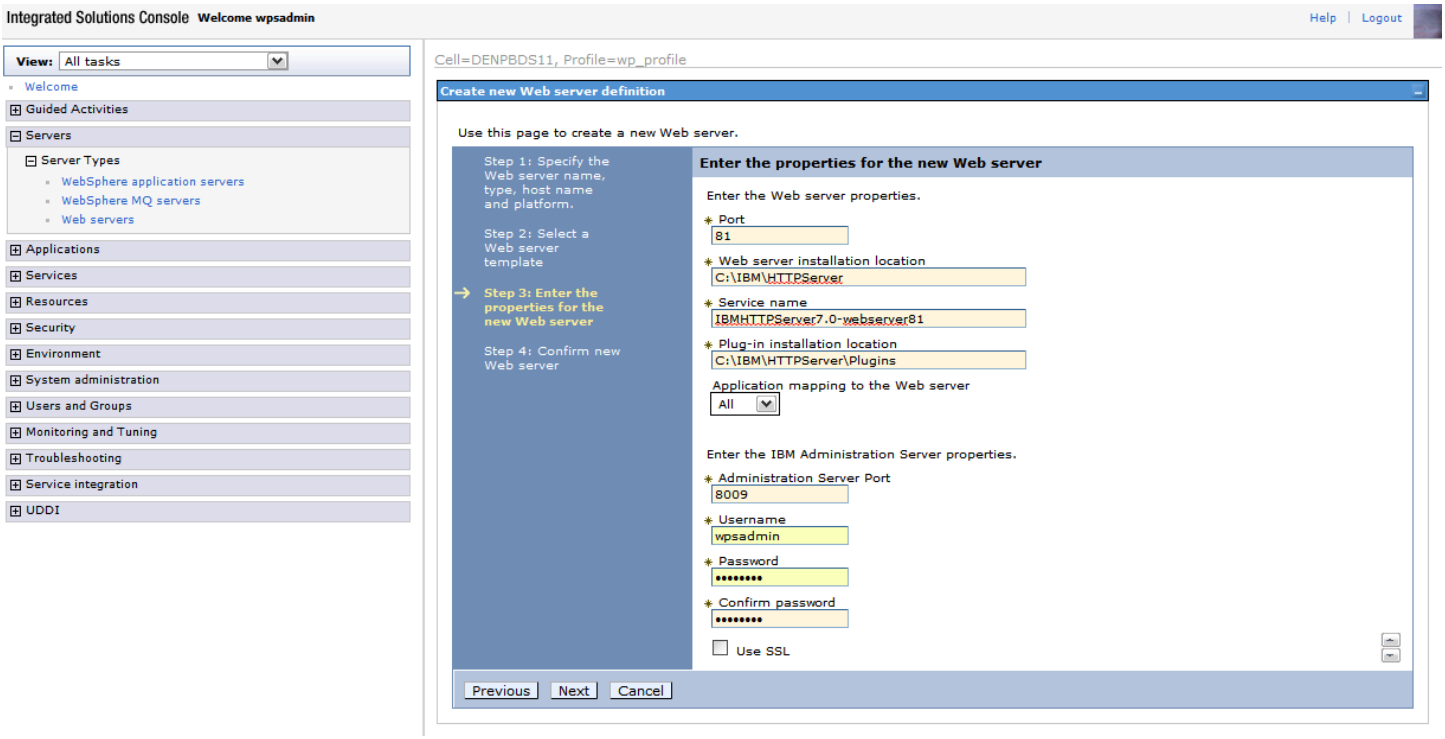
2. Provide the Server name and Host name and the platform, and click Next.



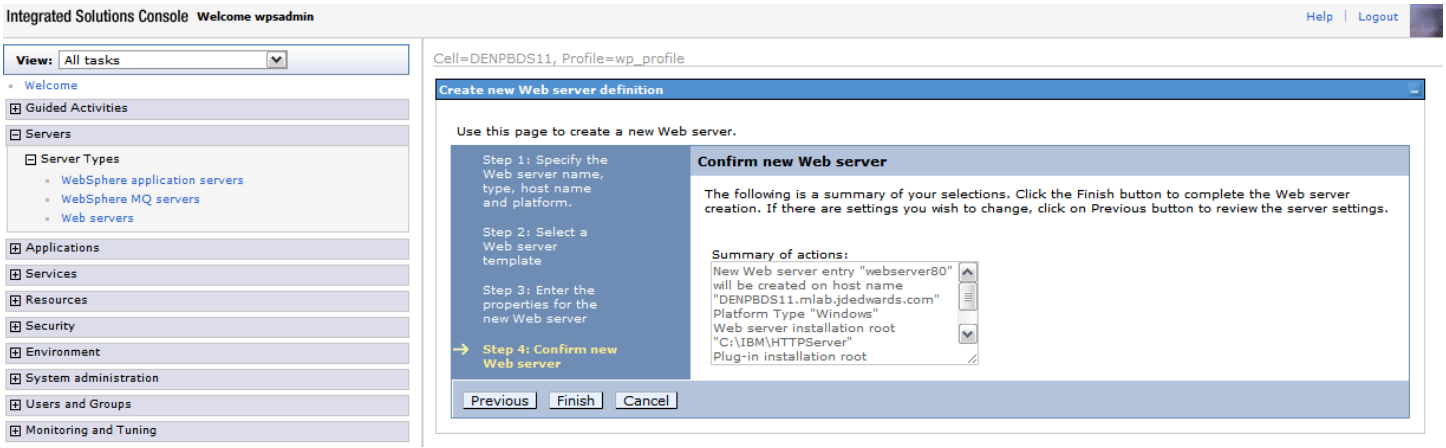
3. Select the IHS Template and proceed by clicking Next.



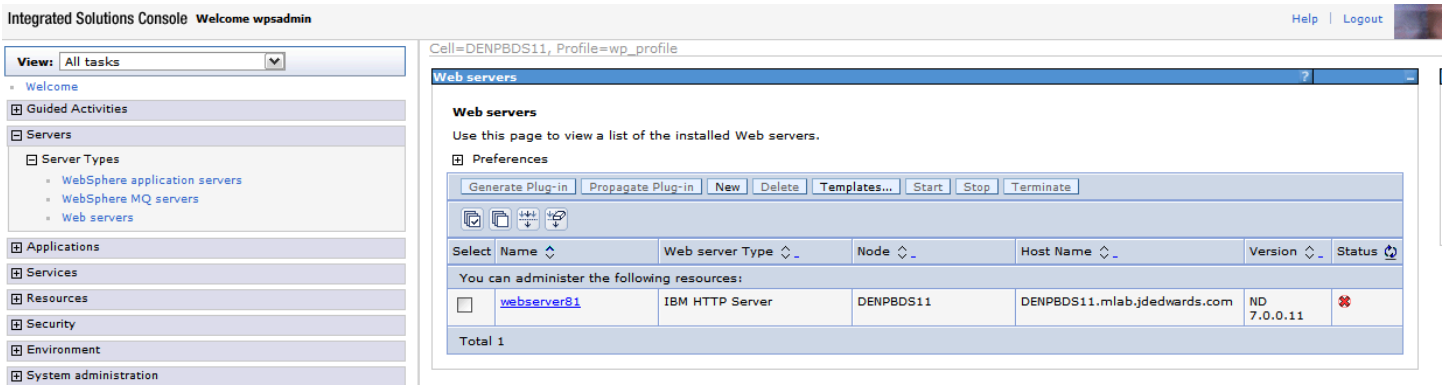
4. Enter details in the following screen to refer to the installation paths, and then click Next.


Integrated Solutions Console Welcome wpsadmin
Help | Logout
View: All tasks
Welcome
Guided Activities
Servers
Server Types
WebSphere application servers
WebSphere MQ servers
Web servers
Applications
Services
Resources
Security
Environment
System administration
Users and Groups
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
Cell=DENPBDS11, Profile=wp_profile
Create new Web server definition
Use this page to create a new Web server.
Step 1: Specify the Web server name, type, host name and platform.
Step 2: Select a Web server template
Step 3: Enter the properties for the new Web server
Step 4: Confirm new Web server
Enter the properties for the new Web server
Enter the Web server properties.
Port
81
Web server installation location
C:\IBM\HTTPServer
Service name
IBMHTTPServer7.0-webserver81
Plug-in installation location
C:\IBM\HTTPServer\Plugins
Application mapping to the Web server
All
Enter the IBM Administration Server properties.
Administration Server Port
8009
Username
wpsadmin
Password
Confirm password
Use SSL
Previous
Next
Cancel

5. Review the information and click Finish.



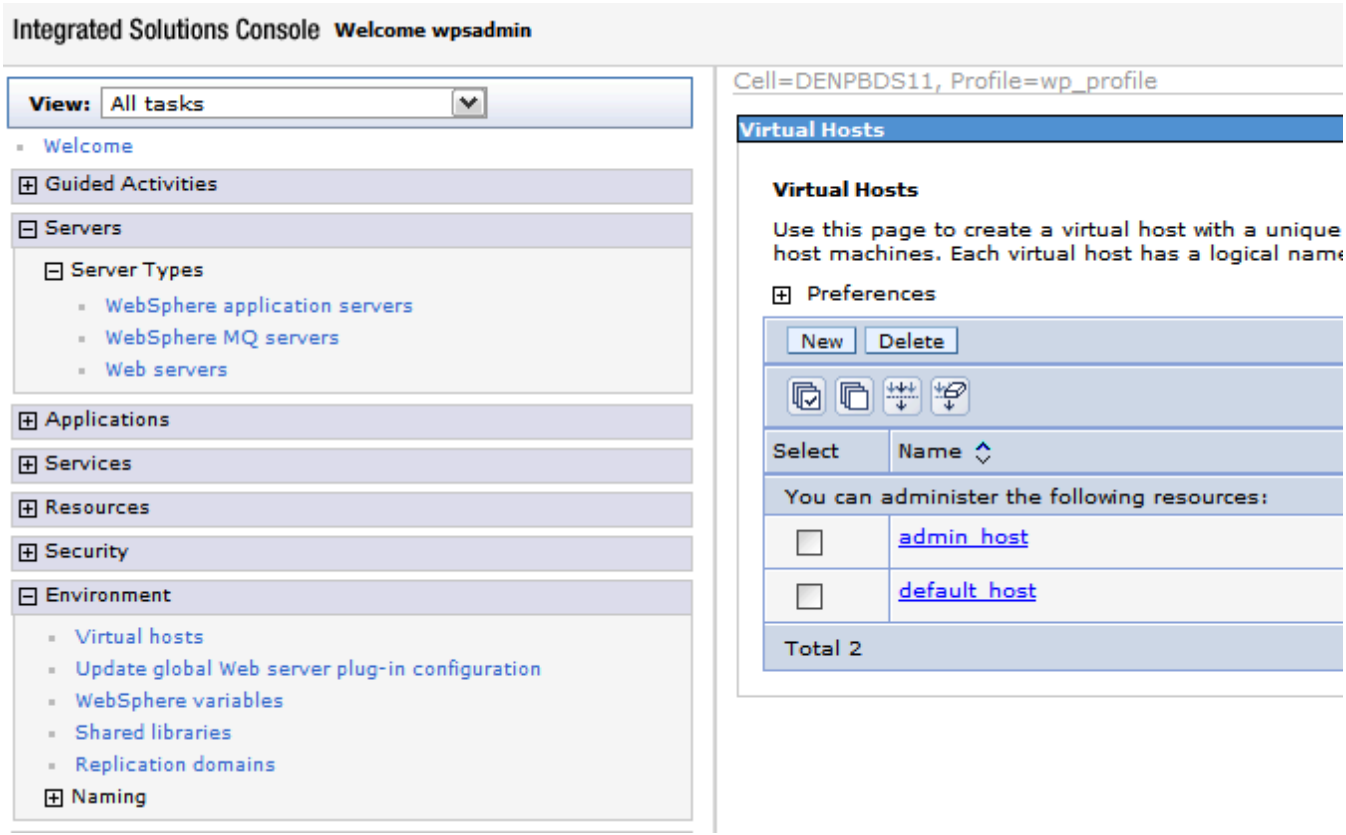
6. In the Web servers page click Save option. After which the following screen appears.



Adding a Virtual Host Definition

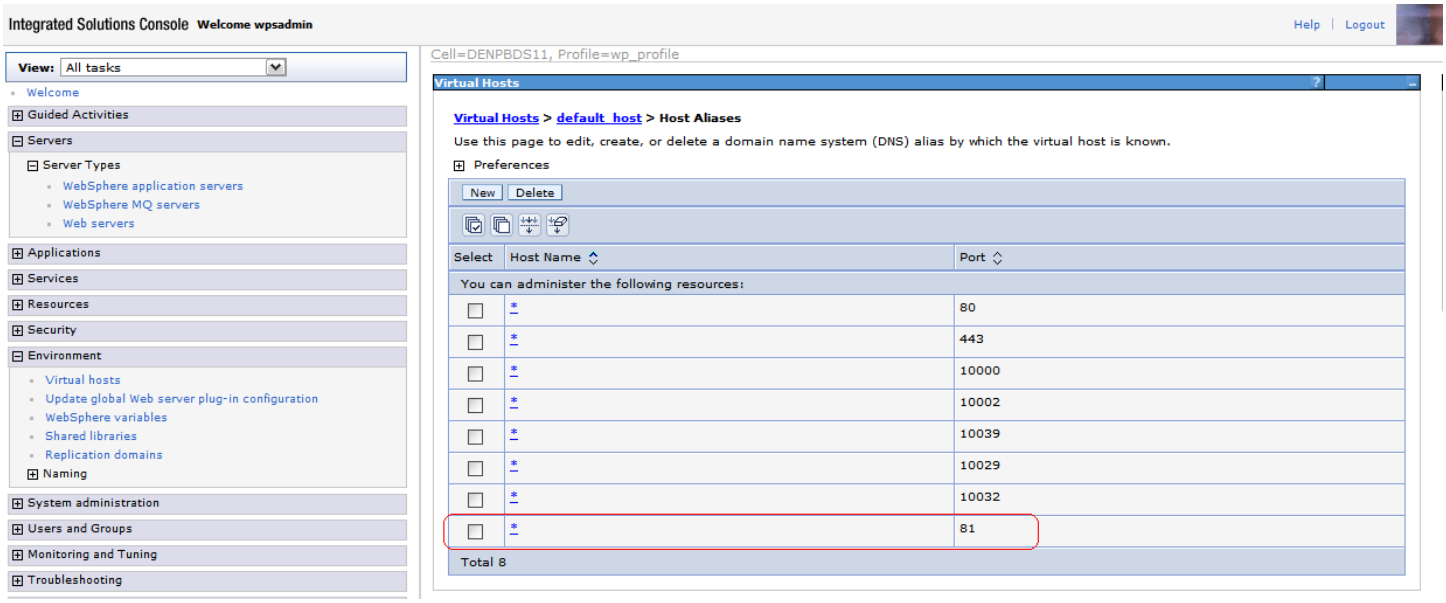
If you want to access WebSphere Portal using a host name and port different from your Web server default (i.e port 80), add the required virtual host definition using the WebSphere Application Server administrative console.

1. Select Environment, Virtual Hosts.



2. Select the **default_host** entry or the entry for the virtual host that is being used to access the WebSphere Portal application.

3. Select **Host Aliases**, and verify whether there is a host name and port entry corresponding to the values used to access WebSphere Portal (for example, *:10039). Select New, and enter the information for the host name and port you want to use. (In the example below port 81 was added.)

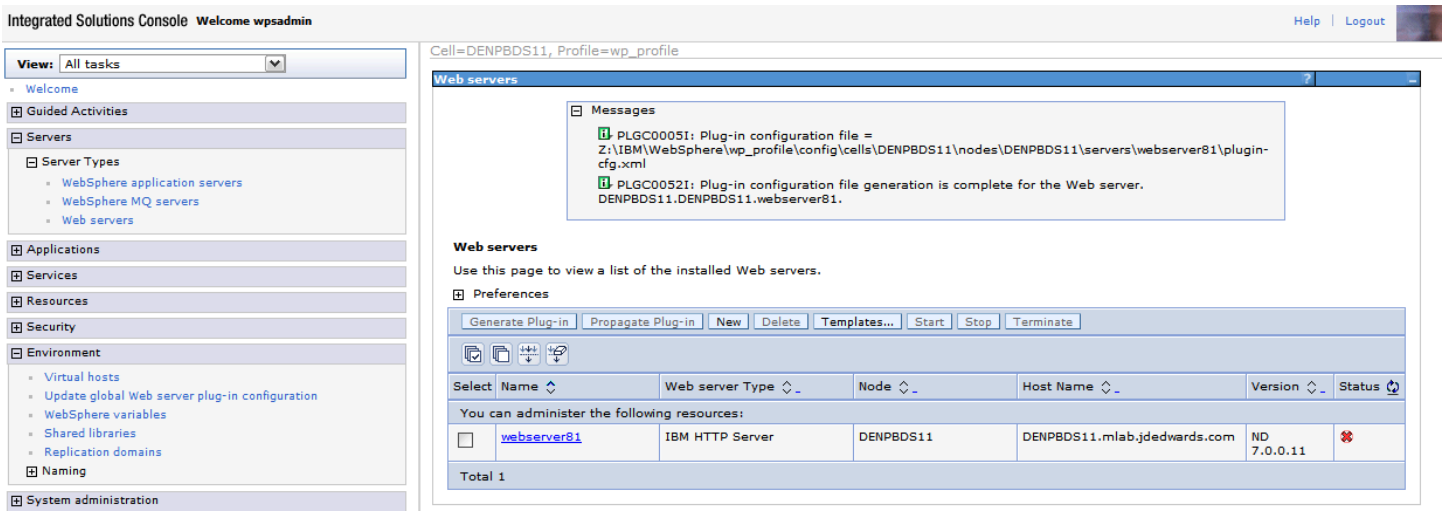


4. Save your changes.

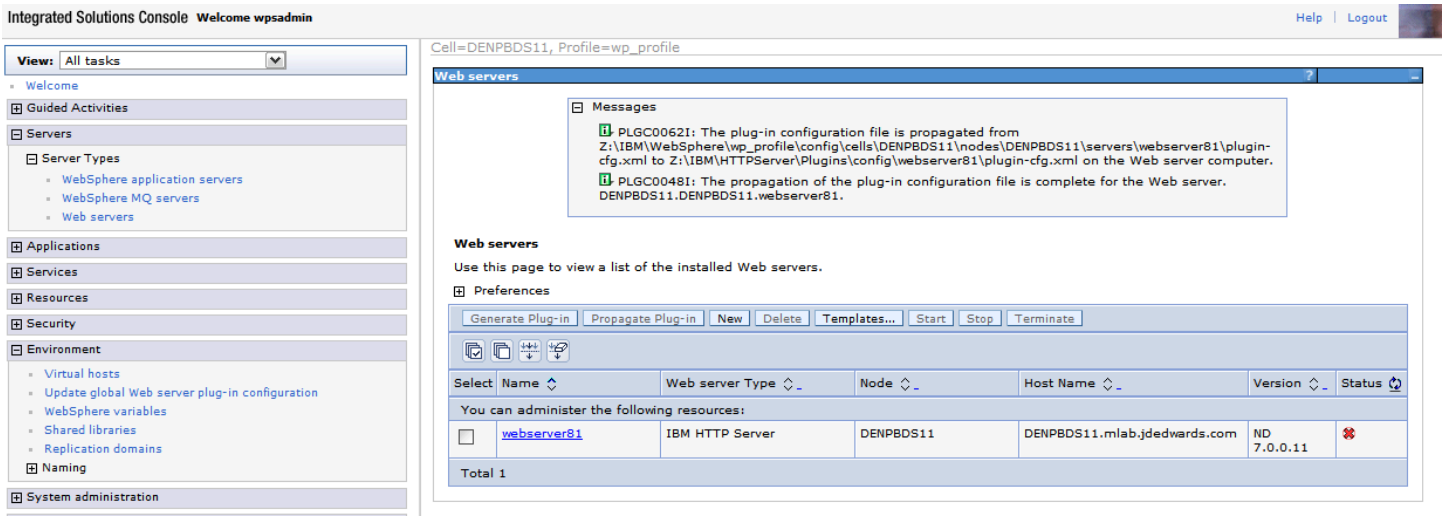
Generate the Web Server Plug-in for wp_profile

To use an external http port to access the portal, you must generate the plugin file with the new changes.

1. From the portal administration console select Servers, Web servers. Select webserver81 which we just created above and click the generate plugin button.



2. From the portal administration console select Servers -> Web servers. Select webserver81 which we just created above and click the propagate plugin button. Note the location of the new plugin that is displayed in the messages section when the generation and propagation completes.



3. Open the httpd.conf file for editing.
4. Add a line for a Listen directive for the external port selected above. For example: Listen 81
5. Locate the entry in the httpd.conf file with the path to the plugin-cfg.xml file. Verify that the path points to the location of the file generated above. If not, change the path to match the file location.

   WebSpherePluginConfig "/u01/IBM/HTTPServer/Plugins/config/wps7httpserver/plugin-cfg.xml"
6. Restart both the Web server (i.e webserver81) and the WebSphere_Portal servers.

Installing the JD Edwards Collaborative Portal

Once the Portal Server is running, you must install the Collaborative Portal, which provides the JD Edwards EnterpriseOne Interface and Portlet Deployment Structure.

Refer to the *JD Edwards EnterpriseOne Tools IBM WebSphere Portal Reference Guide*

8 Appendix A - Start and Stop Portal Servers

Start and Stop Portal Servers

Beginning with Tools release 8.97, management of the application servers can be performed through the JD Edwards EnterpriseOne Server Manager application. This is the recommended method for starting, stopping and configuring application and portal servers. For additional information about Server Manager, refer to the *JD Edwards EnterpriseOne Tools Server Manager Guide* .

The collaborative portal can also be managed through the WebSphere Administration Server and command line commands like previous releases. This remains the only option for JD Edwards EnterpriseOne Xe and ERP8 installations.

Refer to the following Knowledge Document E1: SVM: WebSphere 7.0.0.11 Secure Profile, Server Manager Unable to Detect Status of Servers Correctly (Doc ID 1262748.1) in order for Server Manager to detect the status of WebSphere_Portal server correctly.

> **CAUTION:** The Portal is installed with its own profile which, by default, is wp_profile. When starting and stopping server1 for portal and the WebSphere_Portal server, it is necessary to be in the wp_profile/bin directory. Portal services cannot be managed using the WAS default profile from the profiles/default/bin directory.

Starting and Stopping the WebSphere Portal Administration Server (server1)

To locate the scripts to start and stop the WebSphere Portal Administration Server (server1), navigate to this directory:

```
X:\IBM\WebSphere\AppServer\profiles\<PROFILE_NAME>\bin
```

Starting server1 (Portal Administration Server)

From the above specified /bin directory, you can start server1 by entering this command:

```
startServer server1 -user wpsadmin -password wpsadmin
```

Optionally the server can be started from Windows Services applet (services.msc).

> **Note:** The security user credentials will not be required if you have correctly configured the credentials in the soap.client.props file. This is also a pre-requisite for Server Manager.

Stopping server1 (Portal Administration Server)

From the above specified /bin directory, you can stop server1 by entering this command:

```
stopServer server1 -user wpsadmin -password wpsadmin
```

Optionally the server can be stopped from Windows Services applet (services.msc).

> **Note:** The security user credentials will not be required if you have correctly configured the credentials in the soap.client.props file. This is also a pre-requisite for Server Manager.

Starting and Stopping the WebSphere Portal Server

To locate the scripts to start and stop the WebSphere Portal Server, navigate to this directory:

```
X:\IBM\WebSphere\AppServer\profiles\<PROFILE_NAME>\bin
```

Starting the WebSphere Portal Server

From the above specified /bin directory, you can start the WebSphere Portal Server by entering this command:

```
startServer WebSphere_Portal
```

Optionally the server can be started from Windows Services applet (services.msc).

> **Note:** The security user credentials will not be required if you have correctly configured the credentials in the soap.client.props file. This is also a pre-requisite for Server Manager.

Note: The security user credentials will not be required if you have correctly configured the credentials in the soap.client.props file. This is also a pre-requisite for Server Manager.

Stopping WebSphere Portal Server

From the above specified /bin directory, you can stop the WebSphere Portal Server by entering this command:

```
stopServer WebSphere_Portal -user wpsadmin -password wpsadmin
```

Optionally the server can be stopped from Windows Services applet (services.msc).

Note: The security user credentials will not be required if you have correctly configured the credentials in the soap.client.props file. This is also a pre-requisite for Server Manager.

9 Appendix B - Example of a PortalUsers.ldif File

Example of a PortalUsers.ldif File

This appendix provides an example of a PortalUsers.ldif file. You should edit this file using your company information.

Note: You can find the PortalUsers.ldif template file from the Portal Setup CD.

```
version: 1
# NOTE: you must edit this file before importing it and replace all
# occurrences of the default suffix "dc=yourco,dc=com" with the suffix
# that your LDAP server is configured for.
dn: dc=denver,dc=oracle,dc=com
objectclass: domain
objectclass: top
# Add lines according to this scheme that correspond to your suffix
dc: dc=denver,dc=oracle,dc=com

dn: cn=users,dc=denver,dc=oracle,dc=com
objectclass: container
objectclass: top
cn: users

dn: cn=groups,dc=denver,dc=oracle,dc=com
objectclass: top
objectclass: container
cn: groups

dn: uid=wpsadmin,cn=users,dc=denver,dc=oracle,dc=com
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: inetOrgPerson
uid: wpsadmin
userpassword: wpsadmin
sn: admin
givenName: wps
cn: wps admin

dn: uid=wasadmin,cn=users,dc=denver,dc=oracle,dc=com
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: inetOrgPerson
uid: wasadmin
userpassword: wasadmin
sn: admin
givenName: was
cn: was admin
```

```
dn: uid=wpsbind,cn=users,dc=denver,dc=oracle,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: wpsbind
userpassword: wpsbind
sn: bind
givenName: wps
cn: wps bind

dn: cn=wpsadmins,cn=groups,dc=denver,dc=oracle,dc=com
objectclass: groupOfUniqueNames
objectclass: top
uniquemember: uid=wpsadmin,cn=users,dc=denver,dc=oracle,dc=com
cn: wpsadmins


dn: cn=wpsContentAdministrators,cn=groups,dc=denver,dc=oracle,dc=com
objectclass: groupOfUniqueNames
objectclass: top
uniquemember: uid=wpsadmin,cn=users,dc=denver,dc=oracle,dc=com
cn: wpsContentAdministrators

dn: cn=wpsDocReviewer,cn=groups,dc=denver,dc=oracle,dc=com
objectclass: groupOfUniqueNames
objectclass: top
uniquemember: uid=wpsadmin,cn=users,dc=denver,dc=oracle,dc=com
cn: wpsDocReviewer

dn: cn=wcmadmins,cn=groups,dc=denver,dc=oracle,dc=com
objectclass: groupOfUniqueNames
objectclass: top
uniquemember: uid=wpsadmin,cn=users,dc=denver,dc=oracle,dc=com
cn: wcmadmins
```

10 Glossary

DBCA

An abbreviation for Database Configuration Assistant.

JAR file

JAR files are a Java Archive and are built based on the ZIP file format and use the .jar file extension. This format is typically used to combine Java class files and associated metadata and resources into one file that can distribute application software or libraries for the Java platform.

JDBC

An abbreviation for Java Database Connectivity. The JDBC Connector is a program that allows different databases to be accessed by Java application servers that are run on the J2EE platform.

LDAP directory

LDAP is an abbreviation for Lightweight Directory Access Protocol. This directory is a data store for user data, such as the user ID, password, and user name.

MTR

An abbreviation for Minimum Technical Requirements.

WAR file

A WAR file is a Web application ARchive is a JAR file used to for the distribution of JavaServer Pages, Java Servlets, Java classes, XML files, tag libraries and static Web pages that comprise a Web application.

WAS

An abbreviation for WebSphere Application Server.