

Content Server

Version: 6.3

Installing Content Server with WebSphere Application Server

Document Revision Date: Jun. 15, 2011

FatWire[®]
S O F T W A R E

FATWIRE CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall FatWire be liable for any loss of profits, loss of business, loss of use of data, interruption of business, or for indirect, special, incidental, or consequential damages of any kind, even if FatWire has been advised of the possibility of such damages arising from this publication. FatWire may revise this publication from time to time without notice. Some states or jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

Copyright © 2005–2011 FatWire Corporation. All rights reserved.

This product may be covered under one or more of the following U.S. patents: 4477698, 4540855, 4720853, 4742538, 4742539, 4782510, 4797911, 4894857, 5070525, RE36416, 5309505, 5511112, 5581602, 5594791, 5675637, 5708780, 5715314, 5724424, 5812776, 5828731, 5909492, 5924090, 5963635, 6012071, 6049785, 6055522, 6118763, 6195649, 6199051, 6205437, 6212634, 6279112 and 6314089. Additional patents pending.

FatWire, Content Server, Content Server Bridge Enterprise, Content Server Bridge XML, Content Server COM Interfaces, Content Server Desktop, Content Server Direct, Content Server Direct Advantage, Content Server DocLink, Content Server Engage, Content Server InSite Editor, Content Server Satellite, and Transact are trademarks or registered trademarks of FatWire Corporation in the United States and other countries.

iPlanet, Java, J2EE, Solaris, Sun, and other Sun products referenced herein are trademarks or registered trademarks of Sun Microsystems, Inc. *AIX, IBM, WebSphere*, and other IBM products referenced herein are trademarks or registered trademarks of IBM Corporation. *WebLogic* is a registered trademark of BEA Systems, Inc. *Microsoft, Windows* and other Microsoft products referenced herein are trademarks or registered trademarks of Microsoft Corporation. *UNIX* is a registered trademark of The Open Group. Any other trademarks and product names used herein may be the trademarks of their respective owners.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>) and software developed by Sun Microsystems, Inc. This product contains encryption technology from Phaos Technology Corporation.

You may not download or otherwise export or reexport this Program, its Documentation, or any underlying information or technology except in full compliance with all United States and other applicable laws and regulations, including without limitation the United States Export Administration Act, the Trading with the Enemy Act, the International Emergency Economic Powers Act and any regulations thereunder. Any transfer of technical data outside the United States by any means, including the Internet, is an export control requirement under U.S. law. In particular, but without limitation, none of the Program, its Documentation, or underlying information of technology may be downloaded or otherwise exported or reexported (i) into (or to a national or resident, wherever located, of) Cuba, Libya, North Korea, Iran, Iraq, Sudan, Syria, or any other country to which the U.S. prohibits exports of goods or technical data; or (ii) to anyone on the U.S. Treasury Department’s Specially Designated Nationals List or the Table of Denial Orders issued by the Department of Commerce. By downloading or using the Program or its Documentation, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list or table. In addition, if the Program or Documentation is identified as Domestic Only or Not-for-Export (for example, on the box, media, in the installation process, during the download process, or in the Documentation), then except for export to Canada for use in Canada by Canadian citizens, the Program, Documentation, and any underlying information or technology may not be exported outside the United States or to any foreign entity or “foreign person” as defined by U.S. Government regulations, including without limitation, anyone who is not a citizen, national, or lawful permanent resident of the United States. By using this Program and Documentation, you are agreeing to the foregoing and you are representing and warranting that you are not a “foreign person” or under the control of a “foreign person.”

Installing Content Server with WebSphere Application Server

Document Revision Date: Jun. 7, 2011

Product Version: 6.3

FatWire Technical Support

www.fatwire.com/Support

FatWire Headquarters

FatWire Corporation
330 Old Country Road
Suite 303
Mineola, NY 11501
www.fatwire.com

Table of Contents

1	Installation Overview	5
	What This Guide Covers	6
	Installation Summary	6
	System Requirements	6
	Acronyms in This Guide	7
	Graphics in This Guide	7
2	Installing and Configuring Content Server	9
	Pre-Installation Steps	10
	Installing Content Server	12
	Installing Content Server in a Managed Environment	16
	Post-Installation Steps	20

Appendices

A.	Installing WebSphere Portal Server and Network Deployment Server	43
	Installing WebSphere Portal Server	44
	Installing WebSphere Network Deployment Server	45
B.	Configuring Web Servers and WAS JDBC Providers	47
	Configuring Apache	48
	Configuring IIS	48
	Configuring WAS JDBC Providers	49
C.	Creating and Installing Self-Signed Certificates	51
	Creating a Self-Signed Certificate	52
	Installing a Self-Signed Certificate	53

D. Installing and Configuring the Directory Server for Content Server	55
Installing the Directory Server	56
Configuring the Directory Server	56
E. Integrating LDAP with Network Deployment and WebSphere_Portal	69
LDAP Integration Procedures	70
wpconfig.properties	71
F. Debugging Procedures	73
Connecting to WebSphere Application Server	74
Resolving Content Server Installation Problems.	74
Removing All Files and Tables	74
Resolving HelloCS and pingdb Problems	75
Turning on Debugging.	76

Chapter 1

Installation Overview

This document provides guidelines for installing Content Server on the WebSphere Application Server with IIS or Apache, and connecting to the supported database of your choice.

Note

Anyone using this guide is expected to have experience installing and configuring databases, web servers, and application servers. Selected information regarding the configuration of third-party products is given in this guide. For detailed information about a particular third-party product, refer to that product's documentation.

This chapter provides information that will help you prepare for the Content Server installation. It contains the following sections:

- [What This Guide Covers](#)
- [Installation Summary](#)
- [System Requirements](#)
- [Acronyms in This Guide](#)
- [Graphics in This Guide](#)

What This Guide Covers

This guide covers the following topics:

- Installation, configuration, and maintenance of WebSphere Application Server, as required to support Content Server in a web or portal environment.
- Installation of Content Server in non-clustered environments (where application servers act independently of each other) and clustered environments (where multiple application servers act concurrently to fulfill requests).

Installation Summary

After you install and configure the J2EE components that support Content Server, you will run the Content Server installer, which will guide you through the installation process. You will run the installer on each development, delivery, and management system on which you plan to use Content Server. During the Content Server installation, you will have the option to install or bypass sample sites and sample content, depending on the system you are setting up and on your business needs.

If you are creating a portal installation, you will perform LDAP integration by using the Content Server installer. For web installations, LDAP integration is optional and must be completed after the Content Server installation is successfully running.

Note

The names of the systems in your Content Server environment might vary from the names used in this document. Generally, the management system is also called “staging,” and the delivery system is also called “production.”

System Requirements

System requirements for installing Content Server are given in the following documents, located on your Content Server installation CD:

- *Content Server Supported Platform List*. The list specifies third-party databases and drivers, application servers and web servers, and other software required for installing and running Content Server.
- *Content Server Release Notes*. The notes provide important information about Content Server.

FatWire recommends that you read both of these documents before installing Content Server.

Note

The latest versions of the above-mentioned documents are located at the following URL (password-protected):

<http://e-docs.fatwire.com/CS>

If you need a password, contact FatWire Technical Support. Contact information is available at the following URL:

http://www.fatwire.com/Support/contact_info.html

The e-docs website is organized by product and version number. To obtain the correct documents, follow the link for the version of Content Server you are installing.

Acronyms in This Guide

Term	Definition
ND	Network Deployment
SSL	Secure Sockets Layer
WAS	WebSphere Application Server
WAS ND	WebSphere Application Server Network Deployment

Graphics in This Guide

Many steps in this guide include screen captures of dialog boxes and similar windows that you interact with in order to complete the steps. The screen captures are presented to help you follow the installation process. They are not intended to be sources of specific information, such as parameter values, options to select, or product version number.

Chapter 2

Installing and Configuring Content Server

This chapter provides the steps that you need to complete to install Content Server. It contains the following sections:

- [Pre-Installation Steps](#)
- [Installing Content Server](#)
- [Installing Content Server in a Managed Environment](#)
- [Post-Installation Steps](#)

Pre-Installation Steps

The following steps instruct you to install the third-party products that support Content Server.

To install Content Server's supporting software

1. Make sure that you have licensed copies of all the software you will be installing.

For information about Content Server's supporting software, refer to the latest *Content Server Supported Platform List* and to *Release Notes*. Both are available on the e-docs website (password-protected), at the URL that is given in "[System Requirements](#)," on page 6.

2. Install Apache or IIS. For installation instructions, consult the product vendor's documentation and our configuration guide, *Third-Party Software*.
3. Install, create, and configure a database:

Content Server requires access to a supported database that is specifically configured for Content Server. Before installing any other of Content Server's supporting software, you must complete the following steps:

- a. Install the database management system.
- b. Create a database for Content Server.
- c. Configure the database.

For instructions on installing the database, refer to the product vendor's documentation. For instructions on creating and configuring the database for Content Server, consult our configuration guide, *Third-Party Software*. Note that database configuration is identical across different application servers. Refer to the correct chapter to set up the database of your choice. The end of each chapter guides you to the next step in the Content Server installation procedure.

4. Install WebSphere 5.1.x (referred to as WAS throughout this guide). For an installation example, see [Appendix A, "Installing WebSphere Portal Server and Network Deployment Server"](#). For detailed instructions, refer to the product vendor's documentation.

Note

Installing WebSphere installs the application server, the portal, and WAS Network Deployment.

5. Do one or all of the following, depending on the type of installation you are creating:
 - If you are installing Content Server as a web application, install the application server. For an installation example, see [Appendix A, "Installing WebSphere Portal Server and Network Deployment Server"](#). For detailed instructions, refer to the product vendor's documentation.
 - If you are installing Content Server on a portal, install the portal server and the Network Deployment server. For instructions, see [Appendix A, "Installing WebSphere Portal Server and Network Deployment Server"](#).

- If you are installing a cluster, install the Network Deployment server. For instructions, see [“Installing WebSphere Network Deployment Server,”](#) on page 45.”
6. Set up IIS or Apache to connect to WAS.
This is performed by the WAS installer. However, if the web server is located on a separate machine (suggested), you will need to make the necessary changes manually. If you need instructions, see [Appendix B, “Configuring Web Servers and WAS JDBC Providers”](#) (specifically [“Configuring Apache”](#) or [“Configuring IIS,”](#) both on page 48).
 7. If you are not using one of the JDBC drivers provided with WebSphere, download the JDBC driver required for your database configuration. If you are using MS SQL Server 2000 as the database, use the WebSphere Embedded ConnectJDBC driver for MS SQL Server.
 8. Configure the JDBC provider in WAS. If you need instructions, see [“Configuring WAS JDBC Providers,”](#) on page 49.
 9. If you need to configure international language support for Content Server in WAS, complete the following steps:
 - a. Change to the following directory:
`<WAS install>/AppServer/bin`
 - b. Open `startServer.sh` or `startServer.bat` for editing. For example:
 - Windows: **notepad startServer.bat**
 - UNIX: **vi startServer.sh**
 - c. Go to the line `"-Dwas.install.root=%WAS_HOME%"` and on the next line insert: **"-Dfile.encoding=UTF-8"**

For example, the original lines are as follows:

```
"%JAVA_HOME%\bin\java" %WAS_TRACE% %DEBUG% %CONSOLE_ENCODING%
"%CLIENTSAS%" "-classpath" "%WAS_CLASSPATH%"
"-Dws.ext.dirs=%WAS_EXT_DIRS%" %USER_INSTALL_PROP%
"-Dwas.install.root=%WAS_HOME%"
"-Dibm.websphere.preload.classes=true"
"com.ibm.ws.bootstrap.WSLauncher"
"com.ibm.ws.management.tools.WsServerLauncher" "%CONFIG_ROOT%"
"%WAS_CELL%" "%WAS_NODE%" %*
```

The edited set of lines should look as follows (the inserted line is in boldface type):

```
"%JAVA_HOME%\bin\java" %WAS_TRACE% %DEBUG% %CONSOLE_ENCODING%
"%CLIENTSAS%" "-classpath" "%WAS_CLASSPATH%"
"-Dws.ext.dirs=%WAS_EXT_DIRS%" %USER_INSTALL_PROP%
"-Dwas.install.root=%WAS_HOME%"
"-Dfile.encoding=UTF-8"
"-Dibm.websphere.preload.classes=true"
"com.ibm.ws.bootstrap.WSLauncher"
"com.ibm.ws.management.tools.WsServerLauncher" "%CONFIG_ROOT%"
"%WAS_CELL%" "%WAS_NODE%" %*
```

- d. Save the file.

10. Install a self-signed certificate if one is required for your installation. If you need instructions, see [Appendix C, “Creating and Installing Self-Signed Certificates.”](#)
11. If you are installing a portal, do the following:
 - a. Install and configure the Directory Server. For instructions, see [Appendix D, “Installing and Configuring the Directory Server for Content Server.”](#)
 - b. Configure the portal for use with Content Server. For instructions, see [“Setting Up the Content Server Portal \(Portal Installations Only\),”](#) on page 22.
 - c. Install LDAP with ND and WebSphere_Portal. For instructions, see [Appendix E, “Integrating LDAP with Network Deployment and WebSphere_Portal.”](#)
12. You are now ready to install Content Server. Continue with the next section.

Installing Content Server

This procedure shows how to install Content Server. Follow this procedure when you need to install Content Server in a non-clustered environment, or when you need to create a Content Server instance that will serve as the primary member of a cluster installation.

1. If you have not already done so, complete the procedures in [“Pre-Installation Steps,”](#) on page 10.
2. Extract the Content Server installation files by completing the following steps:
 - a. Create a temporary directory. For example:
 - Windows: `md c:\temp\CS`
 - UNIX: `mkdir /tmp/CS`
 - b. Change to the temporary directory you created. For example:
 - Windows: `cd c:\temp\CS`
 - UNIX: `cd /tmp/CS`
 - c. Copy the Content Server archive file to the target machine (this is the machine on which you are going to install Content Server). For example:
 - Windows: `copy ContentServer.zip c:\temp\cs`
 - UNIX: `cp ContentServer.tar.gz /tmp/cs`
 - d. Decompress the archive you copied in [step c](#) into the temporary directory. For example:
 - Windows, using jar: `jar -xf ContentServer.zip`
 - Windows, using WinZip: right-click and select **Winzip > Extract to here**
 - UNIX, using gzip: `gzip -d ContentServer.tar.gz`
 - UNIX, using tar: `tar -xf ContentServer.tar`

3. Ensure that your path is set to use the correct JRE by opening a command prompt and entering:
 - Windows: `Set Path = <WAS Install Directory>\java\bin;%Path%`
 - UNIX: `export Path = <WAS Install Directory>\java\bin:$PATH`
4. Change the directory to the location of the Content Server Installer and run:
 - Windows: `CombinedInstall.bat`
 - UNIX: `sh ./CombinedInstall.sh`
5. The first screen of the installer is displayed. Complete the following steps:
 - a. In the “Welcome to Installation” screen, select **Install FatWire Products** and click **Next**.
 - b. In the “Installation Directory” screen, browse to the location where you want to install Content Server and click **Next**.

Note that this location is where the application will be installed, not where WAS will deploy the product.
 - c. In the “Select Products to Install” screen, select the products to install: **Content Server v6.3** and **Content Server Applications v6.3**. Click **Next**.
 - d. In the “Installation Type” screen, select **Single Server** and click **Next**.
 - e. In the “Installation Options” screen, do the following:
 - 1) Choose the options that are appropriate for your installation. In most situations, particularly on delivery (production) systems, you do not need to select any of the options.
 - 2) Select **No** for the Property Editor display option. (If you need to modify property values, you can start the Property Editor manually after the installation is complete.) For more information about the Property Editor, see the *Content Server Property Files Reference*.
 - 3) Click **Next**.
 - f. In the “Content Server Configuration” screen, enter the password you wish to use for Content Server (the default is `password`) and click **Next**.
 - g. In the “Satellite Server Configuration” screen, enter the password you wish to use for Satellite Server (the default is `password`) and click **Next**.
 - h. In the “Shared Folder Root” screen, select a shared folder root. You can use the default for most non-clustered installations. Click **Next**.
 - i. In the “Web Server Configuration” screen, enter the name of this server (or IP address) and the port you are running on.

You can install directly against WAS or against the web server.
 - j. In the “Platform Type” screen, select **Application Server Platform** and click **Next**.
 - k. In the “Application Server” screen, select **WebSphere 5.1** and click **Next**.
 - l. On the machine’s file system, create a directory structure called `ContentServer.ear\cs.war` under `<WAS Install directory>\InstalledApps\<Your node name>`

- m. In the “WebSphere Deployment Root” screen, do the following:
 - 1) Browse to where you are going to install Content Server.
 - 2) Select the directory created in [step 1](#) as your installation path.
 - 3) Enter the name of the node you located in [step 1](#).
 - 4) Optional: Change the Web Application Path (the context root).
 - 5) Click **Next**.
- n. In the “Database Configuration” screen, do the following:
 - 1) Select your database type (such as **MS SQL Server**) from the drop-down list.
 - 2) Select the data source that was created when WAS was set up.

Note

The correct data source must be selected for the installation to work.

- 3) Click **Next**.
- o. In the “Server Installation Options” screen, you can select any or all of the options. Select the options that are appropriate for your installation, and click **Next**.
- p. In the “Installation Mode” screen, do one of the following:
 - Select **Content Management** if you are installing Content Server on either a development or management (staging) system *and* you wish to install sample sites and their assets on the system. (By selecting **Content Management**, you allow sample sites and assets to be installed later in the installation process.) Click **Next**.
 - Do not select **Content Management** if you are installing Content Server on a delivery (production) system, or any system where sample sites and assets are unnecessary. (By deselecting **Content Management**, you prevent sample sites and assets from being installed.) Click **Next**.
- q. If you did not select the **Content Management** installation option, skip to [step s](#). Otherwise, continue with the next step.
- r. If you selected the **Content Management** installation option and want sample sites and assets to be installed on the Content Server system, do the following:
 - 1) In the “CS-Site Launcher Prototypes” screen, select the site you want to install, then click **Next**.

Note

FirstSite provides a collection of standard templates and site components that developers can use to learn best practices and implement their web site projects. FirstSite also exemplifies a site that is designed for replication.

- 2) In the “Sample Asset Types” screen, select all asset types and click **Next**.

B. Installing Content Server on a Managed Server

1. Install the WebSphere Network Deployment version (and appropriate patches) so that it matches the version of your WAS installation. For instructions, see [“Installing WebSphere Network Deployment Server,”](#) on page 45.

Note

Often, the WebSphere Network Deployment server will not start properly because, by default, it installs on the same ports as the WebSphere Application Server. It is therefore suggested that you select a set of custom ports for this server during the installation.

2. If you are installing a portal, complete [steps a–d](#), below. Otherwise, skip to [step 3](#).
 - a. Install Directory Server. This will require you to install either a version of DB2 that is part of the distributed file, or else a local full version of DB2. This step is completely independent of the other steps, but needs to be completed before [step 5](#). We suggest that you first complete the installation of the Directory Server.
 - b. Install WebSphere Portal Server and patch it to the correct version. This is relatively straight forward, but very time consuming. For instructions, see [Appendix D, “Installing and Configuring the Directory Server for Content Server.”](#)
 - c. Install WebSphere Network Deployment, and patch it to the correct version. For instructions, see [Appendix A, “Installing WebSphere Portal Server and Network Deployment Server.”](#)
 - d. Integrate the Portal server with the Network Deployment server by using the `addNode` command. For instructions, continue with [steps 3](#) and [4](#) in this procedure.
3. Modify WAS Network Deployment server for `addNode` to succeed:
 - a. Change the Network Deployment server from allocating `-Xmx256` to allocating `-Xmx512` as follows:
 - 1) Select **System Administration > Deployment Manager > Process Definition > Java Virtual Machine**
 - 2) Set Initial Heap Size to 256.
 - 3) Set Maximum Heap Size to 512.
 - b. Check that the files `cmm.jar` and `cmmImpl.jar` do not exist in `<ND root>/lib`.
 - If the files exist in `<ND root>/lib`, copy them to `<App Server root>/lib` and change their permissions to: 655
 - If the files do not exist in `<ND root>/lib`, continue with the next step.
4. Modify WAS Portal for `addNode` to succeed:
 - a. Edit `addNode.sh` by inserting `-Xmx512` as a new line into the `addNode.sh` script, as shown below.
Original line: `"$JAVA_HOME"/bin/java \`

New line: `-Xmx512m \`

Original line: `-Xbootclasspath/p:"$WAS_BOOTCLASSPATH" \`

Note

Remember that you will also have WebSphere_Portal and server1 running at the same time. Make sure there is enough memory for both to run simultaneously.

- b. Stop the Network Deployment and Portal servers, then restart the Network Deployment server. Locate the port on which Network Deployment is listening for SOAP requests:

The SOAP port can be found by looking in Network Deployment admin at **Application Servers > WebSphere_Portal > End Points > SOAP Connector Address**.

- c. On the application server that is integrated with the portal (in `<was home>\bin`) run the following command:

```
./addNode.sh <ip address of dmgr> <soap port of dmgr> \
  -conntype SOAP -includeapps -trace
```

If the operation is successful, the nodes are added to WAS ND.

- d. Log in to Network Deployment admin server and do the following:
 - 1) If the Enterprise Application `wpsAdminConsole` is present, remove it from Network Deployment and save your changes. Make sure the sync nodes checkbox is selected.
 - 2) Modify Virtualhost entries by adding the ports used by server1 and WebSphere_Portal (as these are not present in Network Deployment), and save your changes. Make sure the sync nodes checkbox is selected.

Note

At this point, the original server should no longer be started with `startServer.sh <server name>`, but should be started with the `startNode.sh` command located in the same location.

5. Enable LDAP security and integration with Portal Server, and complete the Portal Server upgrade to version 5.1.0.1. For instructions, see [Appendix E, “Integrating LDAP with Network Deployment and WebSphere_Portal.”](#)
6. Install Content Server. For instructions, see “[Installing Content Server](#),” on page 12.
7. Verify the installation. For instructions, see step “[A. Testing Your Installation \(Web Applications and Portals\)](#),” on page 20.
8. Configure the portlets. For instructions, see “[Setting Up the Content Server Portal \(Portal Installations Only\)](#),” on page 22.
9. Set up the cluster. For instructions, see the next section, “[Setting Up a Cluster.](#)”

C. Setting Up a Cluster

1. Create a new cluster by completing the following steps:
 - a. Select **Server > Clusters**.
 - b. Click the **New** button in the right-hand pane.
 - c. Enter a name for the cluster.
 - d. From the drop-down menu, select the `WebSphere_Portal` server that you imported in step 4d2 (“Modify Virtualhost entries,” directly above the preceding note).
 - e. Click **Next**.
 - f. In the next screen (which prompts you to create new clustered servers), click **Next**.
 - g. Click **Finished**.

You have now created a cluster with a single server, which will be used as a template for creating all other cluster members.
2. Add a member to the cluster by completing the following steps (this will create a new server instance):
 - a. In the left-hand tree, select **Server > Clusters**.
 - b. In the right-hand pane, click the cluster created in [step 1](#).
 - c. Click **Cluster Members**.
 - d. Click the **New** button.
 - 1) Enter a name for the new member.
 - 2) Click **Next**.
 - e. Click **Finished**.
3. Restart the cluster by completing the following steps:
 - a. In the left-hand tree, select **Servers > Clusters**.
 - b. Select the cluster created in [step 1](#) and click **Stop**.
 - c. With the cluster created in [step 1](#) still selected, click **Start**.

Note

A new server instance with the Content Server application now exists. Do not try to connect to the new instance at this point (this instance is not yet usable).

4. Repeat all the steps in “[Installing Content Server](#),” on [page 12](#). Perform the steps **exactly as you performed them in that procedure**, but with the following exceptions:
 - a. In the “Installation Directory” screen, select a directory other than the one used in the previous Content Server installation.
 - b. In the “Installation Type” screen, select **Cluster Member**.

- c. In the “Shared Directory Root” screen, select the same location used for the previous installation.
 - d. In the “Web Server Configuration” screen, use the IP address and port of the server you created in [steps 1 and 2](#) of this procedure.
 - e. When prompted to restart the WebSphere Content Server application, *do not* restart the application; simply click **Next**.
5. After the installation is complete, stop and restart the Content Server application from the WebSphere Network Deployment Administrative Console.
6. If you wish to add more clusters either vertically or on other machines, repeat [steps 2 through 5](#) in this procedure for each new cluster member.
7. Complete the following steps to update the WebSphere plug-in to work with the newly created cluster:
 - a. In the left-hand tree, select **Environment > Update Web Server Plugin** and click **OK**.
 - b. Copy the resulting file to any remote web servers.
 - c. Restart all affected web servers.

At this point, a WebSphere cluster has been configured and is available through the URL of the web server that was configured in the “[Pre-Installation Steps](#),” [on page 10](#).

Post-Installation Steps

This section contains instructions for testing your system, configuring your system (installing the optional search engine Verity, setting up the Content Server portal), and configuring Content Server for its business purpose. The sections are:

- A. [Testing Your Installation \(Web Applications and Portals\)](#)
- B. [Configuring Content Server](#)
- C. [Setting Up Content Server for Its Business Purpose \(All Installations\)](#)

A. Testing Your Installation (Web Applications and Portals)

In this section, you will test your installation by logging in.

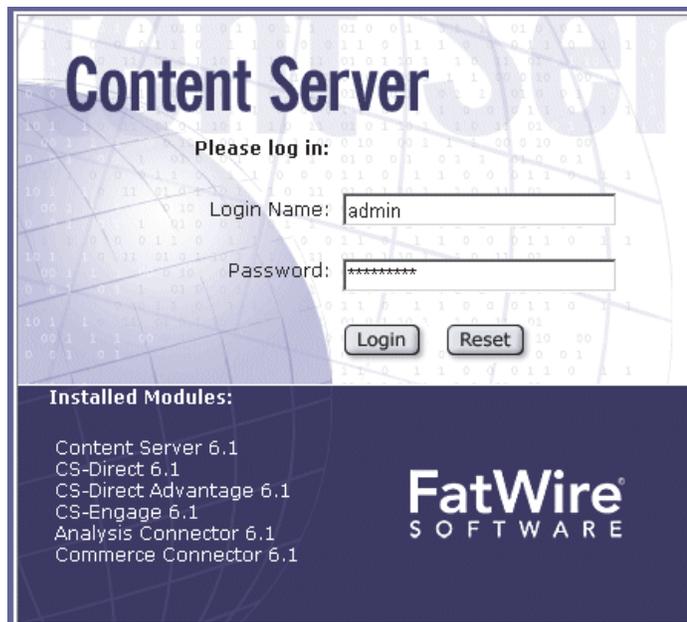
1. Browse to the following URL:

```
http://<hostname>:<port>/<context root>/Xcelerate/  
LoginPage.html
```

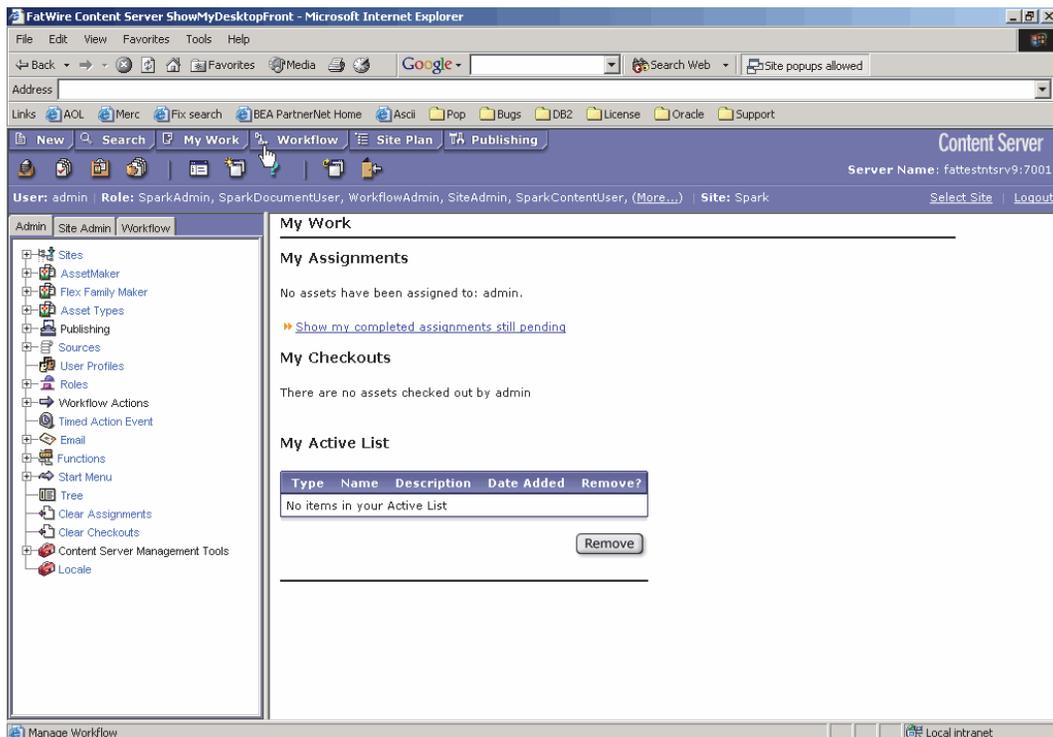
2. In the login screen, enter the following information:

Login Name: fwadmin

Password: xceladmin



Content Server's console is displayed and Content Server is now ready for further configuration.



B. Configuring Content Server

1. Configure Content Server, as necessary, by referring to the instructions in the rest of this section:
 - [Installing Verity Search Engine \(Web Installations and Portals\)](#)
 - [Integrating with LDAP \(Optional. Web Installations Only\)](#)
 - [Setting Up the Content Server Portal \(Portal Installations Only\)](#)
2. When you complete the configuration procedures, set up Content Server for its business use, as explained on [page 40](#).

Installing Verity Search Engine (Web Installations and Portals)

1. Copy the `libFTVeritySearch.so` file into the `<WAS Install>/lib` directory.
2. Add the following directories to the existing classpath, to the system path, and to the library path:

```
<content server installation directory>/VerityK2/<_platform>/  
filters  
  
<content server installation directory>/VerityK2/<_platform>/  
bin
```
3. Restart the affected instance.

Integrating with LDAP (Optional. Web Installations Only)

If you installed Content Server as a web application and wish to integrate with LDAP, follow instructions in the *Content Server Administrator's Guide*.

Setting Up the Content Server Portal (Portal Installations Only)

1. Edit the `registerSparkPortlets.xml` file as follows:
 - a. After line 15 add a new line of the form `<url>file:/<was install root>/installedApps/<network node name>/ContentServer.ear/cs.war</url>`
 - b. On the line `<context-root>/cs</context-root>`, change `/CS` to whatever your context root is.
2. The first time that you log in as `wpsadmin`, you will be prompted to create a new username and password. In this guide, we assume you are using the following:
Username: `csuser`
Password: `<your_password>`
3. Log out, then log back in with username/password `wpsadmin/wpsadmin`.

You see the following display:

The screenshot displays the IBM WebSphere Portal 5.1.0.1 interface within a Microsoft Internet Explorer browser window. The browser's address bar shows a URL from fatwire.com. The portal's navigation bar includes tabs for 'Welcome', 'My Workplace', 'Documents', 'Personalization', 'My Finances', and 'My Work'. A search bar is also present.

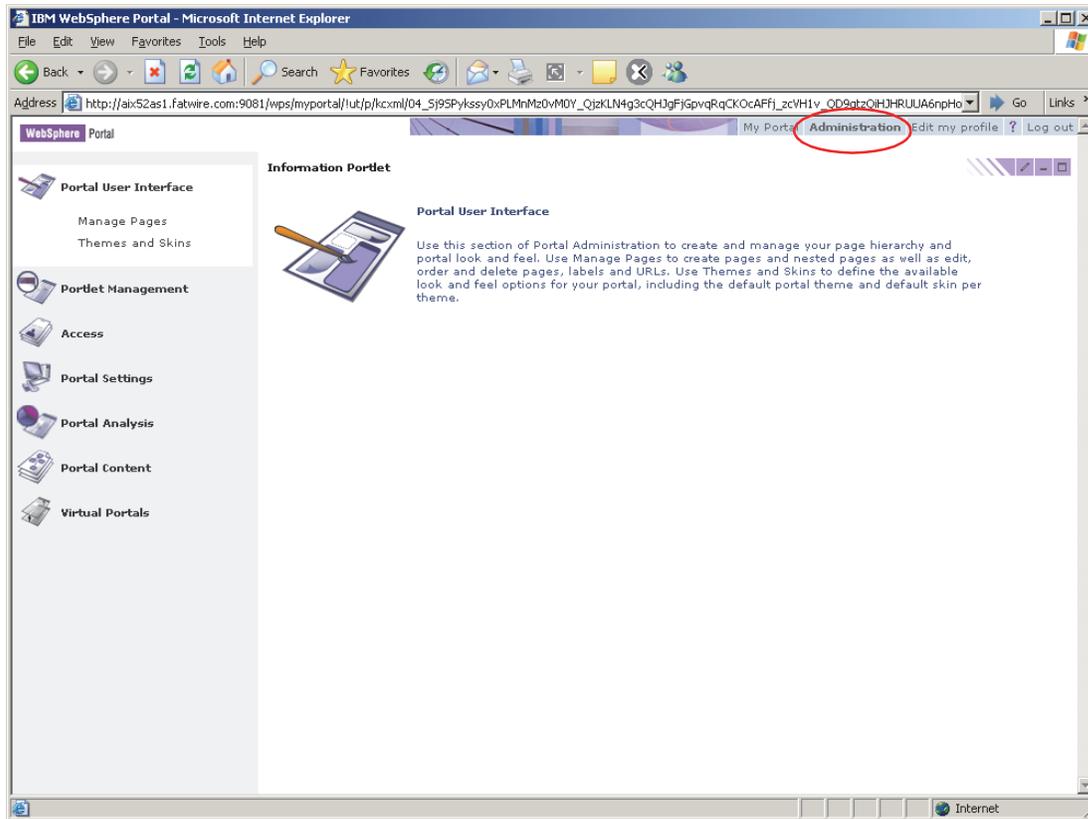
The main content area is divided into several portlets:

- Welcome to WebSphere Portal version 5.1:** Provides instructions on how to rearrange portlets and create new pages.
- My Weather:** Displays weather information for Thursday, August 25, 2005, at 12:18:00 PM GMT. It lists conditions for Raleigh, North Carolina (68°/86°), Stuttgart, Germany (65°/67°), Beijing (Peking), China (82°/87°), Tokyo, Japan (79°/79°), and San Francisco, California (58°/74°).
- My News:** Titled 'Financial Services News', it lists articles such as 'Lenders dinged for catering to poor credit' and 'Fidelity to offer alternative stock exchange based in Boston'.
- My Stocks:** Shows stock market data for Wednesday, August 24, 2005, at 4:03:00 PM EST. It includes a table with columns for stock symbols, prices, and percentage changes.

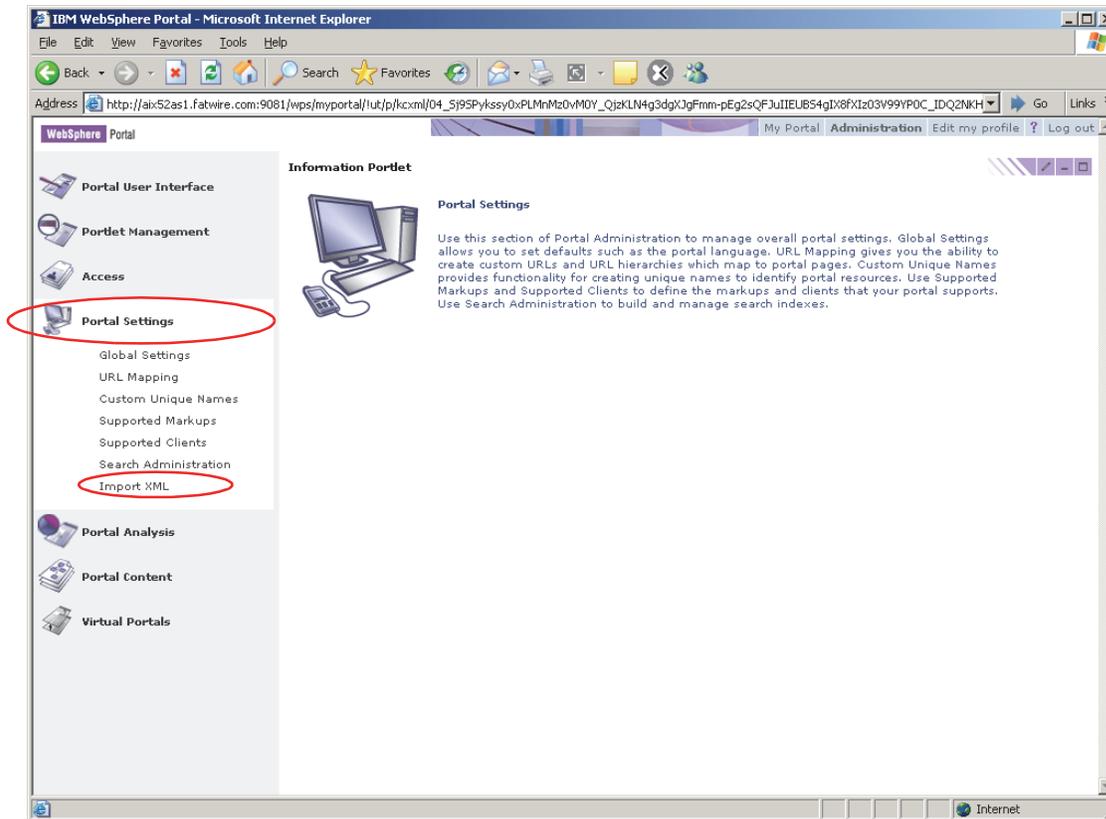
Symbol	Price	Change	% Change
IBM	81.32	0.00	0.00%
\$COMPQ	2,131.82	2.91	0.14%
\$DJI	10,434.87	-84.71	-0.81%
\$SPX	1,210.81	1.22	0.10%

The page footer includes copyright information for IBM and MarketWatch, Inc. 2005, and notes that intraday data is provided by ComStock, an Interactive Data Company.

4. Click on **Administration** (in the top right-hand corner).



5. Import the `registerSparkPortlet.xml` as follows:
 - a. From the left-hand menu bar, select **Portal Settings** > **Import XML**.



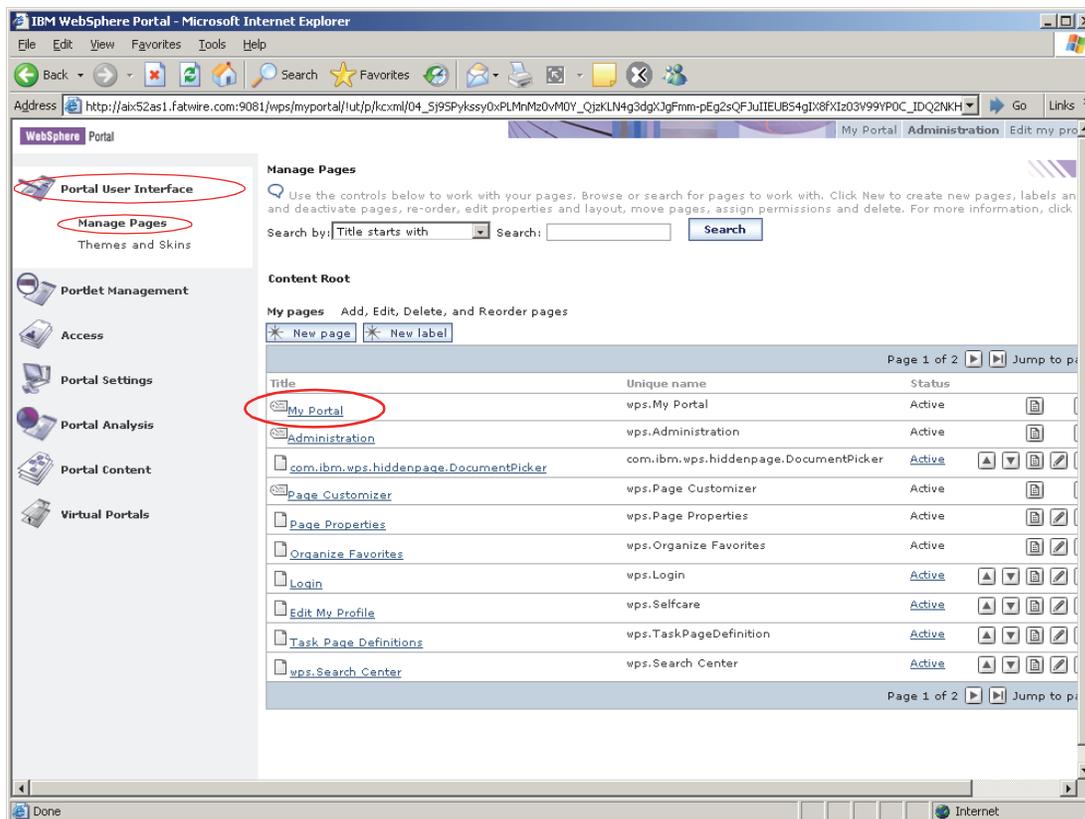
- b. Locate the file `registerSparkPortlet.xml` (it is located with the files that are used to install Content Server).
- c. Click **Import**.
The file is imported.

6. Create the portal pages:

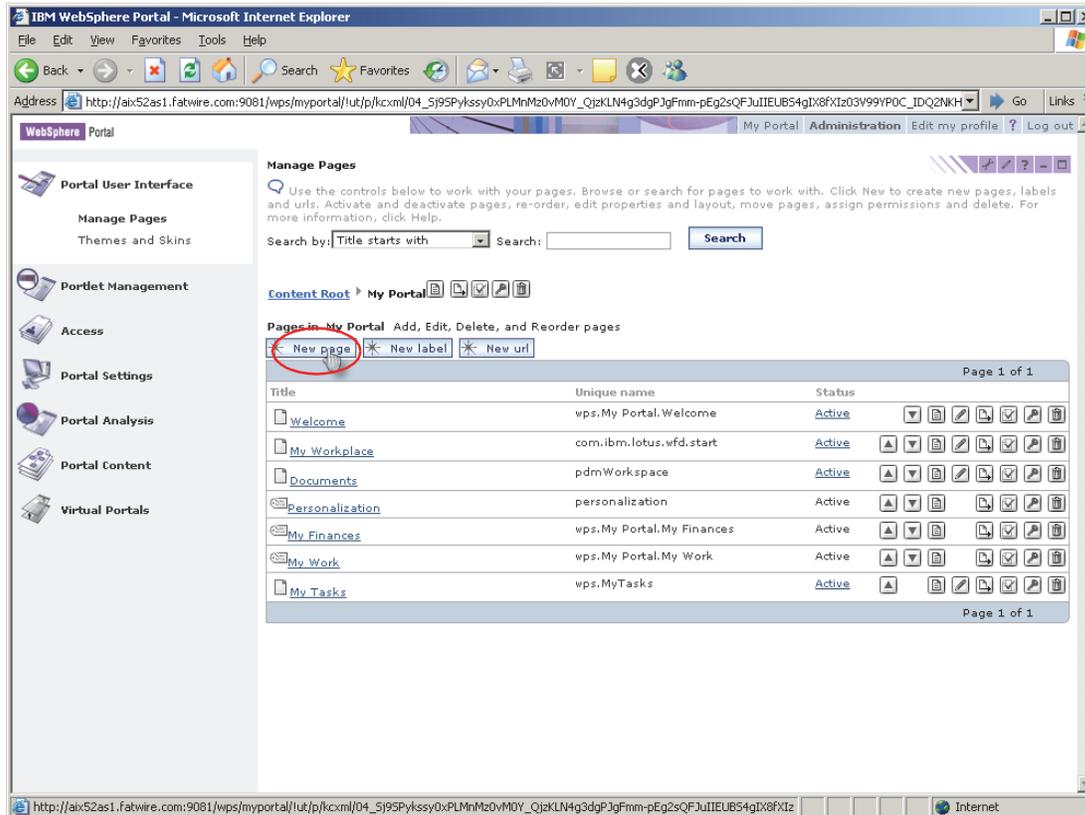
Note

The pages will be used to display the portlets. In this guide, the pages are named “FatWire Content,” “FatWire Documents,” “Admin,” and “Spark Display.” If you need a preview of the finished pages and the portlets they contain, see the figures starting on [page 38](#).

- a. From the left-hand menu bar, select **Portal User interface > Manage Pages**.
- b. In the “Title” column, click **My Portal**.

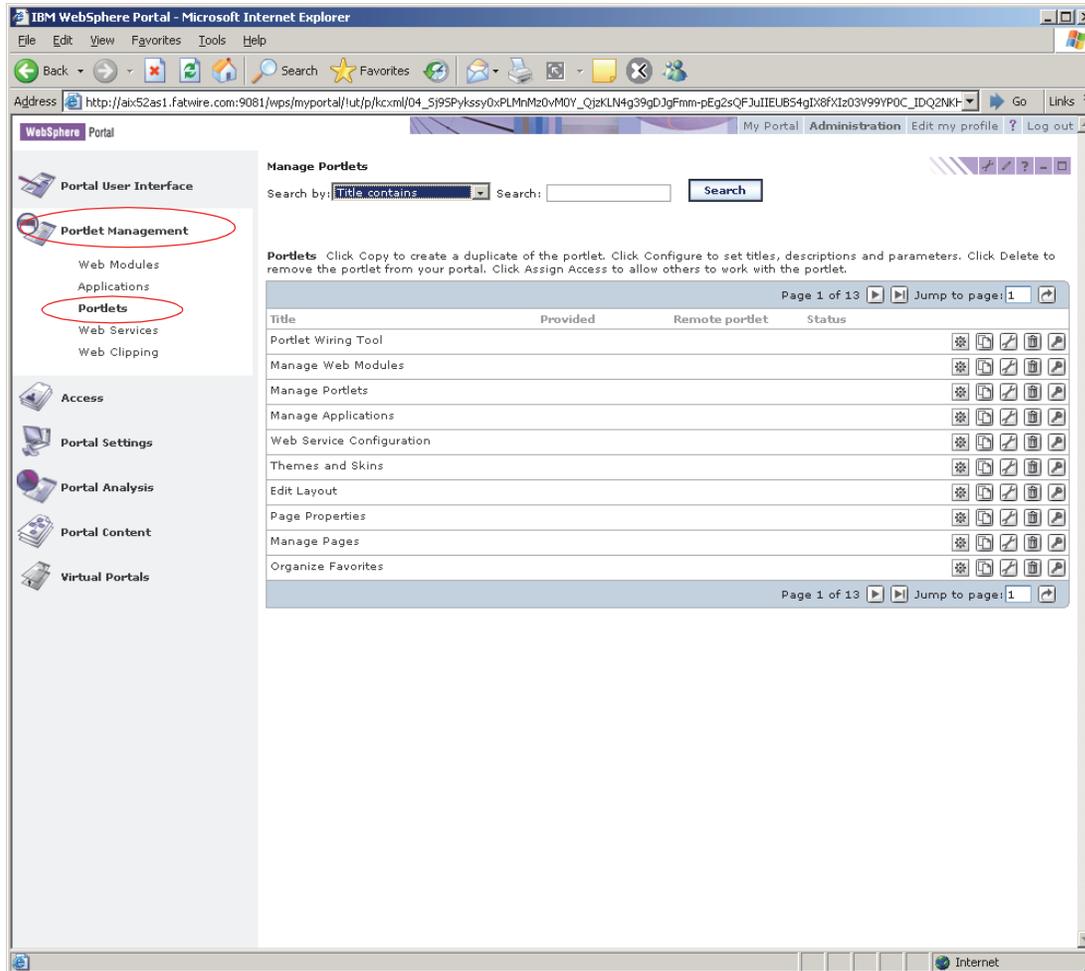


- c. Click **New page**. Specify the name of the page to be **FatWire Content** and the page layout type to be **3 column**. (In a later step, you will arrange the content management portlets to be displayed within the 3 columns on the page). Click **OK**.

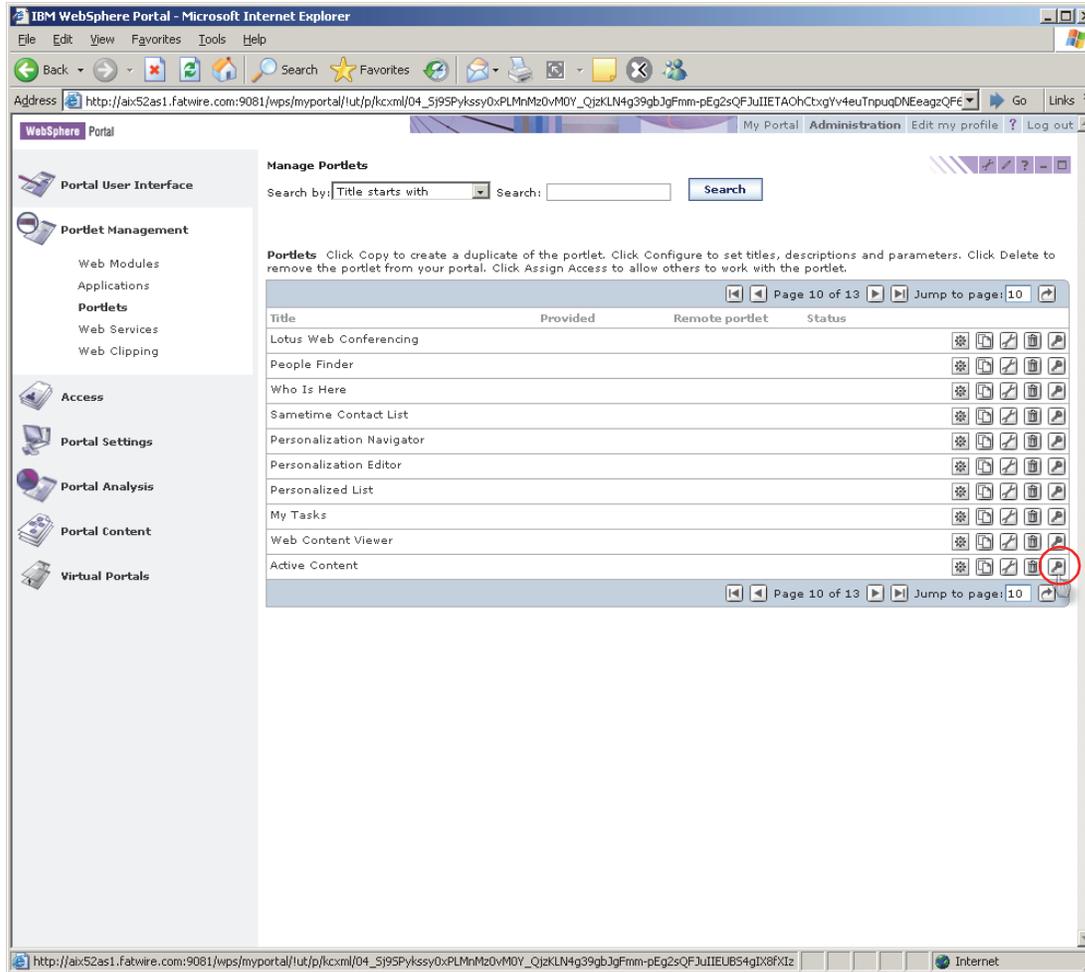


- d. Click **New page** again. Specify the name to be **FatWire Documents** and the page layout type to be **3 column**, then click **OK**.
- e. Click **New page** again. Specify the name to be **Admin** and the page layout type to be **2 column**, then click **OK**.
- f. Click **New page** again. Specify the name to be **Spark Display** and the page layout type to be **2 column**, then click **OK**.

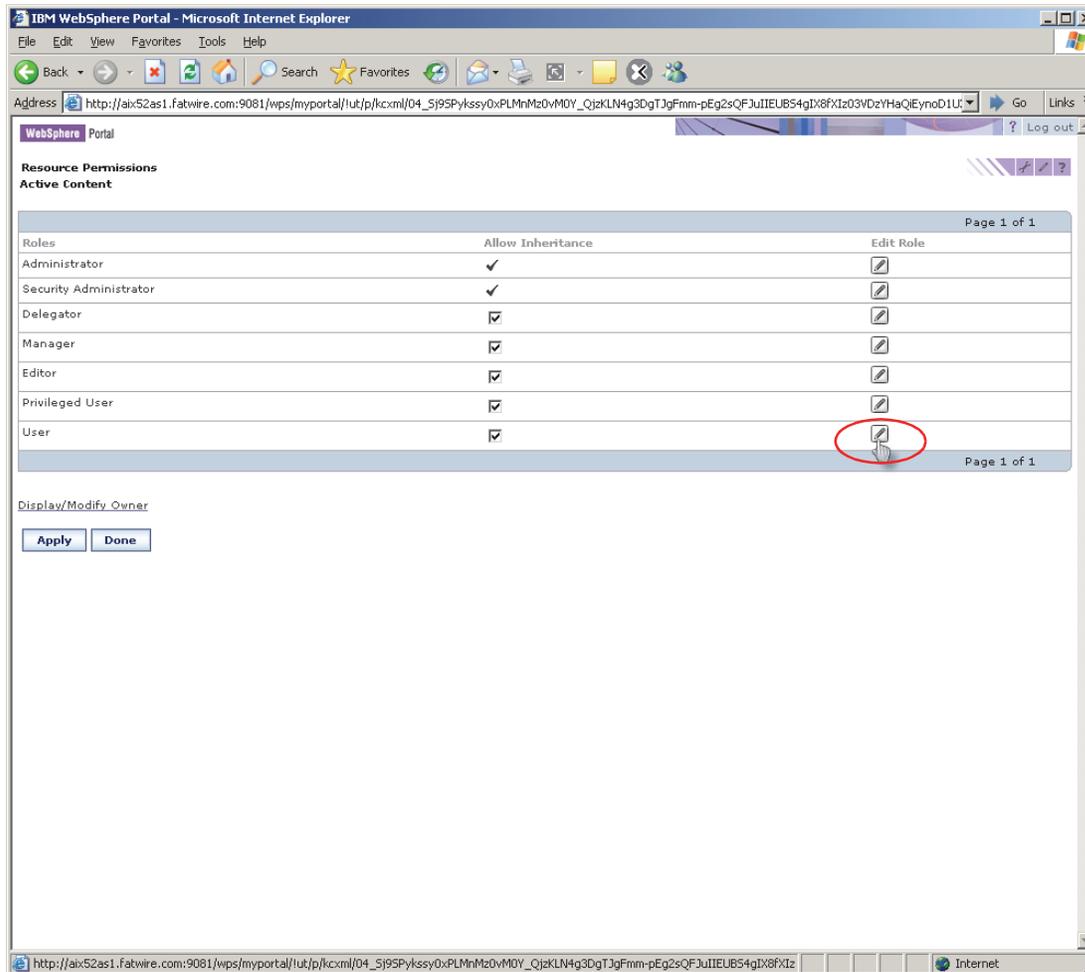
7. Assign permissions to access the portlets as follows:
 - a. From the left-hand menu bar, select **Portlet Management > Portlets**.



- b. Locate the “Active Content” portlet and modify access to the portlet by clicking on the key icon next to the portlet’s name.



c. Click the **Edit** button in the “User” row.



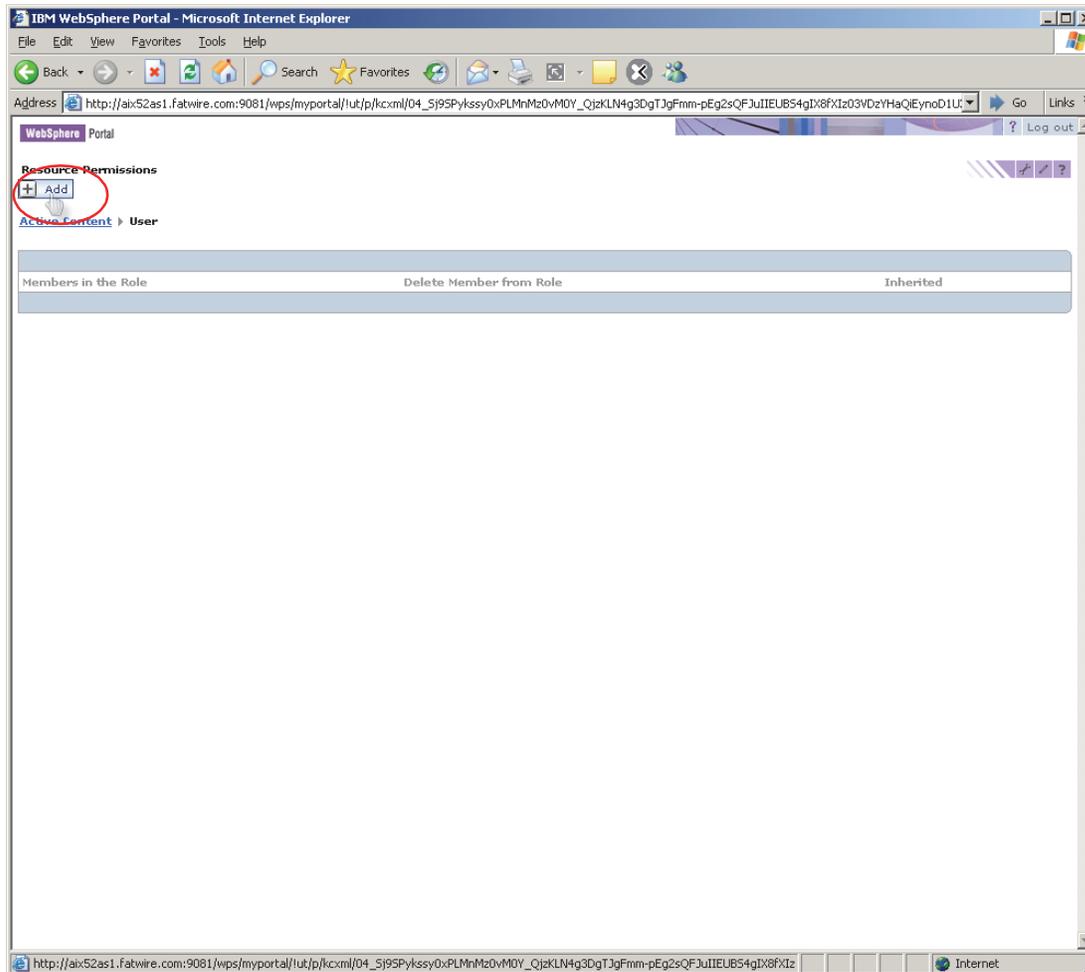
The screenshot shows the IBM WebSphere Portal interface in Microsoft Internet Explorer. The browser title is "IBM WebSphere Portal - Microsoft Internet Explorer". The address bar shows the URL: http://aix52as1.fatwire.com:9081/wps/myportal/!ut/p/kc:ml/04_Sj95Pykssy0xPLMnMz0vMOY_QjzKLNHg3DgTJgFnm-pEg2sQFJuIIEUB54gIX8fXIZ03VDzYHaQIEynoD1U;

The main content area is titled "Resource Permissions" and "Active Content". It displays a table with the following columns: Roles, Allow Inheritance, and Edit Role. The table contains the following rows:

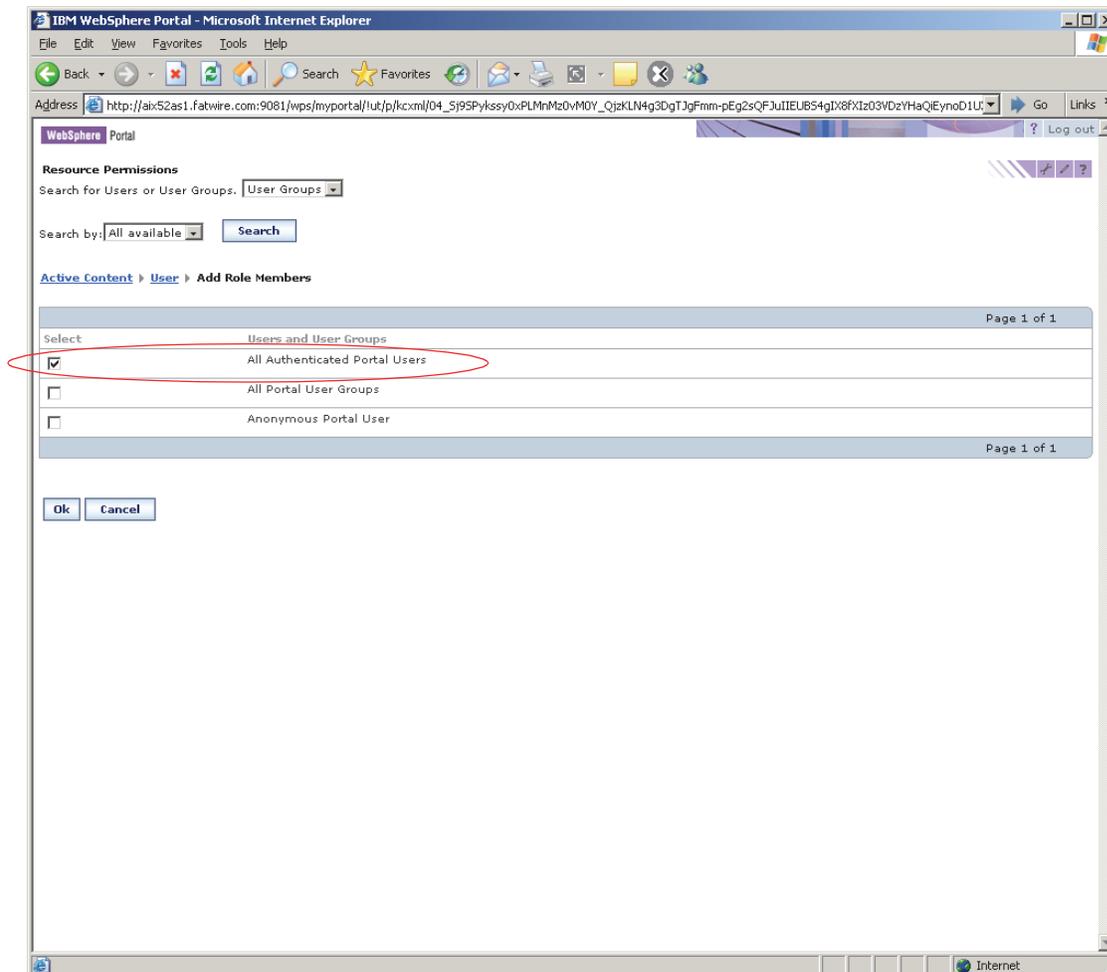
Roles	Allow Inheritance	Edit Role
Administrator	<input checked="" type="checkbox"/>	
Security Administrator	<input checked="" type="checkbox"/>	
Delegator	<input checked="" type="checkbox"/>	
Manager	<input checked="" type="checkbox"/>	
Editor	<input checked="" type="checkbox"/>	
Privileged User	<input checked="" type="checkbox"/>	
User	<input checked="" type="checkbox"/>	

The "Edit Role" button for the "User" row is circled in red. Below the table, there are buttons for "Apply" and "Done".

d. Click the **Add** button.



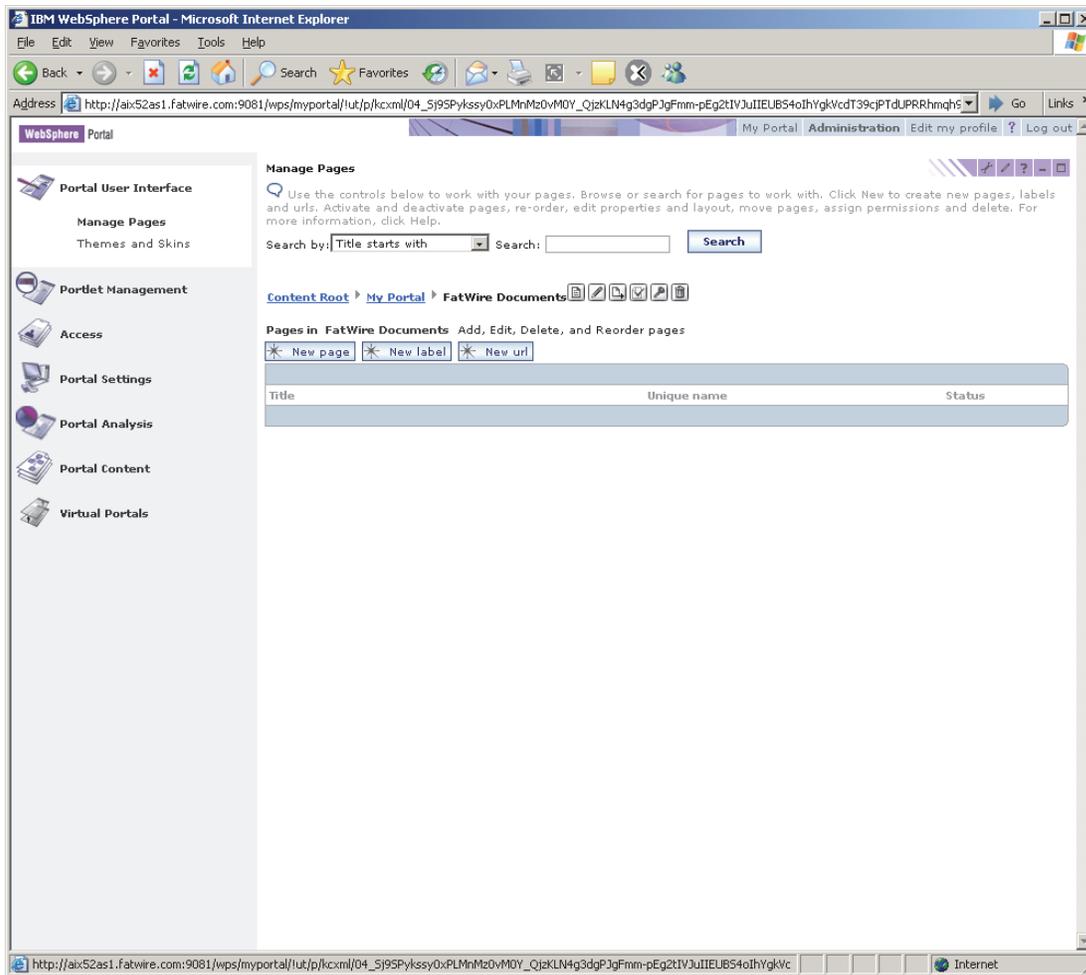
- e. Select the checkbox **All Authenticated Portal Users** and click **OK**.



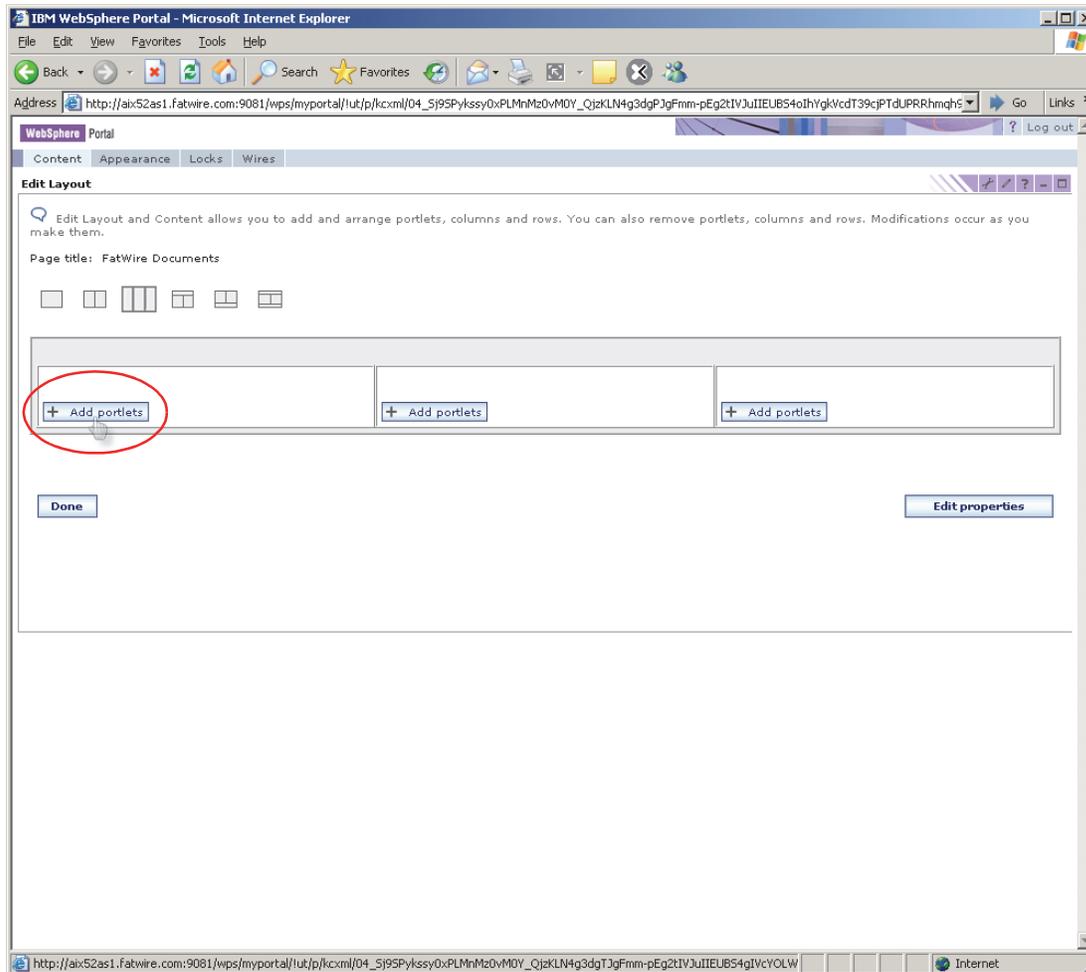
8. Repeat [step 7 on page 28](#) for each of the following portlets:

Active Documents	Create Content	Search Documents
Checked Out Content	Document Assignments	Site Info
Checked Out Documents	Document History	SparkAd
ClearAssignments	My Documents	SparkDocuments
ClearCheckouts	Publish Console	SparkJobs
Content Assignments	PublishTarget	SparkNews
Content History	RolesAdmin	
ContentDefinition	Search Content	

9. Add portlets to one of the pages that was created in [steps 7 and 8](#). Do the following:
 - a. Select the page to which you want to add portlets and click the edit icon.



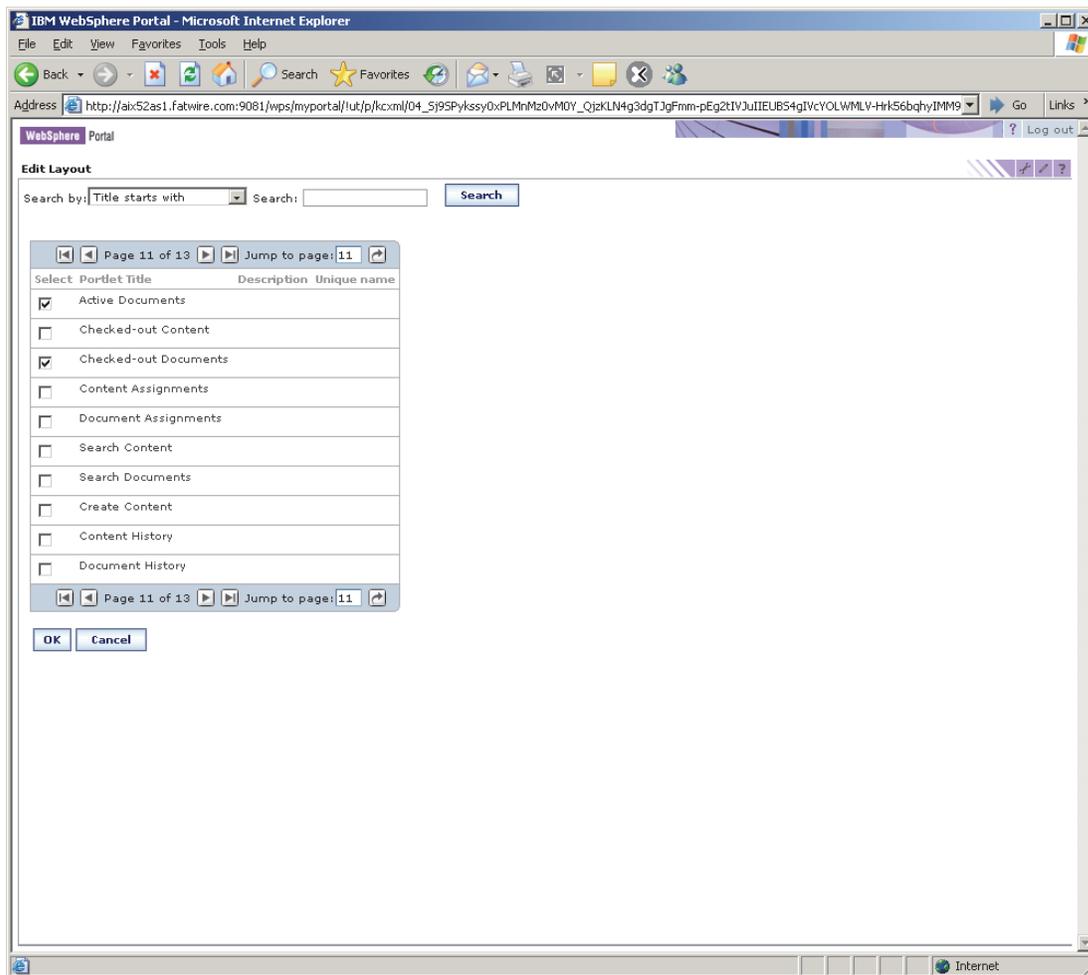
b. Click the **Add portlets** button in the left-most column.



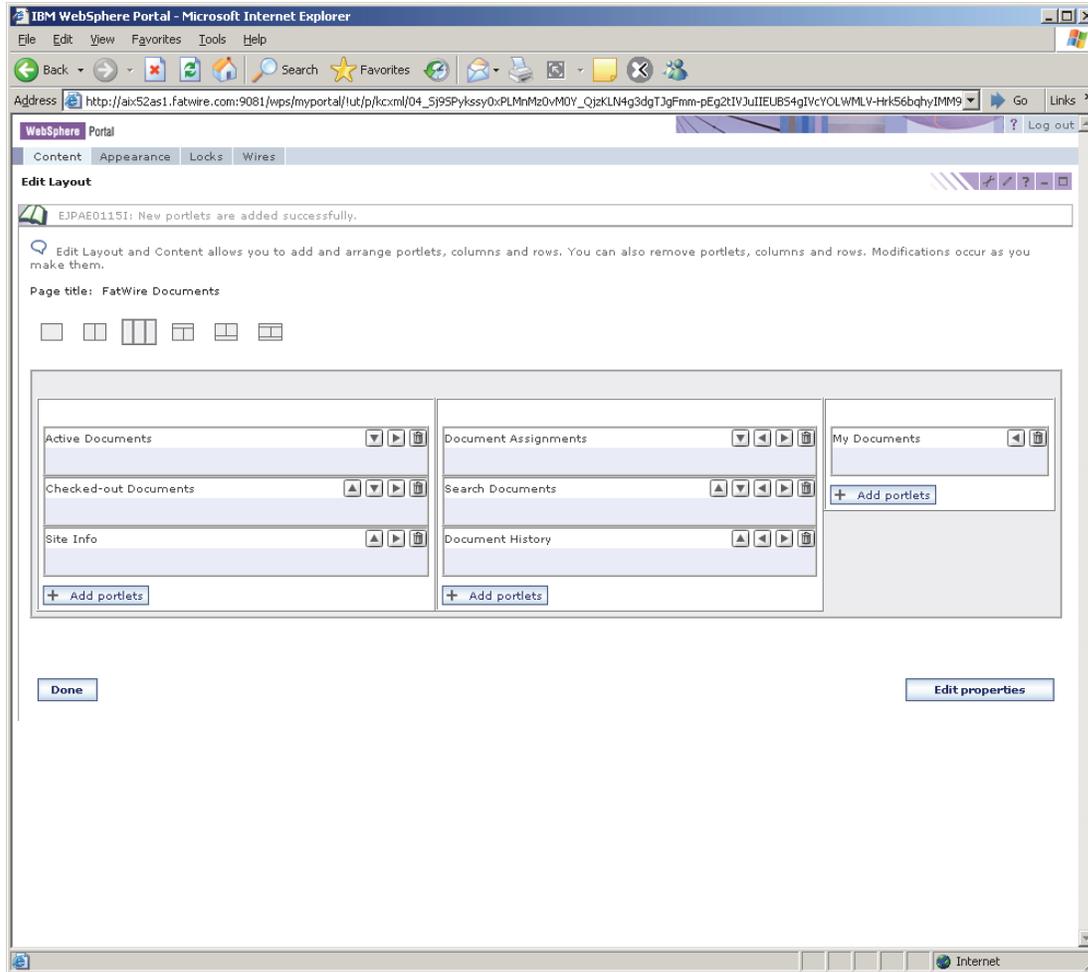
- c. Select the portlets you wish to add to the left-most column (they may span multiple pages) then click **OK**.

Note

If you need guidelines for determining which portlets to place on the page, refer to the figures starting on [page 38](#).



- d. Repeat steps 9a–9c for each remaining column of the page. Once all columns are set up, click **Done**.



10. Repeat [step 9](#) for each remaining page (added in [step 6](#) on [page 26](#)).
11. Verify that the pages you created display the correct portlets:
 - a. Log out of the portal and log back in as **admin** or another valid Content Server user.
 - b. Click on the titles of the pages that you created in [step 6](#).
The pages should look similar to those shown below.
 - “FatWire Content” page

The screenshot shows the 'FatWire Content' page in a Microsoft Internet Explorer browser. The page is divided into several portlets:

- Active Content:** Shows a table with columns 'Type', 'Name', and 'Date Added'. It contains one entry: 'Article (Flex) story1' with a date of '2005-08-26 11:27:41'.
- Content Assignments:** Displays 'No assets in Assignment List'.
- Search Content:** Includes a search box for 'Find Article (Flex)', a dropdown for 'Search Name', and a 'Sort results by Name' dropdown. A 'Search' button is present.
- Content History:** Shows a table with columns 'Type' and 'Name', containing one entry: 'Article (Flex) story1'.
- Site Info:** Displays user information: 'User: admin', 'Site: GE Lighting', and 'Role: Designer, WorkflowAdmin, SiteAdmin, GeneralAdmin'.
- Main Content Table:** A table listing content items with columns 'Name', 'Description', 'Status', and 'Modified'.

Name	Description	Status	Modified
Burlington Promotion	Burlington Promotion	Edited	2000-11-06 23:31:55
Frequent Visitor	Article welcoming frequent visitors	Edited	2000-11-14 16:53:23
story1	How does a light bulb actually work?	Received	2000-10-03 12:31:50
story2	Is voltage important?	Received	2000-10-03 12:31:51
story3	Can fluorescent lights be put on a dimmer?	Received	2000-10-03 12:31:54
- Publish Console:** Includes a 'Select Publish Destination' dropdown set to 'Destination 2 (dynamic) (using Mirror to Server)' and a 'Select Destination' button.
- Running Publish Sessions:** Shows 'No Running Publish Sessions'.
- Scheduled Publish Tasks:** Shows 'No Scheduled Publish Tasks'.
- Publish History:** Shows 'No Publish History'.
- Create Content:** A table listing content creation options:

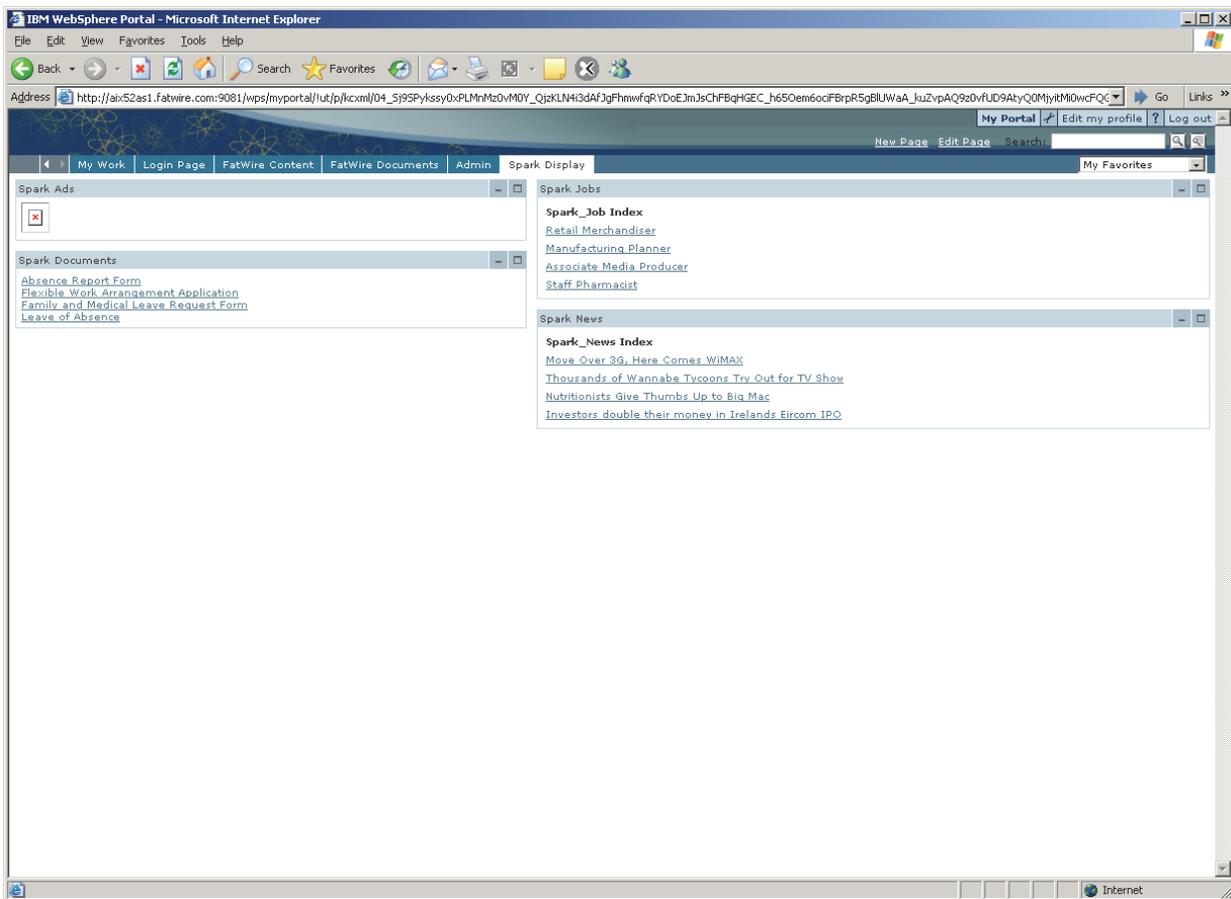
Type	Name
Article (Flex)	New Article (Flex)
Attribute Editor	New Attribute Editor
Collection	New Collection
Content Attribute	New Content Attribute
Content Definition	New Content Definition
Content Parent	New Content Parent
Content Parent Definition	New Content Parent Definition
CSFElement	New CSFElement

- “FatWire Documents” page

- “Admin” page

	Name	Description
🔍	Analyst	Analyst
🔍	Approver	Content Approver
🔍	Author	Content Author
🔍	Checker	Content Checker
🔍	Designer	Site Designer
🔍	Editor	Content Editor
🔍	Expert	Expert
🔍	GeneralAdmin	General Administration
🔍	HelloAuthor	Author role for HelloAssetWorld
🔍	HelloDesigner	Designer role for HelloAssetWorld
🔍	HelloEditor	Editor role for HelloAssetWorld
🔍	Marketer	Marketing Manager
🔍	Pricer	Pricer
🔍	SiteAdmin	Site Administration
🔍	SparkAdmin	Spark Administrator
🔍	SparkContentUser	Spark Content User
🔍	SparkDocumentUser	Spark Document User
🔍	WorkflowAdmin	Workflow Administration

- “Spark Sample” page



C. Setting Up Content Server for Its Business Purpose (All Installations)

For instructions on configuring Content Server for business use, refer to the *Content Server Administrator's Guide* and the *Developer's Guide*. The guides explain how to create and enable a content management environment, including the data model, content management sites, site users, publishing functions, and client interfaces.

Appendices

The appendices provide you with information about installing and configuring Content Server's supporting software.

This part contains the following appendixes:

- [Appendix A, “Installing WebSphere Portal Server and Network Deployment Server”](#)
- [Appendix B, “Configuring Web Servers and WAS JDBC Providers”](#)
- [Appendix C, “Creating and Installing Self-Signed Certificates”](#)
- [Appendix D, “Installing and Configuring the Directory Server for Content Server”](#)
- [Appendix E, “Integrating LDAP with Network Deployment and WebSphere_Portal”](#)
- [Appendix F, “Debugging Procedures”](#)

Appendix A

Installing WebSphere Portal Server and Network Deployment Server

This appendix contains the following sections:

- [Installing WebSphere Portal Server](#)
- [Installing WebSphere Network Deployment Server](#)

Installing WebSphere Portal Server

This section provides an example of how to install the WebSphere Portal on AIX.

Install the following packages in the order shown:

Note

The packages will differ from the ones below according to your operating system.

1. C82UQML.taz: Portal Installation
 - a. 1-6 and 1-5 BISF
 - 1) 1-6: C814LML.taz: BISF
 - 2) 1-5: C814KML.taz: BISF
 - b. 1-17: C814XML.taz: BISF FP1
 - c. C8152ML.zip: Portal CD2
 - d. C8153ML.zip: Portal CD3
2. was511_cf3_aix.zip: Cumulative Patch 3 for WAS
3. WASEfixes.zip: Post Cumulative Patch 3 for WAS
4. PortalUpdateInstaller.zip, WP_PTF_5101.zip
 - a. Unzip PortalUpdateInstaller.zip.
 - b. Create a directory update/fixpacks/ and unzip WP_PTF_5101.zip into this directory.
 - c. Run the following command:

```
./updatePortal.sh -fixpack \  
-installDir "<was PortalServer root>" \  
-fixpackDir "<install root dir>/D/update/fixpacks" \  
-install -fixpackID WP_PTF_5101
```
5. was511_cf5_aix.zip
6. wbisf511_cf2_aix.zip
7. PK01733_5115.jar: Post Cumulative Patch 5 for WAS.txt

Run the same installer as in [step 6](#). When prompted for the location of the patch directory, point to the directory containing the jar file in [step 7](#).

Installing WebSphere Network Deployment Server

This section provides an example of how to install the WebSphere Network Deployment Server on AIX.

Note

Packages required for the installation depend on the operating system.

Install the following files **in the order shown**:

1. C85GJML.taz: Network Deployment Installer
2. BISF installers
 - a. C814KML.taz
 - b. C814LML.taz
3. C811VML.taz:
4. C814XML.taz:
5. was511_nd_cf5_aix.zip Network Deployment Cumulative Patch 5
6. wbisf511_cf2_aix.zip: BISF Cumulative Patch 2
7. PK01733_5115.jar: post Network Deployment Cumulative Patch 5.txt

Appendix B

Configuring Web Servers and WAS JDBC Providers

This appendix contains the following sections:

- [Configuring Apache](#)
- [Configuring IIS](#)
- [Configuring WAS JDBC Providers](#)

Note

Information in this appendix is meant only to supplement the information provided by the vendors and should not be used as the primary source for conducting the installation of these third-party products.

Configuring Apache

This section assumes that you have an operational installation of Apache. Complete the following steps to configure this Apache installation to forward requests to the WebSphere Application Server:

1. If the web server is not located on the same machine as WAS, copy the following files from the WAS server to the web server:
 - Windows: `Mod_was_ap20_http.dll`
`plugin-cfg.xml`
 - UNIX: `Mod_was_ap20_http.so`
`plugin-cfg.xml`
2. Edit the `httpd.conf` file used by your current installation of Apache by adding the following lines to the main server section:
 - UNIX

```
LoadModule was_ap20_module /<path to>/mod_was_ap20_http.so
WebSpherePluginConfig /<path to>/plugin-cfg.xml
```
 - Windows

```
LoadModule was_ap20_module /<path to>/mod_was_ap20_http.dll
WebSpherePluginConfig /<path to>/plugin-cfg.xml
```
3. Restart Apache.

Configuring IIS

This section assumes that you have an operational installation of IIS. Complete the following steps to configure this IIS installation to forward requests to the WebSphere Application Server:

1. If the web server is not located on the same machine as WAS, then copy the `iisWASPlugin.dll` and `plugin-cfg.xml` files from the WAS server to the web server.
2. Add the Internet Services Application Programming Interface (ISAPI) filter into the IIS configuration by completing the following steps:
 - a. Open IIS Manager.
 - b. Right-click the server instance that will redirect traffic to WAS.
 - c. Select **Properties** in the pop-up menu, then complete the following steps in the “Properties” dialog:
 - 1) Select **ISAPI Filters** > **Add** to open the “Filter Properties” window.
 - 2) In the “Filter Name” field, type `iisWASPlugin`.
 - 3) In the “Executable” field, click **Browse** to select the location of the `iisWASPlugin_http.dll` file.
 - 4) Click **OK** to close each dialog box.

3. In the Registry Editor, open:
HKEY_LOCAL_MACHINE > SOFTWARE > IBM > WebSphere Application Server > 5.1.0.0
4. Set the value of the `Plugin Config` variable to the location of the configuration file `plugin-cfg.xml`. If the `Plugin Config` variable does not exist, complete the following steps:
 - a. Right-click the background.
 - b. Select **New >String Value** in the pop-up menu.
 - c. Enter `Plugin Config` as the value for “Name,” and enter the path to the file `plugin-cfg.xml` as the value for “Data.”
5. Restart the IIS installation.

Configuring WAS JDBC Providers

1. Log in to the WebSphere Administrative Console.
2. In the left-hand tree, select **Resources > JDBC Providers**.
3. In the right-hand panel, click **New**, then do the following:
 - a. Select the correct driver and click **OK**.
If you are using MS SQL Server 2000 as the database server, select **WebSphere Embedded ConnectJDBC Driver for MS SQL Server**.
 - b. In the “Configuration” screen:
 - 1) Enter a name (such as `csJDBC`).
 - 2) Enter a description (optional).
 - 3) Select **OK**.
4. In the left-hand tree, select **Security > JAAS Configuration > J2C Authentication Data**.
5. In the right-hand panel, click **New**, then do the following:
 - a. Add an alias of your choice and enter your database user name and password in the fields provided.
 - b. Click **OK**.
6. Select the newly created JDBC Provider from the list on the right. Under “Additional Properties,” select **DataSources**, then click **New** and do the following:
 - a. Add a name (such as `csData`).
 - b. Add a JNDI name (such as `csDataSource`).
 - c. In the **Component-Managed Authentication Alias** drop-down list, select the alias you created in [step 5](#) of this procedure.
 - d. Select **OK**.
7. Select the data source you created in [step 6](#) of this procedure. Under “Additional Properties,” select **Custom Properties** and do the following:

- a. Fill in the following fields: “databaseName,” “ServerName,” and “PortNumber” with the values that are correct for your database.
 - b. Change “PreTestSQLString” to the following value:

```
SELECT count(*) from TABLE dbproperties.
```
 - c. Click **OK**.
8. Go to the top of the right-hand panel and click **Save**.
9. Click **Save** again.
10. Go to the left-hand tree and select the JDBC Provider created in [step 3](#) of this procedure.
 - a. Select **Data Sources** from the bottom of the resulting page.
 - b. Check the box next to the data source created in [step 6](#) of this procedure and select **test connection**. If it passes then you have a connection to the database; if not review the above steps and the WAS product documentation.

Appendix C

Creating and Installing Self-Signed Certificates

This appendix provides instructions for creating and installing self-signed certificates for WebSphere 5.1.x.

This appendix contains the following sections:

- [Creating a Self-Signed Certificate](#)
- [Installing a Self-Signed Certificate](#)

Creating a Self-Signed Certificate

Complete the following steps to create a self-signed certificate. If you already have a valid self-signed certificate, proceed to [“Installing a Self-Signed Certificate,”](#) on page 53.

1. Run the IBM Key Management application:
 - Windows: `ikeyman.bat`
 - UNIX: `keyman.sh`
2. In the top menu bar, select **Key Database File > New**.
 - a. Leave **JKS** selected as the default database type.
 - b. Enter a unique name for the new key database.
 - c. Browse to select the location in which to store the new database.
 - d. Click **OK**.
 - e. When prompted, enter a password (make a note of this password).
 - f. Click **OK**.
3. In the **Key Database Content** section, go to the **Signer Certificates** drop-down menu and select **Personal Certificates**.
4. In the bottom, right corner, click **New Self-Signed**.
5. In the “Create a New Self-Signed Certificate” window, do the following:
 - a. Enter a name for the key in the “Key Label” field.
 - b. Leave the **Version** and **Key Size** options selected.
 - c. In the “Common Name” field, enter the name of the WebSphere application server.
 - d. Complete the remaining options as appropriate.
 - e. Click **OK**.
6. Click the name of the certificate that you created in [step 5](#), then click the **Extract Certificate** button (located in the bottom, right corner) and do the following:
 - a. Leave **Data Type** selected.
 - b. Name the certificate.
 - c. Browse to select the location in which to save the certificate.
 - d. Click **OK**.
7. In the **Key Database Content** section, go to the **Personal Certificates** drop-down menu and select **Signer Certificates**.
8. Click the **Add** button (located on the right side of the console), then do the following:
 - a. Select the file you saved in [step 6](#) and click **OK**.
 - b. Enter a unique name for this certificate.
 - c. Click **OK**.
9. Select **Key Database File > Exit**.

Installing a Self-Signed Certificate

Complete the following steps to install a self-signed certificate. If you need instructions for creating a self-signed certificate, see [“Creating a Self-Signed Certificate,”](#) on page 52.

1. Log in to the WAS Administrative Console.
2. In the left-hand tree, select **Security > SSL**.
3. In the **SSL Configuration Repertoires** section (located in the right-hand side of the WAS Administrative Console), complete the following steps:
 - a. Select **New**.
 - b. Enter an alias.
 - c. In the “Key File” and “Trust File” fields, enter the location and the password for the certificate’s key database file. If you are using a certificate that you created, use the location and the password for the key database file you created in [step 2](#) of [“Creating a Self-Signed Certificate.”](#)
 - d. Click **OK**.
 - e. Save the changes, as prompted.
4. In the left-hand tree, select **Security > Authentication Protocol > CSIV2 Outbound Transport**, then complete the following steps:
 - a. In the “SSL Settings” field, select the alias that you created in [step 3](#).
 - b. Click **OK**.
 - c. Save the changes, as prompted.
5. For each server that will use this certificate, complete the following steps:
 - a. In the WAS Administrative Console, select **Configuration > Web Container > HTTP Transports**.
 - b. For each host where “SSL Enabled” is true, select the host, and in the field next to “SSL,” select the alias created in [step 3](#) of this procedure.
 - c. Save all changes.
6. Restart all affected servers.
7. Because the certificate is self-signed, you will need to import it into the browser (or Internet Explorer in the case of Windows) before SSL-enabled components will function correctly.

Appendix D

Installing and Configuring the Directory Server for Content Server

This appendix contains the following sections:

- [Installing the Directory Server](#)
- [Configuring the Directory Server](#)

Installing the Directory Server

Installation of the Directory Server is completed as part of the portal installation process. However, if you need to have the Directory Server on a separate machine, you will need to install it independently. For installation instructions, see the product documentation.

Configuring the Directory Server

Below is an example of how to configure a Directory Server. The example is for DB2 on AIX.

1. Set up the AIX environment for DB2:
 - a. Ensure AIX aio extensions are installed:

```
lslpp -l bos.rte.aio
```
 - b. Set up aio to be available:

```
smit chgaio
```
 - c. Reboot the server.
2. Download and install one of the following Tivoli Directory Server 5.2 onto your platform (one of the following; the installation requires about 1GB of disk space):
 - AIX: C57KVML.tar
 - LINUX: C57KZML.tar
 - Windows: C57KTML.zip

To install the Tivoli Directory Server, run:

```
./setupIBM
```

Note

On UNIX, Tivoli Directory Server installs into: /usr/ldap, /usr/opt/db2..., /usr/opt/ibm

3. Create a new user (this guide assumes the username to be `wportusr`). Create a home directory with read/write permissions. On UNIX platforms change the ownership of this user's home directory to have write permission for `other`. Run the following command:

```
chmod o+x <user home directory>
```
4. Create a location for the DB2 portal database `/u01/software/Other/WASPortalDB`. In this case, make sure the database is owned by the user that was created in [step 3](#).

5. Create a new DB2 instance by changing to `/usr/opt/db.../instance/` and running `./db2icrt -u wportusr wportusr` (where `wportusr` is the username created in [step 3](#)).

Note

If creation of a new DB2 instance fails with the message: "Failed to add local loop back to database", there is most likely an issue with DB2 on AIX—it is using the 64-bit version of the software and not the 32-bit version. The following commands will correct this error:

```
cd <db2 directory> ;
mv adm64 adm64.old ;
mv adsm64 adsm64.old ;
mv bin64 bin64.old ;
mv dasfcn64 dasfcn64.old ;
mv function64 function64.old ;
mv include64 include64.old ;
mv security64 security64.old

ln -s adm adm64 ;
ln -s adsm adsm64 ;
ln -s bin bin64 ;
ln -s dasfcn dasfcn64 ;
ln -s function function64 ;
ln -s include include64 ;
ln -s security security64
```

6. Start the new DB2 instance by logging in as `wportusr` and running source:


```
./sql1lib/db2profile ;
./sql1lib/adm/db2start
```
7. After the installation is complete, it will start the “Tivoli Directory Server Configuration Tool.” Exit this instance of the tool, change to the home directory of the user created in [step 3](#) above, and restart it by executing `ldapxcfg` (on UNIX systems, this is located in `/usr/ldap/bin/`). Complete the following steps:
 - a. In the “Set the Administrator DN/Password” screen, set a password and click **OK**.
 - b. Click on **Configure database**, then **Create a new database**, and then **Next**.
 - c. Enter the userid and password for the user created in [step 3](#) above and click **Next**.
 - d. Enter a name for the new database: `<CSPORTAL>` in this case and click **Next**.
 - e. Accept the default of UTF-8 and click **Next**.
 - f. Enter the location at which to create the database (see [step 4](#) in this procedure). Click **Next**.
 - g. Click **Finished** and wait for the task to complete.
8. Add a suffix that matches your DNS name suffix. To do so, add a new entry `dc=<domain>,dc=<dns extension>`, then click **Add** followed by **OK**.

9. Import the `.ldif` data file as follows:
 - a. Locate the `portalusers.ldif` file, in `contentserver\portal\ibm`.
 - b. Edit the file by replacing `<dc=fatwire,dc=com>` with the values entered in [step 8](#).
 - c. Import the file using “IBM Tivoli Directory Server Configuration Tool”:
 - 1) Select **Import LDIF file** from the left-hand tree.
 - 2) Click **Browser** and select the file you just modified.
 - 3) Click **Import**.
10. Close “IBM Tivoli Directory Server Configuration Tool.”
11. Start the LDAP admin server (IBM Directory Server):

```
/usr/ldap/bin/ibmdiradm -f /usr/ldap/etc/ibmslapd.conf
```

Note

If you need to stop the LDAP admin server (IBM Directory Server), run the following command, making sure to include `cn=` in the username:

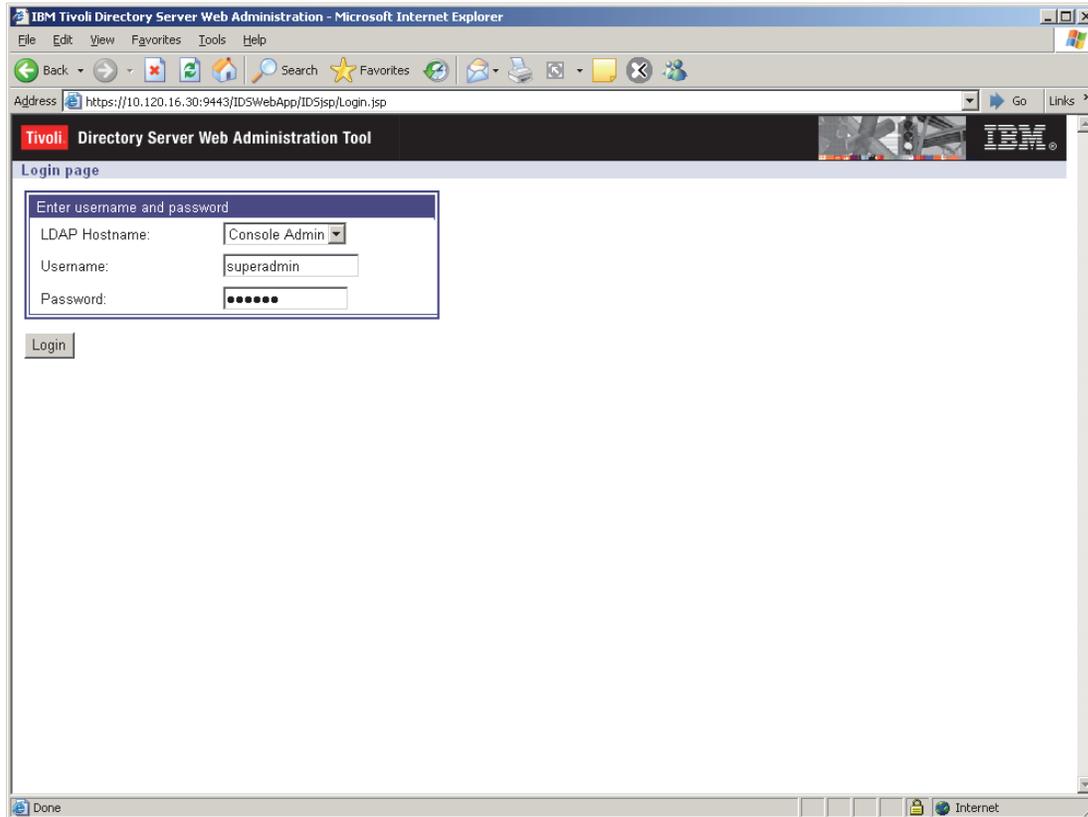
```
/usr/ldap/bin/ibmdirctl \  
-D <step_7a_username_including_cn=> \  
-w <step_7a_password> admstop
```

12. Start the actual LDAP server on the supplied port (include `cn=` in the username):

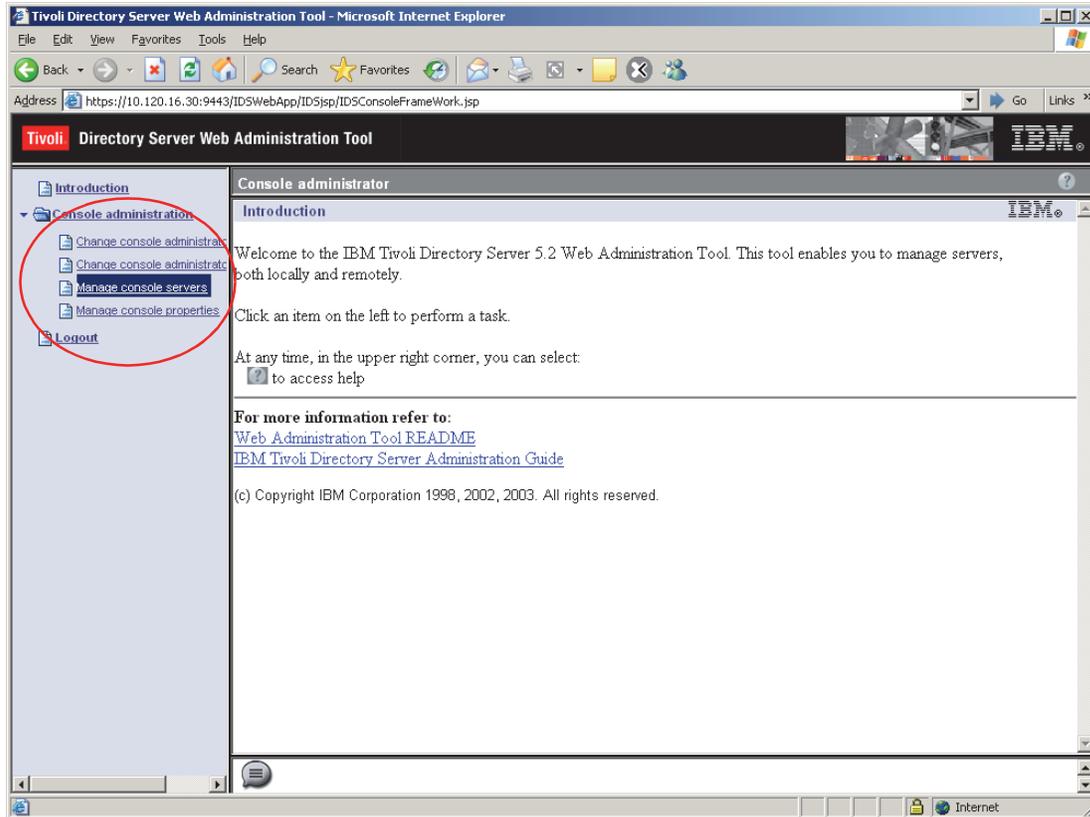
```
ibmdirctl -D <step_7a_username> -w <step_7a_password>  
start|stop|restart|status
```
13. Start the LDAP web administration tool:

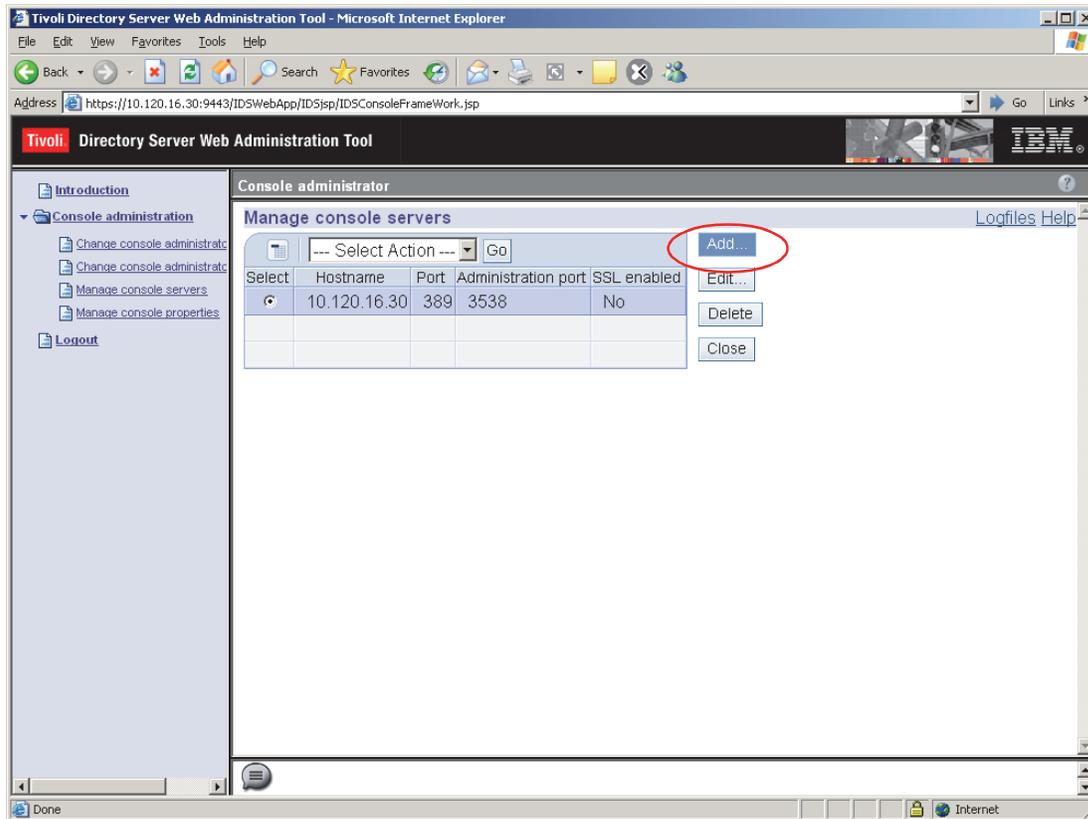
```
/usr/ldap/appsrv/bin/startServer.sh server1
```

- a. Test that you can log in to the following server:
- `http://<hostname>:9780/IsDSWebApp/IDSjsp/Login.jsp`
- Username: superadmin
 - Password: secret

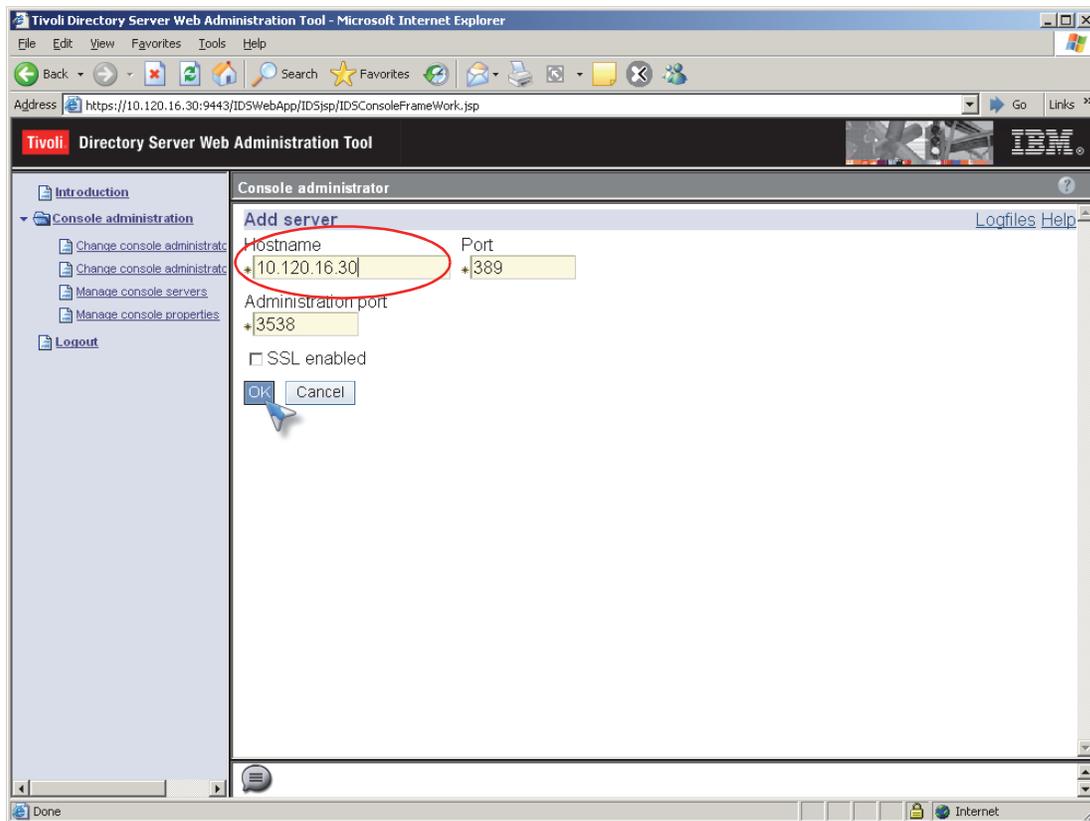


- b. Expand **Console administration** on the left-hand tree and select **Manage console servers**.

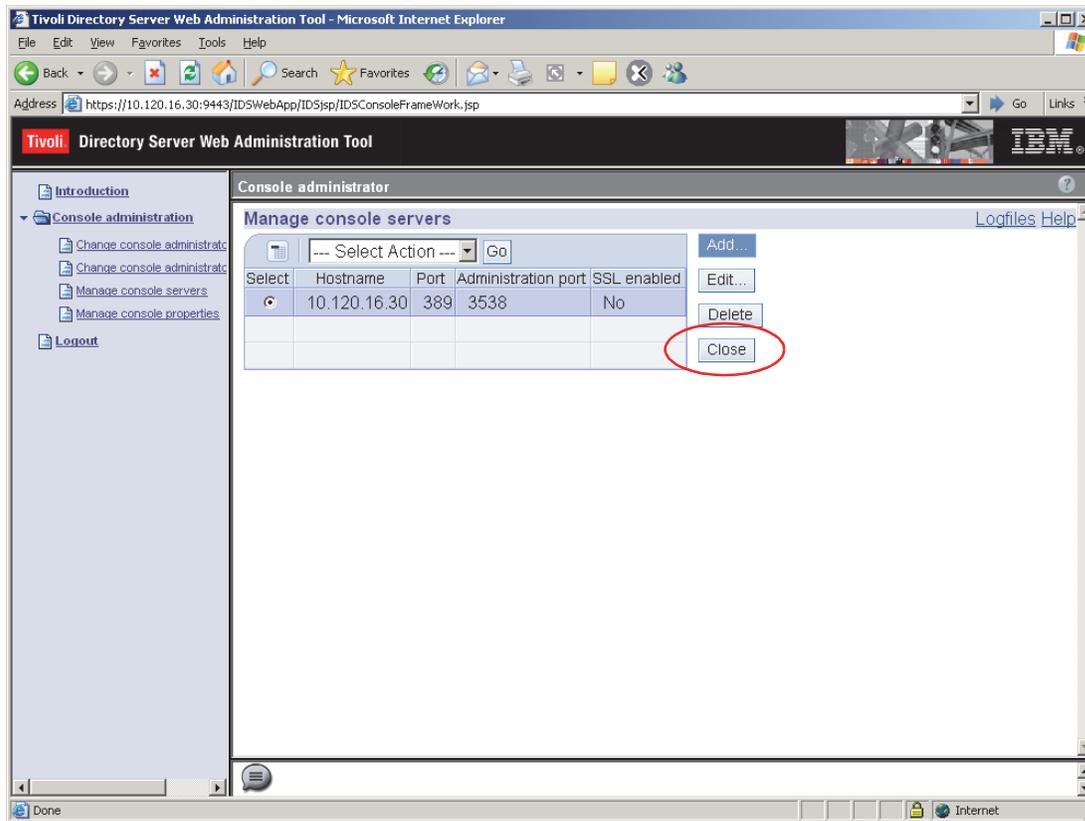


c. Click **Add**.

- d. Enter the host name for the LDAP server and click **OK**.

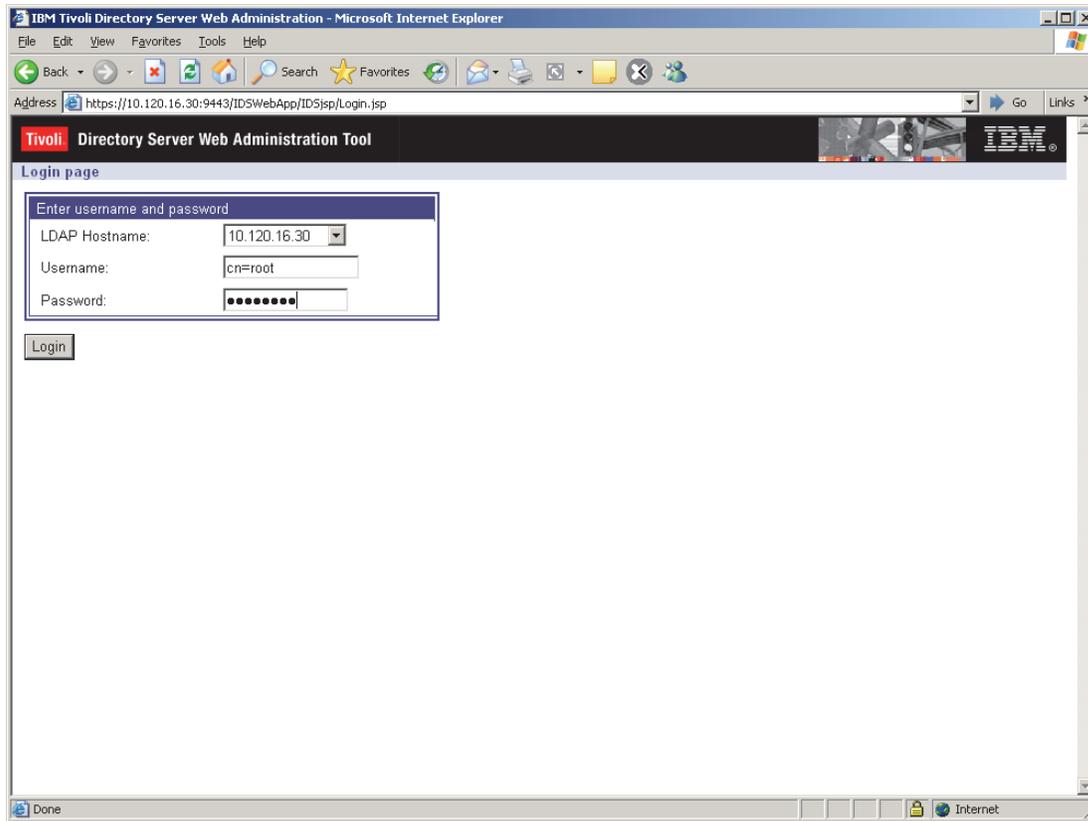


e. Click on **Close**.

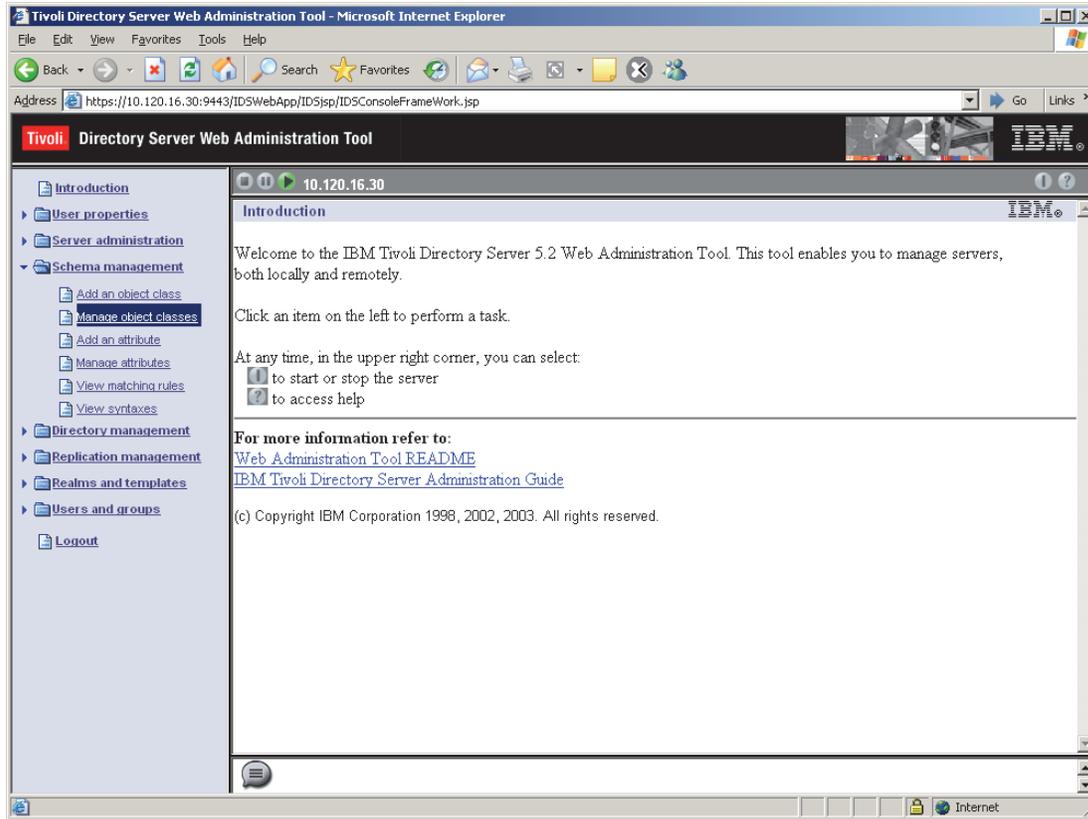


f. Log out of the site.

- g. Log back in using the username and password from [step 7 on page 57](#). Click in the “LDAP Hostname” field and select the server you just added above.



- h. From the left-hand tree, expand **Schema management** and click **Manage object classes**.



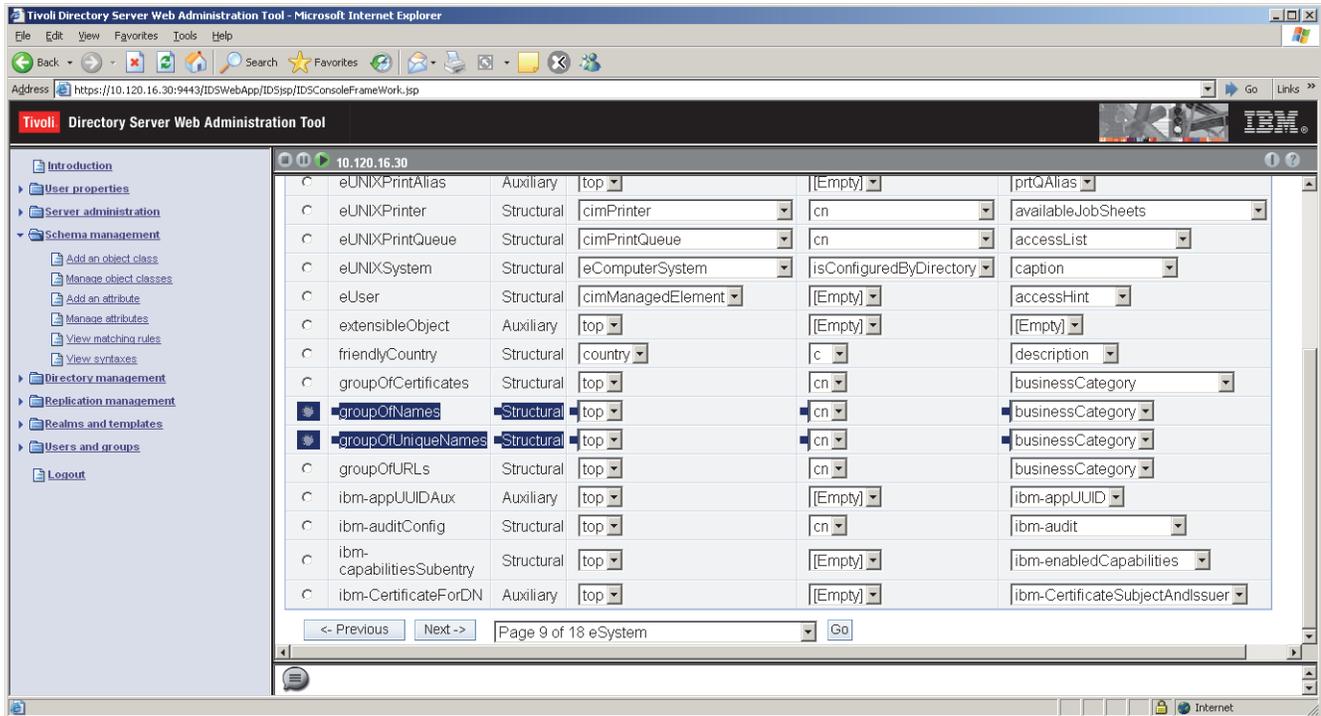
- i. Select **Page 9** from the pull-down menu at the bottom of the page and click **Go**.

The screenshot shows the Tivoli Directory Server Web Administration Tool interface. The left sidebar contains a navigation menu with the following items: Introduction, User properties, Server administration, Schema management (expanded), Directory management, Replication management, Realms and templates, Users and groups, and Logout. The 'Schema management' section is expanded, and the 'Add an object class' link is circled in red. The main area displays a table of object classes with the following columns: Object Class, Type, Parent, and Attribute. A dropdown menu is open at the bottom of the table, showing a list of pages from 'Page 1 of 18' to 'Page 18 of 18'. 'Page 9 of 18 eSystem' is selected and highlighted in blue. The 'Go' button is visible at the bottom right of the table area.

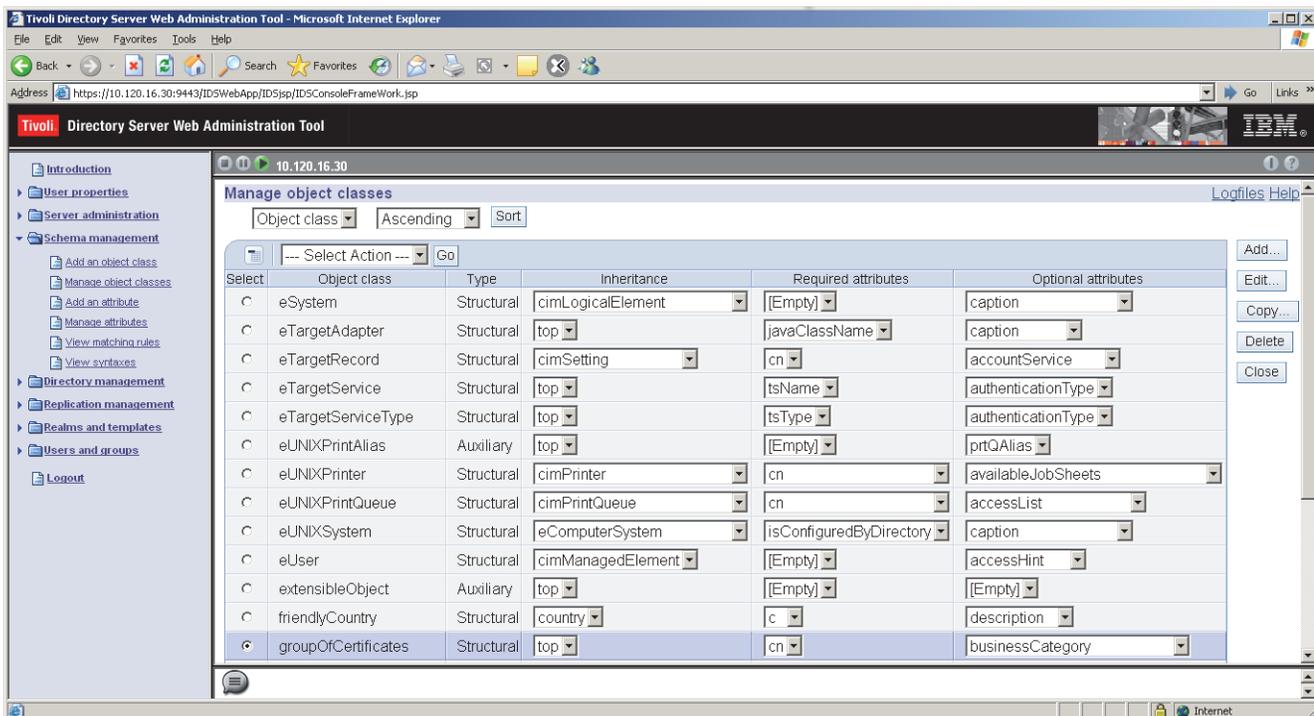
Object Class	Type	Parent	Attribute
<input type="radio"/> AIXAccount	Structural	eAccount	gid
<input type="radio"/> AIXAdmin	Structural	top	[Empty]
<input type="radio"/> aixAuxAccount	Auxiliary	top	[Empty]
<input type="radio"/> aixAuxGroup	Auxiliary	top	[Empty]
<input type="radio"/> alias	Structural	top	aliasedObjectName
<input type="radio"/> aliasObject	Structural	top	[Empty]
<input type="radio"/> applicationEntity	Structural	top	[Empty]
<input type="radio"/> applicationProcess	Structural	top	[Empty]
<input type="radio"/> BBOPIRAliasDef	Structural	top	[Empty]
<input type="radio"/> BBOPIRAttributeDef	Structural	top	[Empty]
<input type="radio"/> BBOPIRConstantDef	Structural	top	[Empty]
<input type="radio"/> BBOPIREnumDef	Structural	top	[Empty]
<input type="radio"/> BBOPIRExceptionDef	Structural	top	[Empty]
<input type="radio"/> BBOPIRInterfaceDef	Structural	top	[Empty]
<input type="radio"/> BBOPIRModuleDef	Structural	top	[Empty]

Page 1 of 18 accessGroup
Page 2 of 18 BBOPIROperationDef
Page 3 of 18 cimDiskDrive
Page 4 of 18 cimPrintQueue
Page 5 of 18 deltaCRL
Page 6 of 18 eDesktopMonitor
Page 7 of 18 eMotherBoardConfiguration
Page 8 of 18 eOnDemandApplicationSystem
Page 9 of 18 eSystem
Page 10 of 18 ibm-changelog
Page 11 of 18 ibm-pwdPolicyExt
Page 12 of 18 ibm-slapiAdmin
Page 13 of 18 ibm-staticGroup
Page 14 of 18 javaMarshaledObject
Page 15 of 18 nsLIProfile
Page 16 of 18 pkiUser
Page 17 of 18 Routing_Information_Object
Page 18 of 18 uniquelyIdentifiedUser

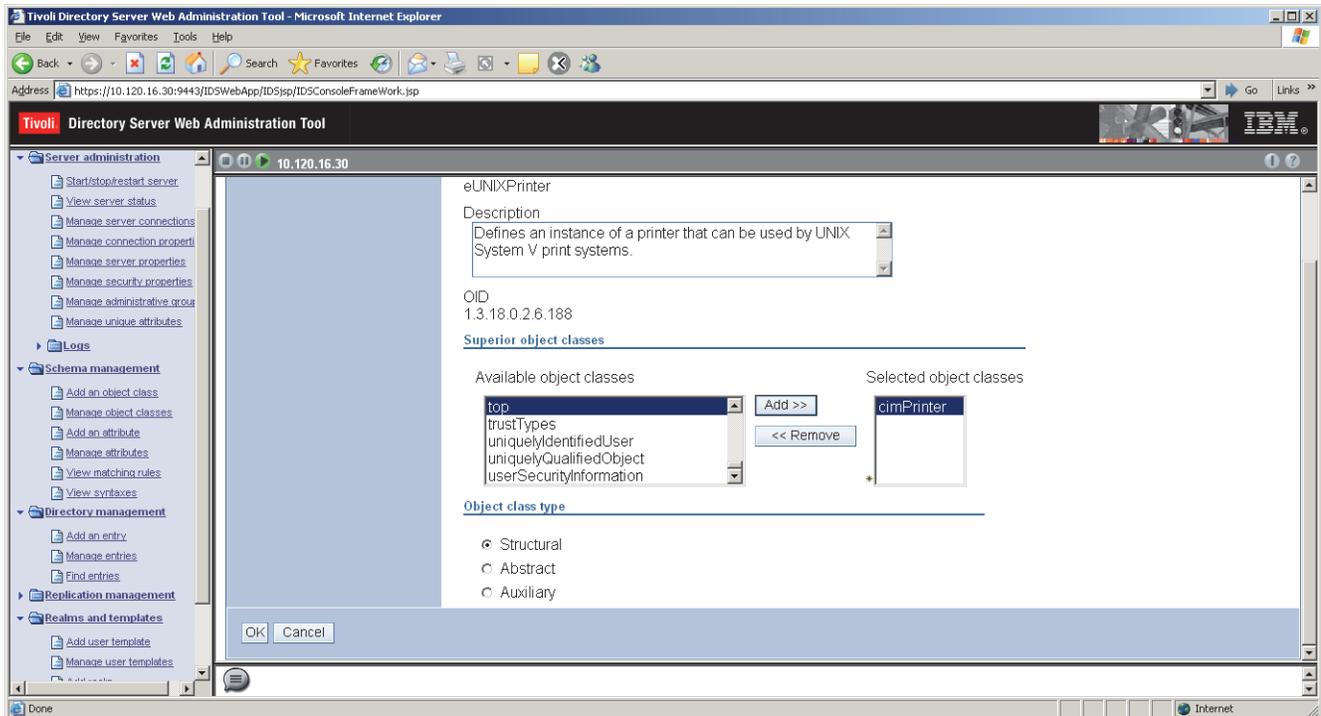
- j. For `groupOfNames` and `groupOfUniqueNames` complete the steps below (ending with step j4 on page 68):



- 1) Select `groupOfNames` (or `groupOfUniqueNames`) and click **Edit**.



- 2) Remove the item Member (or uniquemember) by selecting the item from the list on the right-hand side and clicking **Remove**. Click **OK**.



- 3) Repeat steps j1 and j2 (starting on page [page 67](#)) for the remaining group.
 - 4) Once the offending items have been removed for both groupOfNames and groupOfUniqueNames click on **Close**.
- k. Log out of the site.
 - l. Stop the server:
`/usr/ldap/appsrv/bin/stopServer.sh server1`
14. Install WebSphere Portal Server.

Appendix E

Integrating LDAP with Network Deployment and WebSphere_Portal

This appendix contains the following sections:

- [LDAP Integration Procedures](#)
- `wpsconfig.properties`

LDAP Integration Procedures

1. Stop all running servers:
 - Network Deployment server named “dmgr”
 - WAS WebSphere_Portal
 - server1
 - NodeAgent
2. Restart the Network Deployment server (dmgr) and NodeAgent.
3. Stop and restart the LDAP servers. For instructions, see [steps 11 and 12 on page 58](#).
4. Edit `wpsconfig.properties` (in `<portal install root>/config`) by entering new values for the properties, as shown in [Table E-1, on page 71](#).
5. Validate that the LDAP server is properly configured. Change to the directory `<portal install root>/config`:

```
./WPSconfig.sh validate-ldap \  
-DWasPassword=wpsbind \  
-DPortalAdminPwd=wpsadmin \  
-DLTPAPassword=<password entered in step 3 on page 56> \  
-DLDAPAdminPwd=<password entered in step 3 on page 56> \  
-DWmmSystemIdPassword=wmmssystemid
```

If this step fails, review all the changes. Otherwise, continue with the next step.

6. Enable security for the LDAP server:

```
./WPSconfig.sh enable-security-ldap \  
-DWasPassword=wpsbind \  
-DPortalAdminPwd=wpsadmin \  
-DDbPassword=<password entered in step 3 on page 56> \  
-DLTPAPassword=<password entered in step 3 on page 56> \  
-DLDAPAdminPwd=<password entered in step 3 on page 56> \  
-DWmmSystemIdPassword=wmmssystemid
```

This step will not complete successfully and will need to be run a number of times. Solutions to the failures will differ from machine to machine, but some common solutions are given below:

- The first failure is likely to be the inability to copy one of the many files (likely `wmmLDAPAttributes.xml`). This appears to be a script issue and can be resolved by manually copying the file from `<portal install root>/wmm/backup/wmmDBAttributes.xml_<date and time>` to the ND machine `<nd install root>/config/wmm`.
 - The second failure is likely to be the WebSphere_Portal server not being able to restart. This is because of changes to the security settings. Shut down ND, WebSphere_Portal, server1, and NodeAgent, and restart all of them (note that WebSphere ND will now require a login and password: `wpsbind/wpsbind`).
7. Shut down ND, WebSphere_Portal, server1 and NodeAgent and restart all of them (note that WebSphere ND will now require a login and password: `wpsbind/wpsbind`).
 8. Run post 5.1.0.1 Portal upgrade script:

```
./WPSconfig.sh CONFIG-WP-PTF-5101 -DPortalAdminPwd=wpsadmin \  
-DWasPassword=wpsbind
```

9. Shut down ND, WebSphere_Portal, server1 and NodeAgent and restart all of them (note that WebSphere ND will now require a login and password: wpsbind/wpsbind).

It is now possible to install CS on the WebSphere_Portal server.

10. Connect to the portal `http://<hostname>:<port>/wps/portal/`. Click on **login** in the upper right-hand corner and enter: `wpsadmin/wpsadmin`

wpsconfig.properties

Table E-1 lists properties for which you must provide new values. The properties are located in `wpsconfig.properties` file.

Table E-1: Properties in `wpsconfig.properties`

Property	Original Value	New value
WasUserId	ReplaceWithYourWASUserId	uid=wpsbind, cn=users, dc=<dns step 8 on page 57>, dc=<dns extension step 8 on page 57>
WasPassword	ReplaceWithYourWASUserPwd	wpsbind
WpsHostName		<host name of Portal server>
WpsHostPort	9080	9180 (or the port on which WAS Portal is running)
WpsAdminConsolePort		9190 (or the port on which the admin server is running)
PortalAdminId	uid=portaladminid, o=default organization	uid=wpsadmin, cn=users, dc=<dns step 8 on page 57>, dc=<dns extension step 8 on page 57>
PortalAdminPwd	none	wpsadmin
PortalAdminGroupId	cn=wpsadmins, o=default organization	cn=wpsadmins,cn=groups, dc=<dns step 8 on page 57>, dc=<dns extension step 8 on page 57>
WpsContentAdministrators	cn=wpsContentAdministrators, o=default organization	cn=wpsContentAdministrators, cn=groups, dc=<dns step 8 on page 57>, dc=<dns extension step 8 on page 57>
WpsDocReviewer	cn=wpsDocReviewer, o=default organization	cn=wpsDocReviewer, cn=groups, dc=<dns step 8 on page 57>, dc=<dns extension step 8 on page 57>
WpsDbName	wpsdb	<name entered in step 7 on page 57>

Table E-1: Properties in wpcnfig.properties (continued)

Property	Original Value	New value
DbUser	db2admin	wportusr
DbPassword	ReplaceWithYourDbAdminPwd	<password for user created in step 7 on page 57>
LTPAPassword	none	<password for user created in step 7 on page 57>
SSODomainName	none	<dnsname name>.<dns name extension>;<dnsname name>.<dns name extension>
LDAPHostName	yourldapserver.com	<fully qualified hostname for this server>
LDAPPort	389	389 (nonssl), 636 (SSL)
LDAPAdminPwd	none	Password for user given for LDAPAdminUID
LDAPBindID	uid=wpsbind, cn=users, dc=yourco, dc=com	uid=wpsbind, cn=users, dc=<dns step 8 on page 57>, dc=<dns extension step 8 on page 57>
LDAPBindPassword	none	wpsbind
WmmSystemId	none	uid=wmmssystemid, cn=users, dc=<dns step 8 on page 57>, dc=<dns extension step 8 on page 57>
WmmSystemIdPassword	none	wmmssystemid
LDAPSuffix	dc=yourco,dc=com	dc=<dns step 8 on page 57>, dc=<dns extension step 8 on page 57>
LDAPsslEnabled	FALSE	false (nonssl), true (SSL)
SSORequiresSSL	FALSE	false (nonssl), true (SSL)
CellName	<cell name given during installation>	This will be incorrect as integration with ND has changed it. Look up the correct name of the ND cell and enter it here.
NodeName	<node name given during installation>	This should not need to be changed after integration with ND, but should be verified.

Appendix F

Debugging Procedures

This appendix provides debugging procedures that are applicable should you encounter a problem during the Content Server installation.

This appendix contains the following sections:

- [Connecting to WebSphere Application Server](#)
- [Resolving Content Server Installation Problems](#)

Connecting to WebSphere Application Server

If you are unable to connect to WAS from a web server on another machine or you are running on a non-standard port (not 80 or 443), complete the following steps:

1. Log in to the WAS Administrative Console.
2. In the left-hand tree, select **Environment > Virtual Hosts**.
In the list there are two groups by default:
 - **admin_host** (the administrative console running on 9090)
 - **default_host** (the default host created by the installation and running on 9080)
3. Select **default_host** and under **Additional Properties** select **Host Aliases**.
4. By default there are three entries, one for each of the following ports: 80, 443 and 9080, all associated to * (all hosts).
If you wish to change this so that your system does not accept direct connections to port 9080, remove the entry for 9080.
If you are running on a port other than 80 or 443, add an entry line for the hosts (and their ports) from which you will be connecting.
5. Save the changes.

Resolving Content Server Installation Problems

If a Content Server installation does not complete successfully, procedures in this section can help you resolve the problem. The following procedures are provided:

- [Removing All Files and Tables](#)
- [Resolving HelloCS and pingdb Problems](#)
- [Turning on Debugging](#)

The first procedure provides steps that you **must** follow if a Content Server installation does not complete successfully. The second and third procedures provide optional steps that may help you identify installation problems.

Removing All Files and Tables

If a Content Server installation does not complete successfully, you **must** perform the following steps before you reinstall.

1. Remove the deployment in WAS, then confirm manually that the directories were deleted. Restart WAS.
2. Delete all the files in the following locations:
 - <cs install directory>
 - <cs shared directory>
3. Delete all the tables created by Content Server in the database, as the Content Server installer cannot update existing tables.

Resolving HelloCS and pingdb Problems

If either the HelloCS test or the pingdb test failed when you performed [step 8](#) of “[Installing Content Server](#),” the following sections may be helpful to you. They provide suggestions on how to resolve the problem that may be causing test failure.

HelloCS Test

- If the HelloCS test fails (HelloCS page is not displayed) and you are deploying through a web server, complete the following steps:
 1. Connect directly to WAS instead of deploying through the web server.
 2. Repeat the HelloCS test by going to the following URL:
`http://<hostname>:<port>/<context root>/HelloCS`
 3. If the HelloCS test is then successful with a direct connection to WAS, the web server is not configured correctly. Check the configuration of the web server; if you need help, consult the web server documentation or your web server provider.
 4. If the HelloCS test is not successful, continue reading.
- If the HelloCS test fails with a direct connection to WAS, then the Content Server application may not be deployed correctly. Complete the following steps:
 1. Redeploy the Content Server application by doing the following:
 - a. Log in to the WAS Administrative Console.
 - b. Uninstall the Content Server application in the console.
 - c. Save the changes.
 - d. Redeploy the Content Server application ([step 6](#) in “[Installing Content Server](#)”).
 - e. Start the Content Server application ([step 7](#) in “[Installing Content Server](#)”).
 2. Repeat the HelloCS test.
 3. If the test fails, restart WAS.
 4. Run the “First Steps” demo provided with WAS.
 5. Do one of the following:
 - If the **Verify** option in the “First Steps” demo passes, continue to the next step.
 - If the **Verify** option fails, then WAS is not configured properly. Check the WAS configuration; if you need help, consult the WAS documentation or your WAS provider.
 6. Restart WAS, then repeat the HelloCS test. If the HelloCS test is displayed correctly, you have resolved the installation problem.

pingdb Test

The pingdb test fails if the JDBC data source is not properly configured in WAS, or in Content Server, or both.

Complete the following steps to investigate possible problems related to the JDBC data source:

1. In the WAS Administrative Console, browse to the correct JDBC data source and use the **Test** option to verify that the data source works.
2. If the data source is not working, it is incorrectly configured in WAS. Do the following:
 - a. Reconfigure the data source (if you need instructions, see “[Configuring WAS JDBC Providers](#),” on page 49).
 - b. Test the data source by repeating the pingdb test from [step 1](#).
 - c. When the data source is working, continue to the next step.
3. If the data source is working, test whether Content Server can connect to the database via the application server. Perform the pingdb test by going to the following URL:

```
http://<hostname>:<port>/<context root>/
CatalogManager?ftcmd=pingdb
```

If this test passes, stop here. Otherwise, continue to the next step.
4. If the pingdb test from [step 3](#) failed, confirm that the data source that you configured in Content Server matches the data source configured in WAS. If the data sources do not match, complete the following steps:
 - a. Close the installer.
 - b. Restart the installer ([step 4](#), in “[Installing Content Server](#)”).
 - c. Complete the remaining steps in “[Installing Content Server](#).”

Turning on Debugging

If a Content Server installation does not complete successfully, you may want to turn on debugging when you reinstall Content Server. Doing so might help identify problems during the installation. Note, however, that turning on debugging might significantly increase the time it takes to install Content Server.; so, turn on debugging only if you need to identify an installation problem.

Note

Turning on debugging is helpful only after the Content Server application is deployed.

To turn on debugging

1. Deploy, but do not start, the Content Server application in the WAS Administrative Console ([step 6](#) in “[Installing Content Server](#)”).
2. Browse to the installation location:

```
<WAS Install directory>\InstalledApps\<Node name>\
ContentServer.ear\cs.war\WEB-INF\classes\
```
3. Edit the file named `commons-logging.properties` by replacing every occurrence of `INFO` with `DEBUG` (using capital letters).
See the *Content Server Property Files Reference* if you need more information about editing property files.
4. In the WAS Administrative Console, do the following:

- a. Navigate to the Enterprise Applications selection (just as you would to start the application).
 - b. Select the Content Server application and change the values of the following properties as shown below.
 - **Classloader Mode:** Parent Last
 - **WAR Classloader Policy:** Application
 - c. Save the changes and continue the installation.
5. Navigate to the `<cs install directory>`. You will see a large file named `futuretense.txt`, which contains detailed debugging information.

If you need more information about `futuretense.txt`, see the *Content Server Property Files Reference*

Note

After the installation is complete, turn off debugging (by reversing the changes made in [step 3](#)) to avoid potential adverse effects on performance.

