

# FatWire | Content Server 7

Version 7.0.1

## Configuring Third-Party Software

**Document Revision Date:** Jul. 12, 2007



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 © 2007 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 limitations 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."

#### *Configuring Third-Party Software*

Document Revision Date: Jul. 12, 2007

Product Version: 7.0.1

#### **FatWire Technical Support**

[www.fatwire.com/Support](http://www.fatwire.com/Support)

#### **FatWire Headquarters**

FatWire Corporation  
330 Old Country Road  
Suite 207  
Mineola, NY 11501  
[www.fatwire.com](http://www.fatwire.com)

## Table of Contents

|                                   |          |
|-----------------------------------|----------|
| <b>About This Guide</b> .....     | <b>7</b> |
| How This Guide is Organized ..... | 7        |
| Who Should Use This Guide .....   | 7        |
| Graphics in This Guide .....      | 7        |
| Technical Support .....           | 8        |

### Part 1. Creating and Configuring a Database

|  |           |
|--|-----------|
| <b>1 Creating and Configuring an Oracle 9.2.0.x Database</b> ..... | <b>11</b> |
| Step I. Create an Oracle 9.2.0.x Database .....                    | 12        |
| Step II. Configure the Database for Content Server .....           | 15        |
| Next Step .....  | 19        |
| <b>2 Creating and Configuring an Oracle 10g Database</b> .....     | <b>21</b> |
| Step I. Create an Oracle 10g Database .....                        | 22        |
| Step II. Create a New User for Content Server .....                | 37        |
| Next Step .....  | 44        |
| <b>3 Creating and Configuring an MS SQL Server Database</b> .....  | <b>45</b> |
| Creating a Database on MS SQL Server 2000 SP3+ .....               | 46        |
| Creating a Database on MS SQL Server 2005 .....                    | 46        |
| <b>4 Creating and Configuring an IBM DB2 8.x Database</b> .....    | <b>49</b> |
| Creating and Configuring DB2 8.x for Content Server .....          | 50        |
| <b>5 Creating and Configuring an IBM DB2 9.1 Database</b> .....    | <b>53</b> |
| Installing and Configuring DB2 9.1 for Content Server .....        | 54        |
| A. Install DB2 .....   | 54        |
| B. Create a New DB2 Database .....                                 | 68        |

|   |    |
|---|----|
| C. Create a User for the New Database ..... | 74 |
| D. Configure the Database .....             | 77 |

## Part 2. Installing a Web Server

|   |           |
|---|-----------|
| <b>6 Worksheets for Documenting the Web Server Installation .....</b> | <b>83</b> |
| Key to Sample Values .....  | 84        |
| Web Server Parameters .....   | 84        |
| <b>7 Installing IIS on Windows .....</b>                              | <b>87</b> |
| Step I. Install IIS .....   | 88        |
| Step II. Document Your IIS Installation .....                         | 88        |
| Step III. Verify the Installation .....                               | 88        |
| A. Start IIS .....  | 88        |
| B. Verify that IIS is Serving Pages .....                             | 89        |
| Next Step .....   | 89        |
| <b>8 Installing Apache on Solaris and Linux .....</b>                 | <b>91</b> |
| Step I. Install Apache .....  | 92        |
| Step II. Document Your Apache Parameters .....                        | 92        |
| Step III. Verify that Apache Contains the Correct Module .....        | 93        |
| Step IV. Verify that Apache Runs Properly .....                       | 93        |
| Next Step .....   | 93        |

## Part 3. Installing and Configuring LDAP

|   |            |
|---|------------|
| <b>9 Setting Up Sun Access Manager 7.0 .....</b>      | <b>97</b>  |
| Start/Stop Commands .....                             | 98         |
| Creating CS Users in Sun Access Manager .....         | 98         |
| <b>10 Setting Up Sun Directory Server 6.0 .....</b>   | <b>107</b> |
| Start/Stop Commands .....                             | 108        |
| Sun Directory Server .....                            | 108        |
| Sun Java Web Console .....                            | 108        |
| Installing Sun Directory Server .....                 | 109        |
| Post-Installation Steps .....                         | 114        |
| Completing and Verifying the LDAP Configuration ..... | 115        |
| Modifying User Passwords .....                        | 122        |
| <b>11 Setting Up OpenLDAP 2.3.x .....</b>             | <b>131</b> |
| OpenLDAP Commands .....                               | 132        |

|  |            |
|--|------------|
| Starting OpenLDAP . . . . .  | 132        |
| Searching an OpenLDAP Server . . . . .                                 | 132        |
| Adding an LDIF File to an OpenLDAP Server . . . . .                    | 133        |
| Installing OpenLDAP . . . . .  | 134        |
| Configuring OpenLDAP . . . . .   | 136        |
| Adding Content Server Schema to OpenLDAP . . . . .                     | 139        |
| Modifying User Passwords . . . . .                                     | 141        |
| Modifying User Passwords Using an LDAP Browser . . . . .               | 141        |
| Modifying User Passwords Using the ldapmodify Command . . . . .        | 144        |
| <b>12 Setting Up the WebLogic 9.x Embedded LDAP Server . . . . .</b>   | <b>145</b> |
| Enabling the WebLogic Embedded LDAP Server . . . . .                   | 146        |
| Modifying User Passwords . . . . .                                     | 148        |
| <b>13 Setting Up Oracle Directory Server 10.x . . . . .</b>            | <b>151</b> |
| Start/Stop Commands . . . . .  | 152        |
| Installing Oracle Directory Server . . . . .                           | 152        |
| A. Pre-Installation Steps . . . . .                                    | 152        |
| B. Install Oracle Directory Server . . . . .                           | 154        |
| C. Post-Installation Steps . . . . .                                   | 165        |
| Accessing Oracle Directory Manager . . . . .                           | 166        |
| Configuring ODS Password Security for Content Server . . . . .         | 169        |
| Modifying User Passwords . . . . .                                     | 172        |
| Deleting Users . . . . .   | 173        |
| Connecting to ODS Using an LDAP Browser . . . . .                      | 174        |
| <b>14 Setting Up MS Active Directory Server 2003 . . . . .</b>         | <b>177</b> |
| Installing MS Active Directory Server . . . . .                        | 178        |
| A. Install the Operating System . . . . .                              | 178        |
| B. Set the Machine's Name and Suffix . . . . .                         | 178        |
| C. Configure the Machine's Network Settings . . . . .                  | 180        |
| D. Install the Local DNS Server . . . . .                              | 180        |
| E. Configure the Local DNS Server . . . . .                            | 182        |
| F. Install MS Active Directory Server 2003 . . . . .                   | 189        |
| Accessing the "Active Directory Users and Computers" Console . . . . . | 195        |
| Configuring ADS Password Security for Content Server . . . . .         | 196        |
| Modifying User Passwords . . . . .                                     | 198        |
| Deleting Users . . . . .   | 198        |
| Connecting to ADS Using an LDAP Browser . . . . .                      | 199        |



## About This Guide

This guide contains information about installing and configuring third-party software specifically for use by Content Server. You will use the information in this guide along with the CS installation guide for your platform, and, if you choose to integrate with LDAP, the *LDAP Integration Guide*.

## How This Guide is Organized

The guide is divided into the following parts:

- [Part 1, “Creating and Configuring a Database”](#) – shows you how to create and configure the supported databases before you install Content Server. (Supplements the Content Server installation guides.)
- [Part 2, “Installing a Web Server”](#) – shows you how to install and configure the supported web servers, if you choose to use one. (Supplements the Content Server installation guides.)
- [Part 3, “Installing and Configuring LDAP”](#) – shows you how to set up the supported LDAP server for integration with Content Server. (Supplements the *LDAP Integration Guide*.)

## Who Should Use This Guide

This guide is for installation engineers who have experience installing and configuring enterprise-level software, including databases, database drivers, application servers, portal servers, and LDAP servers.

## Graphics in This Guide

Graphics in this guide are screen captures of dialog boxes and similar windows that you will interact with during the installation or configuration process. These graphics are presented to help you follow the installation and configuration processes. They are not intended to be sources of information such as parameter values, options to select, and product version numbers.

## Technical Support

Help is available from FatWire Technical Support at the following website:

[http://www.fatwire.com/Support/contact\\_info.html](http://www.fatwire.com/Support/contact_info.html)

## Part 1

# Creating and Configuring a Database

Content Server requires access to a supported database that is specifically configured for the product. Supported databases include:

- Oracle 9, 10g
- Microsoft SQL Server 2000 SP3+, 2005
- DB2 8.2, 9.1

The databases listed above are not configured for production, but are set up with full permissions. In practice, the permissions can be curtailed for the user that Content Server will use to access a database. However, the following rights must exist: ability to create, modify, and delete tables and indexes.

If you need instructions on installing a supported database, refer to the product documentation.

Instructions on creating and configuring the databases for Content Server are given in the chapters of this guide. Because database configuration is identical across different application servers, refer to the correct chapter to set up the database of your choice.

This part contains the following chapters:

- [Chapter 1, “Creating and Configuring an Oracle 9.2.0.x Database”](#)
- [Chapter 2, “Creating and Configuring an Oracle 10g Database”](#)
- [Chapter 3, “Creating and Configuring an MS SQL Server Database”](#)
- [Chapter 4, “Creating and Configuring an IBM DB2 8.x Database”](#)
- [Chapter 5, “Creating and Configuring an IBM DB2 9.1 Database”](#)



## Chapter 1

# Creating and Configuring an Oracle 9.2.0.x Database

Use this chapter to set up an Oracle 9.2.0.x database for your Content Server installation. For background information regarding database configuration and users' permissions, see [“Creating and Configuring a Database,” on page 9](#).

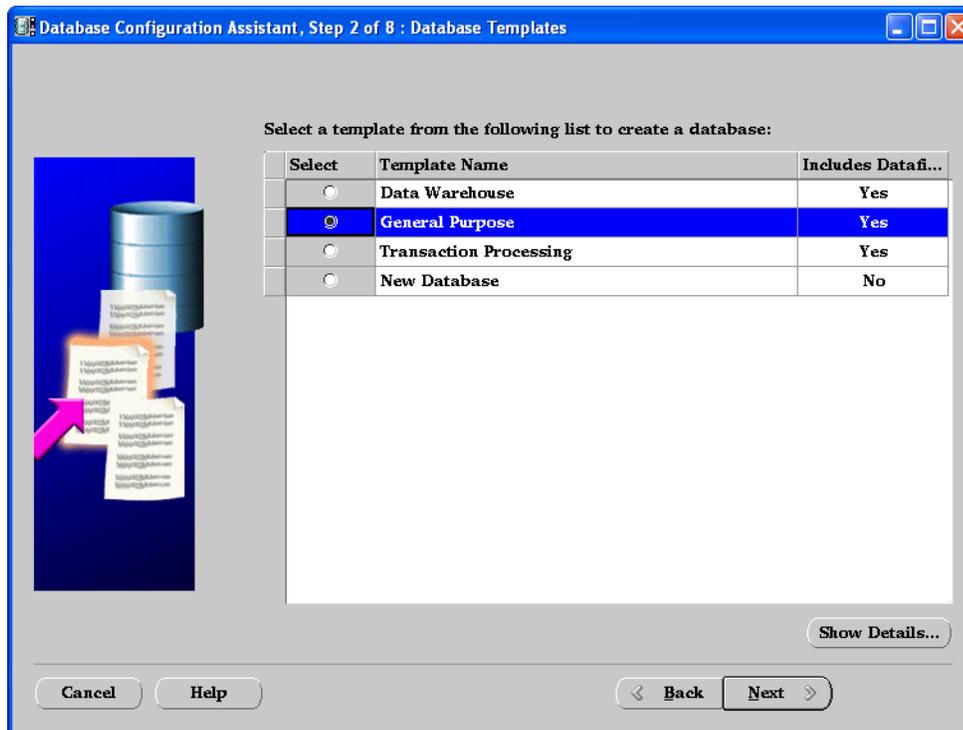
This chapter contains the following sections:

[Step I. Create an Oracle 9.2.0.x Database](#)

[Step II. Configure the Database for Content Server](#)

## Step I. Create an Oracle 9.2.0.x Database

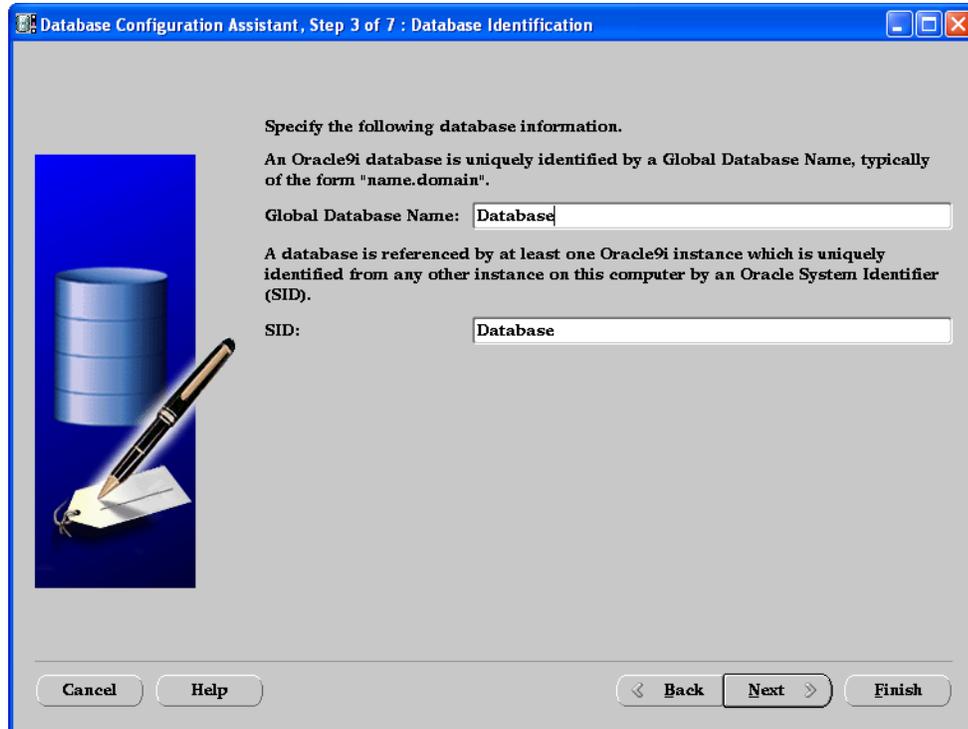
1. Go to the `$ORACLE9_HOME/bin` directory:  
`cd $ORACLE9_HOME/bin`
2. Run the Database Configuration Assistant:  
`dbca`
3. In the welcome screen, click **Next**.
4. Fill in the following screens as shown below:
  - a. On the “Step 1 of 8: Operations” screen, leave **Create a database** selected and click **Next**.
  - b. On the “Step 2 of 8: Database Templates” screen, select **General Purpose** and click **Next**.



### Note

Database block size **must** be at least 4096 bytes. Selecting the **General Purpose** option automatically sets the block size to 8192 bytes.

- c. On the “Step 3 of 7: Database Identification” screen, enter the database name in the Global Database Name field. The SID will be automatically set to the first eight characters of the Database Name. Each SID must be unique. Click **Next**.



Database Configuration Assistant, Step 3 of 7 : Database Identification

Specify the following database information.

An Oracle9i database is uniquely identified by a Global Database Name, typically of the form "name.domain".

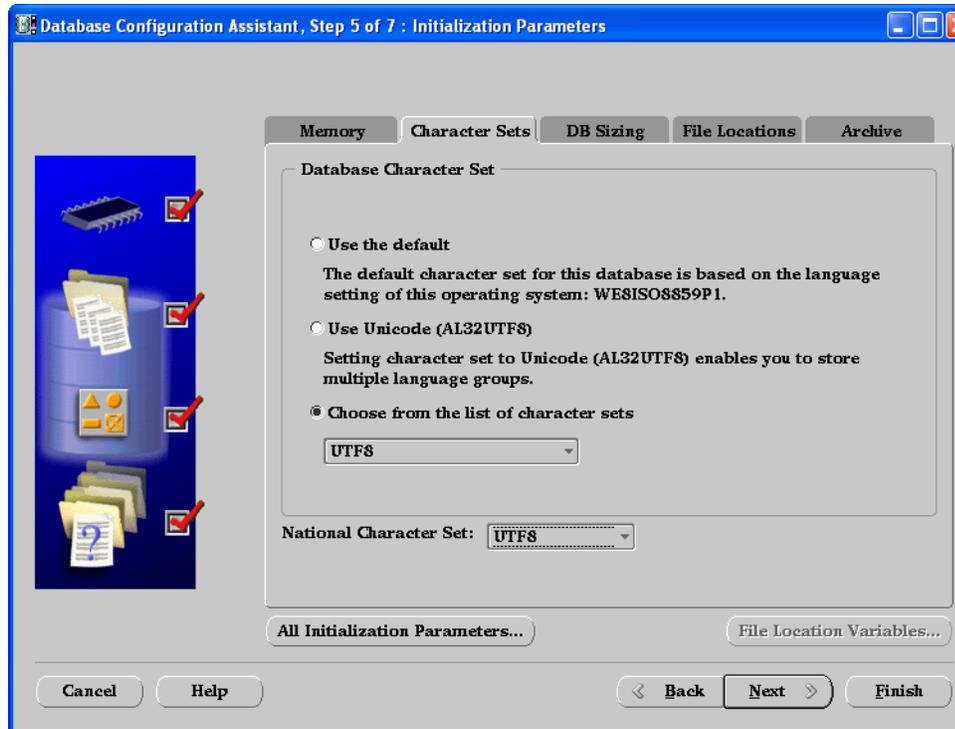
Global Database Name:

A database is referenced by at least one Oracle9i instance which is uniquely identified from any other instance on this computer by an Oracle System Identifier (SID).

SID:

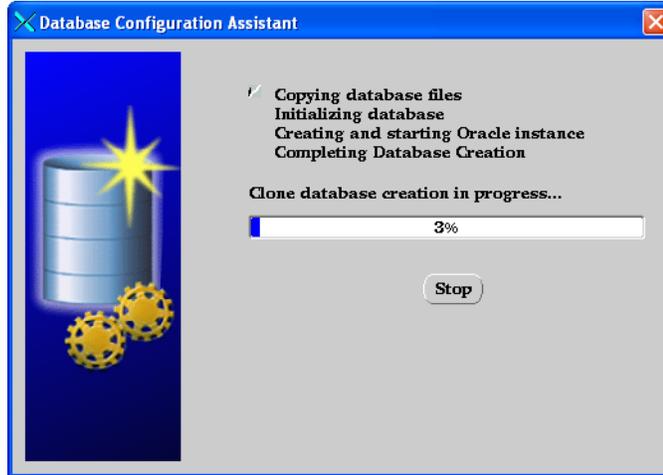
Cancel Help < Back Next > Finish

- d. On the “Step 4 of 7: Database Connection Options” screen, leave **Dedicated Server mode** selected and click **Next**.
- e. On the “Step 5 of 7: Initialization Parameters” screen:
  - 1) Select the tab **Character Sets**.
  - 2) On the character sets screen, select **Choose from the list of character sets** and **UTF8** from the drop-down menu. For the National Character Set select **UTF8** and click **Next**.



- f. On the “Step 6 of 7: Database Storage” screen, click **Next**.
- g. On the “Step 7 of 7: Creation Options” screen, click **Finish**.

5. When the summary screen appears, click **OK**.
6. When the “Installation Progress Screen” appears, wait for the installation to be completed.



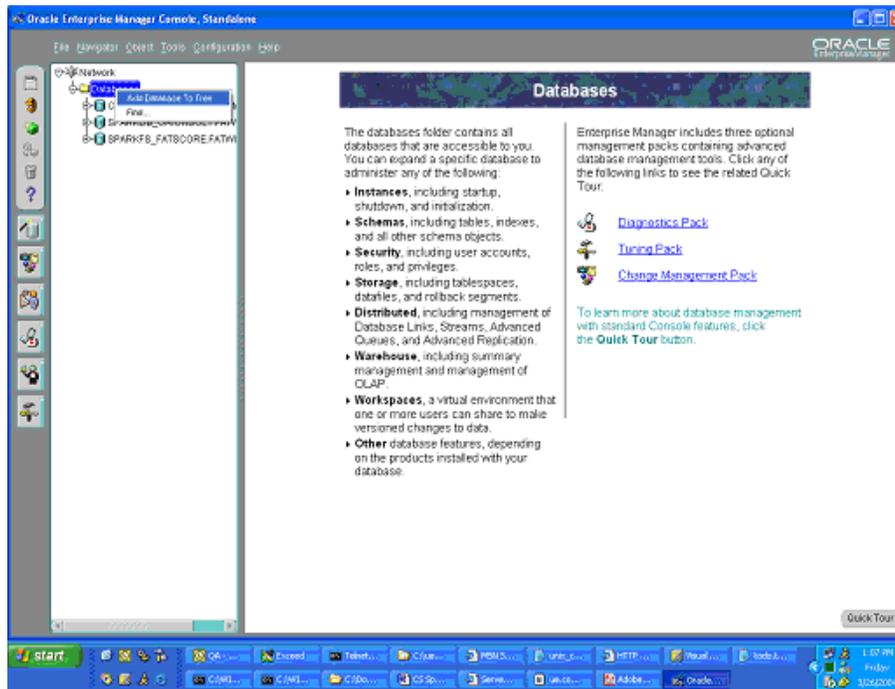
7. After the installation has been completed, the database information screen will appear, listing information about how to connect to this database using the enterprise management console. Click **OK**.

## Step II. Configure the Database for Content Server

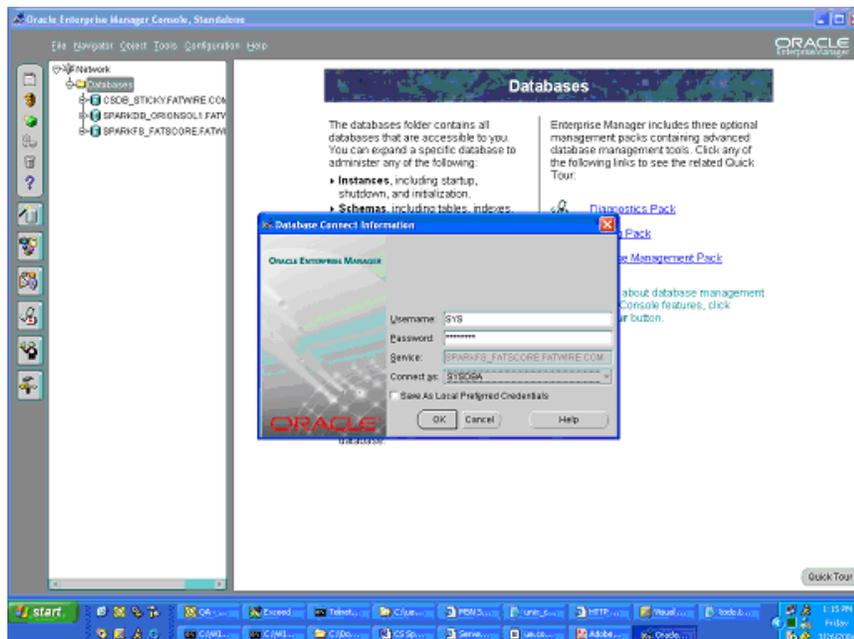
1. Start Oracle Enterprise Manage Console. Click **OK**.



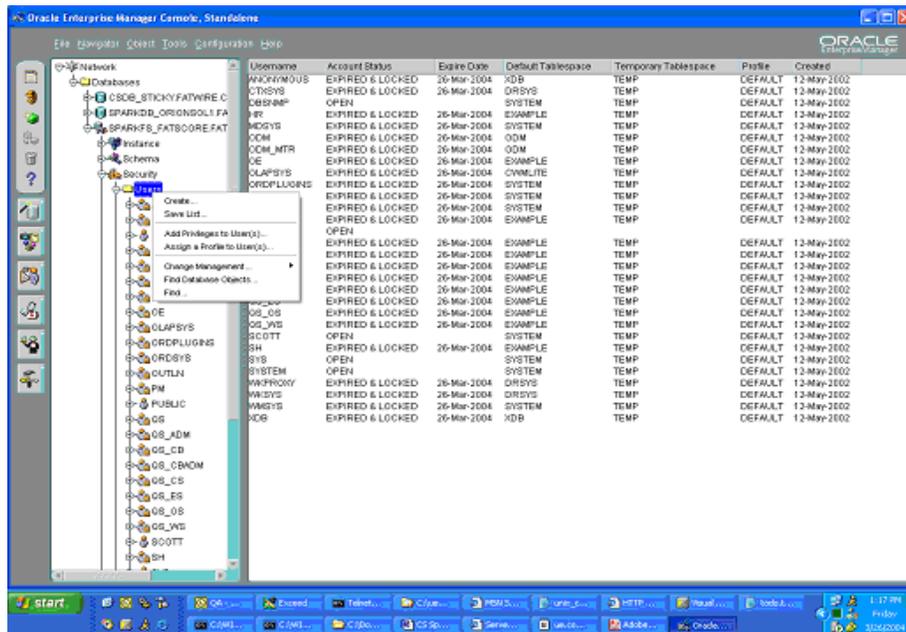
2. Expand **Network > Databases**. Select the database you have created.



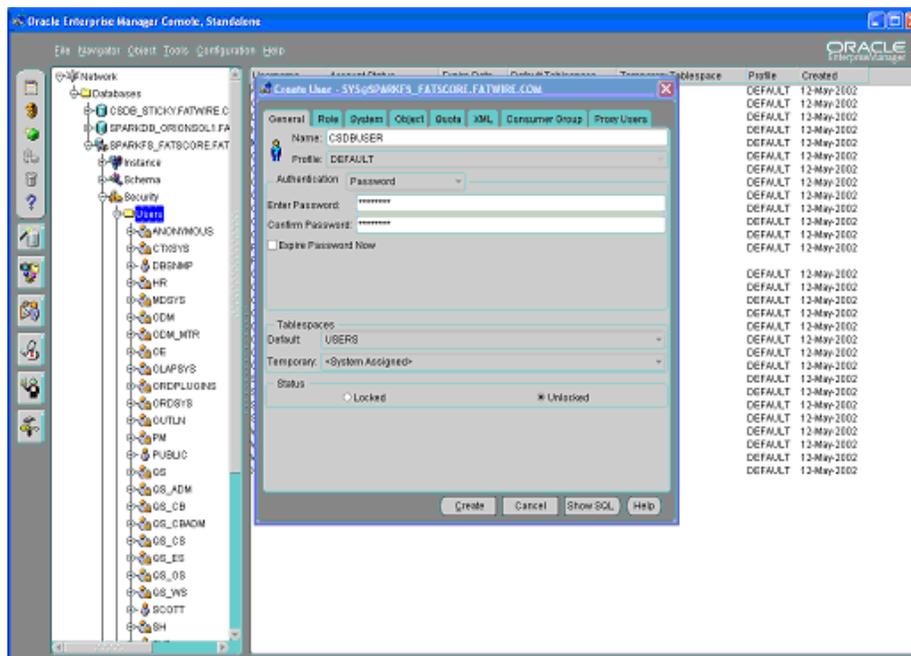
3. In the database login screen, log in as **SYS** and enter the password you specified earlier while creating the database. Click **OK**.



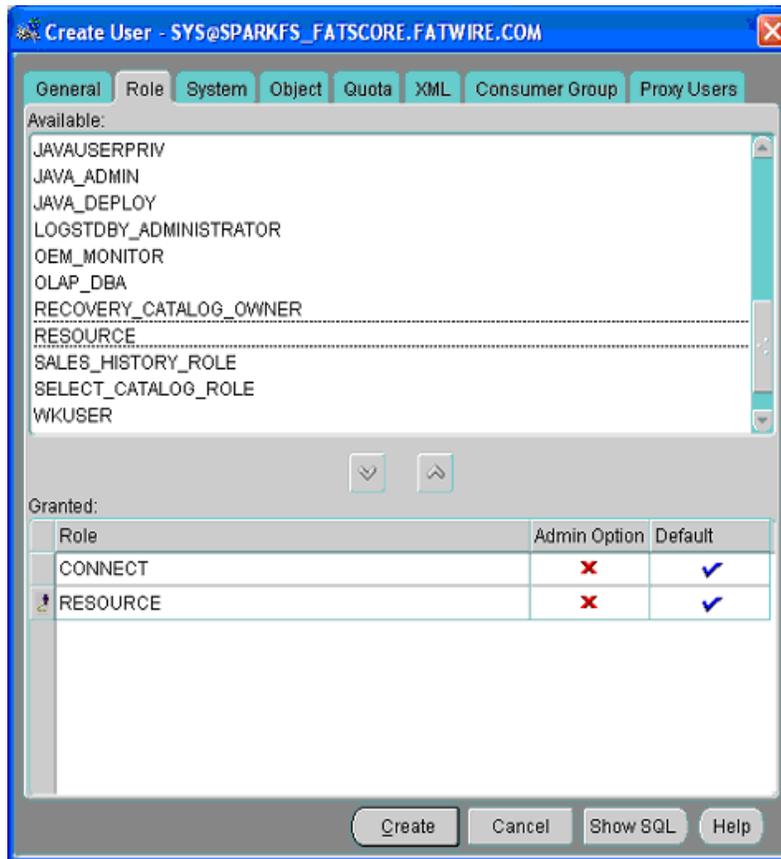
#### 4. Expand Security > Users. Right-click and select Create.



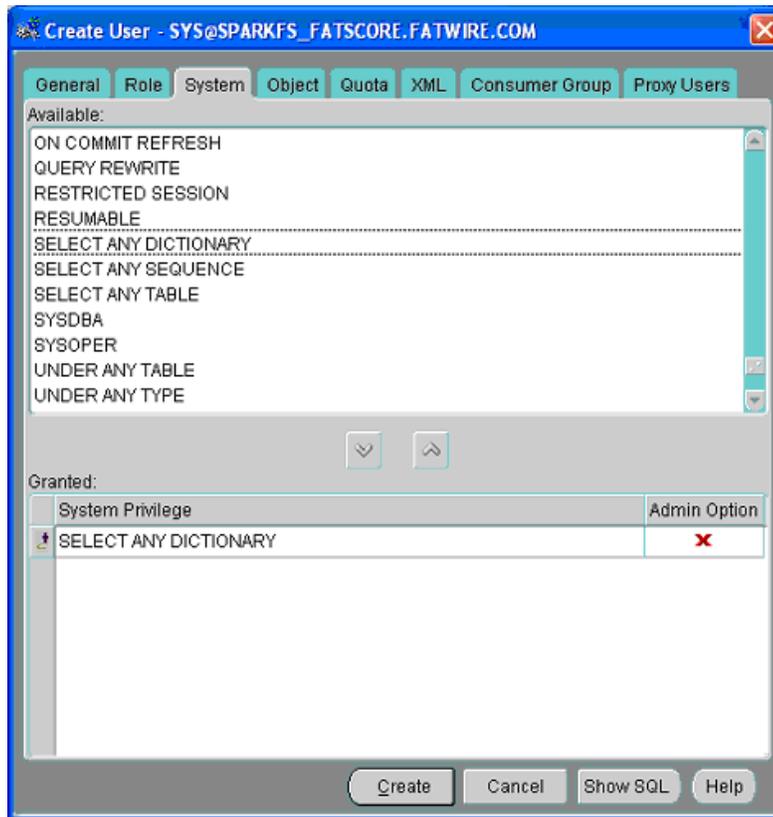
#### 5. On the General tab, enter a username and password.



6. On the **Role** tab, select **Connect** and **Resource**.



7. On the **System** tab, choose **Select Any Dictionary**. Click **Create**.



Database configuration is complete.

## Next Step

You are now ready to create and configure the data source. For instructions, refer to your Content Server installation guide.



## Chapter 2

# Creating and Configuring an Oracle 10g Database

Use this chapter to set up an Oracle 10g database for your Content Server installation. For background information regarding database configuration and users' permissions, see [Part 1, "Creating and Configuring a Database."](#)

This chapter contains the following sections:

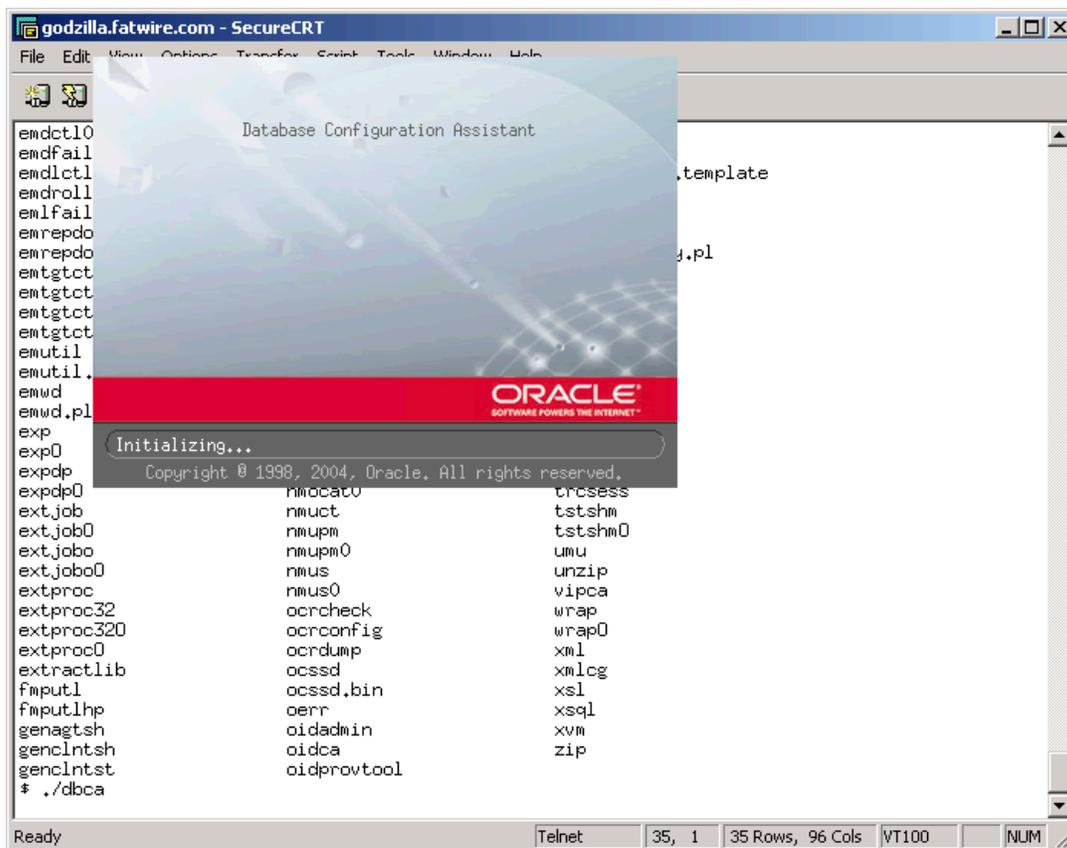
- [Step I. Create an Oracle 10g Database](#)
- [Step II. Create a New User for Content Server](#)

## Step I. Create an Oracle 10g Database

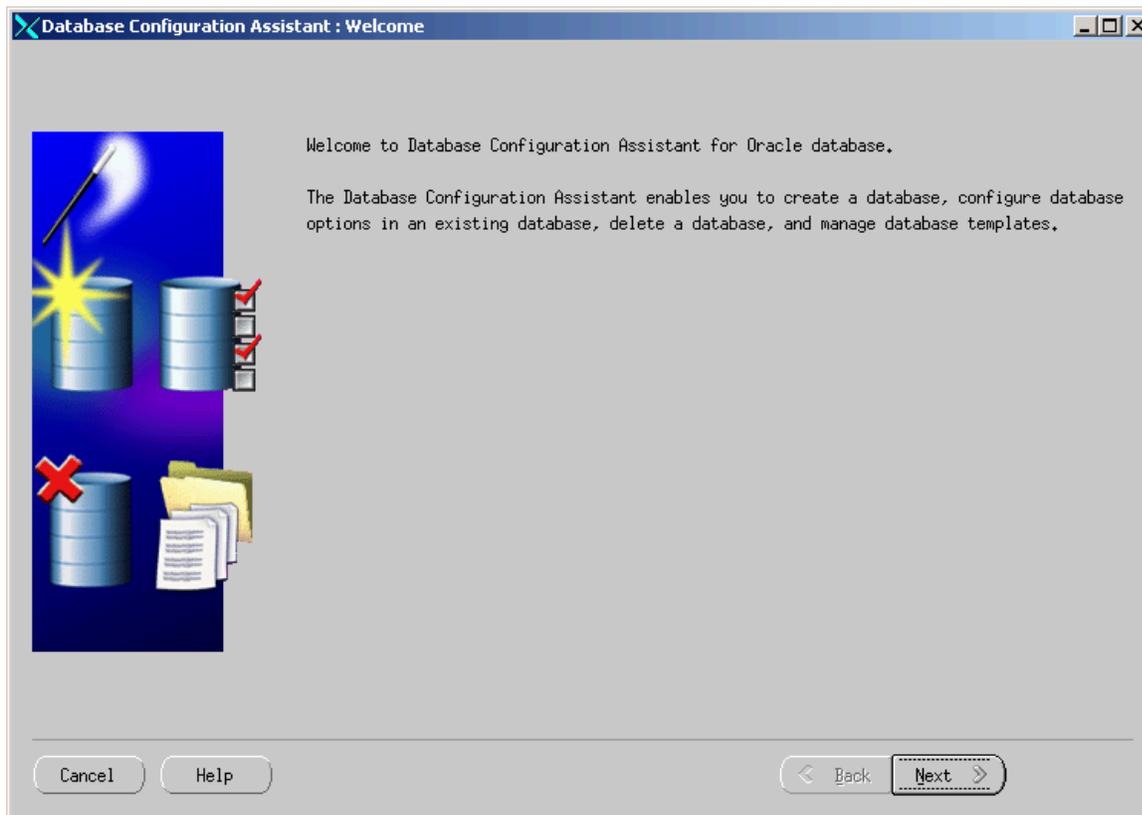
1. Execute the “Oracle Database Configuration Assistant” by doing one of the following:
  - In Unix, execute the command: `dbca`
  - In Windows, go to the “Oracle Programs” group and select **Database Configuration Assistant**.

### Note

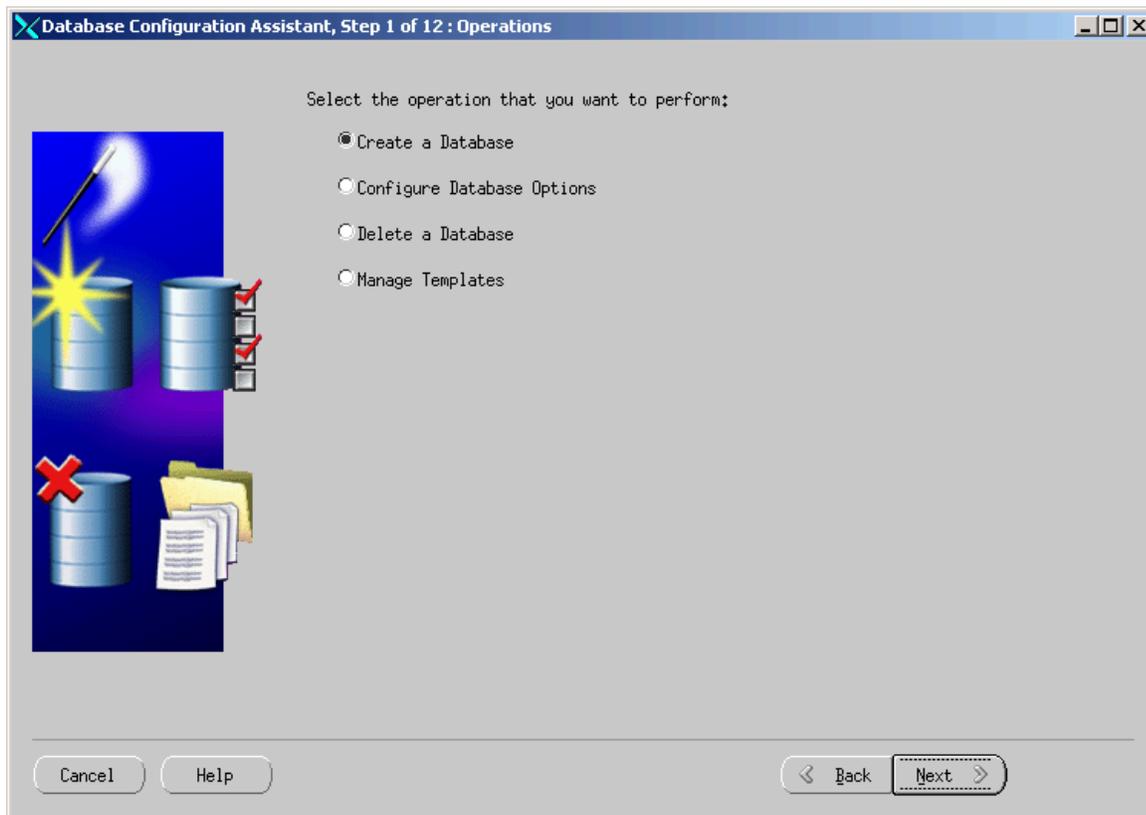
This step displays a load screen that can take some time to complete. Be patient.



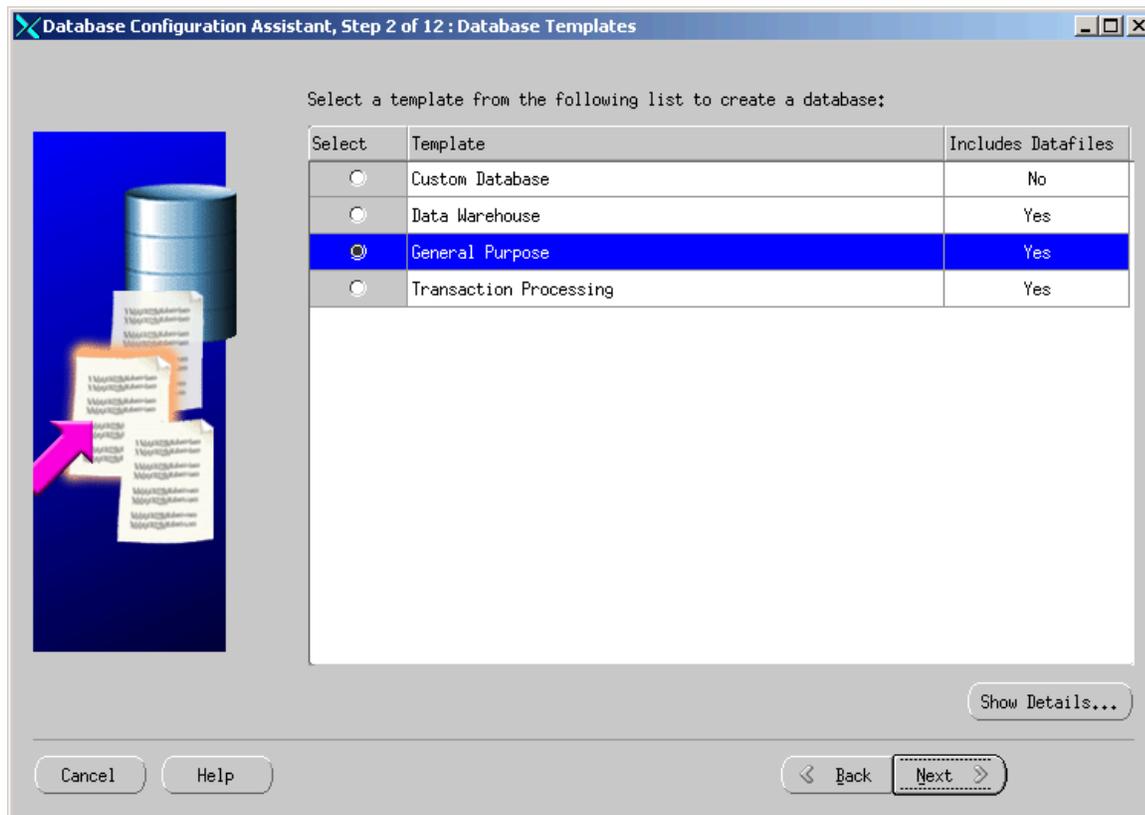
2. On the first screen that is displayed, click **Next**. In the following screen, click **Next**.



3. Select the radio button **Create a Database** and click **Next**.



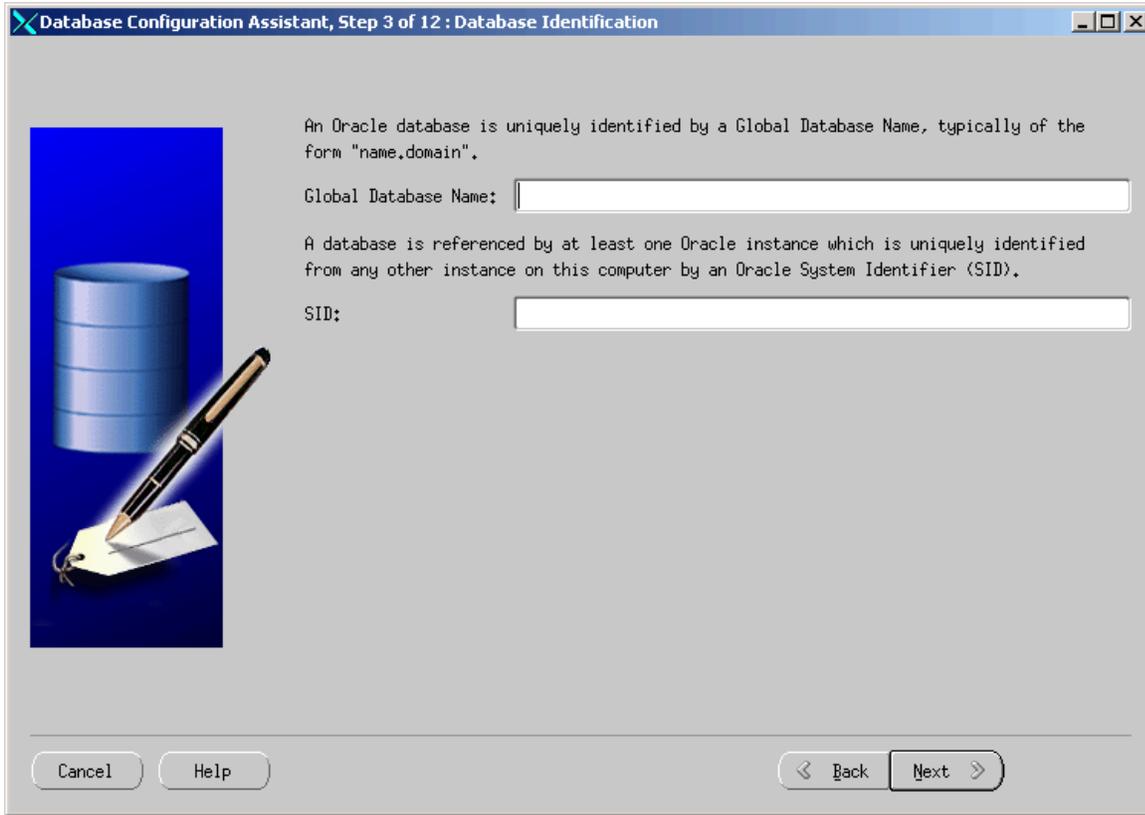
4. Select the radio button **General Purpose** and click **Next**.



**Note**

Database block size **must** be at least 4096 bytes. Selecting the **General Purpose** option automatically sets the block size to 8192 bytes.

5. Enter a unique global database name and SID (in this example the global database name is contentserverdb. The SID is CSDB). Click **Next**.



Database Configuration Assistant, Step 3 of 12 : Database Identification

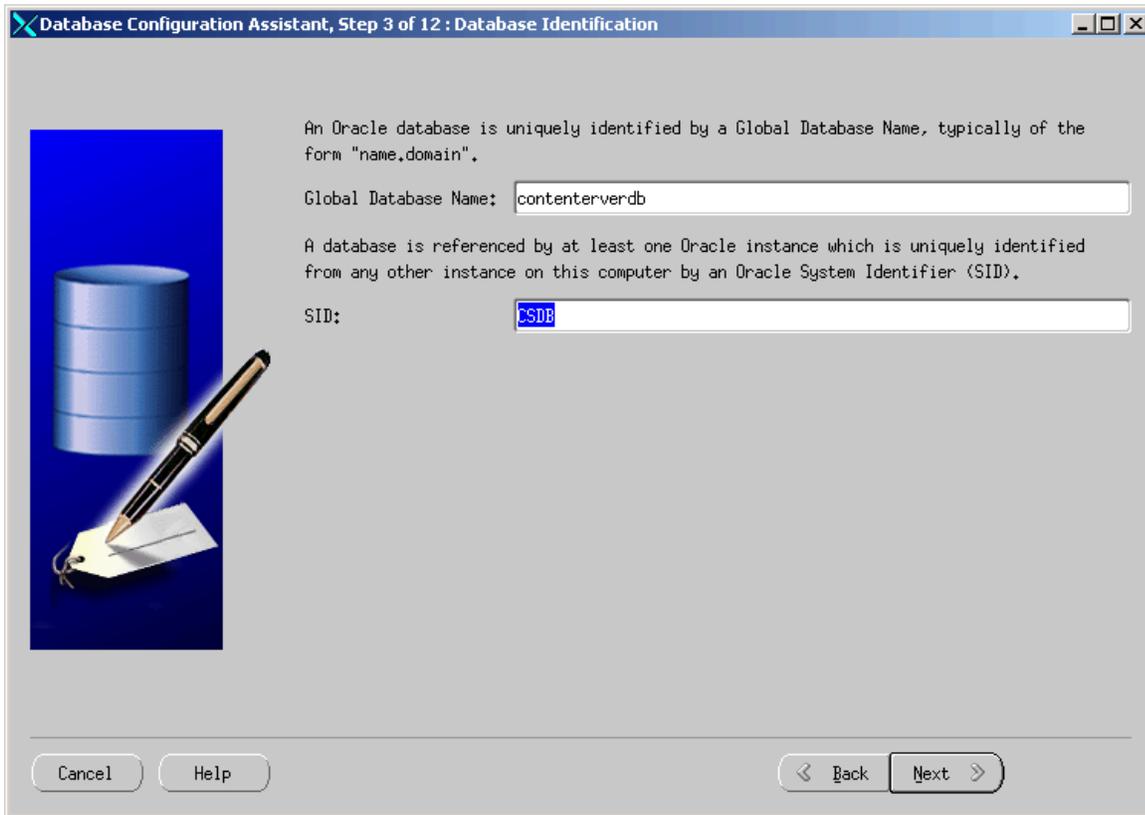
An Oracle database is uniquely identified by a Global Database Name, typically of the form "name.domain".

Global Database Name:

A database is referenced by at least one Oracle instance which is uniquely identified from any other instance on this computer by an Oracle System Identifier (SID).

SID:

Cancel Help < Back Next >

**6. Do not change any options. Click Next.**

Database Configuration Assistant, Step 3 of 12 : Database Identification

An Oracle database is uniquely identified by a Global Database Name, typically of the form "name.domain".

Global Database Name:

A database is referenced by at least one Oracle instance which is uniquely identified from any other instance on this computer by an Oracle System Identifier (SID).

SID:

Cancel Help < Back Next >

7. Do not change any options. Click **Next**.

Database Configuration Assistant, Step 4 of 12 : Management Options

Each Oracle database may be managed centrally using the Oracle Enterprise Manager Grid Control or locally using the Oracle Enterprise Manager Database Control. Choose the management option that you would like to use to manage this database.

Configure the Database with Enterprise Manager

Use Grid Control for Database Management

Select the Management Service: No Agents Found

Use Database Control for Database Management

Enable Email Notifications

Outgoing Mail (SMTP) Server: \_\_\_\_\_

Email Address: \_\_\_\_\_

Enable Daily Backup

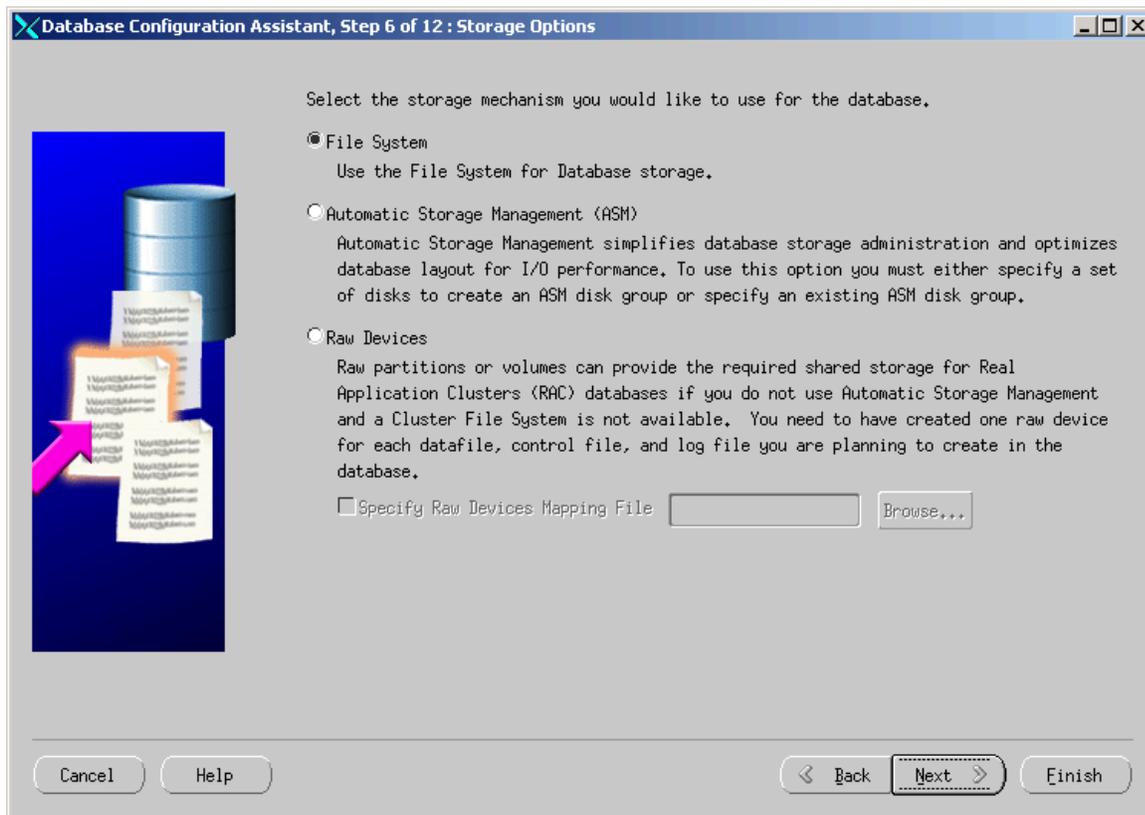
Backup Start Time: 02:00 AM

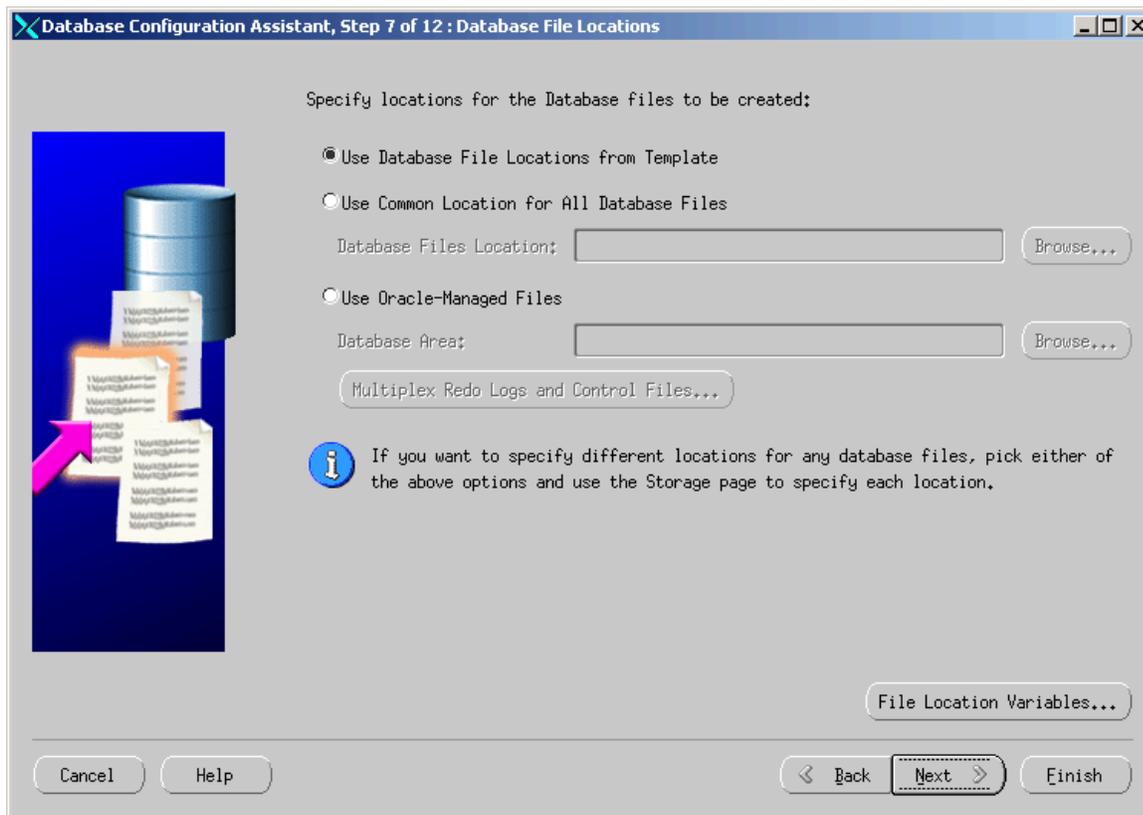
OS Username: \_\_\_\_\_

Password: \_\_\_\_\_

Cancel Help Back Next

8. Enter a password, re-enter the same password in the “Confirm Password” field and click **Next**.
9. For enhanced security select the radio button **Use Different Passwords** and enter a unique password for each of the given users.

**10. Do not change any options. Click Next.**

**11. Do not change any options. Click Next.**

**12. Do not change any options. Click Next.**

Database Configuration Assistant, Step 8 of 12 : Recovery Configuration

Choose the recovery options for the database:

Specify Flash Recovery Area

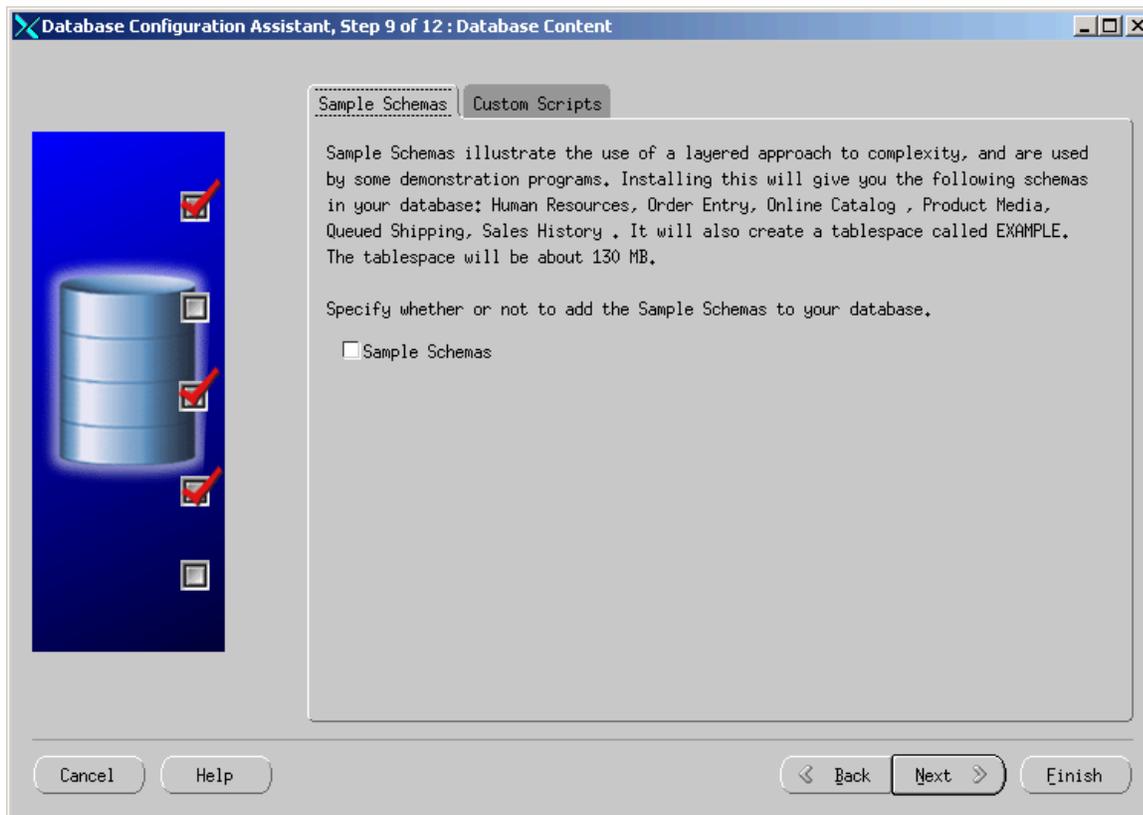
This is used as the default for all backup and recovery operations, and is also required for automatic backup using Enterprise Manager. Oracle recommends that the database files and recovery files be located on physically different disks for data protection and performance.

Flash Recovery Area:  Browse...

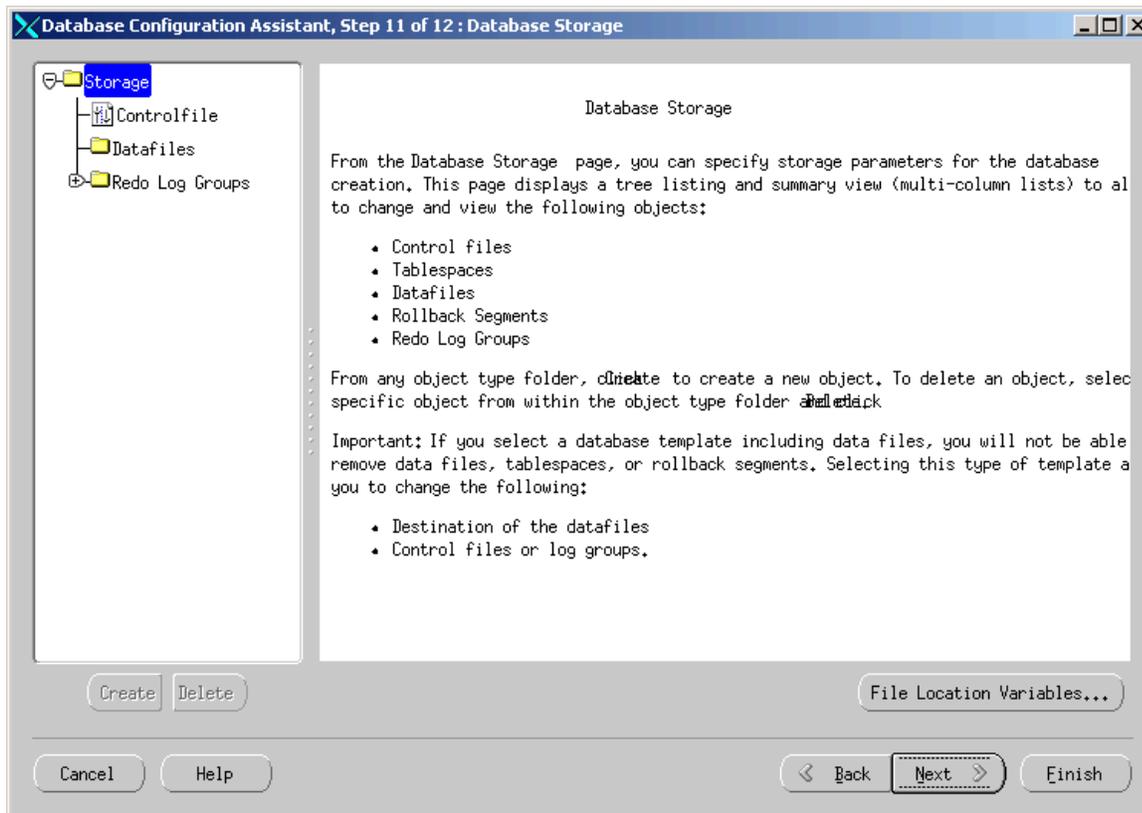
Flash Recovery Area Size:  M Bytes

Enable Archiving

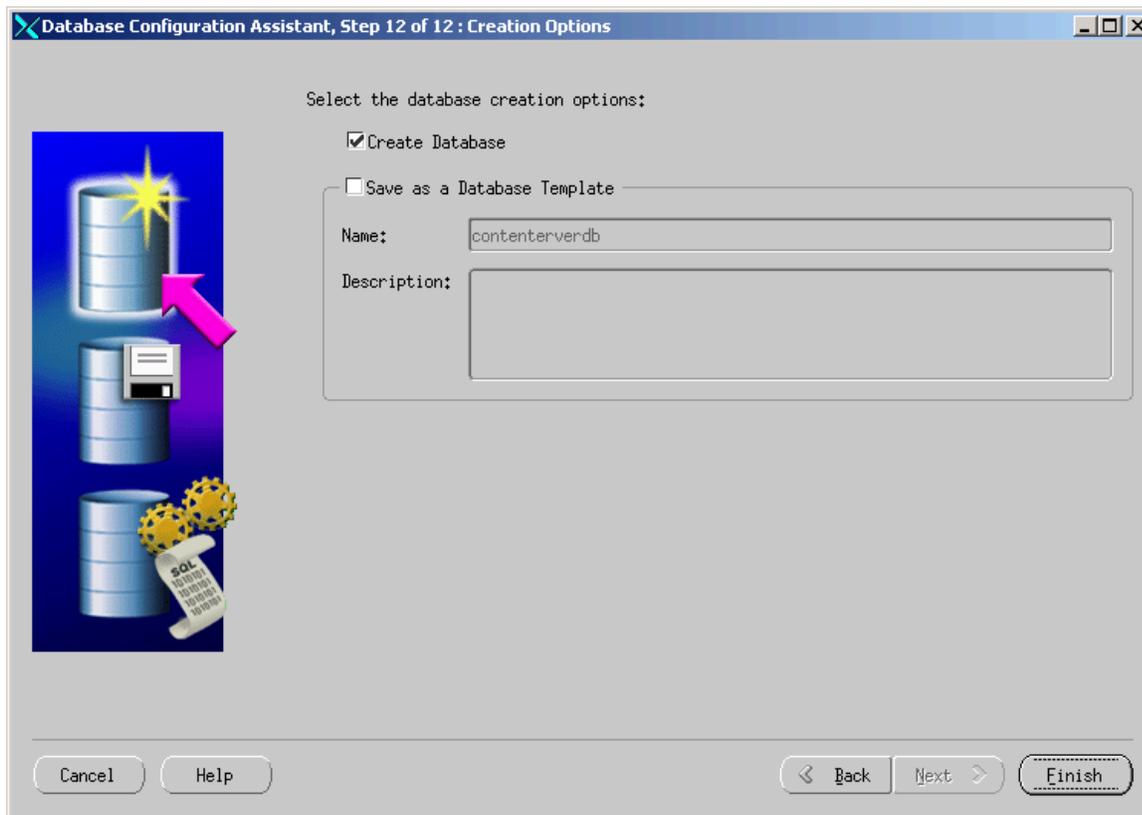
13. Do not change any options. Click **Next**.



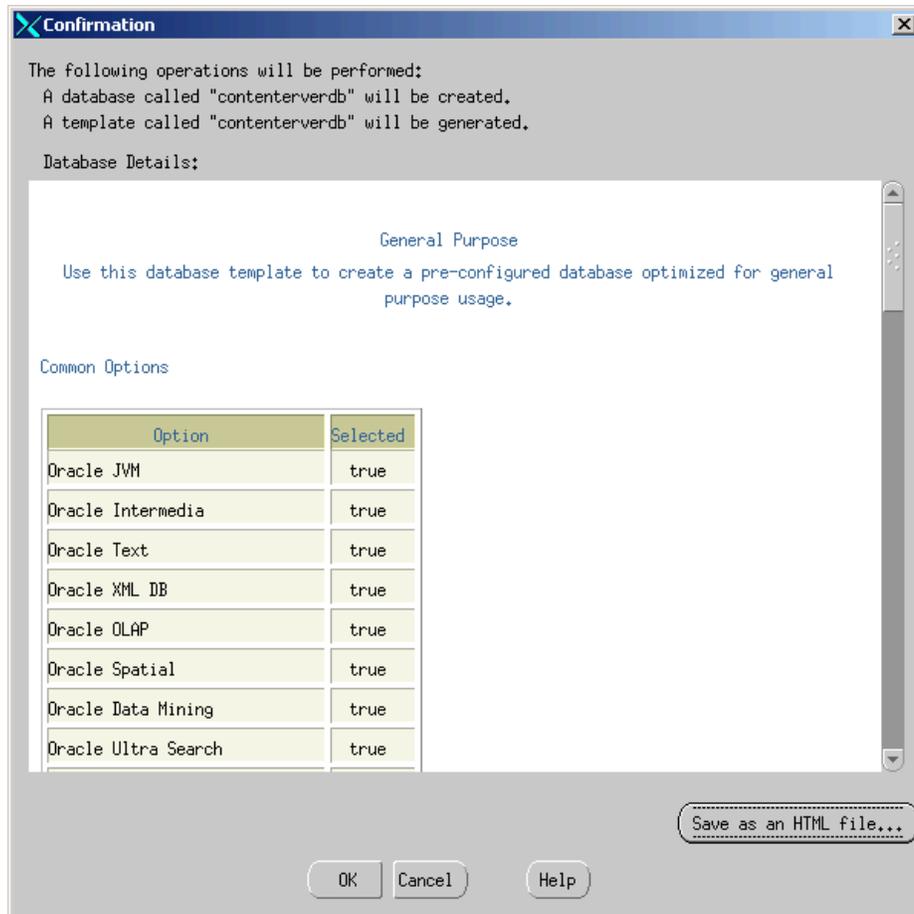
14. Click the **Character Sets** tab and do the following:
  - a. Select **Choose from the list of character sets** and select **UTF-8** from the drop-down menu.
  - b. Click the **National Character Set** drop down-menu and select **UTF8**.
15. Leave all other options on the different tabs as is and click **Next**.
16. For database storage, no options need to be changed. However, if you wish to change the location of the database from the default of `oradata` located under the Oracle installation, you can do so on this page. Click **Next**.



17. Do not change any options. Click **Finish**.



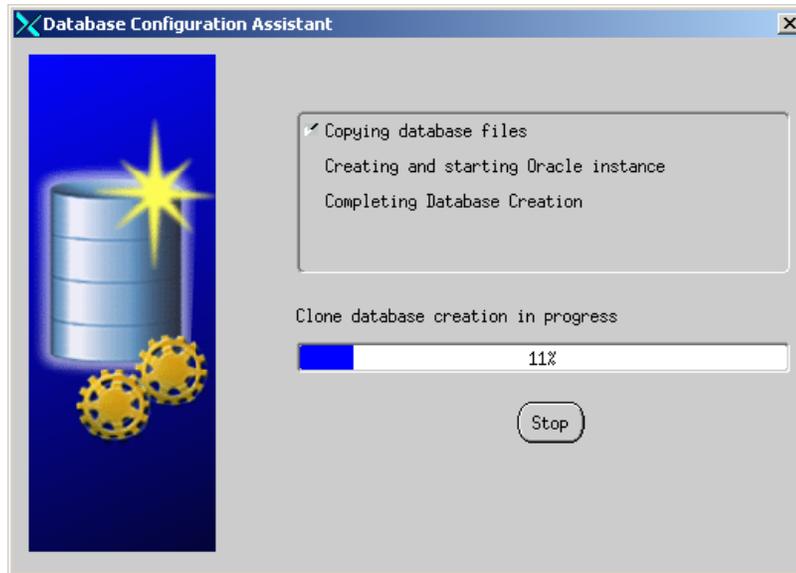
18. In the “Configuration” window, review the choices that you made on the previous screens. If you need to modify your choices, click **Cancel** and make the modifications. Otherwise, click **OK** to continue.



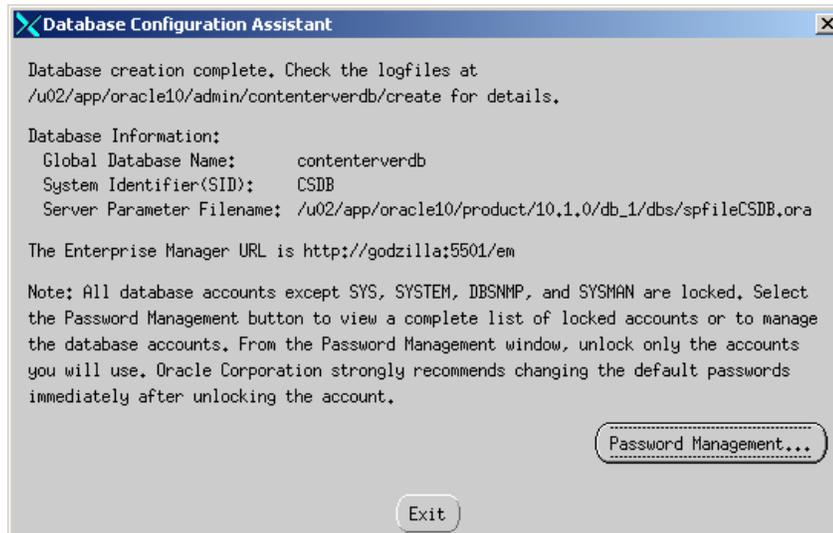
### Note

If you are planning to use internationalization, for Content Server the key value is: National Character Set: UTF8

19. The following window shows the progress of the database creation. This step can take time to complete.



20. When database creation is completed, click **Exit**.



## Step II. Create a New User for Content Server

1. Locate the file `emoms.properties` (in `<oracle home>/<server name>_<SID>/sysman/config/`).
  - a. Find the line: `oracle.sysman.emSDK.svlt.ConsoleServerPort`
  - b. The port after the line in [step a](#) is important. Make a note of it.
2. Run the command: `emctl status dbconsole`

The command should return an output similar to the following:

```
Oracle Enterprise Manager 10g Database Control Release
10.1.0.2.0
Copyright (c) 1996, 2004 Oracle Corporation. All rights
reserved.
```

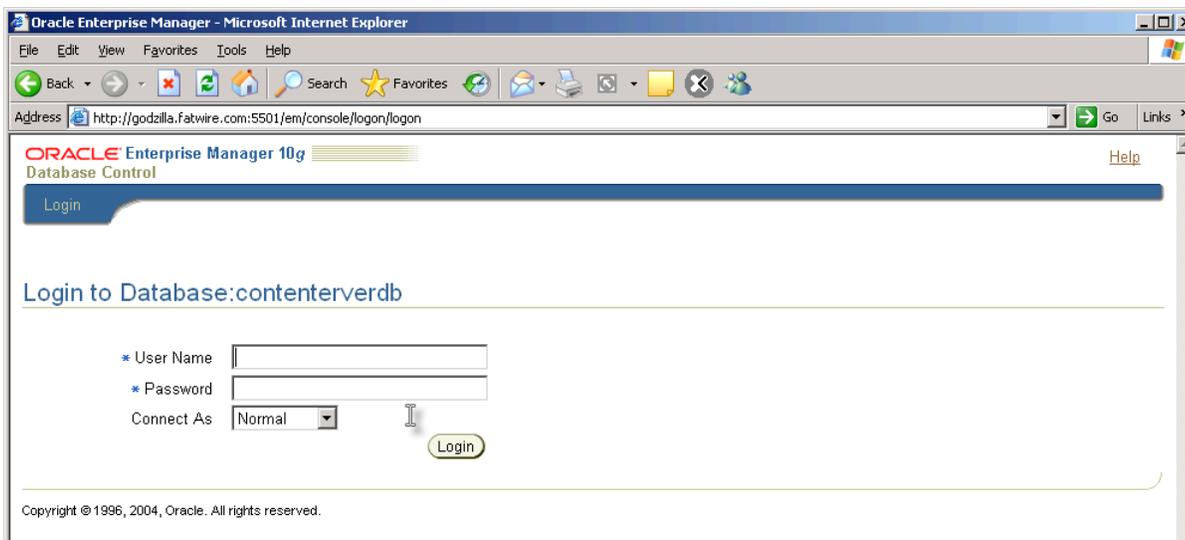
```
http://godzilla:5500/em/console/aboutApplication
Oracle Enterprise Manager 10g is running.
```

-----  
Logs are generated in directory `/u02/app/oracle10/product/10.1.0/db_1/godzilla_orcl10so/sysman/log`

### Note

If the command returns the message that the Oracle Enterprise Manager is not running, start Oracle Enterprise Manager with the command: `emctl start dbconsole`

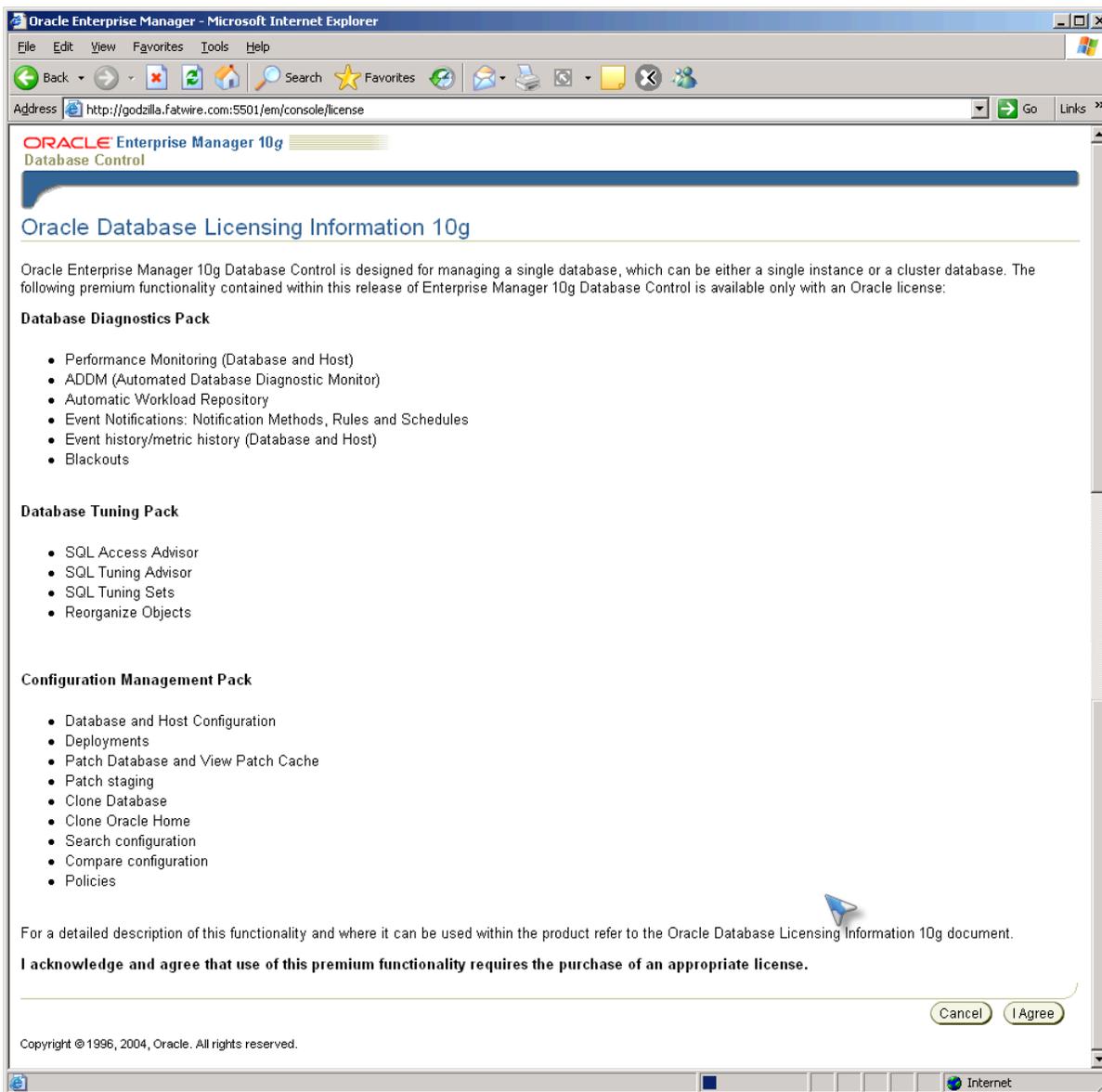
3. Open a browser and do the following:
  - a. Browse to the URL `http://<hostname>:<port>/em` (from [step 2](#)).



b. Log in to the browser, using the following field values:

| Field Name | Field Value                             |
|------------|---|
| User name  | sys                                     |
| Password   | <password entered when creating the db> |
| Connect As | SYSDBA                                  |

c. As this is the first time you are using the Oracle Enterprise Manager, a license page is displayed. Click **I Agree**.



**4. Click the Administration tab.**

The screenshot shows the Oracle Enterprise Manager 10g Database Control interface for the database 'contentverddb'. The browser window title is 'Oracle Enterprise Manager (SYS) - Database: contentverddb - Microsoft Internet Explorer'. The address bar shows the URL: [http://godzilla.fatwire.com:5501/em/console/database/instance/sitemap?event=doLoad&target=contentverddb&type=oracle\\_database](http://godzilla.fatwire.com:5501/em/console/database/instance/sitemap?event=doLoad&target=contentverddb&type=oracle_database). The page is logged in as SYS. The navigation tabs are Home, Performance, Administration, and Maintenance. The 'Administration' tab is selected. The page was refreshed on May 26, 2005 at 10:28:11 AM. The 'View Data' dropdown is set to 'Manually'. The main content area is divided into several sections:

- General:** Status is Up, Up Since May 26, 2005 9:01:04 AM, Time Zone EDT, Availability (%) 100 (Last 24 hours), Instance Name CSDB, Version 10.1.0.2.0, Read Only No, Oracle Home [/u02/app/oracle10/product/10.1.0/db\\_1](#), Listener [LISTENER\\_godzilla](#), Host [godzilla](#). A Shutdown button is present.
- Host CPU:** A line graph showing CPU usage over time. The y-axis ranges from 0 to 100%. The legend includes Other (blue) and CSDB (green).
- Active Sessions:** A pie chart showing session distribution. The y-axis ranges from 0 to 100%. The legend includes CPU (green), I/O (purple), and Wait (yellow). The chart shows 00% CPU, 0.01% I/O, and 0.01% Wait.
- High Availability:** Instance Recovery Time (seconds) 9.
- Space Usage:** Database Size (GB) 1.
- Diagnostic Summary:** Performance No ADDM run.

The bottom status bar shows the URL: [http://godzilla.fatwire.com:5501/em/console/database/instance/sitemap?event=doLoad&target=contentverddb&type=oracle\\_database&p](http://godzilla.fatwire.com:5501/em/console/database/instance/sitemap?event=doLoad&target=contentverddb&type=oracle_database&p) and the Internet icon.

- a. From the **Security** menu, select **Users**. Click the **Create** button.
- b. In the “Create User” screen, fill in required fields with the values that are listed in the following table:

| Field Name       | Field Value     |
|------------------|-----------------|
| Name             | csuser          |
| Enter Password   | <your choice>   |
| Confirm Password | <same password> |

Oracle Enterprise Manager 10g Database Control

Database: contenterverdb > Users > Create User

Logged in As SYS

Create User

General Roles System Privileges Object Privileges Quotas Consumer Groups Proxy Users

\* Name

Profile

Authentication

\* Enter Password

\* Confirm Password

Expire Password now

Default Tablespace

Temporary Tablespace

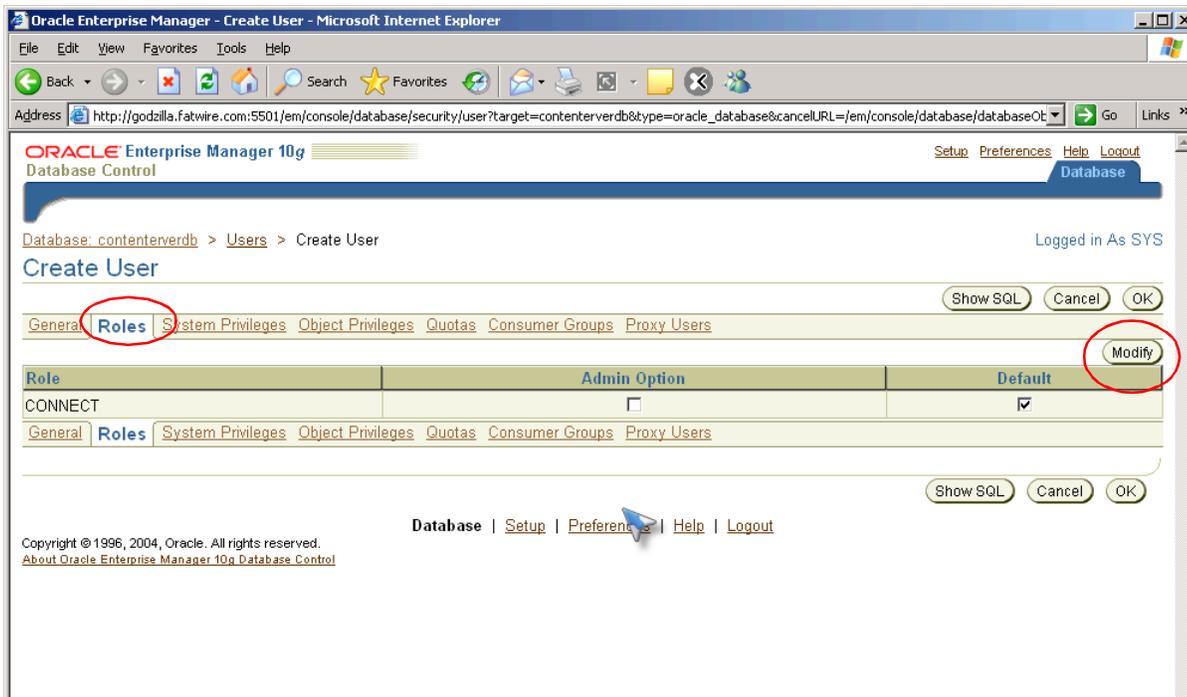
Status  Locked  Unlocked

General Roles System Privileges Object Privileges Quotas Consumer Groups Proxy Users

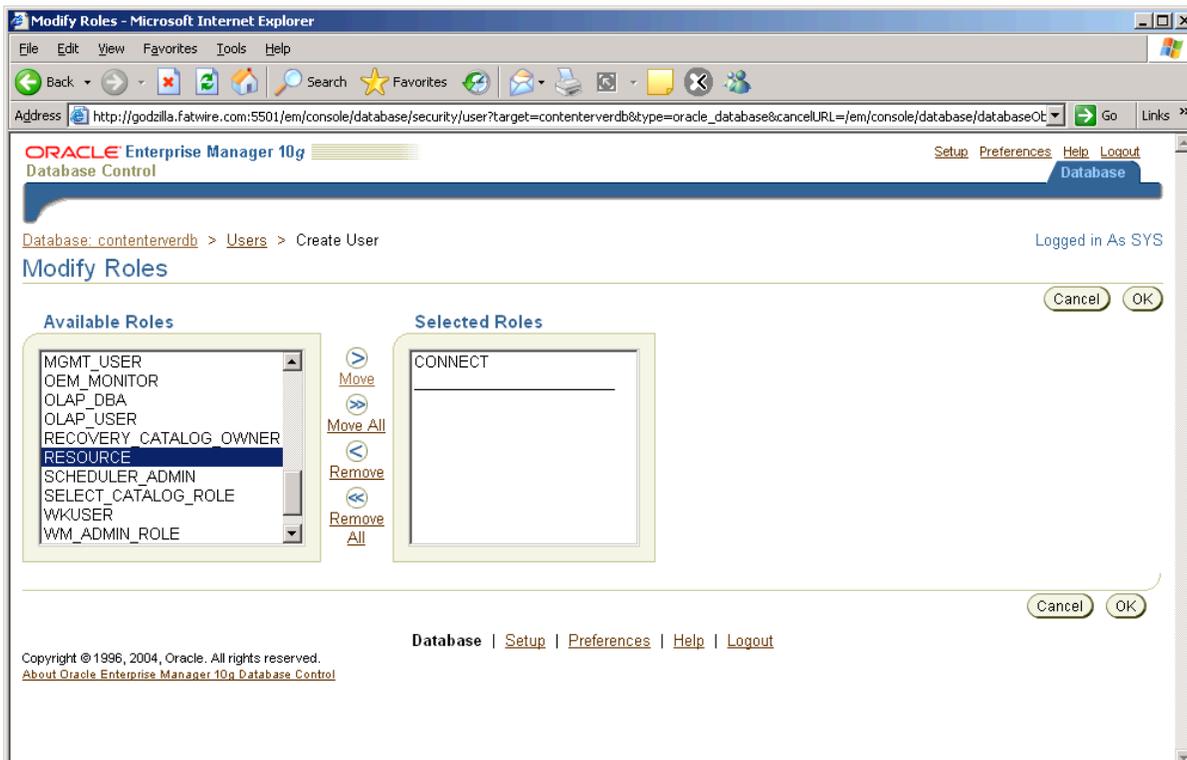
Show SQL Cancel OK

Database | Setup | Preferences | Help | Logout

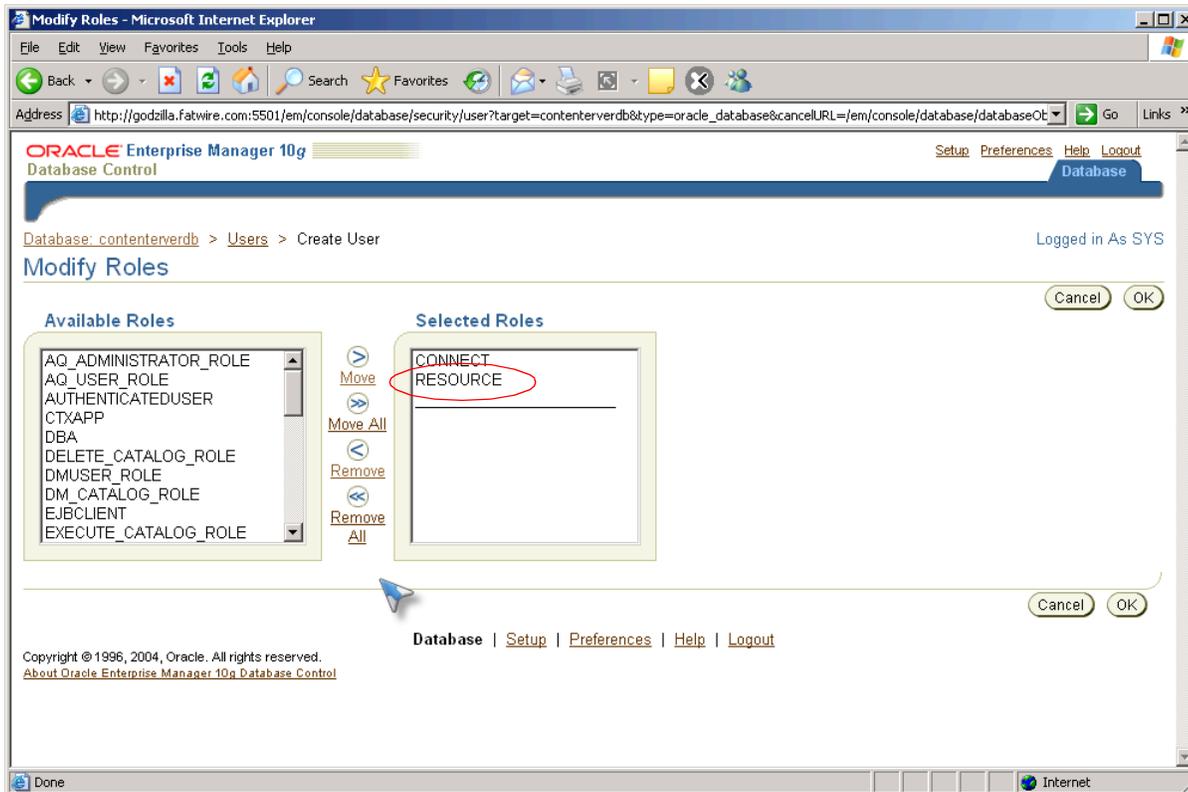
5. Click the **Roles** tab.
  - a. Click the **Modify** button.



- b. From the list of "Available Roles" (left side), select **Resource** and click the **Move** button.

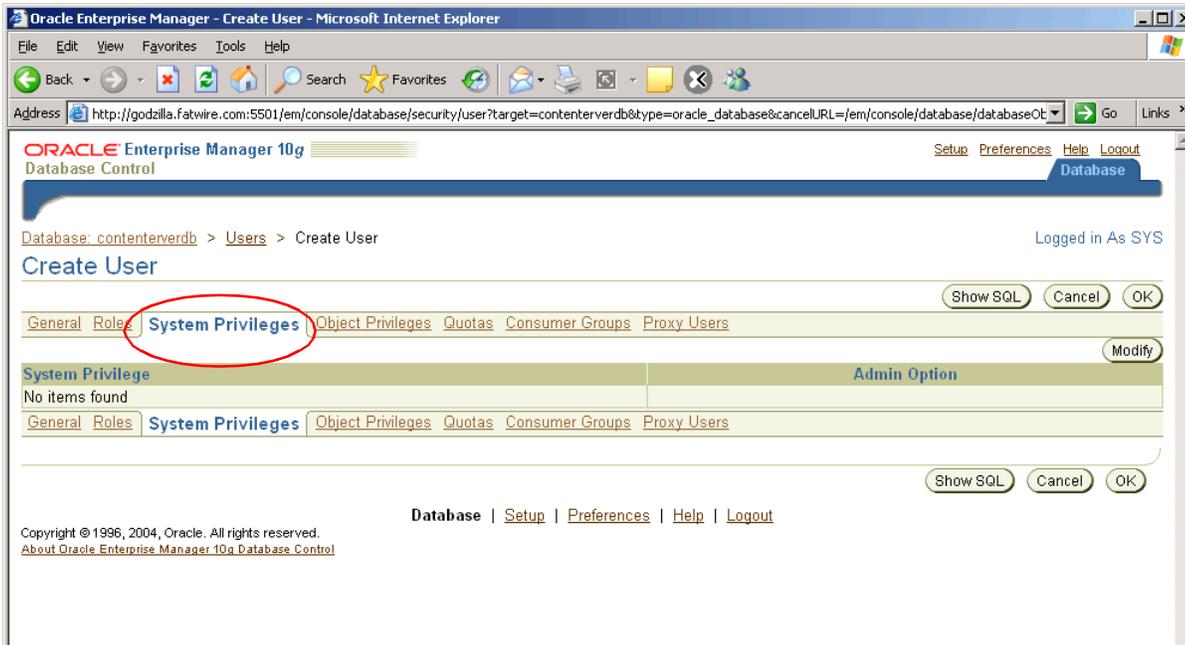


**Resource** is moved to the “Selected Roles” list.

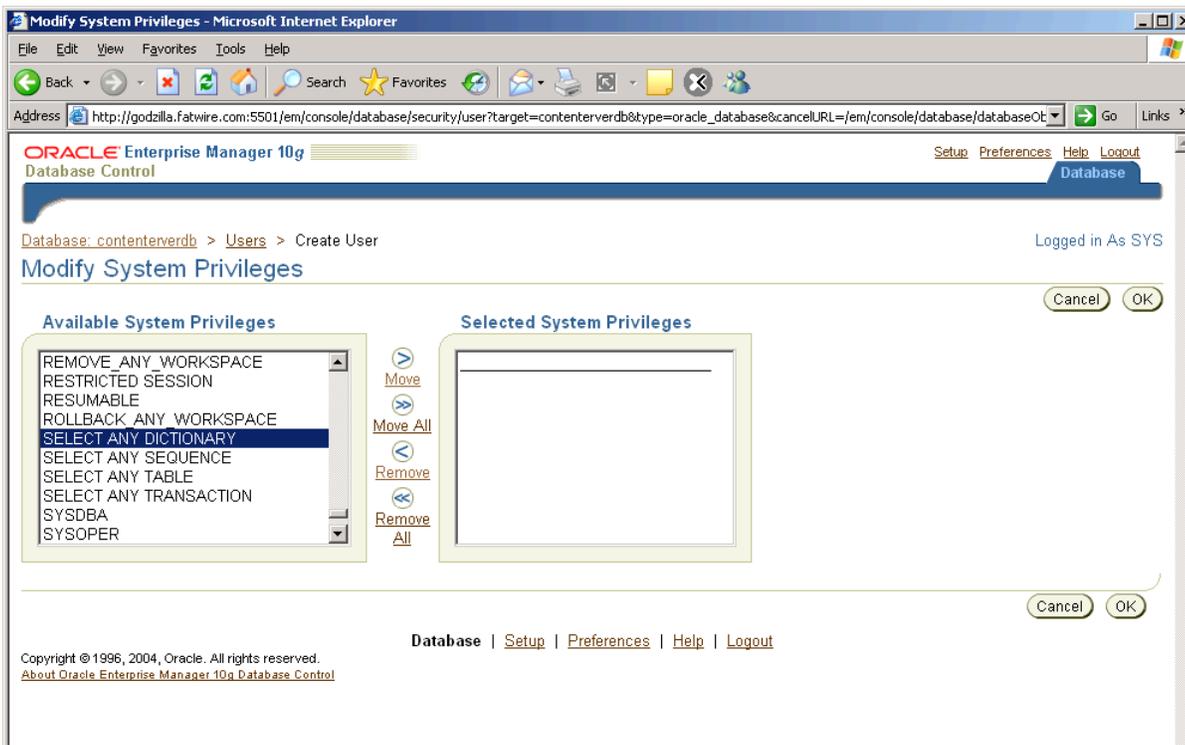


c. Click **OK**.

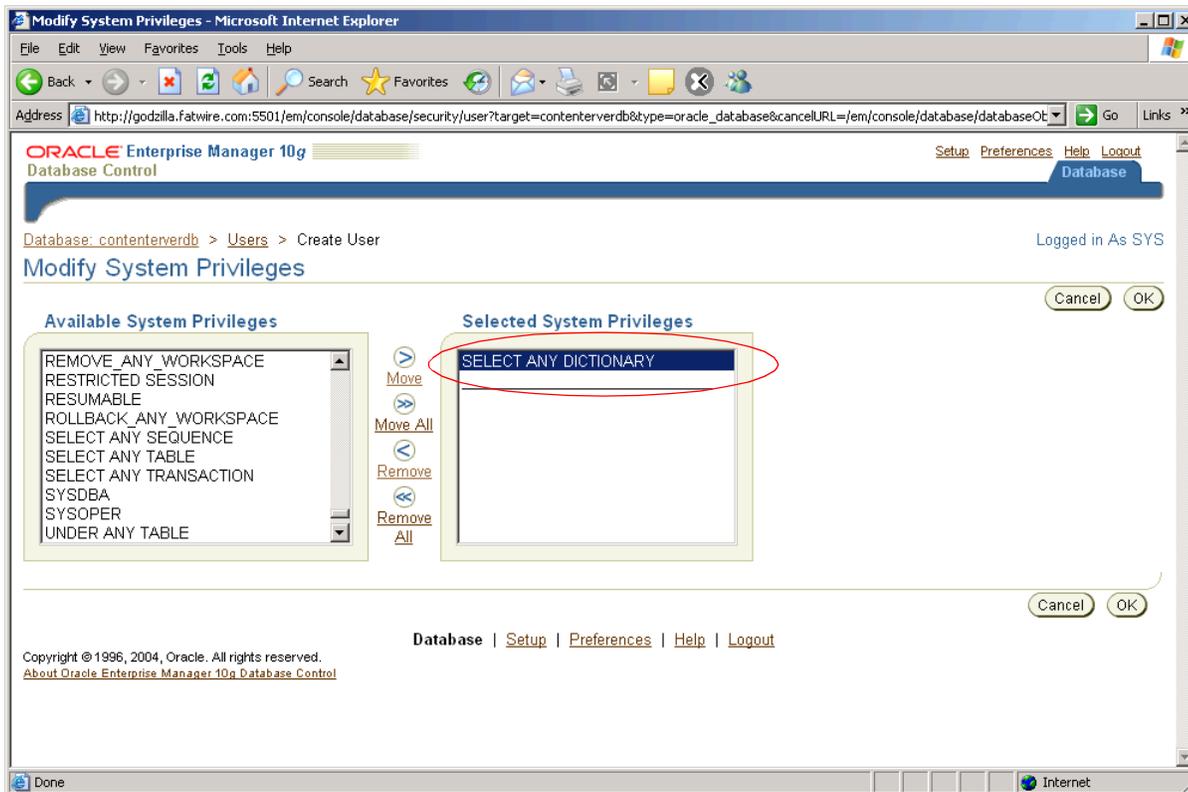
6. Click the **System Privileges** tab.
  - a. Click the **Modify** button.



- b. From the list of "Available System Privileges" (left side), choose **Select Any Dictionary** and click the **Move** button.



Select Any Dictionary is moved to the “Selected System Privileges” list.



- c. (Optional) If you are creating a portal installation on WebLogic, also add the **Create View** privilege (by repeating [step b](#)).
- d. Click **OK**.  
The database is now ready for Content Server.
7. In the upper right-hand corner, click **Logout**.
8. The database is ready for Content Server. You can now create and configure the data source.

## Next Step

You are now ready to create and configure the data source. For instructions, refer to your Content Server installation guide.

## Chapter 3

# Creating and Configuring an MS SQL Server Database

Use this chapter to set up a SQL Server database for your Content Server (Spark) installation. For background information regarding database configuration and users' permissions, see [Part 1, "Creating and Configuring a Database."](#)

This chapter contains the following sections:

- [Creating a Database on MS SQL Server 2000 SP3+](#)
- [Creating a Database on MS SQL Server 2005](#)

## Creating a Database on MS SQL Server 2000 SP3+

To create and configure a database on MS SQL Server 2000 SP3+

1. Create the database login:
  - a. Open “Enterprise Manager.”
  - b. In the left-hand tree, select **Microsoft SQL Servers > SQL Server Group > (Local) > Security**.
  - c. Right-click on **Logins** and select **New Login...**
    - 1) Create a user (such as `csuser`), and select the proper authentication method.
    - 2) Save this user.
2. Create the database:
  - a. In the left-hand tree, select **Microsoft SQL Servers > SQL Server Group > (Local) > Databases**.
  - b. Right-click on **Databases** and select **New Database...**
    - 1) Enter a name (such as `csDB`), then modify the other fields as needed for your installation.
    - 2) Finish creating this database.
3. Assign account privileges:
  - a. Select the newly created database in the left-hand tree and click **Open**.
  - b. Right-click on **Users** and select **Add new Database User...**
  - c. In the drop-down list, choose the user created in [step c](#) of this procedure. In the **Permit role membership** list, check the box next to **db\_owner**.
  - d. Save the new user.

Database configuration is complete. You are now ready to create and configure the data source. For instructions, refer to your Content Server (Spark) installation guide.

## Creating a Database on MS SQL Server 2005

To create and configure a database on MS SQL Server 2005

1. Use the Windows Account Manager to create a new user account for the CS database user (for example, `csuser`), and assign a password to the account.
1. Open SQL Server Manager Studio.
2. Log in to MS SQL Server:
  - a. Enter your user name and password (the default user name is `sa`).
  - b. Click **Connect**.
3. Create the database:
  - a. In the left-hand tree, expand the **Databases** node.
  - b. Right-click the **Databases** node and select **New Database** from the pop-up menu.
  - c. In the “New Database” window, enter a name for your database and click **OK**.  
Your newly created database appears under the **Databases** node in the tree.

4. In the tree, expand the node representing your newly created database, then expand the **Security** node underneath it.
5. Click the **Users** tab.
6. Right-click within the white space underneath the list of existing users and select **New User** from the pop-up menu.
7. In the “Database User - New” window, enter the user name of the CS database user (which you created in [step 1](#) of this procedure) into the **User name** and **Login name** fields.
8. In the “Owned Schemas” and “Role Members” areas, select the **db\_owner** check box.
9. Click **OK**.

Database configuration is complete. You are now ready to create and configure the data source using the user name and password of the CS database user you created in [step 1](#) of this procedure. For instructions, refer to your Content Server (Spark) installation guide.



## Chapter 4

# Creating and Configuring an IBM DB2 8.x Database

Use this chapter to set up a supported IBM DB2 database for your Content Server installation. For background information regarding database configuration and users' permissions, see [Part 1, "Creating and Configuring a Database."](#)

This chapter contains the following sections:

- [Creating and Configuring DB2 8.x for Content Server](#)

## Creating and Configuring DB2 8.x for Content Server

1. Open DB Control Center (**db2cc**).
2. Browse to the instance under which you want to create the new database.  
If you do not have an existing instance in the left-hand tree, do the following:
  - a. Right-click **Instances** and click **Add...**
  - b. Fill in the form provided (or click **Discover**) then click **OK**.
3. Right-click **Branch Databases > Create > Database Using Wizard...**
4. In the “Create Database Wizard,” fill in the following screens as indicated:
  - a. “Database name”  
Enter a unique database name (such as CSDB2), then click **Next**.
  - b. “Specify how and where to store the user tables.”  
Leave the default option **Low maintenance** selected and click **Next**.
  - c. “Specify how and where to store the system catalog tables.”  
Leave the default option **Low maintenance** selected and click **Next**.
  - d. “Specify how and where to store system temporary tables.”  
Leave the default option **Low maintenance** selected and click **Next**.
  - e. “Tune the performance of this database.” Click **Next**.
  - f. “Specify the locale for this database.”  
Complete the following steps:
    - 1) In the **Code Set** drop-down list, select **UTF-8**.
    - 2) Under **Collating Sequence**, leave the default option selected.
    - 3) Click **Next**.
  - g. Review the actions that will take place when you click **Finish**, then click **Finish**.
5. A DB2 message box appears, giving you the option to run the “Configuration Advisor.” Click **No**.  
A new database (with the name you provided in [step 4](#)) is now available in the left-hand tree.
6. In the left-hand tree, right-click **Buffer Pools > Create**.
7. In the “Create Buffer Pool” dialog box, do the following:
  - a. In the “Buffer Pool name” field, add a unique name (such as CSBUFFER32).
  - b. In the **Page size** drop-down list, select **32**.
  - c. Click **OK**.
8. In the left-hand tree, right-click **Table Spaces > Create**.
9. In the “Create Table Space Wizard,” fill in the following screens as explained below:
  - a. “Specify a name for your table space.”  
Enter a unique name (such as csTableSpace) in the “Table Space name” field.  
Then click **Next**.

- b. “Specify the type of table space you want to create.”  
Leave the default value and click **Next**.
  - c. “Specify a buffer pool for your new table space.”  
Select the buffer pool created in [step 7](#) of this procedure and click **Next**.
  - d. “Select the space management system that you want to use.”  
Leave the default option **System-managed space (low maintenance)** selected and click **Next**.
  - e. “Define containers for this table space.”  
Click **Add**, then complete the following steps:
    - 1) In the “Define Container” dialog box, enter a unique name for this container (such as CScontainer).
    - 2) Under “Current Directory,” select a location for this table space (note that you must select a physical location on a mounted disk where you want to place this table space; if you do not have an acceptable location at this point you should create one). Once you have selected a location, click **OK**.
    - 3) Click **Next** in the “Define Container” dialog box.
  - f. “Specify the extent and prefetch sizes for this table space.”  
Leave the default options selected and click **Next**.
  - g. “Select hard drive specifications.”  
Select the appropriate option for your physical media type from the list and click **Next**.
  - h. “Specify the dropped table recovery option for your new table space.” Click **Next**.
  - i. Review the actions that will take place when you click **Finish**, then click **Finish**.
10. Repeat [step 9](#) of this procedure to create a temporary table space, making the following adjustments to the procedure:
- a. When completing [step 9a](#), indicate in the name that this is a temporary table space.
  - b. When completing [step 9b](#), select **System Temporary** for the type of table space.
11. In the left-hand tree, select **User and GroupObjects** and right-click **DB Users > Add**.
- a. In the “Database” tab, do the following:
    - 1) Select a user from the **User** drop-down list.

**Note**

The drop-down list contains all valid system users. If there are no valid system users, you must create one before continuing.

- 2) Under “Grant authorities for the Selected User,” select all the options.

**Note**

This is not recommended for a delivery system. Choose the options that are appropriate for your delivery system)

- b. Click the **Table Space** tab and do the following:
  - 1) Click **Add Tablespace**. In the “Add Tablespace” dialog box, select the tablespace created in [step 9](#) of this procedure and click **OK**.
  - 2) In the “Table Space” tab, the new table space is now selected, but has a  $\emptyset$  symbol next to it. Select **Grant** from the **Privileges** drop-down list (located near the bottom of the tab).
- c. Repeat [step b](#) for the temporary table space created in [step 10](#).
- d. Optionally, repeat [step b](#) to add the default table space USERSPACE1.

#### Note

The default table space was created with the database. Therefore its location is not under your control.

- e. Click **OK**.
12. In the left-hand tree, right-click the database created in [step 4](#) of this procedure and click **Configure Parameters**. In the list that opens, make the following changes:
    - a. Change LOCKLIST/100 to LOCKLIST/1024
    - b. Change LOCKTIMEOUT/None to LOCKTIMEOUT/30
    - c. Change APPLHEAPSZ/256 to APPLHEAPSZ/1024
  13. Database configuration is complete. You are now ready to create and configure the data source. For instructions, refer to your Content Server installation guide.

## Chapter 5

# Creating and Configuring an IBM DB2 9.1 Database

Use this chapter to set up a supported IBM DB2 database for your Content Server installation. For background information regarding database configuration and users' permissions, see [Part 1, "Creating and Configuring a Database."](#)

This chapter contains the following sections:

- [Installing and Configuring DB2 9.1 for Content Server](#)

# Installing and Configuring DB2 9.1 for Content Server

To install and configure a DB2 9.1 database, you will complete the following steps:

- A. [Install DB2](#)
- B. [Create a New DB2 Database](#)
- C. [Create a User for the New Database](#)
- D. [Configure the Database](#)

## A. Install DB2

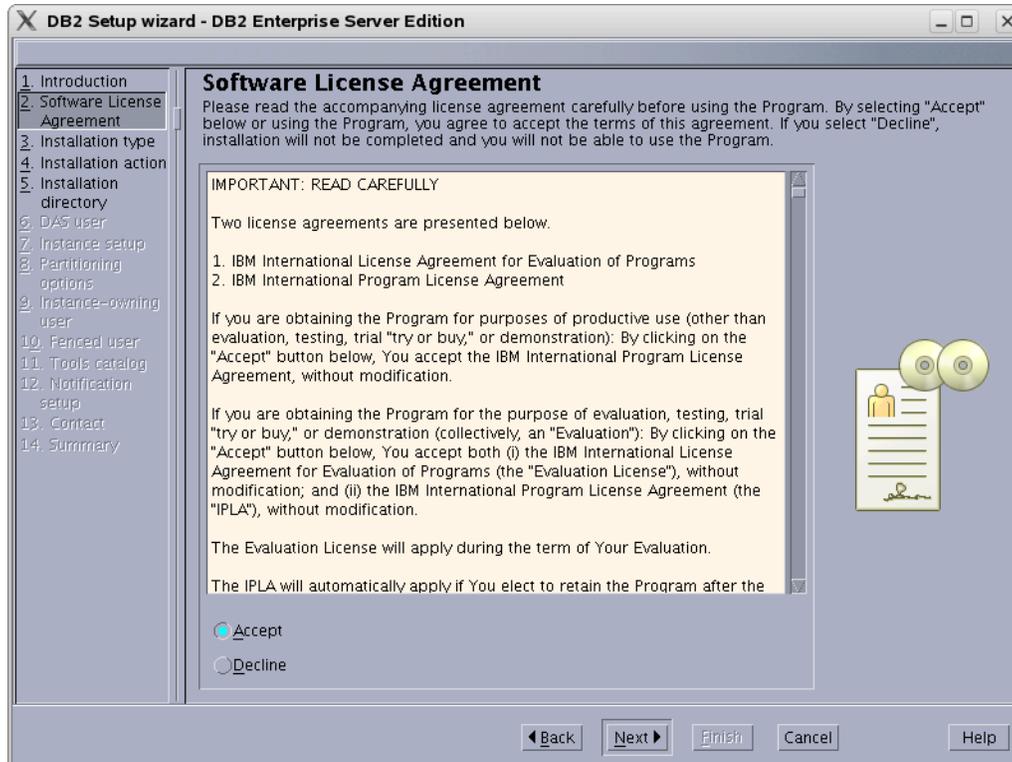
1. Uncompress the correct installation file for your distribution.
2. Run `./db2setup`
3. In the “Information Management Software” screen, select **Install a Product**.



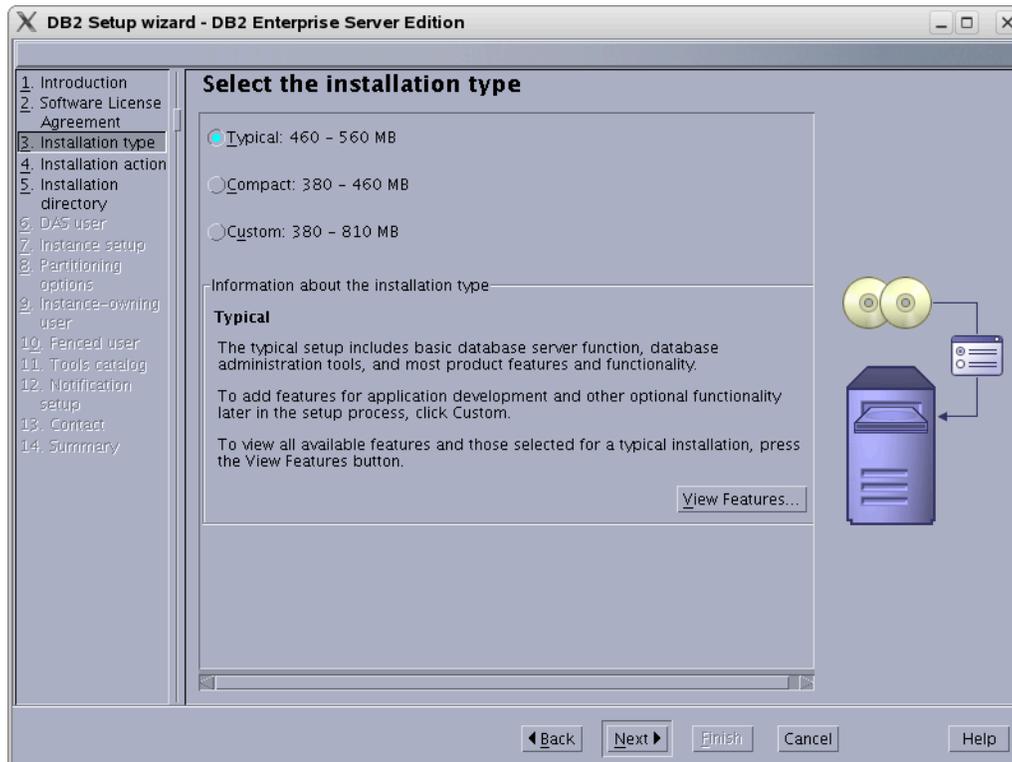
4. Under “DB2 Enterprise Server Edition,” select **Install New**.



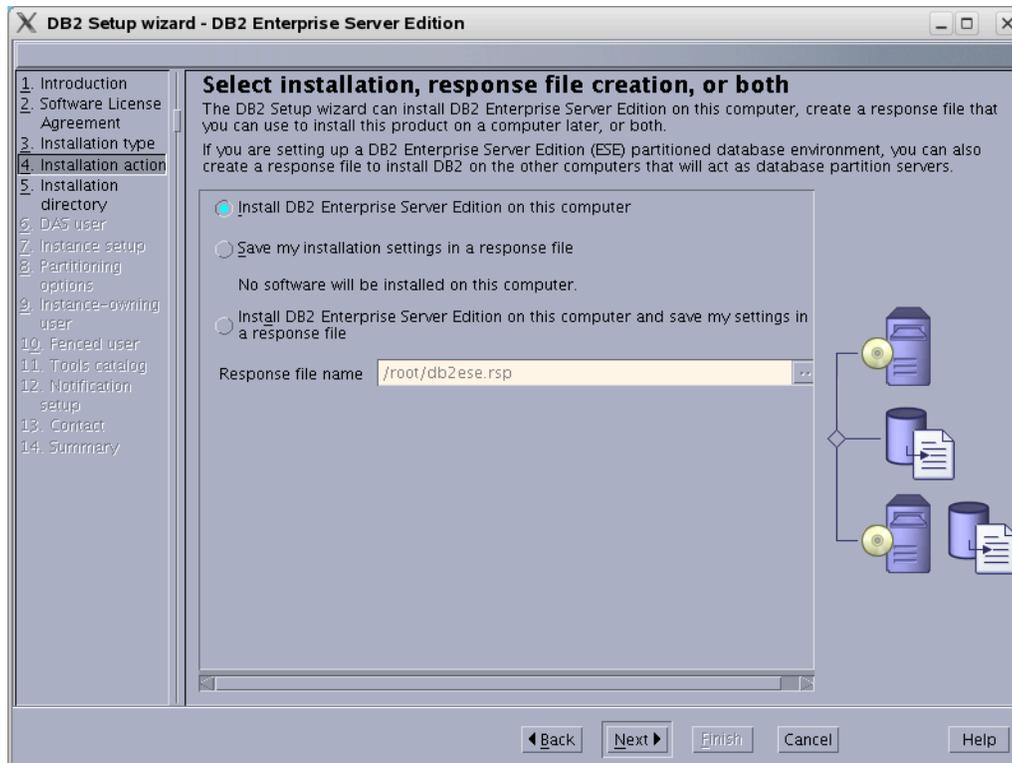
5. In the “Welcome to the DB2 Setup Wizard,” click **Next**.
6. In the “Software License Agreement” screen, click **Accept**, then click **Next**.



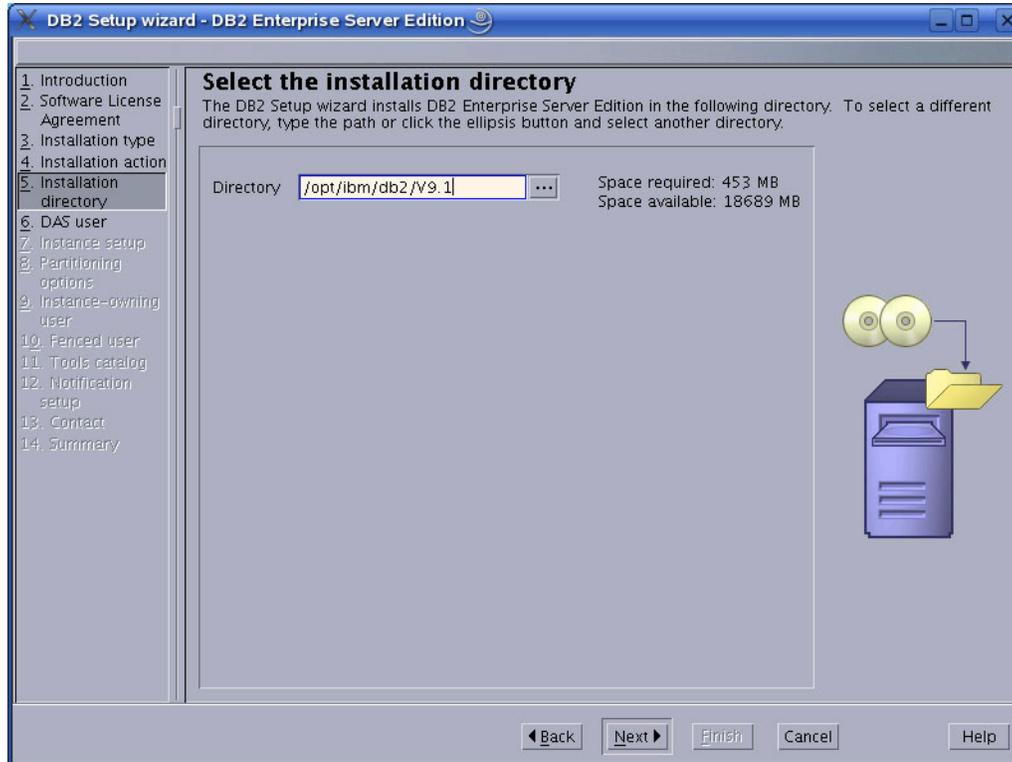
7. In “Select the Installation Type,” select **Typical** and click **Next**.



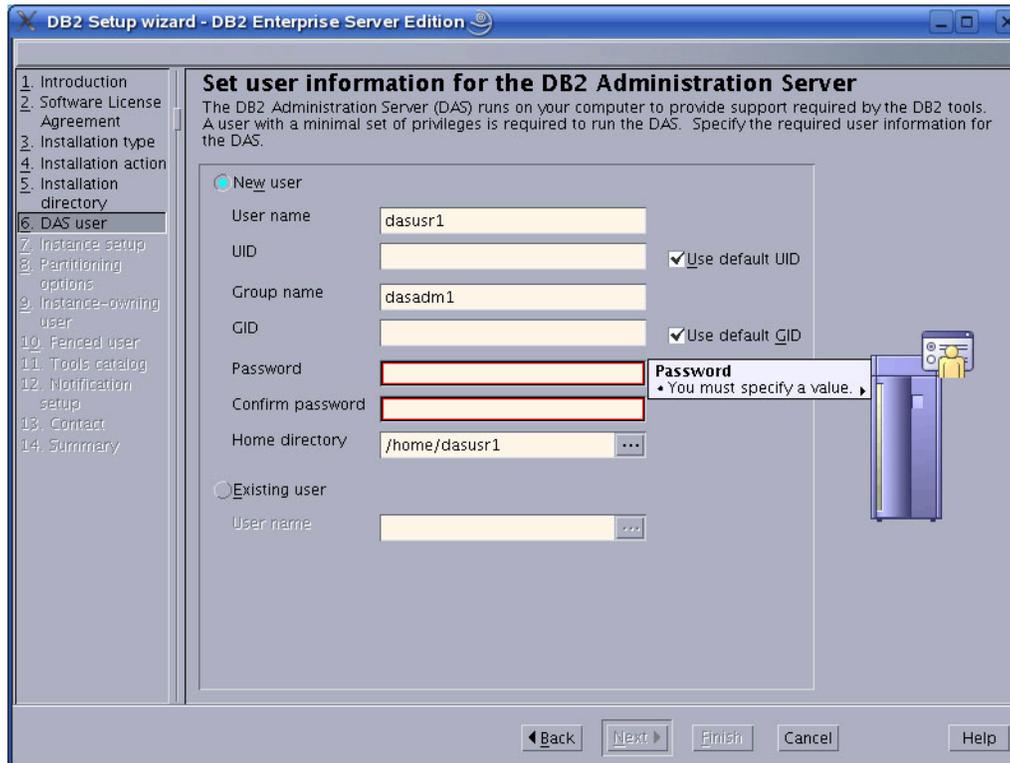
8. In “Select installation, response file creation, or both,” select **Install DB2 Enterprise Server Edition on this Computer** and click **Next**.



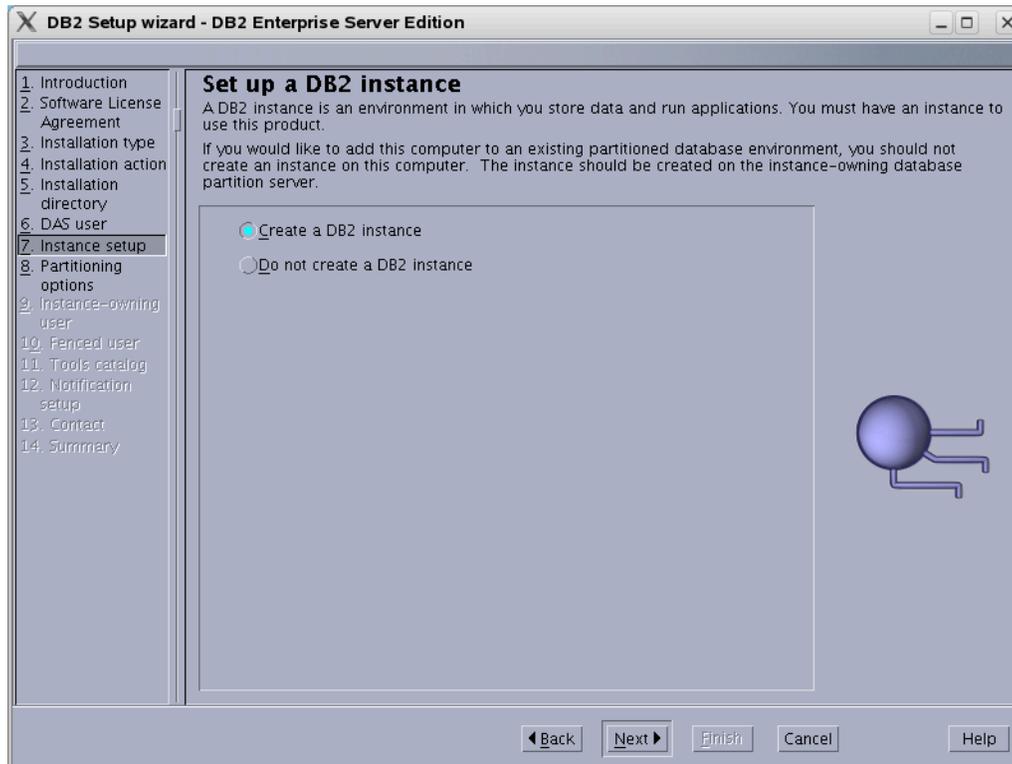
9. In “Select the installation directory,” either enter a directory or use the default and click **Next**.



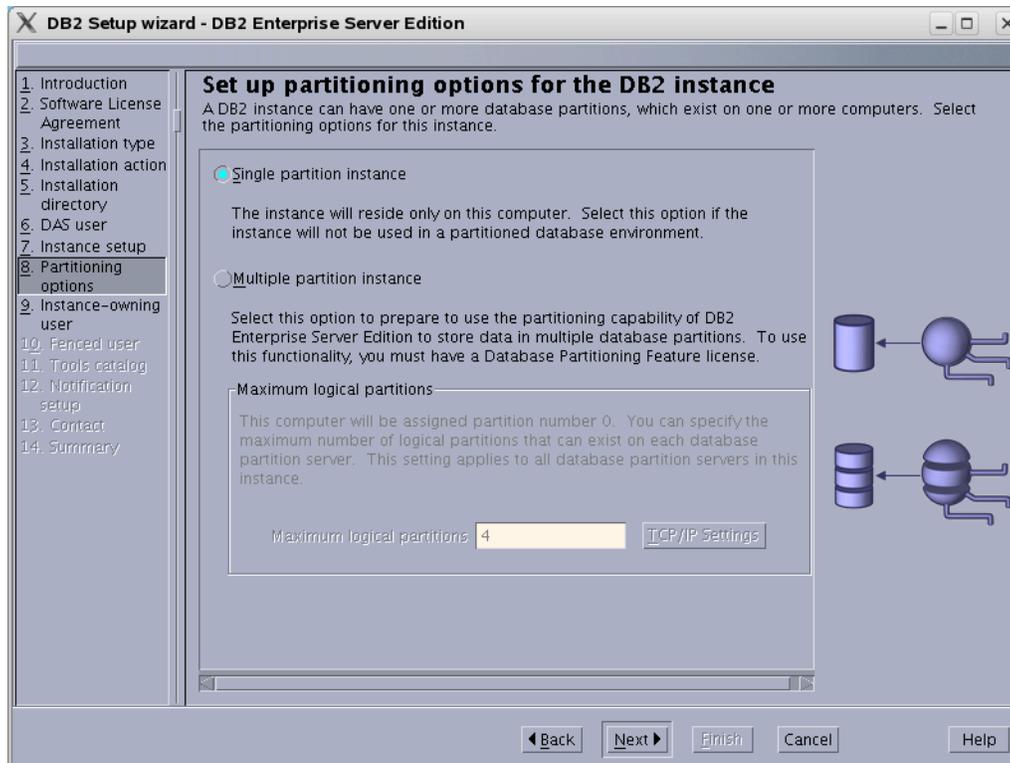
10. In “Set user information for the DB2 Administration Server”:
  - a. Keep the defaults, unless a previous attempt to install DB2 failed.
  - b. Enter a password.
  - c. Click **Next**.



11. In “Set up a DB2 instance,” select **Create a DB2 instance** and click **Next**.



12. In “Set up partitioning options for the DB2 instance,” select **Single partition instance** and click **Next**.



13. In “Set user information for the DB2 instance owner”:
  - a. Keep the defaults, unless a previous attempt to install DB2 failed.
  - b. Enter a password.
  - c. Click **Next**.

**DB2 Setup wizard - DB2 Enterprise Server Edition**

**Set user information for the DB2 instance owner**  
Specify the instance-owning user information for the DB2 instance. DB2 will use this user to perform instance functions, and will store instance information in the user's home directory. The name of the instance will be the same as the user name.

**New user**

User name:

UID:   Use default UID

Group name:

GID:   Use default GID

Password:  **Password**  
• You must specify a value. ▶

Confirm password:

Home directory:  ...

Existing user

User name:  ...

Navigation:

14. In “Set user information for the fenced user”:
  - a. Keep the defaults, unless a previous attempt to install DB2 failed.
  - b. Enter a password.
  - c. Click **Next**.

**DB2 Setup wizard - DB2 Enterprise Server Edition**

**Set user information for the fenced user**  
Specify the required information for the fenced user. Fenced user defined functions (UDFs) and stored procedures will execute under this user and group.

**New user**

User name: db2fenc1

UID:   Use default UID

Group name: db2fgrp1

GID:   Use default GID

Password:  **Password**  
• You must specify a value.

Confirm password:

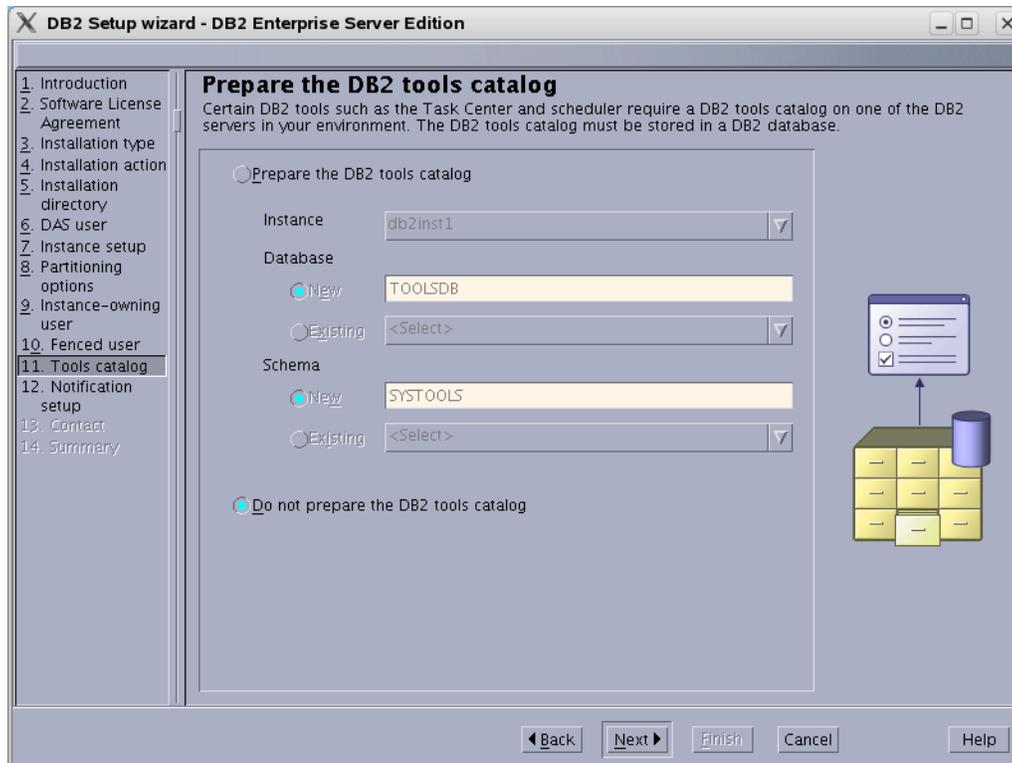
Home directory: /home/db2fenc1

Existing user

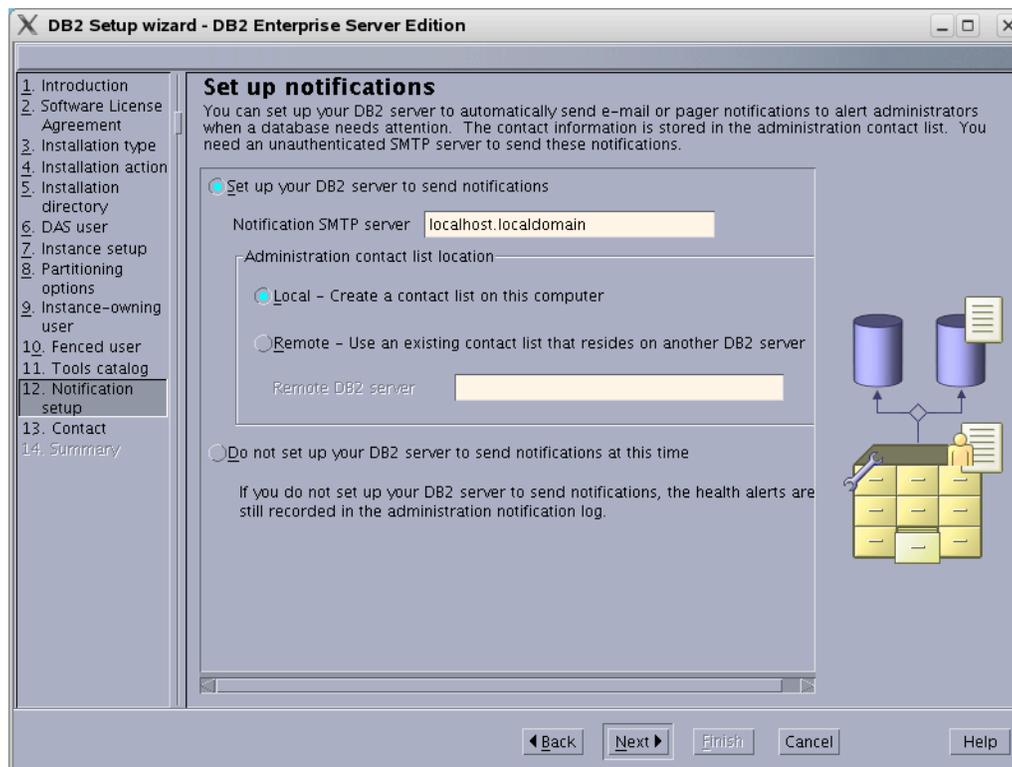
User name:

Back Next Finish Cancel Help

15. In “Prepare the DB2 tools catalog,” select **Do not prepare the DB2 tools catalog** and click **Next**.

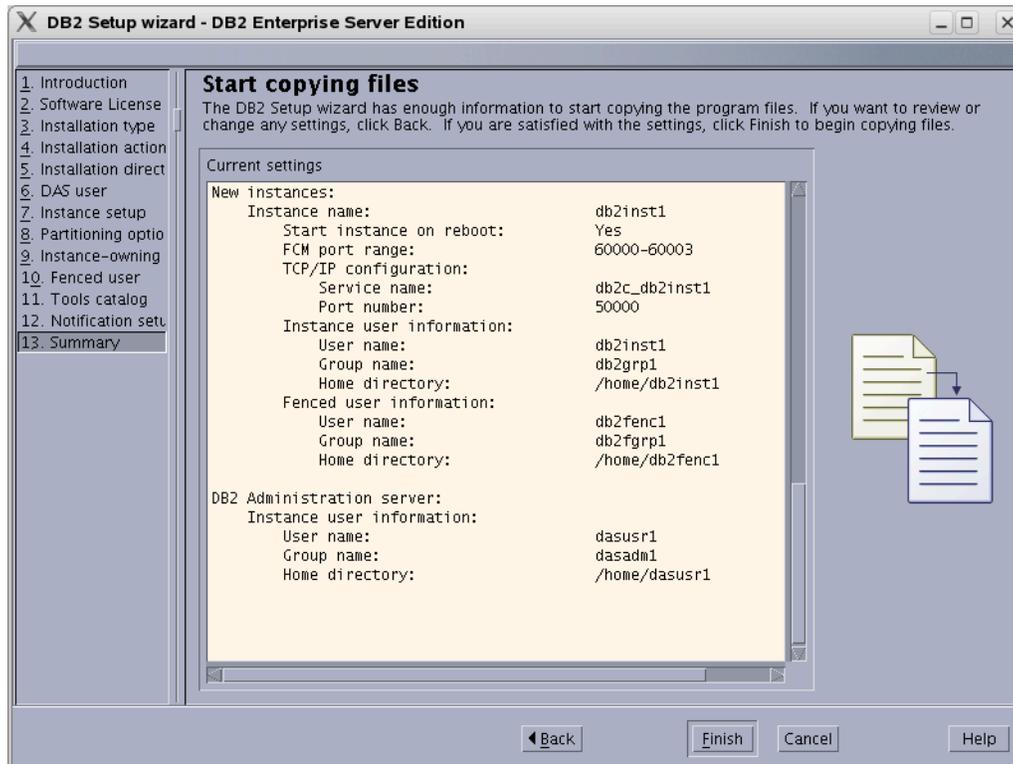


16. In “Set up notifications,” do one of the following:

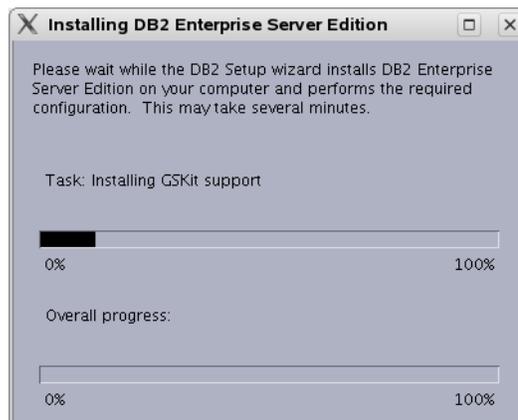


- If your system is a production server, select **Set up your DB2 server to send notifications**, enter a correct address for the local host, and click **Next**.
- If your system is not a production server, you can select **Do not set up your DB2 server to send notifications at this time**, and click **Next**.

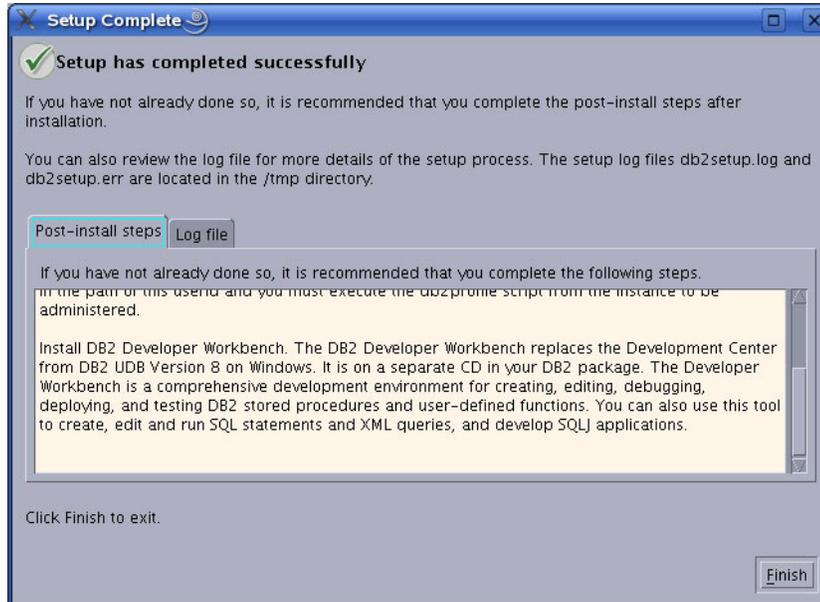
17. In “Start copying files,” check that your options are correct and click **Finish**.



18. Allow the installation to proceed.



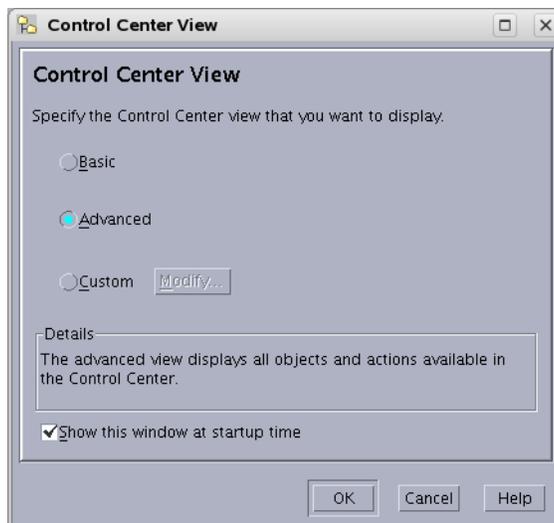
19. In “Setup has completed successfully,” read the notes, check the log tab, and click **Finish**.



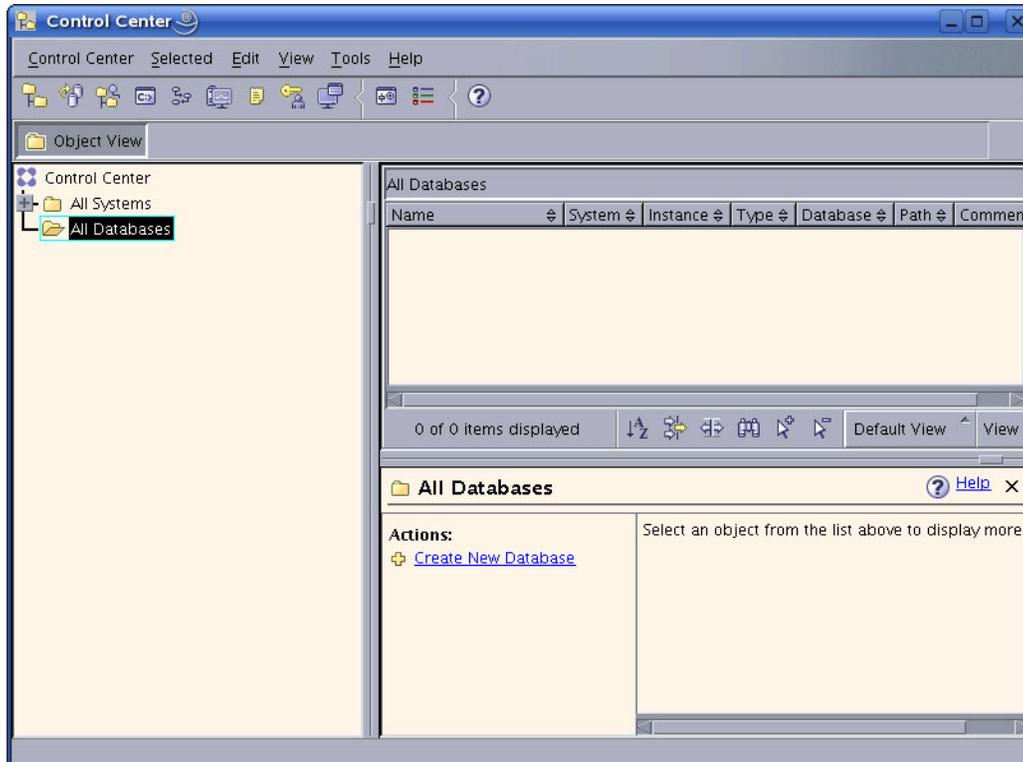
20. The installation of DB2 9.1 is now complete.

## B. Create a New DB2 Database

1. Log in as `db2inst1` (or your instance user created during the installation, step 13).
2. Navigate to: `./sqlllib/bin` and run `db2cc`
3. In the “Control Center View” screen, select **Advanced**.

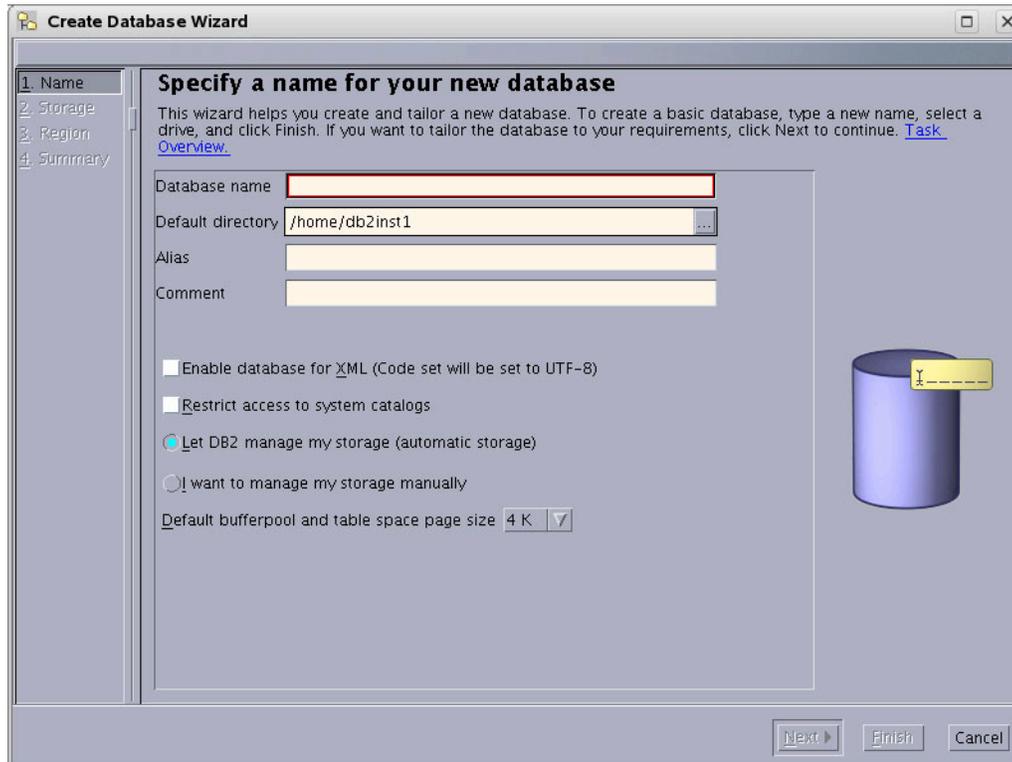


4. In the “Control Center,” open the application for creating a database:
  - a. Click the plus sign next to the tree option **All Systems**.

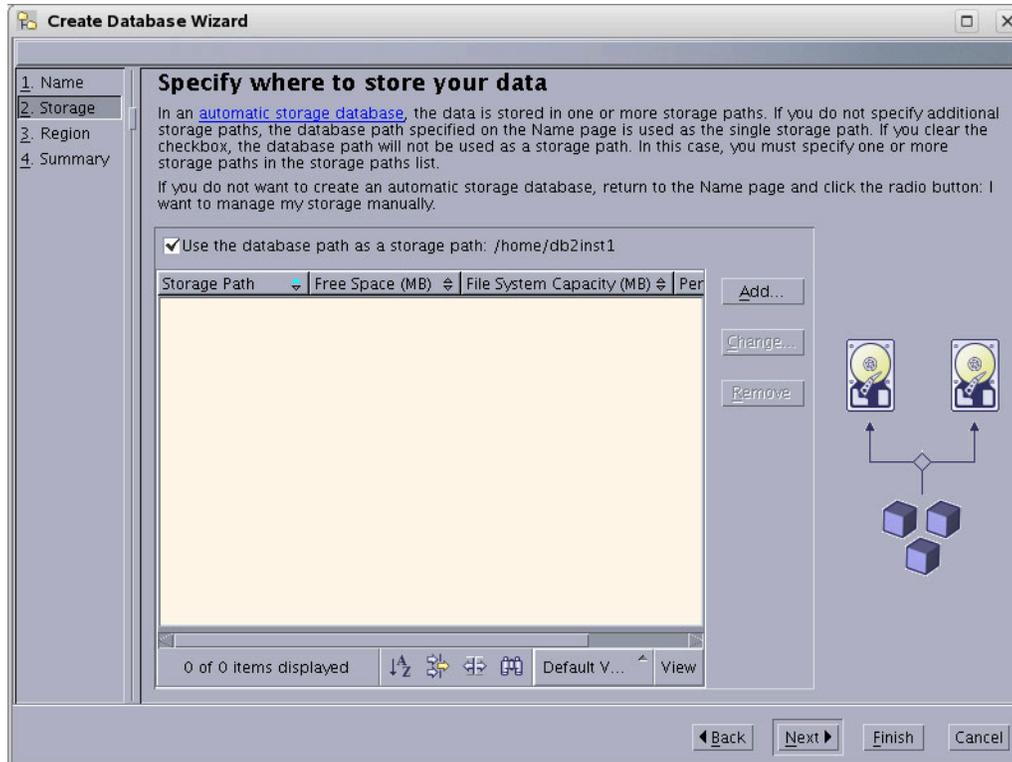


- b. Click on the expanded branch **All Databases**. (If you have not created a database previously, this branch is empty.)
    - c. Right-click on the branch **All Databases** and select **Create Database > Standard**.

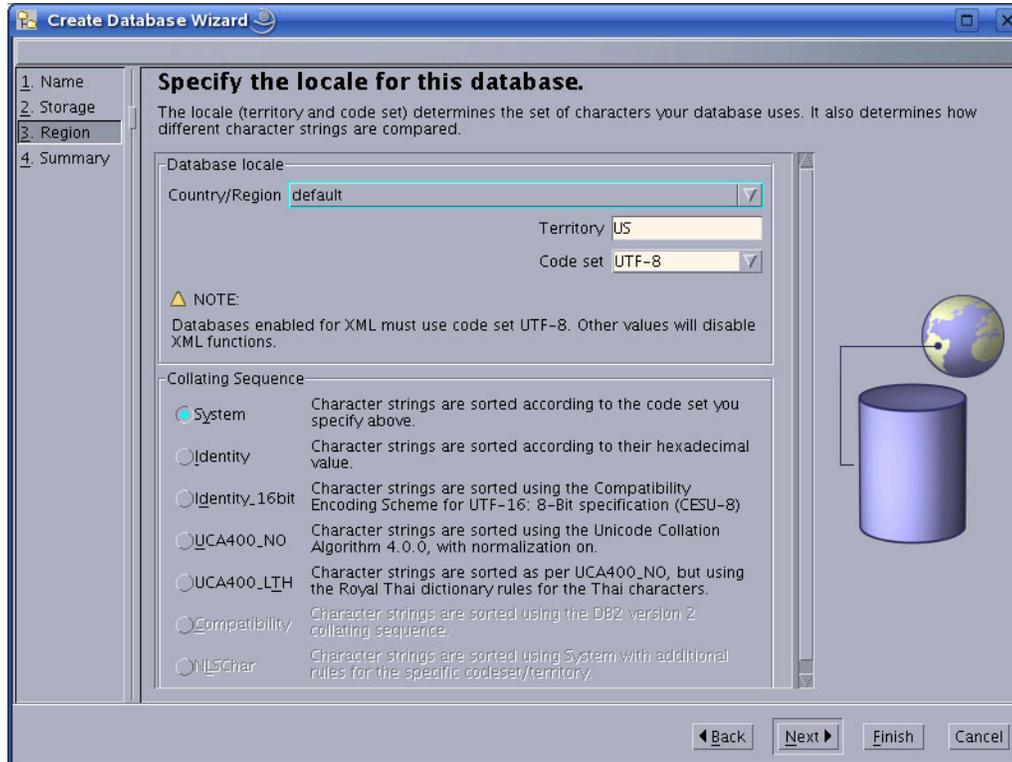
5. In “Specify a name for your new database”:
  - a. Enter a name for this database.
  - b. Select the check box **Enable database for XML**.
  - c. In the drop-down “Default bufferpool and table space page size,” select **32** and click **Next**.



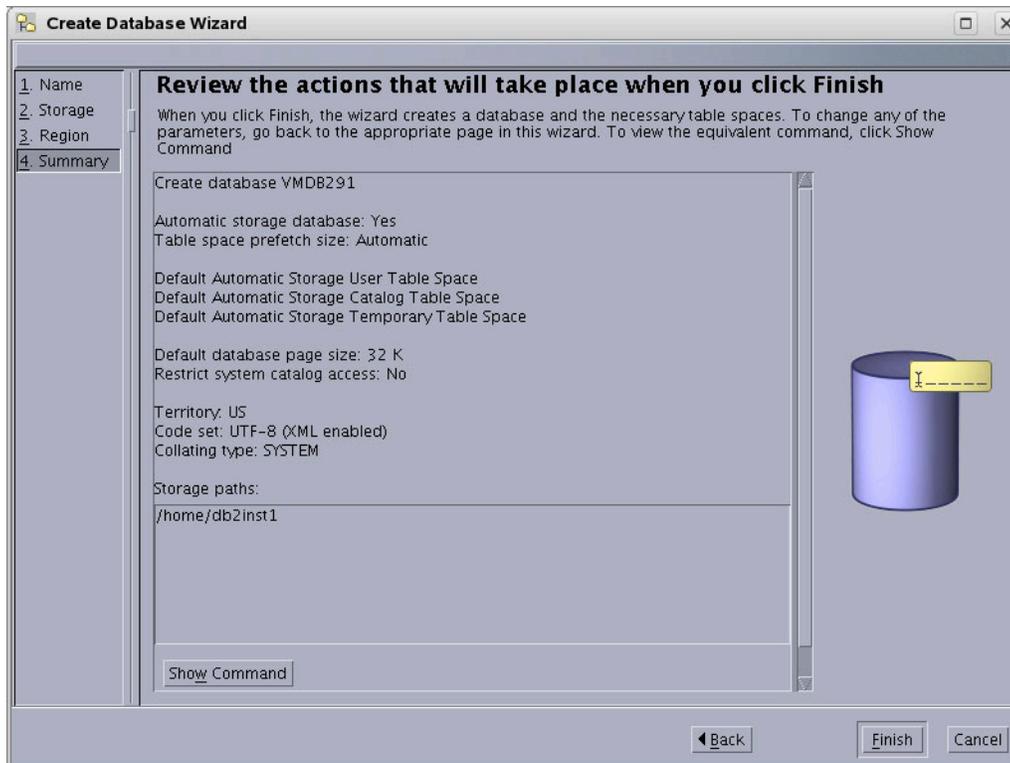
- In “Specify where to store your data,” click **Next** (a value is unnecessary, as we kept the default option of **Let DB2 manage my storage (automatic storage)**, on the previous page).



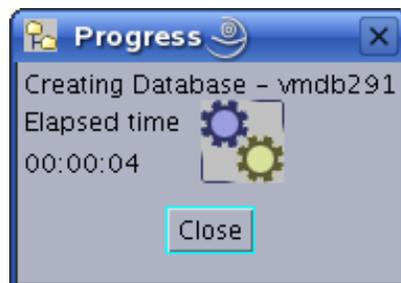
7. In “Specify the locale for this database,” ensure that the drop-down “Code set” displays UTF-8 and click **Next**.



8. In “Review the actions that will take place when you click finish,” confirm that everything looks correct and click **Finish**.

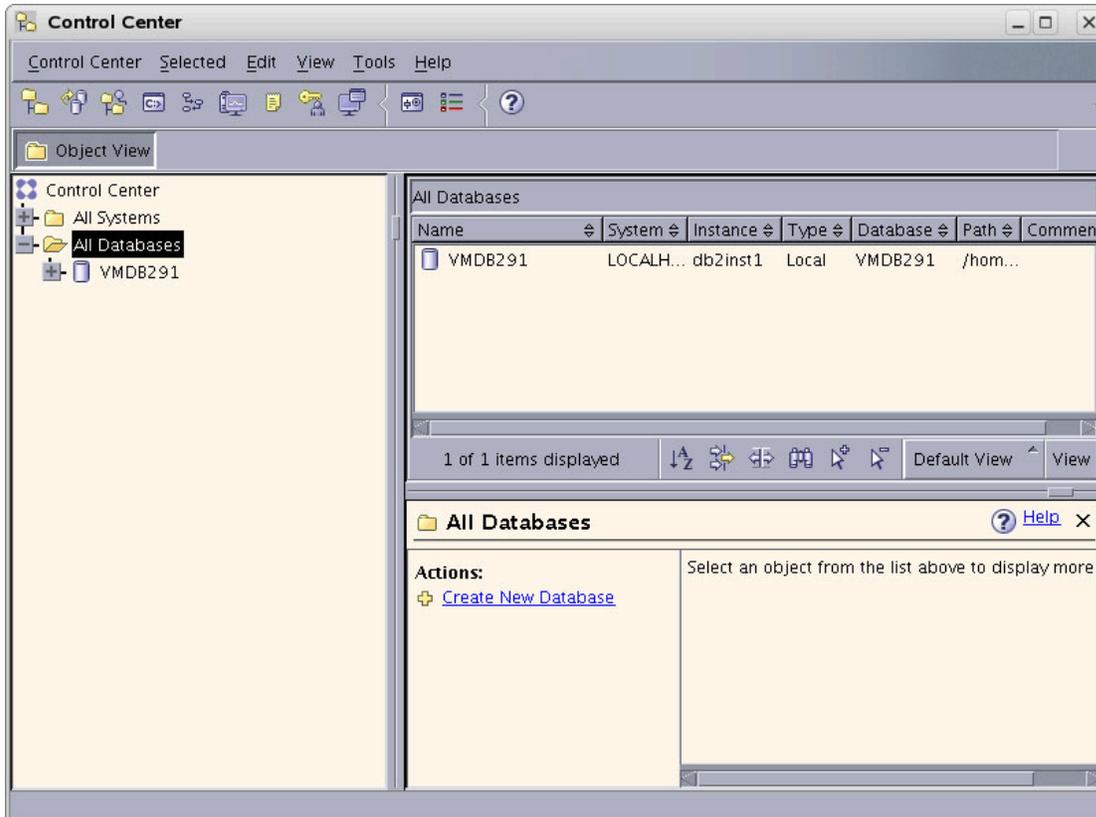


9. Allow the “Progress” window to complete creating the database. The window will close automatically when the database has been created.



10. The database has now been created and is displayed in the control center.

The figure below shows that a single database named `vmdb291` is present in the control center



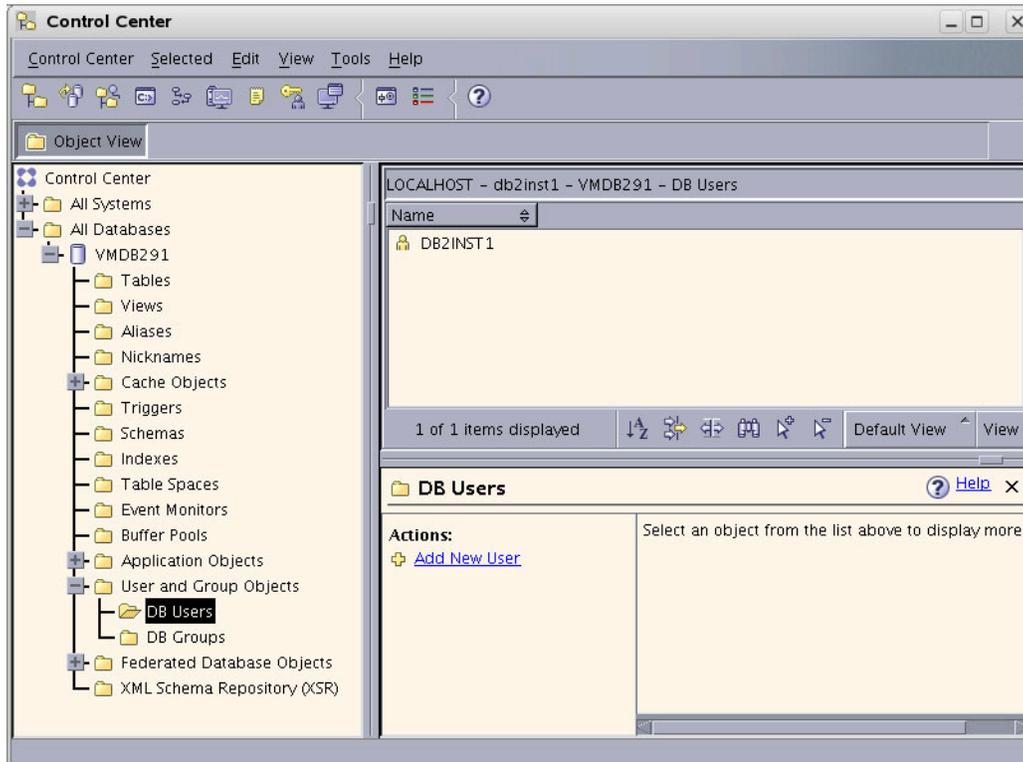
## C. Create a User for the New Database

1. Go to the command line. As the system user, create a new user named `csuser` that will be used to access the database from your FatWire product.

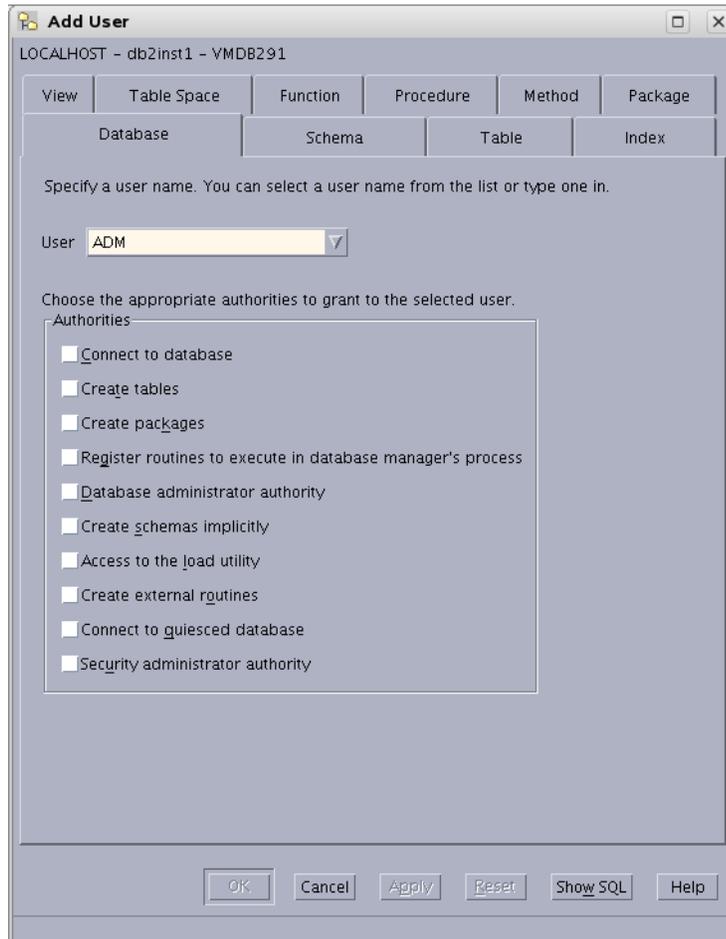
Example of how to create a user named `csuser` on Linux:

```
useradd -d /home/csuser -m -p demo4132 csuser
```

2. Go back to the “Control Center” and add the user:
  - a. Expand the newly created database in the tree by clicking the plus sign, then expanding the branch **User and Group Objects**.
  - b. Click **DB Users** to open the right-hand panel.
  - c. Right-click on the branch **DB Users** and select the **Add** option.



3. In the “Add User” application:
  - a. Select the user that was created in [step C on page 74](#).
  - b. Under “Authorities,” select all check boxes.
  - c. Click **OK**.

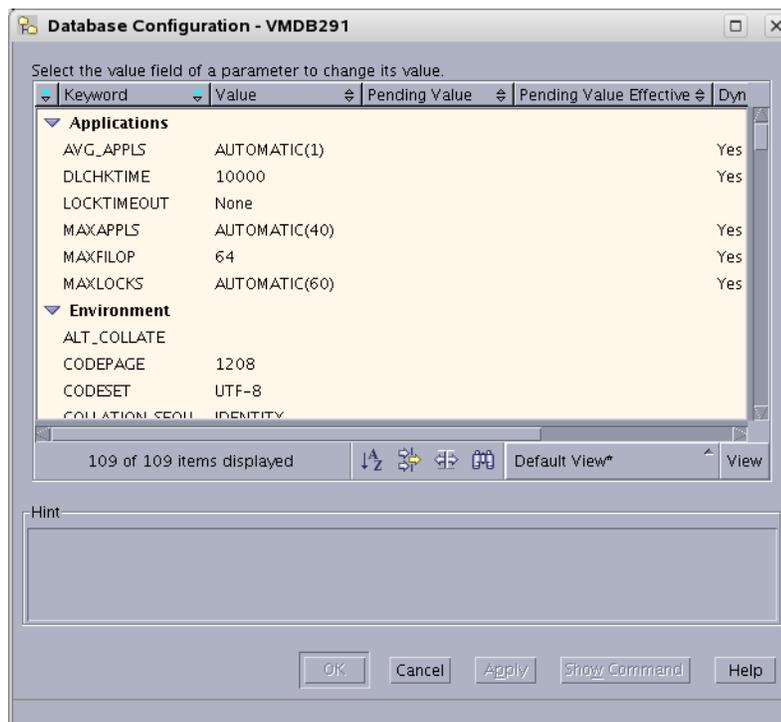


## D. Configure the Database

1. Right-click on the database that you created (listed in the branch that displays the database icon) and select **Configure Parameters**.
2. In “Database Configuration”:
  - a. Scroll through the list of options and replace the values of the following parameters with the values shown here:

|                 |      |
|-----------------|------|
| LOCKTIMEOUT     | 30   |
| APP_CTL_HEAP_SZ | 1024 |
| APPHEAPSZ       | 1024 |

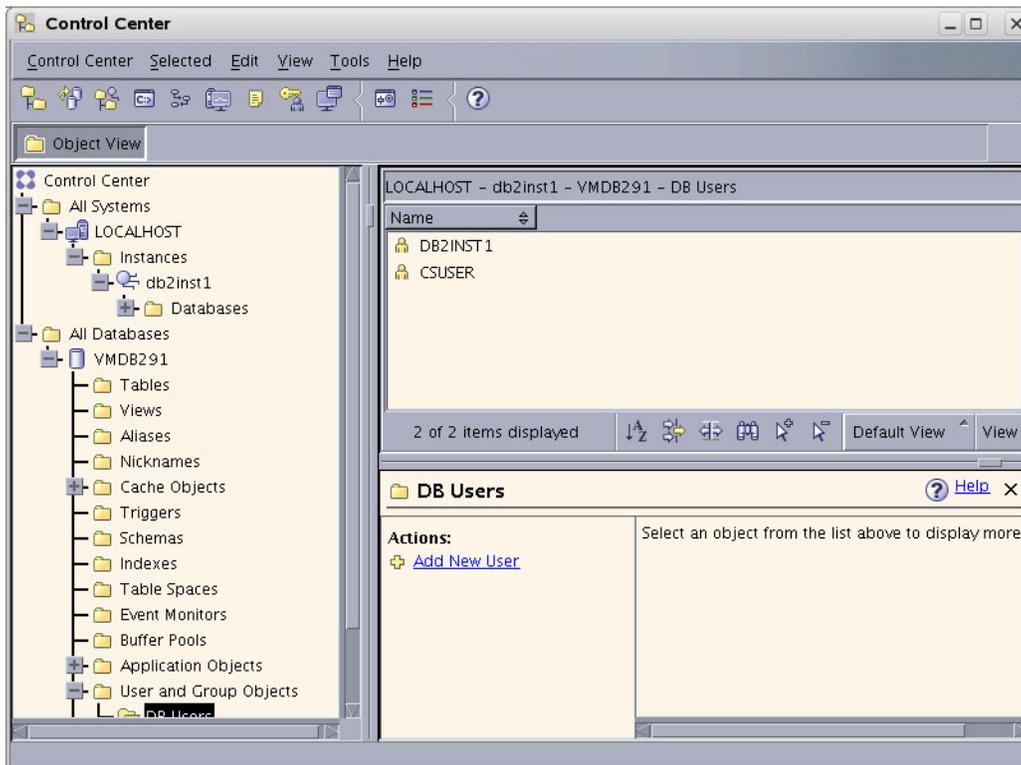
- b. Click **OK**.



3. Right-click on the database that you created (listed in the branch that displays the database icon) and select **Restart**.

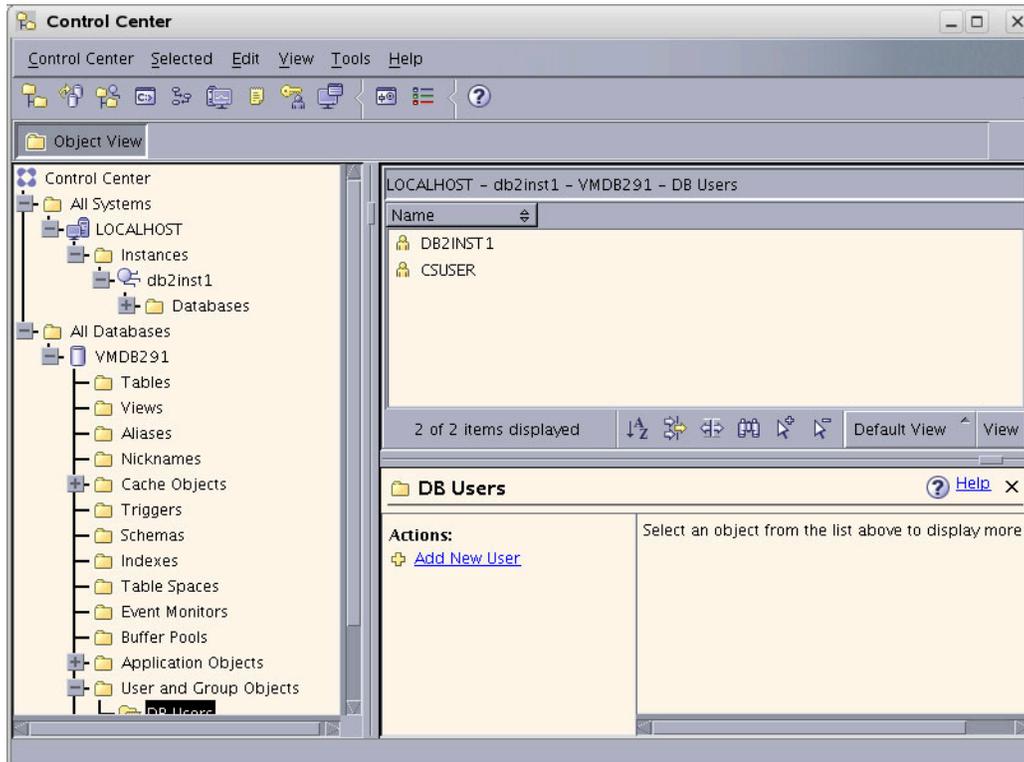
A status window flashes. *This does not mean that the operation has been completed.* Typically, you will need to wait 2 to 3 minutes for the system to restart.

4. Stop the instance:
  - a. Expand the following “Control Center” tree branch: **All Systems > LOCALHOST > Instances > name\_of\_your\_instance**
  - b. Right-click on the instance.
  - c. Select **Stop**.



- d. In the “Confirm stop” dialog box, click **OK**.
- e. Wait for the message that the instance has been stopped.

5. Start the instance:
  - a. Expand the following “Control Center” tree branch: **All Systems > LOCALHOST > Instances > name\_of\_your\_instance**
  - b. Right-click on the instance.
  - c. Select **Start**.



6. Wait for the message that the instance has been started. ***This does not mean that the operation has been completed.*** Typically, you will need to wait 2 to 3 minutes for the system to restart.

Your database is now ready for use with your FatWire software product.



## Part 2

# Installing a Web Server

This part describes how to install a web server. It contains the following chapters:

- [Chapter 6, “Worksheets for Documenting the Web Server Installation”](#)
- [Chapter 7, “Installing IIS on Windows”](#)
- [Chapter 8, “Installing Apache on Solaris and Linux”](#)



## Chapter 6

# Worksheets for Documenting the Web Server Installation

This chapter contains worksheets listing the web server parameters that you need to track. Print this chapter. Then, as you install software, fill in the blank fields in these worksheets with the values of the specified parameters. You will save considerable time by doing this. Additionally, if something fails during the installation, the information in these worksheets will be valuable while you are troubleshooting. Use a separate set of worksheets for each installation so that each installation is fully documented.

The worksheets are constructed as tables that are divided into the following categories:

- [Key to Sample Values](#)
- [Web Server Parameters](#)

## Key to Sample Values

The installation worksheets list parameters along with their sample values. Each sample value is classified as one of the following:

- **Default:** the value is automatically created at the time of the installation.
- **Normal:** the value represents the normal configuration for a simple installation. Do not use a different value unless your system requires it.
- **Option:** the value must be chosen from a preset list of options.
- **Suggested:** the value is recommended for the parameter.

### Note

A **Suggested** account name has an Example password value. We strongly recommend that you select a password for this account that is appropriate for the security of your system.

- **Example:** the value is only an example that must be replaced by the value that is appropriate for your installation. The example value is not likely to be valid in your environment.

## Web Server Parameters

**Table 1:** IIS Web Server Parameters

| Parameter                                     | Shown As          | Comments                       | Your Value |
|---|-------------------|--------------------------------|------------|
| Web Version                                   | <i>WebVersion</i> | Example:<br>Apache 1.3.37      |            |
| Web Host Name                                 | <i>WebHost</i>    | Example:<br>jeeves             |            |
| Web Host IP Address                           | <i>WebIP</i>      | Example:<br>104.222.111.155    |            |
| Web Server Port                               | <i>WebPort</i>    | Default:<br>80                 |            |
| IIS Only:<br>Filter Name (ISAPI plug-in name) | <i>FilterName</i> | Suggested:<br>iisforwardfilter |            |
| Apache Only:<br>Apache Root Directory         | <i>ApacheRoot</i> | Example:<br>/usr/apache        |            |

**Table 2:** Apache Web Server Parameters

| Parameter                                     | Shown As          | Comments                       | Your Value |
|---|-------------------|--------------------------------|------------|
| Web Version                                   | <i>WebVersion</i> | Example:<br>Apache 1.3.37      |            |
| Web Host Name                                 | <i>WebHost</i>    | Example:<br>jeeves             |            |
| Web Host IP Address                           | <i>WebIP</i>      | Example:<br>104.222.111.155    |            |
| Web Server Port                               | <i>WebPort</i>    | Default:<br>80                 |            |
| IIS Only:<br>Filter Name (ISAPI plug-in name) | <i>FilterName</i> | Suggested:<br>iisforwardfilter |            |
| Apache Only:<br>Apache Root Directory         | <i>ApacheRoot</i> | Example:<br>/usr/apache        |            |



## Chapter 7

# Installing IIS on Windows

This chapter explains how to install and test Microsoft's Internet Information Services (IIS). It contains the following sections:

- [Step I. Install IIS](#)
- [Step II. Document Your IIS Installation](#)
- [Step III. Verify the Installation](#)
- [Next Step](#)

### Note

Typically, IIS is either partially or fully installed on most Windows 2000 machines.

- If IIS is only partially installed or not installed, start with the first section, "[Step I. Install IIS](#)," on page 88.
- If IIS is fully installed, start with the section "[Step II. Document Your IIS Installation](#)," on page 88.

## Step I. Install IIS

If IIS is not installed or is only partially installed, follow Microsoft's instruction for installing IIS on a Windows 2000 system.

As a convenience, here is a quick synopsis of the instructions:

1. Select **Start > Settings > Control Panel**.
2. Select **Add/Remove Programs**.
3. Select the **Add/Remove Windows Components** tab on the left.  
The **Add/Remove Windows Components Wizard** appears.
4. Select **Internet Information Services (IIS)** and then follow the instructions for installing it.

## Step II. Document Your IIS Installation

We strongly recommend that you document the details of your IIS installation in [Table 3](#), “[IIS Parameters](#).”

**Table 3:** IIS Parameters

| Parameter                               | What It Holds  | Your Value |
|---|--|------------|
| Web Version<br>( <i>WebVersion</i> )    | The version number of the IIS software that you installed.                               |            |
| Web Host Name<br>( <i>WebHost</i> )     | The name by which the installation machine is known on the network.                      |            |
| Web Host IP Address<br>( <i>WebIP</i> ) | The numeric Internet Protocol address assigned to the web server host machine.           |            |
| Web Server Port<br>( <i>WebPort</i> )   | The port number assigned for web server communications. By default, it has the value 80. |            |

## Step III. Verify the Installation

After you have installed IIS, you start it and then browse to it in a web browser to determine whether it is serving pages as it should.

### A. Start IIS

You can start the various IIS services in various ways. To be sure that all the necessary services are running, start IIS from the **Services** node.

#### To start IIS services

1. Right-click on the **My Computer** icon.

2. Select **Manage** from the right-mouse menu.
3. In the **Computer Management** dialog box, expand the **Services and Applications** node in the tree.
4. Select **Services**.
5. In the list of services on the right, right click **IIS Admin Service**.
6. Select **Start** from the right mouse menu.

#### To start or stop the default web site only

1. Right-click on the **MyComputer** icon.
2. Select **Manage** from the right mouse menu.
3. In the **Computer Management** window, expand the **Services and Applications** node in the tree.
4. Expand the **Internet Information Services** node.
5. Right-click on **Default Web Site**.
6. Select **Start** or **Stop**, as appropriate, from the right mouse menu.

## B. Verify that IIS is Serving Pages

To verify that IIS can serve pages, test it from both the server that is hosting it and from another browser on the network.

#### To verify that IIS can serve pages

1. Start a browser on the host on which IIS is running.
2. From the browser, go to the following URL:  
`http://WebHost:WebPort`
3. Do one of the following:
  - If the browser displays the IIS home page, then IIS is installed and running properly. Continue to step 4.
  - If the browser returns an error, consult Microsoft's documentation, determine what went wrong, and fix it before you continue.
4. Start a browser on another machine on your network (a host other than the machine hosting IIS).
5. From the browser, go to the following URL:  
`http://WebHost:WebPort`  
If the browser displays the IIS "Under Construction" page, then IIS is installed and running and the network naming service appears to be working properly.

## Next Step

Configure the web server to run with WebLogic and Content Server. For instructions, refer to the installation guide for your configuration.



## Chapter 8

# Installing Apache on Solaris and Linux

This chapter describes how to install and configure Apache HTTP Server on Solaris and Linux systems. As previously mentioned, you can install Apache on the same machine that will host WebLogic and Content Server, or you can install and use it on a separate host.

This chapter contains the following sections:

- [Step I. Install Apache](#)
- [Step II. Document Your Apache Parameters](#)
- [Step III. Verify that Apache Contains the Correct Module](#)
- [Step IV. Verify that Apache Runs Properly](#)
- [Next Step](#)

## Step I. Install Apache

1. Apache HTTP Server can be pre-installed on Solaris 8, Solaris 9, Linux RedHat, and Linux SuSE systems. Determine whether Apache is installed on the environment(s) on which you plan to run it.
2. Do one of the following:
  - If Apache is already installed, continue with “[Step II. Document Your Apache Parameters,](#)” on page 92.
  - If Apache is not already installed, you can do one of the following:
    - Install it from your source medium.
    - Download it from the Internet.
    - Build it from source; that is, select the modules and compile the Apache executable yourself. If you want to build it from source, refer to the information that the Apache Foundation makes available at <http://www.apache.org/> and follow their instructions.

## Step II. Document Your Apache Parameters

We strongly recommend that you document the details of your Apache installation in [Table 4, “Apache Parameters.”](#)

**Table 4:** Apache Parameters

| Parameter                                      | What it Holds  | Your Value |
|--|--|------------|
| Web Server Version<br>( <i>WebVersion</i> )    | The version of Apache that the host is running. Note that you must use a version that Content Server supports.                           |            |
| Web Host Name<br>( <i>WebHost</i> )            | The name by which the Apache host machine is known on the network.   |            |
| Web Host IP Address<br>( <i>WebIP</i> )        | The numeric Internet Protocol address assigned to the Apache host machine.   |            |
| Web Server Port<br>( <i>WebPort</i> )          | The port number assigned for Apache communications. By default, it has the value 80.   |            |
| Apache Root Directory<br>( <i>ApacheRoot</i> ) | The top-level directory in which Apache is installed. Immediate subdirectories of <i>ApacheRoot</i> include <i>bin</i> and <i>conf</i> . |            |

## Step III. Verify that Apache Contains the Correct Module

### Note

This section applies only to Apache version 1.3x.

Apache is modular software, built from a set of modules. WebLogic Server requires that the `mod_so.c` module be present on the machine that is hosting the Apache web server. Please verify that your Apache server contains this module by using the command `httpd` with the `-l` option and search for `mod_so` in the output.

For example:

```
$ ApacheRoot/bin/httpd -l | grep 'mod_so'
mod_so.c
```

Examine the output and do one of the following:

- If the output from the preceding command contains `mod_so.c`, then your version of Apache contains the correct module. Proceed to [“Step IV. Verify that Apache Runs Properly,” on page 93](#).
- If the output from the preceding command does not contain `mod_so.c`, you must rebuild and reinstall Apache. For guidelines, see [“Step I. Install Apache,” on page 92](#).

## Step IV. Verify that Apache Runs Properly

In this step, you will start Apache and verify that it is running properly. For verification instructions, see the Apache web site (given in [“Step I. Install Apache,” on page 92](#)).

## Next Step

Configure Apache to run with WebLogic and Content Server. For instructions, refer to the installation guide for your configuration.



## Part 3

## Installing and Configuring LDAP

If you chose to use LDAP, Content Server requires access to a supported LDAP server that is specifically configured for the product. This part describes how to install and configure a supported LDAP server for integration with Content Server.

**Note**

You must set up a supported LDAP server **before** you run the CS LDAP integrator.

This part contains the following chapters:

- [Chapter 9, “Setting Up Sun Access Manager 7.0”](#)
- [Chapter 10, “Setting Up Sun Directory Server 6.0”](#)
- [Chapter 11, “Setting Up OpenLDAP 2.3.x”](#)
- [Chapter 12, “Setting Up the WebLogic 9.x Embedded LDAP Server”](#)
- [Chapter 13, “Setting Up Oracle Directory Server 10.x”](#)
- [Chapter 14, “Setting Up MS Active Directory Server 2003”](#)



## Chapter 9

# Setting Up Sun Access Manager 7.0

This chapter provides instructions for setting up the currently supported Sun Access Manager for use with Content Server.

### Note

Sun Access Manager is installed as part of Sun Portal Server 7, which means that either Sun Access Manager and Sun Directory Server were installed locally on your portal server, or you elected to configure Sun Access Manager to connect to a remote instance of Sun Java Systems Directory Server. In either case, you already have Sun Access Manager installed and configured for your application server and portal server.

Note that you must set up Sun Access Manager before you run the CS LDAP integrator.

This chapter contains the following sections:

- [Start/Stop Commands](#)
- [Creating CS Users in Sun Access Manager](#)

## Start/Stop Commands

This section lists commands for starting and stopping Sun Access Manager.

To start Sun Access Manager:

- On Solaris:  
`./usr/sbin/amserver start`
- On Unix (except Solaris):  
`<sun_portal_home>/identity/bin/amserver start`
- On Windows:  
**Start --> Programs --> Sun Microsystems --> Sun One Identity --> Start Sun One Identity Servers --> Start**

To stop Sun Access Manager:

- On Solaris:  
`./usr/sbin/amserver stop`
- On Unix (except Solaris):  
`<sun_portal_home>/identity/bin/amserver stop`
- On Windows:  
**Start --> Programs --> Sun Microsystems --> Sun One Identity --> Stop Sun One Identity Servers --> Stop**

## Creating CS Users in Sun Access Manager

In this section, you will use the Sun Access Manager console to create Content Server users in the backend LDAP server that is associated with Sun Access Manager.

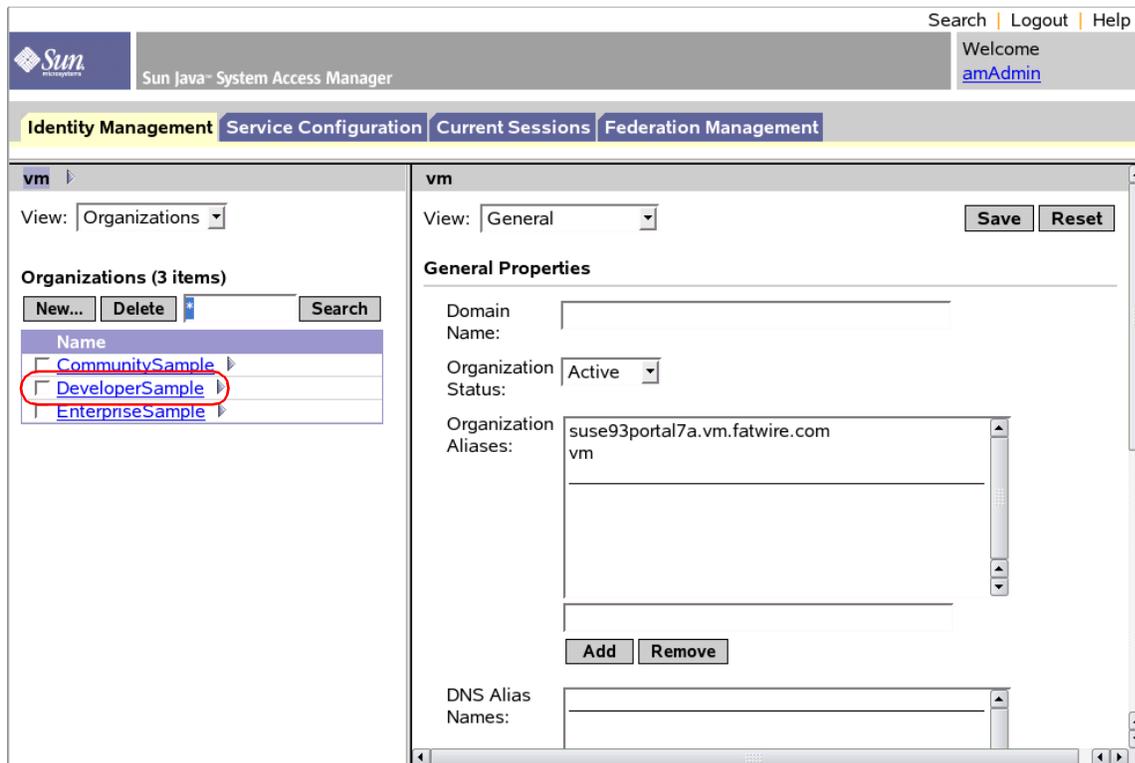
**To create Content Server users in Sun Access Manager**

1. Access the following URL:

`http://<app_server_address>:<port>/amconsole`



2. Log in using the user name (typically `amadmin`) and password that was selected during the installation of Sun Access Manager.
3. When logged in, you will see two large frames. The left-hand frame has a hierarchy that can be navigated. The right-hand frame has details for the item selected on the left.



4. In the left-hand frame, click the link **DeveloperSample** (or the portal site which you used when installing Content Server).

5. Click the **View** drop-down menu. From here you may select **Roles**, **Groups**, or **Users**. As you will be adding a new user, select **Users**.

The screenshot shows the Sun Access Manager web interface. The top navigation bar includes 'Search | Logout | Help' and a 'Welcome amAdmin' message. Below the navigation bar are tabs for 'Identity Management', 'Service Configuration', 'Current Sessions', and 'Federation Management'. The main content area is divided into two panes. The left pane shows a breadcrumb 'vm > DeveloperSample' and a 'View:' dropdown menu with a red circle around it. The dropdown menu is open, showing options: 'Organizations', 'Groups', 'Users', 'Services', 'Roles', 'Policies', and 'Agents'. The right pane is titled 'DeveloperSample' and shows 'View: General' with 'Save' and 'Reset' buttons. Below this is the 'General Properties' section with fields for 'Domain Name', 'Organization Status' (set to 'Active'), and 'Organization Aliases' (containing 'DeveloperSample'). There are 'Add' and 'Remove' buttons for the aliases, and a 'DNS Alias Names' field at the bottom.

6. A list of all known users is displayed in the left frame. Click **New**.

The screenshot shows the Sun Access Manager web interface with the 'fwadmin' user configuration page. The top navigation bar and tabs are the same as in the previous screenshot. The left pane shows a breadcrumb 'vm > DeveloperSample' and a 'View:' dropdown menu set to 'Users'. Below this is a table titled 'Users (1 item)' with columns 'User ID' and 'Full Name'. The table contains one entry: 'fwadmin' with 'fwadmin' as the full name. There are 'New...', 'Delete', and 'Search' buttons, along with an 'Advanced Search...' link. The right pane is titled 'fwadmin' and shows 'View: General' with 'Save' and 'Reset' buttons. Below this is a form for user details with fields for 'First Name', '\* Last Name' (set to 'default'), '\* Full Name' (set to 'fwadmin'), 'Password' (with a 'Change...' link), 'Email Address', 'Employee Number', 'Telephone Number', 'Home Address', '\* User Status' (set to 'Active'), and 'Account Expiration Date' (with a format 'mm/dd/yyyy hh:mm'). A note '\* Indicates required field' is present.

7. Select the following services from the list in the right-hand frame:

- **Mobile Address Book**
- **Mobile Calendar**
- **Mobile Mail**
- **Portal Desktop**
- **Portal Subscriptions**
- **SSO Adapter**

Click **Next**.

The screenshot displays the Sun Access Manager web interface. At the top, there is a navigation bar with 'Search | Logout | Help' and a 'Welcome amAdmin' message. Below this is a menu with 'Identity Management', 'Service Configuration', 'Current Sessions', and 'Federation Management'. The main content area is split into two panes. The left pane, titled 'vm > DeveloperSample', shows a 'View: Users' dropdown and a table with one user: 'fwadmin'. The right pane, titled 'New User - Step 1 of 2', contains the heading 'Select the services to be assigned to the user.' and a list of 'Available Services'. The services listed are: Access List, Authentication Configuration, Mobile Address Book (checked), Mobile Calendar (checked), Mobile Mail (checked), NetFile, Netlet, portal1 Desktop (checked), portal1 Subscriptions (checked), Proxylet, and SSO Adapter (checked). At the bottom of the right pane are 'Back', 'Next', and 'Cancel' buttons.

8. In the “New User” form, fill out the required fields (marked by a red \*). Ensure that “User Status” is set to **Active**. Click **Finish**.

The screenshot shows the Sun Access Manager interface. The top navigation bar includes 'Search | Logout | Help' and 'Welcome amAdmin'. The main navigation tabs are 'Identity Management', 'Service Configuration', 'Current Sessions', and 'Federation Management'. The current page is 'New User - Step 2 of 2' under the 'Identity Management' tab. The left sidebar shows a search bar with 'fwadmin' entered and a table of users:

| User ID | Full Name |
|---------|-----------|
| fwadmin | fwadmin   |

The main form area is titled 'Enter Required User Attributes' and contains the following fields:

- \* User ID: demouser
- First Name: (empty)
- \* Last Name: demo
- \* Full Name: user
- \* Password: \*\*\*\*\*
- \* Password (confirm): \*\*\*\*\*
- \* User Status: Active (dropdown menu)

Buttons at the bottom include 'Back', 'Finish', and 'Cancel'. A legend indicates that an asterisk (\*) denotes a required field.

9. Assign Groups to the user:
  - a. Locate the newly created user (the fastest way is to use the **Search** function).

The screenshot displays the Sun Access Manager 7.0 web interface. At the top, there is a navigation bar with 'Search | Logout | Help' and a welcome message 'Welcome amAdmin'. Below this is a menu with 'Identity Management', 'Service Configuration', 'Current Sessions', and 'Federation Management'. The main content area is split into two panes. The left pane, titled 'vm > DeveloperSample', shows a 'View: Users' dropdown and a search section with 'Users (1 item)', 'New...', 'Delete', a search input field containing '\*user', and a 'Search' button. A table below the search shows one user: 'demouser user', with a red circle around the entry. The right pane, titled 'demouser', shows a 'View: General' dropdown and 'Save' and 'Reset' buttons. It contains a form with various fields: 'First Name', '\* Last Name: demo', '\* Full Name: user', 'Password: Change...', 'Email Address', 'Employee Number', 'Telephone Number', 'Home Address', '\* User Status: Active', 'Account Expiration Date', and a format note 'Format: mm/dd/yyyy hh:mm'. A red asterisk indicates required fields.

- b. In the right-hand frame, select **Groups** from the “View” drop-down menu.

The screenshot shows the Sun Access Manager web interface. The top navigation bar includes 'Search | Logout | Help' and a 'Welcome amAdmin' message. Below this are tabs for 'Identity Management', 'Service Configuration', 'Current Sessions', and 'Federation Management'. The main content area is split into two panes. The left pane, titled 'vm > DeveloperSample', shows a 'View: Users' dropdown and a list of 10 users with columns for 'User ID' and 'Full Name'. The right pane, titled 'demouser', has a 'View: Groups' dropdown (highlighted with a red circle) and a list of available groups. Below the 'Available:' list are buttons for 'Add', 'Add All', 'Remove', and 'Remove All'. The 'Selected:' list is currently empty.

Search | Logout | Help  
Welcome amAdmin

Identity Management Service Configuration Current Sessions Federation Management

vm > DeveloperSample ▾ demouser

View: Users ▾ View: Groups ▾

Users (10 items)  
New... Delete user\* Search  
Advanced Search...

| User ID                                | Full Name       |
|--|-----------------|
| <input type="checkbox"/> demouser      | user ▾          |
| <input type="checkbox"/> user_analyst  | user_analyst ▾  |
| <input type="checkbox"/> user_approver | user_approver ▾ |
| <input type="checkbox"/> user_author   | user_author ▾   |
| <input type="checkbox"/> user_checker  | user_checker ▾  |
| <input type="checkbox"/> user_designer | user_designer ▾ |
| <input type="checkbox"/> user_editor   | user_editor ▾   |
| <input type="checkbox"/> user_expert   | user_expert ▾   |
| <input type="checkbox"/> user_marketer | user_marketer ▾ |
| <input type="checkbox"/> user_pricer   | user_pricer ▾   |

The Selected list contains the groups associated with this user.  
Use Search to find a specific group.

\* Search

Available:

- PageEditor
- GE Lighting-GeneralAdmin
- BurlingtonFinancial-Designer
- GE Lighting-WorkflowAdmin
- FirstSiteII-ProductEditor
- GE Lighting-Designer
- BurlingtonFinancial-Checker
- FirstSiteII-ProductAuthor

Add Add All Remove Remove All

Selected:

- c. In the “Available” list box, select all Groups that you wish this user to have. In this example, three groups were assigned to the user: **Spark-SiteAdmin**, **Spark-SparkContentUser**, **Spark-GeneralAdmin** (listed in the “Selected” list box). For more detailed information about available groups, see the *Content Server Administrator’s Guide*.
- d. Click **Add**.
- e. Click **Save**.

The screenshot displays the Sun Java System Access Manager web interface. At the top, there is a navigation bar with 'Search | Logout | Help' and a welcome message 'Welcome amAdmin'. Below this is a menu with 'Identity Management', 'Service Configuration', 'Current Sessions', and 'Federation Management'. The main content area is split into two panes. The left pane, titled 'vm > DeveloperSample', shows a 'View: Users' dropdown and a search box with 'user\*' and a 'Search' button. Below the search box is a table of users:

| User ID                                | Full Name     |
|--|---------------|
| <input type="checkbox"/> demouser      | user          |
| <input type="checkbox"/> user_analyst  | user_analyst  |
| <input type="checkbox"/> user_approver | user_approver |
| <input type="checkbox"/> user_author   | user_author   |
| <input type="checkbox"/> user_checker  | user_checker  |
| <input type="checkbox"/> user_designer | user_designer |
| <input type="checkbox"/> user_editor   | user_editor   |
| <input type="checkbox"/> user_expert   | user_expert   |
| <input type="checkbox"/> user_marketer | user_marketer |
| <input type="checkbox"/> user_pricer   | user_pricer   |

The right pane is titled 'Use Search to find a specific group.' and contains a search box with an asterisk and a 'Search' button. Below the search box are two list boxes. The 'Available' list contains: PageEditor, GE Lighting-GeneralAdmin, BurlingtonFinancial-Designer, GE Lighting-WorkflowAdmin, FirstSitel-ProductEditor, GE Lighting-Designer, BurlingtonFinancial-Checker, and FirstSitel-ProductAuthor. Below this list are buttons for 'Add', 'Add All', 'Remove', and 'Remove All'. The 'Selected' list contains: Spark-SiteAdmin, Spark-SparkContentUser, and Spark-GeneralAdmin. At the bottom right of the right pane are 'Save' and 'Reset' buttons.

10. (Optional) Test your new user by logging in to the portal (must be the organization under which the user was created and Content Server was installed; for example, DeveloperSample Organization).



## Chapter 10

# Setting Up Sun Directory Server 6.0

This chapter shows you how to set up Sun Directory Server 6.0 for use with Content Server running on Sun Portal Server 7.

### Note

You must set up Sun Directory Server **before** you run the CS LDAP integrator.

This chapter contains the following sections:

- [Start/Stop Commands](#)
- [Installing Sun Directory Server](#)
- [Post-Installation Steps](#)
- [Completing and Verifying the LDAP Configuration](#)
- [Modifying User Passwords](#)

## Start/Stop Commands

This section contains commands for starting and stopping Sun Directory Server and the Sun Java Web Console.

### Sun Directory Server

- To start:  
`/opt/sun/ds6/bin/dsadm start <instance_dir>`
- To stop:  
`/opt/sun/ds6/bin/dsadm stop <instance_dir>`

### Sun Java Web Console

- To start:  
`/opt/sun/webconsole/bin/smcwebserver start`
- To stop:  
`/opt/sun/webconsole/bin/smcwebserver stop`

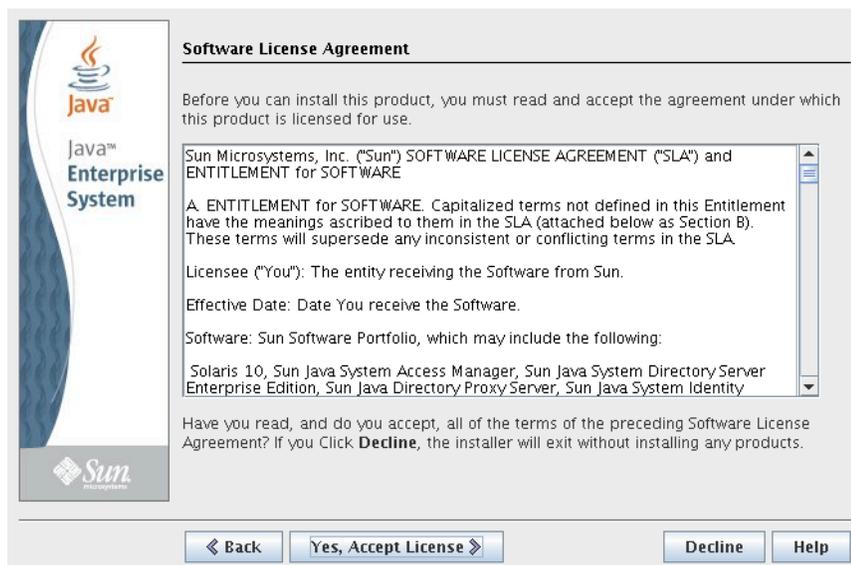
## Installing Sun Directory Server

This section shows you how to install Sun Directory Server 6.

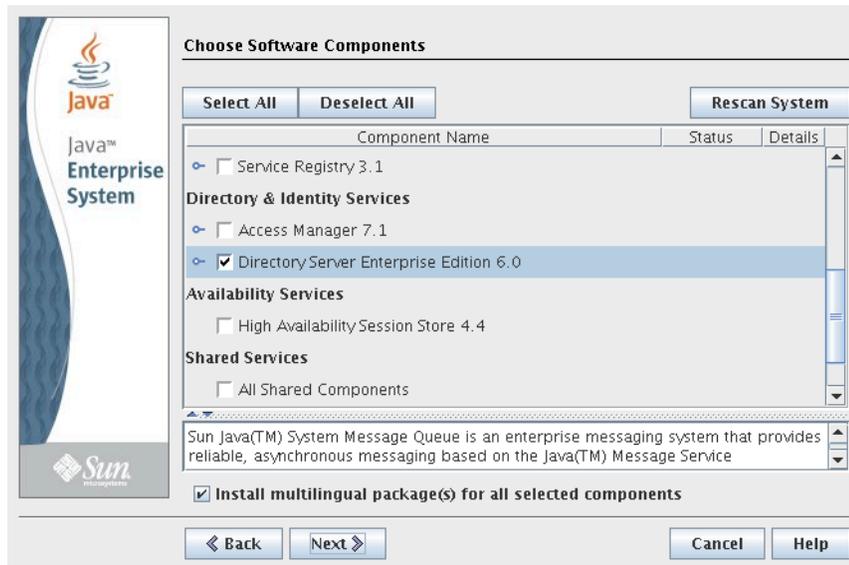
1. Download the Directory Server 6 package from the Sun website.
2. Decompress the file into a temporary directory and change to that directory.
3. Within the temporary directory, change to the directory corresponding to your operating system and launch the installer.
4. In the “Welcome” screen, click **Next**.



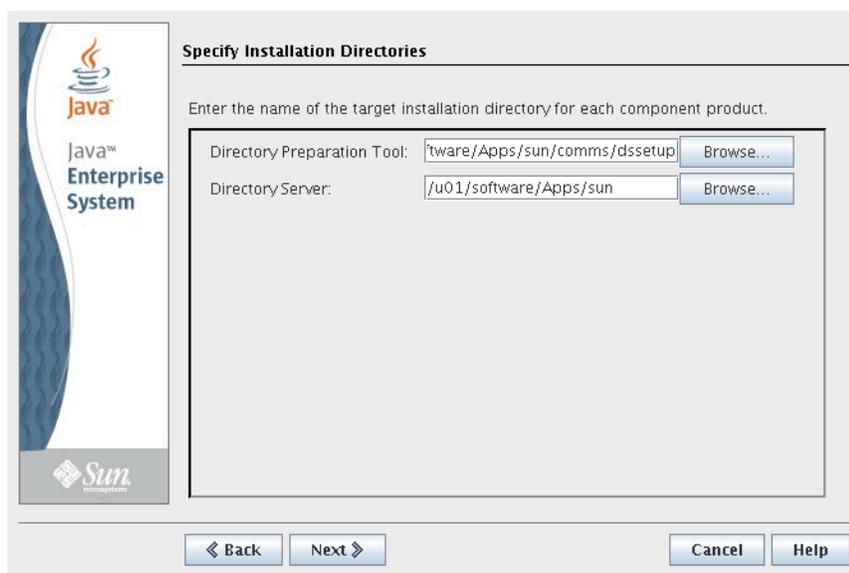
5. In the “Software License Agreement” screen, read the license agreement and click **Yes, Accept License**.



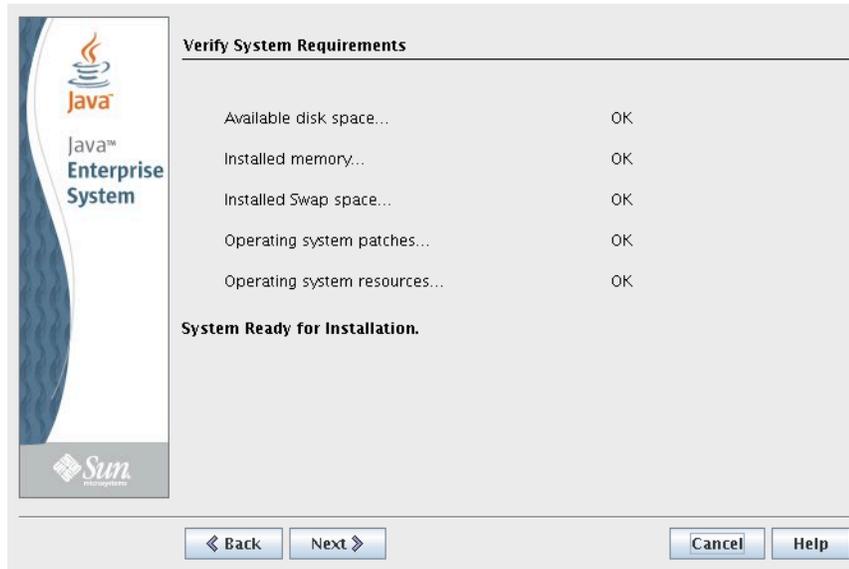
6. In the “Choose Software Components” screen, do the following:
  - a. Select **Directory Server Enterprise Edition 6.0**.
  - b. Expand the node and make sure that **Directory Service Control Center** is listed and selected.
  - c. Click **Next**.



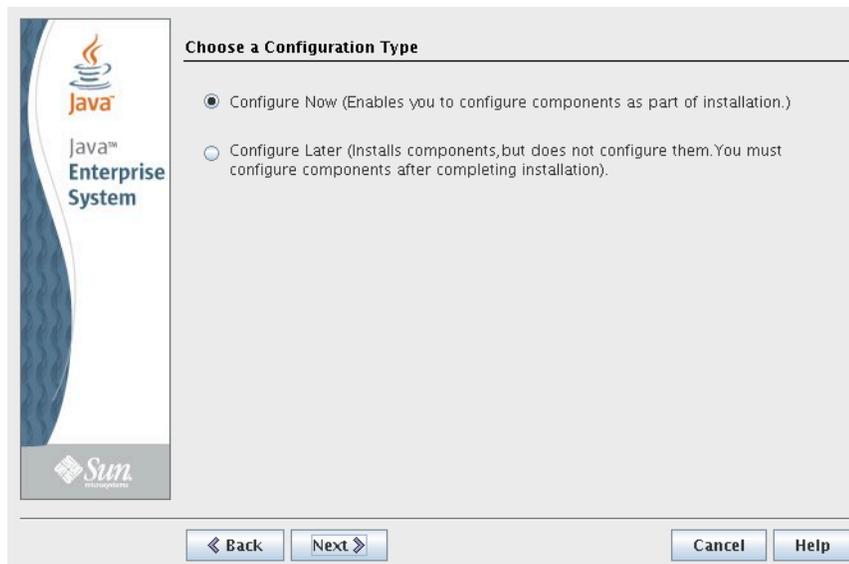
7. In the “Specify Installation Directories” screen, do the following:
  - a. Enter the target installation directory for the Directory Preparation Tool.
  - b. Enter the target installation directory for Sun Directory Server. (This directory will be referred to as `<dirserv_home>` in the remainder of this chapter.)



8. In the “Verify System Requirements” screen, wait until the status of all items reads “OK,” then click **Next**. If any of the items fail the verification, you must remedy the problem and restart the installation.



9. In the “Choose a Configuration Type” screen, select **Configure Now** and click **Next**.



10. In the “Specify Common Server Settings” screen, enter the required information, then click **Next**.

### Note

The host name and IP address of the machine running Directory Server must have a valid DNS entry on your network.

**Specify Common Server Settings**

The following settings will be the default values for all installed component products as needed. The values can be overridden when you configure the products.

Host Name: rho10wl

DNS Domain Name: vm.fatwire.com

Host IP Address: 10.120.19.45

Administrator User ID: admin

Administrator Password: \*\*\*\*\* At least 8 characters long

Retype Password: \*\*\*\*\*

System User: root

System Group: root

The values you enter above will appear as default values on the pages that follow. Fields that include these default values will be marked with this note: \*Shared default value

◀ Back Next ▶ Cancel Help

11. In the “Create Directory Instance” screen, select **Yes** and click **Next**.

**Directory Server: Create Directory Instance**

DirectoryServer Console requires DirectoryServer, but does not require a directory instance.

Although not a requirement, you can create a directory instance now during installation.

Create a directory instance (in addition to installing DirectoryServer)?

Yes

No

◀ Back Next ▶ Cancel Help

12. In the “Specify Instance Creation Information” screen, do the following:
  - a. Specify the directory in which the new Directory Server instance will reside. (This directory will be referred to as `<instance_dir>` in the remainder of this chapter.)
  - b. Specify the values for the **System User** and **System Group** fields.
  - c. Specify a Directory Manager password.
  - d. Specify the value for the **Suffix** field. (This value will be the **DN** value used to connect to this Directory Server instance; you will need it in [step 4 on page 115](#).)
  - e. Click **Next**.

**Directory Server: Specify Instance Creation Information**

Instance Directory:

Directory Instance Port:

Directory Instance SSL Port:

Directory Manager DN:

System User:

System Group:

Directory Manager Password:  At least 8 character

Retype Password:

Suffix:

13. In the “Ready to Install” screen, click **Install** and wait for the installation to complete.

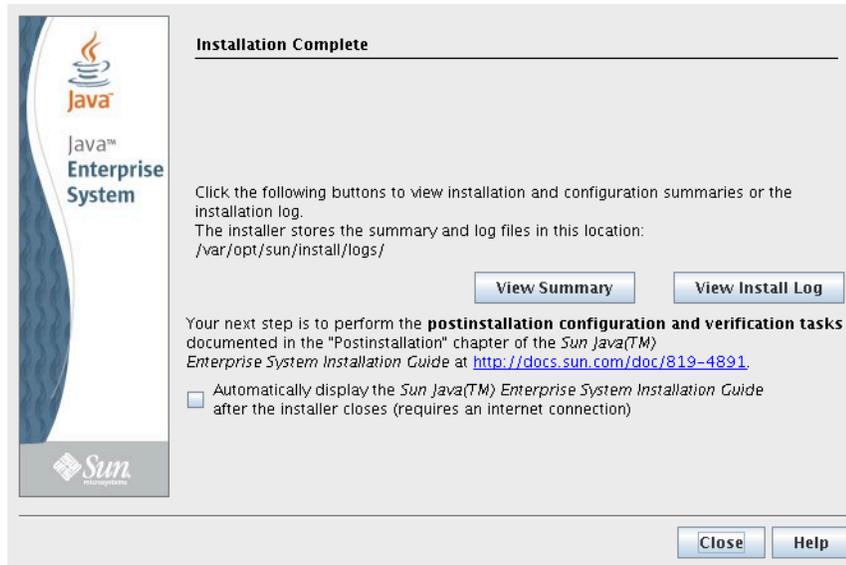
**Ready to Install**

Product: Java Enterprise System 5  
 Uninstall Location: /var/sadm/prod/sun-entsys5  
 Space Required: 209.44 MB

-----

Sun Java(TM) System Directory Preparation Tool  
 Sun Java(TM) System Directory Server Enterprise Edition 6.0  
 Sun Java(TM) System Directory Server Enterprise Edition 6 Command-Line Utilities  
 Java Enterprise System Directory Server 6 Core Server  
 Java Enterprise System Directory Service Control Center  
 Java Enterprise System Directory Proxy Server 6 Core Server

14. In the “Installation Complete” screen, click **Close**.



15. Continue to the next section, “[Post-Installation Steps](#),” to complete the installation.

## Post-Installation Steps

Complete your Directory Server installation by performing the steps in this section. You must perform these steps **before** you run the Content Server LDAP integration program.

1. Start your new Directory Server instance:

```
/opt/sun/ds6/bin/dsadm start <instance_dir>
```

2. Create an LDIF file named `csldap.ldif` with the following contents:

```
dn: dc=vm,dc=fatwire,dc=com
objectClass: dcObject
objectClass: organization
dc: vm
description: Directory Server ldif file
o: Fatwire Software
```

```
dn: ou=People,dc=vm,dc=fatwire,dc=com
objectClass: organizationalUnit
objectClass: top
ou: People
```

```
dn: ou=Groups,dc=vm,dc=fatwire,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Groups
```

3. Change to the `<dirserv_home>/ds6/bin` directory.

4. Import the LDIF file you created in [step 2 on page 114](#) using the following command:

```
./dsconf import <ldif_file> <dn>
```

where:

- <ldif\_file> is the full path to the `csldap.ldif` file you created in [step 2 on page 114](#), including the filename, and
- <dn> is the value you entered in the **Suffix** field in [step 12 on page 113](#).

For example:

```
./dsconf import /u01/csldap.ldif dc=vm,dc=fatwire,dc=com
```

When you run the command, accept the certificate by answering **Yes** at the first prompt. At the second prompt, enter the Directory Manager password (you created this password in [step 12 on page 113](#).)

## Completing and Verifying the LDAP Configuration

This section shows you how to complete and verify your LDAP configuration using the Directory Service Control Center (used to manage Sun Directory Server.)

1. Start the Sun Java Web Console:

```
/opt/sun/webconsole/bin/smcwebserver start
```

2. Initialize the Directory Service Control Center:

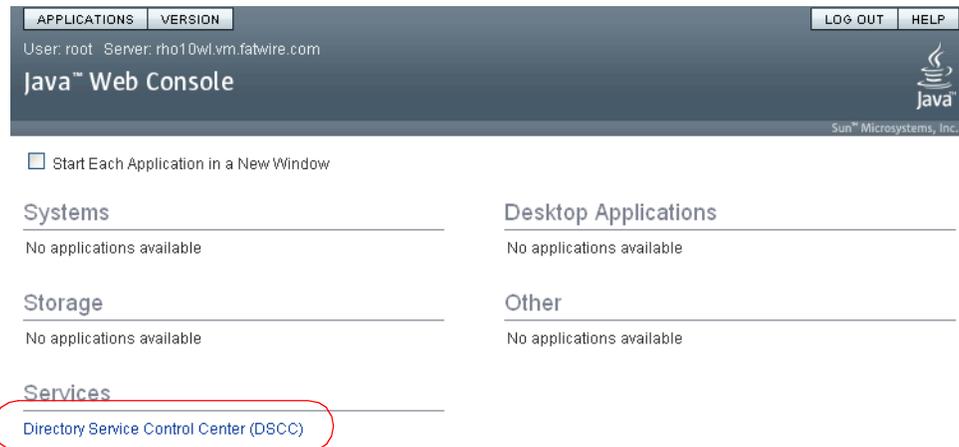
- a. Change to the `<dirserv_home>/dsc6/bin` directory.
- b. Execute the following command: `./dsc6setup initialize`

3. Log in to the Sun Java Web Console as the system user you used to install Sun Directory Server, via the following URL:

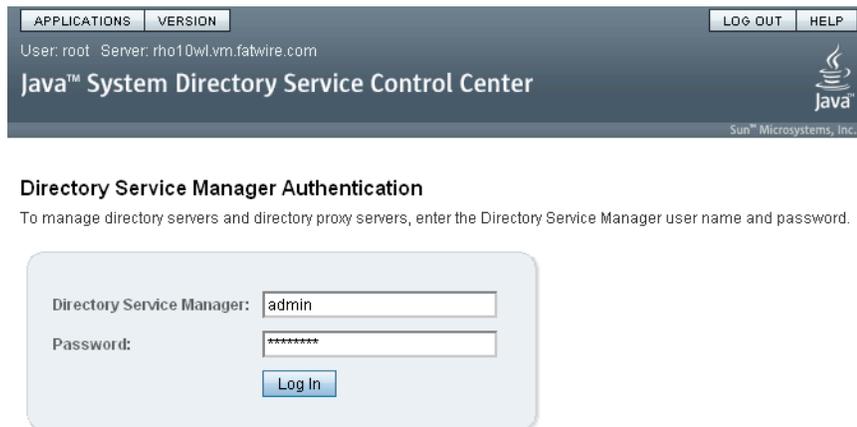
```
https://<server>:6789/
```



4. In the “Services” section, click **Directory Service Control Center (DSCC)**.



5. In the “Directory Service Manager Authentication” screen, log in as the admin user, using the Directory Manager password. (You created this password in [step 12](#) on [page 113](#).)



6. If you see a pop-up error message informing you that the DSCC registry is not running, click **Start DSCC Registry**.



When the DSCC registry has started successfully, a confirmation message appears. Click **Close** to close the pop-up window.

7. In the console, click the **Directory Servers** tab.



8. In the “More Server Actions” drop-down list, select **Register Existing Server**.



### Directory Servers

To manage a server, click a server name. If a server does not appear in the list below, select Register Existing Server from the drop-down menu. >> [More on this table](#)



9. In the pop-up window that appears, enter the full path to the directory holding the target Directory Server instance (<instance\_dir>) and click **Next**.

The screenshot shows the 'Register Existing Directory Server' wizard in the Java System Directory Service Control Center. The title bar reads 'Java™ System Directory Service Control Center'. Below the title bar, the main heading is 'Register Existing Directory Server'. The wizard is currently on 'Step 1: Enter Host and Server Information'. The left sidebar shows three steps: '1. Enter Host and Server Information' (selected), '2. Provide Authentication Information', and '3. Summary'. The main content area contains the following fields and options:

- Host:** A radio button for 'Known Host' is selected, with a dropdown menu showing 'rho10wl.vm.fatwire.com'. A radio button for 'New Host' is unselected, with an empty text field.
- Instance Path:** A text field containing '/u01/software/Apps/sun/dsins1'.
- DSCC Agent Port:** A radio button for 'Default (11162)' is selected, with a radio button for 'Other:' and an empty text field.
- Description:** An empty text field.

A warning icon and text state: 'When this wizard completes, the server will be started, or restarted if it is already running.' At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

10. In the “Review Server Certificate” screen, select the **Accept the Certificate** check box and click **Next**.

The screenshot shows the 'Review Server Certificate' screen of the 'Register Existing Directory Server' wizard. The title bar reads 'Java™ System Directory Service Control Center'. Below the title bar, the main heading is 'Register Existing Directory Server'. The wizard is currently on 'Step 1.1: Review Server Certificate'. The left sidebar shows three steps: '1. Enter Host and Server Information', '1.1 Review Server Certificate' (selected), '2. Provide Authentication Information', and '3. Summary'. The main content area contains the following information:

- Issued To:** CN=rho10wl.vm.fatwire.com\_agent
- Issued By:** CN=rho10wl.vm.fatwire.com\_ca
- Valid From:** 3/26/07 10:13 AM
- Expires On:** 3/26/27 10:13 AM

A 'Show Details' button is located below the certificate information. Below that, there is a checked checkbox labeled 'Accept the certificate'. At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

11. In the “Provide Authentication Information” screen, enter the Directory Manager password into the **Password** field and click **Next**.

The screenshot shows the 'Register Existing Directory Server' wizard at Step 2: Provide Authentication Information. The interface includes a sidebar with steps: 1. Enter Host and Server Information, 1.1 Review Server Certificate, 2. Provide Authentication Information (selected), and 3. Summary. The main area contains instructions: 'To enable the Directory Service Control Center to modify the server configuration, you must provide an Administrative User DN with the appropriate permissions on the server, and the password for the User DN.' Below this are fields for Host (rho10wl.vm.fatwire.com), Instance Path (/u01/software/Apps/sun/dsins1), Server LDAP Port (389), and Server LDAP Secure Port (636). Required fields are marked with an asterisk: Administration DN (cn=Directory Manager) and Password (masked with asterisks). Navigation buttons 'Previous', 'Next', and 'Cancel' are at the bottom.

12. In the “Summary” screen, click **Finish** and wait for the instance to restart.

The screenshot shows the 'Register Existing Directory Server' wizard at Step 3: Summary. The sidebar shows steps 1, 1.1, 2, and 3. Summary (selected). The main area contains instructions: 'Review your settings. If they are not correct, go back to previous steps and modify the settings. If the settings are correct, click Finish.' A yellow warning box states: 'Server Will Be Restarted. When you click Finish, the newly registered server will be restarted.' Below this is a 'Your Settings:' section listing: Host (rho10wl.vm.fatwire.com), Instance path (/u01/software/Apps/sun/dsins1), Administration DN (cn=Directory Manager), DSCC Agent port (11162), and Description. A 'Server Details (Discovered):' section lists: Server Owner User ID (root(root)) and Server LDAP Secure Port (389). Navigation buttons 'Previous', 'Finish', and 'Cancel' are at the bottom.

When the instance has restarted successfully, a confirmation message appears. Click **Close** to close the pop-up window.

13. In the list of directory servers, click the Directory Server instance you just registered.



### Directory Servers

To manage a server, click a server name. If a server does not appear in the list below, select Register Existing Server from the drop-down menu. >> [More on this table](#)



14. In the instance summary screen, click the **Entry Management** tab.



### rho10wl.vm.fatwire.com:389

Start Stop... Restart... --More Server Actions--

#### General

Name: rho10wl.vm.fatwire.com:389

Description: [Edit](#)

Instance Path: /var/opt/sun/dsins1/

Location: [Edit](#)

Servers with the same Location are grouped together when viewing replication topology

#### Run Modes and Status

Operational Status: Started

Read/Write Mode: Read/Write  
>> [More on read/write mode](#)

Referral Mode: Disabled

### 15. Examine the displayed LDAP directory data to make sure it is valid.

#### rho10wl.vm.fatwire.com:389 - Browse Data

You can browse LDAP data on this tab. To browse down the Directory Information Tree (DIT), click +. To browse up the DIT, use the View DN drop-down list. To hide the upper levels of the DIT, select a DN and set it as the View DN by clicking Use Selected Entry. To filter entries, use the View Options settings.

View DN:

dc=vm,dc=fatwire,dc=com

- cn=ContainerDefaultTemplateRole
- cn=Deny Write Access
- cn=SunMobileAppABService
- cn=SunMobileAppCalendarService
- cn=SunMobileAppMailService
- cn=SunPortalportal1 DesktopService
- cn=SunPortalportal1 SubscriptionsService
- cn=SunSSOAdapterService
- cn=Top-level Admin Role
- cn=Top-level Help Desk Admin Role
- cn=Top-level Policy Admin Role
- cn=iPlanetAMAuthConfiguration
- cn=iPlanetAMUserService
- cn=ou=People\_dc=vm,dc=fatwire,dc=com
- cn=srapGatewayAccessService
- cn=srapNetFileService
- cn=srapNetletService
- cn=srapProxyletService
- o=CommunitySample
- o=DeveloperSample
- o=EnterpriseSample
- o=Internet
- ou=ClientData
- ou=DSAME Users
- ou=Groups
- ou=People
- ou=WSRPPProducersportal1
- ou=agents
- ou=services

**Selected Entry**

dn: dc=vm,dc=fatwire,dc=com

ACIs: 32

Object Class: sunISManagedOrganization, sunNameSpace, top, sunManagedOrganization, organization, domain

Children: 30

**View Options**

Filter:

Enter a string to be matched or an LDAP filter.

Display:

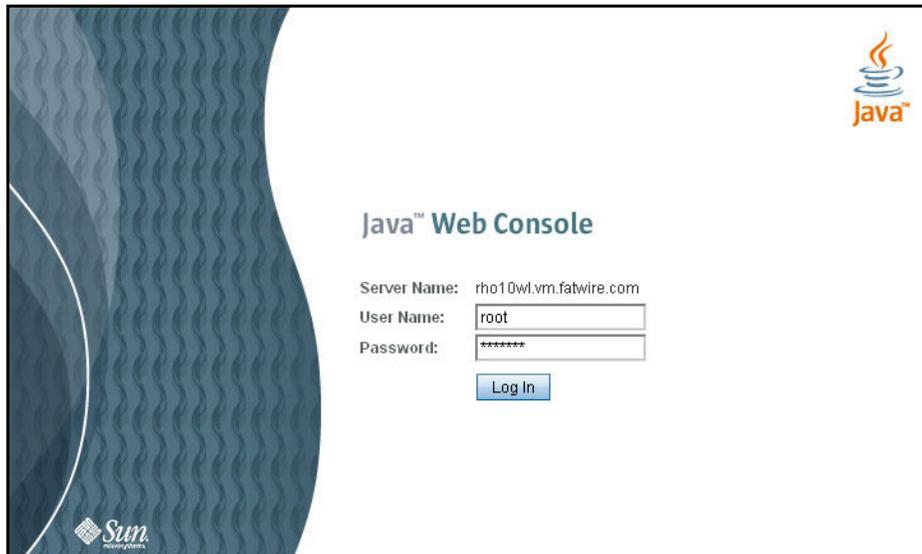
Show Leaf Entries (lowest-level entries)

Show Configuration Suffixes

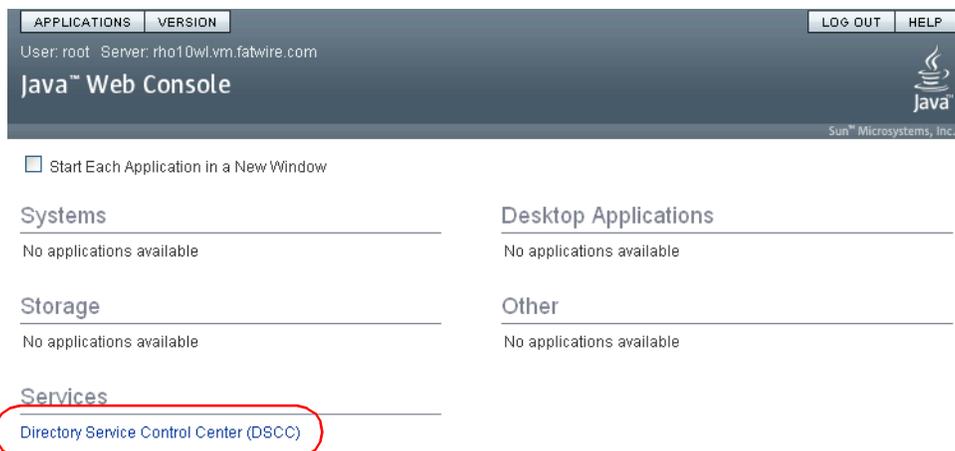
## Modifying User Passwords

This section shows you how to modify user passwords in Sun Directory Server.

1. Start the Sun Java Web Console:  
`/opt/sun/webconsole/bin/smcwebserver start`
2. Log in to the Sun Java Web Console as the system user you used to install Sun Directory Server, via the following URL:  
`https://<server>:6789/`



3. In the “Services” section, click **Directory Service Control Center (DSCC)**.



4. In the “Directory Service Manager Authentication” screen, log in as the `admin` user, using the Directory Manager password. (You created this password in [step 12 on page 113](#).)



#### Directory Service Manager Authentication

To manage directory servers and directory proxy servers, enter the Directory Service Manager user name and password.

The form is titled 'Directory Service Manager Authentication'. It contains two input fields: 'Directory Service Manager:' with the value 'admin' and 'Password:' with '\*\*\*\*\*'. A 'Log In' button is positioned below the password field.

5. If you see a pop-up error message informing you that the DSCC Registry is not running, click **Start DSCC Registry**.



#### DSCC Registry Not Running

The DSCC Registry, which contains configuration data needed by the Directory Service Control Center, is not running. Click Start DSCC Registry to continue.

[Start DSCC Registry](#)

When the DSCC Registry has started successfully, a confirmation message appears. Click **Close** to close the pop-up window.

6. In the console, click the **Directory Servers** tab.

The screenshot shows the Java System Directory Service Control Center interface. At the top, there are tabs for 'APPLICATIONS' and 'VERSION', and buttons for 'REFRESH', 'LOG OUT', and 'HELP'. The user is logged in as 'root' on server 'rho10wl.vm.fatwire.com'. The main navigation bar includes 'Common Tasks', 'Directory Servers' (highlighted with a red circle), 'Proxy Servers', 'Server Groups', and 'Settings'. Below this, there are sections for 'Common Tasks', 'Directory Server Administration', 'Directory Entry Management', 'Proxy Server Administration', and 'Documentation'. Each section contains several buttons for performing specific tasks like 'Manage Registered Directory Servers', 'View Replication Topologies', 'Create New Entry', etc.

7. In the list of directory servers, click the desired Directory Server instance.

This screenshot shows the 'Directory Servers' tab selected in the console. Below the main navigation bar, there are sub-tabs for 'Servers', 'Suffixes', and 'Replication Agreements'. The 'Servers' sub-tab is active, displaying a table of directory servers.

### Directory Servers

To manage a server, click a server name. If a server does not appear in the list below, select Register Existing Server from the drop-down menu. >> [More on this table](#)

The screenshot shows a table titled 'Directory Servers (1)'. The table has the following columns: 'Server', 'Secure Port', 'Operational Status', 'Server Group', 'Description', and 'Instance Path'. The first row is highlighted with a red circle and contains the following data:

| Server                     | Secure Port | Operational Status | Server Group | Description | Instance Path                 |
|----------------------------|-------------|--------------------|--------------|-------------|-------------------------------|
| rho10wl.vm.fatwire.com:389 | 389         | Started            |              |             | /u01/software/Apps/sun/dsins1 |

8. In the instance summary screen, click the **Entry Management** tab.

The screenshot displays the Java System Directory Service Control Center interface. At the top, there are navigation tabs for 'APPLICATIONS' and 'VERSION', and buttons for 'REFRESH', 'LOG OUT', and 'HELP'. The user is logged in as 'root' on the server 'rho10wl.vm.fatwire.com'. The main title is 'Java™ System Directory Service Control Center' with the Sun Microsystems, Inc. logo.

The breadcrumb path is 'Directory Servers > rho10wl.vm.fatwire.com:389'. Below this, there are several tabs: 'Server Operation', 'Suffixes', 'Entry Management' (highlighted with a red circle), 'Schema', 'Security', and 'Server Configuration'. Underneath these are sub-tabs: 'Main', 'Error Logs', 'Access Logs', 'Audit Logs', 'Resource Usage', and 'Suffix Usage'.

The main content area shows the server name 'rho10wl.vm.fatwire.com:389' and a row of buttons: 'Start', 'Stop...', 'Restart...', and '--More Server Actions--' with a dropdown arrow.

The 'General' section contains the following information:

- Name: rho10wl.vm.fatwire.com:389
- Description:
- Instance Path: /var/opt/sun/dsins1/
- Location:   
Servers with the same Location are grouped together when viewing replication topology

The 'Run Modes and Status' section shows:

- Operational Status: Started
- Read/Write Mode: Read/Write  
[>>More on read/write mode](#)
- Referral Mode: Disabled

9. In the list of directory entries, navigate to and double-click the **ou=People** node.



### rho10wl.vm.fatwire.com:389 - Browse Data

You can browse LDAP data on this tab. To browse down the Directory Information Tree (DIT), click +. To browse up the DIT, use the View DN drop-down list. To hide the upper levels of the DIT, select a DN and set it as the View DN by clicking Use Selected Entry. To filter entries, use the View Options settings.

View DN:

- cn=Deny Write Access
- cn=SunMobileAppABService
- cn=SunMobileAppCalendarService
- cn=SunMobileAppMailService
- cn=SunPortalportal1 DesktopService
- cn=SunPortalportal1 SubscriptionsService
- cn=SunSSOAdapterService
- cn=Top-level Admin Role
- cn=Top-level Help Desk Admin Role
- cn=Top-level Policy Admin Role
- cn=iPlanetAMAuthConfiguration
- cn=iPlanetAMUserService
- cn=ou=People\_dc=vm\_dc=fatwire\_dc=com
- cn=srapGatewayAccessService
- cn=srapNetFileService
- cn=srapNetletService
- cn=srapProxyletService
- o=CommunitySample
- o=DeveloperSample
- o=EnterpriseSample
- o=Internet
- ou=ClientData
- ou=DSAME Users
- ou=Groups
- ou=People
- ou=WSRPProducersportal1
- ou=agents
- ou=services
- sunPortalAdminPortalDomainID=defaultDomain

**Selected Entry**

dn: ou=People,dc=vm,dc=fatwire,dc=com

ACIs: 0

Object Class: top, organizationalunit, iplanet-am-managed-people-container

Children: 3

**View Options**

Filter:

Enter a string to be matched or an LDAP filter.

Display:

Show Leaf Entries (lowest-level entries)

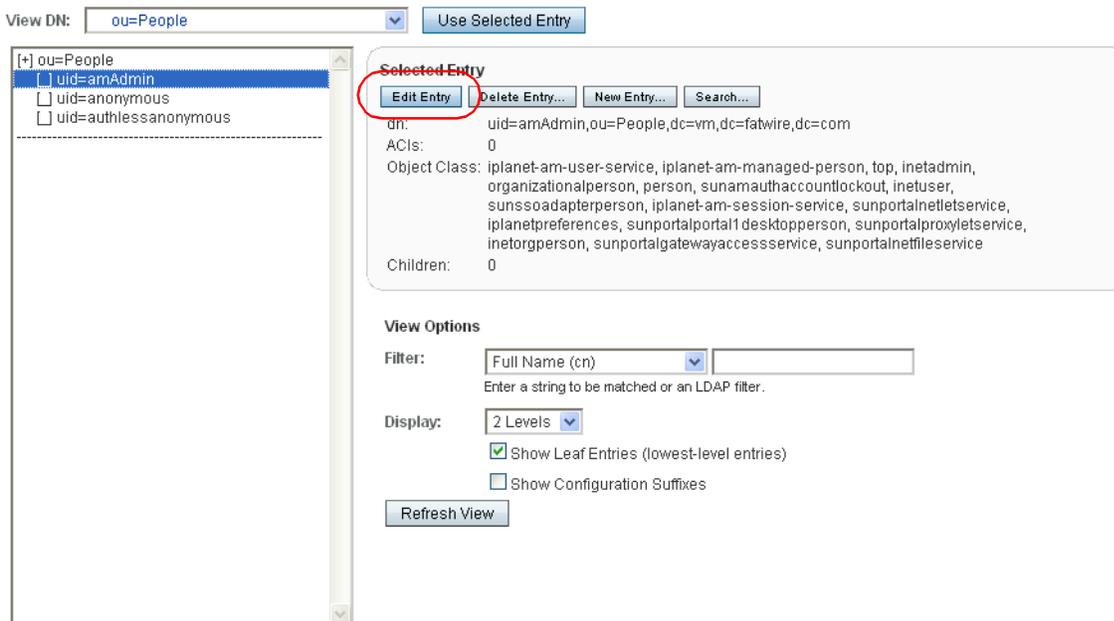
Show Configuration Suffixes

10. Under the **ou=People** node, select the user whose password you want to modify. then click **Edit Entry** in the “Selected Entry” area.



### rho10wl.vm.fatwire.com:389 - Browse Data

You can browse LDAP data on this tab. To browse down the Directory Information Tree (DIT), click +. To browse up the DIT, use the View DN drop-down list. To hide the upper levels of the DIT, select a DN and set it as the View DN by clicking Use Selected Entry. To filter entries, use the View Options settings.



11. Enter the new password into the **Password** and **Confirm Password** fields, then click **OK**.

## rho10wl.vm.fatwire.com:389 - amAdmin - Entry Overview



- ▾ Required Attributes
- ▾ Other
- ▾ Allowed Attributes

\* Indicates required field

## Required Attributes

\* Full Name (cn):

\* Last Name (sn):

[↩ Back to top](#)

## Allowed Attributes

|  |  |
|--|--|
| First Name (givenname):                | <input type="text"/>                   |
| User ID (uid):                         | <input type="text" value="amAdmin"/>   |
| Password (userPassword):               | <input type="password" value="*****"/> |
| Confirm Password:                      | <input type="password" value="*****"/> |
| E-mail (mail):                         | <input type="text"/>                   |
| Telephone Number (telephoneNumber):    | <input type="text"/>                   |
| Fax Number (facsimileTelephoneNumber): | <input type="text"/>                   |
| Locality (l):                          | <input type="text"/>                   |
| Organization (o):                      | <input type="text"/>                   |
| Organizational Unit (ou):              | <input type="text"/>                   |
| aci:                                   | <input type="text"/>                   |
| adminRole:                             | <input type="text"/>                   |
| audio:                                 | <input type="text"/>                   |

12. Repeat [steps 10](#) and [11](#) for each additional user whose password you want to modify.





## Chapter 11

# Setting Up OpenLDAP 2.3.x

This chapter explains how to set up OpenLDAP for use with Content Server.

### Note

You must set OpenLDAP **before** you run the CS LDAP integrator.

It contains the following sections:

- [OpenLDAP Commands](#)
- [Installing OpenLDAP](#)
- [Configuring OpenLDAP](#)
- [Adding Content Server Schema to OpenLDAP](#)
- [Modifying User Passwords](#)

## OpenLDAP Commands

This section contains the most commonly used OpenLDAP commands. Use it as a reference when configuring OpenLDAP for use with Content Server.

### Starting OpenLDAP

#### Note

This section assumes that the `slapd` daemon is located in `/usr/local/libexec`. Depending on your installation, the daemon might be located elsewhere. In such cases, substitute the correct path in the commands listed in this section.

- To start OpenLDAP normally, use the following command:  
`/usr/local/libexec/slapd`
- To start OpenLDAP with full debugging (useful when diagnosing configuration issues and installing Content Server), use the following command:  
`/usr/local/libexec/slapd -h 'ldap:/// ' -d 0x5001`

### Searching an OpenLDAP Server

To search an OpenLDAP Server, do the following:

1. Execute the following command:

```
ldapsearch -x -D "cn=Manager,dc=<domain>,dc=<extension>" -W
  -b '' -s base '(objectClass=*)' namingContexts
```

where `<domain>` and `<extension>` are the values you specified in [step a on page 136](#).

2. When prompted for a password, enter the Root DN user password you specified in [step d on page 137](#).

A typical response from the `ldapsearch` command looks as follows:

```
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <> with scope baseObject
# filter: (objectClass=*)
# requesting: namingContexts
#
#
dn:
namingContexts: dc=fatwire,dc=com
```

```
# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

## Adding an LDIF File to an OpenLDAP Server

To add a well-formed LDIF file to your OpenLDAP Server, use the `ldapadd` command:

```
ldapadd -D 'cn=Manager,dc=<domain>,dc=<extension>'
        -w <root_dn_password> -f <LDIF_file_name>
```

where:

- `<domain>` and `<extension>` are the values you specified in [step a on page 136](#).
- `<root_dn_password>` is the Root DN user password you specified in [step d on page 137](#).
- `<LDIF_file_name>` is the name of the LDIF file you are adding.

## Installing OpenLDAP

This section explains how to install OpenLDAP.

### Note

OpenLDAP is bundled with most Linux distributions. If OpenLDAP is already installed on your system, skip this section.

### To install Open LDAP

1. Download the OpenLDAP `tgz` archive from the OpenLDAP web site:

`http://www.openldap.org/`

For example: `openldap-stable-20070110.tgz`

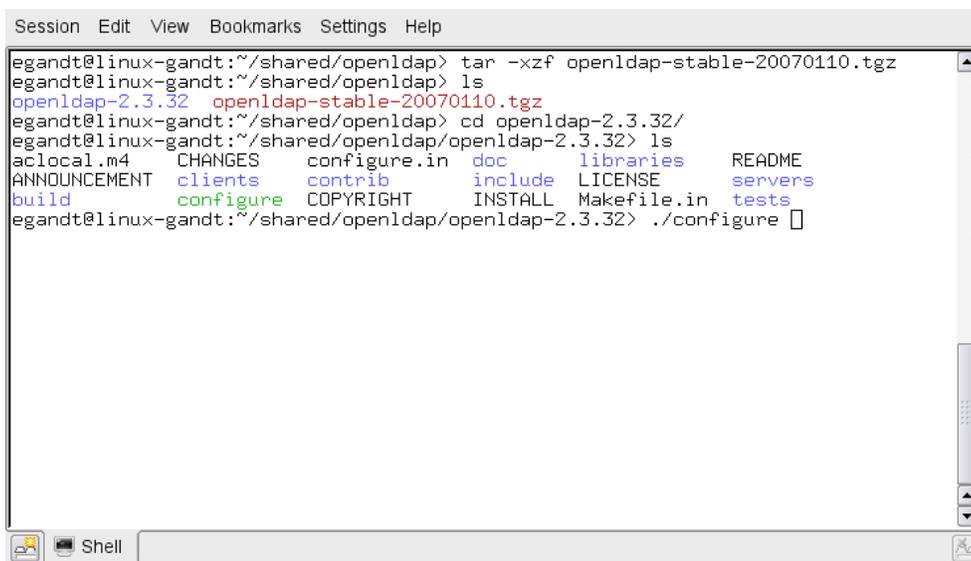
2. Decompress the archive:

- If you are using GNU, use the following command:

```
tar -xvzf openldap-stable-20070110.tgz
```

- If you are not using GNU, use the following command:

```
gzip -d openldap-stable-20070110.tgz ; tar -xvf openldap-stable-20070110.tar
```



```
Session Edit View Bookmarks Settings Help
egandt@linux-gandt:~/shared/openldap> tar -xzf openldap-stable-20070110.tgz
egandt@linux-gandt:~/shared/openldap> ls
openldap-2.3.32  openldap-stable-20070110.tgz
egandt@linux-gandt:~/shared/openldap> cd openldap-2.3.32/
egandt@linux-gandt:~/shared/openldap/openldap-2.3.32> ls
aclocal.m4  CHANGES  configure.in  doc  libraries  README
ANNOUNCEMENT  clients  contrib  include  LICENSE  servers
build  configure  COPYRIGHT  INSTALL  Makefile.in  tests
egandt@linux-gandt:~/shared/openldap/openldap-2.3.32> ./configure []
```

3. Change to the directory containing the OpenLDAP source. For example:

```
cd openldap-2.3.32
```

```

Session Edit View Bookmarks Settings Help
egandt@linux-gandt:~/shared/openldap> tar -xzf openldap-stable-20070110.tgz
egandt@linux-gandt:~/shared/openldap> ls
openldap-2.3.32  openldap-stable-20070110.tgz
egandt@linux-gandt:~/shared/openldap> cd openldap-2.3.32/
egandt@linux-gandt:~/shared/openldap/openldap-2.3.32> ls
acllocal.m4  CHANGES  configure.in  doc  libraries  README
ANNOUNCEMENT  clients  contrib  include  LICENSE  servers
build  configure  COPYRIGHT  INSTALL  Makefile.in  tests
egandt@linux-gandt:~/shared/openldap/openldap-2.3.32> ./configure

```

4. Configure the OpenLDAP source as follows:

```
./configure --enable-crypt --with-tls
```

```

Session Edit View Bookmarks Settings Help
config.status: creating servers/slapd/back-sql/Makefile
config.status: creating servers/slapd/shell-backends/Makefile
config.status: creating servers/slapd/slapi/Makefile
config.status: creating servers/slapd/overlays/Makefile
config.status: creating servers/slurpd/Makefile
config.status: creating tests/Makefile
config.status: creating tests/run
config.status: creating tests/progs/Makefile
config.status: creating include/portable.h
config.status: creating include/ldap_features.h
config.status: creating include/lber_types.h
config.status: executing depfiles commands
config.status: executing default commands
Making servers/slapd/backends.c
Add config ...
Add ldif ...
Add bdb ...
Add hdb ...
Add monitor ...
Add relay ...
Making servers/slapd/overlays/statover.c
Add syncprov ...
Please run "make depend" to build dependencies
egandt@linux-gandt:~/shared/openldap/openldap-2.3.32> make dep

```

The suggested options are:

- **--enable-crypt** — enables password encryption
- **--with-tls** — enables TLS/SSL support

#### Note

If you want to customize OpenLDAP for your system, run **./configure --help** for a complete list of configuration options.

5. Compile OpenLDAP dependencies: `make depend`
6. Compile OpenLDAP: `make`
7. Install OpenLDAP: `make install`

#### Note

By default, OpenLDAP is installed in `/usr/local`.

## Configuring OpenLDAP

This section shows you how to configure your OpenLDAP installation.

1. Edit the `ldap.conf` file as follows:

#### Note

If you installed OpenLDAP manually by following the steps in the previous section, `ldap.conf` is located in `/usr/local/etc`.

- a. Specify your Base DN. Locate the following line (or create it if it does not exist):  

```
BASE dc=<domain>,dc=<extension>
```

where `<domain>` and `<extension>` are, respectively, the domain and TLD of your LDAP server.  
The Base DN for OpenLDAP should always be two dc's in length. For example, if your full domain is `vm.fatwire.com`, your Base DN would be `fatwire.com`, and your BASE line would look as follows:  

```
BASE dc=fatwire,dc=com
```
  - b. Specify your URI(s). Locate the following line (or create it if it does not exist):  

```
URI ldap://<hostname_or_IP> ldap://<hostname_or_IP>
```

Enter the host names and/or IP addresses on which on which OpenLDAP is to listen for connections. Separate the entries with spaces. For example:  

```
URI ldap://127.0.0.1 ldap://localhost ldap://172.19.1.2
```
2. Edit the `slapd.conf` file as follows:

#### Note

If you installed OpenLDAP manually by following the steps in the previous section, `slapd.conf` is located in `/usr/local/etc`.

- a. Locate the following section:  

```
access to *  
    by self write  
    by users read
```

and replace it with:

```

access to *
    by dn="cn=Manager,dc=<domain>,dc=<extension>" write
    by self write
    by users read
    by anonymous auth

```

where <domain> and <extension> are the values you specified in [step 1a](#).

- b.** Specify your suffix. Locate the following line (or create it if it does not exist):

```
suffix dc=<domain>,dc=<extension>
```

where <domain> and <extension> are the values you specified in [step 1a](#).

- c.** Specify your Root DN user. (The Root DN user is used to access the LDAP Server.) Locate the following line (or create it if it does not exist):

```
rootdn cn=<user_name>,dc=<domain>,dc=<domain>
```

Enter `Manager` as the user name and replace <domain> and <extension> with the values you specified in [step 1a](#).

- d.** Specify a password for the Root DN user. Locate the following line (or create it if it does not exist):

```
rootpw<password>
```

#### Note

The password can be either encrypted or unencrypted. (Encrypted passwords start with {SSHA}). If you wish to use an encrypted password, do the following:

1. Generate an encrypted password (hash) using the `slappasswd` command. The command generates a valid encrypted password (hash) and prints it to the terminal.
2. Perform [step e](#) below.

- e.** (Optional) If you chose to use an encrypted password in the previous step, set the password type to SHA. Locate the following line (or create it if it does not exist):

```
password-hash {SSHA}
```

This sets the password type to SHA (the default). You can set other password types; see the OpenLDAP documentation for more information.

- 3.** Edit the `core.schema` file as follows:

#### Note

If you installed OpenLDAP manually by following the steps in the previous section, `core.schema` is located in `/usr/local/etc/schema`.

- a.** Locate the following section:

```

objectclass ( 2.5.6.17 NAME 'groupOfUniqueNames'
    DESC 'RFC2256: a group of unique names (DN and Unique Identifier)'
    SUP top STRUCTURAL

```

```
MAY ( businessCategory $ seeAlso $ owner $ ou $ o
      $ description $ uniqueMember) )
MUST ( uniqueMember $ cn )
```

Comment the section out by placing a # character at the beginning of each line. Then insert the following modified section after it:

```
objectclass ( 2.5.6.17 NAME 'groupOfUniqueNames'
              DESC 'RFC2256: a group of unique names (DN and Unique
                    Identifier)'
              SUP top STRUCTURAL
              MAY ( businessCategory $ seeAlso $ owner $ ou $ o
                    $ description $ uniqueMember) )
              MUST ( cn )
```

The difference between the original and modified sections is the last line:

```
MUST ( uniqueMember $ cn ) becomes MUST ( cn )
```

OpenLDAP is now configured.

## Adding Content Server Schema to OpenLDAP

This section shows you how to add Content Server schema to your OpenLDAP server.

### To configure OpenLDAP for Content Server

1. Create an LDIF file named `pre_cs_openldap.ldif` with the following contents:

```
version: 1
dn: dc=<domain>,dc=<extension>
objectClass: dcObject
objectClass: organization
dc: fatwire
description: OpenLDAP pre_cs_setup
o: Fatwire Software

# LDAP Manager Role
dn: cn=Manager,dc=<domain>,dc=<extension>
objectclass: organizationalRole
cn: Manager

# add the organizational Unit People
dn: ou=People,dc=<domain>,dc=<extension>
objectClass: organizationalUnit
objectClass: top
ou: People

# add the organizational Unit Group
dn: ou=Groups,dc=<domain>,dc=<extension>
objectClass: organizationalUnit
objectClass: top
ou: Groups
```

where `<domain>` and `<extension>` are the values you specified in [step a on page 136](#).

The file will create a new organization (`fatwire`) containing two sub-organizations (`Groups` and `People`) and the `Manager` user. The `Manager` user will be used to access the LDAP server.

2. Add the `pre_cs_openldap.ldif` file to your OpenLDAP server. Execute the following command:

```
ldapadd -D 'cn=Manager,dc=<domain>,dc=<extension>'
-w <root_dn_password> -f pre_cs_openldap.ldif
```

where:

- `<domain>` and `<extension>` are the values you specified in [step a on page 136](#).
- `<root_dn_password>` is the Root DN user password you specified in [step d on page 137](#).

3. Test your OpenLDAP server. Execute the following command:

```
ldapsearch -x -b 'ou=Groups,dc=<domain>,dc=<extension>'
 '(objectclass=*)'
```

where <domain> and <extension> are the values you specified in [step a on page 136](#).

An example response from the `ldapsearch` command looks as follows:

```
# extended LDIF
#
# LDAPv3
# base <ou=Groups,dc=fatwire,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# search result
search: 2
result: 0 Success
# numResponses: 1
```

If the `pre_cs_openldap.ldif` file was successfully inserted into the LDAP server, the `result: 0 Success` line indicates success, at which point you are ready to run the Content Server LDAP integrator. For instructions, see the *LDAP Integration Guide*.

## Modifying User Passwords

When you ran the Content Server LDAP integrator, all Content Server users (except `fwadmin`, `ContentServer`, and `DefaultReader`) were assigned the password which you entered in the “Content Server Configuration” screen. For security reasons, you might want to manually assign unique passwords to those users.

### Note

If you chose to use encrypted passwords when you configured OpenLDAP, you **must** change the passwords for all users on your CS system, or your Content Server installation will not function properly. This is because the CS LDAP integrator writes user passwords into OpenLDAP as plaintext, but OpenLDAP expects password hashes.

The following table shows the passwords you must assign to your Content Server users:

| User                              | Password   |
|-----------------------------------|--|
| <code>DefaultReader</code>        | <code>SomeReader</code>                              |
| <code>ContentServer</code>        | The password you supplied during CS installation     |
| <code>fwadmin</code>              | The password you supplied during CS installation     |
| All other users on your CS system | The password you supplied during CS LDAP integration |

This section covers the following methods for changing passwords in OpenLDAP:

- [Modifying User Passwords Using an LDAP Browser](#)
- [Modifying User Passwords Using the `ldapmodify` Command](#)

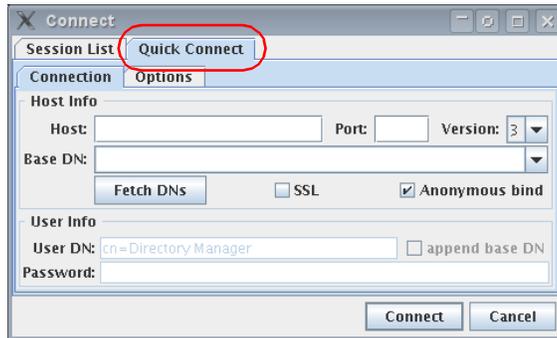
### Modifying User Passwords Using an LDAP Browser

This section shows you how to modify user passwords using the free LDAP Browser/Editor program available at <http://www-unix.mcs.anl.gov/~gawor/ldap/>.

#### To modify user passwords in OpenLDAP using an LDAP browser

1. Download and install the LDAP browser.
2. Start the LDAP browser: `./lbe.sh`

- Click the **Quick Connect** tab.

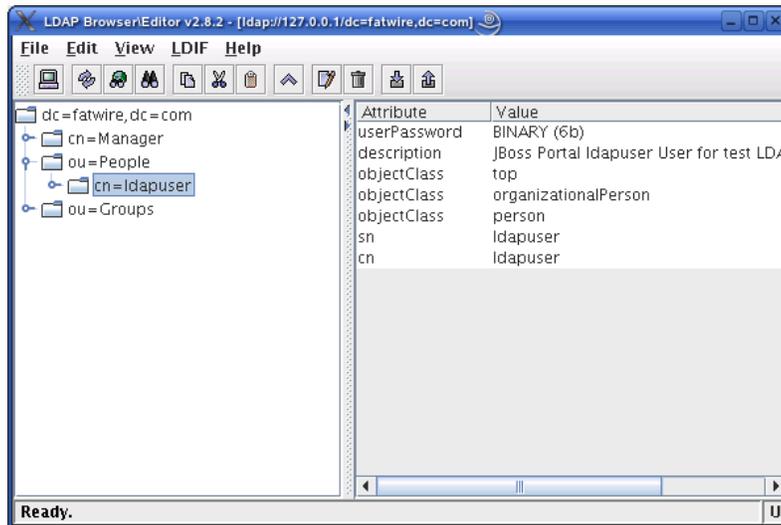


- Fill out the fields as follows:

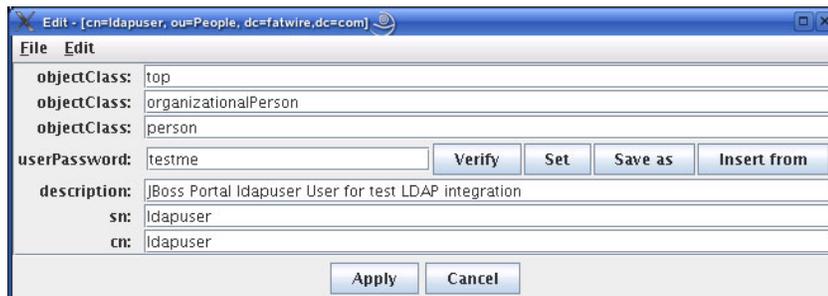
| Field                 | Value   |
|-----------------------|---|
| <b>Hostname</b>       | The host name of your OpenLDAP server.  |
| <b>Port</b>           | <b>389</b>  |
| <b>Version</b>        | <b>3</b>  |
| <b>Base DN</b>        | The Base DN you specified in <a href="#">step a on page 136</a> .               |
| <b>Anonymous bind</b> | <b>Yes</b> (select check box)   |
| <b>User DN</b>        | <b>cn=Manager</b>   |
| <b>Append base DN</b> | <b>Yes</b> (select check box)   |
| <b>Password</b>       | The Root DN user password you specified in <a href="#">step d on page 137</a> . |

- Click **Connect**.

6. In the left-hand tree, expand the **ou=People** node.



7. Double-click the user whose password you want to change and press **Ctrl-E**.  
 8. The plaintext password written by the CS LDAP integrator appears in the **userPassword** field. Click **Set**.

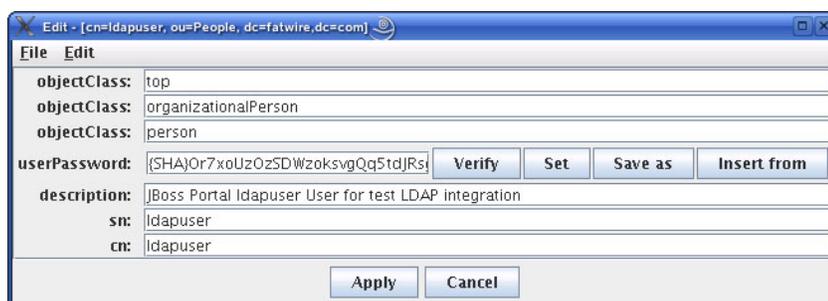


9. In the pop-up window, enter the user's password and click **Set**.



The password appears in its encrypted form.

10. Click **Apply** to save the new password.



- Repeat [steps 7–10](#) for each user whose password you want to change. When you are finished, test your integration by logging in to Content Server.

## Modifying User Passwords Using the `ldapmodify` Command

The `ldapmodify` command provides you with an interface in which you can enter valid LDIF statements to make changes to the configuration of your OpenLDAP server. This section shows you how to use the `ldapmodify` and `sldapasswd` commands to change the passwords of LDAP users.

### To modify user passwords in OpenLDAP using the `ldapmodify` command

- Generate an encrypted password for each user. Run the `sldapasswd` command and enter the plaintext password which you want to encrypt. The command outputs the encrypted password (hash) to the terminal. For example:

```
{SSHA}yDUT5RCpBAU80P0PW8gaHnsmYmL1mUL8
```

#### Note

If you are generating hashes for a large number of users, it is a good idea to store the hashes in a file, so that you can easily retrieve them in [step 3](#). When you finish this procedure, make sure that you destroy the file in which the hashes are stored.

- Execute the `ldapmodify` command as follows:

```
ldapmodify -D 'cn=Manager,dc=<domain>,dc=<extension>'
-w <root_dn_password>
```

where:

- `<domain>` and `<extension>` are the values you specified in [step a on page 136](#).
- `<root_dn_password>` is the Root DN user password you specified in [step d on page 137](#).

When the command returns a blank line, you are ready to input LDIF statements.

- Change the user's password. Issue the following commands:
  - `dn:cn=<user_name>,ou=People,dc=<domain>,dc=<extension>`  
where `user_name` is the user name of the user whose password you want to change, and `<domain>` and `<extension>` are the values you specified in [step a on page 136](#).
  - `changetype:modify`
  - `replace:userPassword`
  - `userpassword:<password_hash>`  
where `<password_hash>` is the hash generated by the `sldapasswd` command in [step 1](#) of this procedure.
  - Press **Ctrl+D**.
  - Repeat [steps a–e](#) for each user whose password you want to change. When you are finished, press **Ctrl+C** to terminate the `ldapmodify` command.

## Chapter 12

# Setting Up the WebLogic 9.x Embedded LDAP Server

This chapter provides instructions on setting up the currently supported WebLogic Embedded LDAP Server for use with Content Server.

### Note

You must set up WebLogic LDAP **before** you run the CS LDAP integrator.

This chapter contains the following sections:

- [Enabling the WebLogic Embedded LDAP Server](#)
- [Modifying User Passwords](#)

## Enabling the WebLogic Embedded LDAP Server

This section explains how to enable the WebLogic Embedded LDAP Server.

### To enable the WebLogic Embedded LDAP Server

1. Log in to the WebLogic Server Administration Console.
2. In the “Domain Structure” tree at the left, click your WebLogic portal domain.
3. Set the Embedded LDAP password:
  - a. In the workspace, select the **Security** tab, then select the **Embedded LDAP** sub-tab.
  - b. In the “Change Center” pane in the upper left, click **Lock & Edit**.
  - c. In the **Credential** field, enter the desired Embedded LDAP password. Reenter the password in the **Confirm Credential** field for verification.
  - d. Click **Save**.

The screenshot displays the WebLogic Server Administration Console interface. The top navigation bar includes the BEA logo, the text "WEBLOGIC SERVER ADMINISTRATION CONSOLE", and a "Welcome, weblogic" message. The left sidebar contains a "Change Center" with a "Lock & Edit" button, a "Domain Structure" tree with "portalDomain" selected, and a "System Status" section showing "Health of Running Servers" with "OK (1)" status. The main workspace shows the "Settings for portalDomain" page, with the "Embedded LDAP" sub-tab selected. The configuration fields are as follows:

| Field                       | Value                               | Description  |
|-----------------------------|-------------------------------------|--|
| Credential:                 | [Redacted]                          | The credential (usually a password) used to connect to the embedded LDAP server. <a href="#">More Info...</a>  |
| Confirm Credential:         | [Redacted]                          | Enter the credential again. <a href="#">More Info...</a>   |
| Backup Hour:                | 23                                  | The hour at which the embedded LDAP server should be backed up. <a href="#">More Info...</a>   |
| Backup Minute:              | 5                                   | The minute at which the embedded LDAP server should be backed up. <a href="#">More Info...</a>   |
| Backup Copies:              | 7                                   | The maximum number of backup copies that should be made for the embedded LDAP server. <a href="#">More Info...</a>   |
| Cache Enabled:              | <input checked="" type="checkbox"/> | Specifies whether a cache is used with the embedded LDAP server. <a href="#">More Info...</a>  |
| Cache Size:                 | 32                                  | The size of the cache (in kilobytes) that is used with the embedded LDAP server. <a href="#">More Info...</a>  |
| Cache TTL:                  | 60                                  | The time-to-live of the cache (in seconds) that is used with the embedded LDAP server. <a href="#">More Info...</a>  |
| Refresh Replica At Startup: | <input type="checkbox"/>            | Specifies whether a Managed Server should refresh all replicated data at boot time. (This is useful if you have made a large amount of changes when the Managed Server was not active, and you want to download the entire replica instead of having the Administration Server push each change to the Managed Server.) <a href="#">More Info...</a> |
| Master First:               | <input type="checkbox"/>            | Specifies whether a Managed Server should always connect to the master LDAP server (contained in the Administration Server), instead of connecting to the local replicated LDAP server (contained in the Managed Server). <a href="#">More Info...</a>   |

4. Create an Embedded LDAP authentication provider:
  - a. In the “Domain Structure” tree, click **Security Realms**.
  - b. In the workspace, click **myrealm** and select the **Providers** tab.

The screenshot shows the WebLogic Server Administration Console interface. The main content area is titled "Settings for myrealm" and has several tabs: Configuration, Users and Groups, Roles and Policies, Credential Mappings, Providers (selected), and Migration. Under the "Providers" tab, there are sub-tabs for Authentication, Authorization, Adjudication, Role Mapping, Auditing, Credential Mapping, Certification Path, and Keystores. The "Authentication" sub-tab is active, showing a text block explaining authentication providers and a table of existing providers.

**Authentication Providers**

| Name                    | Description  | Version |
|-------------------------|--|---------|
| SQLAuthenticator        | Provider that performs DBMS authentication   | 1.0     |
| WSRPIdentityAsserter    | WSRP 8.1 Compatibility, Identity Asserter Provider   | 1.0     |
| DefaultIdentityAsserter | WebLogic Identity Assertion provider   | 1.0     |
| SAMLIdentityAsserter    | WebLogic SAML Identity Assertion Provider. Supports Security Assertion Markup Language v1.1. | 2.0     |
| SAMLAuthenticator       | WebLogic SAML Authentication Provider.   | 1.0     |

- c. Click **New**.
  - d. In the **Name** field, enter a name for the authentication provider.
  - e. In the “Type” drop-down list, select **DefaultAuthenticator**.
  - f. Click **OK**. The new authentication provider appears in the provider list.
5. In the “Change Center,” Click **Activate Changes**.
6. Stop the admin server.

## Modifying User Passwords

This section shows you how to modify user passwords in WebLogic LDAP Server.

### To modify user passwords in WebLogic LDAP Server

1. Log in to the WebLogic Server Administration Console.
2. In the “Domain Structure” tree, click **Security Realms**.
3. In the workspace, click **myrealm** and select the **Users and Groups** tab.

The screenshot shows the WebLogic Server Administration Console interface. The main content area displays the 'Settings for myrealm' page, specifically the 'Users and Groups' tab. A table lists the configured users in this security realm. The user 'firstsite' is highlighted with a red circle, indicating the user whose password is to be modified.

| Name          | Description | Provider     |
|---------------|-------------|--------------|
| Arthur        |             | LDAPProvider |
| Connie        |             | LDAPProvider |
| Conrad        |             | LDAPProvider |
| ContentServer |             | LDAPProvider |
| DefaultReader |             | LDAPProvider |
| Desiree       |             | LDAPProvider |
| firstsite     |             | LDAPProvider |
| fwadmin       |             | LDAPProvider |
| Mark          |             | LDAPProvider |
| Martha        |             | LDAPProvider |

4. Click the user whose password you want to change.

The workspace displays the “Settings for *user name*” screen:

The screenshot shows the 'Settings for firstsite' interface with the 'General' tab selected. At the top, there are three tabs: 'General', 'Passwords', and 'Groups'. Below the tabs is a 'Save' button. The main content area contains the instruction: 'Use this page to change the description for the selected user.' Below this, there are two rows of information. The first row is labeled 'Name:' and shows the value 'firstsite' with a description: 'The login name of this user. [More Info...](#)'. The second row is labeled 'Description:' and has an empty text input field with a description: 'A short description of this user. For example, the user's full name. [More Info...](#)'. At the bottom of the form is another 'Save' button.

5. Select the **Passwords** tab and enter the new password into both fields.

The screenshot shows the 'Settings for firstsite' interface with the 'Passwords' tab selected. At the top, there are three tabs: 'General', 'Passwords', and 'Groups'. Below the tabs is a 'Save' button. The main content area contains the instruction: 'Use this page to change a user's password.' Below this, there are two rows of information. The first row is labeled 'New Password:' and has a text input field containing '\*\*\*\*\*' with a description: 'The new password of this user. [More Info...](#)'. The second row is labeled 'Confirm New Password:' and has a text input field containing '\*\*\*\*\*' with a description: 'The confirmed new password of this user. [More Info...](#)'. At the bottom of the form is another 'Save' button.

6. Click **Save**.

A confirmation message appears.

The screenshot shows a 'Messages' section with a green checkmark icon and the text: 'Settings updated successfully.'



## Chapter 13

# Setting Up Oracle Directory Server 10.x

This chapter provides instructions for setting up the currently supported version of Oracle Directory Server (ODS) for use with Content Server.

### Note

You must set up ODS **before** you run the CS LDAP integrator.

This chapter contains the following sections:

- [Start/Stop Commands](#)
- [Installing Oracle Directory Server](#)
- [Accessing Oracle Directory Manager](#)
- [Configuring ODS Password Security for Content Server](#)
- [Modifying User Passwords](#)
- [Deleting Users](#)
- [Connecting to ODS Using an LDAP Browser](#)

## Start/Stop Commands

This section lists commands for starting and stopping Oracle Directory Server.

- To start:  
`<oracle_home>/opmn/bin/opmnctl startproc ias-component=OID`
- To stop:  
`<oracle_home>/opmn/bin/opmnctl stopproc ias-component=OID`

## Installing Oracle Directory Server

This section shows you how to install Oracle Directory Server for use with Content Server.

### A. Pre-Installation Steps

Complete these steps before installing Oracle Directory Server.

1. Download the following packages from Oracle's website:
  - Oracle Identity Management Infrastructure
  - Oracle Identity Federation
2. Create a temporary directory and decompress the installation packages to this directory using the following command:  
`cpio idmv < <cpio_file>`  
where `<cpio_file>` is the name of the package you want to decompress.
3. Create a new user account to run Oracle Directory Server (named `oracledir` in our example).

#### Note

If you have previously created a user to run Oracle applications on your system, skip this step. In such case, whenever the steps in the remainder of this chapter prompt you to provide the user name of your Oracle user, you must use your existing Oracle user.

- a. Create an Oracle group:  
`groupadd oracledir`
- b. Create an Oracle user:  
`useradd -g oracledir -m -h <user_home_dir> oracledir`  
where `<user_home_dir>` is the Oracle user's home directory.
- c. Set a password for the Oracle user:  
`passwd oracledir`

4. If you are installing on Linux, do the following (otherwise, skip this step):
  - a. Add the following lines to the file `/etc/sysctl.conf`:

```
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
kernel.msgmnb=65535
kernel.msgmni=2878
kernel.sem = 256 32000 100 142
fs.file-max=131072
net.ipv4.ip_local_port_range = 1024 65000
net.core.rmem_default=262144
net.core.wmem_default=262144
net.core.rmem_max=262144
net.core.wmem_max=262144
```
  - b. Run the following command: **`sysctl -p`**
  - c. Add the following lines to `/etc/security/limits.conf`:

```
oracledir soft nproc 2047
oracledir hard nproc 16384
oracledir soft nofile 1024
oracledir hard nofile 65536
```
5. Log in as the Oracle user.

## B. Install Oracle Directory Server

1. Complete the pre-installation steps listed in “[A. Pre-Installation Steps](#),” on page 152 if you have not already done so.
2. Change to the temporary directory into which you decompressed the Oracle Directory Server packages. Within the temporary directory, change to the `Disk1` subdirectory.
3. Start the installer: `./runInstaller`
4. In the “Welcome” screen, click **Next**.



Note: 3a. and 3b only occur if no other Oracle Software was previously installed

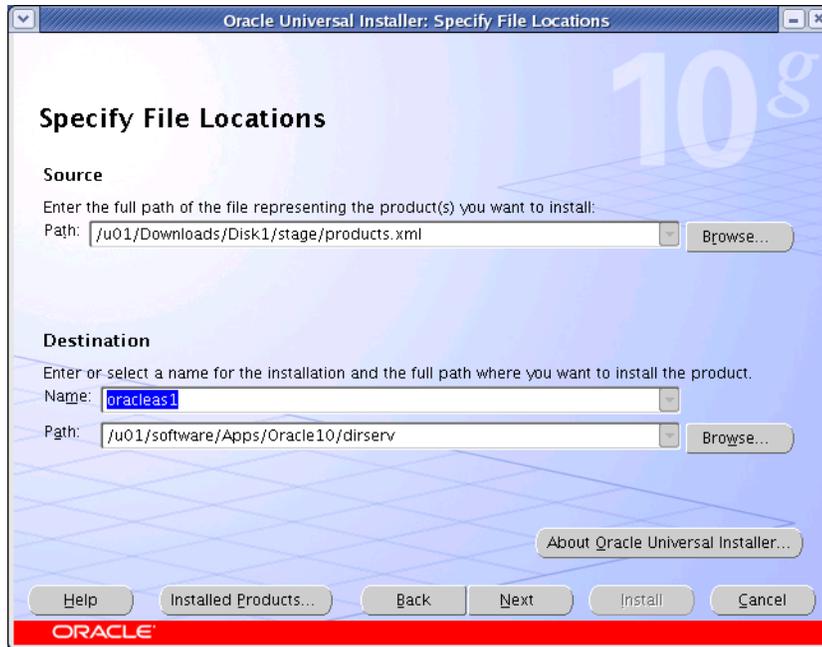
5. If no Oracle products have been installed on this machine, do the following (otherwise, skip this step):
  - a. In the “Specify Inventory Directory and Credentials” screen, specify the location of the Oracle inventory directory and specify the system group of your Oracle user, then Click **Next**.



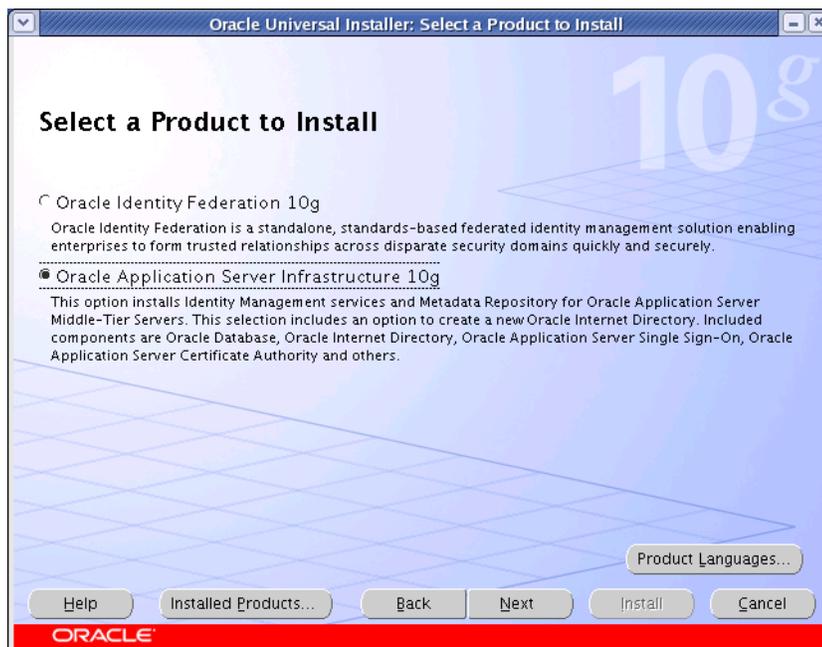
- b. When the following pop-up dialog appears, run the requested script as the `root` user, then click **Continue**.



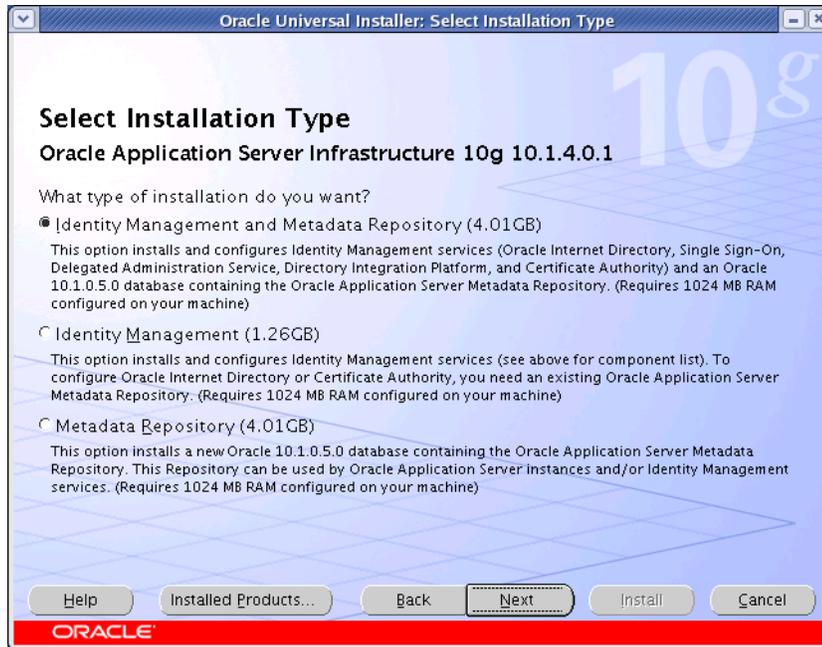
6. In the “Specify File Locations” screen, confirm the path and name of the destination directory, then click **Next**.



7. In the “Select a Product to Install” screen, select the **Oracle Application Server Infrastructure** radio button and click **Next**



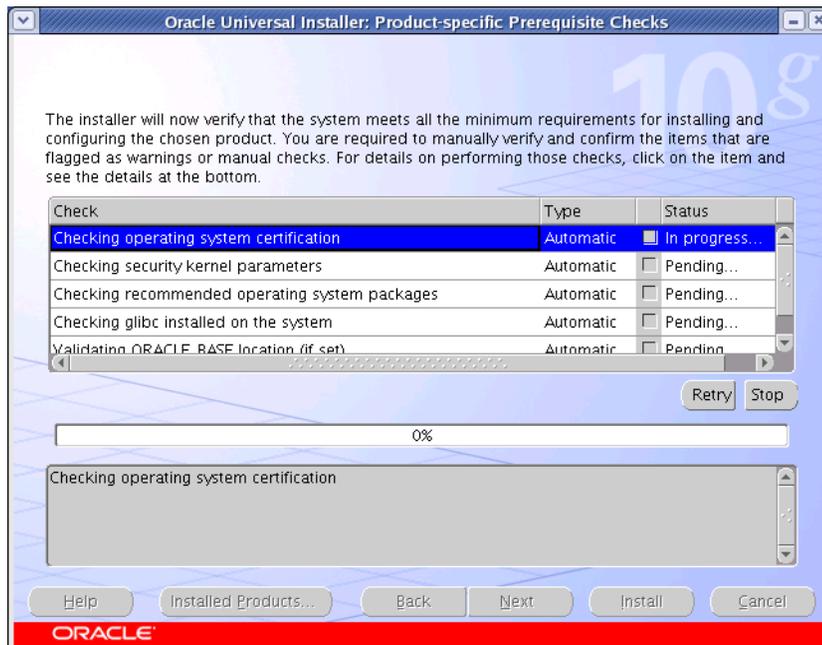
8. In the “Select Installation Type” screen, select the **Identity Management and Metadata Repository** radio button and click **Next**.



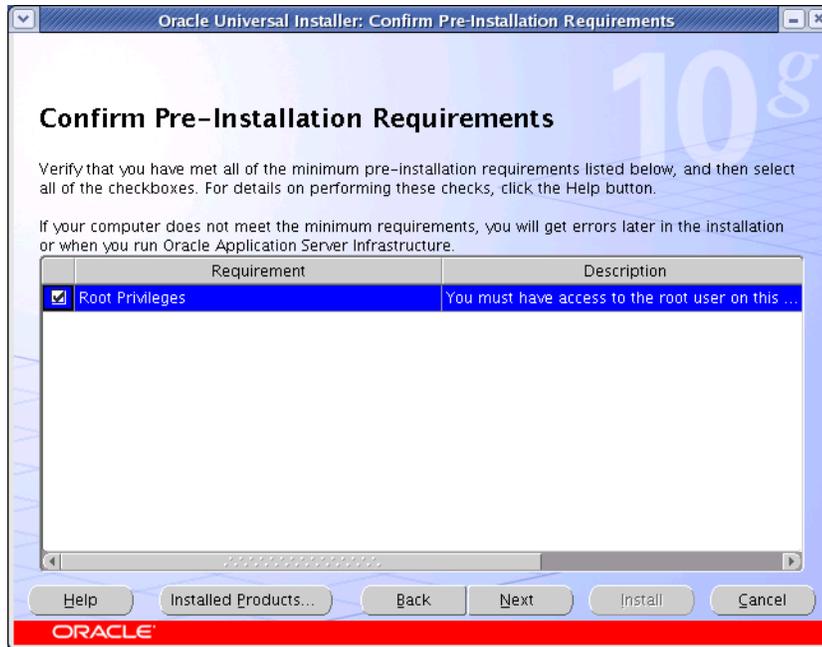
9. In the next screen, allow the prerequisite check to complete. If any checks fail, resolve the issue before continuing. When all checks report as successful, click **Next**.

### Note

If you see a dialog warning you that port 1521 is in use by an Oracle 10.x component, click **OK**. If the dialog reports that an application other than an Oracle 10.x component is using port 1521, you must remedy the situation by following the instructions shown in the dialog before continuing.



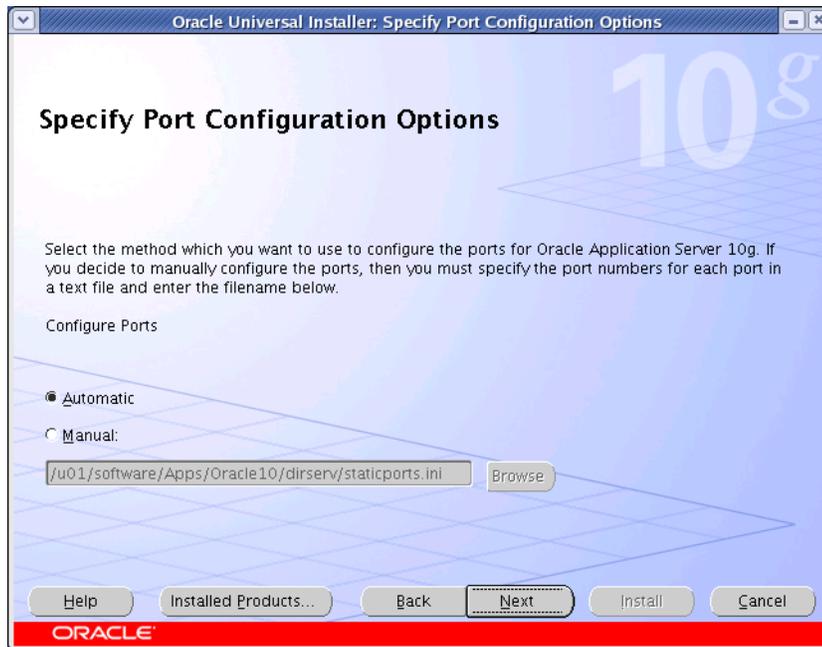
10. In the “Confirm Pre-Installation Requirements” screen, select the check boxes for all items in the list, then click **Next**.



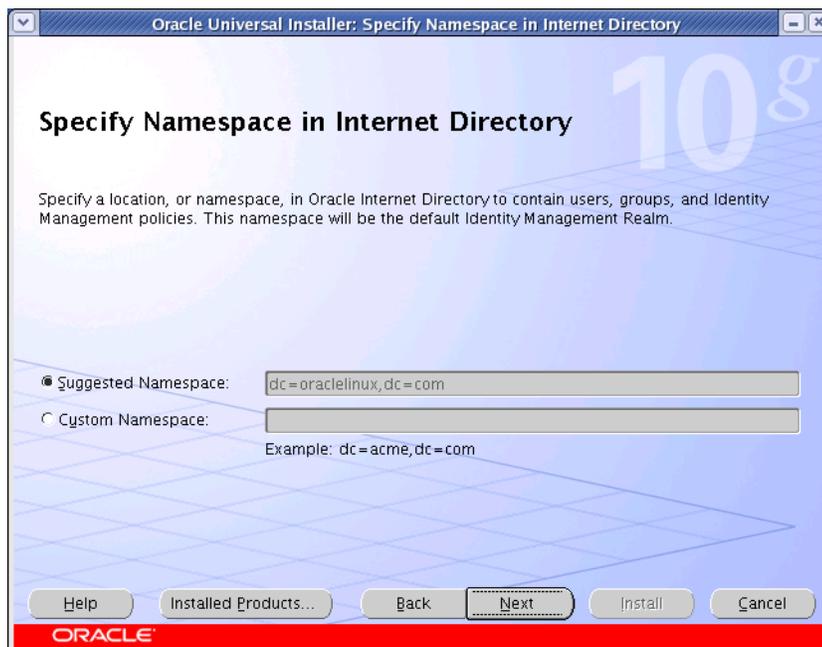
11. In the “Select Configuration Options” screen, click **Next** without making any changes.



12. In the “Specify Port Configuration Options” screen, select **Automatic** and click **Next**.



13. In the “Specify Namespace in Internet Directory” screen, select the **Suggested Namespace** radio button and make a record of the corresponding field value. Click **Next**.



14. In the “Specify Database Configuration Options” screen, enter the required database information, then click **Next**. Make a record of the values you enter.

### Note

If an Oracle database server resides on this machine, the installer will populate the fields in this screen automatically. However, FatWire strongly suggests that you do not use these existing values and instead specify a new, unique SID and database storage (`oradata`) directory.

Oracle Universal Installer: Specify Database Configuration Options

## Specify Database Configuration Options

**Database Naming**  
A Global Database Name, typically of the form "name.domain", uniquely identifies an Oracle database. In addition, each database is referenced by at least one Oracle System Identifier (SID). Specify the Global Database Name and SID for this database.

Global Database Name:  SID:

**Database Character Set**  
The number of language groups to be stored determine which database character set to use. See "Help" for the definition of language groups. For the Unicode database character set, select "Unicode Standard UTF-8 AL32UTF8"

Select Database Character set:

**Database File Location**  
Use the file system for database storage. For best database organization and performance, Oracle recommends installing database files and Oracle software on separate disks.

Specify Database File Location:

ORACLE

15. In the “Specify Database Schema Password” screen, select the **Use the same password for all accounts** radio button, then enter and re-enter the desired password. Make a record of this password, then click **Next**.

**Specify Database Schema Passwords**

The Starter Database contains pre-loaded schemas, most of which have passwords that will expire and be locked at the end of installation. After the installation is complete, you must unlock and set new passwords for those accounts you wish to use. Schemas used for the database management and post-install functions are left unlocked, and passwords for these accounts will not expire. Specify the passwords for these accounts.

Use different passwords for these accounts

| User Name | Enter Password | Confirm Password |
|-----------|----------------|------------------|
| SYS       |                |                  |
| SYSTEM    |                |                  |
| SYSTEM    |                |                  |
| DBSNMP    |                |                  |

Use the same password for all the accounts

Enter Password:  Confirm Password:

Help Installed Products... Back Next Install Cancel

16. In the “Specify Instance Name and ias\_admin password” screen, enter a unique instance name and a unique password. Re-enter the password and make a record of all values in this screen, including the administrator user name (`ias_admin`). When you are finished, click **Next**.

**Specify Instance Name and ias\_admin Password**

All Oracle Application Server Infrastructure instances installed on a host must have unique names. The hostname and domain name of the host are appended to the instance name.

Each Oracle Application Server Infrastructure instance has its own password, regardless of which user performed the installation. Passwords are not shared across instances, even if the instances were installed by the same user.

The password must have a minimum of 5 alphanumeric characters, maximum 30 characters, and at least one of the characters must be a number.

Administrator Username: ias\_admin

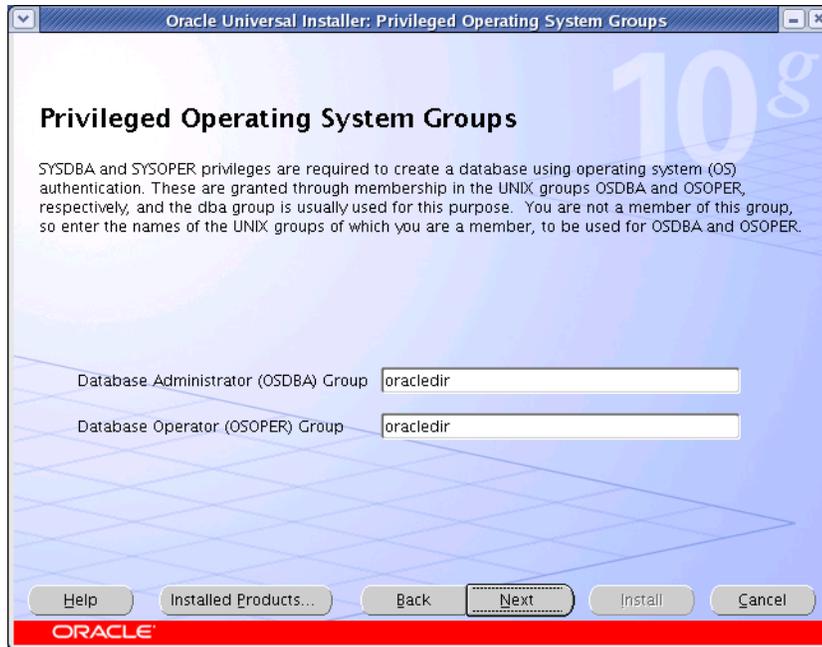
Instance Name:

ias\_admin Password:

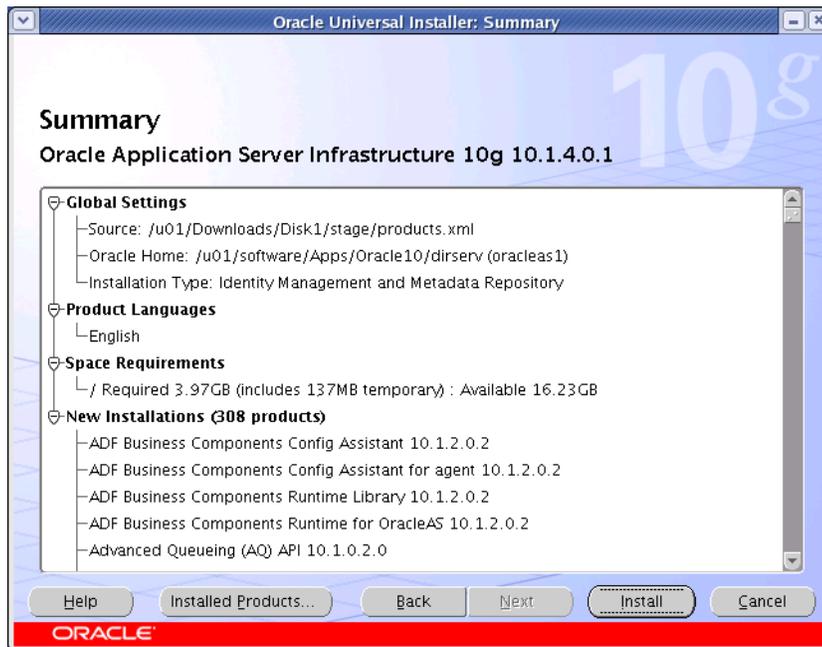
Confirm Password:

Help Installed Products... Back Next Install Cancel

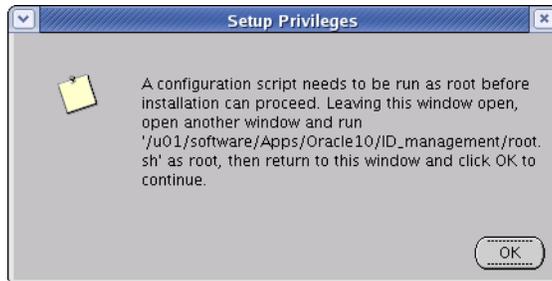
17. In the “Privileged Operating System Groups” screen, keep the default options and click **Next**.



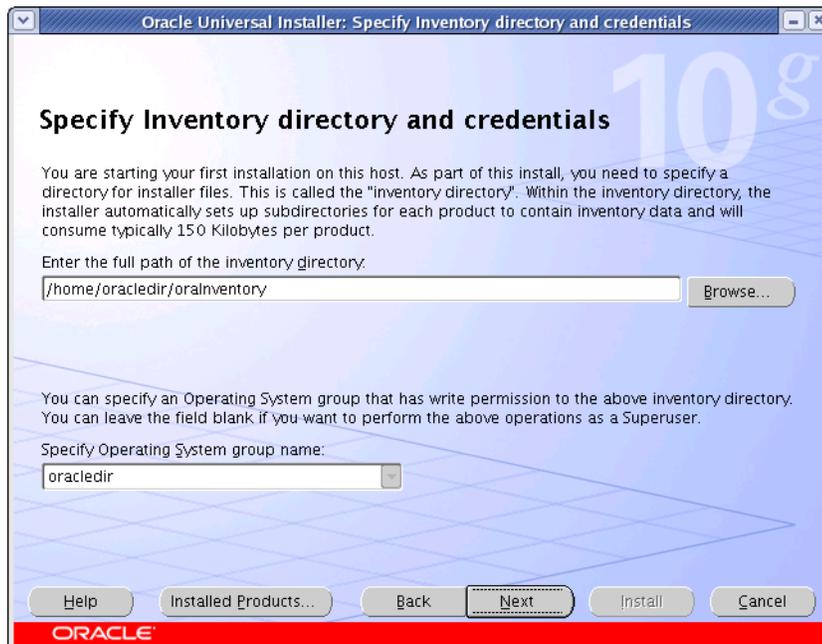
18. In the “Summary” screen, review the configuration choices you have made, then click **Install**. Wait until the installation completes successfully.



19. When the following dialog appears, run the requested script as the `root` user, then click **OK**.



20. In the “Configuration Assistants” screen, allow all configuration steps to complete. If any of the steps fail, correct the indicated problem, then re-run the configuration process. When the configuration process completes successfully, click **Next**.



21. Allow the database configuration to complete.  
22. In the “End of Installation” screen, click **Exit**.

### Note

Make a record of the information displayed in the “Please Remember” dialog box (by copying and pasting it into a text file, for example) for future reference. Additional configuration information for your installation can be found in the file, `<ora_home>/config./ias.properties`. Specifically, look for the string, `OIDport`. This is the port on which Oracle Directory Server is listening for LDAP connections.

## C. Post-Installation Steps

Complete these steps to test your Oracle Directory Server installation.

1. Test the management server:

- a. Log in to the Management Application using the following credentials:

**Note**

By default, the URL is `http://localhost.localdomain:1158/`. The URL for your system is also part of the text file you created in [step 22 on page 164](#).

**User name:** `ias_admin`

**Password:** `<ias_admin_password>` (you created this password in [step 16 on page 162](#))

- b. Log in to the Database Management Application using the following credentials:

**Note**

By default, the URL is `http://localhost.localdomain:5500/em`. The URL for your system is also part of the text file you created in [step 22 on page 164](#).

**User name:** `sys`

**Password:** `<db_schema_password>` (you created this password in [step 15 on page 162](#))

**Connect As:** `SYSDBA`

2. Test the LDAP server:

- a. Change to the `<oracle_home>/bin` directory.

- b. Run the following command:

```
./ldapbind -h localhost -p <OIDport>
```

where `<OIDport>` is the port number you obtained in [step 22 on page 164](#).

Example output:

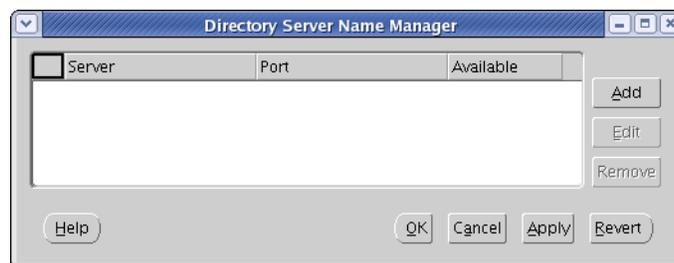
```
bind successful
```

## Accessing Oracle Directory Manager

1. Change to the `<oracle_home>/bin` directory:
2. Run the following command: `./oidadmin`
3. In the “Directory Server Connection” dialog box, click **OK**.



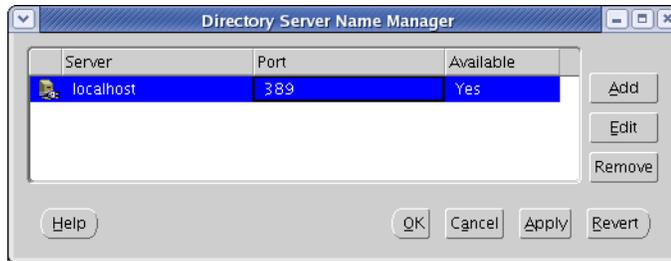
4. Add a connection entry for your Directory Server instance.
  - a. In the “Directory Server Name Manager” screen, click **Add**.



- b. In the “Directory Server Connection” pop-up dialog, enter the following values, then click **OK**.
  - Server: localhost
  - Port: `<OIDport>` (the port number you obtained in [step 22 on page 164](#))



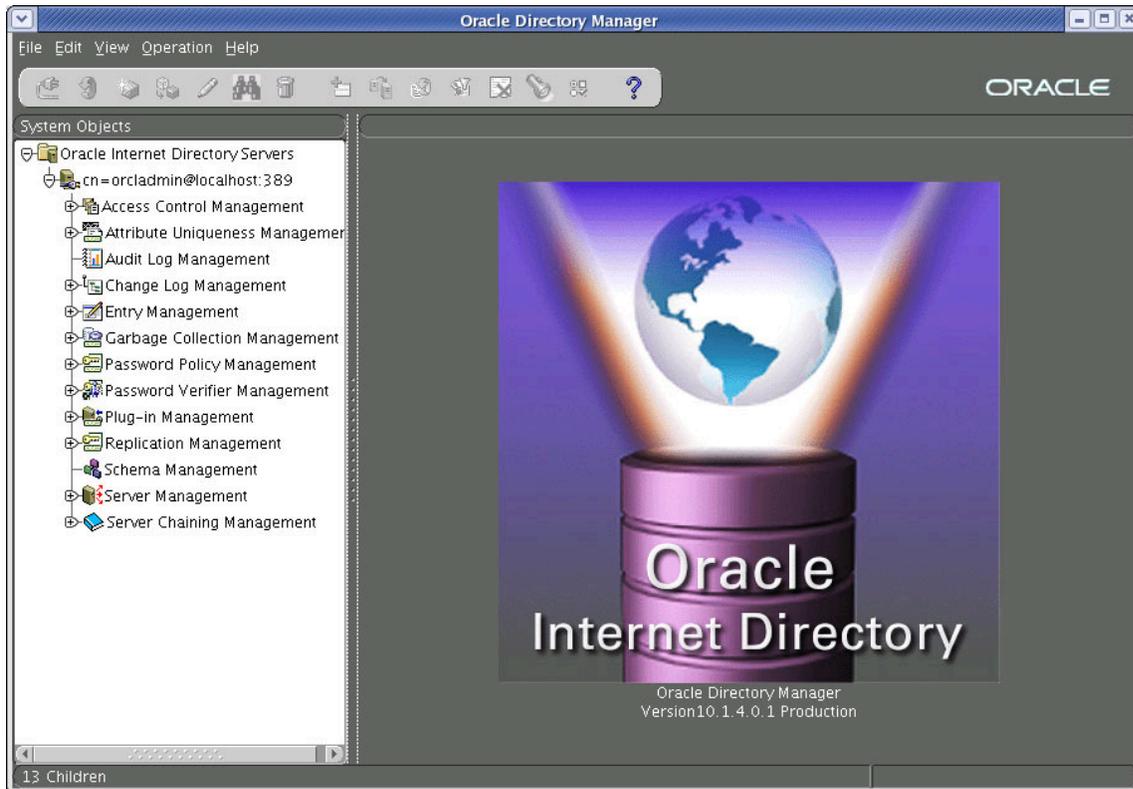
5. In the “Directory Server Name Manager” screen, select the new connection entry and click **OK**.



6. In the **Credentials** tab of the “Oracle Directory Manager Connect” screen, enter the following values:
  - **User:** cn=orcladmin
  - **Password:** <db\_schema\_password> (you created this password in [step 15 on page 162](#))



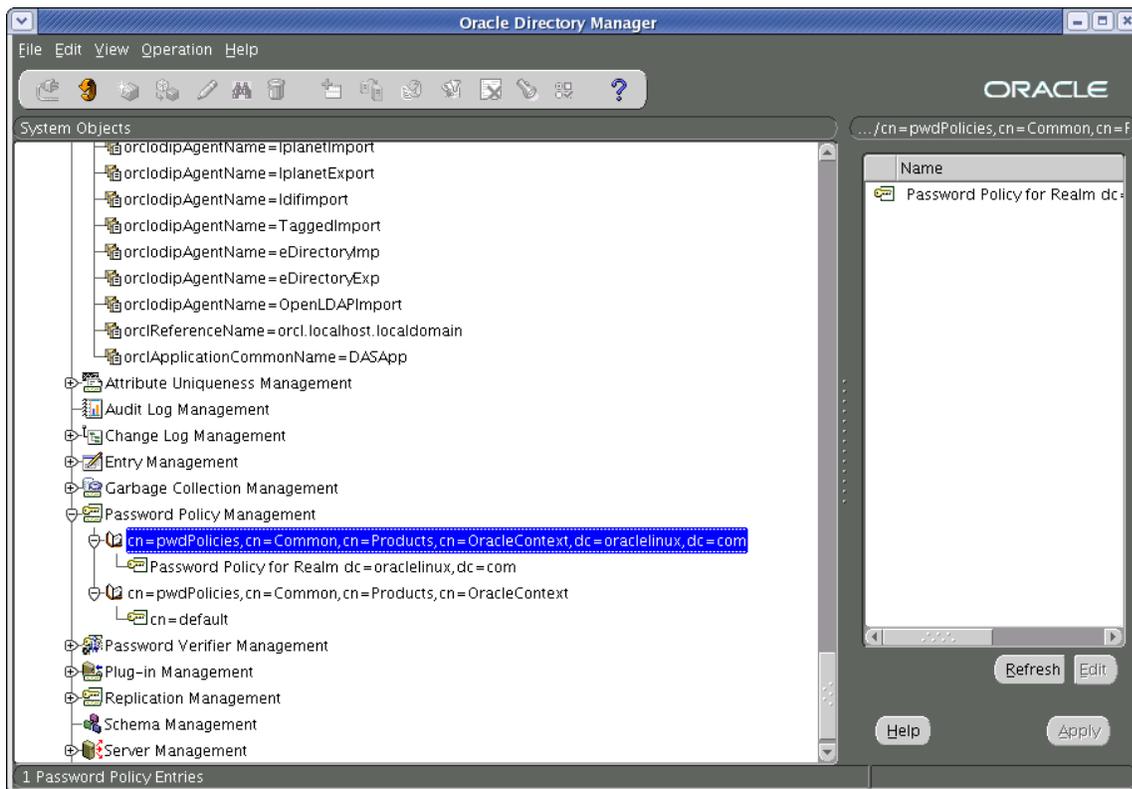
7. Click **Login**. Oracle Directory Manager loads.



## Configuring ODS Password Security for Content Server

This section shows you how to configure password security in Oracle Directory Server to meet Content Server's security requirements.

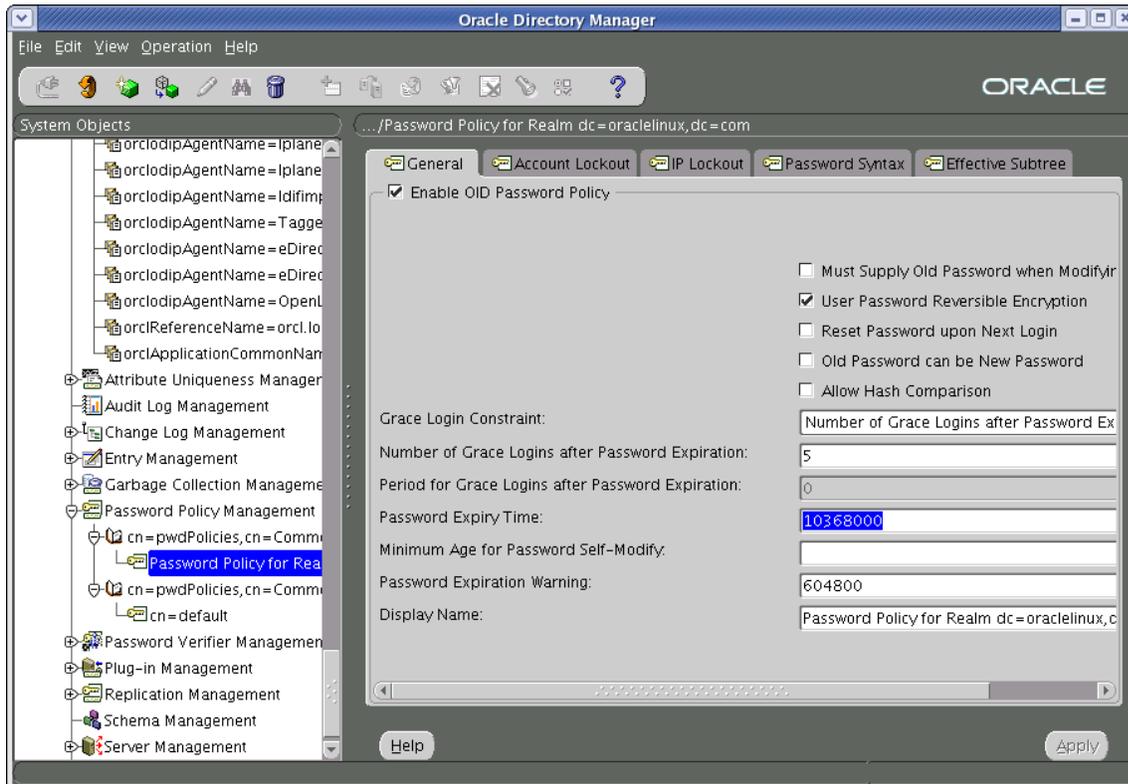
1. Log in to Oracle Directory Manager as `cn=orcladmin`. For instructions, see [“Accessing Oracle Directory Manager,”](#) on page 166.
2. In the tree on the left, expand the **Password Policy Management** node, then the node containing your DN (that is, the namespace you selected in [step 13](#) on page 160):



3. Under the node containing your DN, select the **Password Policy for Realm...** node.

4. Increase the password expiration time from 120 days to 5 years.

In the **General** tab in the main pane, locate the “Password Expire Time” property. The default value of this property, expressed in seconds, is 10368000 (120 days). Change this value to 155520000 (5 years).



5. Select the **Password Syntax** tab.

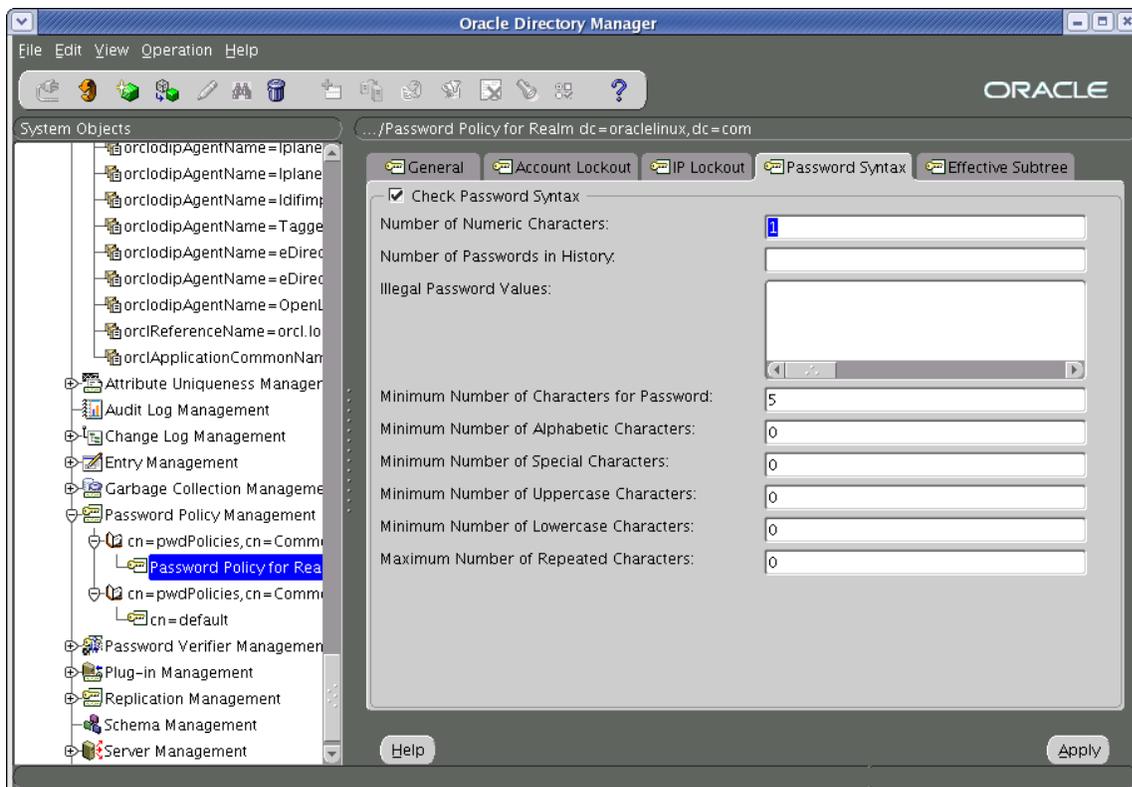
6. Configure password syntax constraints as follows:
  - a. Enable alpha-only passwords (that is, passwords that contain letters, but do not contain digits). You do this by setting the number of required numeric characters to none.

### Note

Default Content Server passwords are alpha-only. If you are using these default passwords on your installation, you **must** enable alpha-only passwords in Oracle Directory Server.

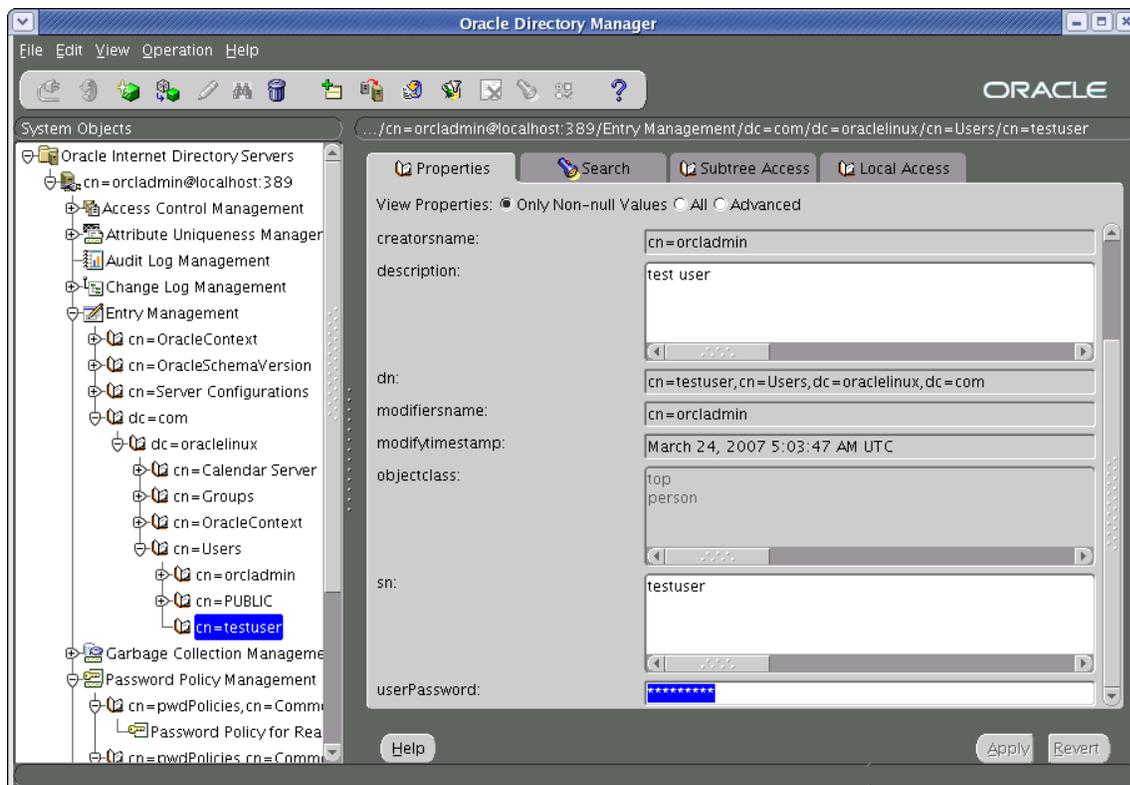
Locate the property named **Number of Numeric Characters** and change its value from 1 (default) to 0.

- b. Reduce the minimum password length to four characters. Locate the property named **Minium Number of Characters for Password** and change its value from 5 (default) to 4.
- c. Click **Apply** to save your changes.



## Modifying User Passwords

1. Log in to Oracle Directory Manager as `cn=orcladmin`. For instructions, see “[Accessing Oracle Directory Manager](#),” on page 166.
2. In the tree on the left, expand the **Password Policy Management** node, then the node containing your DN (that is, the namespace you selected in [step 13 on page 160](#)).
3. Under the node representing your DN, expand the `cn=Users` node and select the user whose password you want to modify.
4. Select the **Properties** tab.
5. In the `userPassword` field, enter the new password.

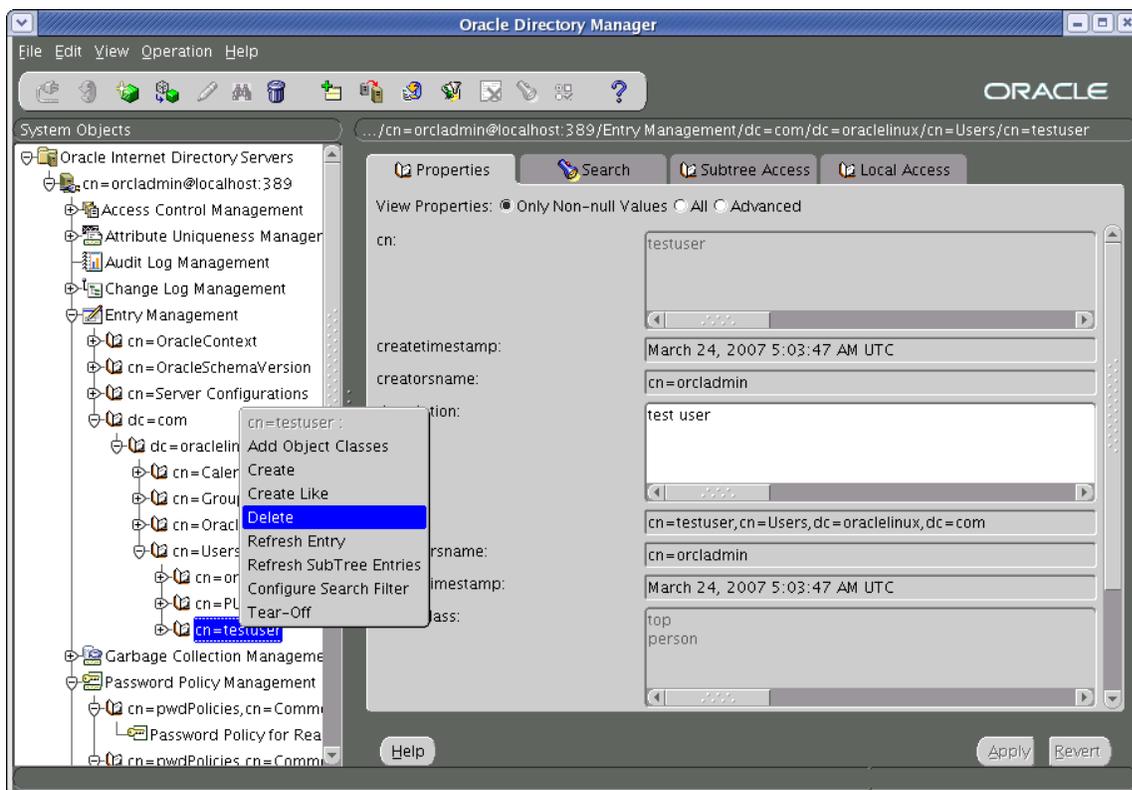


6. Click **Apply** to save your changes.

## Deleting Users

This section shows you how to delete a user in Oracle Directory Server.

1. Log in to Oracle Directory Manager as `cn=orcladmin`. For instructions, see “[Accessing Oracle Directory Manager](#),” on page 166.
2. In the tree on the left, expand the **Password Policy Management** node, then the node containing your DN (that is, the namespace you selected in [step 13 on page 160](#)).
3. Under the node representing your DN, expand the `cn=Users` node and select the user you want to delete.
4. Right-click the selected user and select **Delete** from the context menu.



5. In the confirmation pop-up dialog that appears, click **OK**.

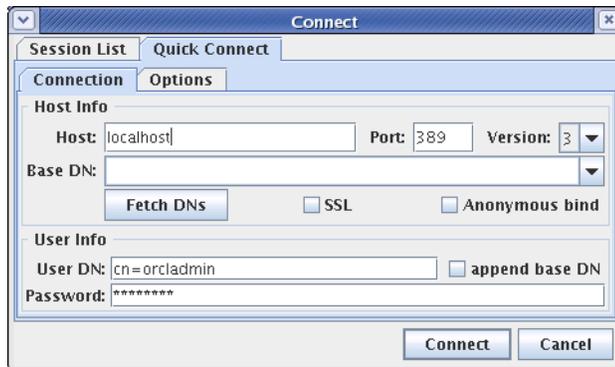
## Connecting to ODS Using an LDAP Browser

This section shows you how to connect to Oracle Directory Server using an LDAP browser.

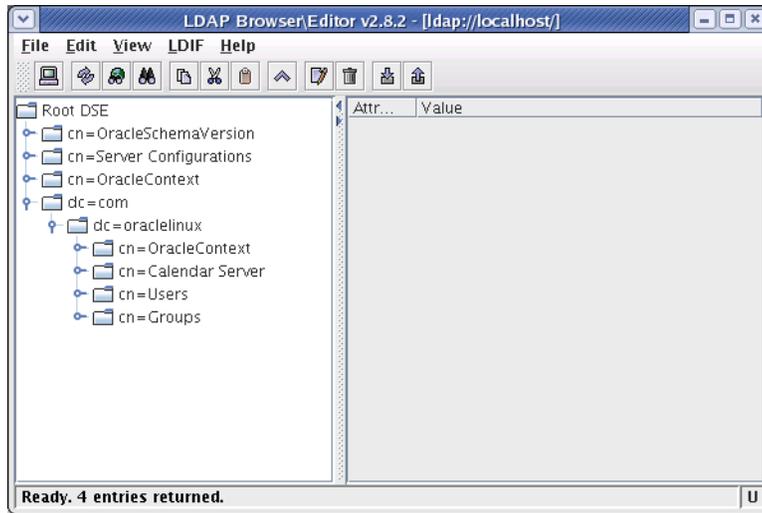
### Note

You cannot add groups, set passwords, or activate accounts using an LDAP browser.

1. Open the LDAP browser.
2. Select the **Quick Connect** tab.
3. Enter the following information:
  - **Host:** localhost (if connecting remotely, enter the actual host name)
  - **Base DN:** leave blank
  - **Anonymous bind:** unchecked
  - **User DN:** cn=orcladmin
  - **Append base DN:** unchecked
  - **Password:** <dbschema\_password> (you created this password in [step 15 on page 162](#))



4. Click **Connect** to start your session.



5. Navigate to your DN (that is, the namespace you selected in [step 13 on page 160](#)).



## Chapter 14

# Setting Up MS Active Directory Server 2003

This chapter provides instructions for setting up the currently supported Microsoft Active Directory Server (ADS) for use with Content Server.

### Note

You must set up ADS **before** you run the CS LDAP integrator.

This chapter contains the following sections:

- [Installing MS Active Directory Server](#)
- [Accessing the “Active Directory Users and Computers” Console](#)
- [Modifying User Passwords](#)
- [Deleting Users](#)
- [Configuring ADS Password Security for Content Server](#)
- [Connecting to ADS Using an LDAP Browser](#)

## Installing MS Active Directory Server

This section shows you how to install MS Active Directory Server 2003 for use with Content Server.

The procedure consists of the following steps:

- A. Install the Operating System
- B. Set the Machine's Name and Suffix
- C. Configure the Machine's Network Settings
- D. Install the Local DNS Server
- E. Configure the Local DNS Server
- F. Install MS Active Directory Server 2003

### A. Install the Operating System

On the target machine, install Windows Server 2003 (any flavor except Web will do).

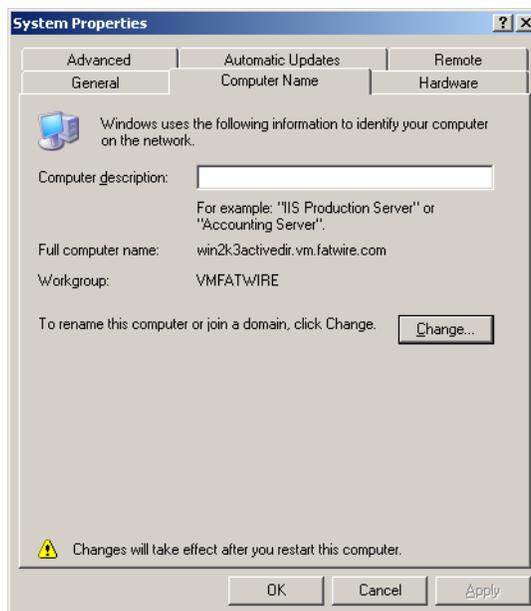
When the installation is complete, leave the installation disc in the drive – you will need it to complete the installation of ADS.

### B. Set the Machine's Name and Suffix

1. Open the “System Properties” dialog.

This can be done in several ways. The fastest way is to right-click the **My Computer** icon on the desktop and select **Properties** from the context menu.

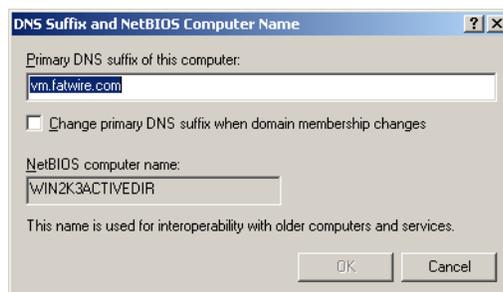
2. Select the **Computer Name** tab.
3. Click **Change**.



4. In the pop-up window that appears, do the following:
  - a. Enter the desired name for this machine. Make a record of this name.
  - b. Select the **Workgroup** radio button and enter a **unique** workgroup name. Make a record of this name.



- c. Click **More**.
  - d. In the second pop-up window that appears, enter the DNS suffix for this machine. Make a record of this suffix.



- e. Make sure the **Change primary DNS suffix when domain membership changes** check box is **not** checked.
  - f. Click **OK** to close the “DNS Suffix and NetBIOS Computer Name” pop-up window.
5. Click **OK** to close the “Computer Name Changes” pop-up window.
6. In the “System Properties” dialog box, click **OK**.
7. Restart the machine.

## C. Configure the Machine's Network Settings

Configure the machine's network settings as follows:

1. Set the IP address to an unused static IP address.
2. Set the preferred DNS server to the machine's IP address.
3. Make sure that the **Append primary and connection-specific DNS suffixes** check box on the **Advanced** tab under **DNS** settings in the **TCP/IP Protocol** properties for the machine's network interface is selected.
4. Make sure that **Append parent suffixes of the primary DNS suffix** check box is selected.

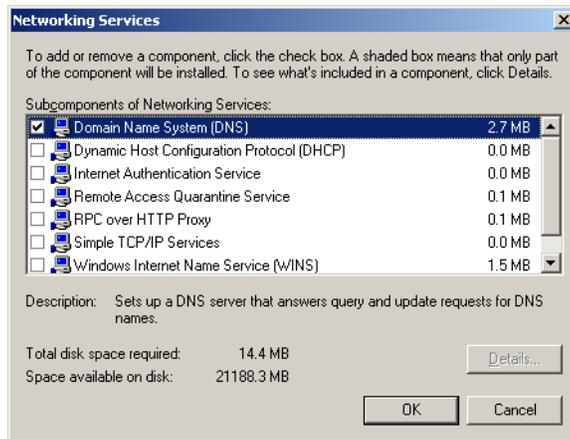
For instructions on configuring your machine's network settings, see the Windows Server 2003 documentation.

## D. Install the Local DNS Server

1. Open the "Control Panel" and double-click **Add and Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. In the "Windows Components Wizard" pop-up window, select the **Networking Services** item (**not** its check box) and click **Details**.



4. In the pop-up window that appears, select the check box next to **Domain Name System (DNS)** and click **OK**. The pop-up window closes.



5. In the "Windows Component Wizard" screen, click **Next**.
6. When the installation completes successfully, click **Finished**.

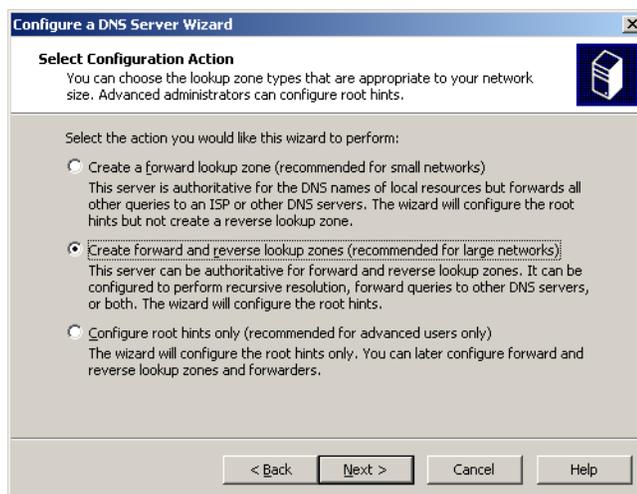


## E. Configure the Local DNS Server

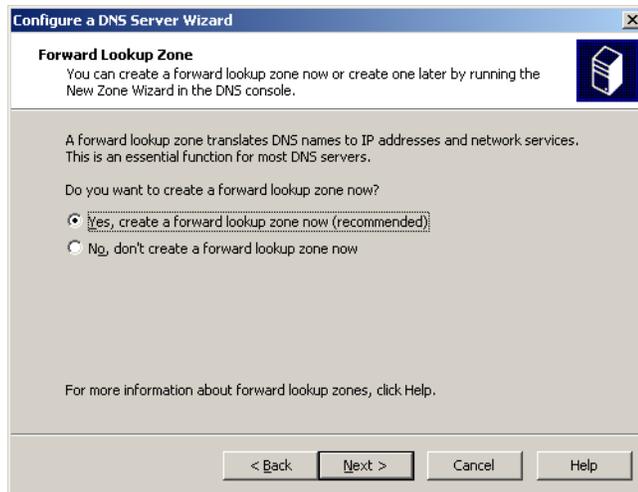
1. In the “Control Panel,” double-click the **Administrative Tools** icon.
2. Double-click the **DNS** icon.
3. In the “dnsmgmt console,” select the machine name you entered in [step 4 on page 179](#).
4. Right-click the machine name and select **Configure this DNS Server** from the context menu.
5. In the “Configure a DNS Server Wizard” pop-up window that appears, click **Next**.



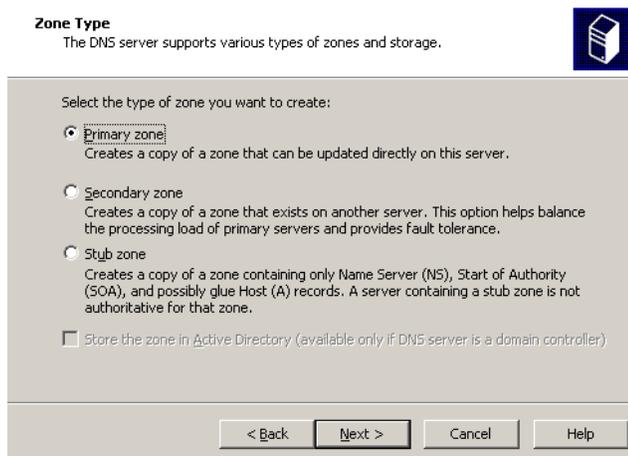
6. In the “Select Configuration Action” screen, select the **Create forward and reverse lookup zones** radio button and click **Next**.



7. In the “Forward Lookup Zone” screen, select the **Yes, create a forward lookup zone (recommended)** radio button and click **Next**.



8. In the “Zone Type” screen, select the **Primary Zone** radio button and click **Next**.



9. In the “Zone Name” screen, enter the name of the zone you are creating. The zone name is the domain suffix you entered in [step d on page 179](#). Click **Next**.

**Zone Name**  
What is the name of the new zone? 

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:

For more information about zone names, click Help.

< Back   Next >   Cancel   Help

10. In the “Zone File” screen, keep the default zone file name and click **Next**.

**New Zone Wizard** 

**Zone File**  
You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

Create a new file with this file name:

Use this existing file:

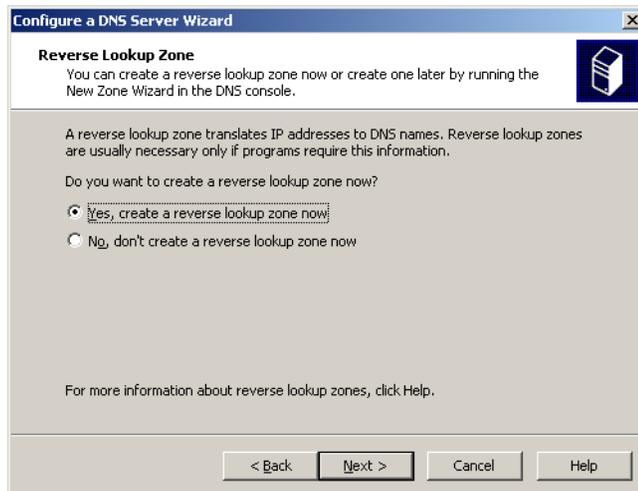
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

< Back   Next >   Cancel   Help

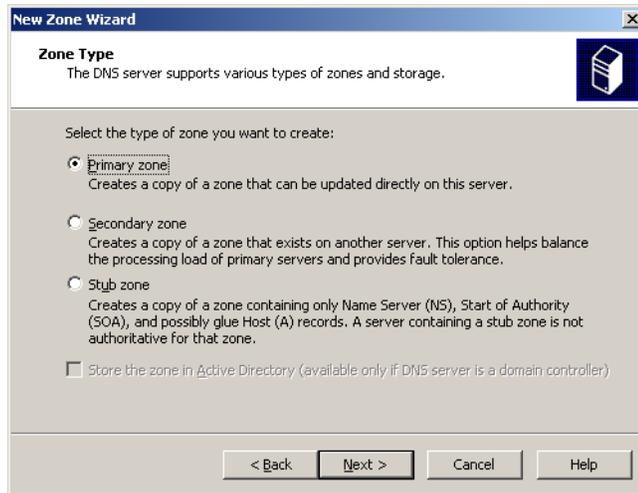
11. In the “Dynamic Update” screen, select the **Allow both nonsecure and secure dynamic updates** radio button and click **Next**.



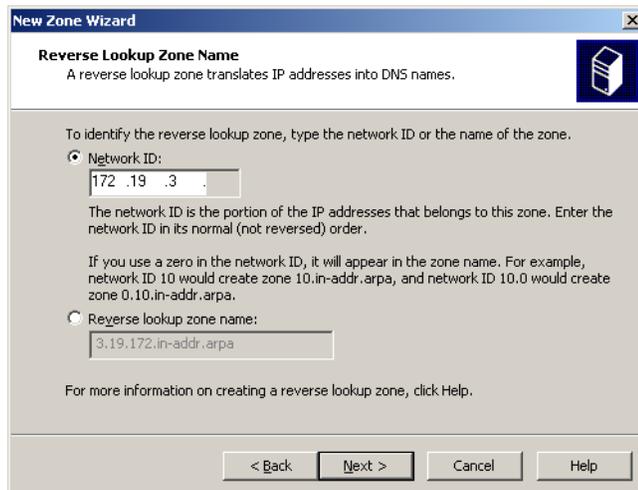
12. In the “Reverse Lookup Zone” screen, select the **Yes, create reverse lookup zone now** radio button and click **Next**.



13. In the “Zone Type” screen, select the **Primary Zone** radio button and click **Next**.



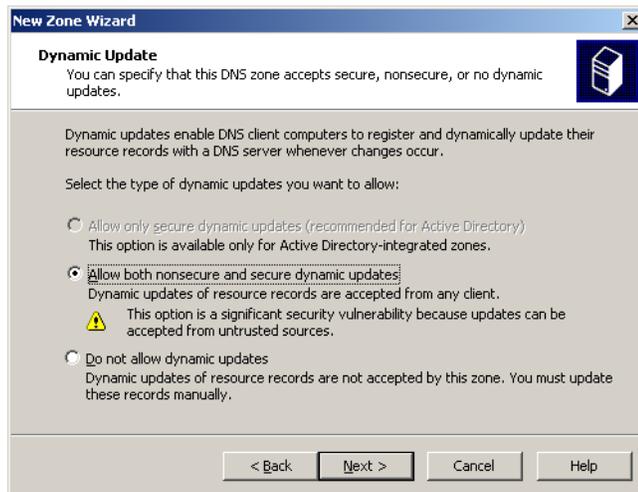
14. In the “Reverse Lookup Zone Name” screen, select the **Network ID** radio button and enter the first three octets of the machine’s IP address (you set this address in [step 1 on page 180](#)), then click **Next**.



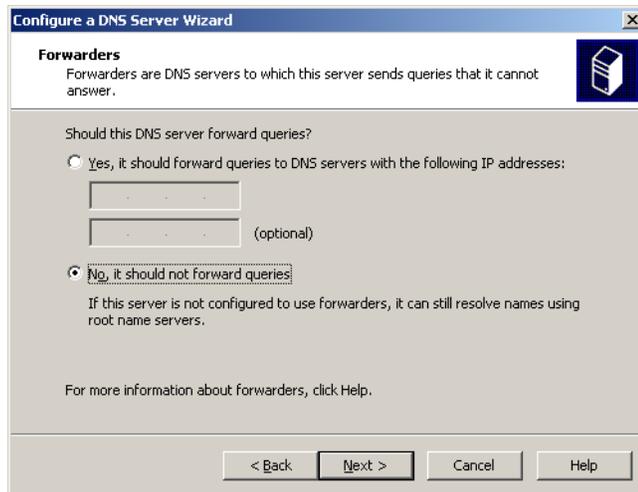
15. In the “Zone File” screen, keep the default zone file name and click **Next**.



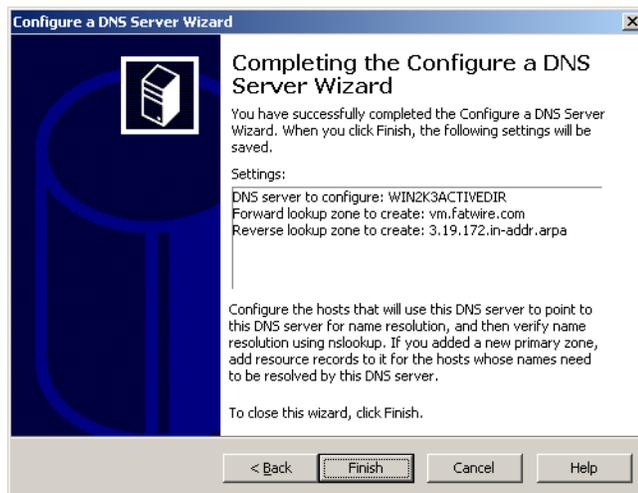
16. In the “Dynamic Update” screen, select the **Allow both nonsecure and secure dynamic updates** radio button and click **Next**.



17. In the “Forwarders” screen, select the **No, it should not forward queries** radio button and click **Next**.



18. In the “Completing the Configure a DNS Server Wizard” screen, click **Finish**.



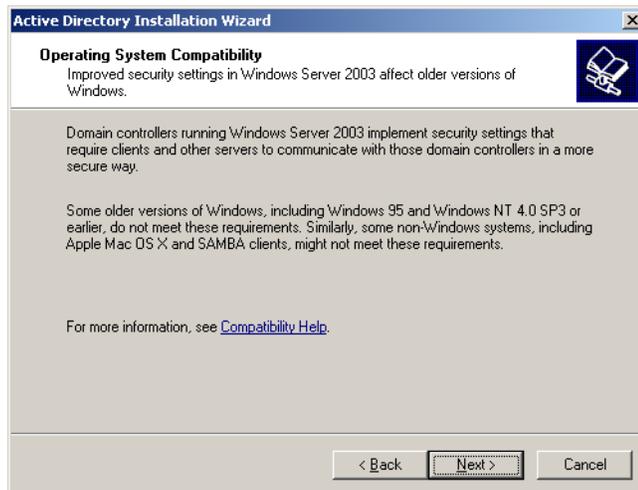
19. Close or minimize the DNS server window.

## F. Install MS Active Directory Server 2003

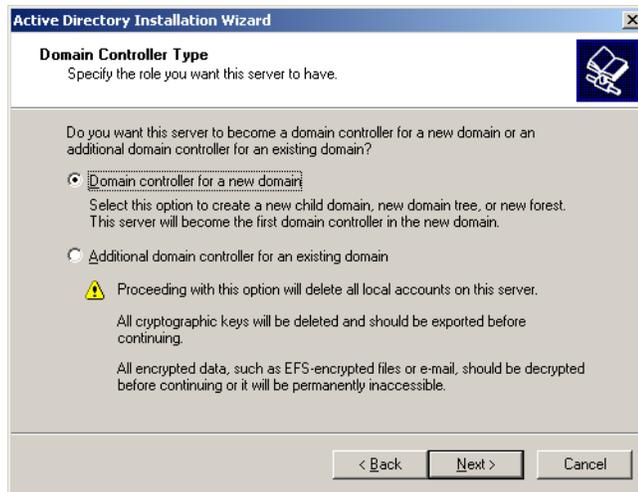
1. Click **Start**, then **Run**, and enter `adpromo` in the “Run” dialog box.
2. In the “Welcome to the Active Directory Installation Wizard” screen, click **Next**.



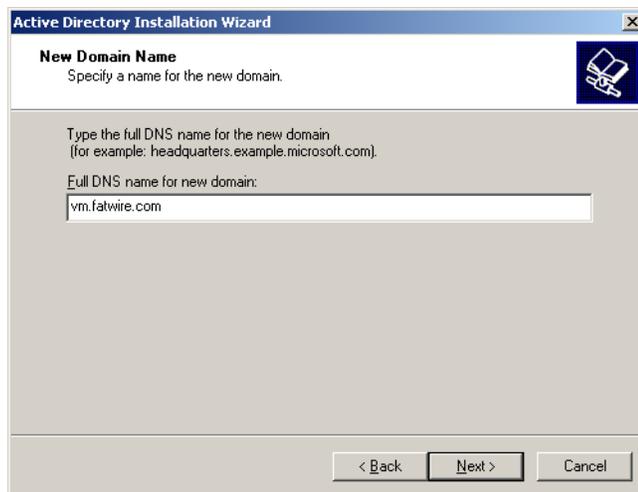
3. In the “Operating System Compatibility” screen, click **Next**.



4. In the “Domain Controller Type” screen, select the **Domain controller for a new domain** radio button and click **Next**.



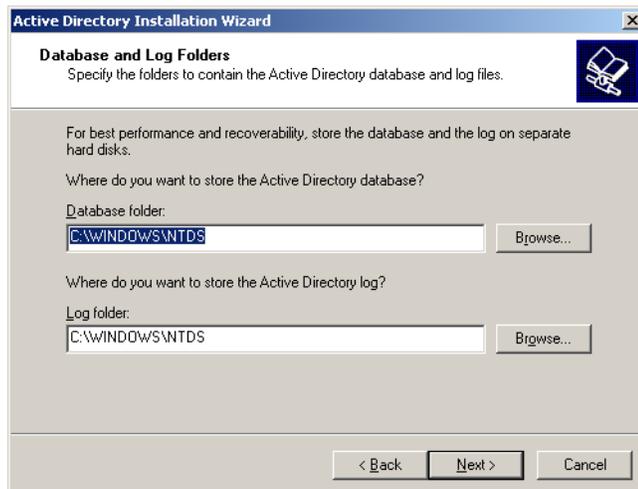
5. “In the “Create a New Domain” screen, select the **Domain in a new forest** radio button and click **Next**.
6. In the “New Domain Name” screen, enter the DNS name you entered in [step 9 on page 184](#), then click **Next**.



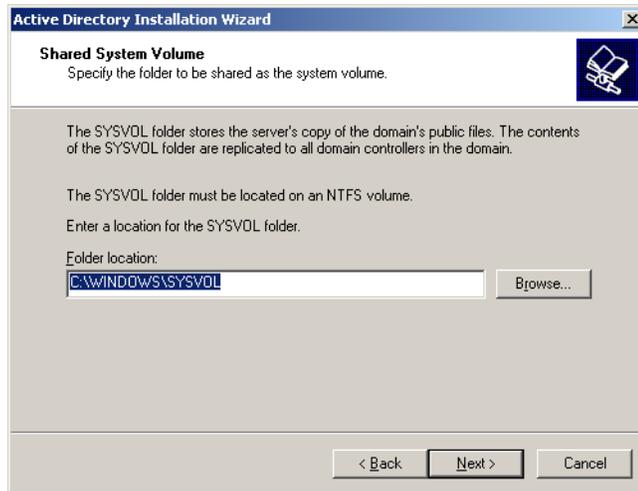
7. In the “NetBIOS Domain Name” screen, keep the default value and click **Next**. Make a record of this value.



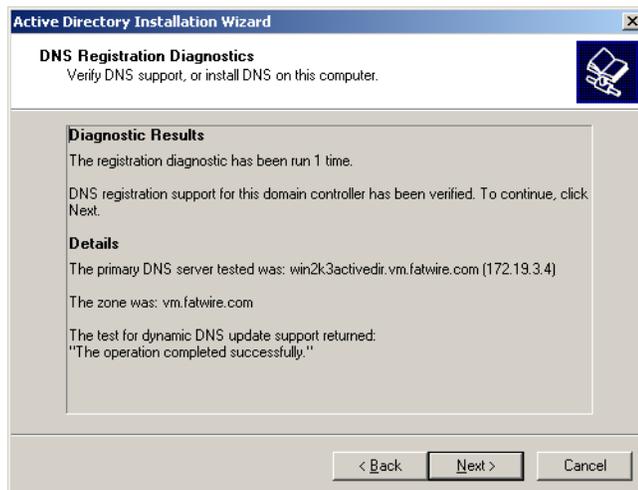
8. In the “Database and Log Folders” screen, click **Next**.



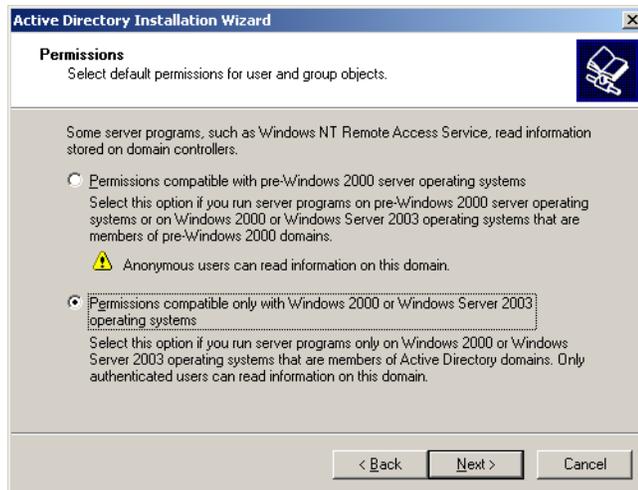
9. In the “Shared System Volume” screen, click **Next**.



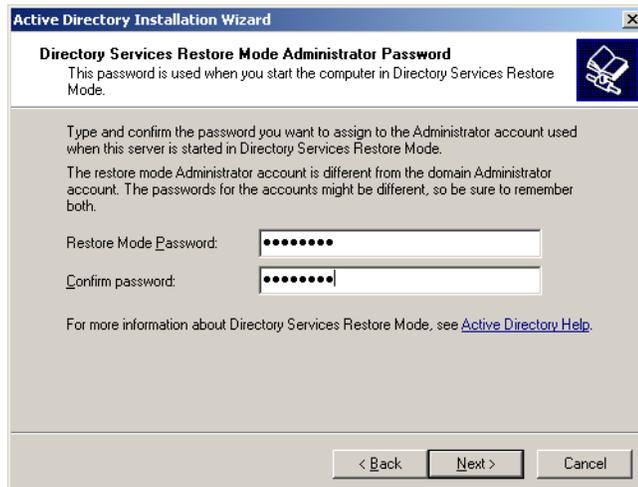
10. In the “Diagnostic Results” screen, make sure that the diagnostic has completed successfully, then click **Next**. If the diagnostic fails, correct the indicated problem, click **Back** and then **Next** to rerun the diagnostic.



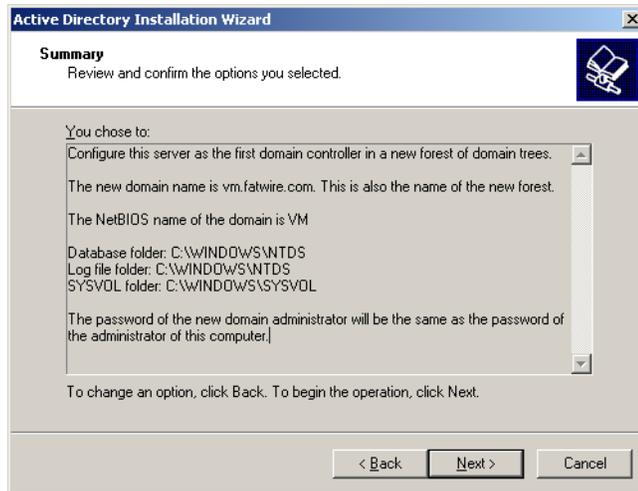
11. In the “Permissions” screen, select the **Permissions compatible only with Windows 2000 and Windows 2003 operating systems** and click **Next**.



12. In the “Directory Services Restore Mode Administrator Password” screen, enter a password and click **Next**. Make a record of this password.



13. In the “Summary” screen, click **Next**.



14. In the “Completing the Active Directory Installation Wizard” screen, click **Next**.



15. In the pop-up dialog that appears, click **Reboot Now** and wait for the machine to restart.



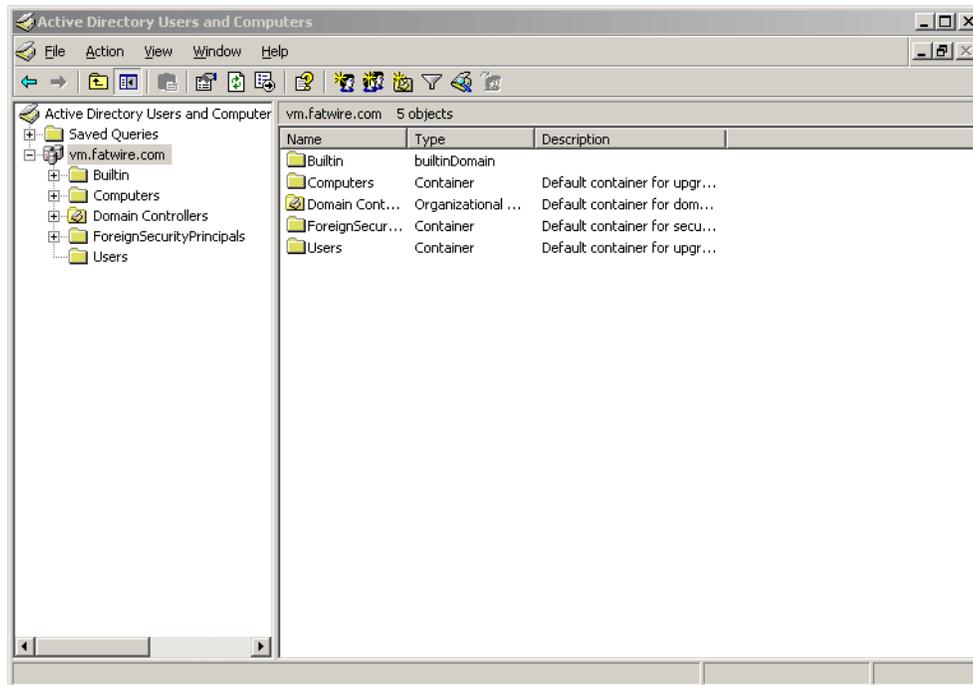
Active Directory Server is now installed and ready for use.

## Accessing the “Active Directory Users and Computers” Console

You use the “Active Directory Users and Computers” console to manage your Active Directory Server configuration. To access the console, perform the following steps:

1. Click **Start**, then **Run** to bring up the “Run” dialog box.
2. In the “Run” dialog box, enter `dsa.msc`.
3. Click **OK**.

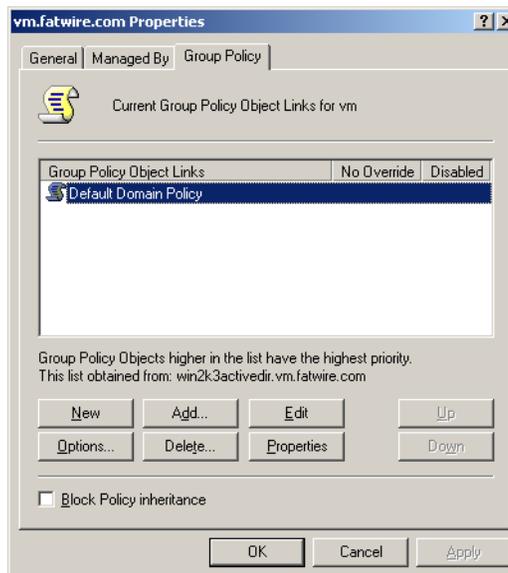
The “Active Directory Users and Computers” console loads.



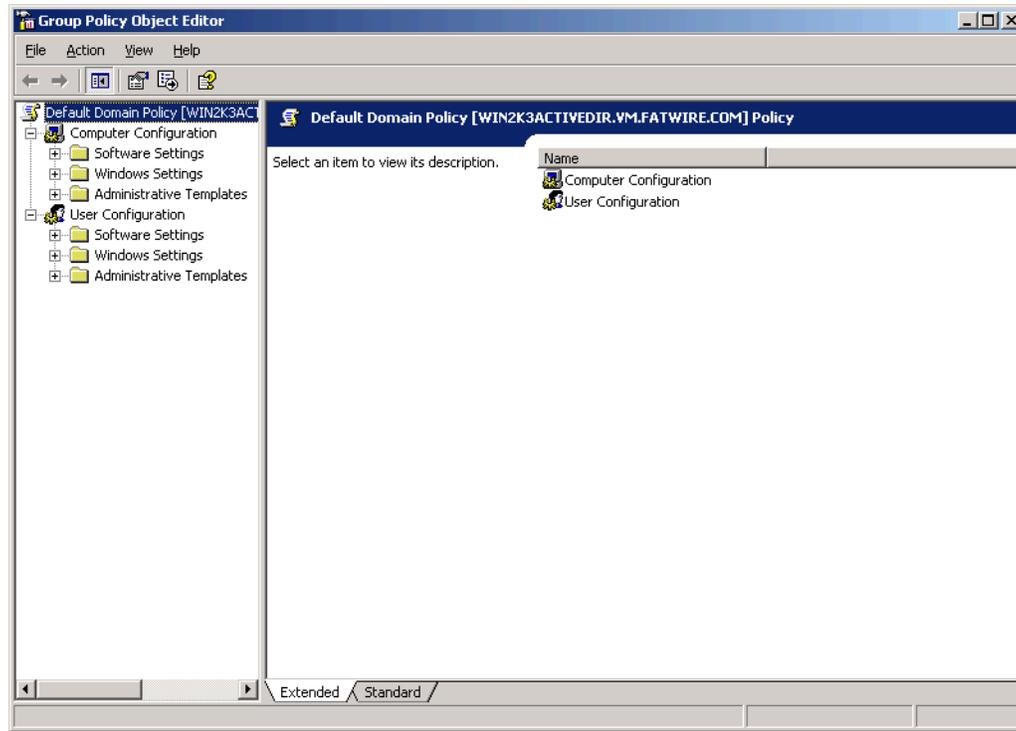
## Configuring ADS Password Security for Content Server

This section shows you how to configure password security in Active Directory Server to meet Content Server's requirements.

1. Open the "Active Directory Users and Computers" console.
2. In the tree on the left, right-click the desired domain and select **Properties** from the context menu.
3. In the dialog that appears, select the **Group Policy** tab.



- The Group Policy Object Editor appears, showing the group policy you selected.



- In the tree on the left, expand **Computer Configuration > Windows Settings > Security Settings > Account Policies** and select **Password Policy**.
- In the main pane, double-click the **Minimum password length** item.
- In the pop-up dialog that appears, enter 4 as the value and click **OK**.



- Double-click the **Password must meet complexity requirements** item.
- In the pop-up window that appears, select the **Disabled** radio button and click **OK**.
- From the **File** menu, select **Exit**, then click **OK**.
- Bring up the “Run” dialog, enter **gpupdate**, and click **OK**.

## Modifying User Passwords

This section shows you how to modify a user's password in Active Directory Server.

1. Open the “Active Directory Users and Computers” console.
2. In the tree on the left, select **Users**.
3. In the main pane, select the user whose password you want to modify.
4. Right-click the desired user name and select **Reset Password** from the context menu.
5. In the dialog that appears, enter and re-enter the new password, then click **OK**.

## Deleting Users

This section shows you how to delete a user in Active Directory Server.

1. Open the “Active Directory Users and Computers” console.
2. In the tree on the left, select **Users**.
3. In the main pane, select the user whose password you want to modify.
4. Right-click the desired user name and select **Delete** from the context menu.
5. In the pop-up dialog that appears, click **Yes**.

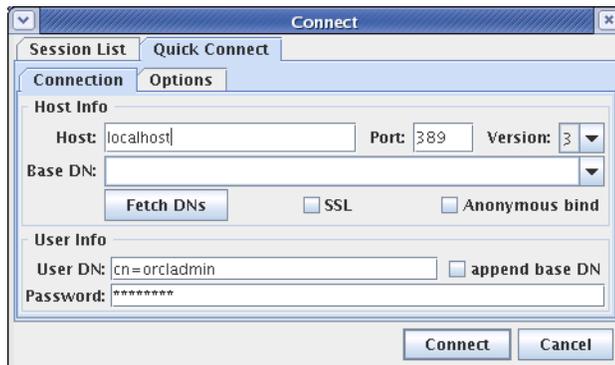
## Connecting to ADS Using an LDAP Browser

This section shows you how to connect to Active Directory Server using an LDAP browser.

### Note

You cannot add groups, set passwords, or activate accounts using an LDAP browser.

1. Open the LDAP browser.
2. Select the **Quick Connect** tab.
3. Fill out the following information:
  - **Host:** localhost (if connecting remotely, enter the actual host name)
  - **Base DN:** <DNS\_suffix> (the part of the DNS name after the host name)
  - **Anonymous bind:** uncheck
  - **User DN:** administrator<DNS\_suffix>
  - **Append base DN:** uncheck
  - **Password:** <ADS\_password> (you created this password in [step 12 on page 193](#))



4. Click **Connect**.

