

Oracle® WebCenter Sites
Configuring Supporting Software
11g Release 1 (11.1.1) Bundled Patch 1

October 2012

Oracle® WebCenter Sites: Configuring Supporting Software, 11g Release 1 (11.1.1) Bundled Patch 1

Copyright © 2012 Oracle and/or its affiliates. All rights reserved.

Primary Author: Melinda Rubenau, Sean Cearley

Contributing Author: Tatiana Kolubayev

Contributor: Eric Gandt, Guthrie Taber, Gaurang Mavadiya, William Habermaas

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

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

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

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

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

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of

Contents

About This Guide	7
Audience	7
How This Guide is Organized	7
Related Documents	8
Graphics in This Guide	8
Conventions	8
Third-Party Libraries	8

Part 1. Creating and Configuring a Database

1 Creating and Configuring an Oracle 11g Database	11
Step I. Create an Oracle 11g Database	12
Step II. Create a New User for WebCenter Sites	24
Next Step	29
2 Creating and Configuring an MS SQL Server Database.	31
Creating a Database on MS SQL Server 2008 R2	32
3 Creating and Configuring an IBM DB2 9.7 Database	33
Installing and Configuring DB2 9.7 for WebCenter Sites	34
A. Install DB2	34
B. Create a New DB2 Database.	44
C. Create a User for the New Database.	49
D. Configure the Database.	52

Part 2. Installing a Web Server

4	Worksheets for Documenting the Web Server Installation	57
	Key to Sample Values	58
	Web Server Parameters	58
5	Installing IBM HTTP Server 7.0	61
	Installation Steps	62
	Installing IHS with WebSphere Application Server on the Local Server	68
6	Installing Internet Information Services on Windows	73
	Step I. Install IIS	74
	Step II. Verify the Installation	79
	Step III. Starting and Configuring IIS	80
	A. IIS Manager	80
	B. Changing the IIS Port	80
	C. Adding a New ISAPI Filter	81
	Proxing Using IIS	83
7	Installing Apache on Solaris and Linux	85
	Step I. Install Apache	86
	Step II. Document Your Apache Parameters	86
	Step III. Verify that Apache Contains the Correct Module	87
	Step IV. Verify that Apache Runs Properly	87
	Next Step	87

Part 3. Installing and Configuring an LDAP Server

8	Installing Active Directory Server 2008	91
	Installation Steps	92
	Configuring the Network Settings	95
	Installing Active Directory 2008 Services	98
	Installing Active Directory 2008 Installation Wizard	103
	Checking Group Policies	110
	Changing Group Policies	112
	Connecting to ADS Using an LDAP Browser	115
9	Setting Up IBM Tivoli Directory Server 6.x	117
	IBM Tivoli Directory Server Commands	118
	Before Installing IBM Tivoli Directory Server	119
	Installing IBM Tivoli Directory Server	119
	Configuring Tivoli Directory Server	127
	Connecting to IBM TDS Using the LDAP Browser	134

10 Setting Up OpenLDAP 2.3.x	137
OpenLDAP Commands	138
Starting OpenLDAP	138
Searching an OpenLDAP Server	138
Adding an LDIF File to an OpenLDAP Server	139
Installing OpenLDAP	140
Configuring OpenLDAP	142
Adding WebCenter Sites Schema to OpenLDAP	145
Modifying User Passwords	147
Modifying User Passwords Using an LDAP Browser	147
Modifying User Passwords Using the ldapmodify Command	150
11 Setting Up the WebLogic 10.3.5 Embedded LDAP Server	151
Enabling the WebLogic Embedded LDAP Server	152
Modifying User Passwords	154
12 Setting Up MS Active Directory Server 2003	157
Installing MS Active Directory Server	158
A. Install the Operating System	158
B. Set the Machine's Name and Suffix	158
C. Configure the Machine's Network Settings	160
D. Install the Local DNS Server	160
E. Configure the Local DNS Server	162
F. Install MS Active Directory Server 2003	169
Accessing the "Active Directory Users and Computers" Console	175
Configuring ADS Password Security for WebCenter Sites	176
Modifying User Passwords	178
Deleting Users	178
Connecting to ADS Using an LDAP Browser	179

Part 4. Installing and Configuring Authentication Services

13 Clustering the Central Authentication Service Application	183
Deploying Secondary CAS Cluster Members	184
Redeploying CAS on a New Server	186
14 Oracle Access Manager Integration Setup	189
Overview	190
Integration Components	190
Flow for Browser Requests	191
REST Service Flow	192
OAM Integration Prerequisites	193
Installing OAM Components	193

Preparing OAM for Integration	197
Integrating OAM with Oracle WebCenter Sites	199
Before You Start	199
Integration Steps	200
Integrating OAM with Oracle WebCenter Sites: Satellite Server.	218
Before You Start	218
Integration Steps	218

About This Guide

This guide contains information about pre-installing and configuring databases, web servers, and other software used by Oracle WebCenter Sites.

Applications discussed in this guide are former FatWire products. Naming conventions are the following:

- *Oracle WebCenter Sites* is the current name of the application previously known as *FatWire Content Server*. In this guide, *Oracle WebCenter Sites* is also called *WebCenter Sites*.
- *Oracle WebCenter Sites: Satellite Server* is the current name of the application previously known as *FatWire Satellite Server*. In this guide, *Oracle WebCenter Sites: Satellite Server* is also called *Satellite Server*.

Audience

This guide is intended for installation engineers with experience installing and configuring enterprise-level software, including databases, database drivers, application servers, web servers, and LDAP servers.

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 supported databases before installing WebCenter Sites. (This part supplements the WebCenter Sites installation guides.)
- [Part 2, “Installing a Web Server”](#) shows you how to install and configure supported web servers, if you choose to use one. (This part supplements the WebCenter Sites installation guides.)
- [Part 3, “Installing and Configuring an LDAP Server”](#) shows you how to set up the supported LDAP server for integration with WebCenter Sites. (This part supplements the guide named *Oracle WebCenter Sites: Integrating with LDAP*.)
- [Part 4, “Installing and Configuring Authentication Services”](#) shows you how to integrate WebCenter Sites with supported third-party applications that provide

authentication services and single sign-on. (This part supplements the WebCenter Sites installation guides.)

Related Documents

For more information, see the following documents:

- *Oracle WebCenter Sites: Installing on Apache Tomcat Application Server*
- *Oracle WebCenter Sites: Installing on IBM WebSphere Application Server*
- *Oracle WebCenter Sites: Installing on Oracle WebLogic Application Server*
- *Oracle WebCenter Sites: Installing Satellite Server*

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. The 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.

Conventions

The following text conventions are used in this guide:

- **Boldface** type indicates graphical user interface elements that you select.
- *Italic* type indicates book titles, emphasis, or variables for which you supply particular values.
- `Monospace` type indicates file names, URLs, sample code, or text that appears on the screen.
- **Monospace bold** type indicates a command.

Third-Party Libraries

Oracle WebCenter Sites and its applications include third-party libraries. For additional information, see *Oracle WebCenter Sites 11gR1: Third-Party Licenses*.

Part 1

Creating and Configuring a Database

WebCenter Sites requires access to a supported database configured specifically for WebCenter Sites. Instructions for creating and configuring supported databases are available in the following chapters:

- [Chapter 1, “Creating and Configuring an Oracle 11g Database”](#)
- [Chapter 2, “Creating and Configuring an MS SQL Server Database”](#)
- [Chapter 3, “Creating and Configuring an IBM DB2 9.7 Database”](#)

The databases listed above are not configured for production; they are set up with full permissions. In practice, the permissions can be restricted for the user that WebCenter Sites 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. For instructions on creating and configuring a supported database refer to the chapters listed above. (Note that database configuration is identical across different application servers.)

Chapter 1

Creating and Configuring an Oracle 11g Database

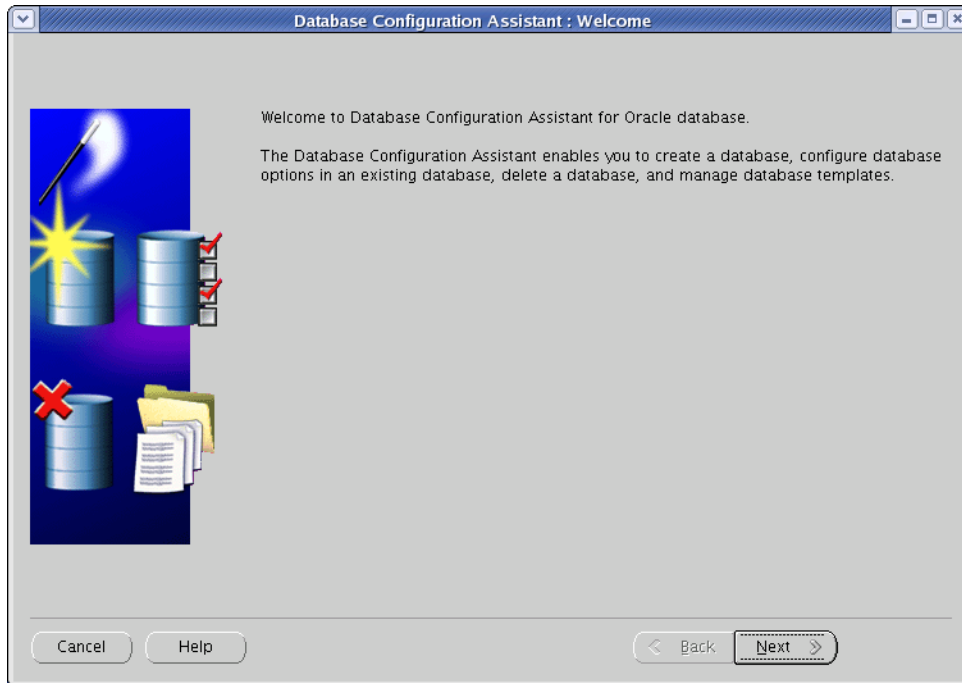
Use this chapter to set up an Oracle 11g database for your WebCenter Sites installation. For background information regarding database configuration and Users' permissions, see [Part 1, "Creating and Configuring a Database."](#)

This chapter contains the following sections:

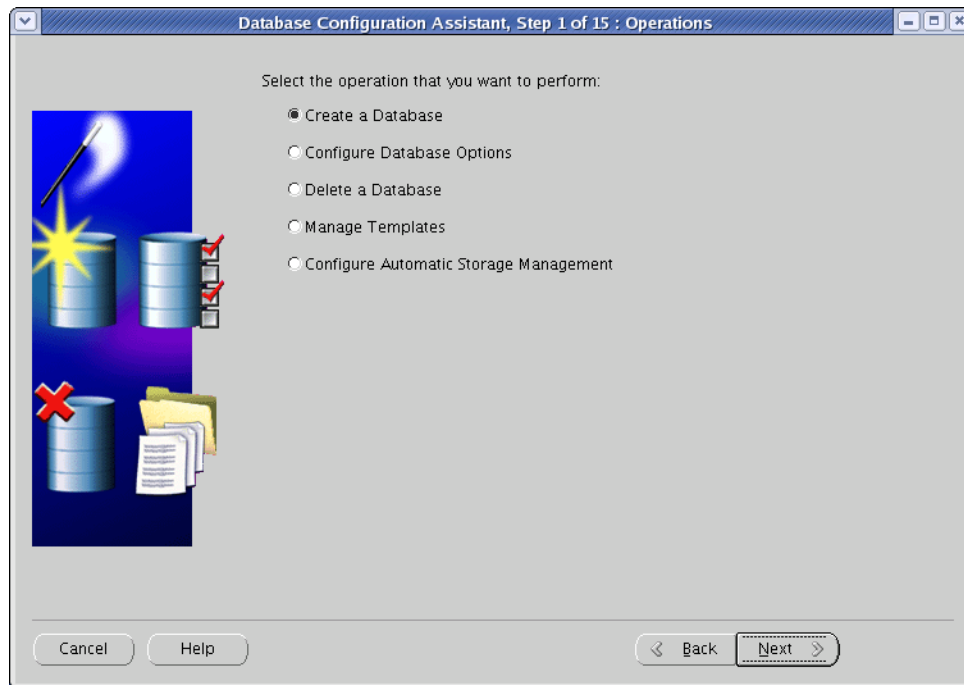
- [Step I. Create an Oracle 11g Database](#)
- [Step II. Create a New User for WebCenter Sites](#)

Step I. Create an Oracle 11g Database

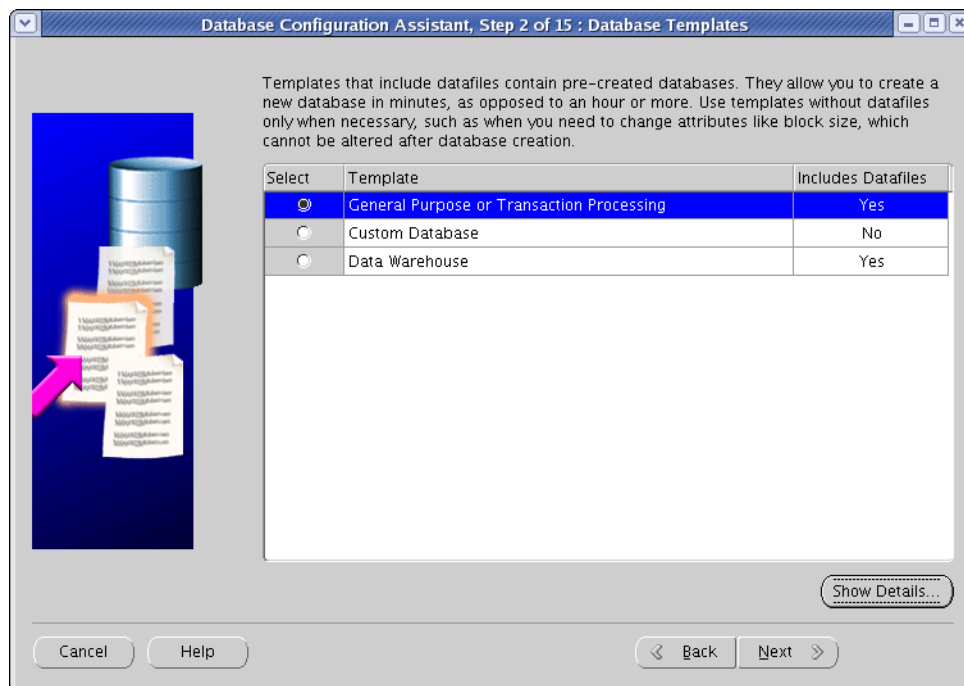
1. Launch the Oracle Database Configuration Assistant by executing the following command:
`<ora_home>/bin/dbca`
2. In the “Welcome” screen, click **Next**.



3. In the “Operations” screen, select **Create a Database** and click **Next**.



4. In the “Database Templates” screen, select **General Purpose or Transaction Processing** and click **Next**.



5. In the “Database Identification” screen, enter the global database name and the SID. (Oracle recommends using the same value for both; in our example, we are using contentDB.) When you are finished, click **Next**.

Database Configuration Assistant, Step 3 of 15 : 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. In the “Management Options” screen, select the **Configure Enterprise Manager** check box. Select other options as desired. When you are finished, click **Next**.

Database Configuration Assistant, Step 4 of 15 : Management Options

Configure Enterprise Manager

Register with Grid Control for centralized management

Management Service:

Configure Database Control for local management

Enable Alert Notifications

Outgoing Mail (SMTP) Server:

Recipient Email Address:

Enable Daily Disk Backup to Recovery Area

Backup Start Time: : AM PM

OS Username:

OS Password:

Cancel Help < Back Next >

7. In the “Database Credentials” screen, do one of the following:
- If you are installing a production system, select **Use Different Administrative Passwords**, enter a unique password for each database user shown in the table, and click **Next**.
 - If you are installing a non-production system, select **Use the Same Administrative Password for All Accounts**, enter and re-enter a password, and click **Next**.

Database Configuration Assistant, Step 5 of 15 : Database Credentials

For security reasons, you must specify passwords for the following user accounts in the new database.

Use Different Administrative Passwords

User Name	Password	Confirm Password
SYS		
SYSTEM		
DBSNMP		
SYSMAN		

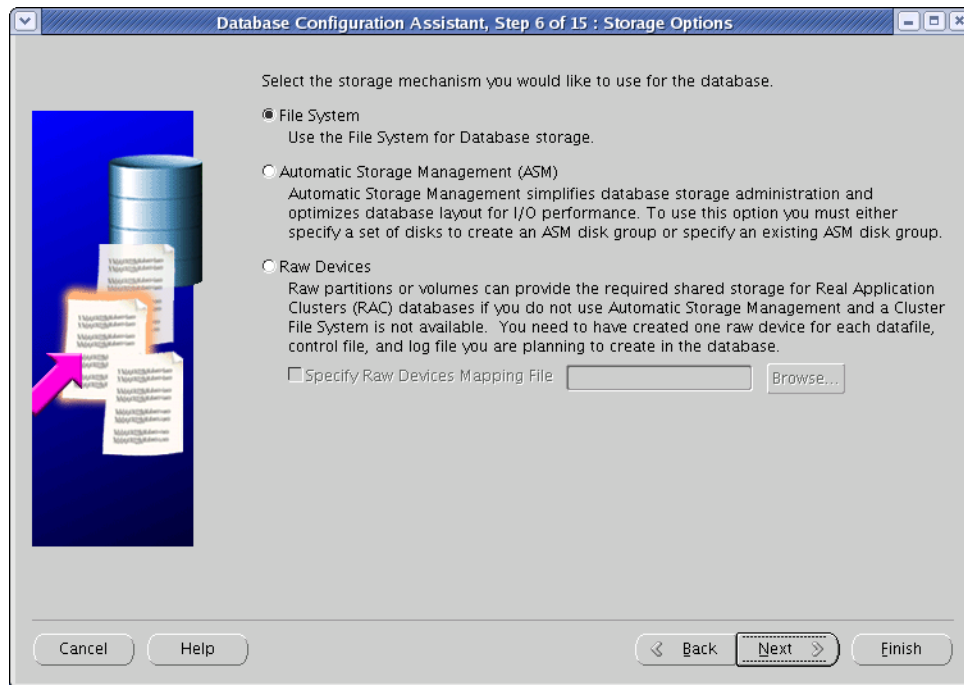
Use the Same Administrative Password for All Accounts

Password:

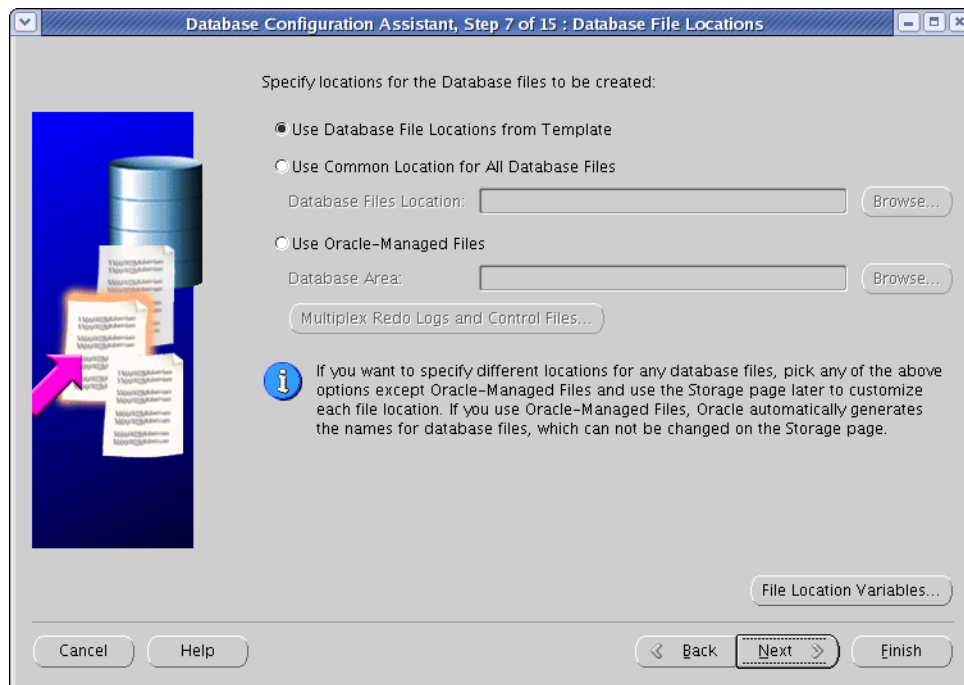
Confirm Password:

Cancel Help Back Next

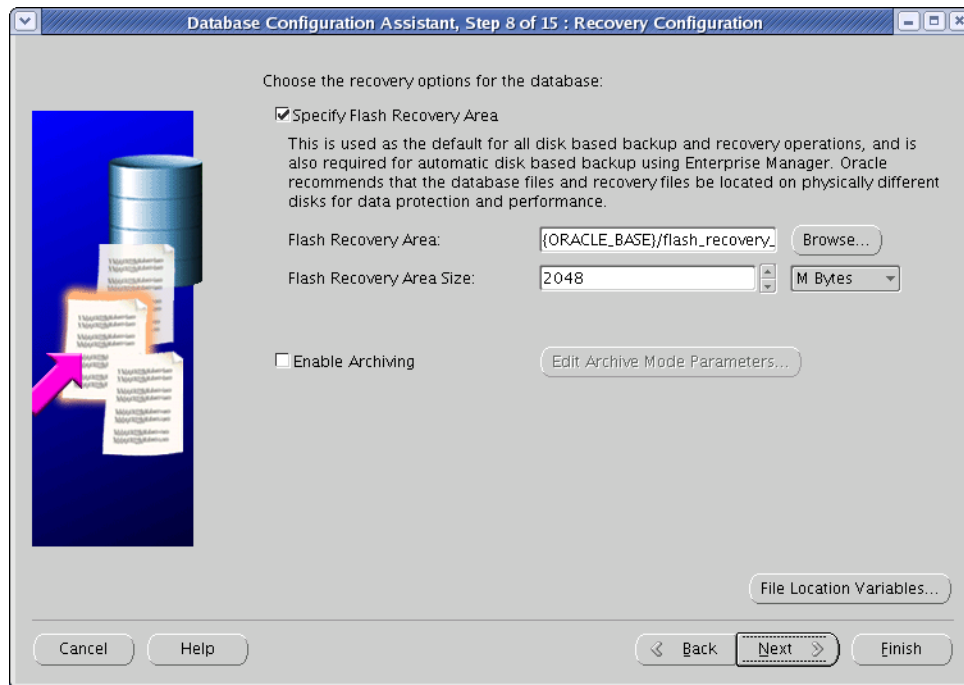
8. In the “Storage Options” screen, select **File System** and click **Next**.



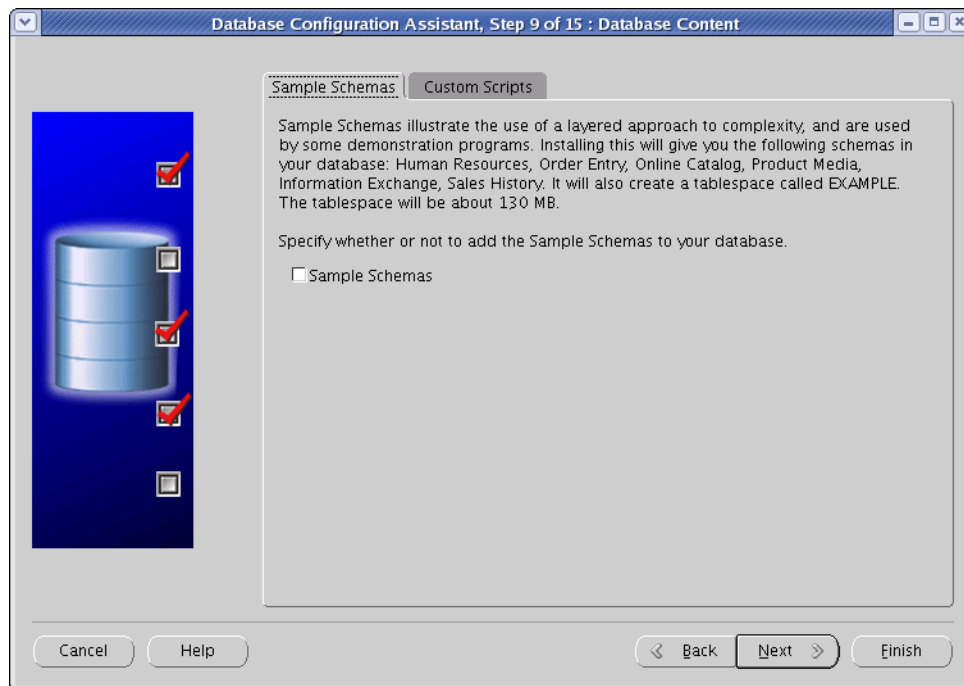
9. In the “Database File Locations” screen, select **Use Database File Locations from Template** (unless you want to use custom file names and locations) and click **Next**.



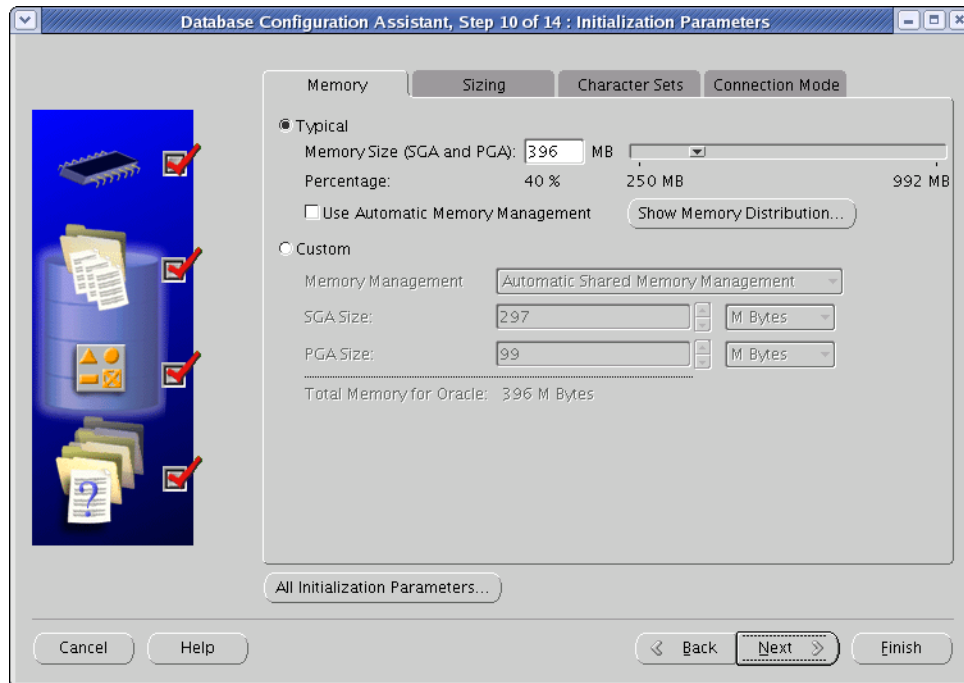
10. In the “Recovery Configuration” screen, leave the default values and click **Next**.



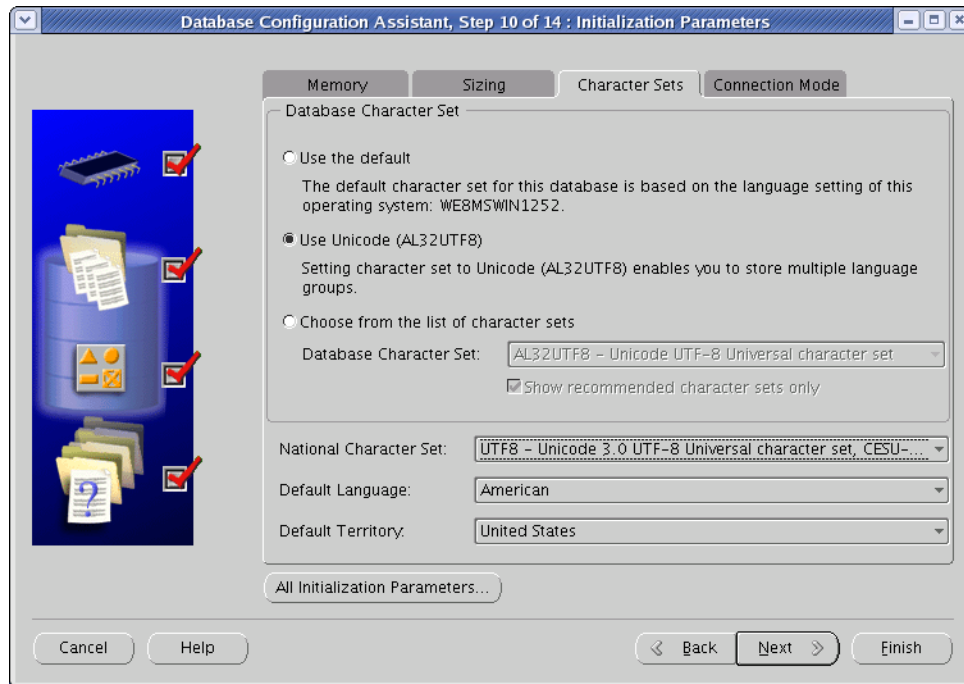
11. In the “Database Content” screen, click **Next**.



12. In the “Initialization Parameters” screen, do the following:
- In the **Memory** tab, set the preferred memory size for your database. The value you enter here will depend on the size and contents of your database. Oracle recommends a minimum of 384MB.

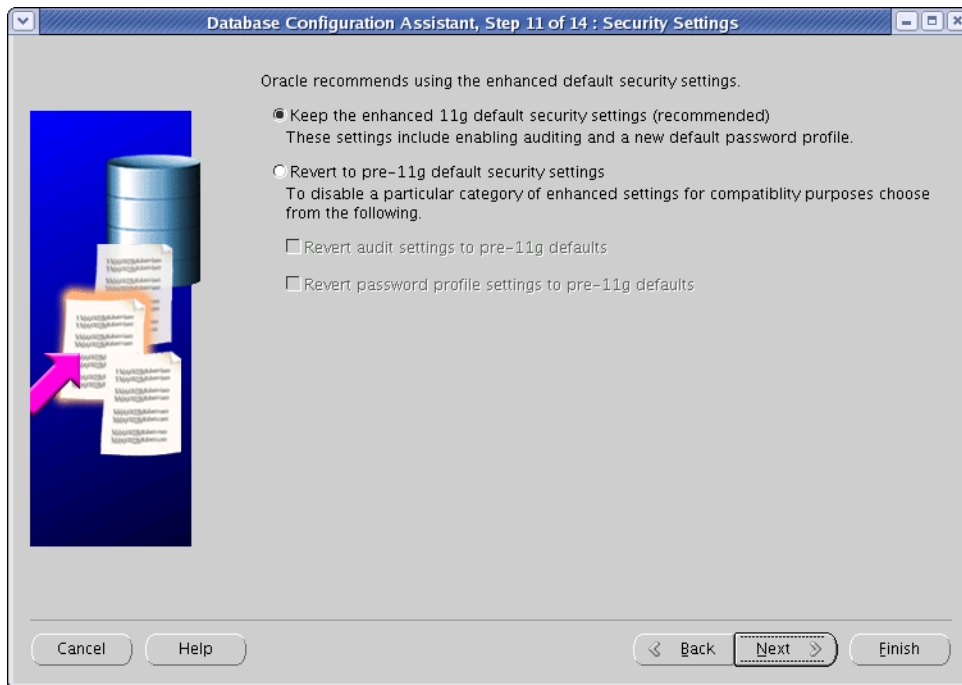


- b. In the **Character Sets** tab, do the following:
- 1) Select the **Use Unicode (AL32UTF8)** radio button.
 - 2) In the “National Character Set” drop-down list, select **UTF-8 - Unicode 3.0 UTF-8 Universal Character Set**.

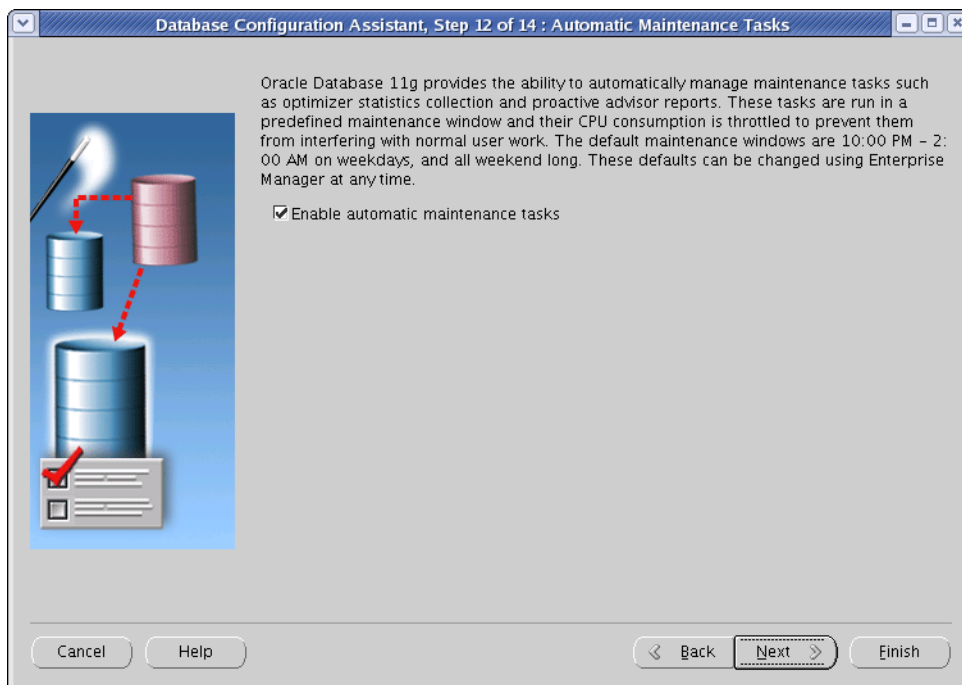


- c. Click **Next**.

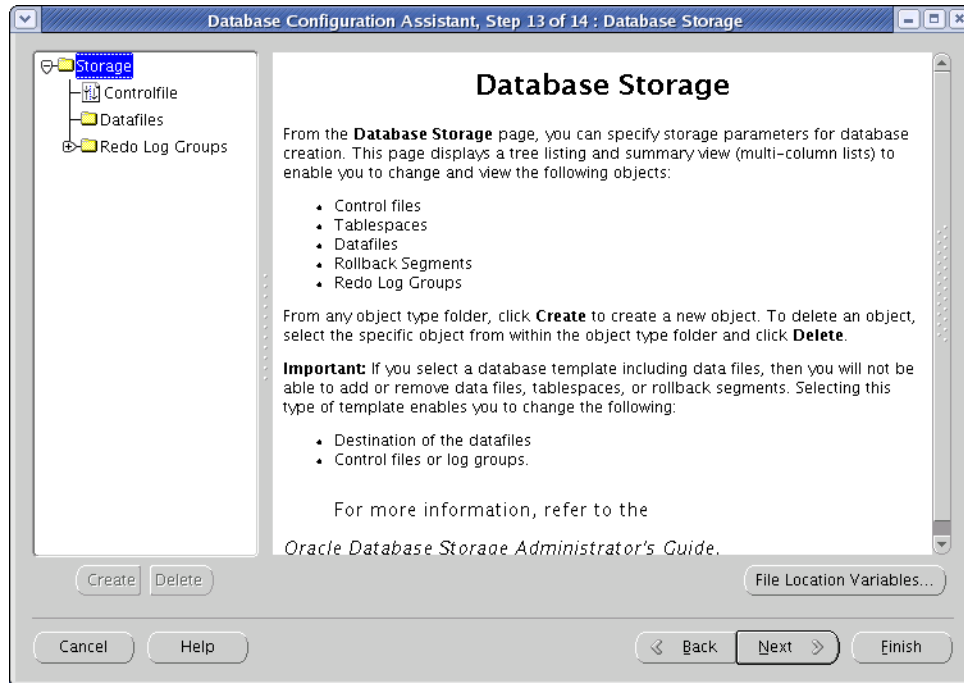
13. In the “Security Settings” screen, click **Next**.



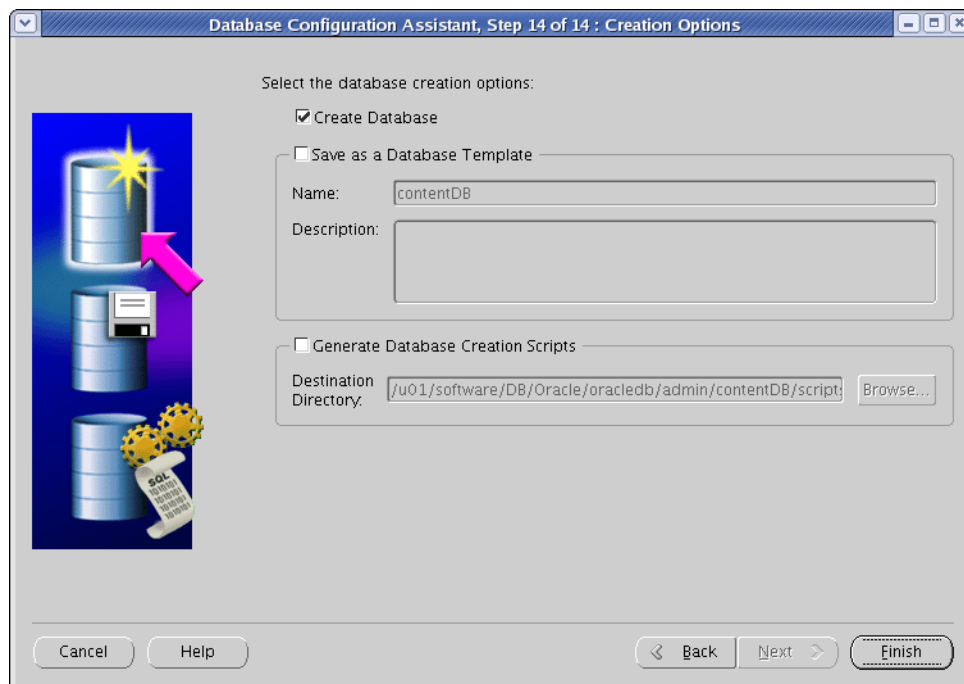
14. In the “Automatic Maintenance Tasks” screen, click **Next**.



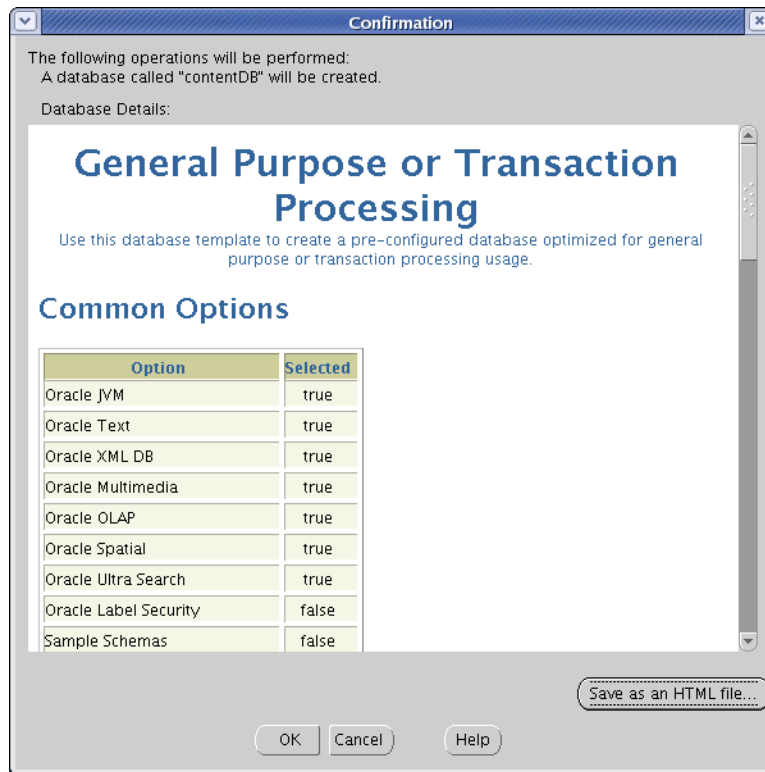
15. In the “Database Storage” screen, review the selected file locations. (If you need to make changes, click **File Location Variables**.) Click **Next**.



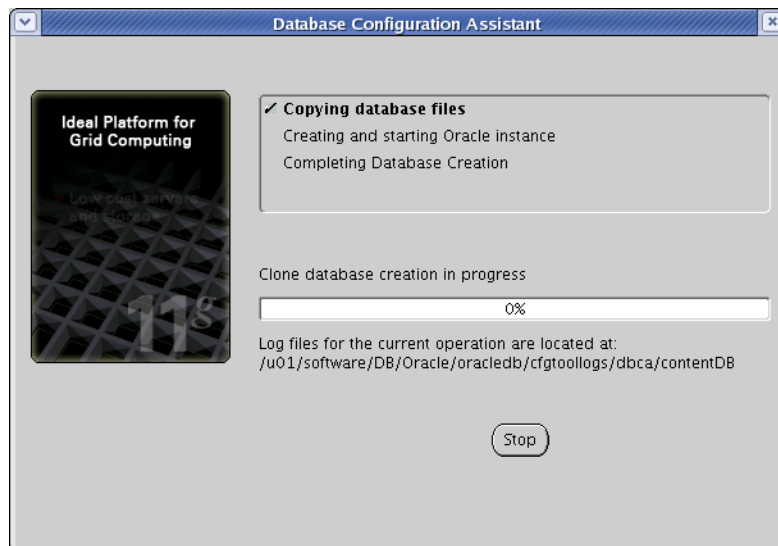
16. In the “Creation Options” screen, click **Finish**.



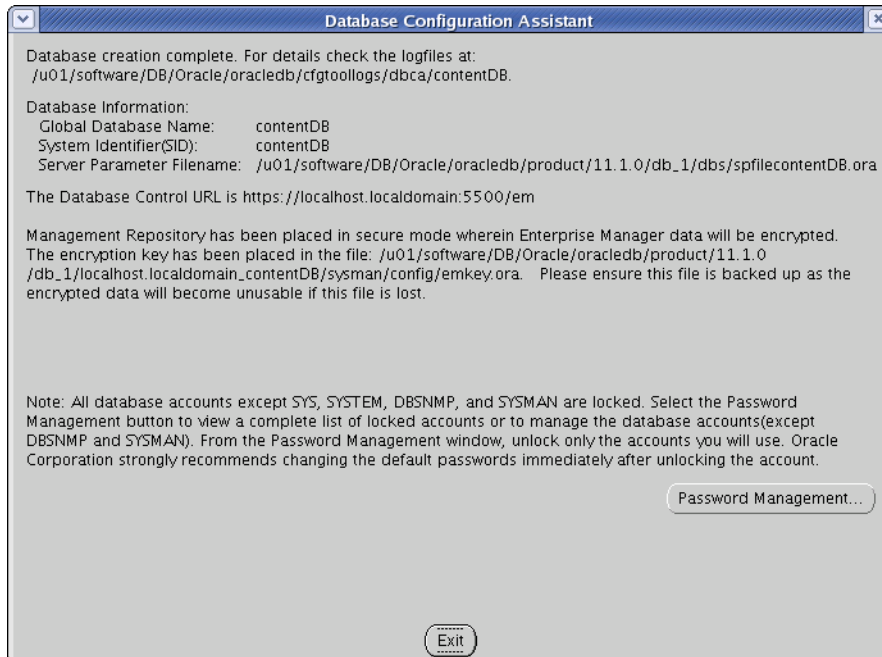
17. In the “Confirmation” screen, review the selected options, then click **OK**.



18. Allow the database creation tasks to complete. If any one of the tasks fails, remedy the problem before continuing.



19. At the summary screen, make a record of the database SID and the database control URL, then click **Exit**.



Step II. Create a New User for WebCenter Sites

1. Determine the Console Server port:
 - a. Open the `emoms.properties` file in a text editor. The file is located in:


```
<ora_home>/<servername>_<SID>/sysman/config/
```
 - b. Find the line,


```
oracle.sysman.emSDK.svlt.ConsoleServerPort
```

 and make a record of the port number value at the end of the line.
2. Log in to the Oracle Enterprise Manager console:
 - a. Execute the following command: **emctl status dbconsole**
 The command should return an output similar to the following:


```
Oracle Enterprise Manager 11g Database Control Release 11.1.0.6.0
Copyright (c) 1996, 2007 Oracle Corporation. All rights reserved.
https://localhost.localdomain:1158/em/console/aboutApplication
Oracle Enterprise Manager 11g is running.
-----
Logs are generated in directory /u01/software/DB/Oracle/oracledb/
product/11.1.0/db_1/localhost.localdomain_vmorcldb/sysman/log
```
 - b. Open a browser and go to the URL highlighted in bold in [step a](#) above. If you see a “Security Mismatch” error, ignore it (the error appears if you are using a self-signed certificate).
 - c. Log in as the `sys` user (you specified a password for this user in [step 7](#) on [page 15](#)) connecting as **SYSDBA**.

ORACLE Enterprise Manager 11g Database Control [Help](#)

Login

* User Name

* Password

Connect As

Login

Copyright © 1996, 2007, Oracle. All rights reserved.
 Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
 Unauthorized access is strictly prohibited.

3. In the tab bar, click **Server**.

ORACLE Enterprise Manager 11g Database Control Setup Preferences Help Logout

Database


Logged in As SYS

Database Instance: vmorcldb

Home Performance Availability **Server** Schema Data Movement Software and Support

Latest Data Collected From Target Oct 1, 2007 4:38:29 PM EDT View Data Automatically (60 sec) ▼

General



Status [Up](#)

Up Since **Oct 1, 2007 12:50:34 PM EDT**

Instance Name **vmorcldb**

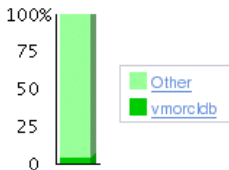
Version **11.1.0.6.0**

Host [localhost.localdomain](#)

Listener [LISTENER_localhost.localdomain](#)

[View All Properties](#)

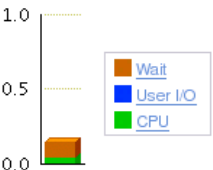
Host CPU



Load [4.43](#) Paging [0.00](#)

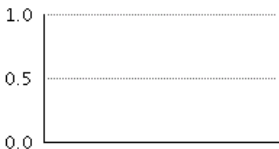
Maximum CPU **1**

Active Sessions



Maximum CPU **1**

SQL Response Time



Reference collection is empty.


SQL Response Time (%) **Unavailable**

Diagnostic Summary

ADDM Findings [7](#)

Period Start Time **Oct 1, 2007 3:00:02 PM EDT**

Alert Log [No ORA- errors](#)

Active Incidents  [0](#)

[Database Instance Health](#)

Space Summary

Database Size (GB)	1.485
Problem Tablespace	0
Segment Advisor Recommendations	0
Policy Violations	0 ✓
Dump Area Used (%)	65

High Availability

Instance Recovery Time (sec)	22
Last Backup	n/a
Usable Flash Recovery Area (%)	100
Flashback Database Logging	Disabled

4. Create the new user. Do the following:
 - a. In the “Security” section of the page, click **Users**.

ORACLE Enterprise Manager 11g Database Control Setup Preferences Help Logout

Database

Logged in As SYS

Database Instance: vmorcldb

Home Performance Availability **Server** Schema Data Movement Software and Support

Storage

- [Control Files](#)
- [Tablespaces](#)
- [Temporary Tablespace Groups](#)
- [Datafiles](#)
- [Rollback Segments](#)
- [Redo Log Groups](#)
- [Archive Logs](#)
- [Migrate to ASM](#)
- [Make Tablespace Locally Managed](#)

Statistics Management

- [Automatic Workload Repository](#)
- [AWR Baselines](#)

Database Configuration

- [Memory Advisors](#)
- [Automatic Undo Management](#)
- [Initialization Parameters](#)
- [View Database Feature Usage](#)

Resource Manager

- [Getting Started](#)
- [Consumer Groups](#)
- [Consumer Group Mappings](#)
- [Plans](#)
- [Settings](#)
- [Statistics](#)

Oracle Scheduler

- [Jobs](#)
- [Chains](#)
- [Schedules](#)
- [Programs](#)
- [Job Classes](#)
- [Windows](#)
- [Window Groups](#)
- [Global Attributes](#)
- [Automated Maintenance Tasks](#)

Security

- [Users](#)**
- [Roles](#)
- [Profiles](#)
- [Audit Settings](#)
- [Transparent Data Encryption](#)
- [Virtual Private Database Policies](#)
- [Application Contexts](#)

- b. Click **Create** near the top right corner of the user list.

ORACLE Enterprise Manager 11g Database Control Setup Preferences Help Logout

Database

Logged in As SYS

Database Instance: vmorcldb >

Users

Object Type: User

Search

Enter an object name to filter the data that is displayed in your results set.

Object Name

By default, the search returns all uppercase matches beginning with the string you entered. To run an exact or case-sensitive match, double quote the search string. You can use the wildcard symbol (%) in a double quoted string.

Selection Mode:

Select	UserName	Account Status	Expiration Date	Default Tablespace	Temporary Tablespace	Profile	Created
<input type="checkbox"/>	ANONYMOUS	EXPIRED & LOCKED	Sep 25, 2007 3:39:21 PM EDT	SYSaux	TEMP	DEFAULT	Aug 3, 2007 1:34:38 AM EDT
<input type="checkbox"/>	APEX_PUBLIC_USER	EXPIRED & LOCKED	Sep 25, 2007 3:39:21 PM EDT	USERS	TEMP	DEFAULT	Aug 3, 2007 2:04:08 AM EDT

- c. In the “Create User” form, fill in all required fields (marked with an asterisk).
Fill in all other fields as necessary.

ORACLE Enterprise Manager 11g Database Control Setup Preferences Help Logout

Database Instance: contentDB > Users > Logged in As SYS

Create User

Show SQL Cancel OK

General Roles System Privileges Object Privileges Quotas Consumer Group Privileges Proxy Users

* Name

Profile


Authentication


* Enter Password

* Confirm Password

For Password choice, the role is authorized via password.

Expire Password now

Default Tablespace 

Temporary Tablespace 

Status Locked Unlocked

Show SQL Cancel OK

[Database](#) | [Setup](#) | [Preferences](#) | [Help](#) | [Logout](#)

Copyright © 1996, 2009, Oracle. All rights reserved.
Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
[About Oracle Enterprise Manager](#)

5. Select the default and temporary tablespaces for the new user. Do the following:
- a. Select the default tablespace:
 - 1) In the “Create User” form, click the **flashlight** button next to the **Default Tablespace** field.
 - 2) In the form that appears, select the **USERS** radio button.
 - 3) Click **Select**.

Search and Select: Tablespace Cancel Select

Search

Search for Tablespace

Results

Select	Tablespace
<input type="radio"/>	SYSAUX
<input type="radio"/>	SYSTEM
<input type="radio"/>	TEMP
<input type="radio"/>	UNDOTBS1
<input checked="" type="radio"/>	USERS

Cancel Select

- b. Select the temporary tablespace:
 - 1) In the “Create User” form, click the **flashlight** button next to the **Temporary Tablespace** field.
 - 2) In the form that appears, select the **TEMP** radio button.
 - 3) Click **Select**.
6. Assign system privileges to the new user. Do the following:
 - a. In the tab bar, click **System Privileges**.

Database Instance: contentDB > Users > Logged in As SYS

Create User

General Roles **System Privileges** Object Privileges Quotas Consumer Group Privileges Proxy Users

System Privilege Admin Option

No items found

General Roles **System Privileges** Object Privileges Quotas Consumer Group Privileges Proxy Users

Show SQL Cancel OK

Database | Setup | Preferences | Help | Logout

Copyright © 1996, 2009, Oracle. All rights reserved.
 Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
[About Oracle Enterprise Manager](#)

- b. Click **Edit List** at the top right corner of the list of privileges.
- c. In the “Available System Privileges” list, select **CREATE SESSION**, **CREATE TABLE**, **CREATE VIEW**, and **UNLIMITED TABLESPACE**, then click **Move**.
 The privileges appear in the “Selected System Privileges” list.
- d. Click **OK**.

ORACLE Enterprise Manager 11g Setup Preferences Help Logout

Database Control Database

Database Instance: contentDB > Users > Logged in As SYS

Modify System Privileges

Available System Privileges Selected System Privileges

ACCESS_ANY_WORKSPACE
 ADMINISTER_ANY_SQL_TUNING_SET
 ADMINISTER_DATABASE_TRIGGER
 ADMINISTER_RESOURCE_MANAGER
 ADMINISTER_SQL_MANAGEMENT_OBJECT
 ADMINISTER_SQL_TUNING_SET
 ADVISOR
 ALTER_ANY_ASSEMBLY
 ALTER_ANY_CLUSTER
 ALTER_ANY_CUBE

Move
 Move All
 Remove
 Remove All

CREATE_SESSION
 CREATE_TABLE
 CREATE_VIEW
 UNLIMITED_TABLESPACE

Cancel OK

Database | Setup | Preferences | Help | Logout

Copyright © 1996, 2009, Oracle. All rights reserved.
 Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
[About Oracle Enterprise Manager](#)

A message confirming the creation of the new user is displayed. The user appears in the list of users.

ORACLE Enterprise Manager 11g Database Control Setup Preferences Help Logout

Database Instance: contentDB > Database

Database Instance: contentDB > Logged in As SYS

Users

Object Type:

Search

Enter an object name to filter the data that is displayed in your results set.

Object Name:

By default, the search returns all uppercase matches beginning with the string you entered. To run an exact or case-sensitive match, double quote the search string. You can use the wildcard symbol (%) in a double quoted string.

Selection Mode:

Actions:

Select	UserName	Account Status	Expiration Date	Default Tablespace	Temporary Tablespace	Profile	Created	User Type
<input checked="" type="radio"/>	CSUSER	OPEN	Jul 3, 2012 7:16:53 AM EDT	USERS	TEMP	DEFAULT	Jan 5, 2012 7:16:53 AM EST	LOCAL

Next Step

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

Chapter 2

Creating and Configuring an MS SQL Server Database

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

This chapter contains the following section:

- [Creating a Database on MS SQL Server 2008 R2](#)

Creating a Database on MS SQL Server 2008 R2

To create and configure a database on MS SQL Server 2008 R2

1. Use the Windows Account Manager to create a new user account for the WebCenter Sites 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 WebCenter Sites 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**.
The database is created.
10. After the database has been created, turn on `READ_COMMITTED_SNAPSHOT` as shown below. For more information, refer to the vendor documentation.

```
ALTER DATABASE <your_db_name>  
SET ALLOW_SNAPSHOT_ISOLATION ON GO
```

```
ALTER DATABASE <your_db_name>  
SET READ_COMMITTED_SNAPSHOT ON GO
```

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

Chapter 3

Creating and Configuring an IBM DB2 9.7 Database

Use this chapter to set up a supported IBM DB2 database for your WebCenter Sites 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 9.7 for WebCenter Sites](#)

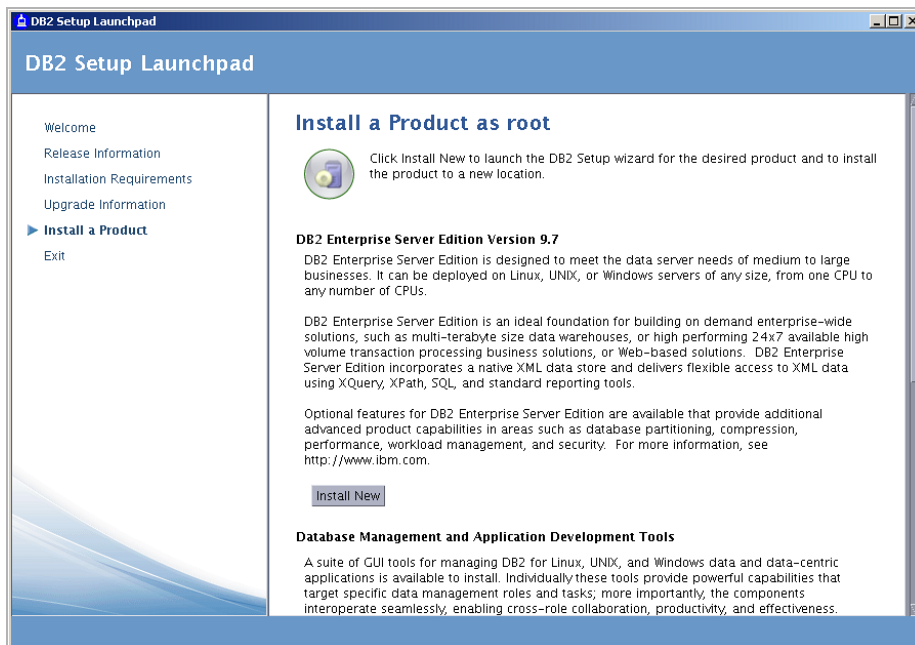
Installing and Configuring DB2 9.7 for WebCenter Sites

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

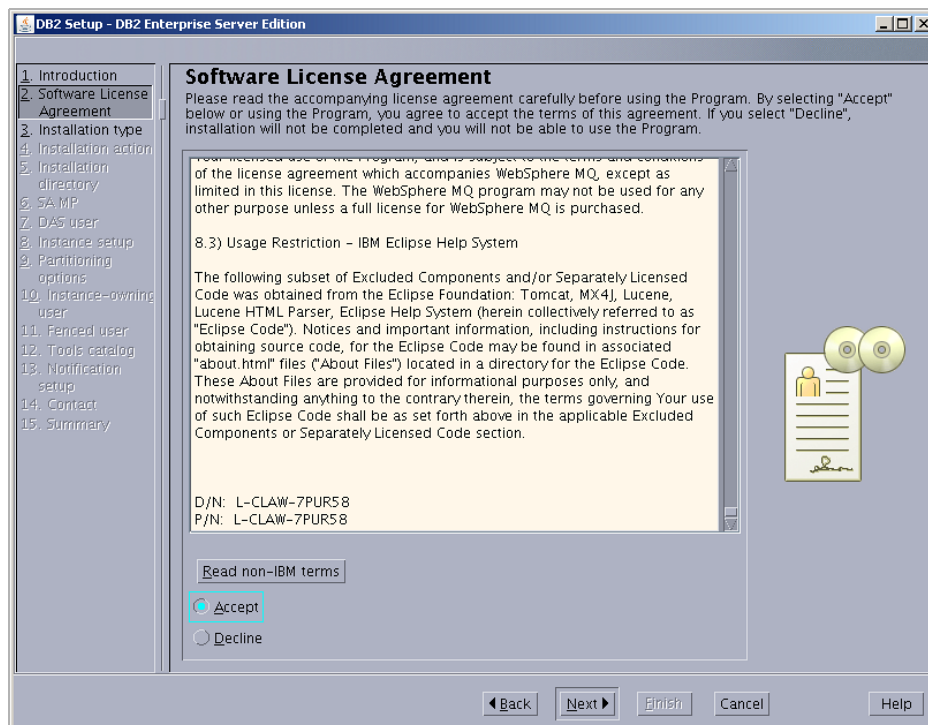
1. Uncompress the correct installation file for your distribution.
2. Run `./db2setup`
3. In the “Information Management Software” screen, select **Install a Product**.
4. Under “DB2 Enterprise Server Edition,” select **Install New**.



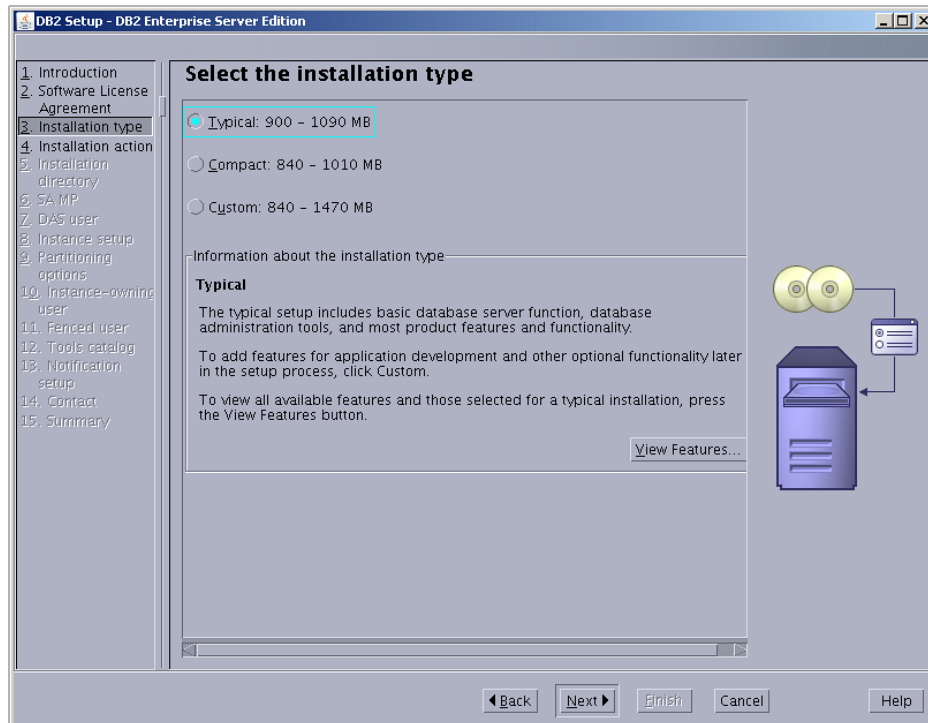
5. In the “Welcome to the DB2 Setup Wizard,” click **Next**.



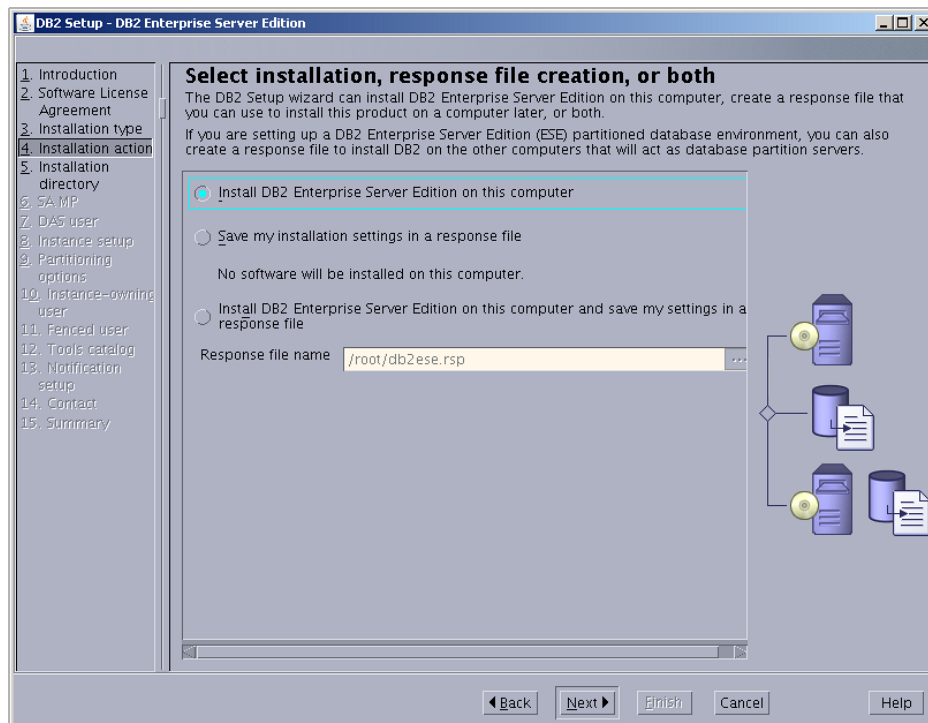
6. In the “Software License Agreement” screen, click **Accept**, then click **Next**.



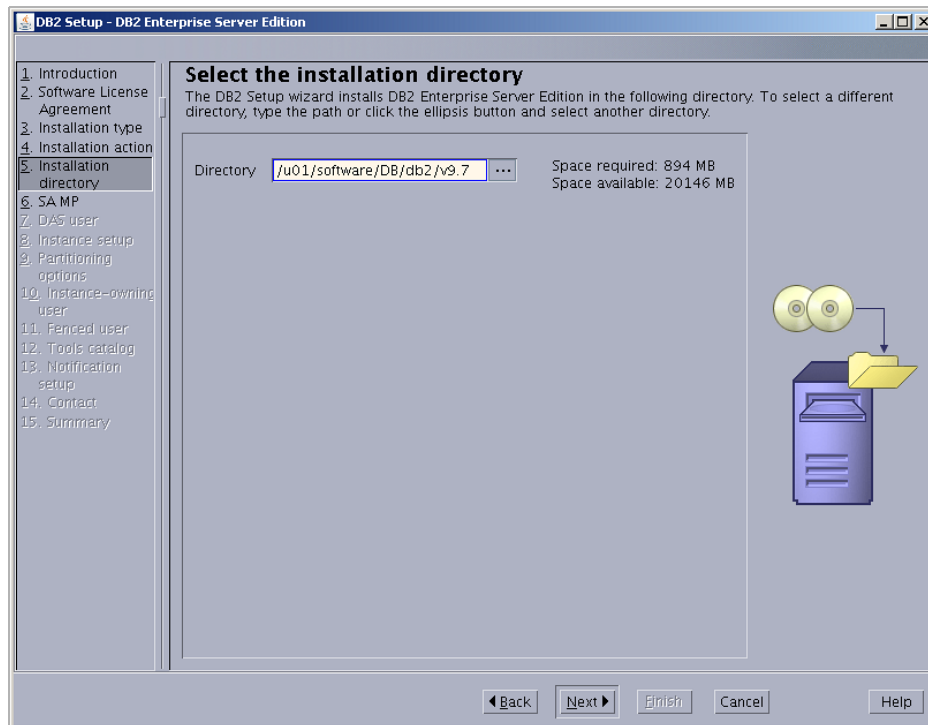
7. In “Select the Installation Type,” select **Typical** and click **Next**.



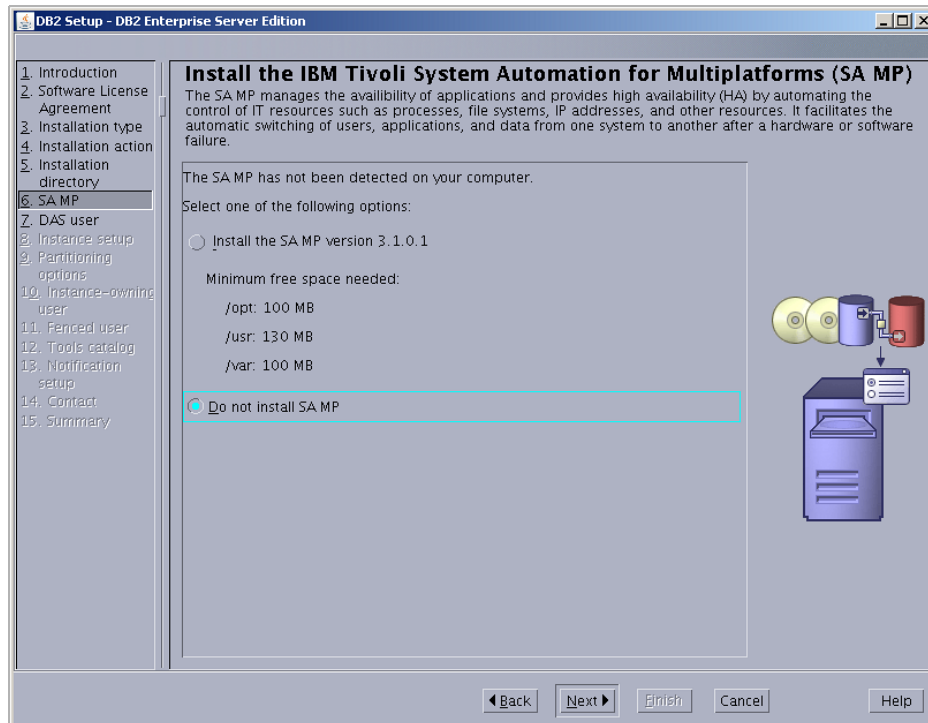
8. In “Select installation, response file creation, or both,” select **Install DB2 Enterprise Server Edition on this Computer** and click **Next**.



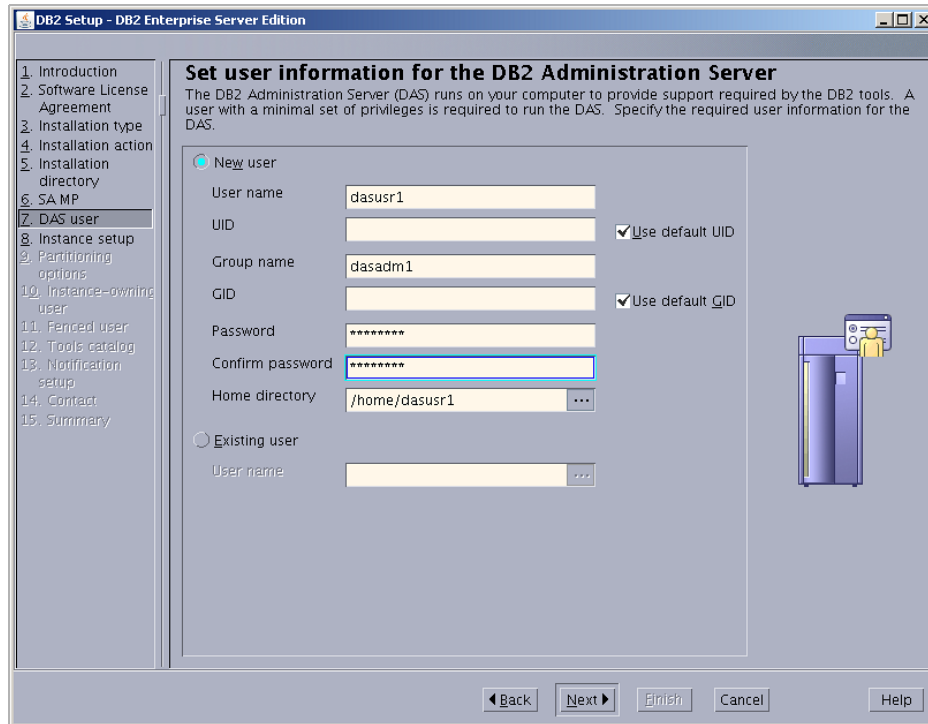
9. In “Select the installation directory,” either enter a directory or use the default and click **Next**.



10. In “Install the IBM Tivoli System Automation for Multiplatforms (SA MP),” select **Do not install SA MP**, unless “SA MP” is required by your environment.



11. 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**.



The screenshot shows the 'DB2 Setup - DB2 Enterprise Server Edition' window. The main title is 'Set user information for the DB2 Administration Server'. Below the title, there is a descriptive paragraph: 'The DB2 Administration Server (DAS) runs on your computer to provide support required by the DB2 tools. A user with a minimal set of privileges is required to run the DAS. Specify the required user information for the DAS.'

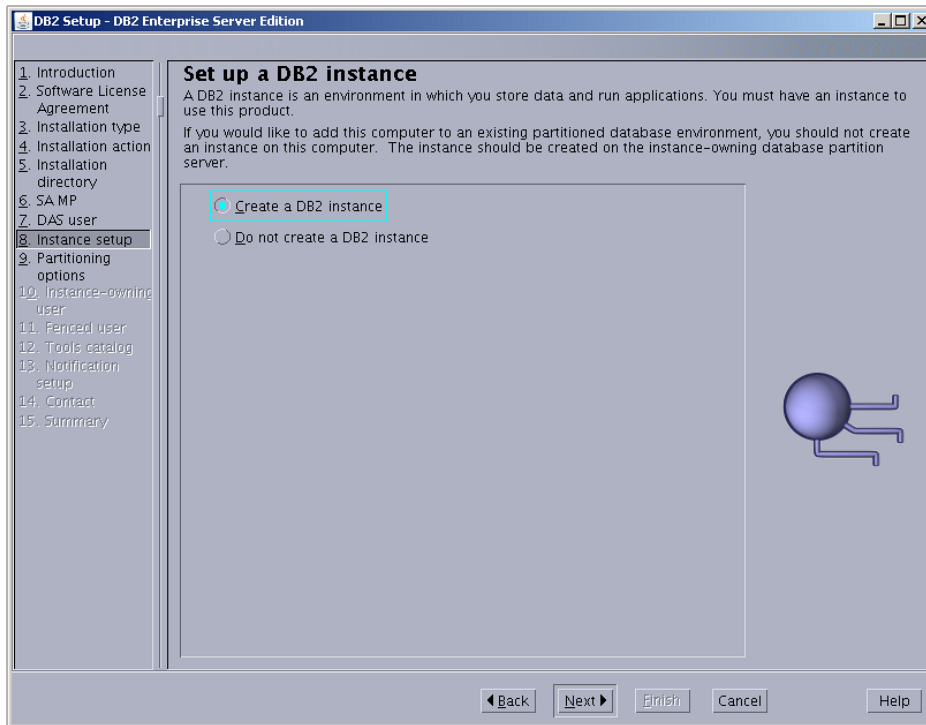
The 'New user' section is selected with a radio button. The fields are as follows:

- User name: dasusr1
- UID: (empty) with a checked 'Use default UID' checkbox.
- Group name: dasadm1
- GID: (empty) with a checked 'Use default GID' checkbox.
- Password: (masked with asterisks)
- Confirm password: (masked with asterisks, highlighted with a blue border)
- Home directory: /home/dasusr1

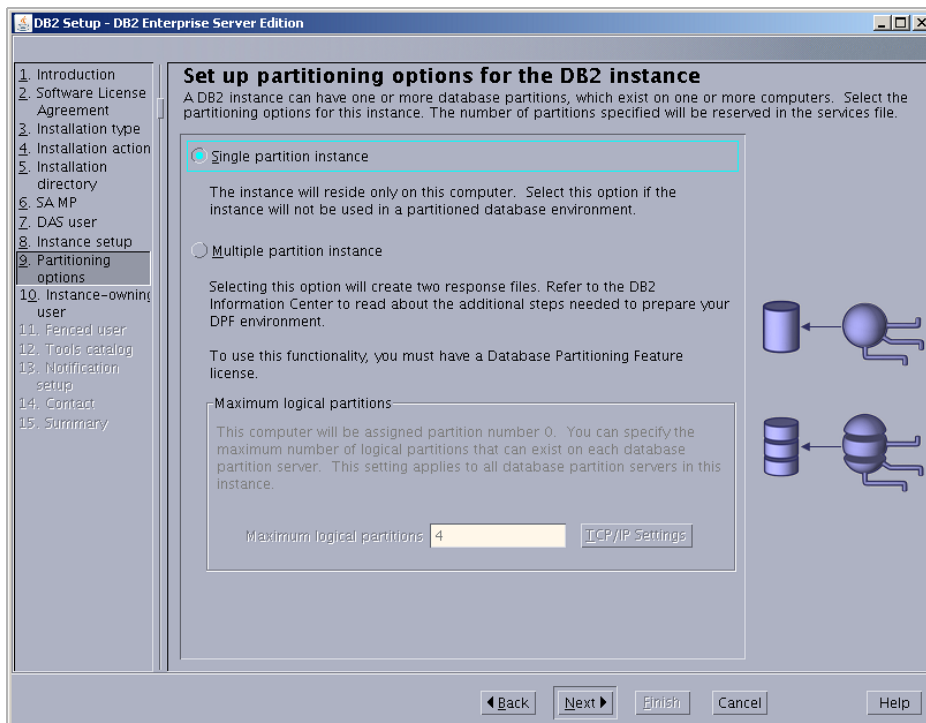
The 'Existing user' section is unselected. It has a 'User name' field with a dropdown arrow.

At the bottom of the window, there are buttons for 'Back', 'Next', 'Finish', 'Cancel', and 'Help'.

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



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



14. 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 - 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:

Confirm password:

Home directory: ...

Existing user

User name: ...

Navigation:

15. 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 - 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.

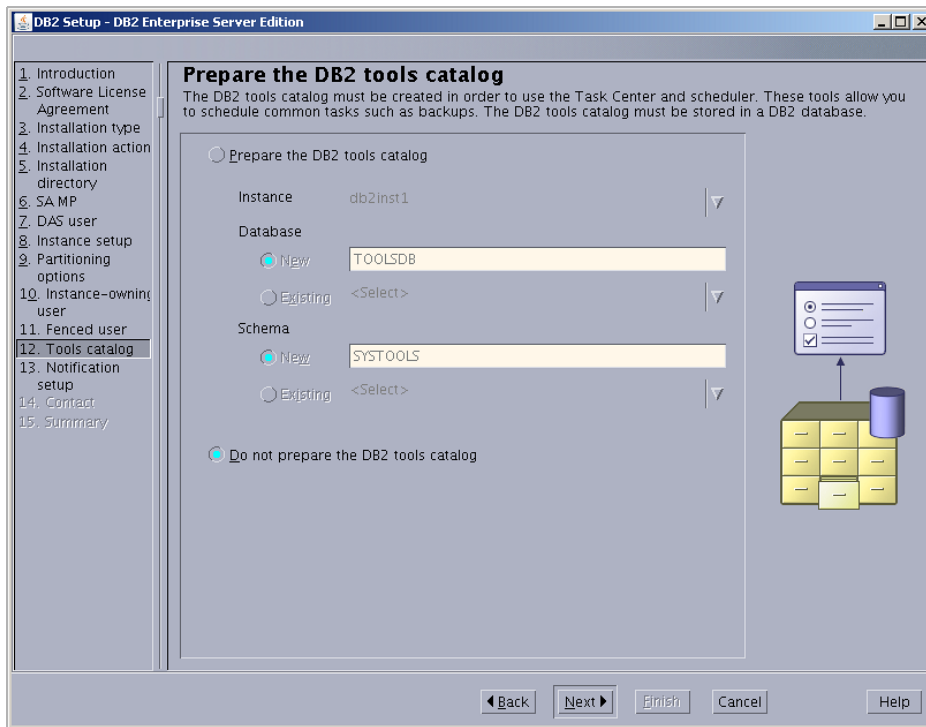
New user

User name: db2fenc1
UID: Use default UID
Group name: db2fadm1
GID: Use default GID
Password:
Confirm password:
Home directory: /home/db2fenc1

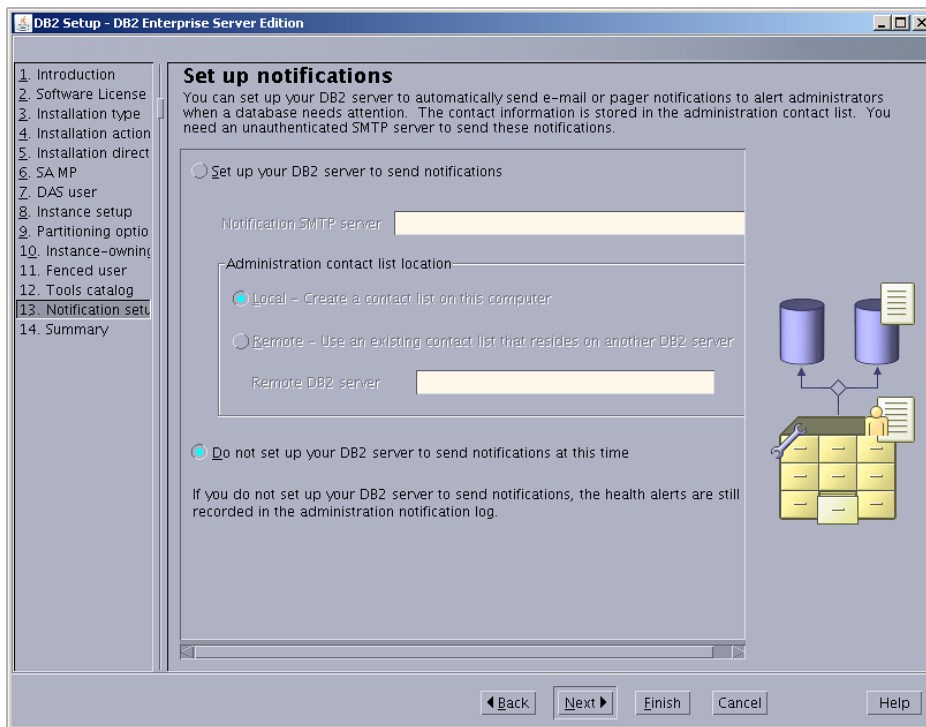
Existing user

User name:

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

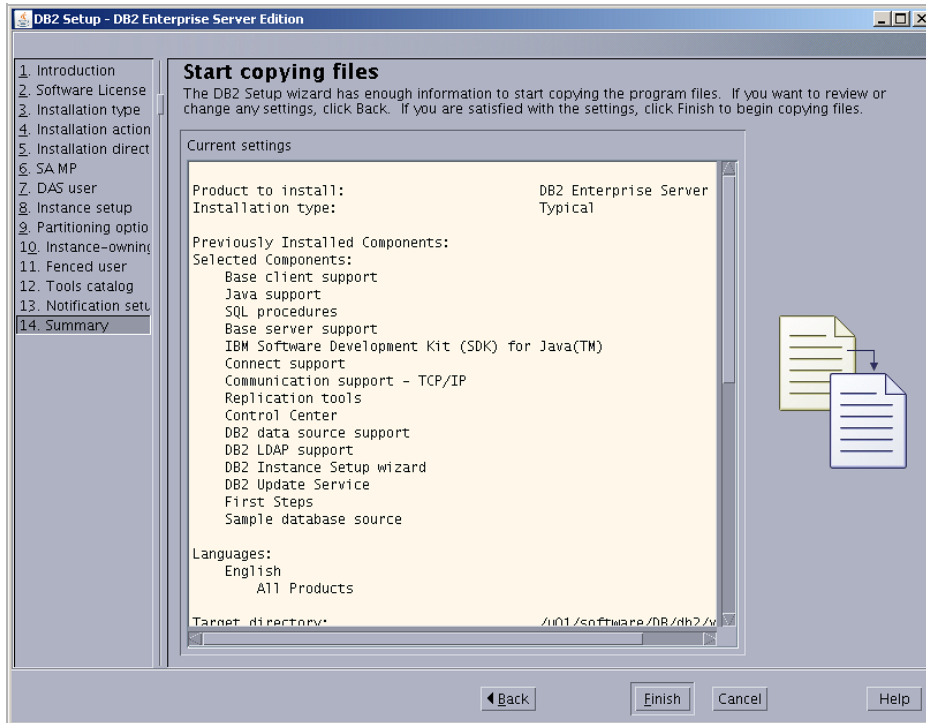


17. In “Set up notifications,” do one of the following:

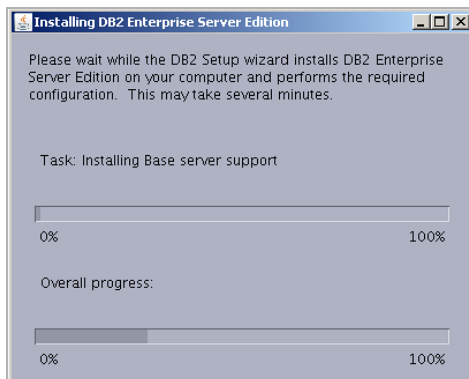


- If your system is a production server, select **Set up your DB2 server to send notifications**, enter a correct address for the local host, and click **Next**.

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



19. Allow the installation to proceed.

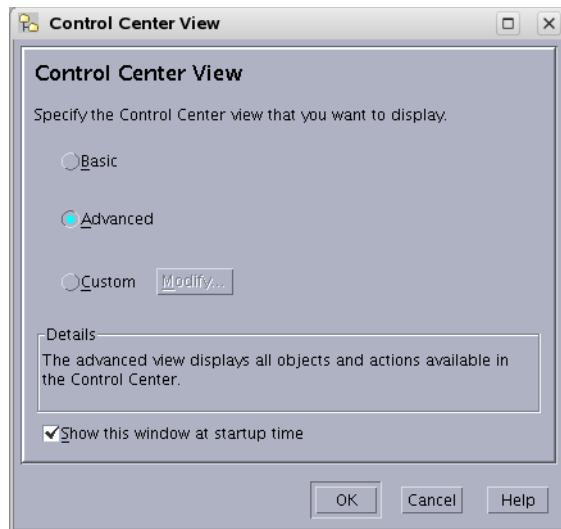


20. In “Setup has completed successfully,” read the notes, check the log tab, and click **Finish**.

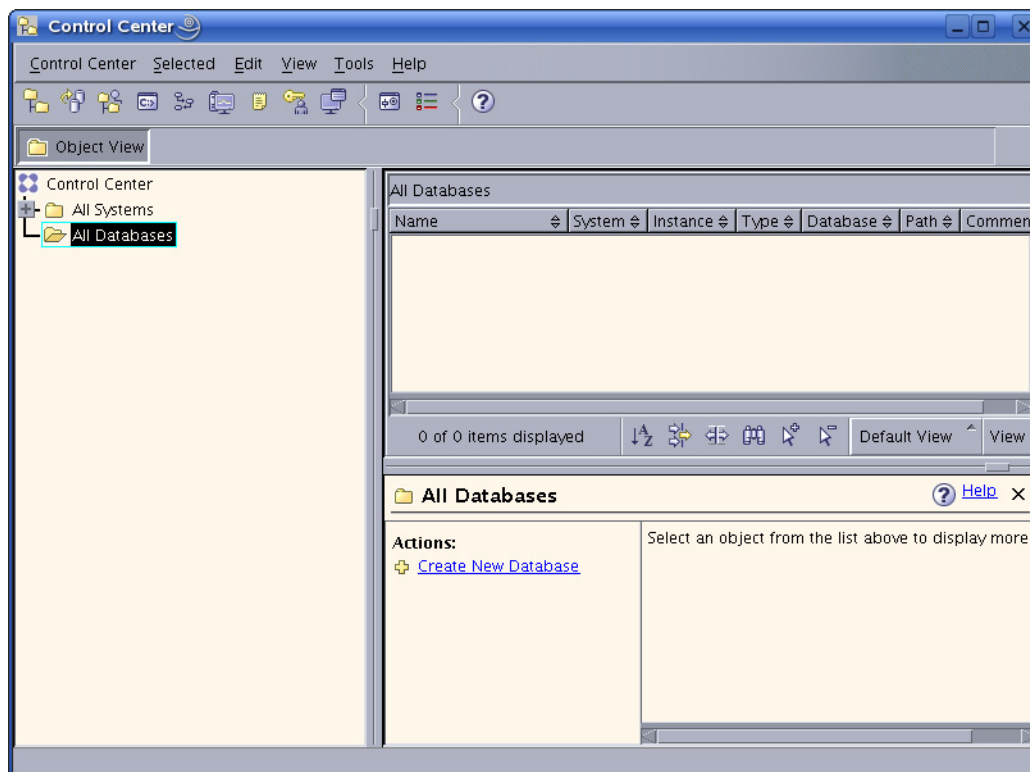
The installation of DB2 9.7 is now complete.

B. Create a New DB2 Database

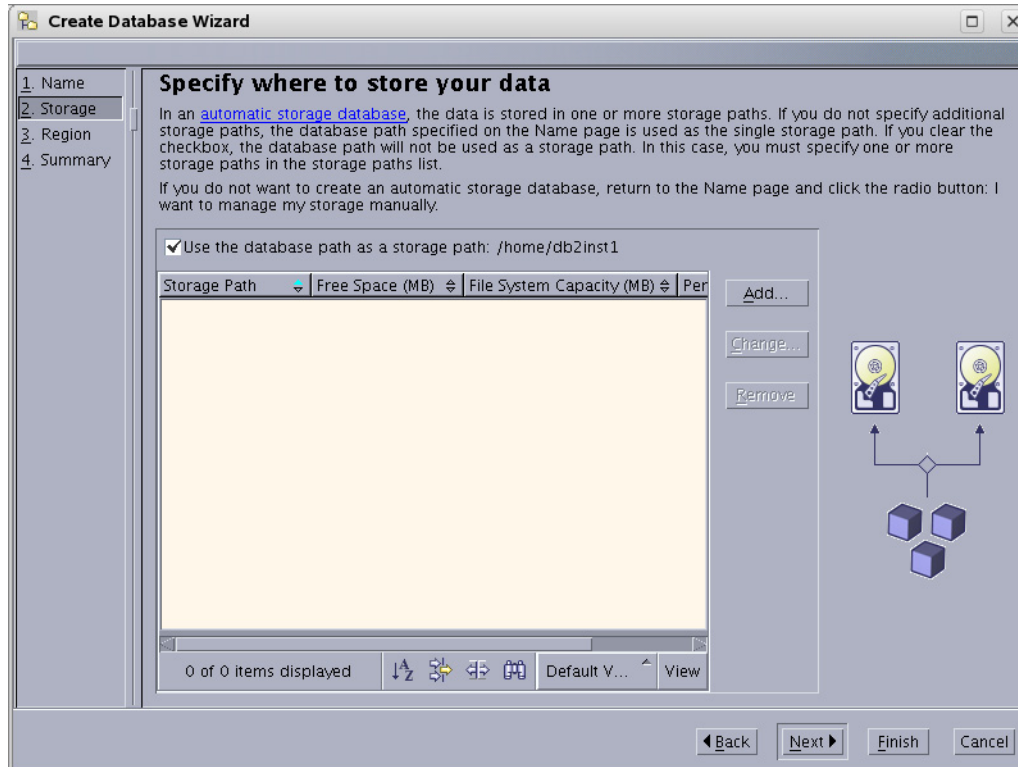
1. Log in as `db2inst1` (or your instance user created during the installation, [step 14](#)).
2. Navigate to: `./sqlllib/bin` and run `db2cc`
3. In the “Control Center View” screen, select **Advanced**.



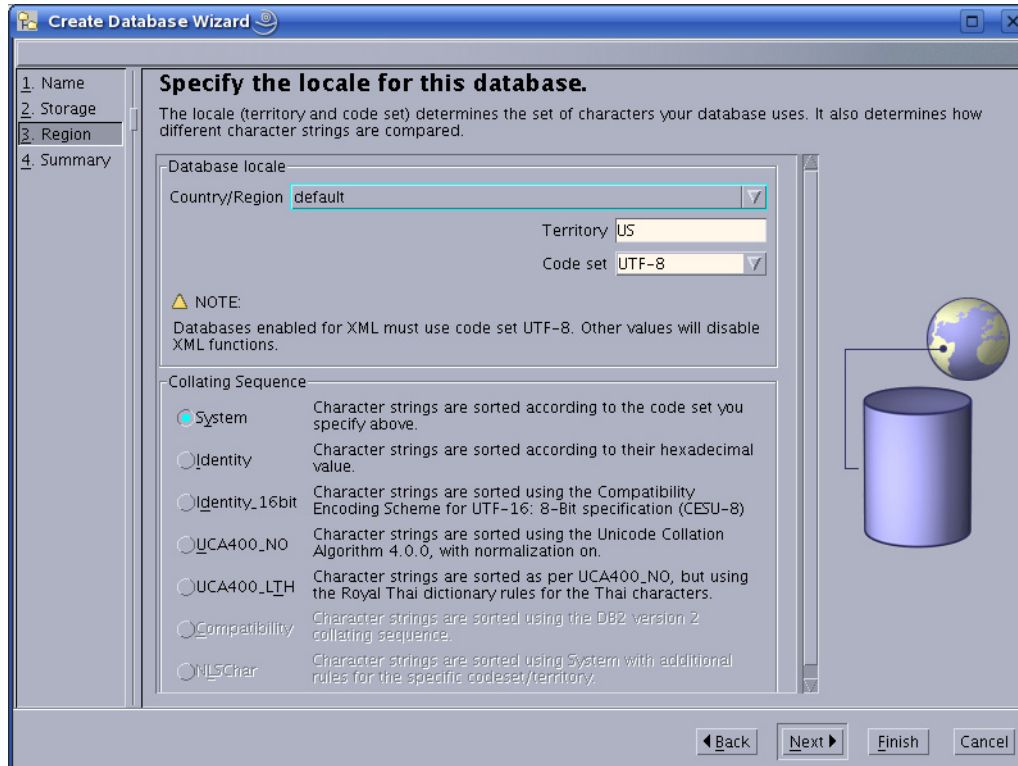
4. In the “Control Center,” open the application for creating a database:
 - a. Click the plus sign next to the tree option **All Systems**.



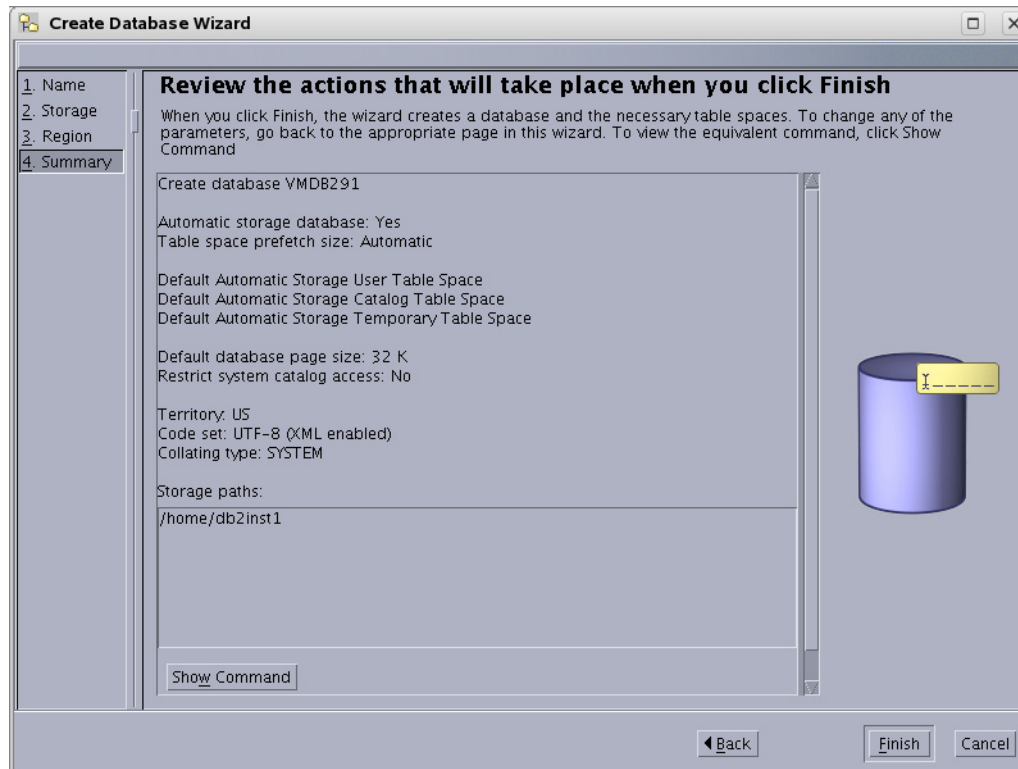
- In “Specify where to store your data,” click **Next** (a value is unnecessary, as we kept the default option of **Let DB2 manage my storage (automatic storage)**, on the previous page).



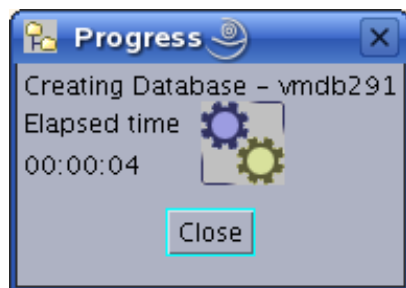
7. In “Specify the locale for this database,” ensure that the drop-down “Code set” displays UTF-8 and click **Next**.



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

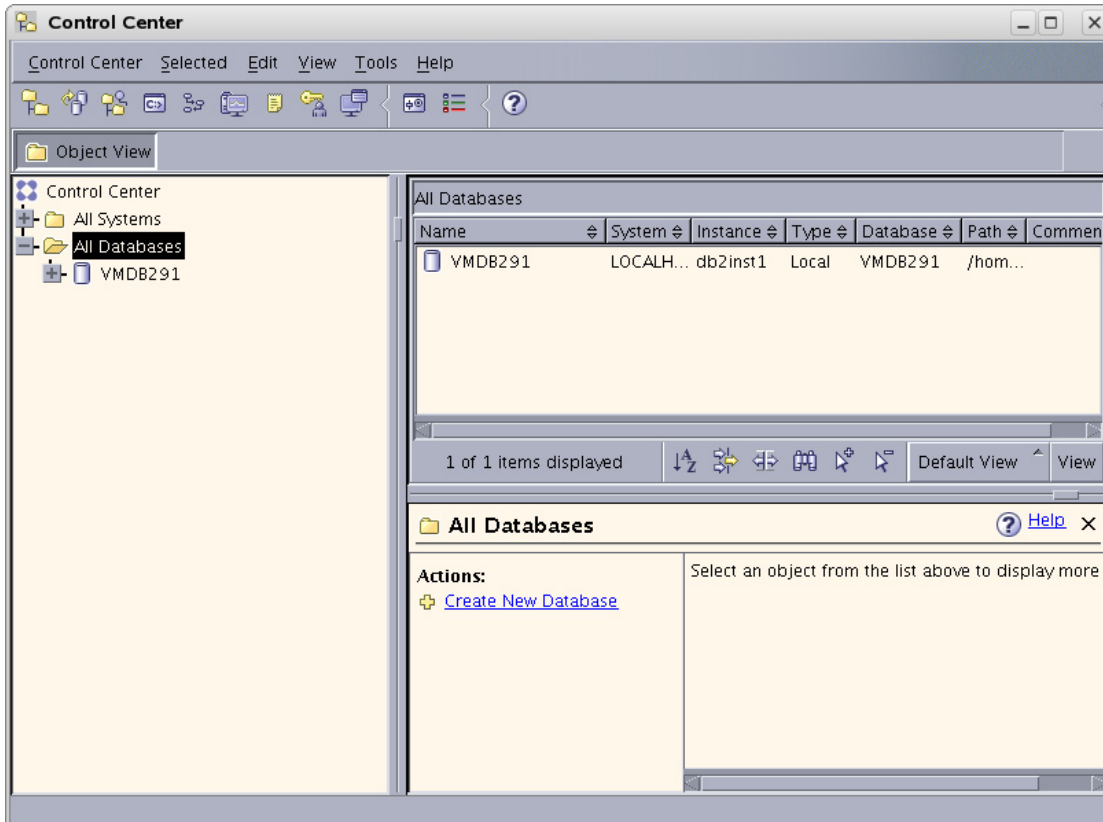


9. Allow the “Progress” window to complete creating the database. The window will close automatically when the database has been created.



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



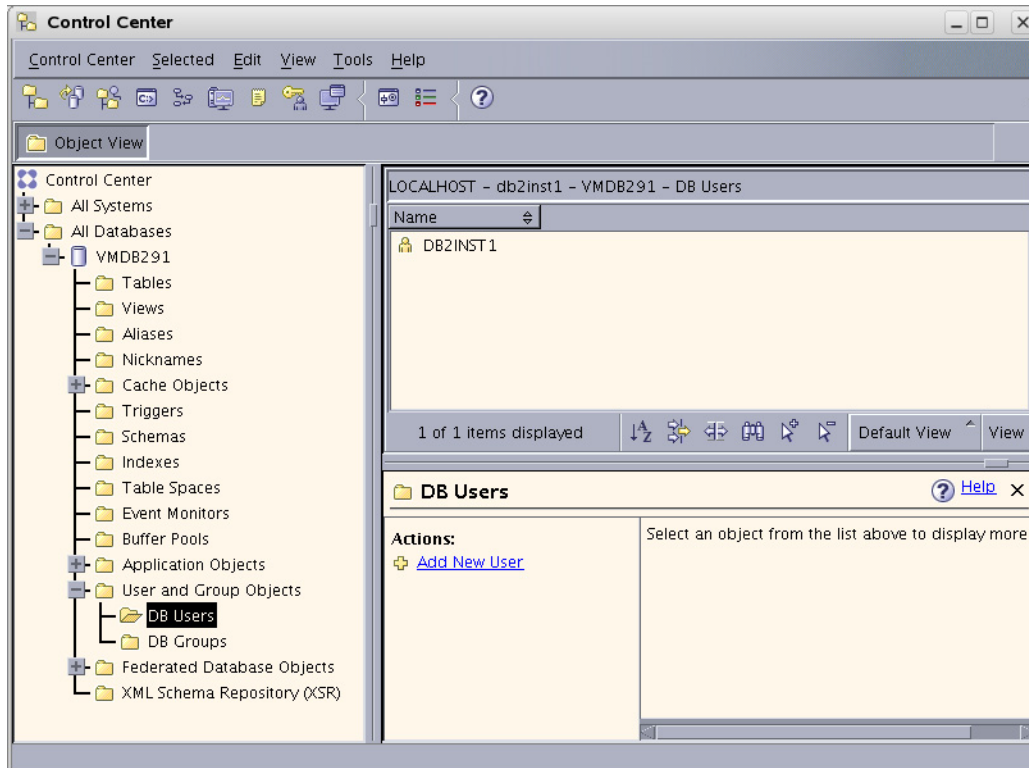
C. Create a User for the New Database

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 Oracle product.

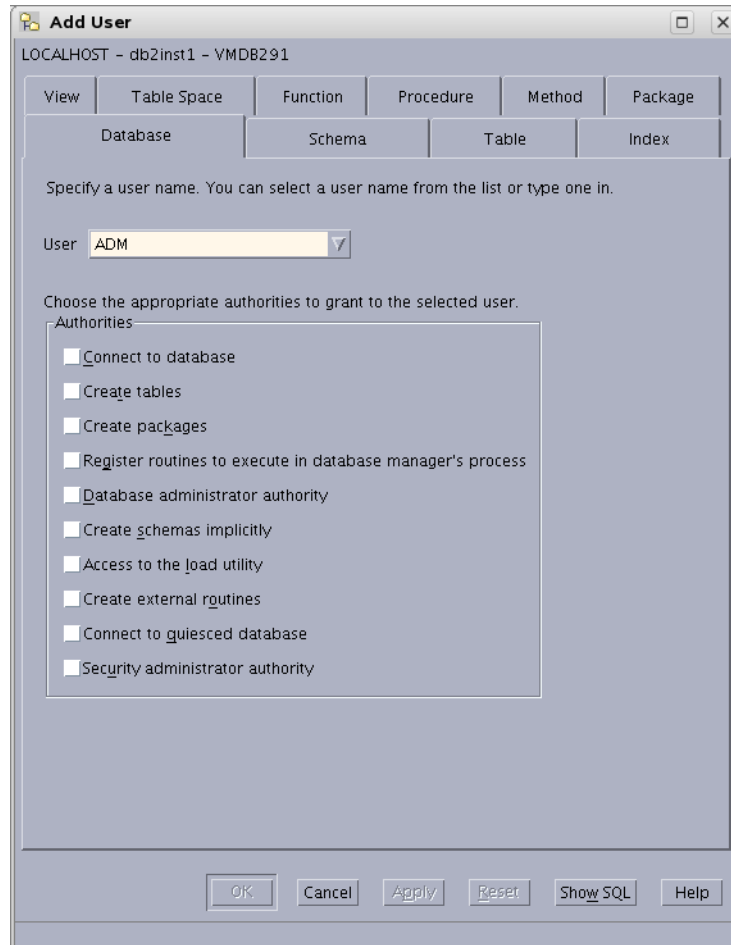
For example, to create a user named `csuser` on Linux:

```
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 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 49](#).
 - b. Under “Authorities,” select all check boxes.
 - c. Click **OK**.



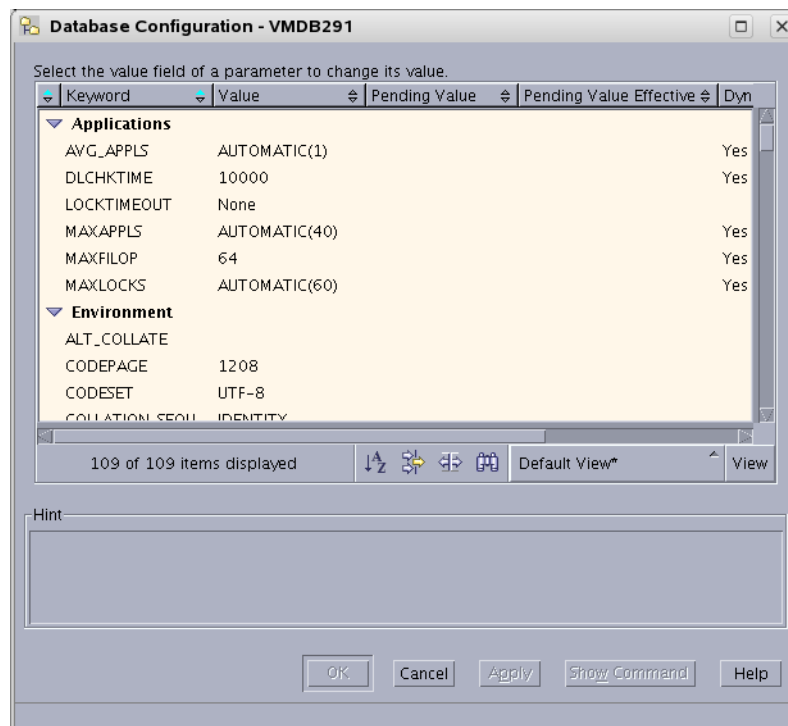
D. Configure the Database

1. Right-click 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
LOGFILSIZ	32768

Note: 32768 is the recommended value for this parameter. However, for large publishing jobs, this parameter may need further tuning to suit your setup.

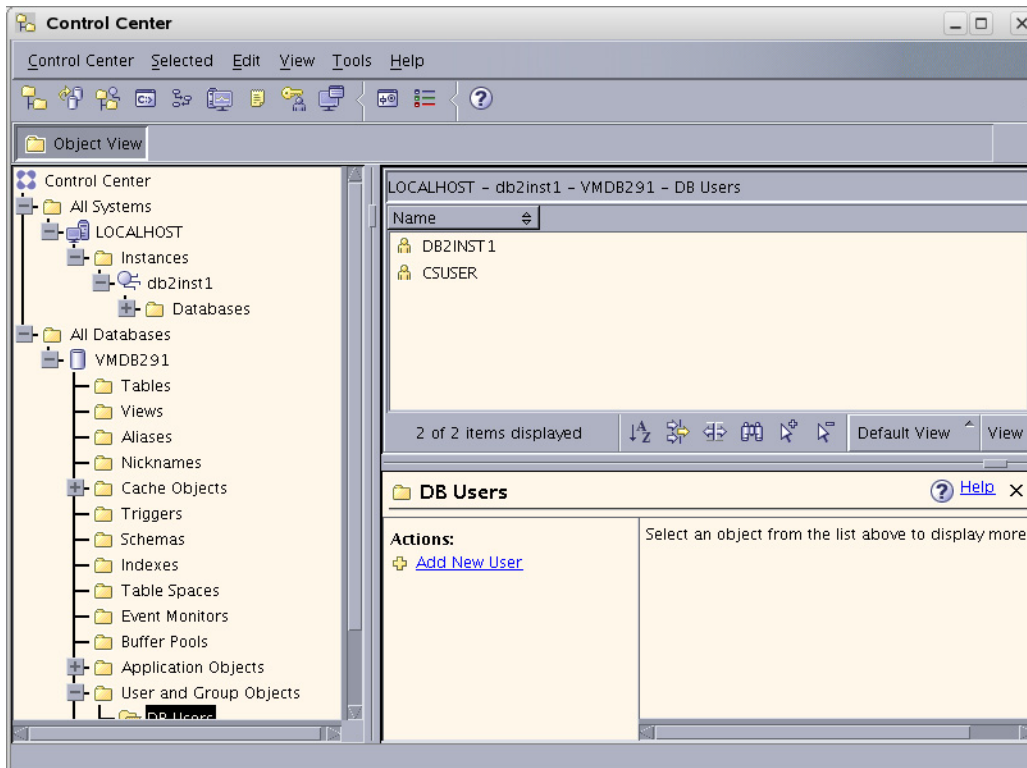
- b. Click **OK**.



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

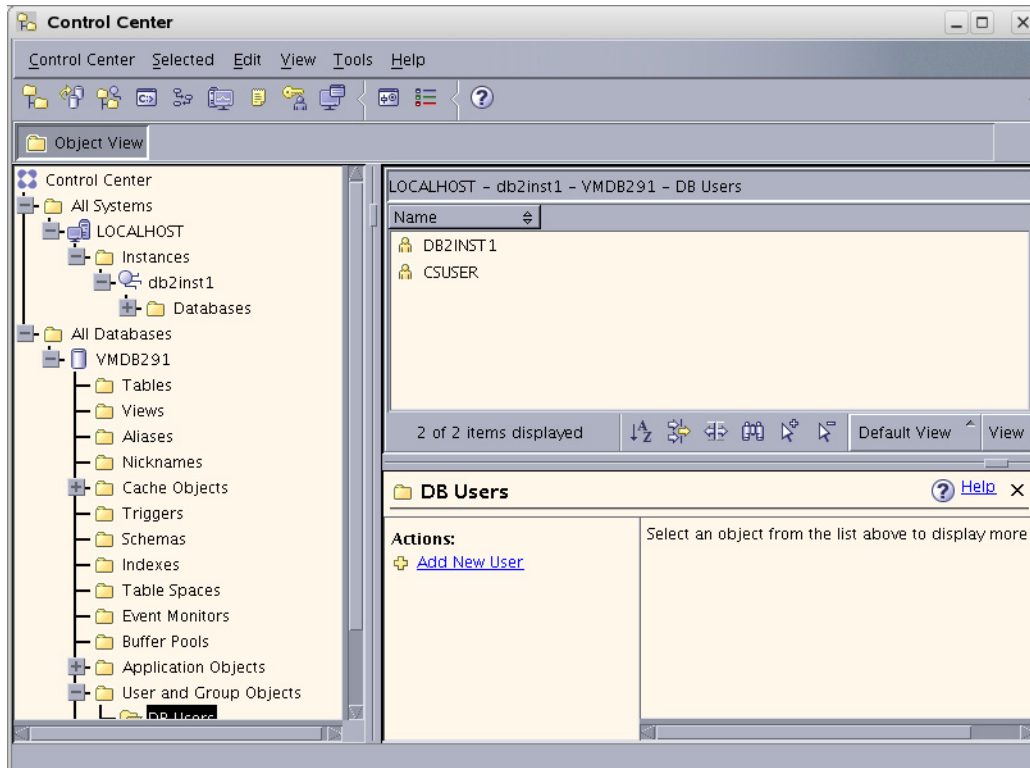
A status window flashes. *This does not mean that the operation has been completed.* Typically, you will need to wait 2 to 3 minutes for the system to restart.

4. Stop the instance:
 - a. Expand the following “Control Center” tree branch: **All Systems > LOCALHOST > Instances > name_of_your_instance**
 - b. Right-click 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 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 Oracle software product.

Part 2

Installing a Web Server

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

- [Chapter 4, “Worksheets for Documenting the Web Server Installation”](#)
- [Chapter 5, “Installing IBM HTTP Server 7.0”](#)
- [Chapter 6, “Installing Internet Information Services on Windows”](#)
- [Chapter 7, “Installing Apache on Solaris and Linux”](#)

Chapter 4

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

Table 2: Apache Web Server Parameters

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

Chapter 5

Installing IBM HTTP Server 7.0

This chapter contains the following sections:

- [Installation Steps](#)
- [Installing IHS with WebSphere Application Server on the Local Server](#)

Note

In this guide, IBM HTTP Server is referred to as “IHS.” WebSphere Application Server is referred to as “WAS.”

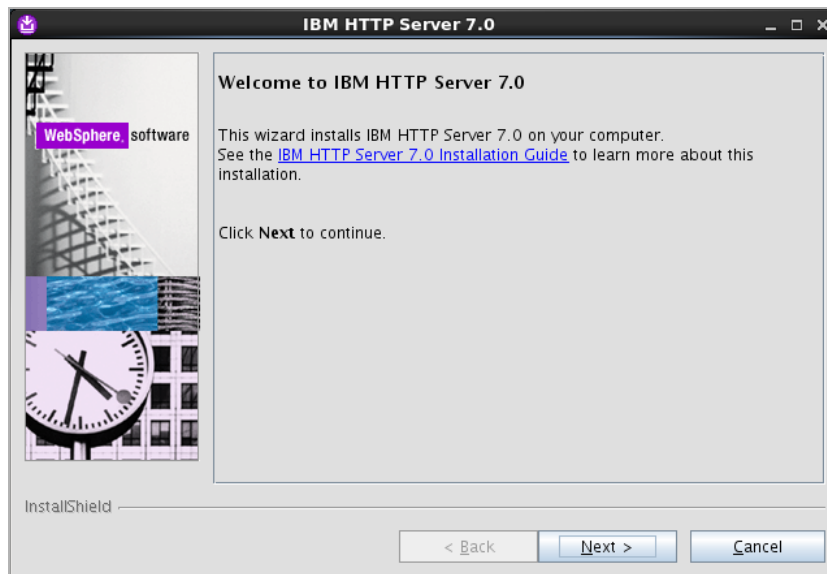
Installation Steps

1. Download the correct file, WebSphere Plugins, for your IBM operating system.
2. Extract the file to a temporary directory.
 - On Unix: `tar -xvf <file name>`
For example:

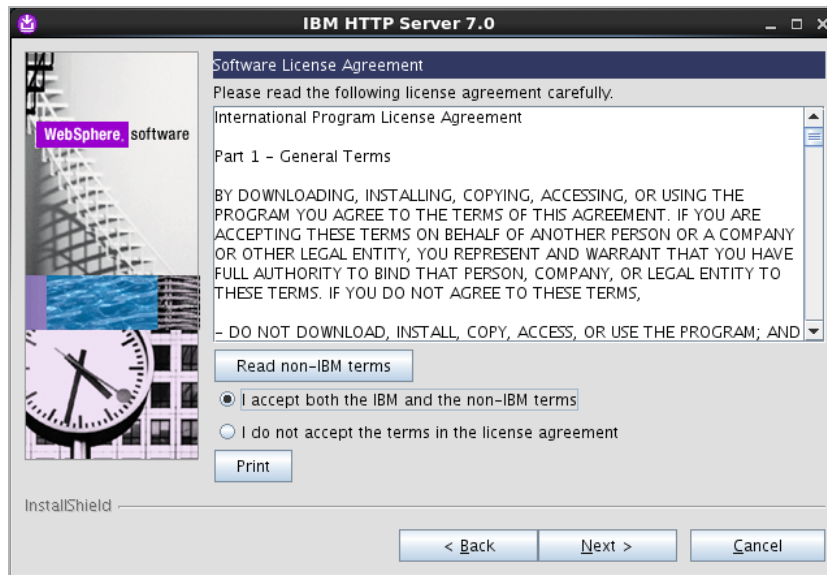
```
gzip -d C87XTML_Plugins.tar.gz
tar -xvf C87XTML_Plugins.tar
```
 - On Windows: `unzip <file name>`
For example:

```
unzip C87XTML_Plugins.zip
```
3. Change the directory to IHS/.
For example:

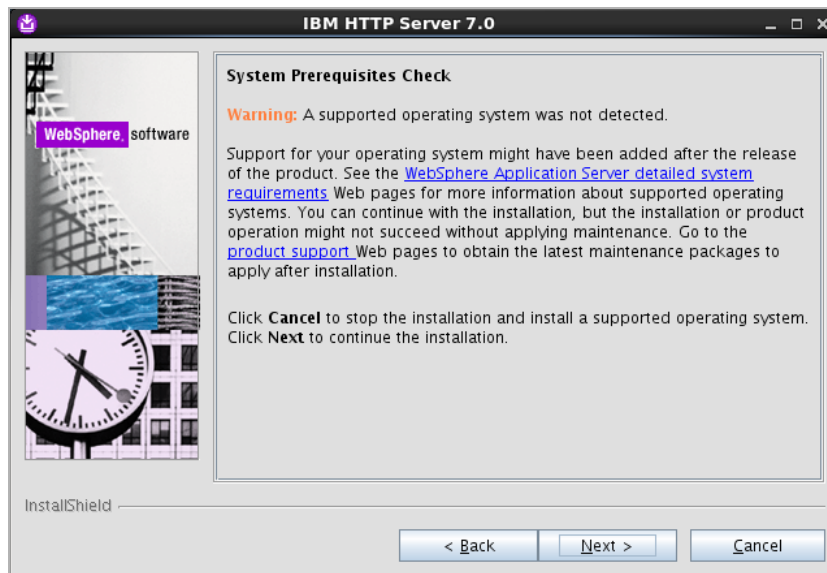
```
cd IHS/
```
4. Run the installer:
 - For Unix: `./install`
 - For Windows: `install.exe`
5. The “GUI” installer appears. Click **Next**.



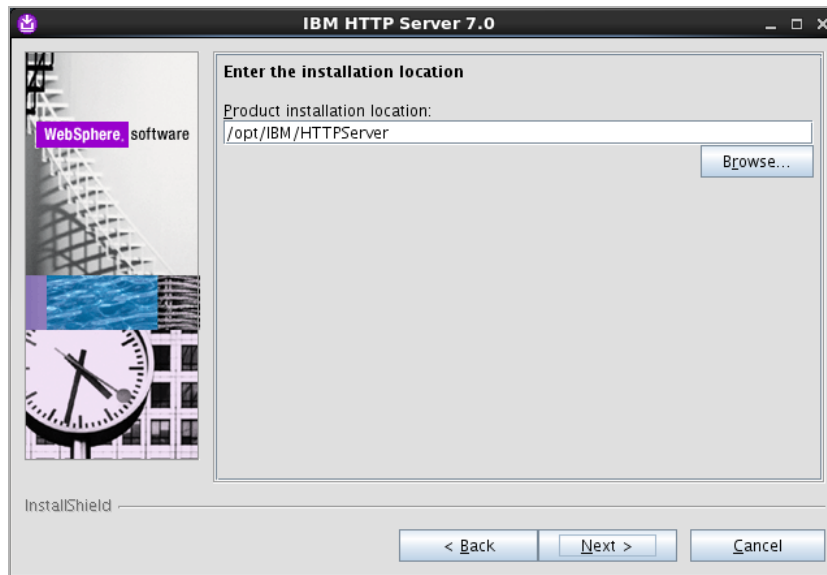
- Click the radio button **I accept the IBM and non-IBM terms**, to accept the license agreement and click **Next**.



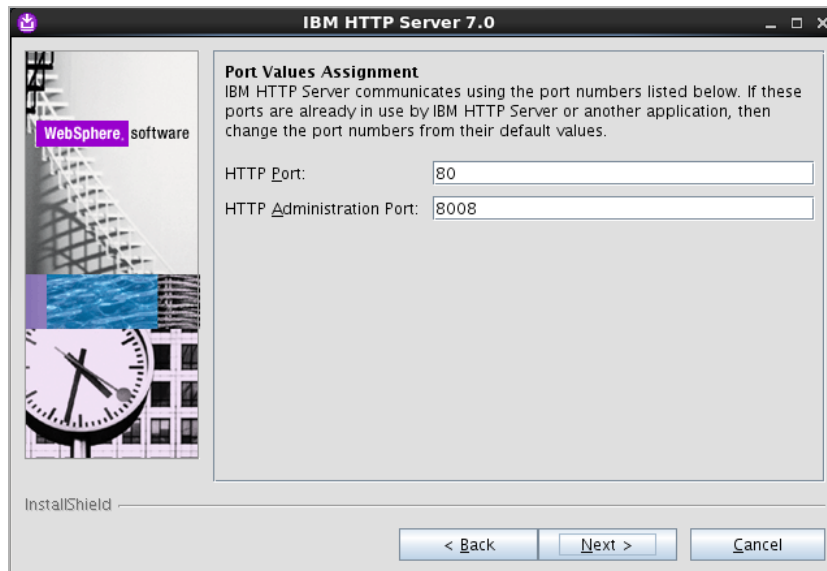
- In the "System prerequisites check" screen click **Next**.



8. In the “Enter the Install location” screen, select a location to install IHS 6.1 by using the **Browse** button, then click **Next**.



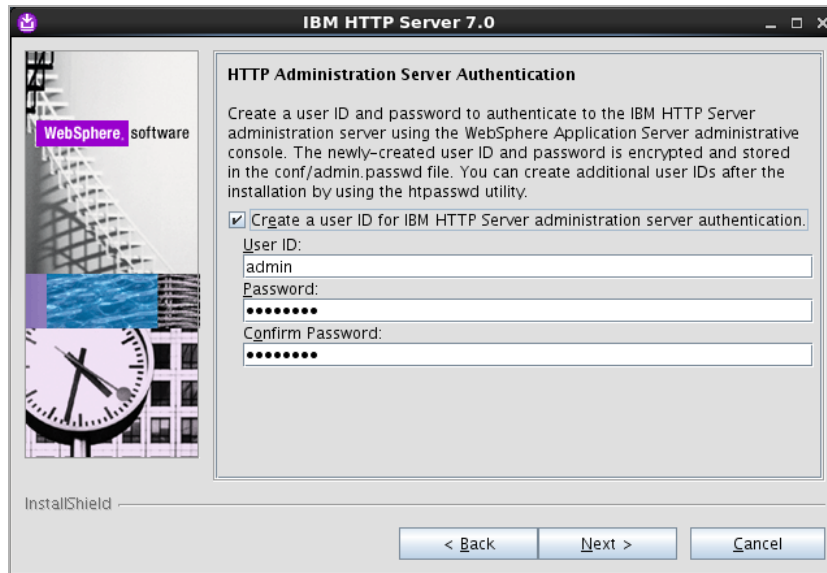
9. In the “Port Values Assignment” screen, enter the ports on which you wish to run IHS. Then click **Next**.



Note

We assume throughout this guide that you are using the default ports: 80 and 8008. If you have changed them, replace the values given with the ports you have selected.

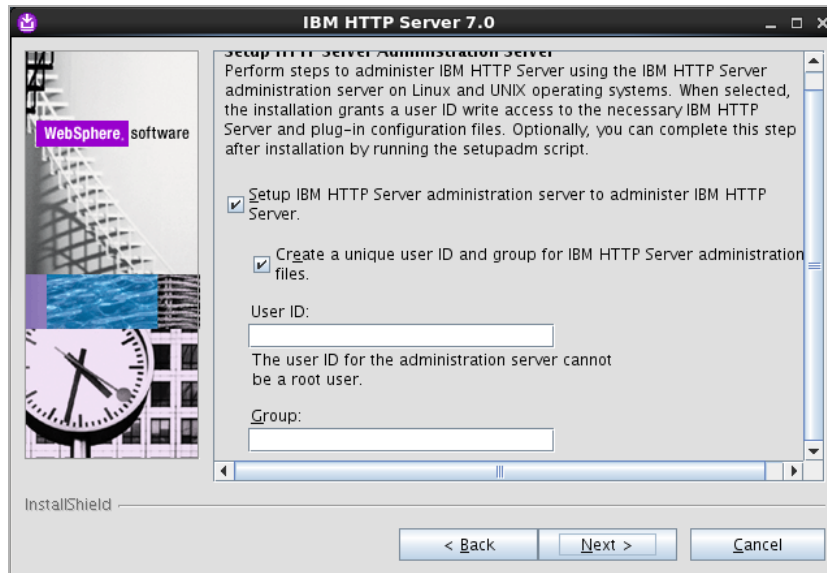
10. In the “HTTP Administration Server Authentication” screen:
 - a. Select **Create a user ID for IBM administration server authentication**.
 - b. Fill in the fields:
 - **User ID:** admin
 - **Password:** <enter and confirm>
 - c. Click **Next**.



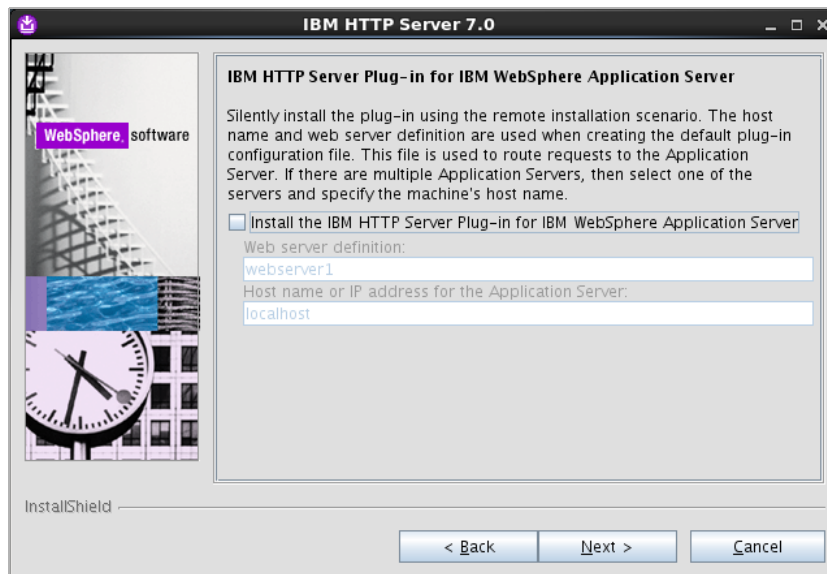
11. In the “Setup HTTP Administration Server” screen:
 - a. Select:
 - **Setup IBM HTTP administration server to administer IBM HTTP Server**
 - **Create a unique ID and Group for the IBM HTTP Server administration**
 - b. Fill in the fields. For example:
 - **User ID:** ihs7
 - **Group:** ihs7

Note

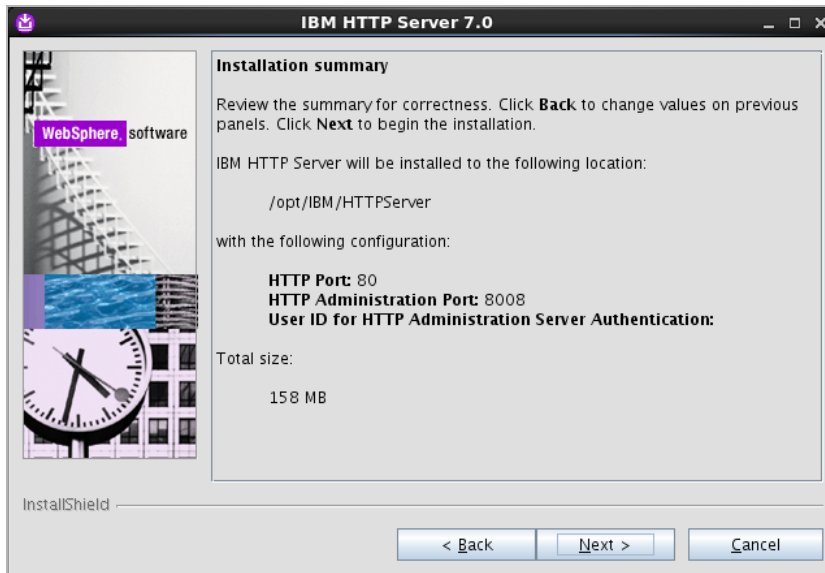
Record the unique name for the User ID and Group. They are needed to integrate with WAS. The User ID and Group can be anything you choose; ihs61 is only an example.

c. Click **Next**.

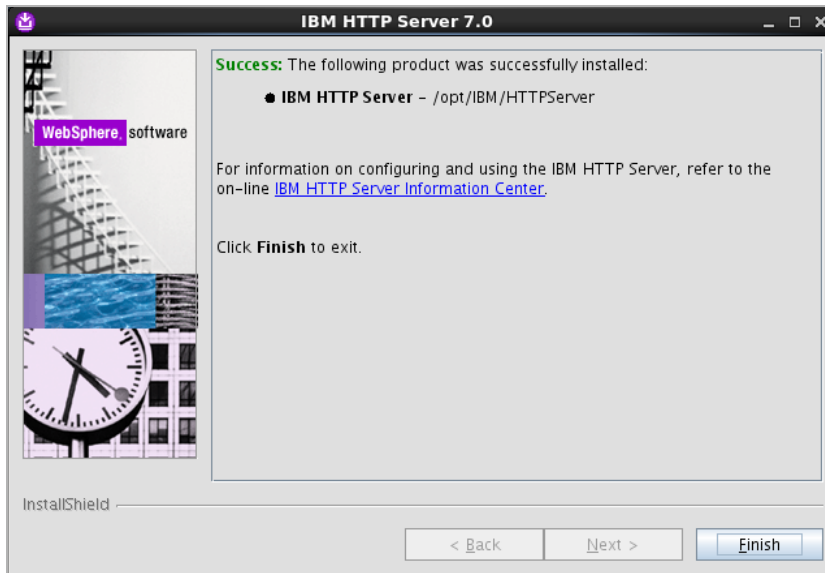
12. In the "IBM HTTP Server Plug-in for IBM WebSphere Application Server" screen:
- Select **Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server**.
 - Fill in the fields:
 - **Web server definition:** webserver1
 - **Host name:** Enter the hostname on which the application server is found.
 - Click **Next**.



13. In the “Installation summary” screen, click **Next**.



14. Allow the installer to finish.
15. When the installation is complete, click **Finish**.



Note

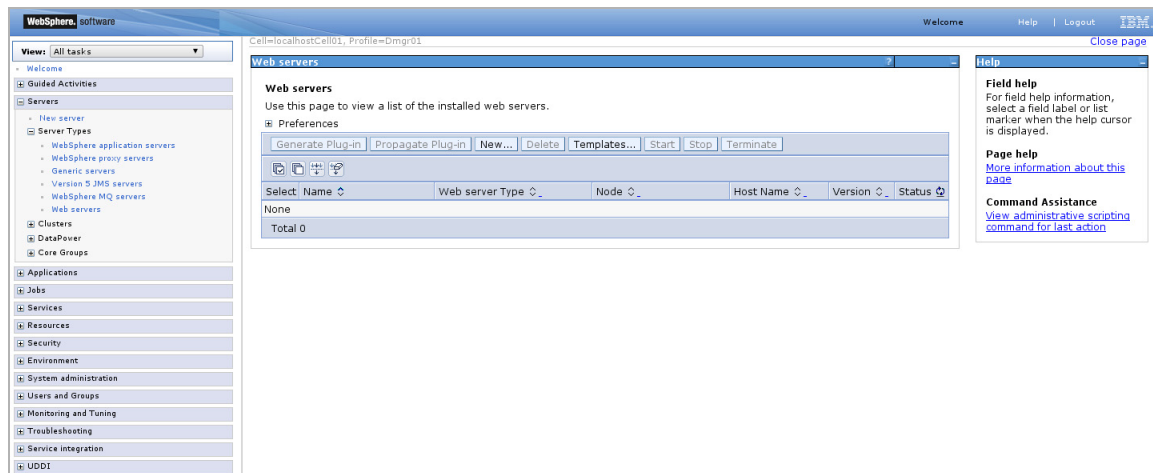
Now, you will need to use the update installer to patch IBM HTTP Server to the same version as WebSphere. Information on using the update installer can be found on the IBM site when you download updates. You will need to update both the IHS server and the IHS plugins separately. To do so, you will need the WebSphere and the plugin fixpacks.

Installing IHS with WebSphere Application Server on the Local Server

Note

It is preferable to perform this installation after WebCenter Sites is already installed. Then the plugin, `cfg.xml`, is automatically updated to include WebCenter Sites.

1. Browse to the WAS management console, for example:
`http://<DM_host>:<DM_console_port>/ibm/console`
where `<DM_host>` is the host name or IP address of the Deployment Manager host and `<DM_console_port>` is the port number on which the Deployment Manager console is listening for connections.
2. Log in to the Admin Site.
3. Select: **Servers > Web Servers.**

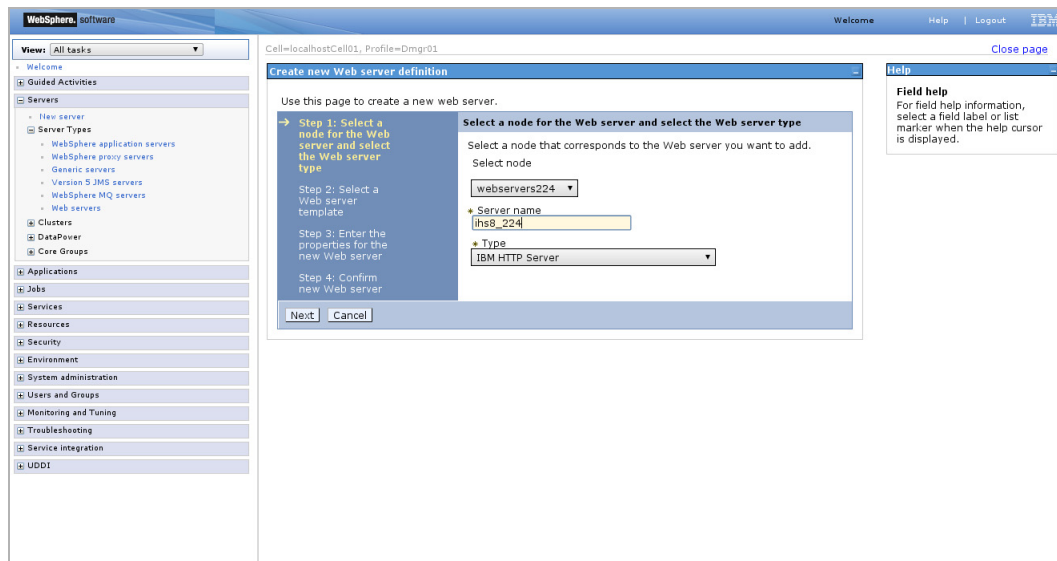


4. Click **New.**

5. To link IHS to WAS:

a. Fill in the fields:

- **Select node:** Select the node that you want to federate with (normally this is the node of the application server or cluster on which WebCenter Sites is installed).
- **Server name:** Enter the unique name for this web server, which was entered when you installed IHS.
- **Type:** Keep the type as **IBM HTTP Server**.

b. Click **Next**.6. In the “Select a Web server template” screen click **Next**.

7. On the “Property Page”:
 - a. Ensure that all entries are correct. The only entries that typically need to be changed are the locations for the IHS server and the Plugin Directory.
 - b. Click **Next**.

WebSphere software

Cell=localhostCell01, Profile=Dmgr01

Welcome Help Logout IBM

Close page

View: All tasks

Guided Activities

Servers

New server

Server Types

WebSphere application servers

WebSphere proxy servers

Generic servers

Version 5 JMS servers

WebSphere MQ servers

Web servers

Clusters

DataPower

Core Groups

Applications

Jobs

Services

Resources

Security

Environment

System administration

Users and Groups

Monitoring and Tuning

Troubleshooting

Service integration

UDDI

Create new Web server definition

Use this page to create a new web server.

Step 1: Select a node for the Web server and select the Web server type

Step 2: Select a Web server template

→ Step 3: Enter the properties for the new Web server

Step 4: Confirm new Web server

Enter the properties for the new Web server.

Port: 80

Web server installation location: /U01/software/Apps/IBM/HTTPServer

Plugin installation location: /U01/software/Apps/IBM/WebSphere/Plugins

Application mapping to the Web server: All

Enter the IBM Administration Server properties.

Administration Server Port: 8008

Username: admin

Password: *****

Confirm password: *****

Use SSL

Field help: For field help information, select a field label or list marker when the help cursor is displayed.

Previous Next Cancel

8. Confirm the new Web server, then click **Finish**.

WebSphere software

Cell=localhostCell01, Profile=Dmgr01

Welcome Help Logout IBM

Close page

View: All tasks

Guided Activities

Servers

New server

Server Types

WebSphere application servers

WebSphere proxy servers

Generic servers

Version 5 JMS servers

WebSphere MQ servers

Web servers

Clusters

DataPower

Core Groups

Applications

Jobs

Services

Resources

Security

Environment

System administration

Users and Groups

Monitoring and Tuning

Troubleshooting

Service integration

UDDI

Create new Web server definition

Use this page to create a new web server.

Step 1: Select a node for the Web server and select the Web server type

Step 2: Select a Web server template

Step 3: Enter the properties for the new Web server

→ Step 4: Confirm new Web server

Confirm new Web server

The following is a summary of your selections. Click the Finish button to complete the Web server creation. If there are settings you wish to change, click on Previous button to review the server settings.

Summary of actions:

New Web server entry "ihs8_224" will be created on node "webservers224"

Platform Type "Linux"

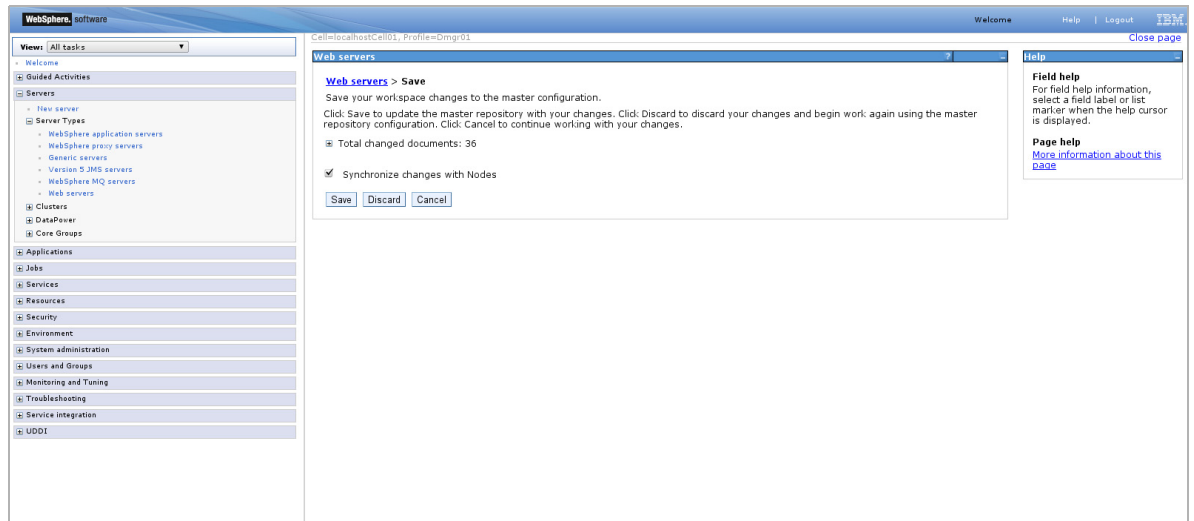
Web server installation root "/U01/software/Apps/IBM/HTTPServer"

Plugin installation root "/U01/software/Apps/IBM/WebSphere/PI"

Field help: For field help information, select a field label or list marker when the help cursor is displayed.

Previous Finish Cancel

9. Save the changes as requested.



10. You can now start and stop the web server from the WAS console, using the Web servers selection.

Chapter 6

Installing Internet Information Services on Windows

This chapter explains how to install and test Microsoft's Internet Information Services (IIS) 7.0/7.5 on Windows 2008 Server.

This chapter contains the following sections:

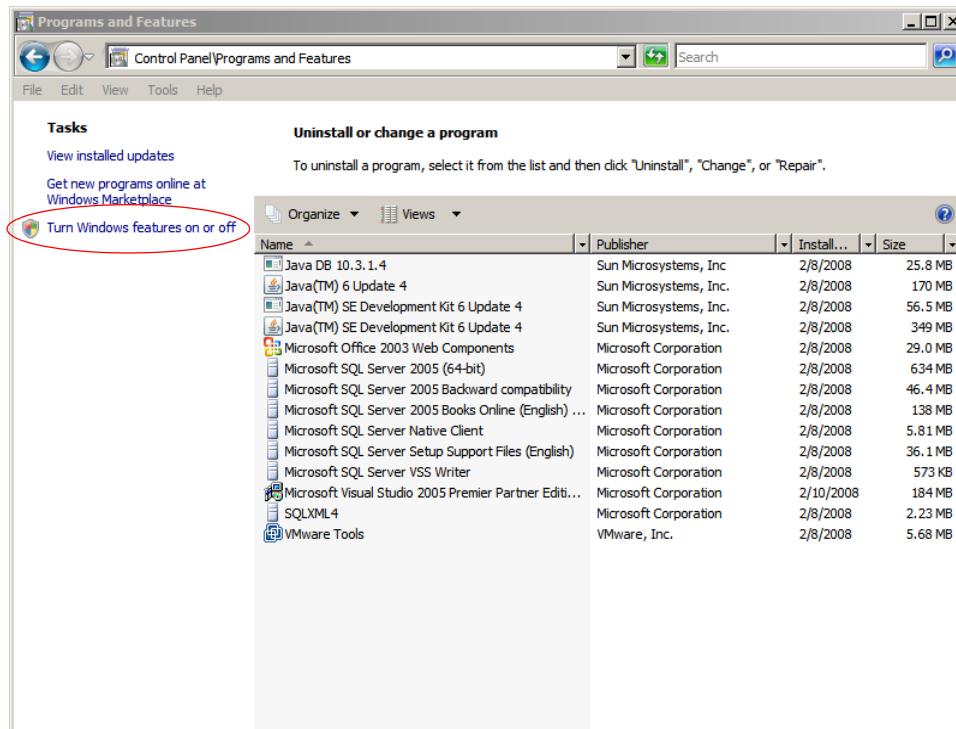
- [Step I. Install IIS](#)
- [Step II. Verify the Installation](#)
- [Step III. Starting and Configuring IIS](#)

Step I. Install IIS

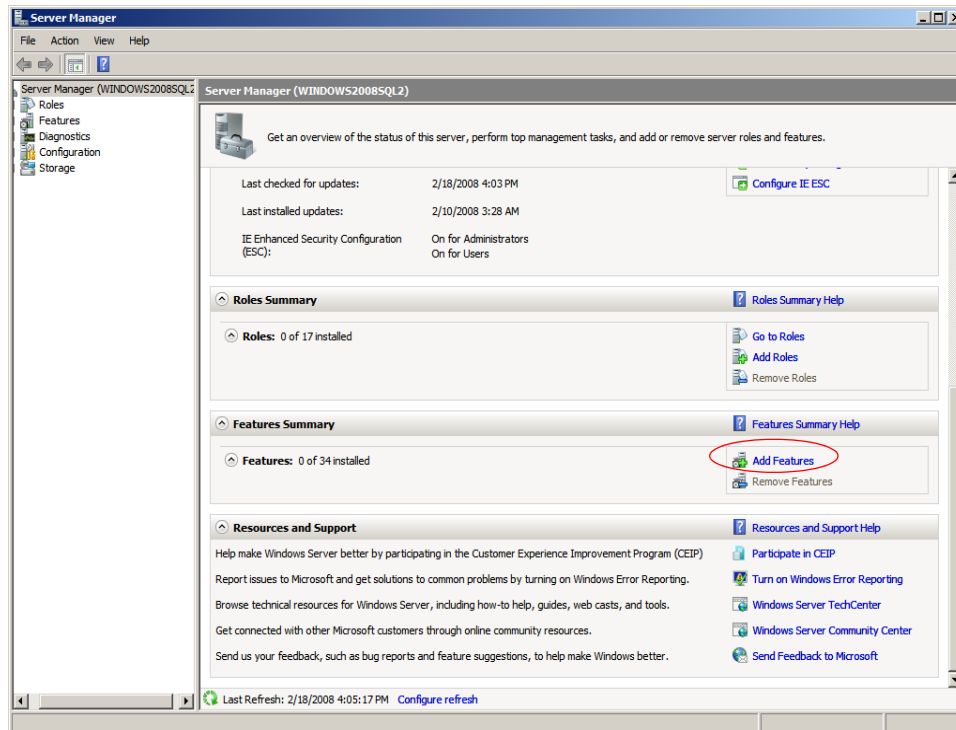
If IIS is not installed or is only partially installed, follow Microsoft's instruction for installing either IIS 7.0 on Windows 2008 Server or IIS 7.5 on Windows 2008 R2 Server.

Here is a summary of the instructions:

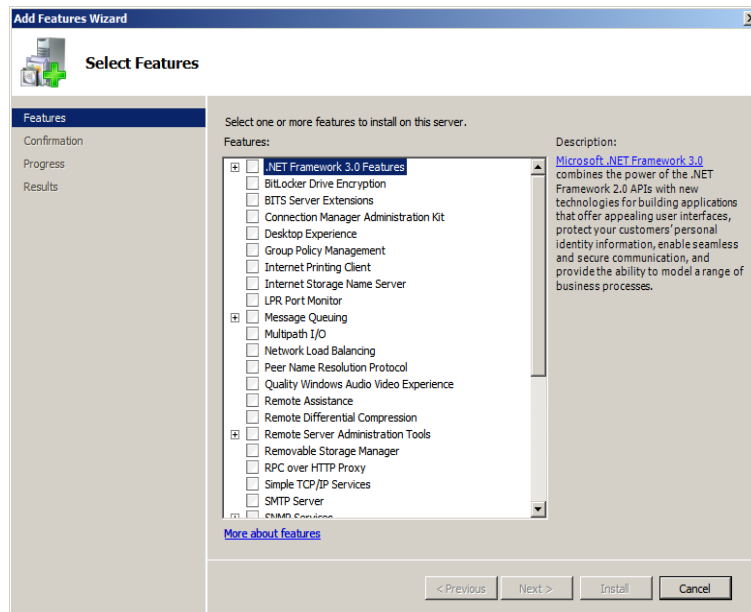
1. Select **Start > Settings > Control Panel**.
2. Select **Programs and Features**
3. Select **Turn Windows features on or off**.



4. In the “Server Manager” window, scroll down to the “Features Summary” section and click **Add Features**.



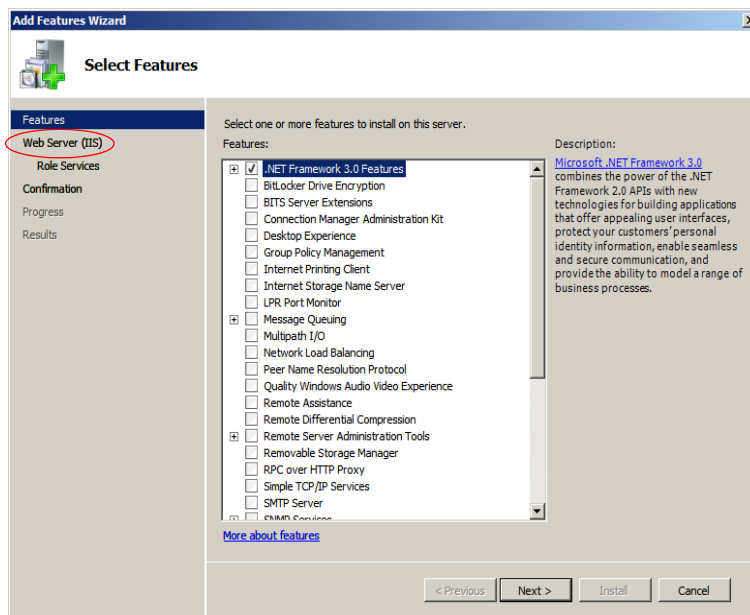
5. In the “Select Features” screen, select **.NET Framework 3.0 Features**.



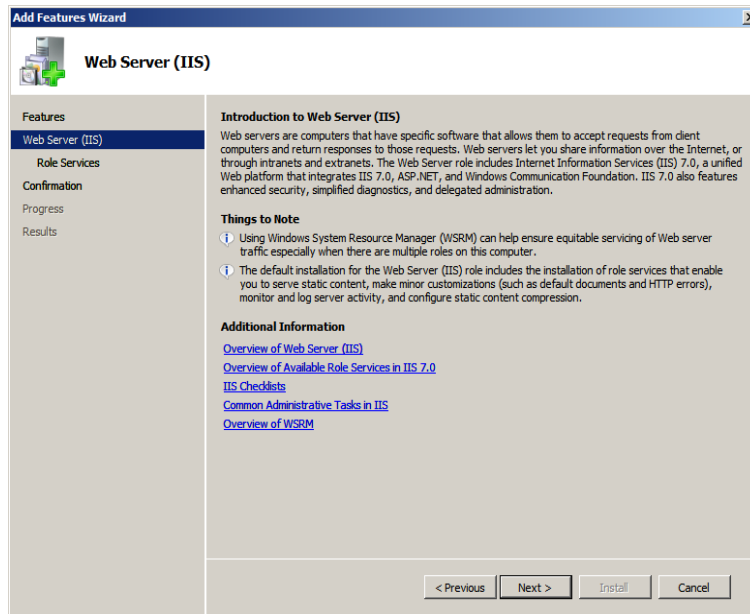
6. In the “Add Features Wizard” dialog box, select **Add Required Role Services**.



7. The **Web Server (IIS)** option appears in the “Add Features Wizard.” Click **Next**.



8. In the “Introduction to Web Server (IIS)” screen, click **Next**.

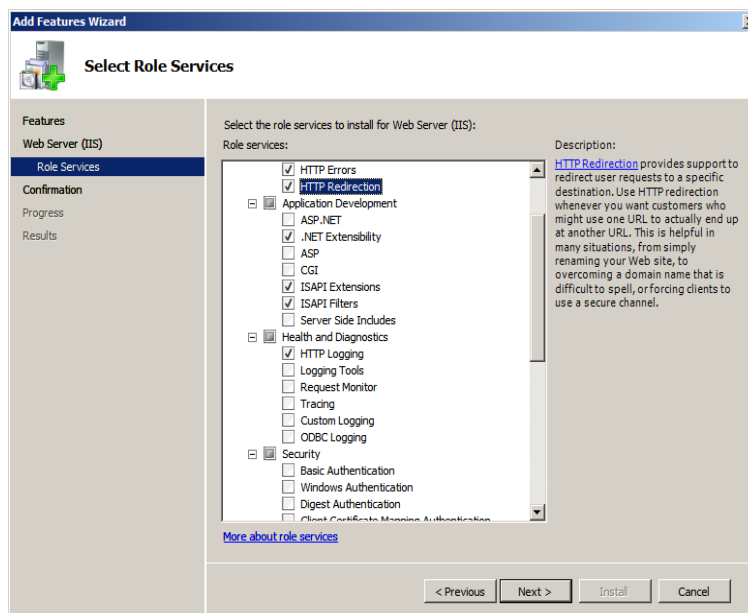


9. In the “Select Role Services” screen:

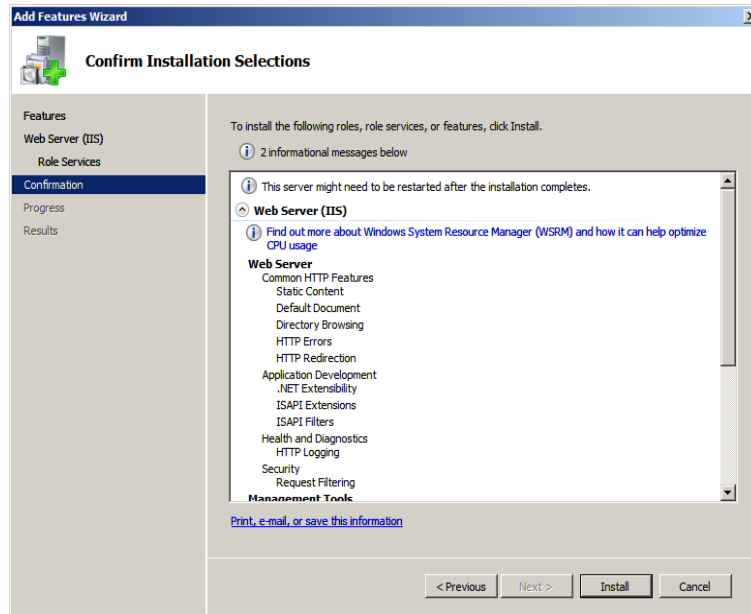
- a. Select the following:

- **Common HTTP Features**
- **ISAPI Extensions**
- **ISAPI Filters**
- **HTTP Logging**
- **Management Tools**
- Any other roles that are required for your installation, such as **HTTP Redirection**

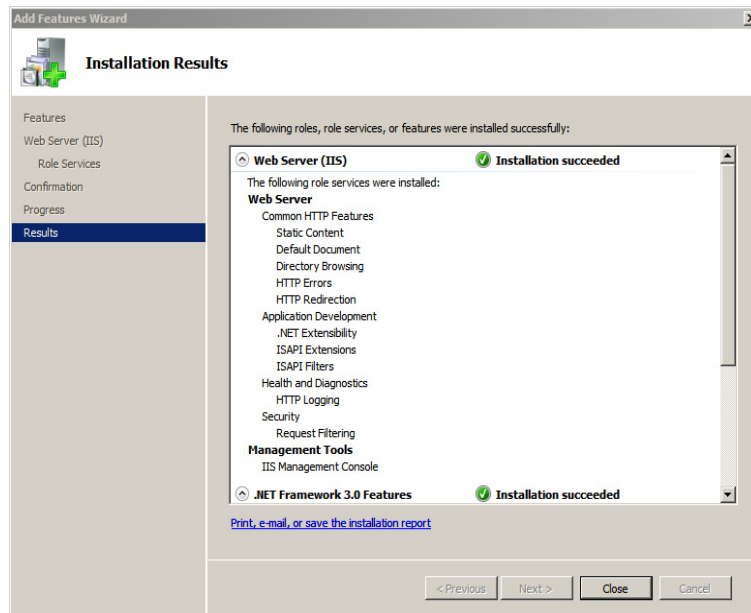
- b. Click **Next**.



10. In the “Confirm Installation Selections” screen, confirm your choices and click **Install**.



11. Allow the installation to complete, then review the results.
12. Click **Close**.



13. It is suggested at this point to reboot, but it is not required.

Step II. Verify the Installation

After installing IIS, you must verify the installation to determine whether it is serving pages properly. Test the installed IIS from the server that is hosting it as well as from another browser on the network.

To verify that IIS is serving pages

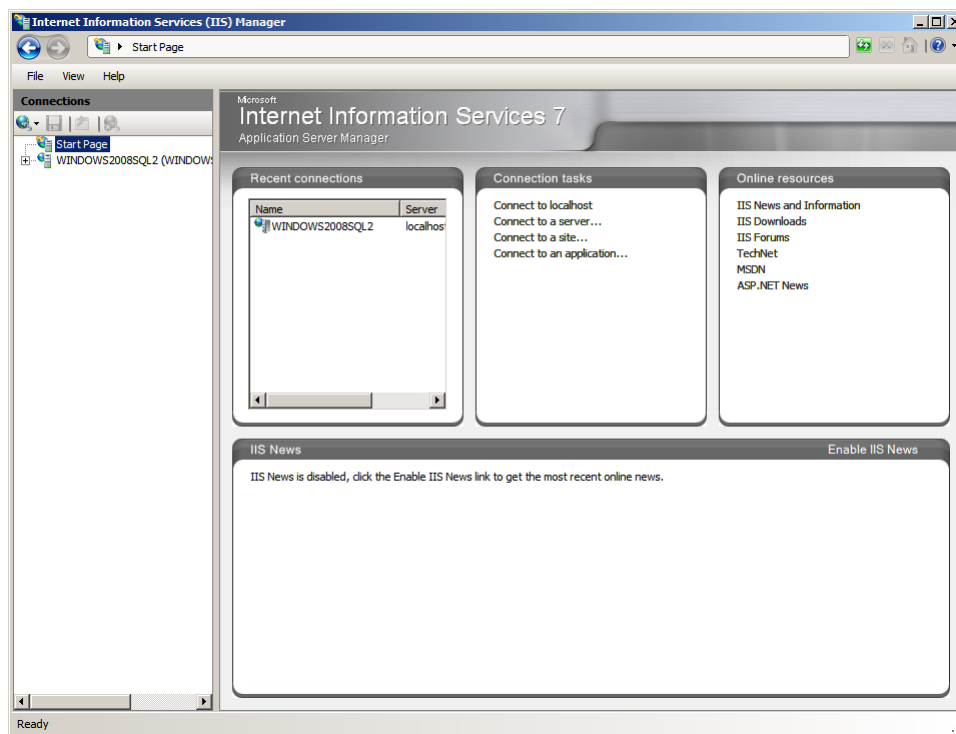
1. Start a browser on the host that IIS is running on.
2. From the browser, go to the following URL: **http://localhost/**
IIS is installed and running if the browser displays the “IIS7” page.



Step III. Starting and Configuring IIS

A. IIS Manager

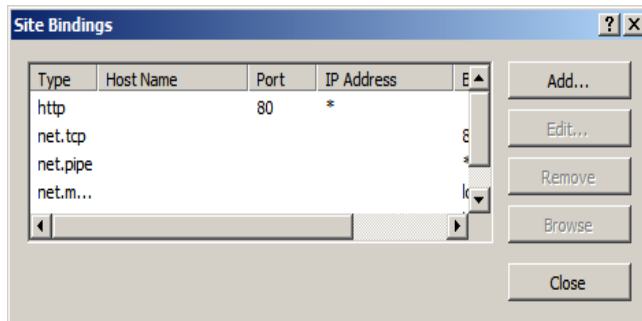
1. Start the management console, which is required before any other actions are taken.
2. Select: **Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager**
3. When the “Internet Information Services (IIS) Manager” loads:
 - a. Expand the left-hand tree that starts with the current system’s name.
 - b. In the “Sites Entry” field, select **Default Web Site**.



B. Changing the IIS Port

1. Open the management console and browser to the **Default Site**
2. Right-click the **Default Web Site** entry and select **Edit Bindings** from the menu.

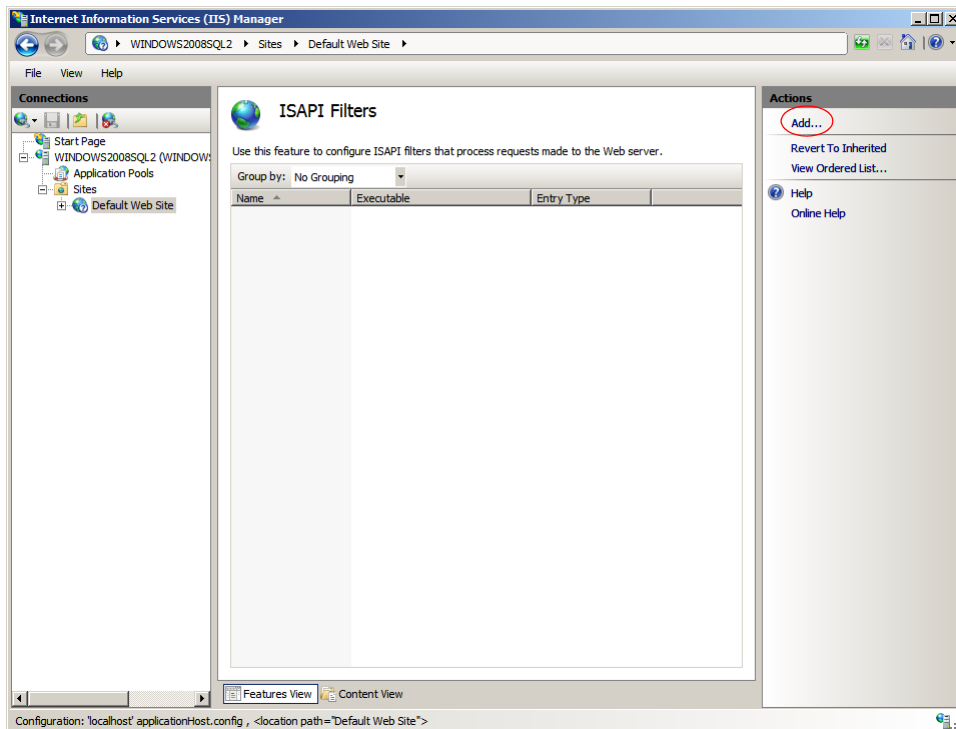
3. In the “Site Bindings” dialog box you can add or change the ports and IP address on which the Server IIS will bind.



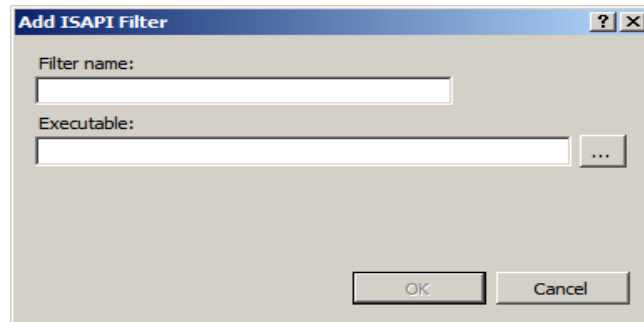
4. Click **Close** after all changes have been made.

C. Adding a New ISAPI Filter

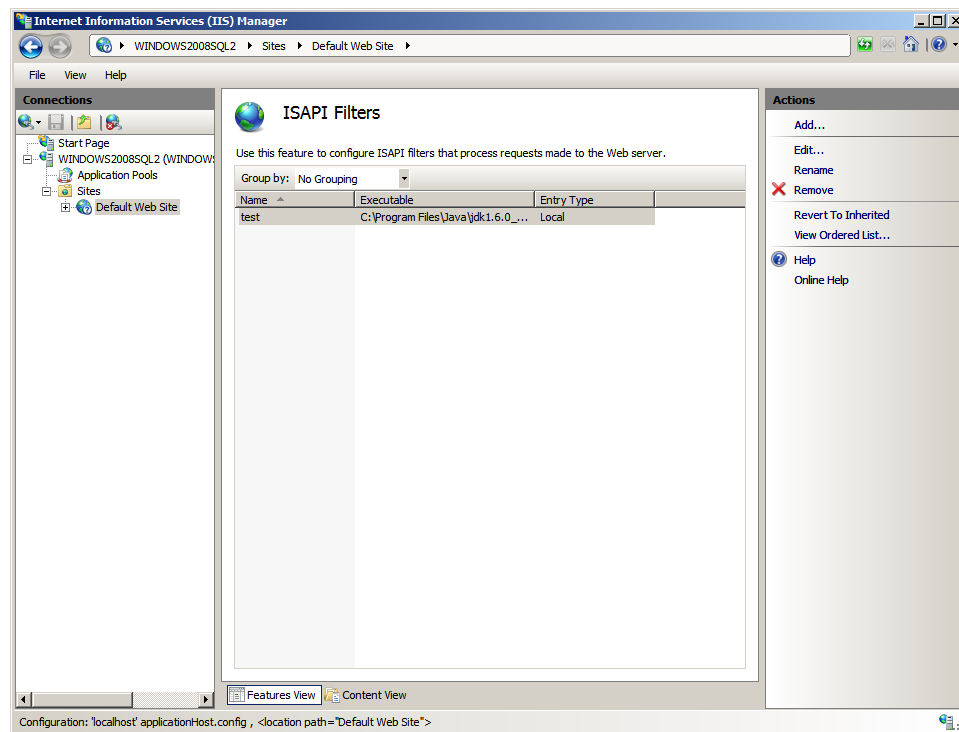
1. Open the management console and browser to the **Default Site**.
2. In the center list, click **ISAPI Filters** and click **Add**.



3. The “Add ISAPI Filter” dialog box appears.
 - a. Fill in the fields provided:
 - **Filter name:** Enter a filter name.
 - **Executable:** Enter the location of the Executable.
 - b. Click **OK**.

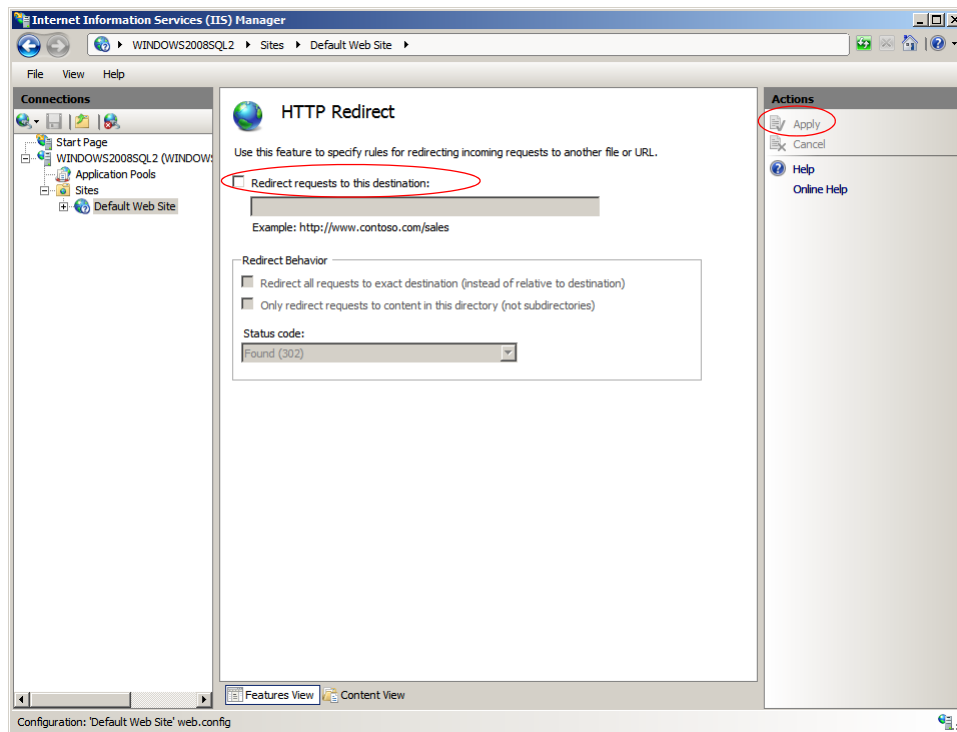


The new filter is added to the “ISAPI Filters” list.



Proxing Using IIS

1. Open the management console and browser to the Default Site.
2. In the center list, click **HTTP Redirect**.
3. In the center panel of the “Internet Information Services (IIS) Manager”:
 - a. Select the **Redirect requests to this destination** option.
 - b. Enter the location of the remote server in the text field (for WebCenter Sites or Remote Satellite Server include the context root).
 - c. Click **Apply**.



Chapter 7

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 WebCenter Sites, 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 86.
 - 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 3](#), “[Apache Parameters.](#)”

Table 3: Apache Parameters

Parameter	What it Holds	Your Value
Web Server Version (<i>WebVersion</i>)	The version of Apache that the host is running. Note that you must use a version that WebCenter Sites supports.	
Web Host Name (<i>WebHost</i>)	The name by which the Apache host machine is known on the network.	
Web Host IP Address (<i>WebIP</i>)	The numeric Internet Protocol address assigned to the Apache host machine.	
Web Server Port (<i>WebPort</i>)	The port number assigned for Apache communications. By default, it has the value 80.	
Apache Root Directory (<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 87](#).
- 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 86](#).

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 86](#)).

Next Step

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

Part 3

Installing and Configuring an LDAP Server

If you choose to use LDAP, WebCenter Sites must have access to a supported LDAP server specifically configured for WebCenter Sites. This part describes how to install and configure a supported LDAP server for integration with WebCenter Sites.

Note

- You must set up a supported LDAP server **before** you run the WebCenter Sites-LDAP integrator.
- If you are integrating with LDAP, but no content management sites exist in WebCenter Sites, then upon completion of the LDAP integration, refer to instructions in *Oracle WebCenter Sites: Integrating with LDAP* (“Step 8. Post Integration. If Content Management Sites are Not Installed”).

This part contains the following chapters:

- [Chapter 8, “Installing Active Directory Server 2008”](#)
- [Chapter 9, “Setting Up IBM Tivoli Directory Server 6.x”](#)
- [Chapter 10, “Setting Up OpenLDAP 2.3.x”](#)
- [Chapter 11, “Setting Up the WebLogic 10.3.5 Embedded LDAP Server”](#)
- [Chapter 12, “Setting Up MS Active Directory Server 2003”](#)

Chapter 8

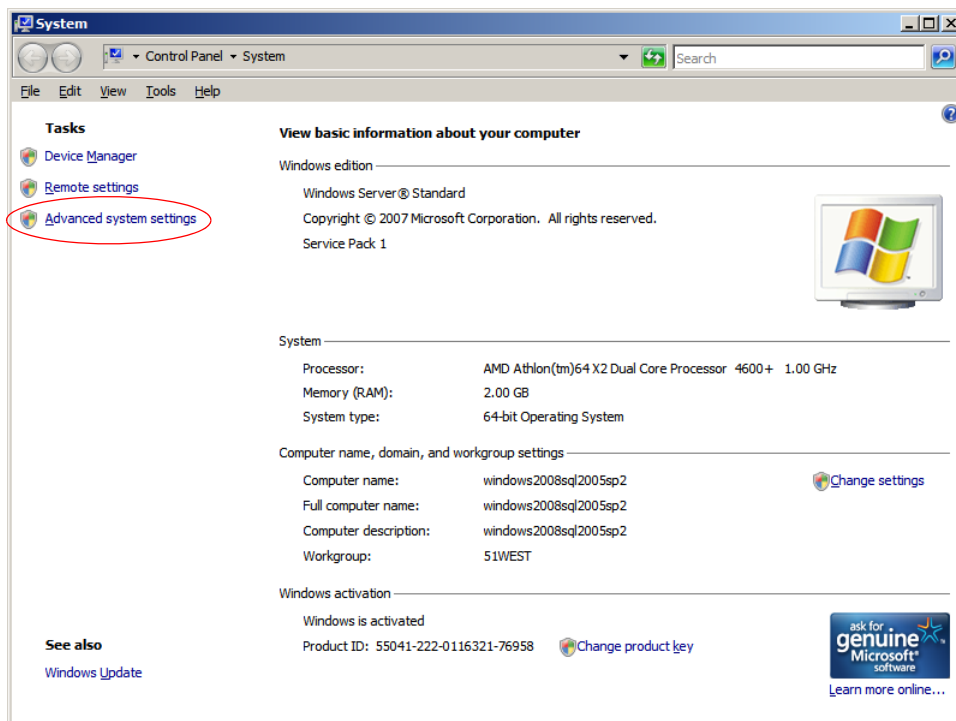
Installing Active Directory Server 2008

This chapter includes the following sections:

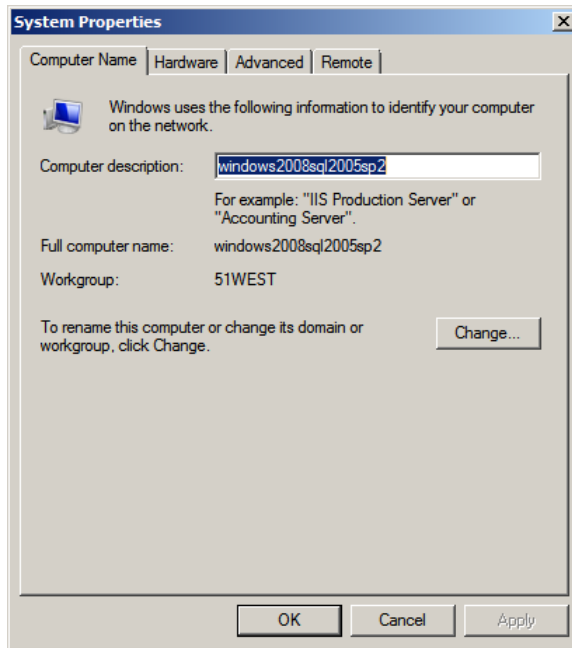
- [Installation Steps](#)
- [Configuring the Network Settings](#)
- [Installing Active Directory 2008 Services](#)
- [Installing Active Directory 2008 Installation Wizard](#)
- [Checking Group Policies](#)
- [Changing Group Policies](#)

Installation Steps

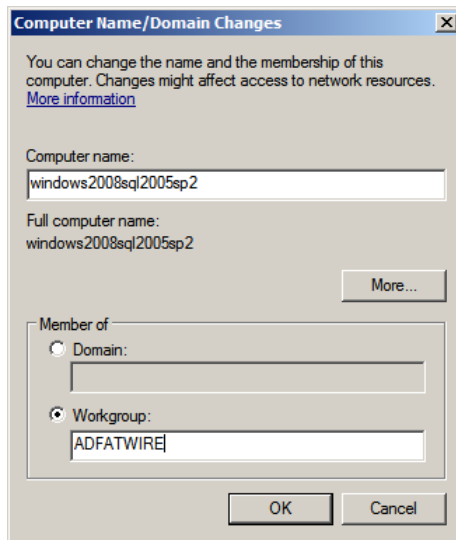
1. Install the Operating System:
 - a. Install Windows Server 2008 (any Windows server except Web).
 - b. When the installation is complete, leave the installation disc in the drive, you will need it to complete the installation of ADS.
 - c. Set the Computer's **Name** and **Suffix**.
2. Open the "System Properties" dialog box. Click **Start**, then right-click the computer icon.
3. In the "System" window select **Advanced system settings**.



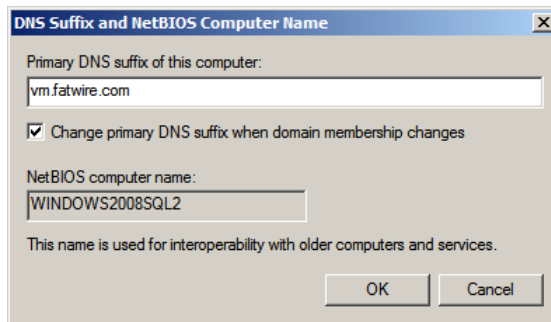
4. Select the **Computer Name** tab.
 - a. Click **Change**.



5. In the pop-up window that appears, fill in the following fields:
 - **Computer name:** Enter the name you wish to designated for your computer. (Make a record of this name).
 - **Member of:** Select the **Workgroup** radio button, then enter a unique workgroup name. (Make a record of this name).



a. Click **More...**

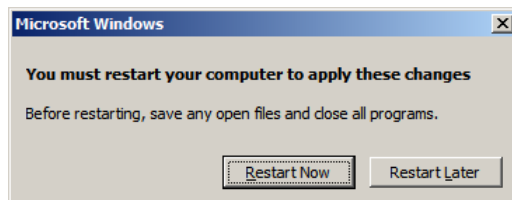


b. In the “DNS Suffix and NetBIOS Computer Name” dialog box, do the following:

- **Primary DNS suffix of this computer:** Enter the DNS suffix of your computer (Make a record of this suffix).
- **Change Primary DNS Suffix when domain membership changes:** If checkbox is selected, deselect it.

c. Click **OK** to close the dialog box.

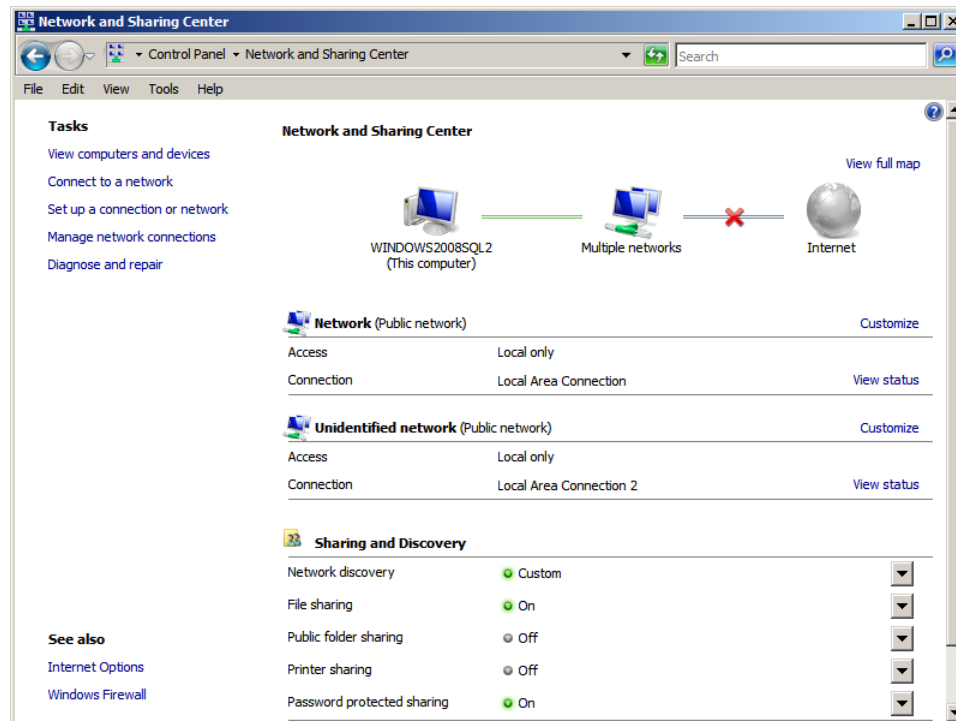
6. In the “Computer Name/Domain Changes” dialog box, click **OK**.
7. In the “System Properties” window click **Close**.
8. In the reboot dialog box click **Restart Later**.



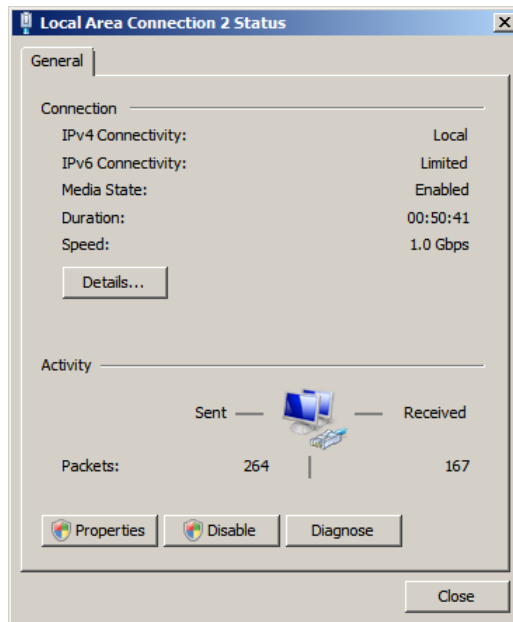
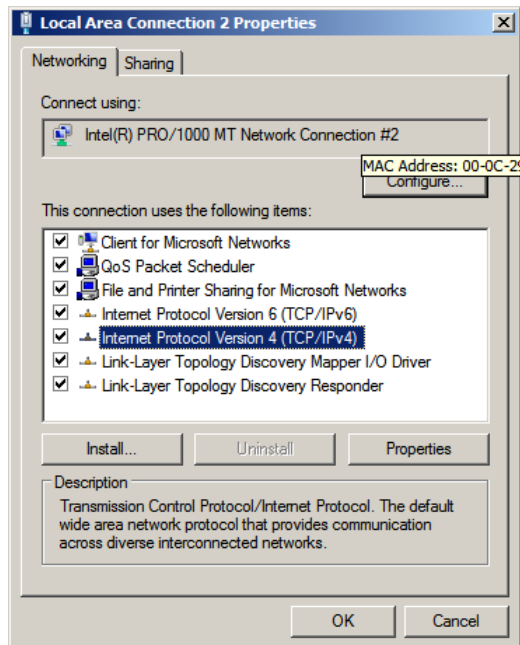
Configuring the Network Settings

To configure the network settings:

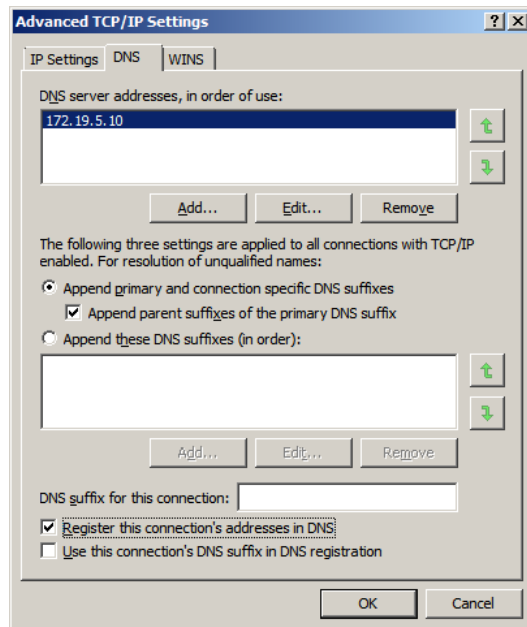
1. Open “Network Properties.”
 - a. Select **Start > Control Panel**.
 - b. Click the **Network and Sharing Center** icon.
 - c. Select the Network Connection to edit (if you have more than one see `ipconfig` result, make sure to select the correct one).



2. Select **View Status**, located next to the network connection you have selected.

3. Click Properties.**4. Select Internet Protocol Version 4 (TCP/Iv4).**

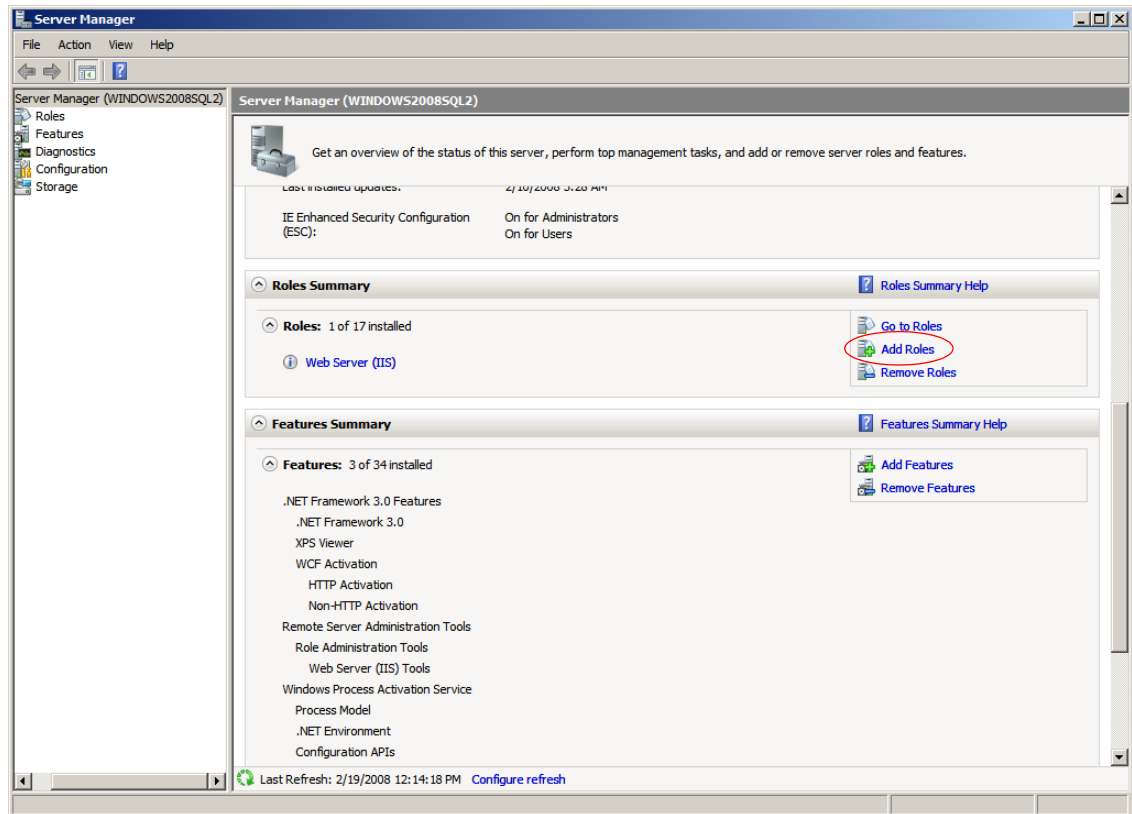
- a. Set the IP address to an unused, static IP address.
- b. Set the preferred DNS server to your computer's IP address.

c. Click **Advanced:**

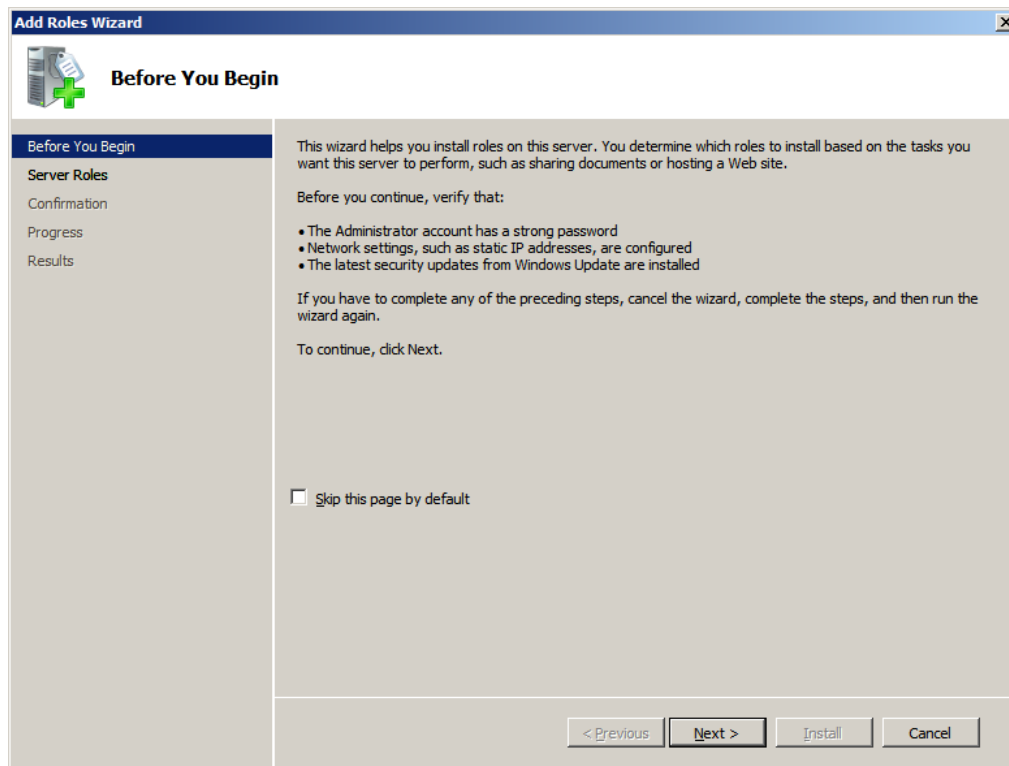
- Select the check box **Append primary and connection-specific DNS suffixes**.
 - Select the check box **Append parent suffixes of the primary DNS suffix**.
5. Click on until you have exited the properties pane, then click **Close**.
 6. Restart the computer.

Installing Active Directory 2008 Services

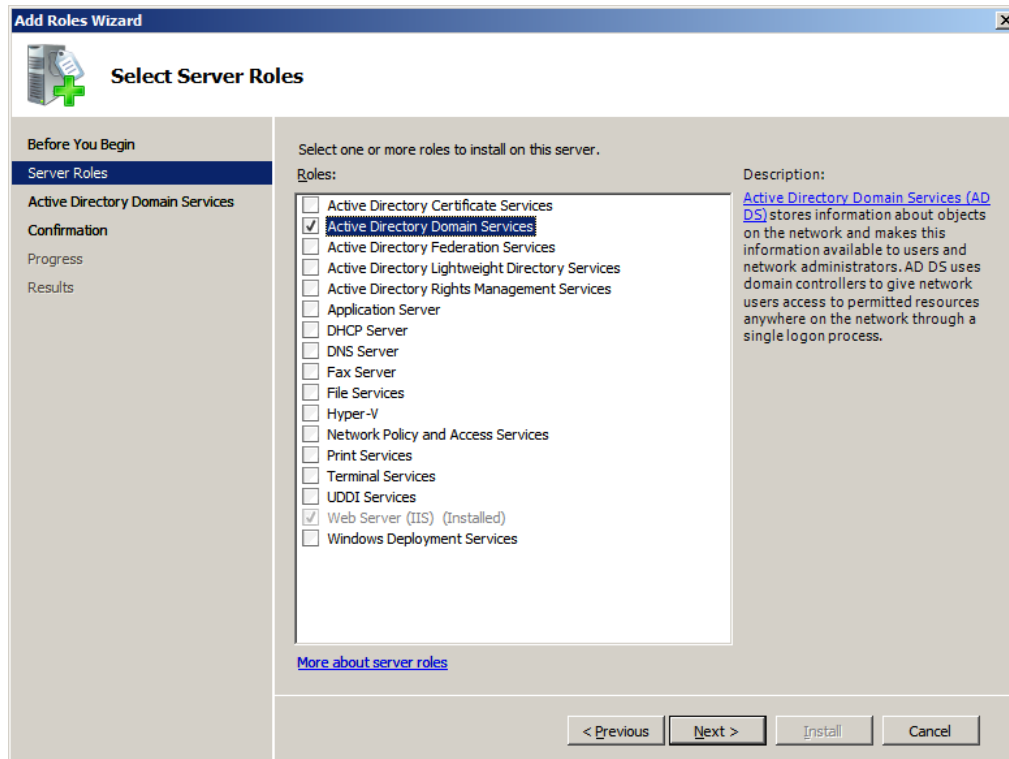
1. Select **Start > Server Manger**.
2. In the “Roles” section click **Add Roles**.



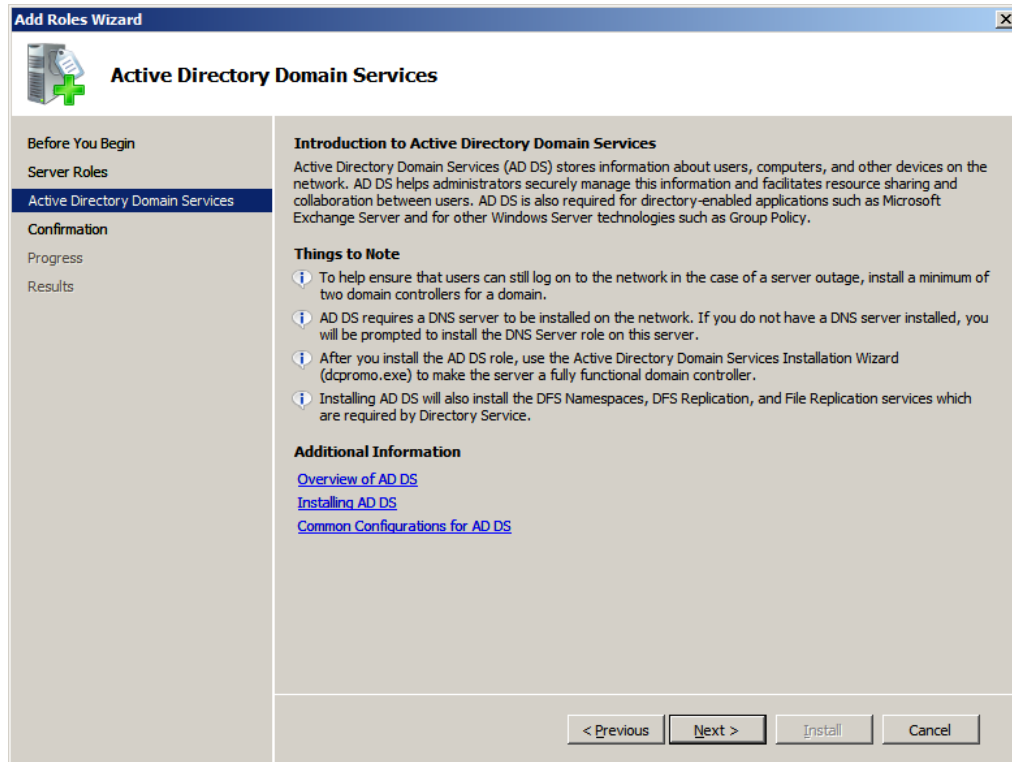
3. In the “Add Roles Wizard” click **Next**.



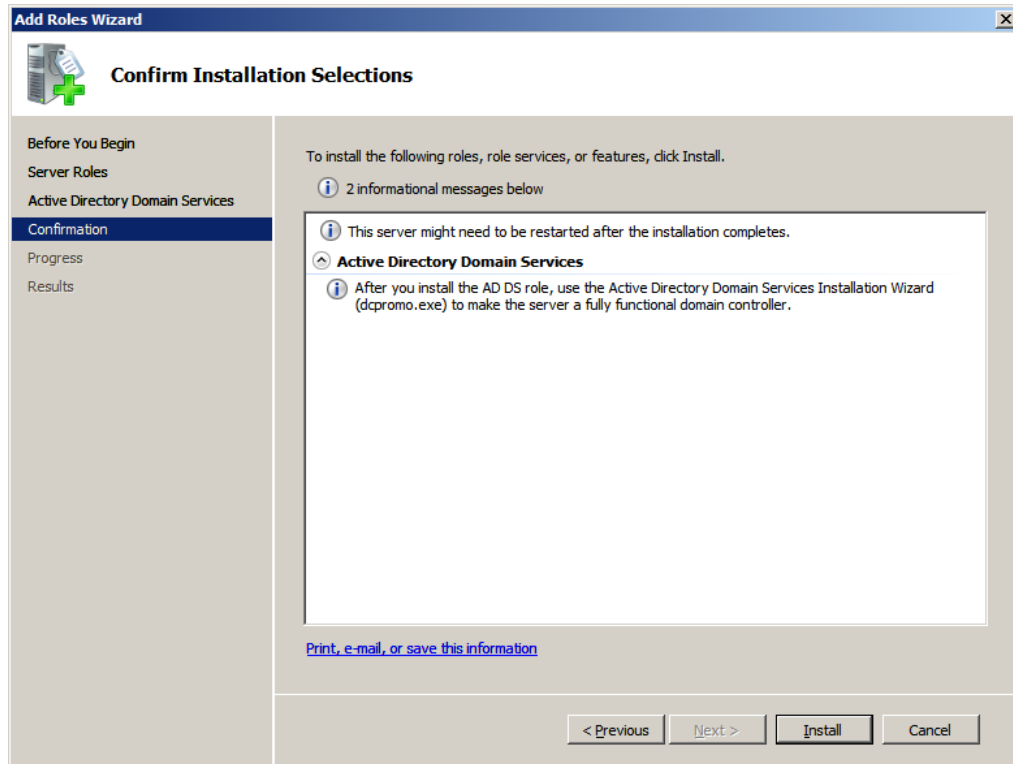
4. Select **Active Directory Domain Services** and click **Next**.



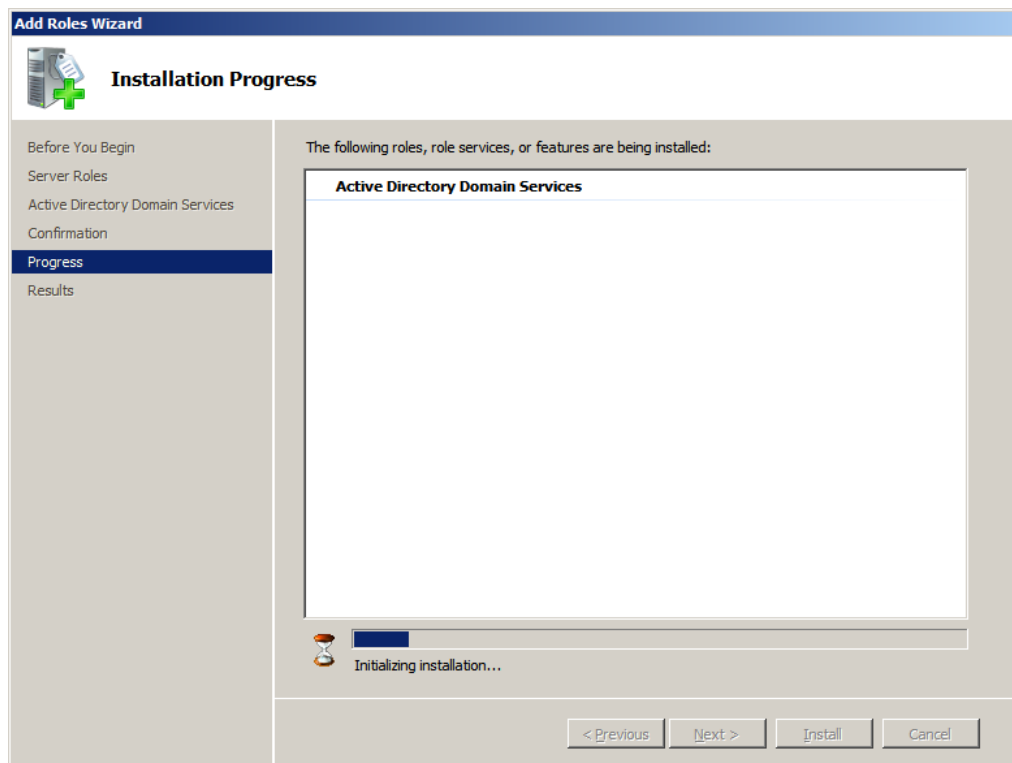
5. Review the list of additional services to be installed along with Active Directory and click **Next**.



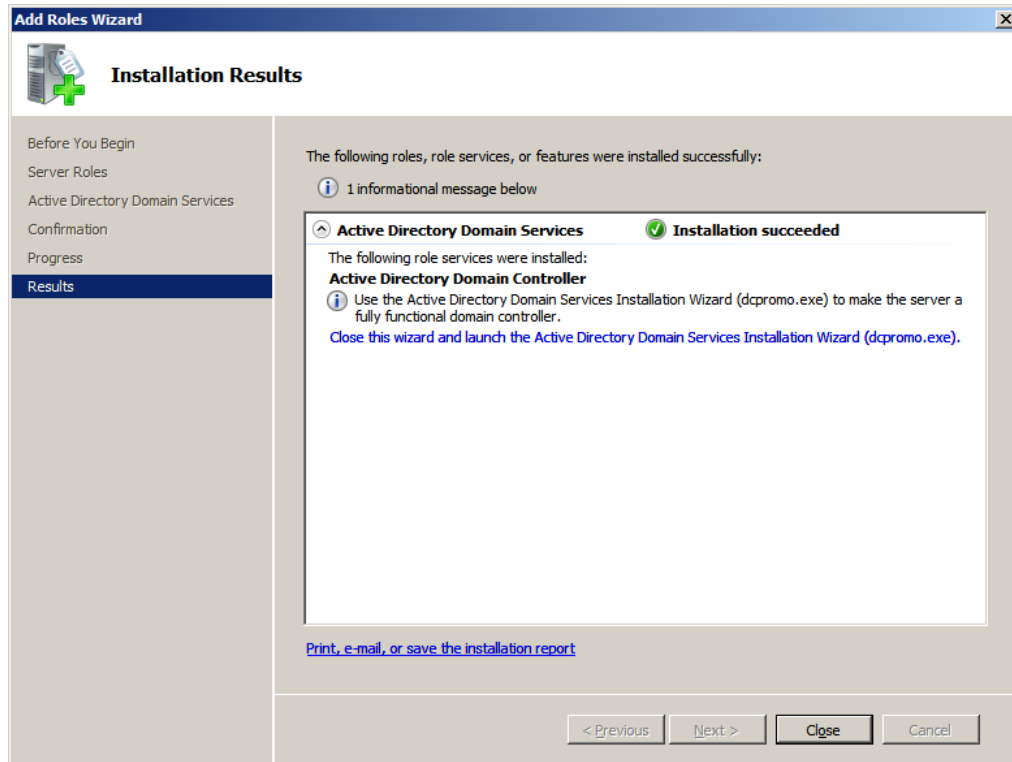
6. Click **Install** to begin installation of “Active Directory 2008.”



7. Allow the installation to complete.



8. Review the results of the “Add Roles Wizard” page. Click: **Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)**.

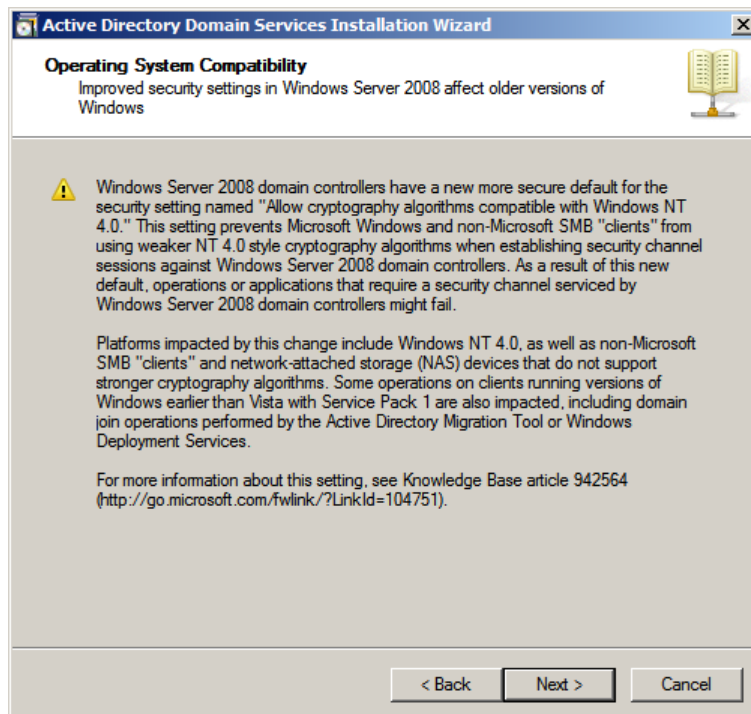


Installing Active Directory 2008 Installation Wizard

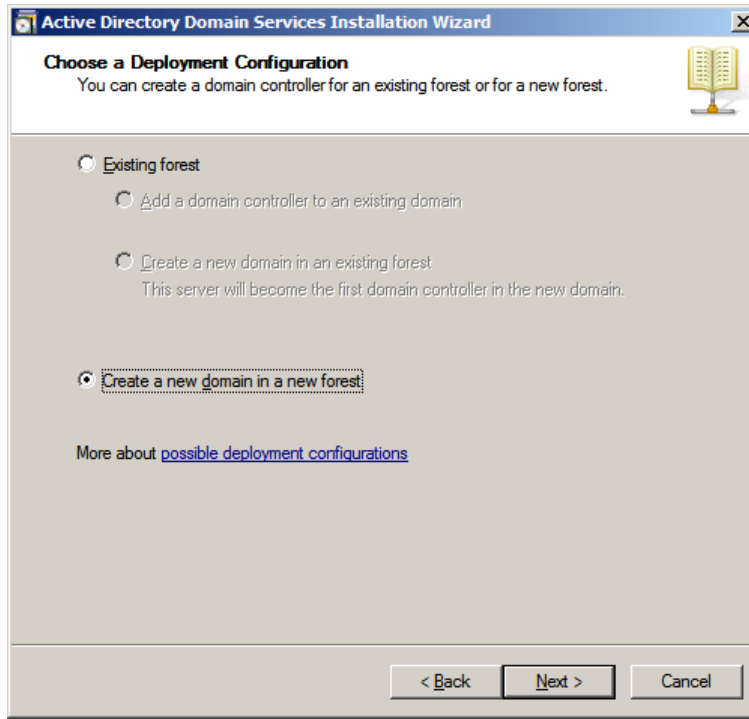
1. In the welcome screen click **Next**.



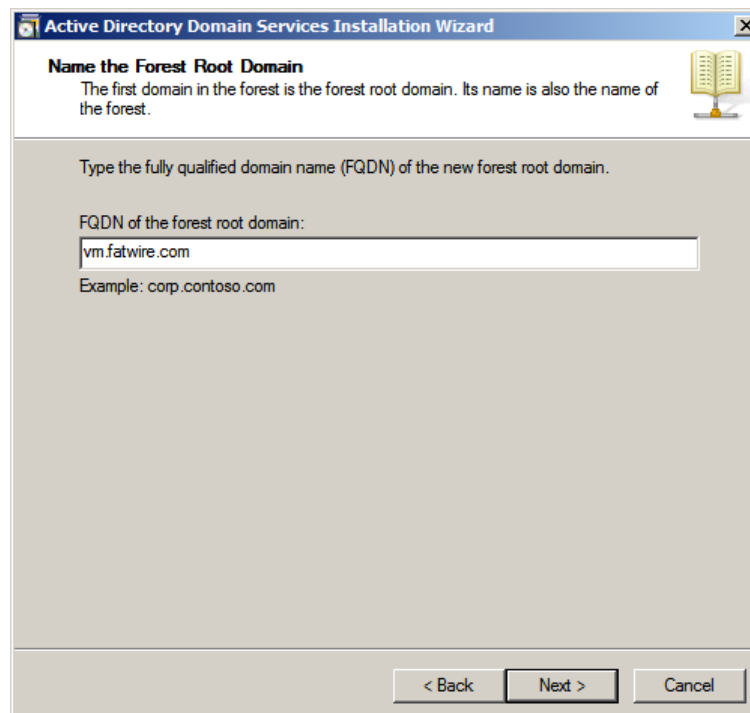
2. In the "Operating System Compatibility" screen click **Next**.



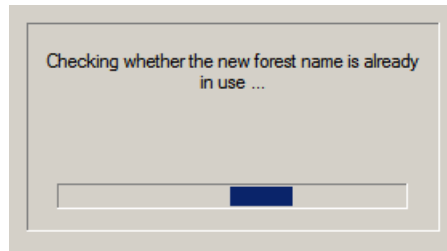
3. In the “Choose a Deployment Configuration” screen select **Create a new Domain in a forest**, then click **Next**.



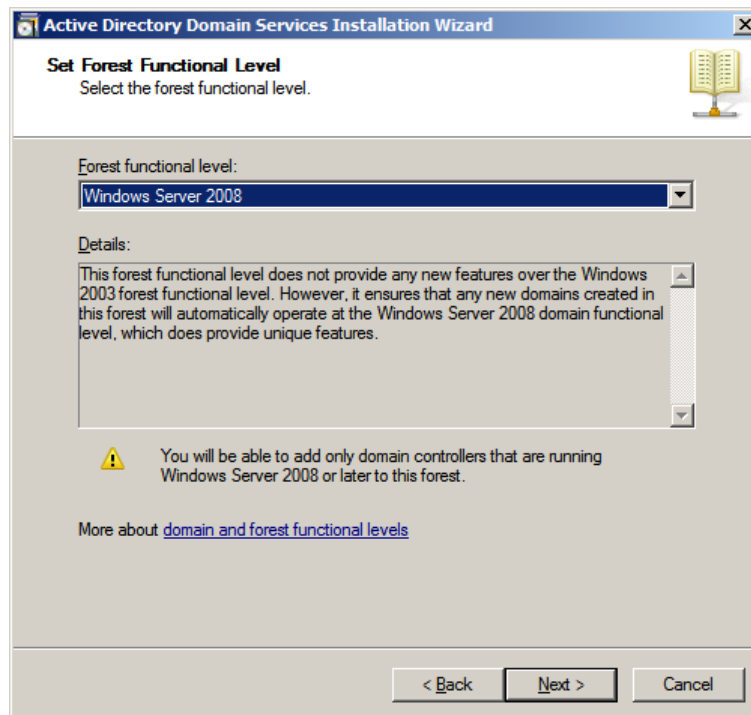
4. Name the “Forest Root Domain”:
 - a. Enter the name of the new forest, which is the DNS root domain that you created previously. Click **Next**.



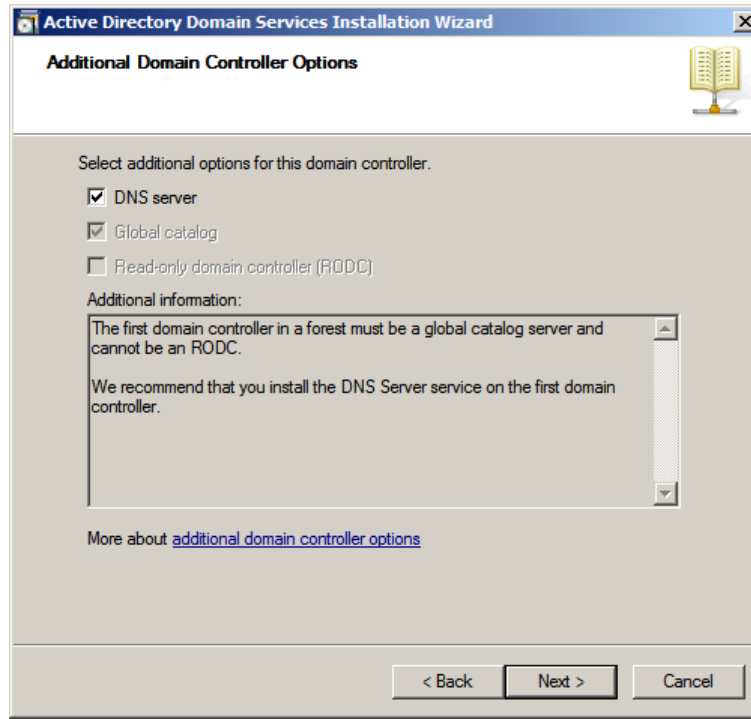
- b. Allow the check dialog to complete.



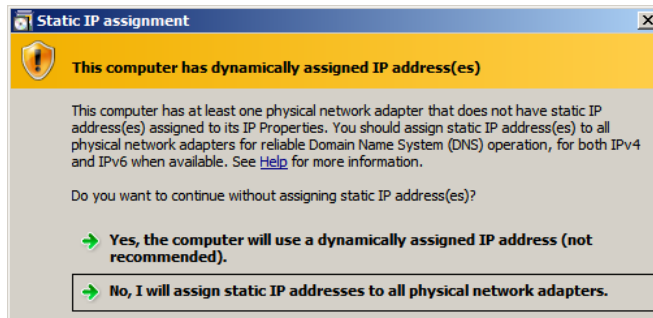
5. In the “Set Forest Functional Level” screen, select **Windows Server 2008**, then click **Next**.



6. In the “Additional Domain Controller Options” screen, ensure that **DNS Server** is selected, then click **Next**.

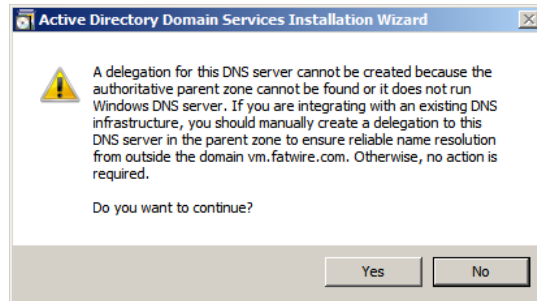


If you have a DHCP based adapter you will see the following pop-up message:



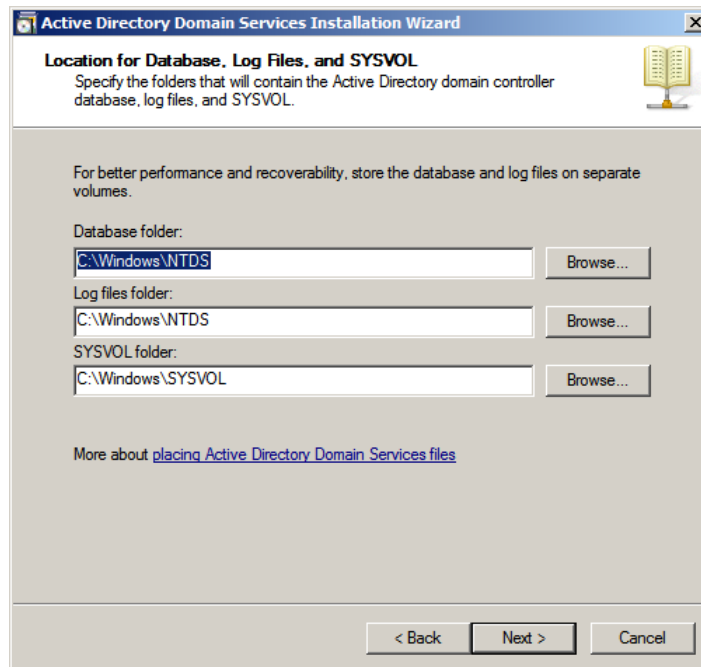
Select **No, I will assign static IP addresses to all physical adapters** to continue with the installation. After the installation completes you can change any DHCP adapter back.

7. If the DNS zone you are creating does not have an authoritative parent zone, the following pop-up message may be displayed:

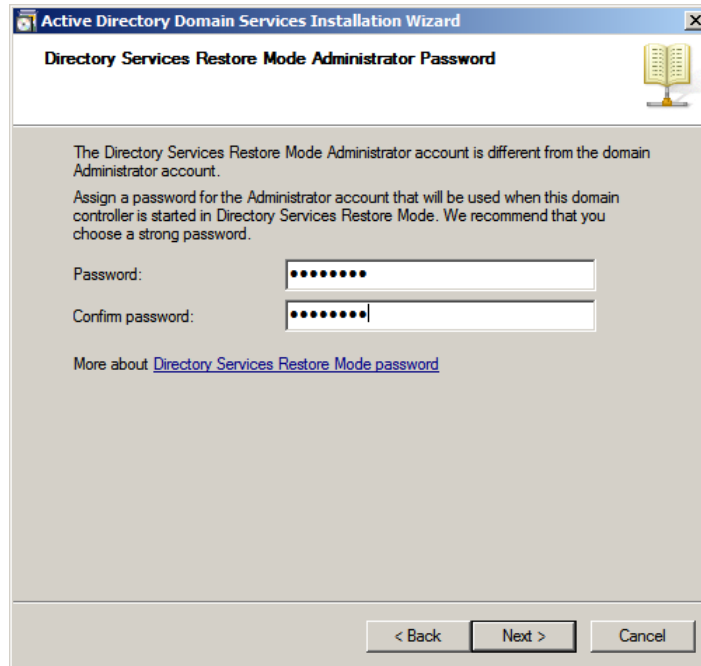


Select **Yes** to continue with the installation.

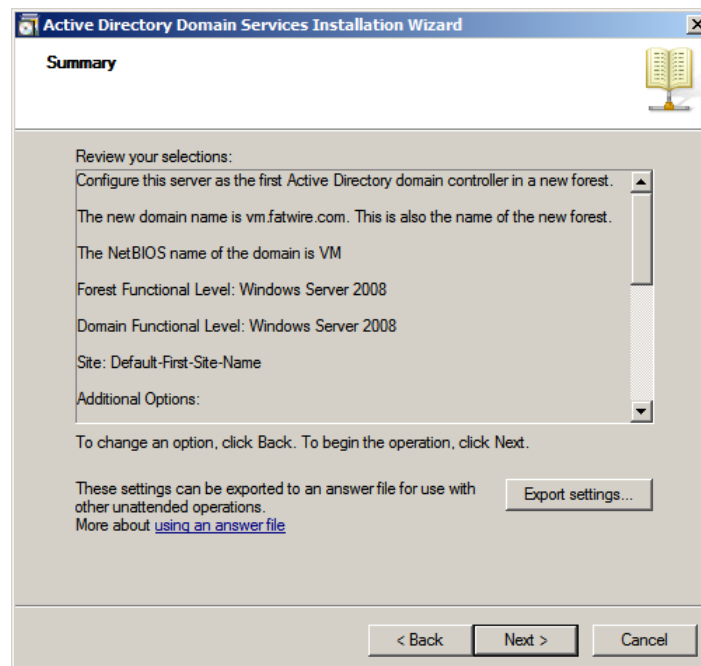
8. In the "Location for Database, Log Files, and SYSVOL" screen select the default in the **Database folder** field or change it as required by your system, then click **Next**.



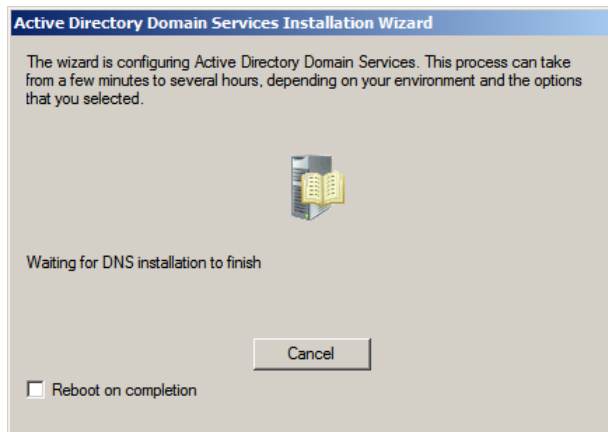
9. In the “Directory Services Restore Mode Administrator Password” screen, enter a password and make a record of it.



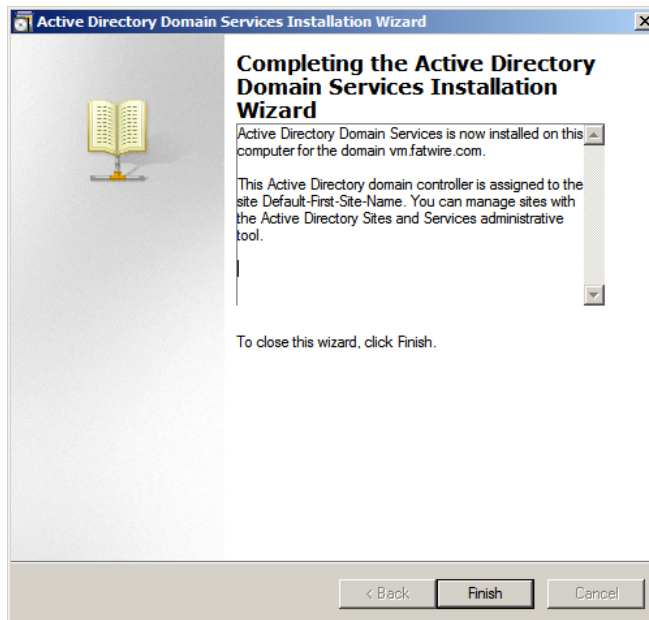
10. In the “Summary” screen:
 - a. Review your settings.
 - b. Export your settings.
 - c. Click **Next**.



11. Wait for the installation to complete.



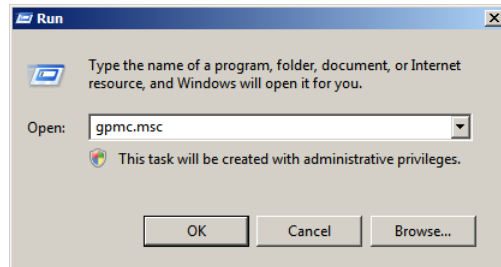
12. In the Active Directory Domain Services Installation Wizard, click **Finish** to complete the installation.



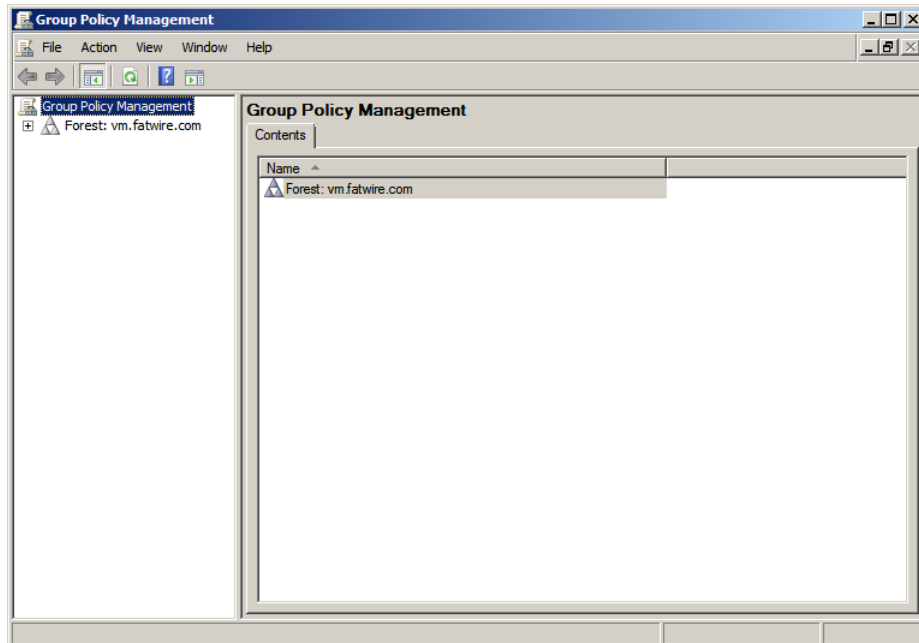
13. Reboot the System.

Checking Group Policies

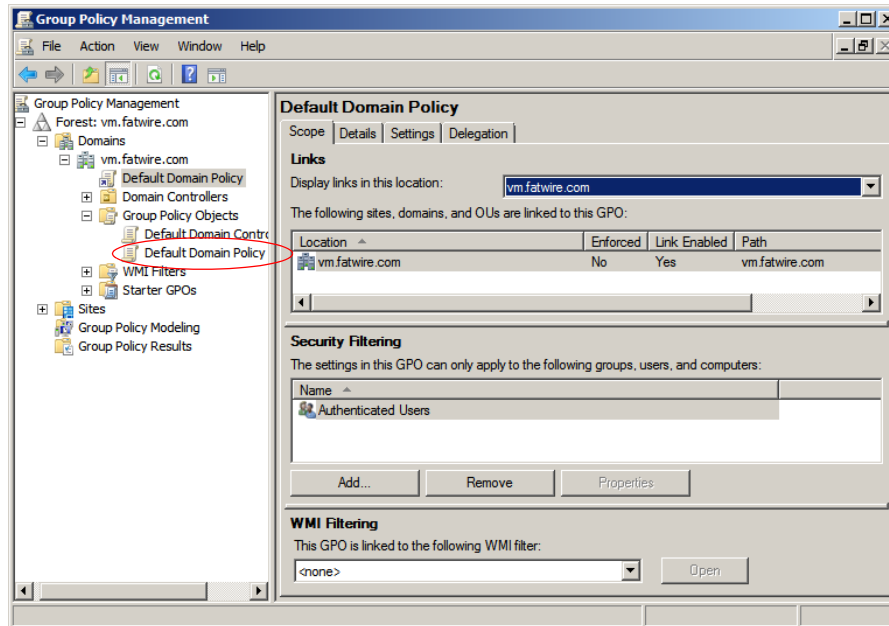
1. Select **Start > Run**.
 - a. Enter `gpmmc.msc` in the available field.
 - b. Click **OK**.



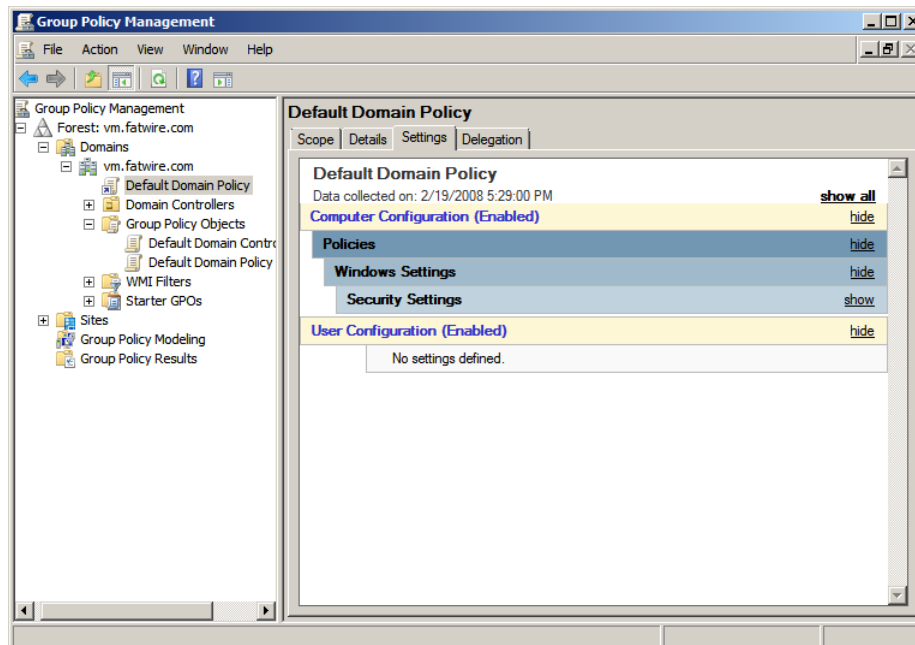
2. "Group Policy Management" opens.



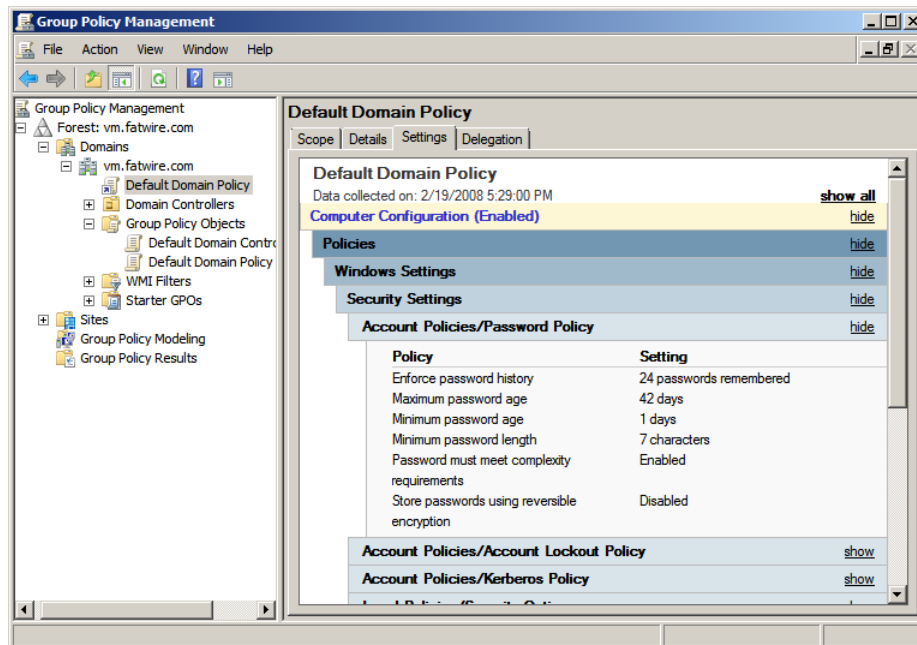
- a. Expand the tree **Domains** > *your domain name*, then select **Default Domain Policy**, located in the left panel of the “Group Policy Management” screen.



- b. Select the **Settings** tab.



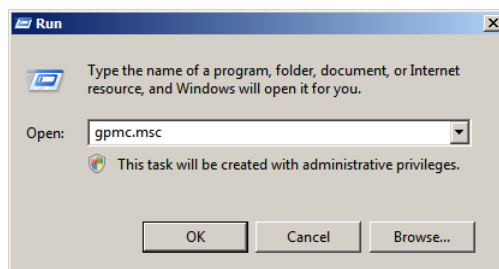
- c. Expand **Security > Account Policy/Password Policy** section, by clicking **show**.



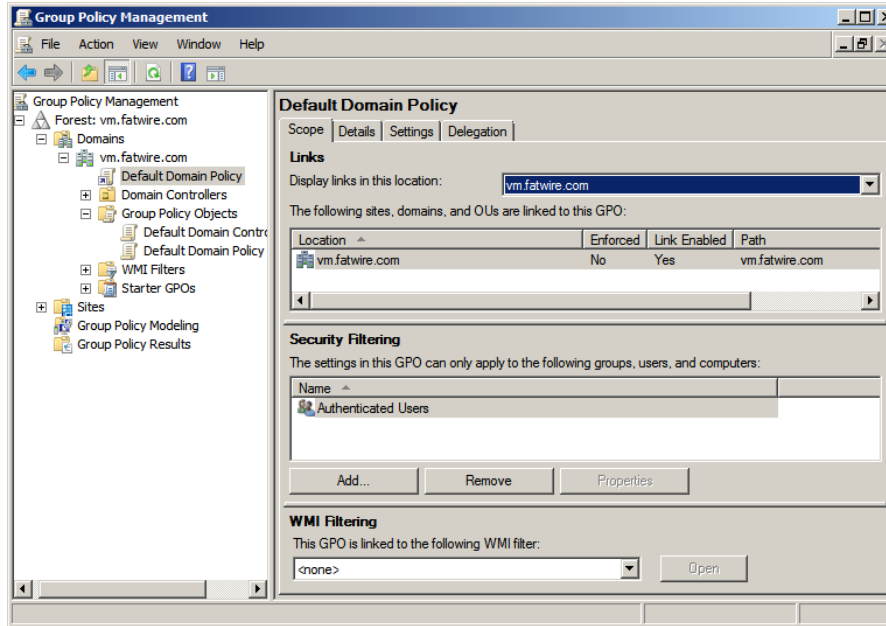
3. Review the “Policy” list. The option **Password must meet complexity requirements** is set to true by default. Change this option to **Disabled** (default WebCenter Sites passwords do not meet these requirements).

Changing Group Policies

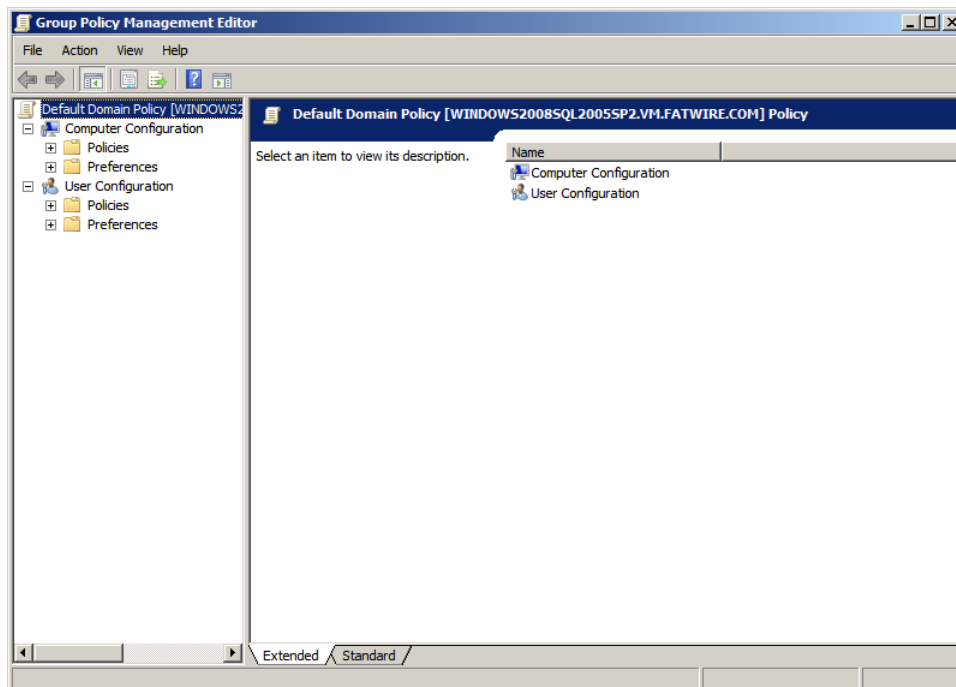
1. Select **Start > Run**.
 - a. Enter: `gpmmc.msc` in the field provided.
 - b. Click **OK**.



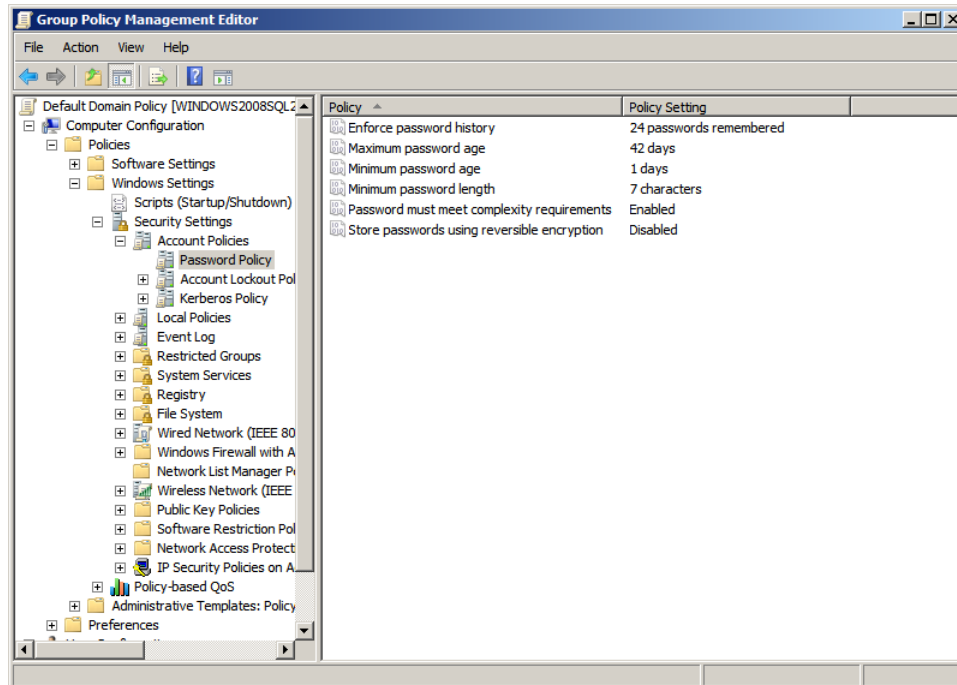
2. In the “Group Policy Management” screen, expand the tree **Domains** > *name of your domain*. Select the **Default Domain Policy**, located on the right of the screen, then select **edit**.



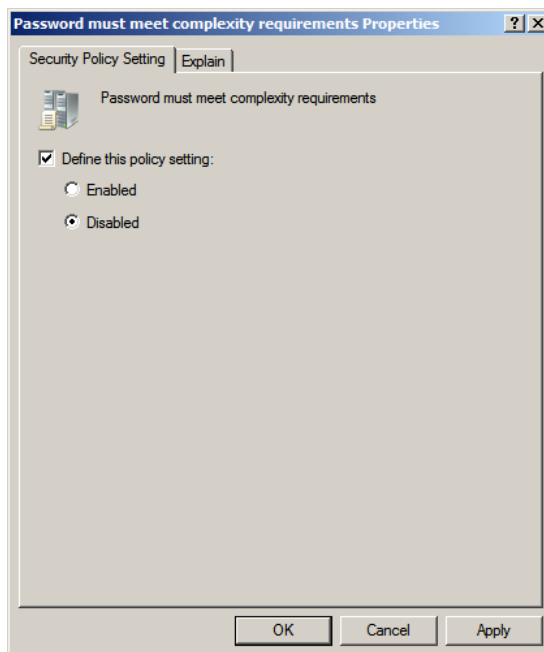
3. The “Group Policy Management Editor” window opens.



- a. In the left hand tree expand: **Computer Configuration > Policies > Windows Settings > Security Settings > Account Settings > Password Policy**



- b. Right-click **Password must meet complexity requirements**, located on the right side of the screen, then select **Properties**.
- c. In the “Password must meet complexity requirements Properties” dialog box select the radio button **Disabled**, then click **OK**.



- d. Close the “Group Policy Management Editor” and “Group Policy Management” windows.
4. The domain will no longer check for password complexity. WebCenter Sites default passwords can now be used.

When WebCenter Sites is installed you can reverse [step 2](#) by clicking **Enabled** to re-engage the security settings.

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:** deselect
 - **User DN:** administrator@<DNS_suffix>
 - **Append base DN:** deselect
 - **Password:** <ADS_password> (you created this password in [step 9](#) on page 108)
4. Click **Connect**.

Edit Session

Name Connection Options

Host Info

Host: localhost Port: 389 Version: 3

Base DN: DC=vm,DC=fatwire,DC=com

Fetch DNS SSL Anonymous bind

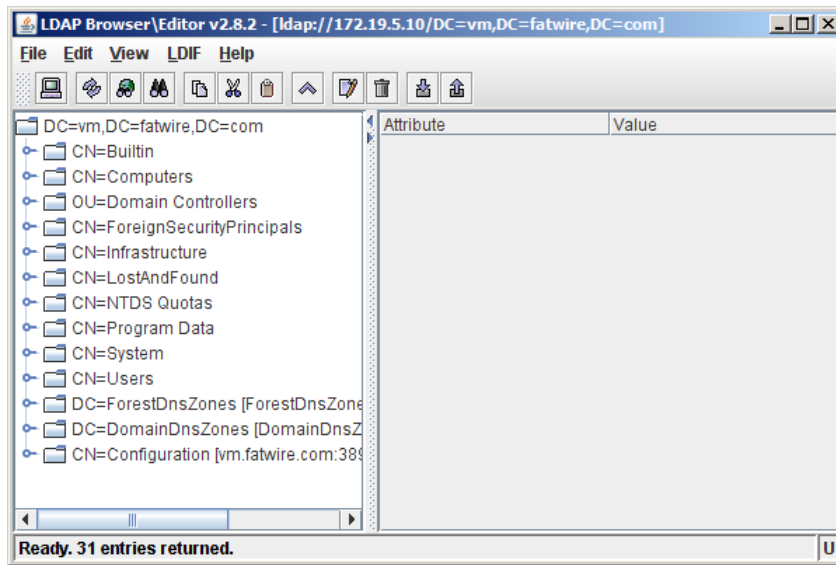
User Info

User DN: Administrator@vm.fatwire.com append base DN

Password:

Save Cancel

5. Show the default view on the LDAP tree.



Chapter 9

Setting Up IBM Tivoli Directory Server 6.x

This chapter contains the following sections:

- [IBM Tivoli Directory Server Commands](#)
- [Before Installing IBM Tivoli Directory Server](#)
- [Installing IBM Tivoli Directory Server](#)
- [Configuring Tivoli Directory Server](#)
- [Connecting to IBM TDS Using the LDAP Browser](#)

Note

In this guide, Tivoli Directory Server is also referred to as “TDS.”

IBM Tivoli Directory Server Commands

Table 4: IBM Tivoli Directory Server Commands

Action	Command
Starting an instance	<LDAP Install directory>/sbin/idsslapd -I <instance name>
Stopping an instance	<LDAP Install directory>/bin/ibmdirctl stop -h localhost -D cn=root -w <password for cn=root>
Checking an instance	<LDAP Install directory>/bin/ibmdirctl status -h localhost -D cn=root -w <password entered for cn=root>
Displaying list of instances	<LDAP Install directory>/sbin/idsilist
Loading the instance administration tool	<LDAP Install directory>/sbin/idsxinst
Loading the configuration tool for an instance	<LDAP Install directory>/sbin/idsxcfg -I <name of instance>



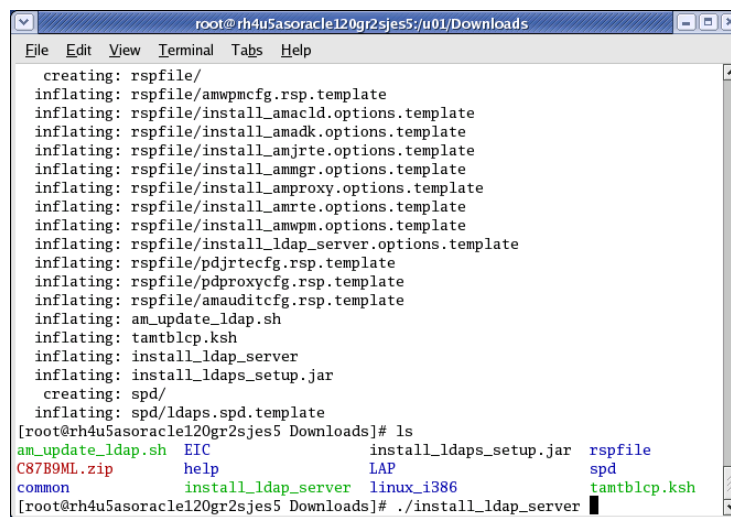
Before Installing IBM Tivoli Directory Server

1. Create the following group: `idsldap`
2. Create a user for the LDAP instance and write down the password, for example, `ldapdb2`. This password will be used in [step 7](#) of “Installing IBM Tivoli Directory Server.”
3. Check that `pdksh` is installed.

Installing IBM Tivoli Directory Server

1. Download the Tivoli Directory Server from IBM.
2. Unzip the archive into a temporary directory.
3. Go to the temporary directory and run:

```
./install_ldap_server.
```



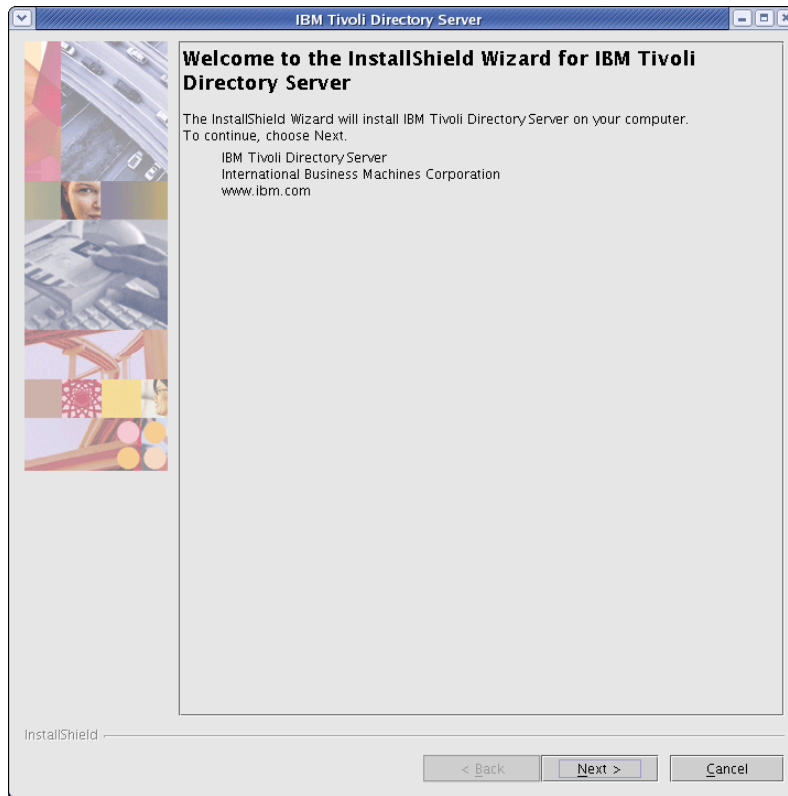
```

root@rh4u5asoracl120gr2sjes5/Downloads
File Edit View Terminal Tabs Help
creating: rspfile/
inflating: rspfile/amwpmcfg.rsp.template
inflating: rspfile/install_anacl.d.options.template
inflating: rspfile/install_anacl.d.options.template
inflating: rspfile/install_anjrte.options.template
inflating: rspfile/install_amgr.options.template
inflating: rspfile/install_amproxy.options.template
inflating: rspfile/install_amrte.options.template
inflating: rspfile/install_amwpm.options.template
inflating: rspfile/install_ldap_server.options.template
inflating: rspfile/pdjrtecfg.rsp.template
inflating: rspfile/pdproxycfg.rsp.template
inflating: rspfile/amauditcfg.rsp.template
inflating: am_update_ldap.sh
inflating: tamtblcp.ksh
inflating: install_ldap_server
inflating: install_ldaps_setup.jar
creating: spd/
inflating: spd/ldaps.spd.template
[root@rh4u5asoracl120gr2sjes5 Downloads]# ls
am_update_ldap.sh  EIC                install_ldaps_setup.jar  rspfile
C87B9ML.zip       help              LAP                    spd
common            install_ldap_server  linux_i386             tamtblcp.ksh
[root@rh4u5asoracl120gr2sjes5 Downloads]# ./install_ldap_server

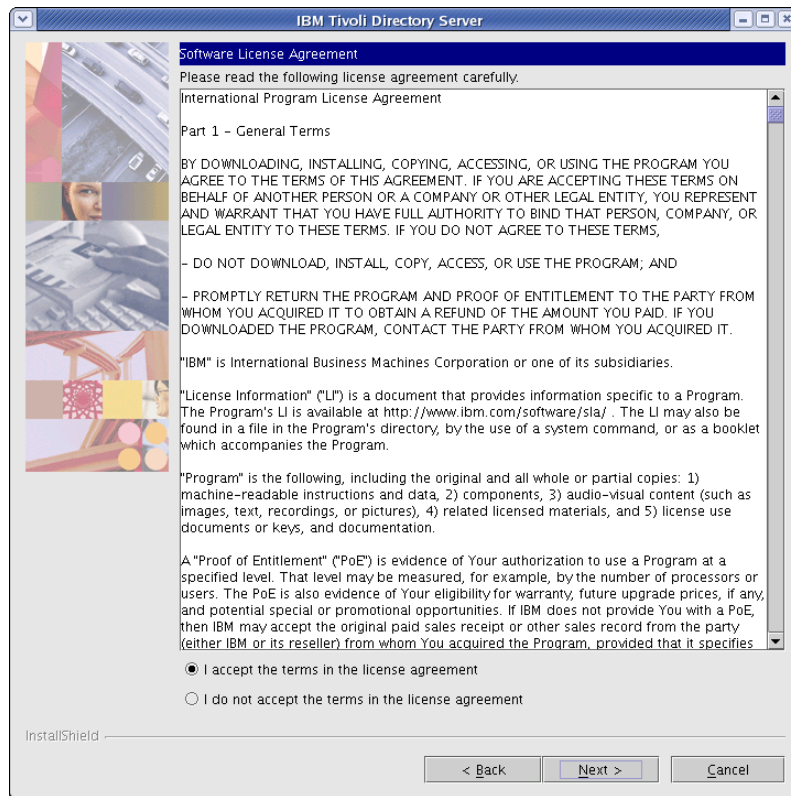
```

4. When the installation dialog box appears, select your language and click **OK**.



5. Click Next.

6. On the “License Agreement” screen select **I Accept the terms in this license agreement**, then click **Next**.



7. On the first configuration screen, fill in the fields:
 - **DB2 administrator ID:** Name of the user you created for the LDAP instance.
 - **DB2 administrator password:** Enter the password (ldapdb2) given to the LDAP instance user in [step 2](#), “Before Installing IBM Tivoli Directory Server.”
 - Keep the default values for the other fields.
 - Click **Next**.

IBM Tivoli Directory Server

To configure IBM Tivoli Directory Server, specify the following database information.

DB2 administrator ID (also used for the instance name) *

ldapdb2

DB2 administrator password *

Password confirmation *

Group for the DB2 administrator (UNIX)

root

Create the DB2 administrator if it does not already exist

Directory server database home *

/home/ldapdb2

DB2 database name *

amdb

Encryption seed *

0123456789012

InstallShield

< Back Next > Cancel Help

8. On the second configuration screen, fill in the fields:
 - a. **Administrator password:** Enter a password and remember it. This password will re-occur throughout the configuration and will be referred to as `sn=root`.
 - b. **User-defined suffix:**
`dc=<domain>,dc=<ext>`
For example, if your domain is `fatwire.com`, then the User-defined suffix should read: `dc=fatwire,dc=com`.
 - c. Confirm that the **Local hostname** is correct.
 - d. Click **Next**.

IBM Tivoli Directory Server

To configure IBM Tivoli Directory Server, specify the following database information.

Administrator ID *

Administrator password *

Password confirmation *

User-defined suffix *

Local host name *

< Back Next > Cancel Help

9. On the third configuration page:
 - a. Fill in the fields:
 - **SSL key file password:** Enter a password for SSL.
 - **Non-SSL port:** Confirm the Non-SSL port value is set to 389. If the Non-SSL has been changed, use the new value when installing WebCenter Sites.
 - b. Click **Next**.

IBM Tivoli Directory Server

To configure IBM Tivoli Directory Server, specify the following database information.

Non-SSL port *

389

SSL port *

636

SSL key file with full path *

/opt/ibm/ldap/V6.0/lib/am_key.kdb

Browse

SSL key file password *

Password confirmation *

Certificate label

PDLDAAP

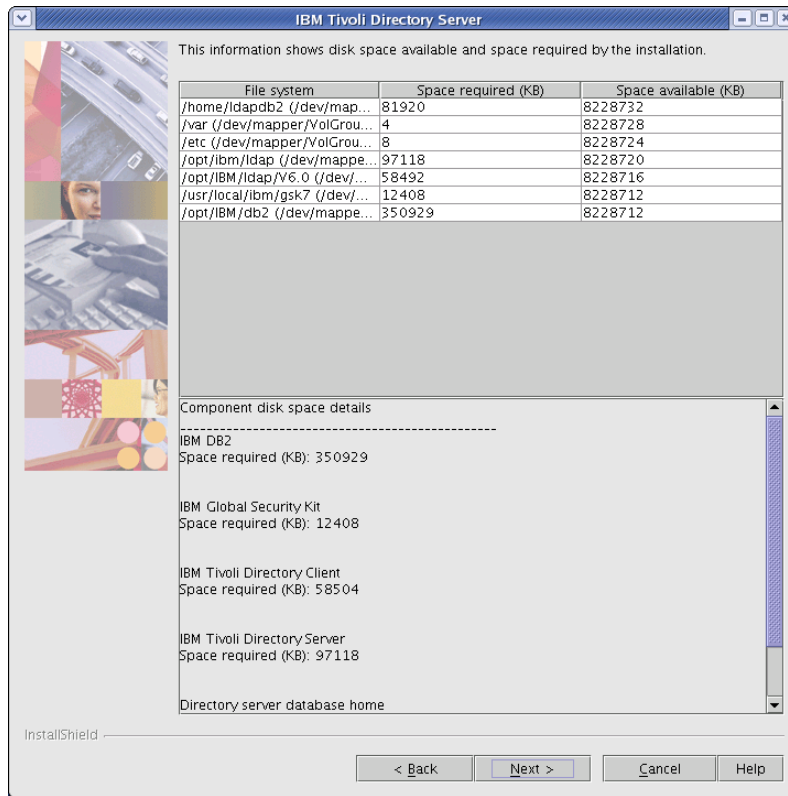
Create SSL key file

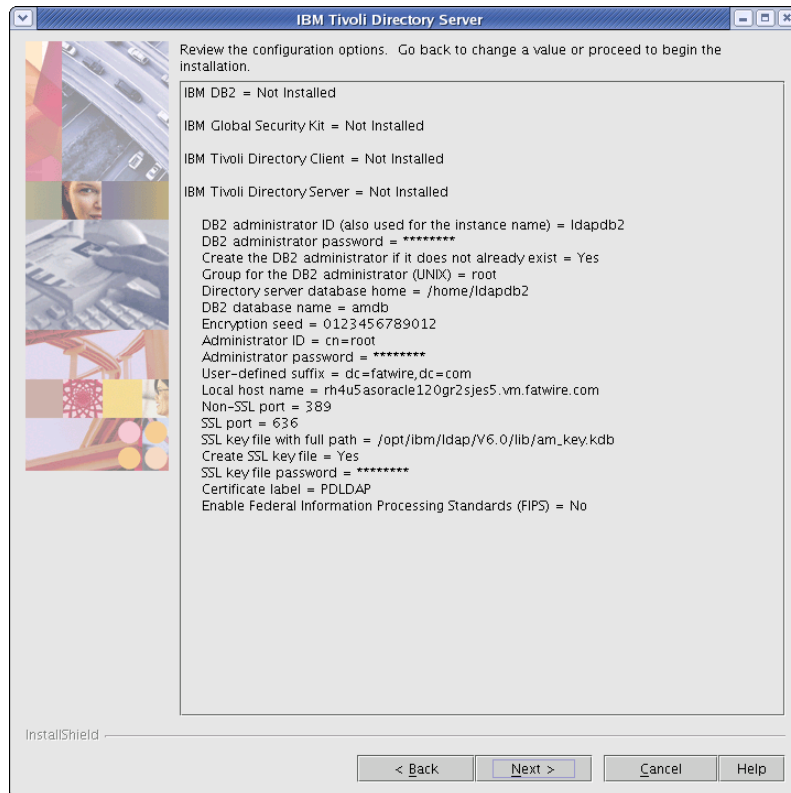
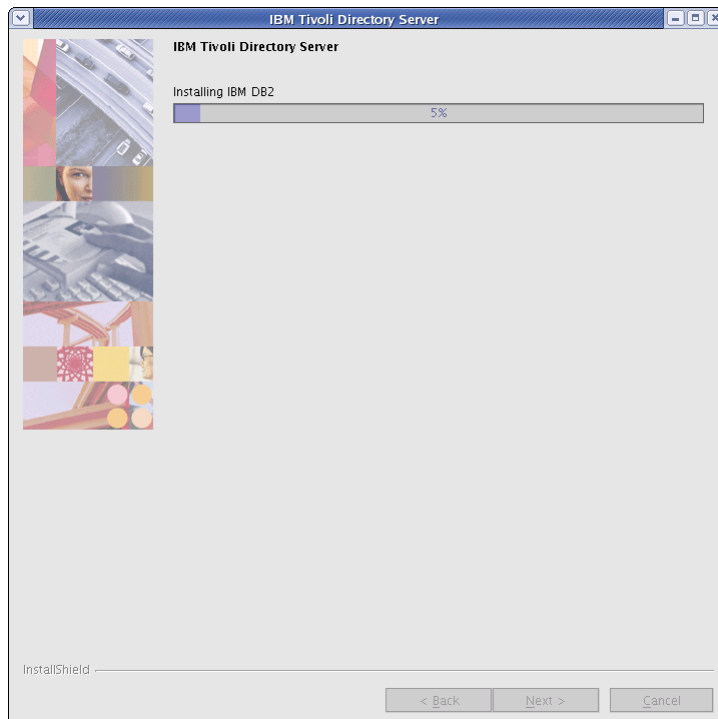
Enable Federal Information Processing Standards (FIPS)

InstallShield

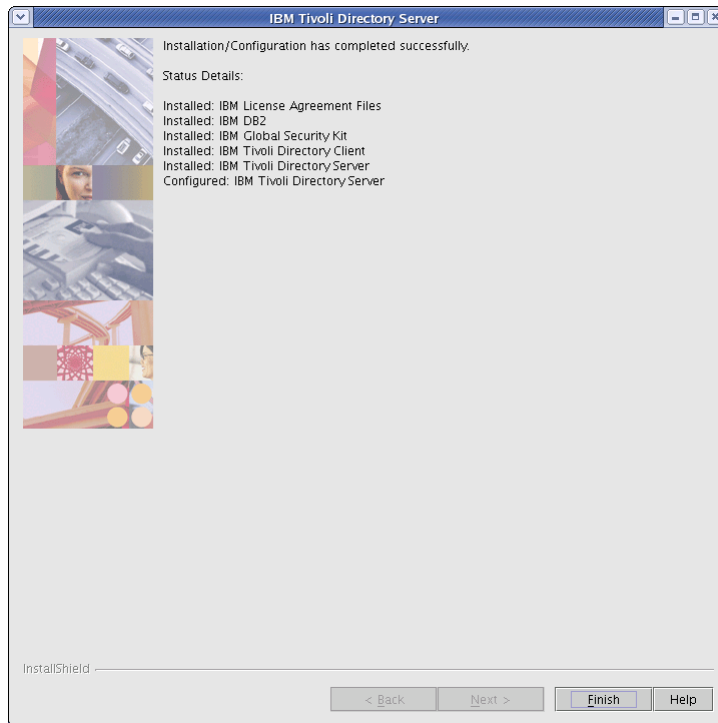
< Back Next > Cancel Help

10. Confirm that enough disk space exists for the installation to succeed and click **Next**.



11. Review the summary and click Next.**12. Wait for the installer to finish.**

13. Click **Finish**. The installation is now complete.



Configuring Tivoli Directory Server

Note

Only IBM TDS with sha encryption is supported by WebCenter Sites.

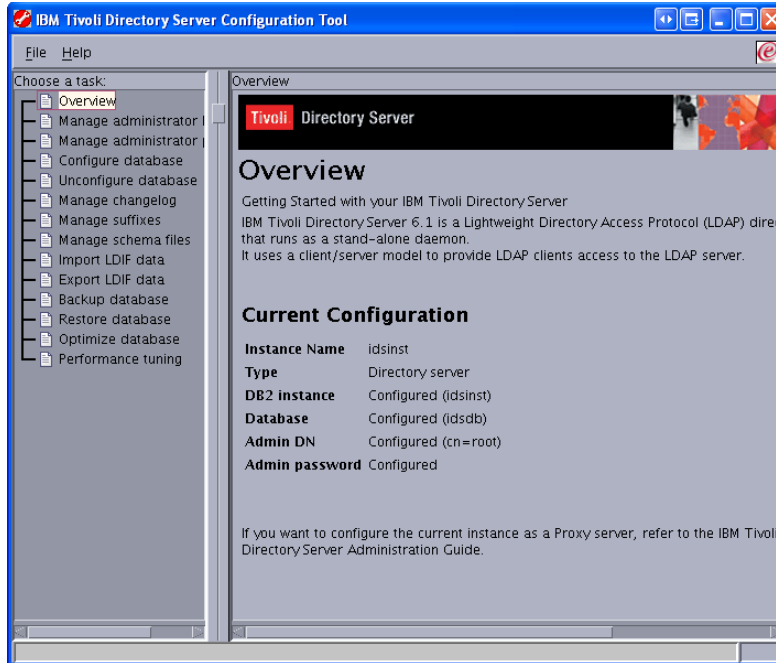
1. In a text editor open:
`/home/<ldap user>/idsslapd-<ldap user>/etc/ibmslapd.conf.`
2. Search for the `ibm-slapdPwEncryption` parameter and change the value to `sha`.
3. Save the change in the text editor.

Completing and Verifying the LDAP Configuration

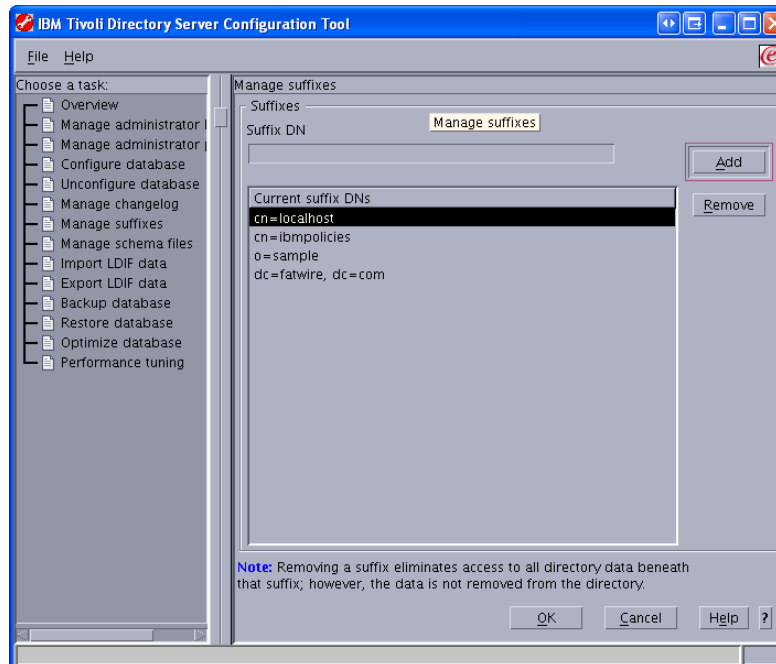
1. Start the IBM TDS instance:
`<LDAP Install directory>/sbin/idsslapd -I <instance name>`

2. Start the IBM TDS instance configuration tool (your display must be set in order to continue the configuration process):

```
<LDAP Install directory>/sbin/idsxcfg -I <name of instance>
```



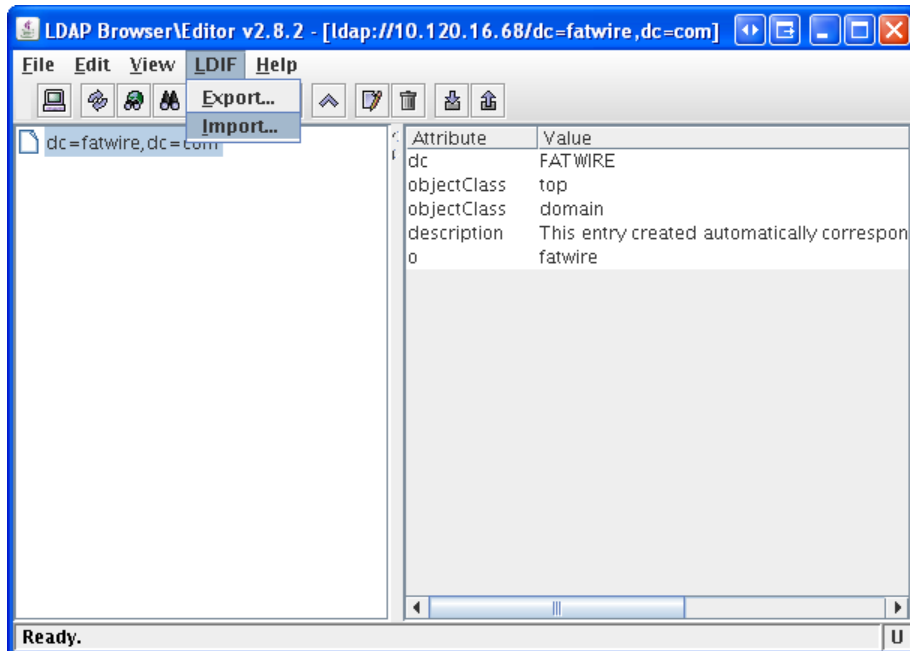
3. Select **Manage suffixes**.



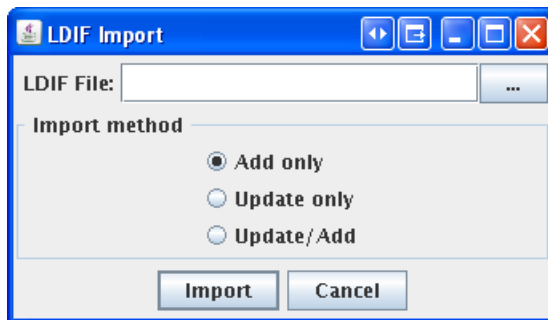
4. Make sure the User-defined suffix that was specified during installation appears in the list, then click **OK**.

Importing an LDIF file (LDAP Browser)

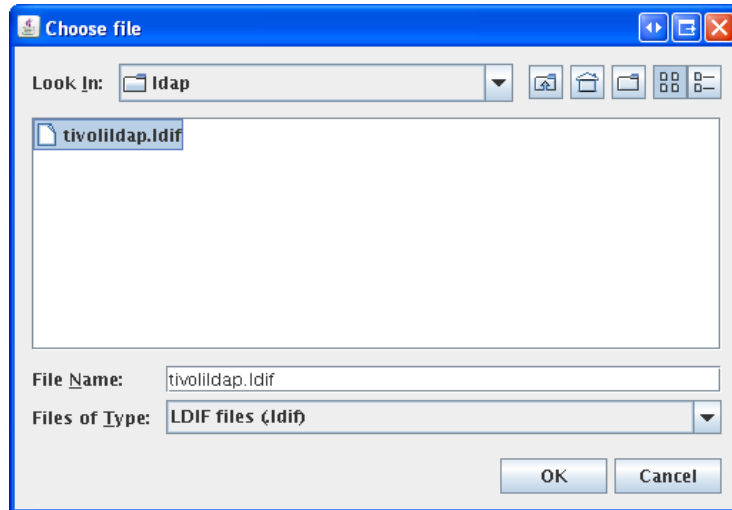
1. Start the IDM TDS instance:
`<LDAP Install directory>/sbin/idsslapd -I <instance name>`
2. Connect to IBM TDS using the LDAP browser, for instructions see [“Connecting to IBM TDS Using the LDAP Browser,”](#) on page 134.
3. Select: `dc=<domain>,dc=<ext>`
 - a. Click the **LDIF** menu, and select **Import**.



4. Click the **Add only** button.



5. Browse to the LDIF file `<cs_install_dir/ldap>/tivolildap.ldif` and click **OK**.



6. Click **Import**.

Note

The root entry will fail to import because it already exists, but all others will import successfully.

7. Click **OK**.



Importing an LDIF file (Configuration Tool)

1. Convert the LDIF file to Unix format using the `dos2unix` utility.

- **Linux:**
`dos2unix <tivolildap.ldif>`
- **Solaris:**
`mv tivolildap.ldif > tivolildap2.ldif`
`dos2unix tivoli.ldap2.ldif > tivolildap.ldif`

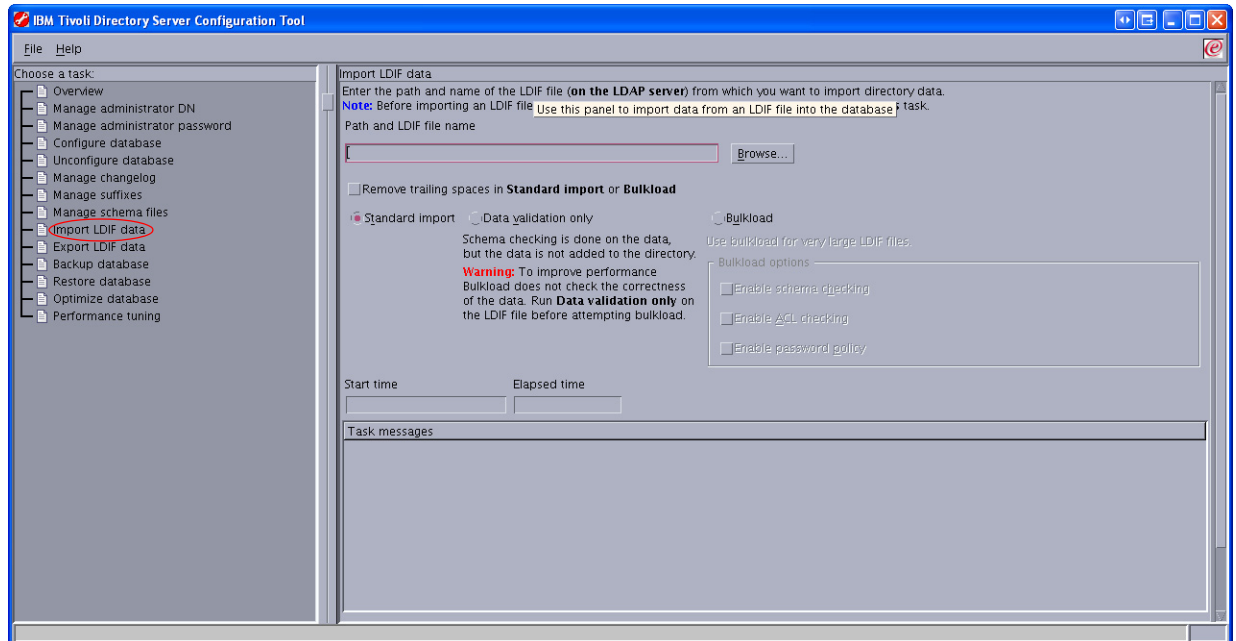
2. Stop the IBM TDS instance:

```
<LDAP Install directory>/bin/ibmdirctl stop -h localhost -D
cn=root -w <password for cn=root>
```

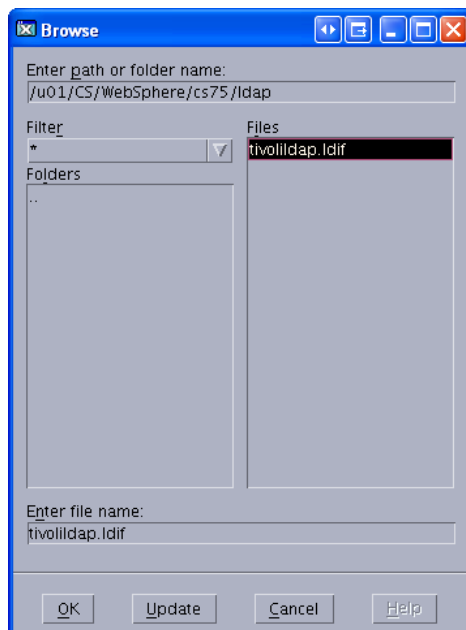
3. Start the IBM TDS instance configuration tool (your display must be set in order to continue with the import process):

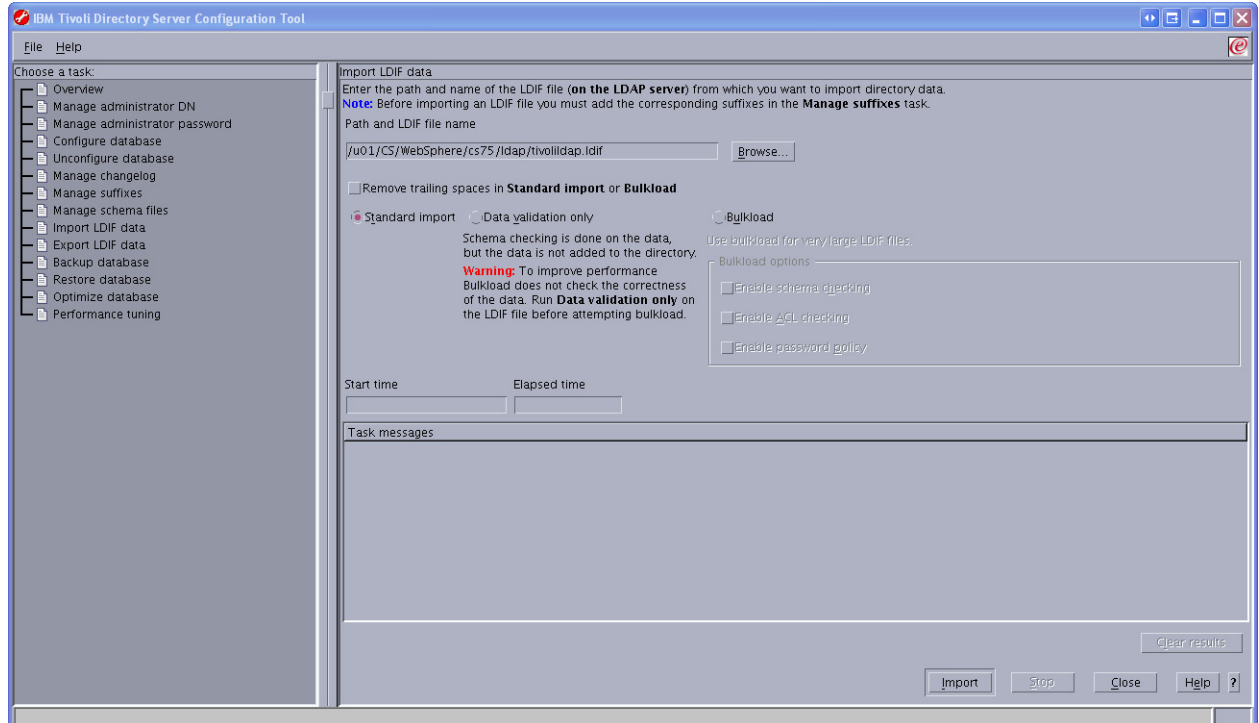
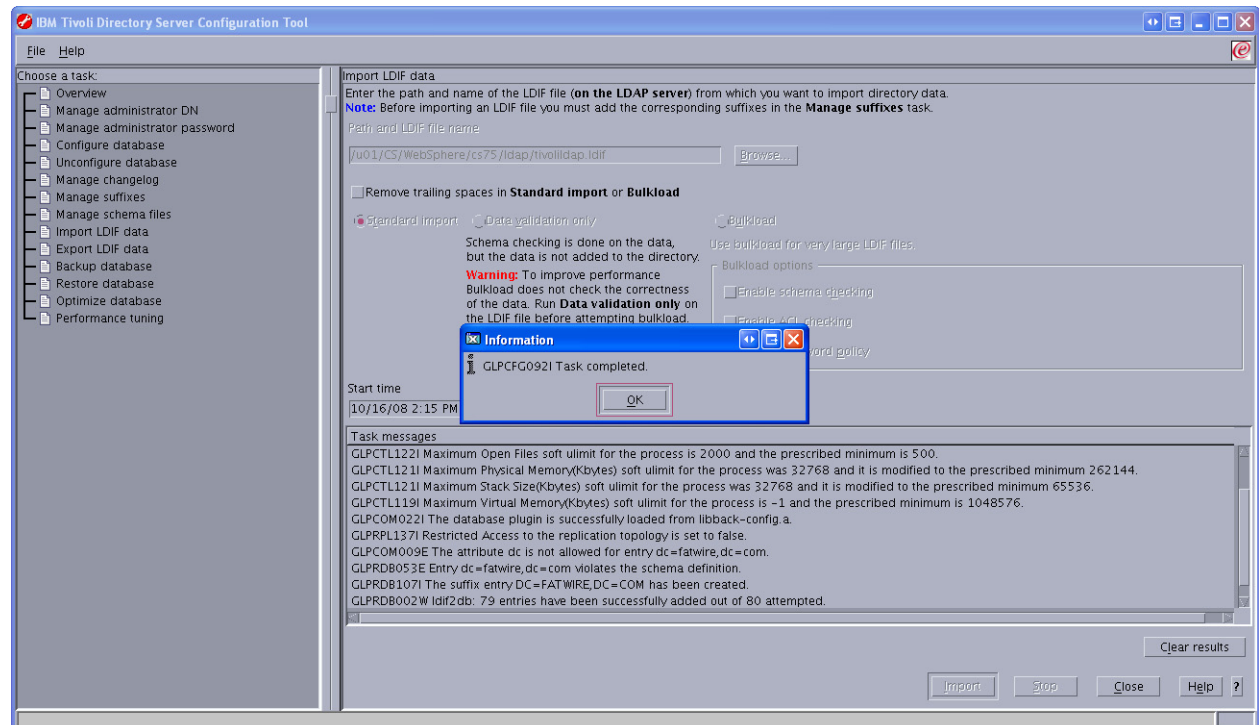
```
<LDAP Install directory>/sbin/idsxcfg -I <name of instance>
```

4. Select **Import LDIF data**.



5. Click **Browse**.
6. Browse to the LDIF file you wish to import and click **OK**.



7. Click **Import**.8. Click **OK** when the import is complete.

Adding Users and ACLs using an LDIF file

1. Create a blank LDIF file (for example, addstuff.ldif).
2. For each user that you wish to add, add the following to the LDIF file:

```
dn: uid=<User_Name>,cn=users,dc=<domain>,dc=<ext>
userPassword: <password>
uid: <User_Name>
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
sn: <User_Name>
cn: <User_Name>
```
3. For each ACL you wish to add, add the following to the LDIF file:

```
dn: cn=<ACL Name>,cn=groups,dc=<domain>,dc=<ext>
objectClass: top
objectClass: groupOfNames
member: uid=<User_Name 1>,cn=users,dc=<domain>,dc=<ext>
member: uid=<User_Name 2>,cn=users,dc=<domain>,dc=<ext>
.
.
.
member: uid=<User_Name n>,cn=users,dc=<domain>,dc=<ext>
```
4. Import the LDIF file by following the steps in the section [“Importing an LDIF file \(LDAP Browser\),”](#) on page 129 or [“Importing an LDIF file \(Configuration Tool\),”](#) on page 130.

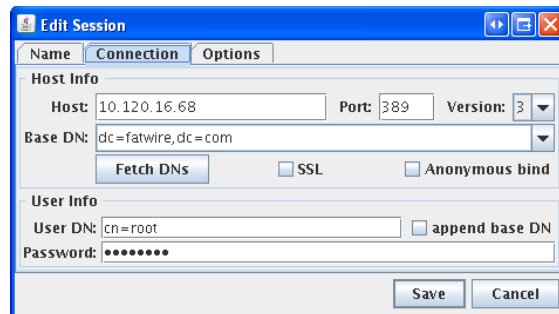
Connecting to IBM TDS Using the LDAP Browser

1. Download and install the LDAP browser.
2. Start the LDAP browser:
 - `./lbe.sh`
3. Fill in the required fields:
 - **Host:** Enter the IP or hostname of IBM TDS.

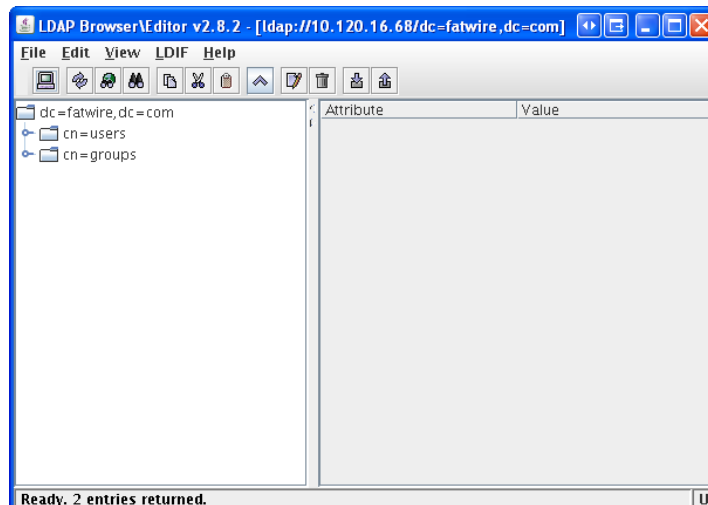
Note

The default port which IBM TDS runs on is 389.

- **Port:** Enter the port on which IBM TDS is running.
- **Base DN:** Enter the user-defined suffix that was entered during the installation of IBM TDS (see [step 8 on page 123](#) for more information about the User-defined suffix).
- **Anonymous bind:** Deselect the check box
- **User DN:** Enter `cn=root`
- **Password:** Enter the password for `cn=root`



4. Click **Save**.



Chapter 10

Setting Up OpenLDAP 2.3.x

This chapter explains how to set up OpenLDAP for use with WebCenter Sites.

Note

You must set OpenLDAP **before** you run the WebCenter Sites-LDAP integrator.

It contains the following sections:

- [OpenLDAP Commands](#)
- [Installing OpenLDAP](#)
- [Configuring OpenLDAP](#)
- [Adding WebCenter Sites 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 WebCenter Sites.

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 WebCenter Sites), 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 142](#).

2. When prompted for a password, enter the Root DN user password you specified in [step d on page 143](#).

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 142](#).
- `<root_dn_password>` is the Root DN user password you specified in [step d on page 143](#).
- `<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`

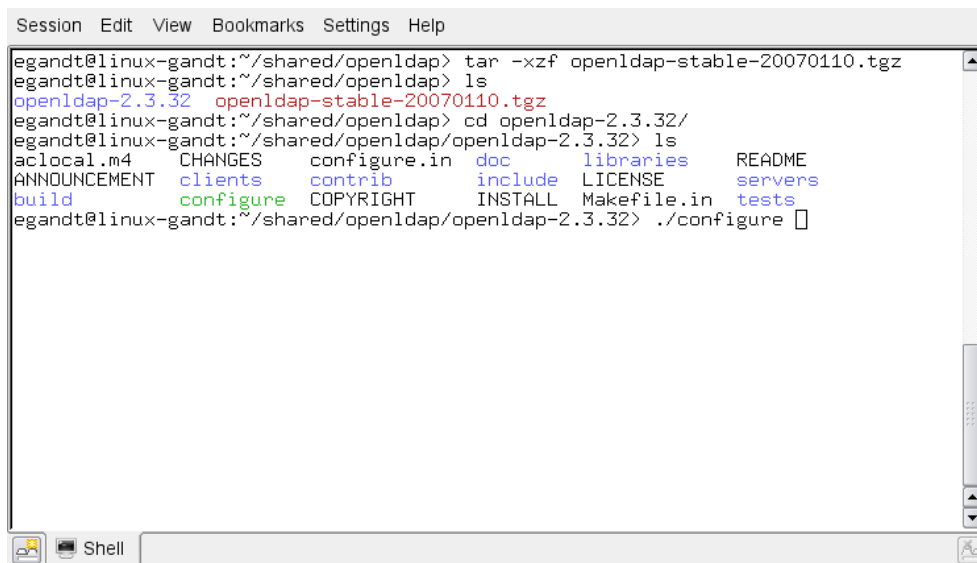
2. Decompress the archive:

- 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/slaped/back-sql/Makefile
config.status: creating servers/slaped/shell-backends/Makefile
config.status: creating servers/slaped/slapi/Makefile
config.status: creating servers/slaped/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/slaped/backends.c
  Add config ...
  Add ldif ...
  Add bdb ...
  Add hdb ...
  Add monitor ...
  Add relay ...
Making servers/slaped/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 )

```

- b. 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 WebCenter Sites Schema to OpenLDAP

This section shows you how to add WebCenter Sites schema to your OpenLDAP server.

Note

If you are copying the contents of the sample LDIF file below, make sure to insert an empty line between `dn` sections and at the end of the file.

To configure OpenLDAP for WebCenter Sites

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

```

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 142](#).

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 142](#).
- <root_dn_password> is the Root DN user password you specified in [step d on page 143](#).

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 142](#).

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 WebCenter Sites LDAP integrator. For instructions, see *Oracle WebCenter Sites: Integrating with LDAP*.

Modifying User Passwords

When you ran the WebCenter Sites LDAP integrator, all WebCenter Sites users (except `fwadmin`, `ContentServer`, and `DefaultReader`) were assigned the password which you entered in the “WebCenter Sites 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 WebCenter Sites system, or your WebCenter Sites installation will not function properly. This is because the WebCenter Sites-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 WebCenter Sites users:

User	Password
<code>DefaultReader</code>	<code>SomeReader</code>
<code>ContentServer</code>	The password you supplied during WebCenter Sites installation
<code>fwadmin</code>	The password you supplied during WebCenter Sites installation
All other users on your WebCenter Sites system	The password you supplied during WebCenter Sites-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](#)

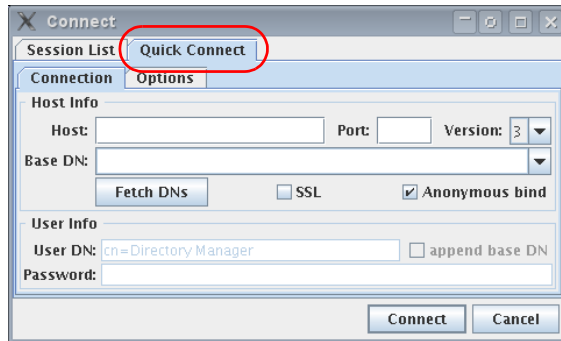
Modifying User Passwords Using an LDAP Browser

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`

3. Click the **Quick Connect** tab.

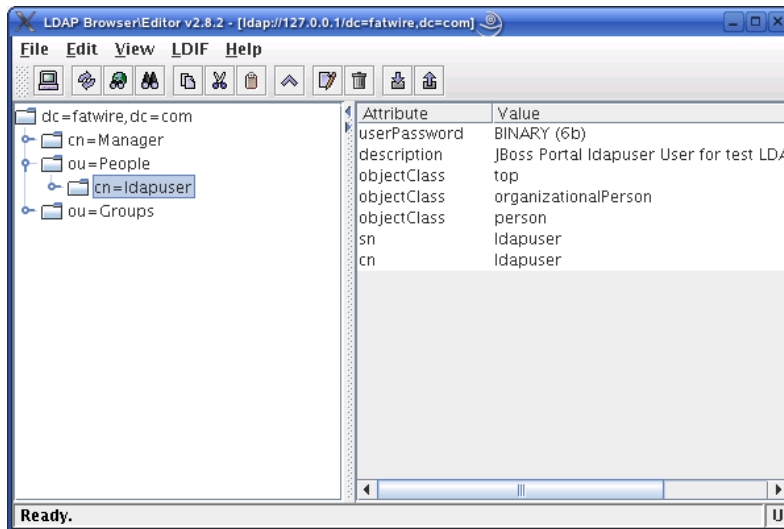


4. Fill out the fields as follows:

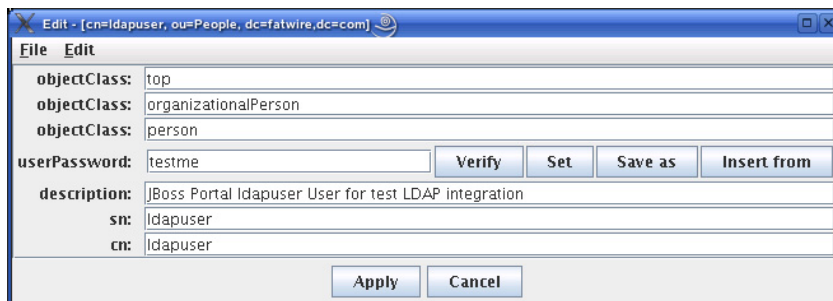
Field	Value
Hostname	The host name of your OpenLDAP server.
Port	389
Version	3
Base DN	The Base DN you specified in step a on page 142 .
Anonymous bind	Yes (select check box)
User DN	cn=Manager
Append base DN	Yes (select check box)
Password	The Root DN user password you specified in step d on page 143 .

5. Click **Connect**.

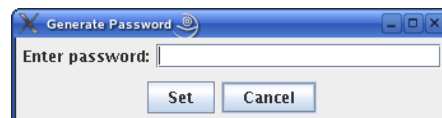
6. In the left-hand tree, expand the **ou=People** node.



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

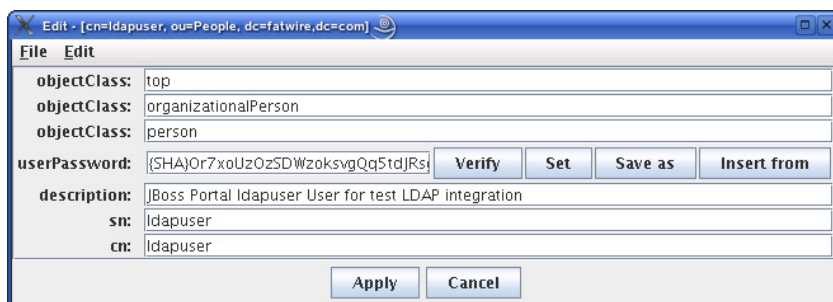


9. In the pop-up window, enter the user's password and click **Set**.



The password appears in its encrypted form.

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



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

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

1. 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}yDUT5RCpBAU80P0PW8gaHnsmYmLlUL8
```

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.

2. 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 142](#).
- `<root_dn_password>` is the Root DN user password you specified in [step d on page 143](#).

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

3. Change the user's password. Issue the following commands:
 - a. `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 142](#).
 - b. `changetype:modify`
 - c. `replace:userPassword`
 - d. `userpassword:<password_hash>`
where `<password_hash>` is the hash generated by the `sldapasswd` command in [step 1](#) of this procedure.
 - e. Press **Ctrl+D**.
 - f. 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 11

Setting Up the WebLogic 10.3.5 Embedded LDAP Server

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

Note

You must set up WebLogic LDAP **before** you run the WebCenter Sites-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. Re-enter the password in the **Confirm Credential** field for verification.
 - d. Click **Save**.

The screenshot displays the Oracle WebLogic Server Administration Console interface. The main content area is titled "Settings for cs8_cluster_hotspot" and is under the "Security" tab, specifically the "Embedded LDAP" sub-tab. The page includes a "Save" button and a description: "This page allows you to configure the embedded LDAP server for this WebLogic Server domain." The configuration fields are as follows:

- Credential:** A text field containing masked characters (dots). A tooltip indicates: "The credential (usually a password) used to connect to the embedded LDAP server. [More Info...](#)"
- Confirm Credential:** A text field containing masked characters.
- Backup Hour:** A text field with the value "23". A tooltip indicates: "The hour at which the embedded LDAP server should be backed up. [More Info...](#)"
- Backup Minute:** A text field with the value "5". A tooltip indicates: "The minute at which the embedded LDAP server should be backed up. [More Info...](#)"
- Backup Copies:** A text field with the value "7". A tooltip indicates: "The maximum number of backup copies that should be made for the embedded LDAP server. [More Info...](#)"
- Cache Enabled:** A checkbox that is checked. A tooltip indicates: "Specifies whether a cache is used with the embedded LDAP server. [More Info...](#)"
- Cache Size:** A text field with the value "32". A tooltip indicates: "The size of the cache (in kilobytes) that is used with the embedded LDAP server. [More Info...](#)"
- Cache TTL:** A text field with the value "60". A tooltip indicates: "The time-to-live of the cache (in seconds) that..."

On the left side of the console, there are three panels: "Change Center" (with "View changes and restarts" and a note about configuration editing), "Domain Structure" (showing a tree view with "cs8_cluster_hotspot" selected), and "System Status" (showing "Health of Running Servers" with a bar chart indicating 1 OK server).

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 Oracle WebLogic Server Administration Console. The main content area is titled "Settings for myrealm" and has several tabs: Configuration, Users and Groups, Roles and Policies, Credential Mappings, **Providers**, and Migration. Under the "Providers" tab, there are sub-tabs for Authentication, Password Validation, Authorization, Adjudication, Role Mapping, and Auditing. The "Authentication" sub-tab is active, showing a description of authentication providers and a table of existing providers.

Authentication Providers

<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
<input type="checkbox"/>	falcon	WebLogic 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

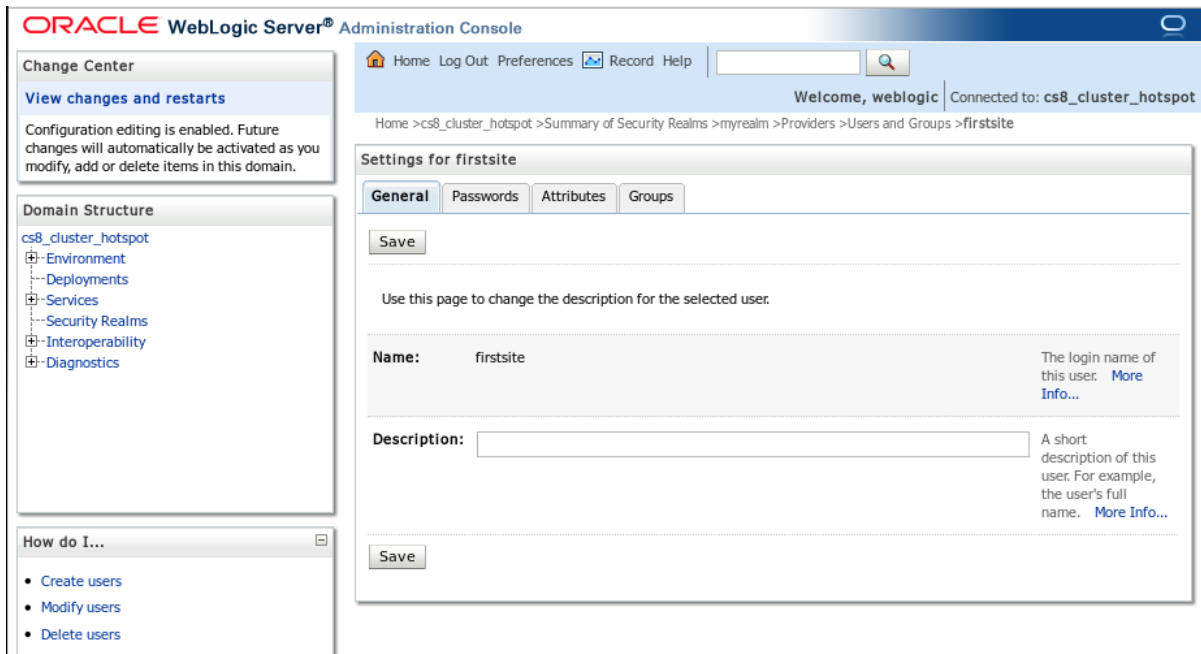
1. Log in to the WebLogic Server Administration Console.
2. In the “Domain Structure” tree, click **Security Realms**.
3. In the workspace, click **myrealm** and select the **Users and Groups** tab.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area is titled 'Settings for myrealm' and has tabs for 'Configuration', 'Users and Groups', 'Roles and Policies', 'Credential Mappings', 'Providers', and 'Migration'. The 'Users and Groups' tab is active, showing a table of users. The table has columns for 'Name', 'Description', and 'Provider'. The 'weblogic' user is highlighted, with a description stating 'This user is the default administrator.' and a provider of 'DefaultAuthenticator'. Other users listed include OracleSystemUser, ContentServer, DefaultReader, fwadmin, Conrad, firstsite, Mark, Mary, and Napoleon. The console also shows a 'Domain Structure' tree on the left and a 'System Status' panel at the bottom left.

Name	Description	Provider
OracleSystemUser	Oracle application software system user.	DefaultAuthenticator
weblogic	This user is the default administrator.	DefaultAuthenticator
ContentServer		DefaultAuthenticator
DefaultReader		DefaultAuthenticator
fwadmin		DefaultAuthenticator
Conrad		DefaultAuthenticator
firstsite		DefaultAuthenticator
Mark		DefaultAuthenticator
Mary		DefaultAuthenticator
Napoleon		DefaultAuthenticator

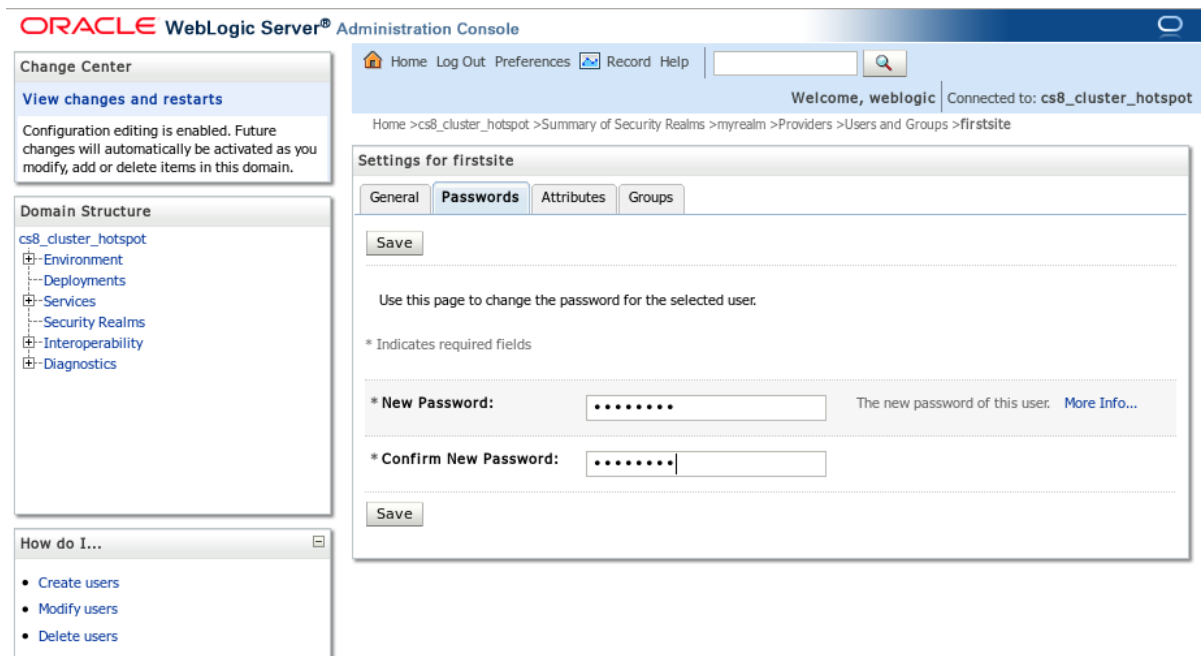
4. Click the user whose password you want to change.

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



The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains a 'Change Center' section with a 'View changes and restarts' button and a 'Domain Structure' tree showing a hierarchy from 'cs8_cluster_hotspot' down to 'Diagnostics'. Below the tree is a 'How do I...' section with links for 'Create users', 'Modify users', and 'Delete users'. The main content area shows the 'Settings for firstsite' page with tabs for 'General', 'Passwords', 'Attributes', and 'Groups'. The 'General' tab is active, displaying a 'Save' button, a description prompt, and two fields: 'Name' (set to 'firstsite') and 'Description' (empty). Each field has a 'More Info...' link.

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



The screenshot shows the Oracle WebLogic Server Administration Console with the 'Passwords' tab selected in the 'Settings for firstsite' page. The 'Save' button is at the top. Below it is a description prompt. A note states '* Indicates required fields'. There are two required fields: '* New Password:' and '* Confirm New Password:', both with masked input boxes. Each field has a 'More Info...' link. A 'Save' button is at the bottom.

6. Click **Save**.

Chapter 12

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 WebCenter Sites.

Note

You must set up ADS **before** you run the WebCenter Sites-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 WebCenter Sites](#)
- [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 WebCenter Sites.

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 type other than Web Edition).

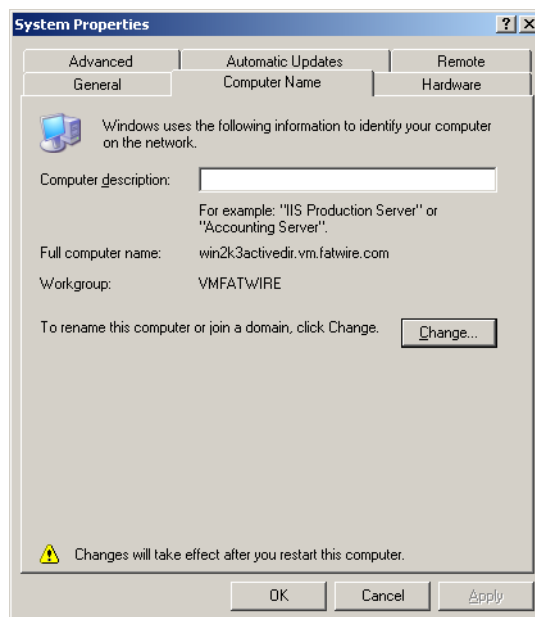
When the installation is complete, leave the installation disc in the drive – you will need it to complete the installation of ADS.

B. Set the Machine's Name and Suffix

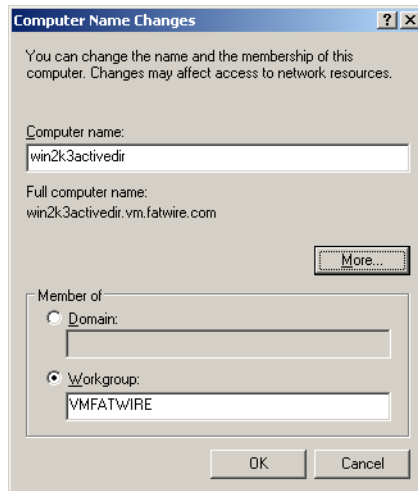
1. Open the “System Properties” dialog.

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.

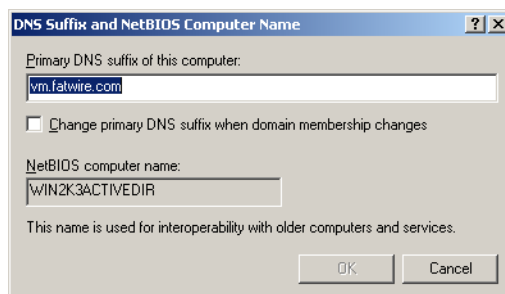
2. Select the **Computer Name** tab.
3. Click **Change**.



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

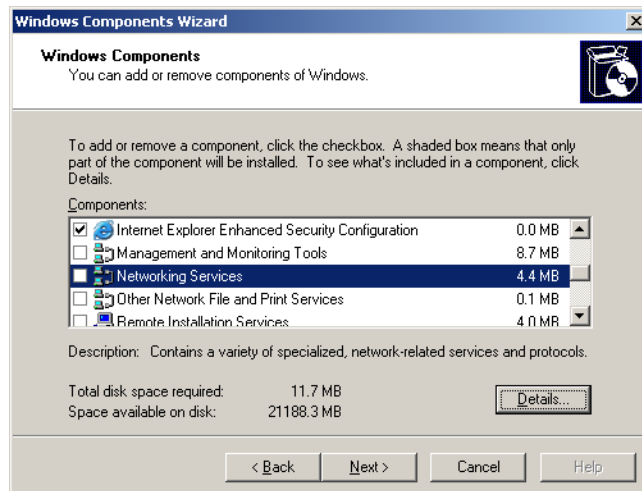
Configure the machine's network settings as follows:

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.

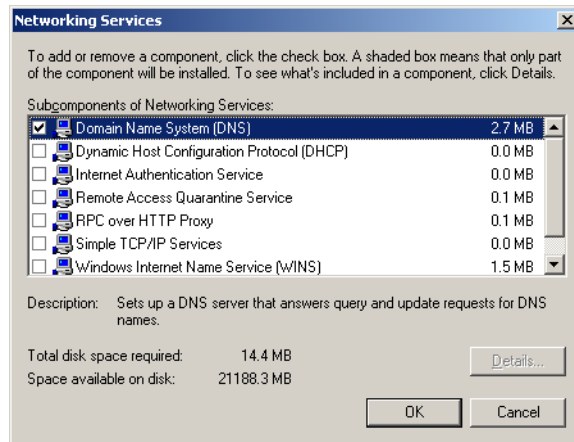
For instructions on configuring your machine's network settings, see the Windows Server 2003 documentation.

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**.

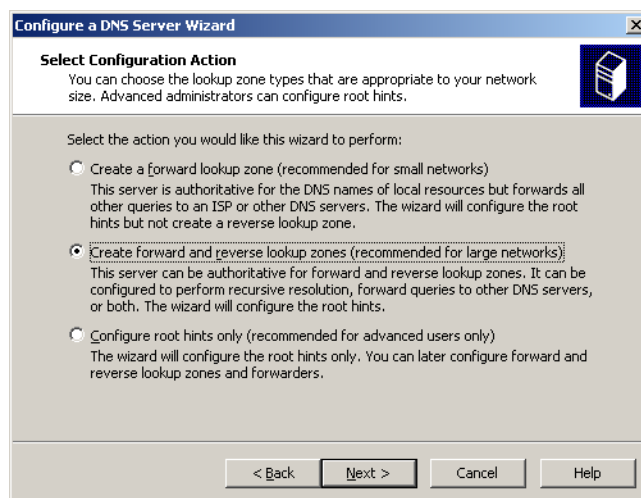


E. Configure the Local DNS Server

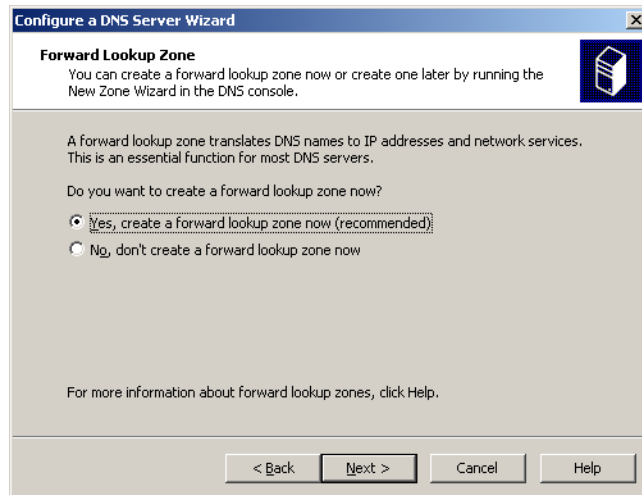
1. In the “Control Panel,” double-click the **Administrative Tools** icon.
2. Double-click the **DNS** icon.
3. In the “dnsmgmt console,” select the machine name you entered in [step 4 on page 159](#).
4. Right-click the machine name and select **Configure this DNS Server** from the context menu.
5. In the “Configure a DNS Server Wizard” pop-up window that appears, click **Next**.



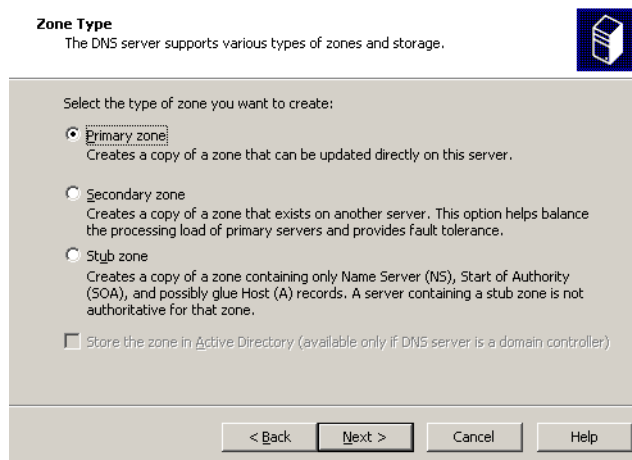
6. In the “Select Configuration Action” screen, select the **Create forward and reverse lookup zones** radio button and click **Next**.



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 159](#). 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:

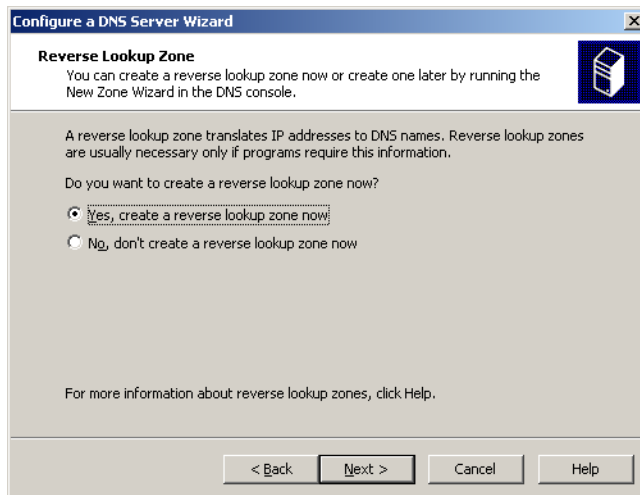
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

< Back Next > Cancel Help

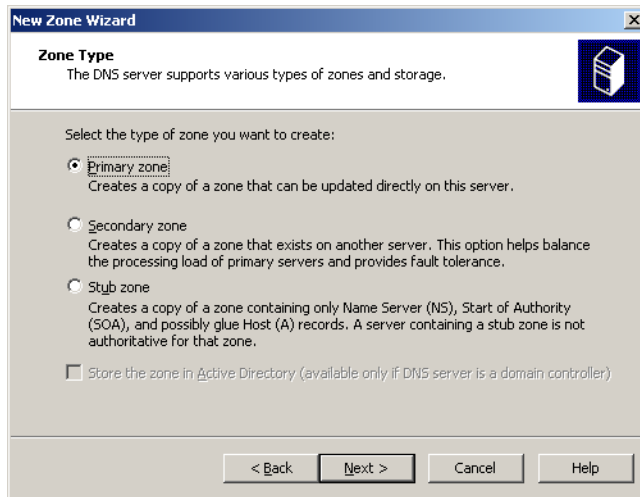
11. In the “Dynamic Update” screen, select the **Allow both nonsecure and secure dynamic updates** radio button and click **Next**.



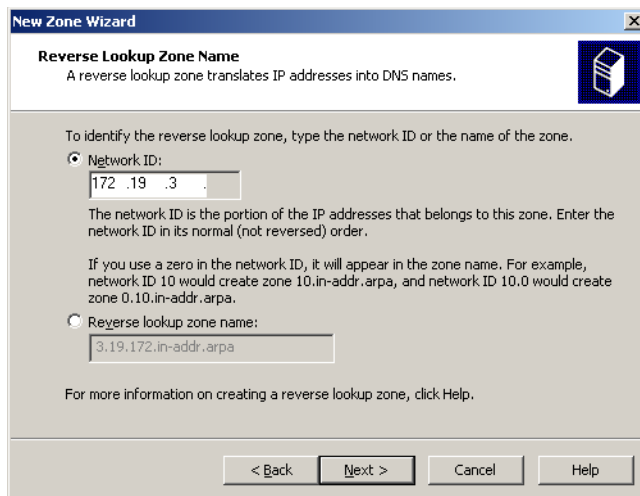
12. In the “Reverse Lookup Zone” screen, select the **Yes, create reverse lookup zone now** radio button and click **Next**.



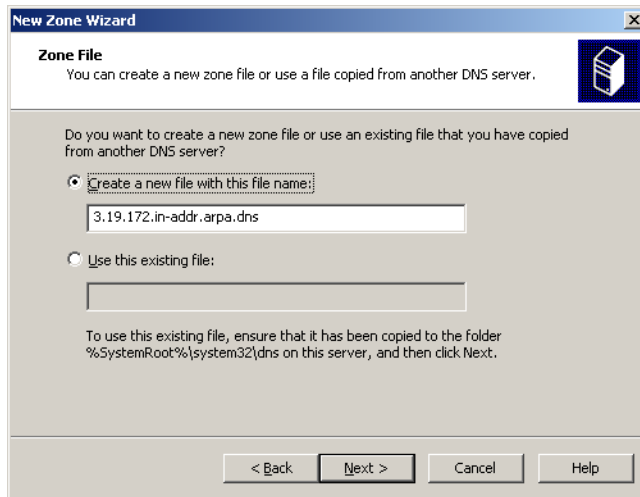
13. In the “Zone Type” screen, select the **Primary Zone** radio button and click **Next**.



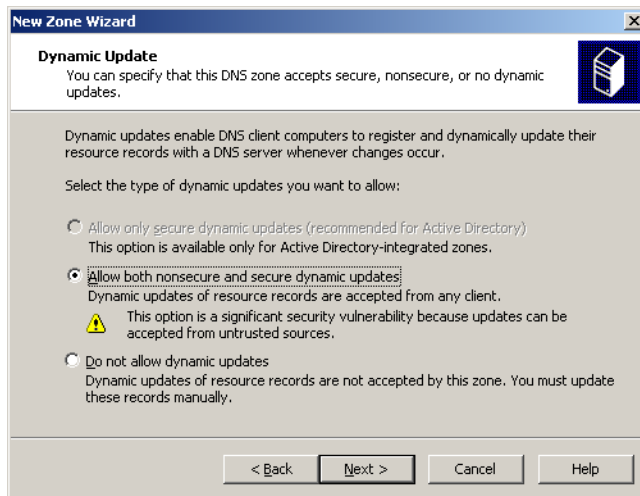
14. In the “Reverse Lookup Zone Name” screen, select the **Network ID** radio button and enter the first three octets of the machine’s IP address (you set this address in [step 1 on page 160](#)), then click **Next**.



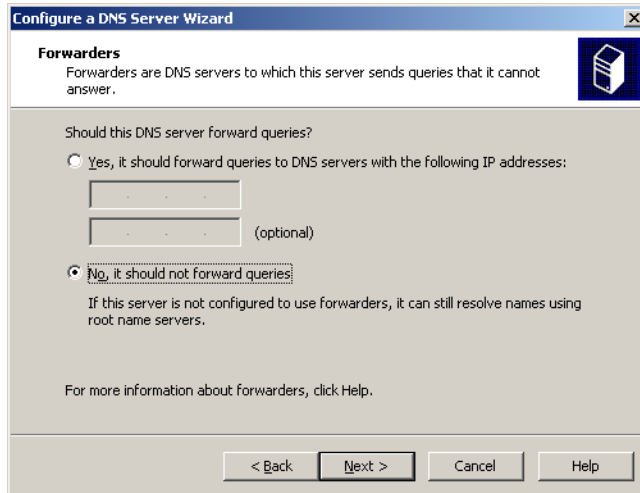
15. In the “Zone File” screen, keep the default zone file name and click **Next**.



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**.



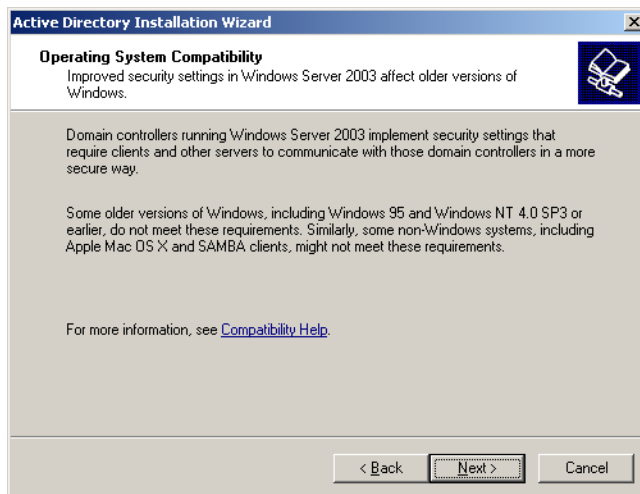
19. Close or minimize the DNS server window.

F. Install MS Active Directory Server 2003

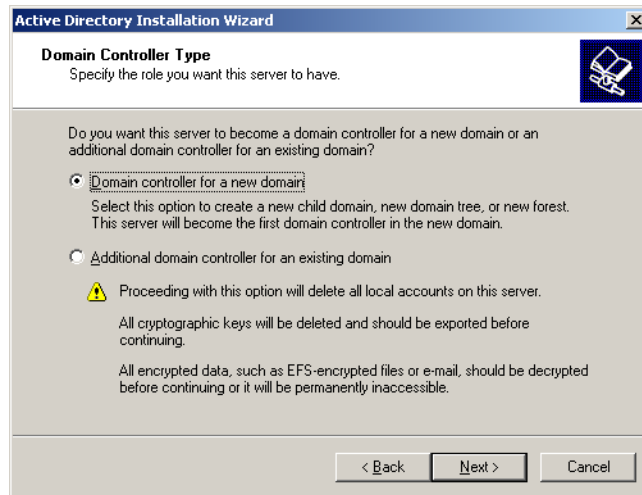
1. Click **Start**, then **Run**, and enter **dcpromo** in the “Run” dialog box.
2. In the “Welcome to the Active Directory Installation Wizard” screen, click **Next**.



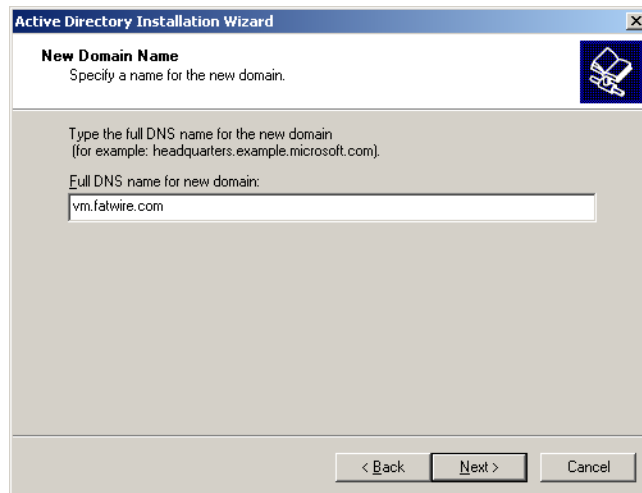
3. In the “Operating System Compatibility” screen, click **Next**.



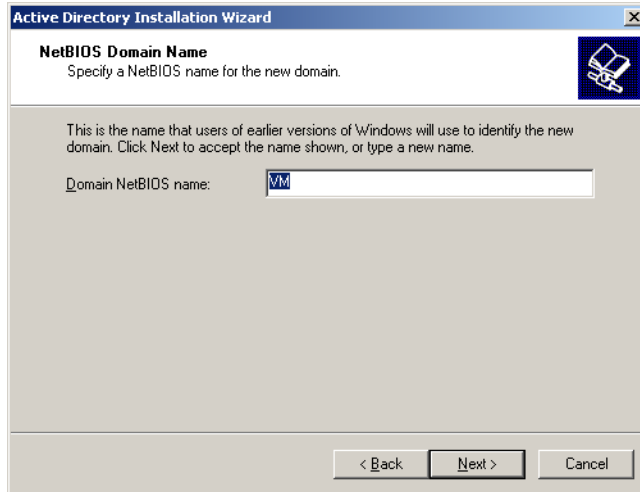
4. In the “Domain Controller Type” screen, select the **Domain controller for a new domain** radio button and click **Next**.



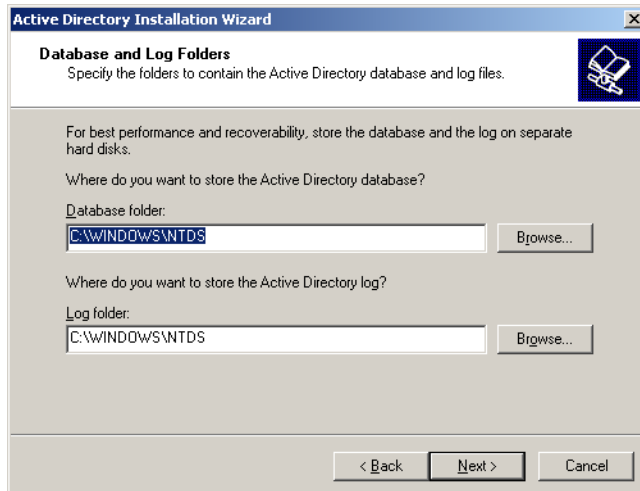
5. “In the “Create a New Domain” screen, select the **Domain in a new forest** radio button and click **Next**.
6. In the “New Domain Name” screen, enter the DNS name you entered in [step 9 on page 164](#), then click **Next**.



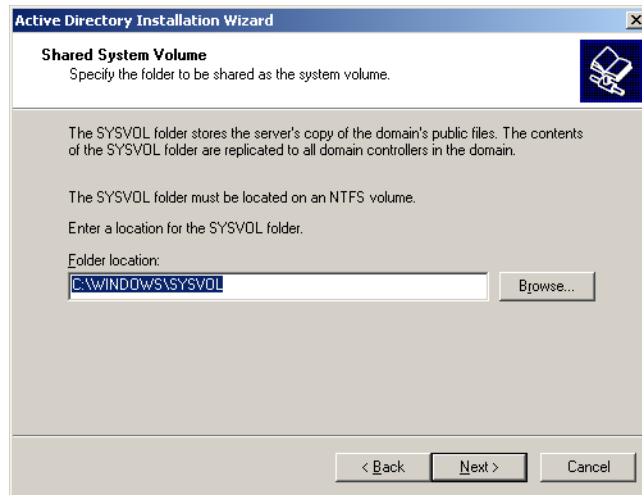
7. In the “NetBIOS Domain Name” screen, keep the default value and click **Next**. Make a record of this value.



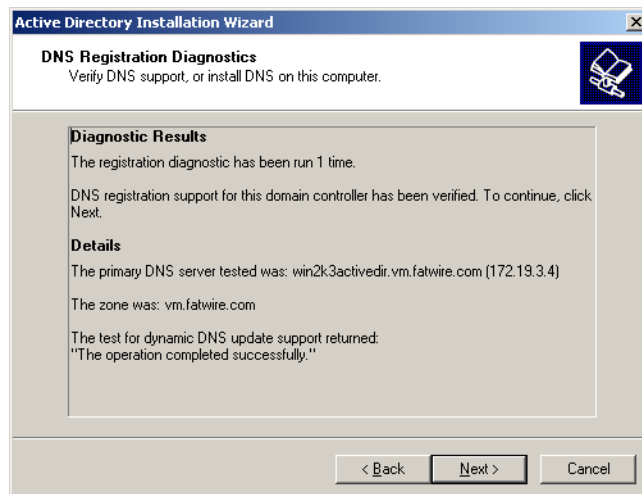
8. In the “Database and Log Folders” screen, click **Next**.



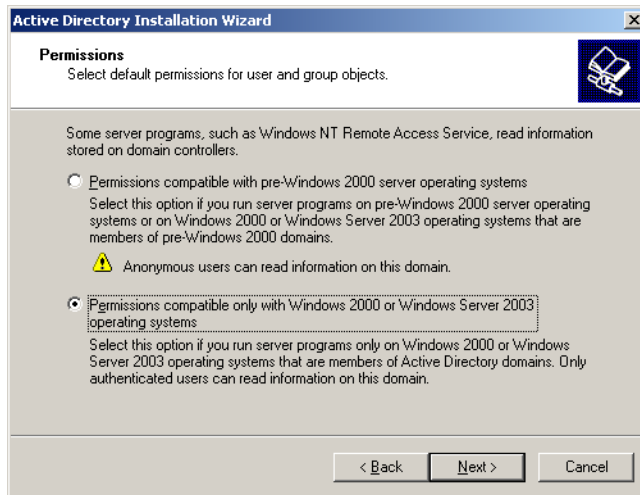
9. In the “Shared System Volume” screen, click **Next**.



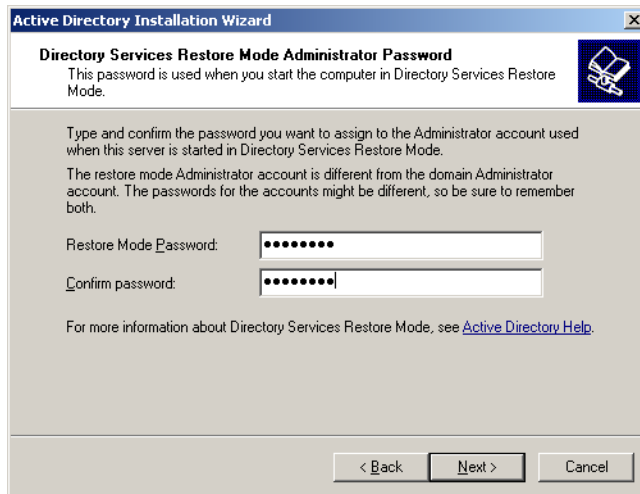
10. In the “Diagnostic Results” screen, make sure that the diagnostic has completed successfully, then click **Next**. If the diagnostic fails, correct the indicated problem, click **Back** and then **Next** to rerun the diagnostic.



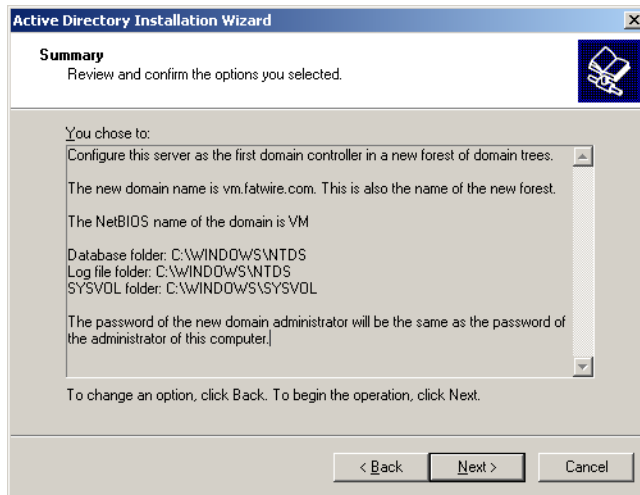
11. In the “Permissions” screen, select the **Permissions compatible only with Windows 2000 and Windows 2003 operating systems** and click **Next**.



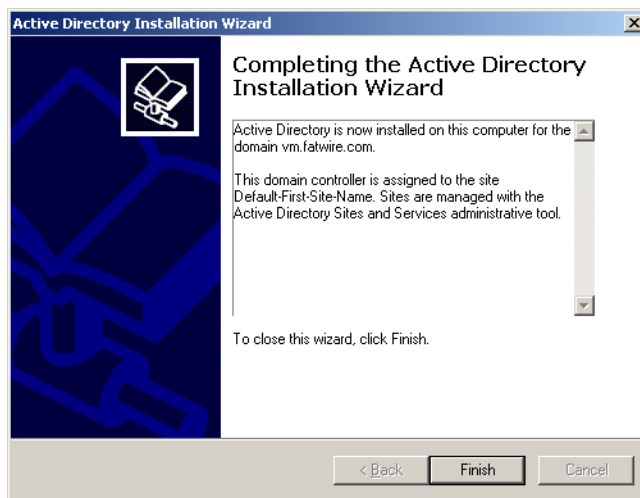
12. In the “Directory Services Restore Mode Administrator Password” screen, enter a password and click **Next**. Make a record of this password.



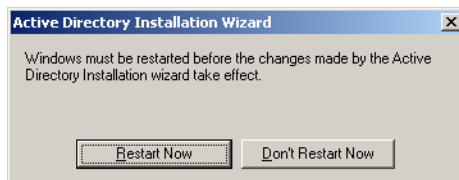
13. In the “Summary” screen, click **Next**.



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.



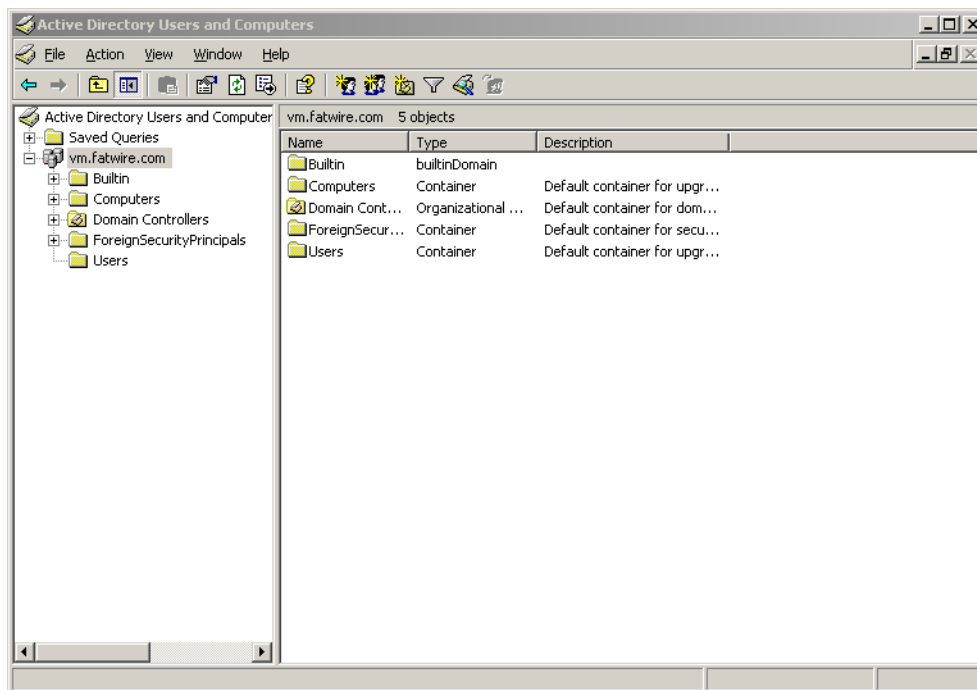
Active Directory Server is now installed and ready for use.

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**.

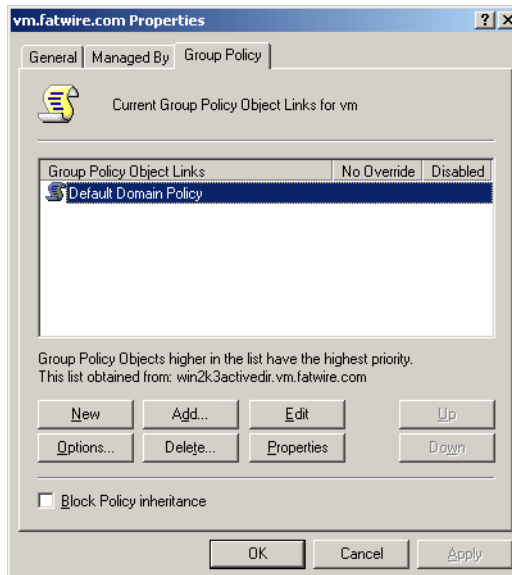
The “Active Directory Users and Computers” console loads.



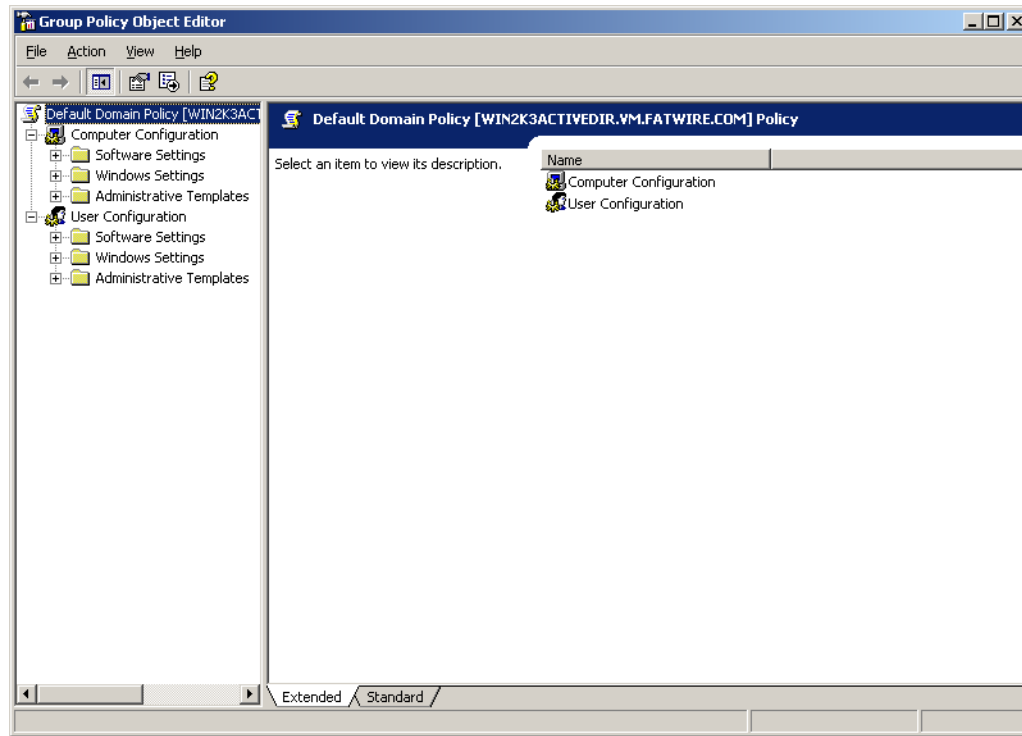
Configuring ADS Password Security for WebCenter Sites

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

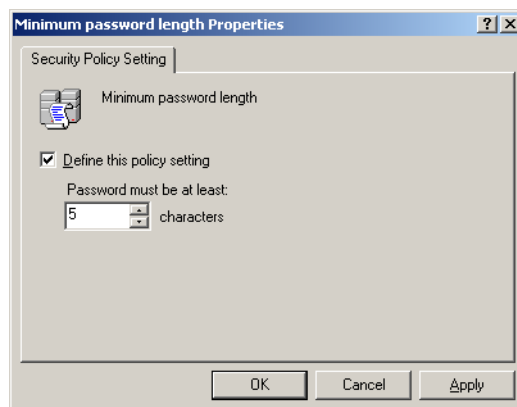
1. Open the “Active Directory Users and Computers” console.
2. In the tree on the left, right-click the desired domain and select **Properties** from the context menu.
3. In the dialog that appears, select the **Group Policy** tab.



4. The “Group Policy Object Editor” appears, showing the group policy you selected.



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



8. Double-click the **Password must meet complexity requirements** item.
9. In the pop-up window that appears, select the **Disabled** radio button and click **OK**.
10. From the **File** menu, select **Exit**, then click **OK**.
11. 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**.

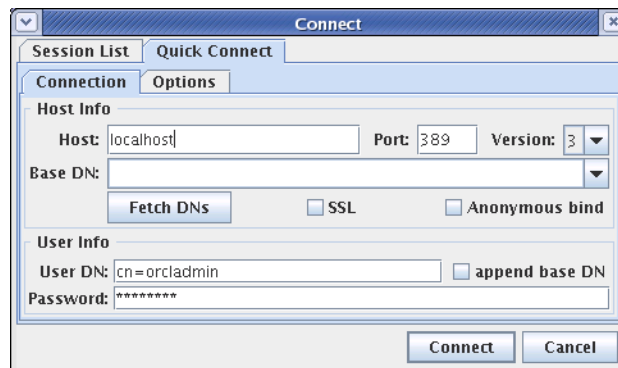
Connecting to ADS Using an LDAP Browser

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:** deselect
 - **User DN:** administrator<DNS_suffix>
 - **Append base DN:** deselect
 - **Password:** <ADS_password> (you created this password in [step 12 on page 173](#))



4. Click **Connect**.

Part 4

Installing and Configuring Authentication Services

WebCenter Sites can be integrated with supported third-party applications that provide authentication services and single sign-on.

This part contains the following chapters:

- [Chapter 13, “Clustering the Central Authentication Service Application”](#)
- [Chapter 14, “Oracle Access Manager Integration Setup”](#)

Chapter 13

Clustering the Central Authentication Service Application

WebCenter Sites uses the Central Authentication Service (CAS) web application for authentication and single sign-on. CAS can also be clustered to balance the load of user authentication for WebCenter Sites. The CAS web application is deployed during the installation of WebCenter Sites. The installation process configures and deploys only the primary cluster member. Additional cluster members must be configured and deployed manually.

This chapter contains the following sections:

- [Deploying Secondary CAS Cluster Members](#)
- [Redeploying CAS on a New Server](#)

Deploying Secondary CAS Cluster Members

The WebCenter Sites installer configures and deploys CAS only on the primary WebCenter Sites cluster member. If you are clustering CAS to balance the load of user authentications, you must configure and deploy secondary CAS cluster members manually.

Before you begin, make sure you have completed the following:

- You have configured your application server to support CAS clustering.
- WebCenter Sites and CAS have been installed successfully on the primary cluster member.

If either one of these steps have not been completed, refer to the Oracle WebCenter Sites installation guide for the application server you are using.

To configure and deploy a secondary CAS cluster member

1. Copy the following configuration files from the `<cs_install_dir>/bin` directory of the primary member to the `<cs_install_dir>/bin` of the secondary member:
 - `cas.properties`
 - `host.properties`
 - `jbossTicketCacheReplicationConfig.xml`
2. Update the following property in the `host.properties` file:

```
host.name=cas-<host name of server where cluster member will  
be deployed>-<cluster member number>
```

Note

The host name and member number should be unique for each cluster member. For example, for a primary and secondary member, the property might differ as follows:

```
host.name=cas-10.120.12.123-1  
host.name=cas-10.120.12.127-2
```

3. Update the `jbossTicketCacheReplicationConfig.xml` file as follows:
 - In the "ClusterName" attribute, replace `TreeCache-Cluster` with a unique name:

```
<attribute name="ClusterName">TreeCache-Cluster  
</attribute>
```

Note

This name must be the same for all cluster members. If you are using more than one CAS cluster, make sure to use a different name for each cluster.

- In the "ClusterConfig" attribute, update the following parameters:

```
<UDP mcast_addr="multicast address"
    mcast_port="multicast port"
    bind_addr="host name of server where cluster member
              will be deployed"
    ip_ttl="number of network hops between cluster
           members"
    ... />
```

Note

The `mcast_addr` and `mcast_port` parameters are set to 239.555.0.0 and 48866 by default. Since these values must be the same for all cluster members, if you change them for one member, be sure to change them for all other members as well.

The `ip_ttl` parameter is set to 0 by default. If cluster members are on the same host, retain this default value. However, if cluster members are on the same subnet, set `ip_ttl` to 1, or if cluster members are on the same site, set `ip_ttl` to 32.

4. On the application server of the secondary cluster member, add `<cs_install_dir>/bin` to the `CLASSPATH` environment variable. If the class path is not set properly, CAS will not start.
5. The `cas.war` file generated for the primary member is the clustered and generic version of CAS. Deploy this `cas.war` file on the application server of the secondary cluster member.

Note

If you are using the WebLogic application server, before deploying the secondary CAS cluster member, add the following to the `<weblogic-web-app>` tag in the `weblogic.xml` file (located in `cas/WEB-INF`):

```
<session-descriptor>
  <persistent-store-type>replicated
</persistent-store-type>
  <url-rewriting-enabled>true
</url-rewriting-enabled>
</session-descriptor>
```

6. Repeat this process for each additional cluster member.
7. Allow synchronization of CAS tickets between WebCenter Sites members. For each cluster member, edit the file `WEB-INF/classes/cas-cache.xml` as follows:
 - a. Locate the line `multicastGroupPort=4666, timeToLive=0`
 - Ensure the port is unique for each WebCenter Sites cluster (all members must use the same port).
 - Change `timeToLive` to 1 if the cluster members reside on different physical servers.

- b. Save the updated file.

Redeploying CAS on a New Server

Note

This section applies to non-clustered CAS or a primary CAS cluster member.

During the installation process, the installer entered your CAS deployment information into the following files, enabling WebCenter Sites to connect to CAS:

- SSOConfig.xml in WEB-INF/classes
- Files in <cs_install_dir>/bin:
 - cas.properties
 - host.properties
 - jbossTicketCacheReplicationConfig.xml

When the installation process is complete and you need to redeploy CAS on a new server, you must manually reconfigure the above files and CAS, as follows:

1. Remove CAS from the server where it was deployed previously.
2. Deploy cas.war (or cas.ear) on the new server. If you are clustering CAS, the server is defined as the primary CAS cluster member.
3. Reconfigure WebCenter Sites to detect CAS by updating the casURL property in the SSOConfig.xml file in the WEB-INF/classes directory of the cs.war file:

- **For non-clustered CAS**

```
property name="casUrl" value="http://<CAS host name>:<CAS
port number>/cas"
```

- **For the primary CAS cluster member**

```
property name="casUrl" value="http://<load balancer host
name>:<load balancer port number>/cas"
```

4. Copy the following CAS configuration files from the <cs_install_dir>/bin directory to a directory on the new server:

- cas.properties
- host.properties
- jbossTicketCacheReplicationConfig.xml

5. Update the CAS configuration files:

- **For non-clustered CAS**

- In the cas.properties file, update the following properties:

```
cas.securityContext.serviceProperties.service=http://
<CAS host name>:<CAS port number>/cas/services/
j_acegi_cas_security_check
```

```
cas.securityContext.casProcessingFilterEntryPoint.  
    loginUrl=http://<CAS host name>:<CAS port number>/  
    cas/login  
cas.securityContext.ticketValidator.casServerUrlPrefix  
    =http://<CAS host name>:<CAS port number>/cas
```

- In the `host.properties` file, update the following property:

```
host.name=cas.<CAS host name>-1
```

- In the `jbossTicketCacheReplicationConfig.xml` file, do the following:

- In the "ClusterName" attribute, replace *TreeCache-Cluster* with a unique name:

```
<attribute name="ClusterName">TreeCache-Cluster  
</attribute>
```

- In the "ClusterConfig" attribute, update the following parameter:

```
bind_addr="host name of server where cluster  
member will be deployed"
```

- **For the primary CAS cluster member**

Update the `host.properties` and `jbossTicketCacheReplicationConfig.xml` files as described in [step 2](#) and [step 3 on page 184](#).

6. On the new server, add the directory containing the CAS configuration files to the CLASSPATH environment variable. If the class path is not set properly, CAS will not start.

Chapter 14

Oracle Access Manager Integration Setup

Use this chapter to integrate Oracle Access Manager (OAM) with Oracle WebCenter Sites installations.

This chapter contains the following sections:

- [Overview](#)
- [OAM Integration Prerequisites](#)
- [Integrating OAM with Oracle WebCenter Sites](#)
- [Integrating OAM with Oracle WebCenter Sites: Satellite Server](#)

Overview

This section contains the following topics:

- [Integration Components](#)
- [Flow for Browser Requests](#)
- [REST Service Flow](#)

Integration Components

Integration with Oracle Access Manager requires replacement of the Single Sign-On (SSO) authentication plug-in classes for the WebCenter Sites application, and the addition of a token authority servlet for REST client authentication. Optionally the WebCenter Sites challenge (login) page can be deployed.

Note

When integrated with WebCenter Sites systems running in content management (development) mode, Oracle Access Manager, is used for browser and REST authentication. On production systems (running in delivery mode), OAM is used strictly for REST authorization.

Each component is described more fully in the following:

1. SSO authentication plug-in classes are delivered in the `wem-ssso-api-oam-1.2.jar` that is included with the WebCenter Sites product. There are three primary classes included in this JAR that must be configured to load with the Sites application when it starts.
 - a. `OAMFilter` provides recognition of an authenticated user (either by WebLogic Server (WLS) perimeter security or REST credential token) before allowing access to a protected resource.
 - b. `OAMProvider` contains the JAVA API which is used by REST client programs to obtain an authenticated credential before requesting a resource from the Sites application. It also contains methods used internally to authenticate REST credentials by `OAMFilter`.
 - c. `OAMListener` is a session filter that monitors the creation and termination of HTTP sessions to facilitate cleanup of session related cached information.
2. The token authority servlet is delivered in the `oamtoken.war` file. It is an OAM AccessGate that will either authenticate a user against the OAM server or check, upon request, that an OAM authenticated session is still valid.
3. The WebCenter Sites challenge page is optional and is delivered in the `oamlogin.war` file. The servlet within `oamlogin.war` provides a custom branded challenge request when OAM must obtain credentials to authenticate a user. It is included to provide a replacement of the standard WebCenter Sites branded login page that is installed with the Central Authentication Service (CAS). This page is called directly by OAM and must be specifically configured within the OAM Authentication Scheme used to protect WebCenter Sites resources.

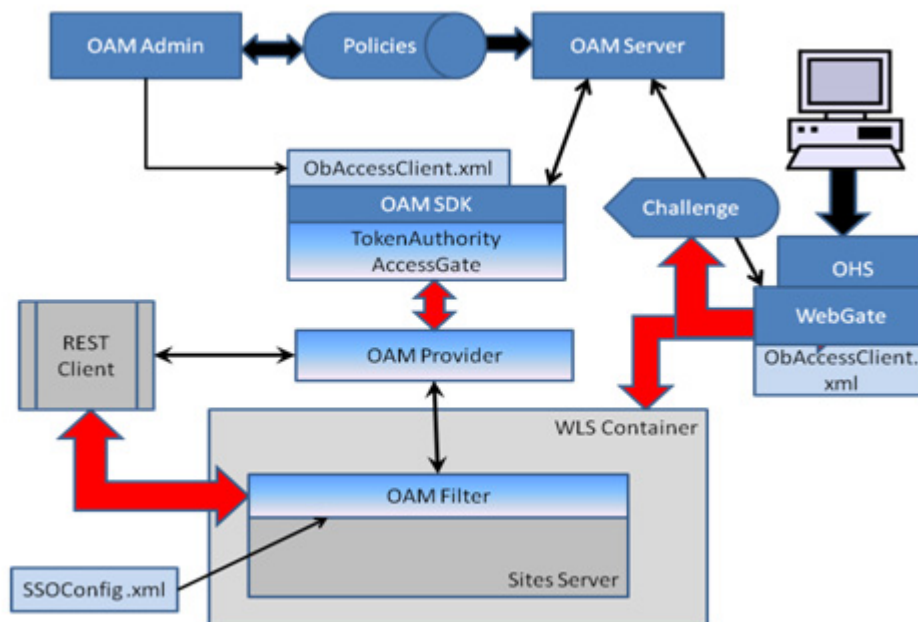
Installation of these components and the configuration of the Oracle Access Manager must be done to complete an operational OAM integration with WebCenter Sites.

Much of OAM integration regards the configuration of the elements of OAM itself. OAM configuration is done mainly within the OAM Administrative console, as well as across several Sites server configuration files, and the Oracle HTTP Server (OHS) configuration files. The Host Identifiers, URL Resources, Domain policies, and OAM Agents must be properly configured to achieve proper operation. The WebCenter Sites challenge screen is supplied as an independent HTTP Servlet. You have the choice to use the WebCenter Sites challenge screen, the default OAM challenge screen, or a custom challenge screen through the Authentication Scheme attached to the configured policies. Control over all policies for authentication and authorization through the OAM Administrator console provides extensive configuration capabilities.

Flow for Browser Requests

OAM Integration components and process flow for logging in to and out of WebCenter Sites is shown in [Figure 1](#). The core integration revolves around the OAMFilter and OAMProvider classes. These classes are injected into the WebCenter Sites Web application by Spring initialization to replace CAS equivalents which are not necessary with OAM. There are no internal changes to the Sites application to accommodate this integration.

Figure 1: OAM Flowchart



Login Processing

All browser access is directed through the standard OHS WebGate and using perimeter security provided by the WLS container. The WebGate functions as a reverse proxy,

checks protection policies through Access Manager. It issues the challenge/login form when necessary. A request is never passed directly to the WLS container but always passes through the WebGate to ensure authentication and authorization are satisfied. When a valid request is received from the WebGate, the WLS container presents an identity assertion to the OAM filter. This assertion will identify the authenticated user and cause the information for that user to be fetched from the Sites `SystemUsers` table. User information consists of the user ID, name, and ACL needed to prepare the proper internal assertion for reference within the Sites application. The user name in the Sites `SystemUsers` table and in the Oracle Internet Directory (or LDAP directory) must match exactly for authentication to work properly. Although OAM includes authorization protection as well as authentication, WebCenter Sites uses only OAM authentication and does not rely on full OAM authorization.

When the OAMFilter receives control, the request has already been authenticated by the WebGate and an OAM Identity Assertion created by WLS perimeter security. This assertion provides the authenticated user's name which is used to find that user information in the Sites `SystemUsers` table. The information thus obtained is used to create an internal assertion used within the Sites application.

After an OAM Identity Assertion has been converted into an internal Assertion, the internal Assertion is added to the HTTP Session object. This allows subsequent requests to access URLs (resources) directly for the lifetime of the application session. However, the WebGate provides overriding protection based upon the OAM security policies in effect. If the OAM user session (different from HTTP session) expires, then the user will be required to re-authenticate.

SSO and Logoff

The WebGate manages the OAM cookies which govern SSO. This is transparent to the Sites OAM Filter and provides a seamless integration with other Oracle applications.

When WebCenter Sites logoff is requested, the standard OAM logoff facility is invoked by the OAM logoff URL which includes an `end_URL` parameter. The `end_URL` parameter establishes the next page that must appear after OAM finishes all logoff activities. OAM removes the SSO cookies, terminates the OAM session, and calls the registered logout success URL. The logout success URL is recognized by the OAM Filter to invalidate the HTTP session. After OAM logout has completed all its work it redirects the browser back to the WebCenter Sites welcome URL, specified through the `end_URL` parameter. This triggers a new challenge for the user to supply login credentials. The Logout URL settings are defined in the OHS WebGate configuration and the `end_URL` is defined in the `SSOConfig.xml` file.

REST Service Flow

REST processing follows a slightly different flow. This is also illustrated in [Figure 1](#). The REST client uses the OAM Provider API to obtain a service ticket from the Token Authority. This ticket is required as a parameter in the REST request to grant access to a resource on the Sites server. The TokenAuthority functions as an OAM Access Gate. It will authenticate the user against the policies defined for the REST endpoint URL. When a proper username and password has passed authentication, the REST client is issued a service ticket to be used when requesting the resource. The TokenAuthority is an HTTP Servlet and it is recommended it be secured through SSL. The TokenAuthority performs three services:

- **Request** – Takes a username/password combination and endpoint URL (as the resource) and authenticate through the OAM SDK. The result is an OAM UserSession for the request. The associated session token is extracted from the UserSession and retained in a cache keyed by UUID. The UUID is returned to the requestor to be used as the service request ticket associated with the OAM Session.
- **Validate** – Given a request ticket, the associated session token is retrieved from the cache and the authenticated username is returned. The OAM UserSession is checked to make sure it remains valid. If the session is no longer valid or indicates that the user associated with the ticket is no longer logged in then a 'not authorized' 403 status is returned.
- **Invalidate** – Given a request ticket, the associated session token is retrieved from the cache, removed, and then converted into an OAM UserSession object which is immediately terminated. This invalidates the OAM session and occurs after a request ticket has been used.

When the OAM Filter receives a REST request it must always be accompanied by a parameter that supplies a request ticket. This ticket is validated through the OAM Provider (the SSO Provider calls the Token Authority) before access to the resource is granted. A normal ticket request is for one time only and its maximum lifetime is dictated by the OAM session timeout. For a valid ticket, the OAM user session is invalidated immediately and access to the resource is allowed only once. A multi-ticket is handled in a similar manner but the ticket is cached locally so it may be reused by the REST client for a finite amount of time.

The published REST API remains the same. REST client programming is not affected by this integration and works exactly as it did with the CAS provider. Internally, the API dynamically instantiates the required classes based on which authentication provider is being used. Remote REST client programs are written in JAVA and require the `wem-ssapi-oam-1.2.jar` for compilation and execution.

The REST client goes directly to the Sites server directly as shown in [Figure 1](#). The client has the choice of two possible endpoints. It can go directly to the Sites application as shown in the figure or pass through the OHS WebGate. A policy is defined for the latter case which allows this endpoint to be used. The decision of which endpoint to use is a choice dependent upon performance and/or security concerns.

OAM Integration Prerequisites

This section contains the following topics:

- [Installing OAM Components](#)
- [Preparing OAM for Integration](#)

Installing OAM Components

Before you set up Oracle Access Manager integration, the Oracle components needed to support the environment must be installed and working properly. If you already have OAM installed and running at the support level specified in the *Oracle WebCenter Sites Certification Matrix* and in this document then you can disregard this section and skip to “[Integrating OAM with Oracle WebCenter Sites](#),” on page 199. Otherwise, continue with the steps below.

Note

Install the system components listed below in the order given. The steps as listed are not comprehensive steps, and should be treated as guidelines.

Be careful to observe that the proper versions are being used. The Oracle installer for each package requires that particular versions of related components are installed on the system. If version requirements are not observed then the installer will not allow a specific installation to continue. Each listed package includes one or more links to additional documentation.

All components listed can be downloaded from the Oracle EDelivery site. Though all these components are installed, OAM integration requires only Oracle Internet Directory Server, Oracle HTTP Server, and Oracle Access Manager Server to be operating.

Install the following Oracle components in the order given:

1. [Oracle Database 11g - Version 11.2.0](#)
2. [Oracle Fusion Middleware Repository Creation Utility 11g \(11.1.1.5.x\)](#)
3. [Oracle WebLogic Server \(10.3.5\) Generic and Coherence](#)
4. [Oracle Identity Management 11g \(11.1.1.5.x\)](#)
5. [Oracle Identity Management and Access Management 11g \(11.1.1.5.0\)](#)
6. [Oracle Fusion Middleware Web Tier Utilities 11g \(11.1.1.2.0\)](#)
7. [Oracle Access Manager WebGates \(11.1.1.5.x\)](#)

Oracle Database 11g - Version 11.2.0

1. Install Oracle Database 11g - Version 11.2.0.
http://docs.oracle.com/cd/E11882_01/install.112/e24321/toc.htm
2. Create and configure an Oracle 11g database. For specific instructions, see [Chapter 1, "Creating and Configuring an Oracle 11g Database."](#)
3. Increase the maximum processes and open cursors allowed for the newly created database by running the following commands in sqlplus and restarting the database:

```
alter system set processes=500 scope=spfile;  
alter system set open_cursors=800 scope=both;
```

Oracle Fusion Middleware Repository Creation Utility 11g (11.1.1.5.x)

1. Check that the database to be used satisfies the requirements for the Repository Creation Utility.
http://docs.oracle.com/html/E18558_01/fusion_requirements.htm#CHDJGECA
2. Create Schemas using the Repository Creation Utility.
http://docs.oracle.com/cd/E12839_01/doc.1111/e14259/rcu.htm#CHDGJCGJ

Select all components.

Oracle WebLogic Server (10.3.5) Generic and Coherence

Install WebLogic Server.

http://docs.oracle.com/cd/E21764_01/doc.1111/e14142/toc.htm

Do not create a domain as it will be created later.

Oracle Identity Management 11g (11.1.1.5.x)

This requires Oracle Identity Management (11.1.1.2.0) and Oracle Identity Management 11g Patch Set 4 (11.1.1.5.0).

http://docs.oracle.com/cd/E21764_01/install.1111/e12002/instps2.htm#BGBDGICJ

1. Install Oracle Identity Management 11g (11.1.1.2.0).

Select **Install Software - Do Not Configure**, as configuration must be done after the patch has been applied.

2. Install Oracle Identity Management 11g Patch Set 4 (11.1.1.5.0).

3. Configure Oracle Identity Management (11.1.1.5.0).

http://docs.oracle.com/cd/E21764_01/install.1111/e12002/oid.htm#BABGDJFC

- a. Run `<ORACLE_HOME>/bin/config.sh`

For example:

```
/u01/software/Apps/OraMiddleware/Oracle_IDM1/bin/config.sh
```

- b. On the “Select Domain” screen, select **Create New Domain** and provide the configuration data.
- c. On the “Specify Schema Database” screen, select **Use Existing Schema** and enter a connection string containing the information for the database containing the schemas created by the Repository Creation Utility.

For example:

```
localhost:1521:oamdb
```

Oracle Identity Management and Access Management 11g (11.1.1.5.0)

1. Install Oracle Identity Management and Access Management 11g.

http://docs.oracle.com/cd/E21764_01/install.1111/e10033/configtwo.htm#CEGFJHDF

Use the existing schema created by the Repository Creation Utility and the WebLogic domain created in [step b](#) of the installation of “[Oracle Identity Management 11g \(11.1.1.5.x\)](#),” on page 195.

2. Extend the existing domain.

- a. Run `<WL_HOME>/common/bin/config.sh`

For example:

```
/u01/software/Apps/OraMiddleware/wlserver_10.3/common/bin/config.sh
```

- b. Select **Extend** and existing WebLogic domain.
Select the domain created in [step b](#) of the installation of “[Oracle Identity Management 11g \(11.1.1.5.x\)](#),” on [page 195](#).
- c. Make sure the following products are selected and click **Next**:
Basic WebLogic Server Domain – 10.3.4.0 [wlserver_10.3]*
Oracle Enterprise Manager – 11.1.1.0 [oracle_common]
Oracle Access Manager with Database Policy Store – 11.1.1.3.0 [Oracle_IDM2]
Oracle Identity Management – 11.1.1.2.0 [Oracle_IDM1]
Oracle JRF – 11.1.1.0 [oracle_common]
- d. Ensure all configurations are complete.

Oracle Fusion Middleware Web Tier Utilities 11g (11.1.1.2.0)

Requires: Oracle Fusion Middleware Web Tier Utilities 11g (11.1.1.2.0) and Oracle Fusion Middleware Web Tier Utilities Patch Set 4 (11.1.1.5.0).

1. Install Oracle Fusion Middleware Web Tier Utilities 11g (11.1.1.2.0).
http://docs.oracle.com/cd/E12839_01/doc.1111/e14260/install.htm#CHDHCJEC
Select **Install Software - Do Not Configure**, as configuration must be done after the patch has been applied.
2. Install Oracle Fusion Middleware Web Tier Utilities Patch Set 4 (11.1.1.5.0).
3. Configure Oracle Fusion Middleware Web Tier Utilities 11g (11.1.1.5.0).
http://docs.oracle.com/cd/E12839_01/doc.1111/e14260/install.htm#autoId14
 - a. Run `<WEB_TIER_ORACLE_HOME>/bin/config.sh`
For example:
`/u01/software/Apps/OraMiddleware/Oracle_WT1/bin/config.sh`
 - b. On the “Configure Components” screen, select **Oracle HTTP Server**, **Oracle Web Cache**, and **Associate Selected Components with WebLogic Domain**, and provide the configuration data.
 - c. On the “Specify WebLogic Domain” Screen, select the domain created in [step b](#) of the installation of “[Oracle Identity Management 11g \(11.1.1.5.x\)](#),” on [page 195](#).

Oracle Access Manager WebGates (11.1.1.5.x)

The OAM Access Manager WebGates documentation is located at:

http://docs.oracle.com/cd/E21764_01/install.1111/e12002/webgate.htm

1. Install Third-Party GCC Libraries
 - a. For 64-bit systems, the `libgcc_s.so.1` and `libstdc++.so.6` version 3.4.6 64-bit libraries need to be in a directory on the system before Oracle Access Manager WebGates can be installed.
 - b. Run the following commands and ensure that their output is always greater than 0:
`strings -a libgcc_s.so.1 | grep -c "GCC_3.0"`

```
strings -a libgcc_s.so.1 | grep -v "GCC_3.3.1" | grep -c
"GCC_3.3"
strings -a libgcc_s.so.1 | grep -c "GCC_4.2.0"
file libgcc_s.so.1 | grep "64-bit" | grep -c "x86-64"
file libstdc++.so.6 | grep "64-bit" | grep -c "x86-64"
```

2. Install Oracle Access Manager WebGates (11.1.1.5.0).
3. Complete the Post-Installation steps from Section 20.4 of the OAM Access Manager WebGates documentation:

http://docs.oracle.com/cd/E21764_01/install.1111/e12002/webgate.htm#autoId11

Note

In this example, the Oracle HTTP Server installed with Oracle Identity Management is being used with the WebGate.

Example values for the parameters:

<MW_HOME>

/u01/software/Apps/OracleMiddleware

<Webgate_Home> and <Webgate_Oracle_Home>

/u01/software/Apps/OraMiddleware/Oracle_OAMWebGate1

<Webgate_Instance_Directory>

/u01/software/Apps/OraMiddleware/asinst_1/config/OHS/ohs1

<Oracle_Home_for_Oracle_HTTP_Server>

/u01/software/Apps/OraMiddleware/Oracle_IDM1

Preparing OAM for Integration

1. Start the WebLogic Admin Server.

```
<domain_home>/bin/startWebLogic.sh
```

For example:

```
/u01/software/Apps/OraMiddleware/user_projects/domains/
OAMDomain/bin/startWebLogic.sh
```

2. Start the WebLogic Node Manager.

```
<weblogic_home>/server/bin/startNodeManager.sh
```

For example:

```
/u01/software/Apps/OraMiddleware/wlserver_10.3/server/bin/
startNodeManager.sh
```

3. View the Enterprise Manager Farm Application.

- a. From a browser, go the following URL:

```
http://<weblogic_admin_host>:<weblogic_admin_port>/em
```

- b. Log in using the WebLogic server credentials.
- c. Under Farm_ <your_domain> expand WebLogic Domain and then <your_domain>.

You should see the following: AdminServer, oam_server1, wls_ods1, and wls_oif1.

This is the WebLogic Admin Server, Oracle Access Manager Server web application, Oracle Directory Server web application, and Oracle Identity Federation Server web application.

- d. Expand Identity and Access.

You should see the following: OAM, oid1, and ovd1.

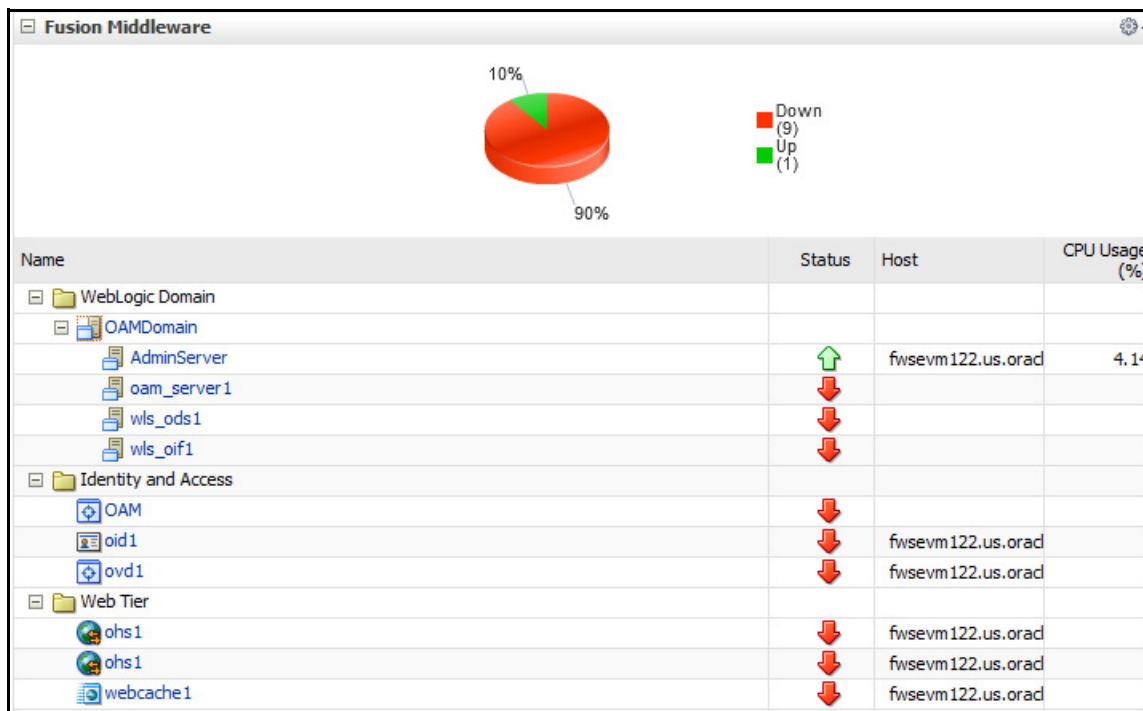
This is the Oracle Access Manager Server, Oracle Internet Directory Server, and Oracle Virtual Directory Server.

- e. Expand Web Tier.

You should see the following: ohs1, ohs1, and webcache1.

This is the Oracle HTTP Server installed with Web Tier, the Oracle HTTP Server installed with Identity Management, and the Web Cache Server.

- f. On the right side, under Fusion Middleware, you can view the status for each of the applications and servers. Currently only the AdminServer should be shown as running.



- 4. Start Oracle Access Manager.
 - a. From the Farm Application:
 - 1) Click **oam_server1** under Fusion Middleware.
 - 2) Under oam_server1, click **WebLogic Server** which becomes a drop-down menu.

- 3) Hover over **Control** and click **Start Up**.
 - 4) After startup has completed, the status arrow will change to green.
- b. From the WebLogic Admin Console:
- 1) Click **Servers**.
 - 2) Click the **Control** tab.
 - 3) Select the **oam_server1** checkbox and click **Start**.
 - 4) After startup has completed, click **Servers** again and the State will show as **RUNNING**.
- c. Go to the OAM Console.
- 1) From a browser, go to:
`http://<weblogic_host>:<weblogic_admin_port>/oamconsole`
 - 2) Log in using the WebLogic server credentials.
 - 3) Access to the OAM Console is required for integration.

Integrating OAM with Oracle WebCenter Sites

This section includes the following topics:

- [Before You Start](#)
- [Integration Steps](#)

Before You Start

There are some important considerations regarding the integration of WebCenter Sites with OAM authentication:

- Up to this point, this chapter has described the required software and related components needed to integrate OAM with Oracle WebCenter Sites. If you have not reviewed the chapter, and have not ensured that the required components are installed and properly set up, then review the document.
- WebCenter Sites must be installed and working properly with the default CAS.

Note

If you plan on using an LDAP Server to store roles for WebCenter Sites, this configuration should be done before OAM Integration.

You may want to use the same LDAP Server for WebCenter Sites and OAM if user duplication is an issue.

- OAM integration requires that Oracle HTTP Server, Oracle Internet Directory Server, and Oracle Access Manager Server are running.
- The Oracle Access Manager Administration Console (OAMCONSOLE) application is required to perform a majority of the setup activities. Ensure you have permission to use this facility.

The integration procedure is a set of manual steps to be completed as described in the rest of this chapter.

Integration Steps

1. Define Sites users in the OAM User Identity Store.

Note

OAM is used for authentication only and does not rely on OAM authorization. While Oracle Internet Directory, Oracle Directory Server, and others can be used as user identity stores, Oracle WebLogic Embedded LDAP is the default, and is the user identity store used throughout the rest of this chapter. User names must match the user names located in the Sites `SystemUsers` table.

OAM provides enforcement of authentication and authorization policies. WebCenter Sites uses only the authentication policies to protect resources. WebCenter Sites uses its own authorization policies.

User names in Oracle WebLogic Embedded LDAP must match the user names located in the WebCenter Sites `SystemUsers` table. The steps for adding users to WebLogic Embedded LDAP are as follows:

- a. Log in to WebLogic Admin Console.
- b. Click **Security Realms**.
- c. Click **myrealm**.
- d. Select the **Users and Groups** tab.

Settings for myrealm

Configuration **Users and Groups** Roles and Policies Credential Mappings Providers Migration

Users Groups

This page displays information about each user that has been configured in this security realm.

Note: The authentication provider named IAMSuiteAgent does not support viewing or managing its users through the WebLogic console.

[Customize this table](#)

Users

New Delete Showing 1 to 4 of 4 Previous | Next

<input type="checkbox"/>	Name	Description	Provider
<input type="checkbox"/>	firstsite	firstsite WCSites user	DefaultAuthenticator
<input type="checkbox"/>	fwadmin	fwadmin WCSites user	DefaultAuthenticator
<input type="checkbox"/>	OracleSystemUser	Oracle application software system user.	DefaultAuthenticator
<input type="checkbox"/>	weblogic		DefaultAuthenticator

New Delete Showing 1 to 4 of 4 Previous | Next

For each user to be added, complete the following steps:

- 1) Click **New**.
- 2) Enter the user name.

- 3) Enter a description for the user.
- 4) Select **DefaultAuthenticator** for Provider.
- 5) Enter a password for the user.
- 6) Re-enter the password for the user.
- 7) Click **OK**.

Create a New User

OK Cancel

User Properties

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

* Indicates required fields

What would you like to name your new User?

* **Name:** fwadmin

How would you like to describe the new User?

Description: fwadmin WCSites user

Please choose a provider for the user.

Provider: DefaultAuthenticator ▼

The password is associated with the login name for the new User.

* **Password:** ●●●●●●

* **Confirm Password:** ●●●●●●

OK Cancel

2. Create an OAM WebGate Agent for deployment on OHS.
 - a. Log in to the OAM Console application.
`http://<weblogic_host>:<weblogic_admin_port>/oamconsole`
 - b. Select the **System Configuration** tab.
 - c. Under SSO Agents, click **New OAM 11g Webgate**.
 - d. For Name, enter `WCSitesWebGate` and click **Apply**.
 - e. For Preferred Host, enter `WCSites`.
 - f. For Logout Callback URL, enter `<sites context root>/oam_logout_success`.
 - g. For Logout Redirect URL, enter `http://<weblogic_host>:<oam_server_port>/oam/server/logout`.
 - h. Click **Apply**.

- i. Copy the newly created WebGate configuration files (ObAccessClient.xml and cwallet.sso) into the OHS configuration:

```
cp <domain_home>/output/WCSitesWebGate/*
```

```
<ohs_instance_home>/config/OHS/ohs1/webgate/config
```

For example:

```
cp /u01/software/Apps/OraMiddleware/user_projects/domains/
OAMDomain/output/WCSitesWebGate/*
/u01/software/Apps/OraMiddleware/asinst_1/config/OHS/ohs1/
webgate/config
```

WCSitesWebGate

Name: WCSitesWebGate

Access Client Password:

* Security: Open, Simple, Cert

* State: Enable, Disable

* Max Cache Elements: 100000

* Cache Timeout (Seconds): 1800

* Token Validity Period (Seconds): 3600

* Max Connections: 1

* Max Session Time: 3600

* Failover Threshold: 1

* AAA Timeout Threshold: -1

* Preferred Host: WCSites

Logout URL:

Logout Callback URL: /servlet/oam_logout_success

Logout Redirect URL: ade.com:14100/oam/server/logout

Logout Target URL:

User Defined Parameters: proxySSIHeaderVar=IS_SSI, URLInUTF8Format=true, client_request_retry_attempts=1, inactiveReconfigPeriod=10

* Sleep for: 60

Cache Pragma Header: no-cache

Cache Control Header: no-cache

Debug:

IP Validation:

Deny On Not Protected:

Allow Management Operations:

Server Lists

Primary Server List

Server Name	Host Name	Host Port	Max Number
oam_server	fwsevm122.us.c	5575	1

Secondary Server List

Server Name	Host Name	Host Port	Max Number
-------------	-----------	-----------	------------

3. Create an OAM WebGate Agent for deployment on the oamtoken web application.
 - a. Log in to the OAM Console application.
http://<weblogic_host>:<weblogic_admin_port>/oamconsole
 - b. Click the **System Configuration** tab.
 - c. Under SSO Agents, click **New OAM 11g Webgate**.
 - d. For Name, enter `WCSites.REST.AccessGate` and click **Apply**.
 - e. For Preferred Host, enter `WCSites`.

- f. For Logout Callback URL, enter /oam_logout_success.
- g. For Logout Redirect URL, enter `http://<weblogic_host>:<oam_server_port>/oam/server/logout`.
- h. Click **Apply**.

The WebGate configuration file will be copied in [step 5](#).

WCSites.REST.AccessGate

Name: WCSites.REST.AccessGate

Access Client Password: [Text Field]

* Security: Open, Simple, Cert

* State: Enable, Disable

* Max Cache Elements: 100000

* Cache Timeout (Seconds): 1800

* Token Validity Period (Seconds): 3600

* Max Connections: 1

* Max Session Time: 3600

* Failover Threshold: 1

* AAA Timeout Threshold: -1

* Preferred Host: WCSites

Logout URL: [Text Field]

Logout Callback URL: /oam_logout_success

Logout Redirect URL: acle.com:14100/oam/server/logout

Logout Target URL: [Text Field]

User Defined Parameters: proxySSLHeaderVar=IS_SSL, URLInUTF8Format=true, client_request_retry_attempts=1, inactiveReconfigPeriod=10

* Sleep for: 60

Cache Pragma Header: no-cache

Cache Control Header: no-cache

Debug:

IP Validation:

Deny On Not Protected:

Allow Management Operations:

Server Lists

Primary Server List

Server Name	Host Name	Host Port	Max Number
oam_server	fwsevm122.us.c	5575	1

Secondary Server List

Server Name	Host Name	Host Port	Max Number
-------------	-----------	-----------	------------

4. Create a host identifier for WebCenter Sites.
 - a. Under Host Identifiers, check for WCSites. If WCSites exists, double-click **WCSites** and go to step e, otherwise go to step b.
 - b. Click **Host Identifiers**.
 - c. Click the **Create** icon.
 - d. For the Name, enter WCSites.
 - e. For the Description, enter "This is the host identifier for WebCenter Sites."
 - f. On the operations panel, click the **Add (+)** icon and enter WCSites for Host Name.

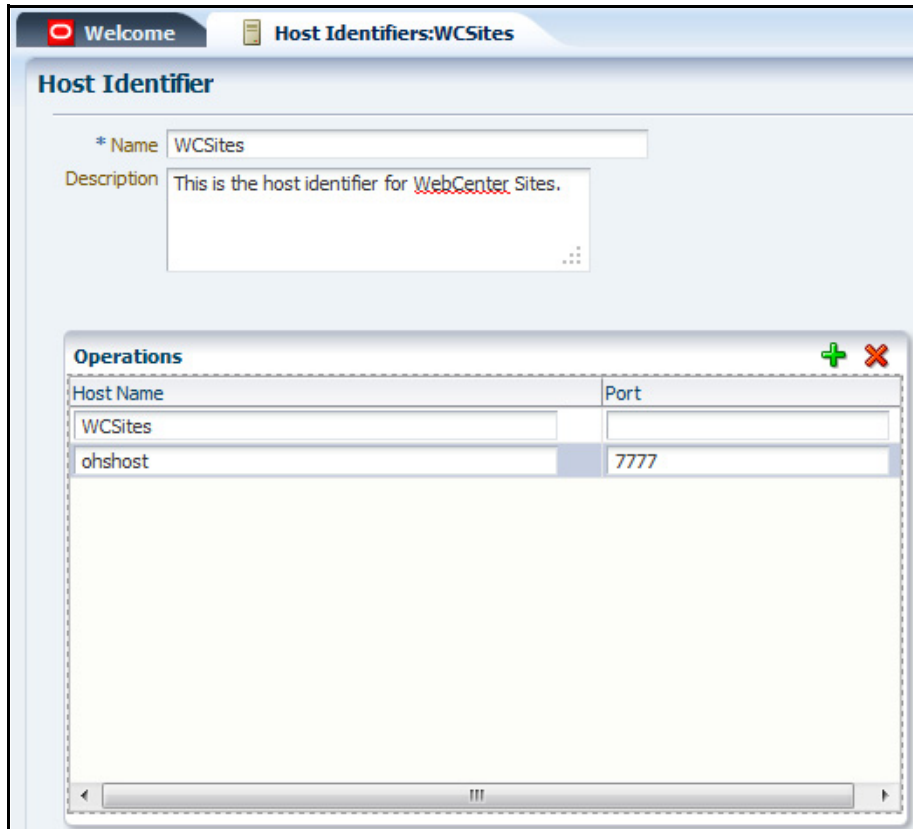
Note

The Host Name specified here must match the Preferred Host specified in the WebGate.

- g. Click the **Add (+)** icon again and enter the hostname for the OHS server for Host Name and the port for the OHS server for Port.

If you are using multiple hosts in a load balancing arrangement then repeat this step for each OHS instance.

- h. Click **Apply**.



5. Deploy the `oamtoken.war` file:
- Create a directory where the `oamtoken.war` file will be deployed from, and explode the `oamtoken.war` file into the directory from the `wem` directory of the Sites installer.

For example:

```
mkdir /u01/software/Apps/Weblogic1035/user_projects/domains/OAMCSDomain/applications/oamtoken
```

```
cd /u01/software/Apps/Weblogic1035/user_projects/domains/OAMCSDomain/applications/oamtoken
```

```
jar -xvf /u01/CS/installation_files/ContentServer/wem/oamtoken.war
```

- Copy the WebGate configuration file created in [step 2](#) to the `WEB-INF/oblix/lib` directory of the exploded `oamtoken` web application. Overwrite any existing file.

The WebGate configuration file is located at `<domain_home>/output/WCSites.REST.AccessGate/ObAccessClient.xml` on the system where OAM is deployed.

- c. Create a file named `tokenauthority.xml` in the `WEB-INF/classes` directory of the exploded `oamtoken` web application, using the xml below. Modify the value of the `oblixPath` property to point to the location of the `WEB-INF` directory of the exploded `oamtoken` web application. If the `oamtoken` web application is to be deployed to a different location, the `oblixPath` property must be modified to reflect the new location.

For example:

```
/u01/software/Apps/Weblogic1035/user_projects/domains/
  OAMCSDomain/applications/oamtoken/WEB-INF
```

`tokenauthority.xml`:

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xsi:schemaLocation="http://www.springframework.org/
schema/beans http://www.springframework.org/schema/beans/
spring-beans-2.0.xsd" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns="http://www.springframework.org/
schema/beans">
  <bean class="com.fatwire.wem.sso.oam.token.TokenConfig"
id="configuration">
    <property value="{path_to_oamtoken_WEB-INF_directory}"
name="oblixPath"/>
  </bean>
</beans>
```

- d. Deploy the exploded `oamtoken` web application.

Note

On WebLogic, make the deployment accessible from the current location.

The servlet contained in the `oamwebtoken` web application may be called with visible username and password credentials. It is recommended to deploy the application as a secured web application using SSL.

- 6. Deploy the `oamlogin.war` file.

This web application contains the WebCenter Sites challenge page.

Note

This step is optional and can be skipped if using the default OAM login form or another custom login form.

- a. Create a directory where the `oamlogin.war` file will be deployed from, and explode the `oamlogin.war` file into the directory from the `wem` directory of the Sites installer.

For example:

```
mkdir /u01/software/Apps/Weblogic1035/user_projects/domains/  
OAMCSDomain/applications/oamlogin
```

```
cd /u01/software/Apps/Weblogic1035/user_projects/domains/  
OAMCSDomain/applications/oamlogin
```

```
jar -xvf /u01/CS/installation_files/ContentServer/wem/  
oamlogin.war
```

- b. Create a file named `wbsites_settings.properties` in the `WEB-INF/classes` directory of the exploded `oamlogin` web application, using the code below. Replace the variables, in brackets, with the correct values for your environment:

```
oamredirect=http://<weblogic_host>:<oam_server_port>/oam/  
server/auth_cred_submit
```

```
oamlogout=http://<weblogic_host>:<oam_server_port>/oam/  
server/logout
```

```
forgotpassword=<email_account>@<email_domain>
```

Note

If the `oamredirect` property is not configured correctly, the username and password will fail to authenticate.

- c. Deploy the exploded `oamlogin` web application.

Note

On WebLogic, make the deployment accessible from the current location.

7. Create an authentication scheme that redirects to the WebCenter Sites challenge page.

Note

This step is optional and can be skipped if using the default OAM login form or another custom login form.

- a. Log in to the OAM Console application.
`http://<weblogic_host>:<weblogic_admin_port>/oamconsole`
- b. Click **Authentication Schemes**, and then click **Create**.
- c. Enter a name for the authentication scheme.
- d. Enter Challenge for WebCenter Sites applications for description.
- e. Enter 2 for Authentication Level.
- f. Select **FORM** for Challenge Method.
- g. Enter `/oam/server/` for Challenge Redirect URL.
- h. Select **LDAP** for Authentication Module.

- i. Enter `http://<oamlogin_app_server_host>:<oamlogin_port>/oamlogin/oamsso/oamLoginView.jsp` for Challenge URL.
- j. Select **external** for Context Type.
- k. Click **Apply**.

Authentication Schemes

* Name: LDAPWemScheme

Description: Challenge for WebCenter Sites applications

* Authentication Level: 2

Default:

* Challenge Method: FORM

Challenge Redirect URL: /oam/server/

* Authentication Module: LDAP

* Challenge URL: oamlogin/oamsso/oamLoginView.jsp

* Context Type: external

Challenge Parameters:

8. Set up the `mod_wl_ohs.conf` OHS configuration file.

This file resides in the `ohs1` directory of the OHS instance used in previous steps.

For example:

```
/u01/software/Apps/OraMiddleware/asinst_1/config/OHS/ohs1/
  mod_wl_ohs.conf
```

An additional entry for the `/oamlogin` context root (required only if using the Sites challenge page) and the Sites context root should be added to the file as shown below. The values for `WebLogicHost` and `WebLogicPort` are the hostname and port of the application server where the given web application resides.

```
# NOTE : This is a template to configure mod_weblogic.
LoadModule weblogic_module    "${ORACLE_HOME}/ohs/modules/
mod_wl_ohs.so"
# This empty block is needed to save mod_wl related
configuration from EM to this file when changes are made at the
Base Virtual Host Level
<IfModule weblogic_module>
#     WebLogicHost {WEBLOGIC_HOST}
#     WebLogicPort {WEBLOGIC_PORT}
#     Debug ON
#     WLLogFile /tmp/weblogic.log
#     MatchExpression *.jsp
</IfModule>
<IfModule weblogic_module>
  <location /oamlogin>
```

```

    SetHandler weblogic-handler
    WebLogicHost {name/IP of WebLogic server where Sites is
deployed}
    WebLogicPort 7002
  </location>
</IfModule>
<IfModule weblogic_module>
  <location /servlet>
    SetHandler weblogic-handler
    WebLogicHost {hostname/IP of WebLogic server where Sites is
deployed}
    WebLogicPort 7001
  </location>
</IfModule>
# <Location /weblogic>
#     SetHandler weblogic-handler
#     PathTrim /weblogic
#     ErrorPage http://WEBLOGIC_HOME:WEBLOGIC_PORT/
# </Location>

```

Note

Make sure there is an include statement in the `http.conf` file for the `mod_wl_ohs.conf` file.

For example:

```

include "/u01/software/Apps/OraMiddleware/asinst_1/
config/
OHS/ohs1/mod_wl_ohs.conf"

```

9. Start the HTTP Server, Internet Directory Server, and Virtual Directory Server.**Note**

This is the HTTP Server that is installed with Identity Management, and the one used throughout this guide.

a. Enter the following commands:

- 1) `export ORACLE_INSTANCE=/u01/software/Apps/OraMiddleware/asinst_1`
- 2) `/u01/software/Apps/OraMiddleware/Oracle_IDM1/opmn/bin/opmnctl startall`

b. From the Enterprise Manager Farm Application you should see the following are now started: Oracle Internet Directory Server (oid1), Oracle Virtual Directory Server (ovd1), and OHS installed with Identity Management (ohs1).**10. In this step, you will modify the `SSOConfig.xml` file of the WebCenter Sites deployment. This file controls which authentication classes are loaded and the various properties that are required by those classes.**

- a. Back up the `SSOConfig.xml` file, located in the deployed `WEB-INF/classes` directory of the deployed WebCenter Sites application.

For example:

```
/u01/software/Apps/Weblogic1035/user_projects/domains/
  OAMCSDomain/applications/CS/WEB-INF/classes/SSOConfig.xml
```

- b. Modify `SSOConfig.xml` to look like the file shown below.

Note

In the file below, you will set the following properties: `serviceUrl`, `ticketUrl`, `signoutURL`, `dbUsername`, and `dbPassword`.

The `signoutUrl` property specifies the URL to be used when invoking WebCenter Sites logout. It includes the encoded URL where the browser will return after all logout processing has been completed by OAM.

For the `dbUsername` and `dbPassword` properties, you can enter the credentials of the WebCenter Sites general administrator (by default, `fwadmin/xceladmin`). The values for these properties will be encrypted on startup of the WebCenter Sites application.

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:context="http://www.springframework.org/schema/
context"
  xsi:schemaLocation="
    http://www.springframework.org/schema/beans http://
www.springframework.org/schema/beans/spring-beans-2.5.xsd
    http://www.springframework.org/schema/context http://
www.springframework.org/schema/context/spring-context-2.5.xsd">
  <!-- Single Sign On provider -->
  <bean id="ssoprovider"
class="com.fatwire.wem.sso.oam.OAMProvider">
  <property name="config" ref="ssoconfig" />
  </bean>
  <!-- Single Sign On filter -->
  <bean id="ssofilter"
class="com.fatwire.wem.sso.oam.filter.OAMFilter">
  <property name="config" ref="ssoconfig" />
  <property name="provider" ref="ssoprovider" />
  </bean>
  <!-- Single Sign On listener -->
  <bean id="ssolistener"
class="com.fatwire.wem.sso.oam.listener.OAMListener">
  </bean>
  <!-- Single Sign On configuration -->
  <bean id="ssoconfig"
class="com.fatwire.wem.sso.oam.conf.OAMConfig">

  <!-- URL prefix for REST service endpoint -->
```

```

    <property name="serviceUrl" value="http://
{OHS_host}:{OHS_port}/{Sites_context_root}/REST" />

    <!-- URL prefix for Token Service servlet -->
    <property name="ticketUrl" value="http://
{oamtoken_app_server_host}:{oamtoken_port}/oamtoken" />

    <!-- URL to be called when WEM logout is required. -->
    <property name="signoutUrl" value="http://
{weblogic_host}:{oam_server_port}/oam/server/
logout?end_url=http%3A%2F%2F{OHS_host}%3A{OHS_port}%2F{Sites_co
ntext_root}%2Fwem%2Ffatwire%2Fwem%2FWelcome />

    <!-- Do not proxy tickets, tt's the last server in the
call chain -->
    <property name="proxyTickets" value="false" />

    <!-- Database Credentials needed by user lookup in
OAMFilter -->
    <property name="dbUsername" value="{user with authority to
read the WebCenter Sites SystemUser table}" />

    <property name="dbPassword" value="{above user's password}"
/>

    <!-- Your application protected resources (relative to
applicationUrl) -->
    <property name="protectedMappingIncludes">
    <list>
        <value>wem/fatwire/**</value>
        <value>/faces/jsp/**</value>
        <value>/ContentServer?[pagename=OpenMarket/
Xcelerate/UIFramework/LoginPage|OpenMarket/Xcelerate/
UIFramework/ShowMainFrames|fatwire/getAllUserGroups|fatwire/
getAllSecurityConfigs|rest/asset,#]</value>
        <value>Satellite?[pagename=fatwire/
insitetemplating/request|OpenMarket/Xcelerate/ControlPanel/
Request|OpenMarket/Xcelerate/ControlPanel/EditPanel|fatwire/
wem/ui/Ping|fatwire/wem/sso/validateMultiticket|OpenMarket/
Xcelerate/UIFramework/ShowPreviewFrames,#]</value>
    </list>
    </property>
    <property name="protectedMappingStatelessIncludes">
    <list>
        <value>/REST/**</value>
    </list>
    </property>
    <!-- Your application protected resources excludes
(relative to applicationUrl) -->
    <property name="protectedMappingExcludes">
    <list>
        <value>/wem/fatwire/wem/ui/SysLocStrSvc</value>

```

```

    </list>
  </property>
</bean>

</beans>

```

- 11.** Copy the `wem-ss-o-api-oam-1.2.jar` file to the WebCenter Sites deployment.

The file is located in the `wem` directory of the Sites installer, and needs to be copied to the `WEB-INF/lib` directory of the deployed Sites application.

For example:

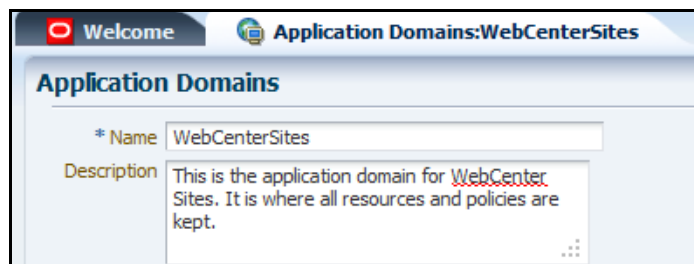
```

cp /u01/CS/installation_files/ContentServer/wem/wem-ss-o-api-
oam-1.2.jar /u01/software/Apps/Weblogic1035/user_projects/
domains/OAMCSDomain/applications/CS/WEB-INF/lib

```

The remaining steps are performed from the Oracle Access Manager Console to complete the Policy Configuration needed to protect the WebCenter Sites application.

- 12.** Create an application domain for WebCenter Sites.
- a. Click **Application Domains** and click the **Create** icon.
 - b. For the Name, enter `WebCenterSites`.
 - c. For the Description, enter "This is the application domain for WebCenter Sites. It is where all resources and policies are kept."
 - d. Click **Apply**.



In steps [steps 13 – 15](#), you will be creating authentication policies for the WebCenter Sites application domain.

The following authentication policies need to be created:

- Protected Resource Policy for Browsers
- Protected Resource Policy for REST Clients
- Unprotected Public Resource Policy

These policies are enforced by the WebGate. The first two policies apply to any resource that is accessed and must require a challenge if not already authenticated. The third policy will be applied for all resources that do not require authentication. Although resources defined in the third policy do not need authentication, they still conform to specific policy directives. Objects that do not need to be authenticated (for example, graphical images, animations, publicly viewed pages) are ignored by the WebGate, but still must be declared so they will function properly with the reverse proxy.

Note

The authentication policies will be created without resources. The resources will be added in a later step.

13. Create Protected Resource Policy for Browsers.

- a. Expand the WebCenterSites application domain created in [step 12 on page 211](#).
- b. Click **Authentication Policies**.
- c. Click the **Create** icon.
- d. For the Name, enter “Protected Resource Policy for Browsers”.
- e. For the Description, enter "This policy is for all protected URLs that require a challenge if not authenticated."
- f. For Authentication Scheme, select **LDAPWemScheme** if you are using the WebCenter Sites challenge page, **LDAPScheme** if you are using the default OAM login form, or another scheme if using some other custom login form.
The LDAPWemScheme is the authentication scheme that was created in [step 7 on page 206](#).
- g. Click the **Identity Assertion** checkbox.

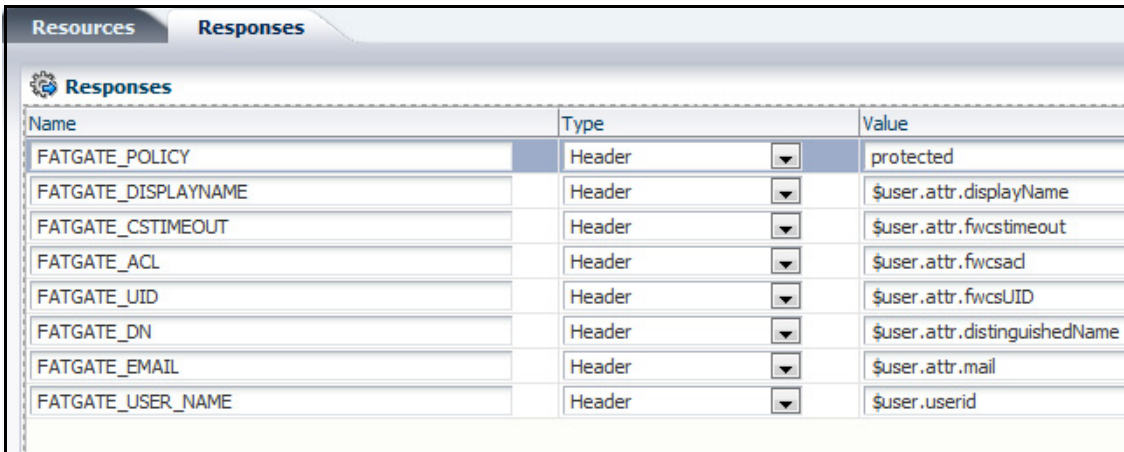
When an Authentication policy is satisfied, it can create responses. The responses are required by the WebCenter Sites HTTP filter to recognize LDAP attributes and provide information about the authenticated user. In the steps that follow, you will add the responses to the **Responses** tab.

- h. Click the **Responses** tab.
- i. Click the **Add (+)** icon.
- j. Enter the Name, Select the Type, and enter the Value.

Repeat steps i and j for the following entries: FATGATE_POLICY and FATGATE_EMAIL.

Note

Only the FATGATE_POLICY and FATGATE_EMAIL responses are required. The remaining responses are optional.



Name	Type	Value
FATGATE_POLICY	Header	protected
FATGATE_DISPLAYNAME	Header	\$user.attr.displayName
FATGATE_CSTIMEOUT	Header	\$user.attr.fwcstimeout
FATGATE_ACL	Header	\$user.attr.fwcsad
FATGATE_UID	Header	\$user.attr.fwcsuid
FATGATE_DN	Header	\$user.attr.distinguishedName
FATGATE_EMAIL	Header	\$user.attr.mail
FATGATE_USER_NAME	Header	\$user.userid

k. Click **Apply**.

14. Create Protected Resource Policy for REST Clients.

a. Click **Authentication Policies**.

b. Click the **Create** icon.

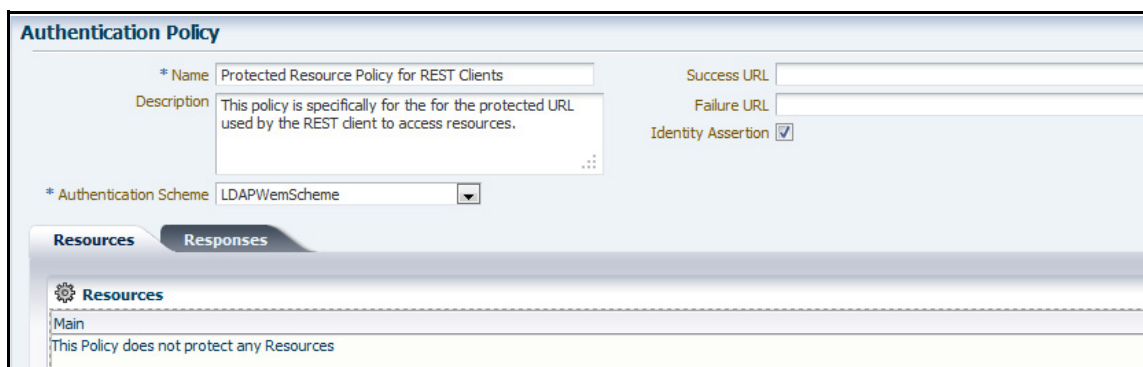
c. For Name, enter "Protected Resource Policy for REST Clients".

d. For Description, enter "This policy is specifically for the protected URL used by the REST client to access resources."

e. For Authentication Scheme, select **LDAPWemScheme** if you are using the WebCenter Sites challenge page, **LDAPScheme** if you are using the default OAM login form, or another scheme if using some other custom login form.

The LDAPWemScheme is the authentication scheme that was created in [step 7 on page 206](#).

f. Select the **Identity Assertion** checkbox.



g. Click the **Responses** tab.

h. Click the **Add (+)** icon.

i. Enter the Name, Select the Type, and enter the Value.

Repeat steps h and i for the following entries: FATGATE_REST_USER and FATGATE_POLICY. Both responses are required.

Name	Type	Value
FATGATE_REST_USER	Header	\$user.userid
FATGATE_POLICY	Header	protected

- j. Click **Apply**.
15. Create Unprotected Resource Policy.
 - a. Click **Authentication Policies**.
 - b. Click the **Create** icon.
 - c. For the Name, enter “Unprotected Public Resource Policy”.
 - d. For the Description, enter "This policy is used for all resources that do not require authentication."
 - e. Select **AnonymousScheme** for Authentication Scheme.
 - f. Click the **Identity Assertion** checkbox.

Authentication Policy

* Name: Unprotected Public Resource Policy

Description: This policy is used for all resources that do not require authentication.

* Authentication Scheme: AnonymousScheme

Success URL:

Failure URL:

Identity Assertion:

Resources | **Responses**

Resources

Name	Type	Value
Main		This Policy does not protect any Resources

- g. Click the **Responses** tab.
- h. Click the **Add (+)** icon.
- i. Enter the Name, Select the Type, and enter the Value.

Complete steps h and i for the following entry: FATGATE_POLICY.

Name	Type	Value
FATGATE_POLICY	Header	unprotected

- j. Click **Apply**.
16. Create the authorization policy for the WebCenter Sites application domain.

The authorization policy will be applied to all WebCenter Sites resources as authorization is done internally by the Sites application based upon its database settings. However, it is necessary to define an authorization policy using implied constraints so the WebGate will pass the resource requests on to the Sites application.

- a. Click **Authorization Policies**.

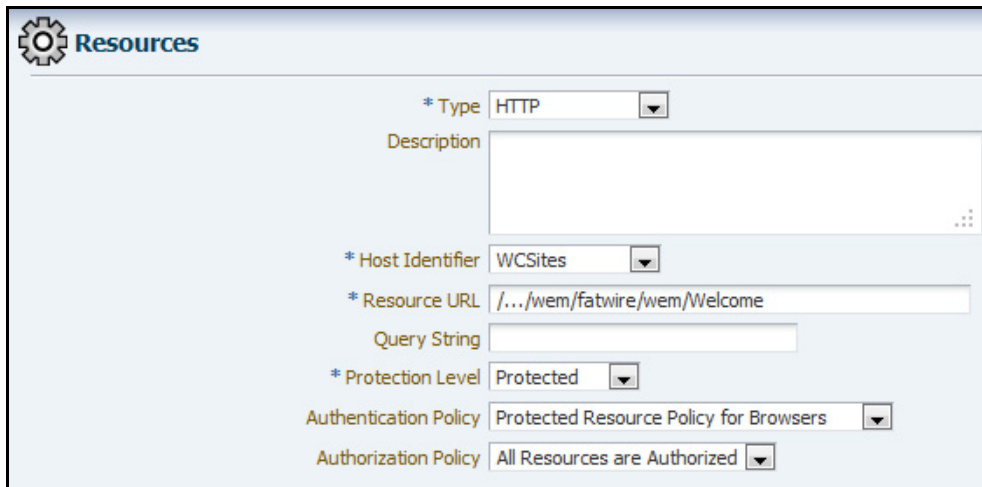
- b. Click the **Create** icon.
- c. For the Name, enter “All Resources are Authorized”.
- d. For the Description, enter "This policy allows all resources to be fully authorized without constraints."
- e. Ensure the **Use Implied Constraints** checkbox is checked.

- f. Click **Apply**.
17. Create resource definitions for the WebCenter Sites application domain:
- a. Double-click **Resources**.

This panel will display only the resources that match the search criteria. Each time a new resource is added, the **Search** button must be clicked for the resource to appear in the Search Results list.

- b. Click **New Resource** to open the Create Resource panel.
- c. Select a Type.
All resources are of type HTTP.
- d. Select a Host Identifier.
All resources use WCSites for Host Identifier.
- e. Enter a Resource URL.
- f. Select a Protection Level.
If selecting Excluded, skip steps g and h.
- g. Select an Authentication Policy.
- h. Select an Authorization Policy.

- i. Click **Apply**.



Resources

* Type HTTP

Description

* Host Identifier WCSites

* Resource URL /.../wem/fatwire/wem/Welcome

Query String

* Protection Level Protected

Authentication Policy Protected Resource Policy for Browsers

Authorization Policy All Resources are Authorized

- j. Repeat steps b through i using the list of resources below.

Note

The only Unprotected resource is /.../*
 Any resources with a policy are Protected.
 The remaining resources are Excluded.

Table 5: Resources

Resource URL	Protection Level	Authentication	Authorization
/.../* .jpg	Excluded		
/.../* .css	Excluded		
/.../* .png	Excluded		
/.../* .swf	Excluded		
/.../* .html	Excluded		
/.../* .jar	Excluded		
/.../* .gif	Excluded		
/.../* .jsp	Excluded		
/.../* .jspx	Excluded		
/.../faces/jsp/logout.jsp	Excluded		
/oamlogin/oamssso/*	Excluded		
/index.html	Excluded		
/.../home	Excluded		

Table 5: Resources

Resource URL	Protection Level	Authentication	Authorization
/.../*	Unprotected	Public	All Allowed
/.../wem/fatwire/wem/Welcome	Protected	Browser	All Allowed
/oamlogin/test	Protected	Browser	All Allowed
/.../REST/*	Protected	REST	All Allowed
/.../wem/fatwire/*	Protected	Browser	All Allowed
/.../faces/jsp/*	Protected	Browser	All Allowed
/.../ContentServer/*	Protected	Browser	All Allowed
/.../Satellite/*	Protected	Browser	All Allowed

- k. After you have finished adding all resources, compare your list of defined resources with Table 5, “Resources” to make sure all policies have been properly defined. Make sure all leading /.../ contain three periods. Make sure each Resource URL is entered in the exact case. The Sites application will not work properly if these policies are not entered correctly.
18. Configuration is now complete and OAM will be used to authenticate users of the WebCenter Sites content management and development installations.
- Stop and then restart all applications, including the OHS server, for all changes to take effect.
19. This step is optional and can be performed only if you have deployed the oamlogin.war file.

- a. Enter the following URL on any browser:

`http(s)://<OHS_host>:<OHS_port>/oamlogin/test`

If the system is operating properly you should see the WebCenter Sites challenge form.

The screenshot shows a web browser window with the title 'ORACLE WebCenter Sites' and 'Version: 11gR1'. The main content area displays the 'Access Manager Secure User Login' form. On the left is the Oracle logo. To the right, there is a title 'Access Manager Secure User Login'. Below this, there are two input fields: 'Username' with the value 'fwadmin' and 'Password'. A 'Forgot password?' link is positioned below the password field. A 'Login' button is centered below the fields. At the bottom right, there is a checked checkbox labeled 'Remember me'.

- b. Enter the username and password and then click **Login**. Remember that the password is defined in LDAP and not the Sites database.
 - c. When the system is working properly a test page will appear that displays all the information provided by the WebGate. This includes the Responses specified in the policies you have created. Refresh this page and it will redisplay updated information.
 - d. Click **Logout** on the test form. The standard OAM logoff acknowledgement form opens.
 - e. Re-enter the URL to display the custom challenge form.
- Carefully review the configuration to ensure the expected results.

Integrating OAM with Oracle WebCenter Sites: Satellite Server

Configuring a Satellite Server for Oracle Access Manager integration is a simpler procedure than for WebCenter Sites. The procedure outlined in this section is specific to configuring a single Satellite Server, but the process is the same for additional Satellite Servers.

This section includes the following topics:

- [Before You Start](#)
- [Integration Steps](#)

Before You Start

Ensure the following actions are complete before integrating Satellite Server:

- Oracle Access Manager is installed and running.
- WebCenter Sites has been successfully integrated with OAM.
- Satellite Server is installed.

Integration Steps

In these steps, you will modify the `SSOConfig.xml` file of the WebCenter Sites deployment. This file controls which authentication classes are loaded and the various properties that are required by those classes.

1. Back up the `SSOConfig.xml` file, located in the deployed `WEB-INF/classes` directory of the deployed WebCenter Sites application.

For example:

```
/u01/software/Apps/Weblogic1035/user_projects/domains/  
OAMCSDomain/applications/SS/WEB-INF/classes/SSOConfig.xml
```

2. Modify `SSOConfig.xml` to look like the file shown below.

Note

In the file below, you will set the following properties: `serviceUrl`, `ticketUrl`, and `signoutUrl`.

The `signoutUrl` property specifies the URL to be used when invoking WebCenter Sites logout. It includes the encoded URL where the browser will return after all logout processing has been completed by OAM.

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xmlns:context="http://www.springframework.org/schema/
context"
       xsi:schemaLocation="
           http://www.springframework.org/schema/beans http://
www.springframework.org/schema/beans/spring-beans-2.5.xsd
           http://www.springframework.org/schema/context http://
www.springframework.org/schema/context/spring-context-2.5.xsd">
  <!-- Single Sign On provider -->
  <bean id="ssoprovider"
class="com.fatwire.wem.sso.oam.OAMProvider">
  <property name="config" ref="ssoconfig" />
</bean>
  <!-- Single Sign On filter -->
  <bean id="ssofilter"
class="com.fatwire.wem.sso.oam.filter.OAMFilter">
  <property name="config" ref="ssoconfig" />
  <property name="provider" ref="ssoprovider" />
</bean>
  <!-- Single Sign On listener -->
  <bean id="ssolistener"
class="com.fatwire.wem.sso.oam.listener.OAMListener">
</bean>
  <!-- Single Sign On configuration -->
  <bean id="ssoconfig"
class="com.fatwire.wem.sso.oam.conf.OAMConfig">

  <!-- URL prefix for REST service endpoint -->
  <property name="serviceUrl" value="http://
{OHS_host}:{OHS_port}/{Sites_context_root}/REST" />

  <!-- URL prefix for Token Service servlet -->
  <property name="ticketUrl" value="http://
{oamtoken_app_server_host}:{oamtoken_port}/oamtoken" />

  <!-- URL to be called when WEM logout is required. -->
  <property name="signoutUrl" value="http://
{weblogic_host}:{oam_server_port}/oam/server/
logout?end_url=http%3A%2F%2F{OHS_host}%3A{oam_server_port}%2F{Sites_co
ntext_root}%2Fwem%2Ffatwire%2Fwem%2Fwelcome" />

```

```
<!-- Proxy tickets, tt's the last server in the
call chain -->
  <property name="proxyTickets" value="true" />

  <!-- Your application protected resources (relative to
applicationUrl) -->
  <!-- For Oracle Access Manager these URLs are not used and
are defined as OAM Authentication Policy resources -->
  <property name="protectedMappingIncludes">
    <list>
    </list>
  </property>
  <property name="protectedMappingStatelessIncludes">
    <list>
      <value>/REST/**</value>
    </list>
  </property>
  <!-- Your application protected resources excludes
(relative to applicationUrl) -->
  <property name="protectedMappingExcludes">
    <list>
    </list>
  </property>
</bean>

</beans>
```

Ensure that the `proxyTickets` parameter is set to `true`. This is required so that Satellite Server will pass authenticated tickets allocated by REST client programs to WebCenter Sites.

The location of the REST endpoint (defined by the `serviceUrl` property) depends on the location of the Satellite Server. When located inside the firewall, it can refer directly to the WebCenter Sites to achieve the highest performance without compromising security. When the Satellite Server is located elsewhere, or exposed directly to the Internet, the endpoint must direct all requests through the OHS to secure and protect WebCenter Sites.

An advanced configuration using OHS in front of Satellite Server is an alternative way of securing the WebCenter Sites configurations. This configuration would access the WebCenter Sites.