Server Installation Guide on UNIX using WebLogic

Version 4.5.1
IBM Tivoli Identity Manager

Server Installation Guide on UNIX using WebLogic

Version 4.5.1
Note:
Before using this information and the product it supports, read the information in Appendix E, “Notices,” on page 125.

Second Edition (February 2004)
This edition applies to version 4.5.1 of Tivoli Identity Manager and to all subsequent releases and modifications until otherwise indicated in new editions.
This edition replaces SC32-1334-00.

© Copyright International Business Machines Corporation 2004. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
## Preface

Who Should Read This Book ................................................................. vii
Publications ......................................................................................... vii
   Tivoli Identity Manager Library ...................................................... vii
   Prerequisite Product Publications .................................................. viii
   Related Publications ...................................................................... ix
   Accessing Publications Online ...................................................... ix
Accessibility ......................................................................................... ix
Contacting Software Support ............................................................. ix
Conventions Used in This Book ......................................................... x
   Typeface Conventions ................................................................... x
   Operating System Differences ...................................................... x
   Revision Bars used in the Version 4.5.1 Library .............................. x
   Definitions for HOME Directory Variables ..................................... x

## Chapter 1. Introduction

Hardware and Software Requirements ............................................... 1
   Using the 4.5.1 Installation Image .................................................. 1
   Upgrading an Existing Tivoli Identity Manager .............................. 1
   Installing Tivoli Identity Manager Version 4.5.1 on a New Computer .... 2

## Chapter 2. Server Configuration and Implementation Overview

WebLogic Terminology ......................................................................... 3
Single-Server Configuration ................................................................. 4
Cluster Configuration ............................................................................ 6

## Chapter 3. Database Configuration

Oracle Installation and Configuration for Tivoli Identity Manager ......... 9
   Preparing to Install Oracle on AIX .................................................. 9
   Preparing to Install Oracle on Solaris ............................................ 11
   Preparing to Install Oracle on HP-UX ........................................... 12
   Preparing to Install Oracle on Windows ....................................... 13
   Configuring Oracle after Installation ............................................ 14

## Chapter 4. Directory Server Configuration

Sun ONE Directory Server Configuration ............................................ 17

## Chapter 5. Single Server Installation: Tivoli Identity Manager Server

Before You Begin .................................................................................. 19
   Information Worksheet for Single-Server Installation ..................... 19
Installing the Tivoli Identity Manager Server .................................... 23
   Navigate Initial Welcome and Licensing Windows .......................... 25
   Select the Installation Type and Directories .................................. 27
   Define the Tivoli Identity Manager Installation Location .................. 27
   Specify the Encryption Key and Install the Tivoli Identity Manager Server .................................................. 29
   Initial Configuration of Tivoli Identity Manager Database .............. 30
   Initial Configuration of the Directory for Tivoli Identity Manager .... 31
   Initial Configuration of Tivoli Identity Manager Server .................. 33
Optionally Installing a Language Pack .............................................. 37
Starting and Stopping the Tivoli Identity Manager Server .................. 37
Testing Tivoli Identity Manager Server Communication .................... 38
Certificate Authority for Server-Agent Communication ..................... 38
Increasing the System Memory Usage .............................................. 39
Chapter 6. Cluster Installation: Tivoli Identity Manager Server ........................................... 41

Before You Begin .................................................................................................................. 41
  Information Worksheet for Clustered Installation ................................................................. 42
Installing the Tivoli Identity Manager Server ......................................................................... 45
  Installing the Admin Server ................................................................................................ 47
  Installing a Managed Server ............................................................................................... 62
Optionally Installing a Language Pack .................................................................................. 75
Starting and Stopping the Tivoli Identity Manager Server ............................................... 75
Testing Tivoli Identity Manager Server Communication .................................................... 75
Certificate Authority for Server-Agent Communication ..................................................... 76
Configuring the Proxy Server ............................................................................................... 76
  IIS HTTP Server Configuration ........................................................................................ 76
  Apache HTTP Server Configuration .................................................................................. 77
Increasing the System Memory Usage .................................................................................. 78

Appendix A. Installation Images as Compact Discs and Fix Packs ........................................ 79

I Obtaining 4.5.1 Fix Packs ..................................................................................................... 79
Version 4.5.0 Compact Discs ............................................................................................... 79
  Language Packs CD ............................................................................................................ 79
  Base Code Solaris CD for Tivoli Identity Manager using WebSphere Application Server .... 80
  Base Code Solaris CD for Tivoli Identity Manager for non-IBM Application Servers ....... 80
  Supplemental Solaris CD 1 ............................................................................................... 80
  Supplemental Solaris CD 2 ............................................................................................... 80
  Supplemental Solaris CD 3 ............................................................................................... 81
  Supplemental Solaris CD 4 ............................................................................................... 81
  Base Code AIX CD for Tivoli Identity Manager using WebSphere Application Server .... 81
  Base Code AIX CD for Tivoli Identity Manager for non-IBM Application Servers ........ 81
  Supplemental AIX CD 1 ................................................................................................... 82
  Supplemental AIX CD 2 ................................................................................................... 82
  Supplemental AIX CD 3 ................................................................................................... 82
  Base Code HP-UX CD for Tivoli Identity Manager for non-IBM Application Servers ...... 83
  Base Code Windows 2000 CD for Tivoli Identity Manager using WebSphere Application Server 83
  Base Code Windows 2000 CD for Tivoli Identity Manager for non-IBM Application Servers 83
  Supplemental Windows 2000 CD 1 ................................................................................ 83
  Supplemental Windows 2000 CD 2 ................................................................................ 84
  Supplemental Windows 2000 CD 3 ................................................................................ 84
  Supplemental Windows 2000 CD 4 ................................................................................ 84

Appendix B. Upgrading from Tivoli Identity Manager 4.3 to Version 4.5 using WebLogic, and then to Version 4.5.1 ....................................................................... 85

Before Upgrading .................................................................................................................. 86
Upgrading from Single Server Version 4.3 to Single Server Version 4.5 ......................... 87
  Prepare to Upgrade the Server ......................................................................................... 87
  Select the Installation Type and Directories .................................................................... 88
  Define the Installation Location. ....................................................................................... 88
  Upgrade the Tivoli Identity Manager Server Schemas ..................................................... 90
  Complete the Upgrade Process ......................................................................................... 91
  Updating Certificate Information ...................................................................................... 91
  Re-implement Customizations ......................................................................................... 92
  Starting and Stopping the Tivoli Identity Manager Server .............................................. 92
  Testing Tivoli Identity Manager Server Communication ................................................. 93
Upgrading from Cluster Version 4.3 to Cluster Version 4.5 .............................................. 93
  Upgrade the Admin Server ............................................................................................... 93
  Upgrade the Managed Servers ......................................................................................... 99
  Updating Certificate Information ...................................................................................... 104
  Re-implement Customizations ......................................................................................... 104
  Starting and Stopping the Tivoli Identity Manager Server .............................................. 105
  Testing Tivoli Identity Manager Server Communication ................................................. 105
I Upgrading Version 4.5 using WebLogic to 4.5.1 ............................................................ 106
Appendix C. Upgrading from Tivoli Identity Manager 4.5 to Version 4.5.1 using WebLogic ................................................................. 107
| Before Upgrading ........................................................................... 107 |
| Upgrading from Single Server Version 4.5 to Single Server Version 4.5.1 ........................................................................ 108 |
| - Prepare to Upgrade the Server .................................................. 108 |
| - Select the Installation Type and Directories .................................. 108 |
| - Define the Installation Location .................................................. 109 |
| - Upgrade the Tivoli Identity Manager Server Schemas ..................... 110 |
| - Complete the Upgrade Process ................................................... 111 |
| - Re-implement Customizations .................................................... 111 |
| - Starting and Stopping the Tivoli Identity Manager Server ............... 112 |
| - Testing Tivoli Identity Manager Server Communication .................. 112 |
| Upgrading from Cluster Version 4.5 to Cluster Version 4.5.1 ............... 113 |
| - Upgrade the Admin Server ....................................................... 113 |
| - Upgrade the Managed Servers ................................................... 117 |
| - Re-implement Customizations .................................................... 120 |
| - Starting and Stopping the Tivoli Identity Manager Server ............... 121 |
| - Testing Tivoli Identity Manager Server Communication .................. 121 |

Appendix D. Uninstalling ................................................................. 123
Steps to Uninstall Tivoli Identity Manager ........................................ 123

Appendix E. Notices ........................................................................ 125
Trademarks ...................................................................................... 126

Glossary ......................................................................................... 129

Index .............................................................................................. 133
Preface

The IBM® Tivoli® Identity Manager Server Installation Guide on UNIX using WebLogic describes how to install and configure the Tivoli Identity Manager Server on a UNIX server to manage resources from a central location.

Who Should Read This Book

This manual is intended for system and security administrators who install, maintain, or administer software on their site’s computer systems. Readers are expected to understand system and security administration concepts. Additionally, the reader should understand administration concepts for the following:

- Directory server
- Database server
- WebSphere® embedded messaging support
- WebSphere Application Server or WebLogic
- IBM HTTP Servers

Publications

Read the descriptions of the Tivoli Identity Manager library, the prerequisite publications, and the related publications to determine which publications you might find helpful. After you determine the publications you need, refer to the instructions for accessing publications online.

Tivoli Identity Manager Library

The publications in the Tivoli Identity Manager technical documentation library are organized into the following categories:

- Release Information
- Online User Assistance
- Server Installation
- Administration and Configuration
- Technical Supplements
- Agent Installation

Release Information:

- IBM Tivoli Identity Manager Release Notes
  Provides software and hardware requirements for Tivoli Identity Manager, and additional fix, patch, and other support information.
- Tivoli Identity Manager Read This First Card

Online User Assistance:

- Online user assistance for Tivoli Identity Manager
  Provides integrated online help topics for all Tivoli Identity Manager administrative tasks.

Server Installation:
• **IBM Tivoli Identity Manager Server Installation Guide on UNIX and Linux using WebSphere**  
  Provides installation information for Tivoli Identity Manager.

• **IBM Tivoli Identity Manager Server Installation Guide on Windows using WebSphere**  
  Provides installation information for Tivoli Identity Manager.

• **IBM Tivoli Identity Manager Server Installation Guide on UNIX using WebLogic**  
  Provides installation information for Tivoli Identity Manager.

• **IBM Tivoli Identity Manager Server Installation Guide on Windows 2000 using WebLogic**  
  Provides installation information for Tivoli Identity Manager.

**Administration and Configuration:**

• **IBM Tivoli Identity Manager Policy and Organization Administration Guide**  
  Provides topics for Tivoli Identity Manager administrative tasks.

• **IBM Tivoli Identity Manager End User Guide**  
  Provides beginning user information for Tivoli Identity Manager.

• **IBM Tivoli Identity Manager Configuration Guide**  
  Provides configuration information for single-server and cluster Tivoli Identity Manager configurations.

**Technical Supplements:**

• **IBM Tivoli Identity Manager Problem Determination Guide**  
  Provides additional problem solving information for the Tivoli Identity Manager product.

**Agent Installation:**

• The Tivoli Identity Manager technical documentation library also includes an evolving set of platform-specific installation documents for the Agent component of a Tivoli Identity Manager implementation.

**Prerequisite Product Publications**

To use the information in this book effectively, you must have knowledge of the products that are prerequisites for Tivoli Identity Manager. Publications are available from the following locations:

• WebLogic Server  
  [http://e-docs.bea.com/](http://e-docs.bea.com/)

• Database servers  
  – Oracle  

• Directory server applications  
  – Sun ONE Directory Server  

• Web Proxy Server  
  – Microsoft IIS HTTP Server  
  – Apache HTTP Server  
  [http://httpd.apache.org/docs-project](http://httpd.apache.org/docs-project)
Related Publications

Information related to Tivoli Identity Manager Server is available in the following publications:

- The Tivoli Software Library provides a variety of Tivoli publications such as white papers, datasheets, demonstrations, redbooks, and announcement letters. The Tivoli Software Library is available on the Web at: http://www.ibm.com/software/tivoli/library/
- The Tivoli Software Glossary includes definitions for many of the technical terms related to Tivoli software. The Tivoli Software Glossary is available, in English only, from the Glossary link on the left side of the Tivoli Software Library Web page at: http://www.ibm.com/software/tivoli/library/

Accessing Publications Online

The publications for this product are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli software library:

http://www.ibm.com/software/tivoli/library

To locate product publications in the library, click the Product manuals link on the left side of the library page. Then, locate and click the name of the product on the Tivoli software information center page.

Product publications include release notes, installation guides, user’s guides, administrator’s guides, and developer’s references.

Note: To ensure proper printing of PDF publications, select the Fit to page check box in the Adobe Acrobat Print window (which is available when you click File → Print).

Accessibility

The product documentation includes the following features to aid accessibility:

- Documentation is available in both HTML and convertible PDF formats to give the maximum opportunity for users to apply screen-reader software.
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

Contacting Software Support

Before contacting IBM Tivoli Software Support with a problem, refer to the IBM Tivoli Software Support site by clicking the Tivoli support link at the following Web site:

http://www.ibm.com/software/support/

If you need additional help, contact software support by using the methods described in the IBM Software Support Guide at the following Web site:

http://techsupport.services.ibm.com/guides/handbook.html

The guide provides the following information:
• Registration and eligibility requirements for receiving support
• Telephone numbers, depending on the country in which you are located
• A list of information you should gather before contacting customer support

Conventions Used in this Book

This reference uses several conventions for special terms and actions and for operating system-dependent commands and paths.

Typeface Conventions

The following typeface conventions are used in this reference:

**Bold** Lowercase commands or mixed case commands that are difficult to distinguish from surrounding text, keywords, parameters, options, names of Java classes, and objects are in **bold**.

*Italic* Variables, titles of publications, and special words or phrases that are emphasized are in *italic*.

Monospaced Code examples, command lines, screen output, file and directory names that are difficult to distinguish from surrounding text, system messages, text that the user must type, and values for arguments or command options are in monospace.

Operating System Differences

This book uses the UNIX convention for specifying environment variables and for directory notation. When using the Windows command line, replace $variable with %variable% for environment variables and replace each forward slash (/) with a backslash (\) in directory paths. If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Revision Bars used in the Version 4.5.1 Library

The Tivoli Identity Manager version 4.5.1 technical documentation library makes use of revision bar characters to indicate where technical changes have occurred to the information previously found in the version 4.5 library. Revision bars are indicated by a vertical line (| ) in the page margin to the left of the change.

Definitions for HOME Directory Variables

The following table contains the default definitions used in this document to represent the "HOME" directory level for various product installation paths. You can customize the installation directory and HOME directory for your specific implementation. If this is the case, you need to make the appropriate substitution for the definition of each variable represented in this table.

<table>
<thead>
<tr>
<th>Path Variable</th>
<th>Default Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITIM_HOME</td>
<td>Windows: \c:.itim45\</td>
</tr>
<tr>
<td></td>
<td>UNIX: /itim45/</td>
</tr>
<tr>
<td>Path Variable</td>
<td>Default Definition</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>BEA_HOME</td>
<td>Windows: c:\bea\</td>
</tr>
<tr>
<td></td>
<td>UNIX: /usr/local/bea/</td>
</tr>
</tbody>
</table>
Chapter 1. Introduction

This manual describes installing, initially configuring, and verifying the Tivoli Identity Manager Server on either a single-server or cluster configuration. Use the installation documentation that matches the operating system and Web application on your system. There is also a *Tivoli Identity Manager Server Installation Guide for Windows using WebLogic*.

Major steps to install and begin to use the Tivoli Identity Manager Server vary depending on whether installation is for a single-server or cluster configuration. An overview of steps includes the following:

1. Determining whether your configuration should be a single server, or requires a more scalable cluster solution, described in Chapter 2, “Server Configuration and Implementation Overview,” on page 3.


Installing Tivoli Identity Manager Server in a clustered configuration is described in Chapter 6, “Cluster Installation: Tivoli Identity Manager Server,” on page 41.

Hardware and Software Requirements

For a list of software and hardware requirements, refer to the *IBM Tivoli Identity Manager Release Notes*.

Using the 4.5.1 Installation Image

The Tivoli Identity Manager Server version 4.5.1 is provided as fix packs. For more information, see Appendix A, “Installation Images as Compact Discs and Fix Packs,” on page 79.

You can use the Tivoli Identity Manager version 4.5.1 installation image to do the following:

- Upgrade a previously-installed Tivoli Identity Manager from version 4.5.0 to version 4.5.1. For more information, see “Upgrading an Existing Tivoli Identity Manager.”

- Install Tivoli Identity Manager version 4.5.1 on a new computer. For more information, see “Installing Tivoli Identity Manager Version 4.5.1 on a New Computer” on page 2.

Upgrading an Existing Tivoli Identity Manager

Use the Tivoli Identity Manager version 4.5.1 fix pack installation program to upgrade Tivoli Identity Manager.
The upgrade steps will vary, depending on the previous version of Tivoli Identity Manager. For more information, refer to the appendixes in this publication that describe upgrading Tivoli Identity Manager.

**Installing Tivoli Identity Manager Version 4.5.1 on a New Computer**

On a new computer with no previous instance of Tivoli Identity Manager, use the Tivoli Identity Manager version 4.5.1 fix pack to install Tivoli Identity Manager. Use the version 4.5.0 CDs for all required middleware, fix packs, and files.
Chapter 2. Server Configuration and Implementation Overview

Servers in a WebLogic environment are organized in either a single-server configuration or a cluster configuration. This section provides a brief, high-level description of configuration options and an overview of their implementation sequences. Subsequent chapters provide greater implementation detail.

Notes:
1. Sample configurations in this chapter require a number of prior planning activities before taking the steps that install and configure this product. For additional documentation that describes planning to meet your business needs, contact your customer representative.
2. For additional information about the WebLogic products, refer to additional documentation cited in “Prerequisite Product Publications” on page viii.
3. Patches are required for most applications. For more information, refer to the IBM Tivoli Identity Manager Release Notes.

WebLogic Terminology

The following terms describe elements in WebLogic configurations:

admin server
  The administration server (admin server) provides a central point for managing a WebLogic Server domain. Tivoli Identity Manager resources are installed on the admin server. Installing the Tivoli Identity Manager resources on the admin server enables control of all connection information from one location. The Tivoli Identity Manager Application Server is not installed on the admin server.

managed server
  A WebLogic Server instance in a domain that is not the admin server. The Tivoli Identity Manager Application Server is installed on a managed server. Users log into the Tivoli Identity Manager Application Server on the managed server to use the Tivoli Identity Manager application.

Web proxy server
  A server that stands in for another server, routing files and requests to other servers. A Web proxy server is typically used to enhance security.

cluster
  A logical grouping of one or more functionally identical application servers. A cluster provides ease of deployment, configuration, workload balancing, and fallback redundancy. A cluster is a collection of servers working together as a single system to ensure that mission-critical applications and resources remain available to clients. A Tivoli Identity Manager cluster is located in a WebLogic Server domain.

single-server
  A configuration that consists of only one instance of the Tivoli Identity Manager Server. The physical location of the Tivoli Identity Manager Server with respect to the directory server or the database is irrelevant.
A single-server configuration of Tivoli Identity Manager has only one instance of the Tivoli Identity Manager Server installed and running. As long as the Tivoli Identity Manager Server can connect to the database and the directory server, the physical location of the Tivoli Identity Manager Server is irrelevant with respect to the physical locations of the database or the directory server. The following figures display three possible single-server configurations for Tivoli Identity Manager. There are many other configurations possible.

**Note:** If the Tivoli Identity Manager Server is not installed on the same system as the database, a database client must be installed on the system where the Tivoli Identity Manager Server is installed.

---

*Figure 1. Single-server configuration on one physical computer*
Figure 2. Single-server configuration on two physical computers
Cluster Configuration

A clustered configuration has multiple instances of the Tivoli Identity Manager Server configured to work together to improve performance and scalability. One of the Tivoli Identity Manager Servers must be designated as an admin server. The admin server manages the resource allocation in the cluster. All other Tivoli Identity Manager Servers must be installed as managed servers.

Notes:

1. All of the Tivoli Identity Manager Servers in the cluster must be installed on the same operating system.
2. Do not place members from two different clusters on the same physical computer.
Figure 4. Clustered configuration
Chapter 3. Database Configuration

This chapter describes configuring a database for use with Tivoli Identity Manager Server. For more information on supported database releases and required patches for Tivoli Identity Manager Server using WebLogic, refer to the IBM Tivoli Identity Manager Release Notes.

This section describes "Oracle Installation and Configuration for Tivoli Identity Manager."

Oracle Installation and Configuration for Tivoli Identity Manager

This section describes pre-installation procedures and post-installation configuration steps for an installation of Oracle within a framework of Tivoli Identity Manager.

In all cases, refer to the installation guide for Oracle for complete information.

Note: When you install Oracle, you must include the JServer option as part of the install. If you choose a typical Oracle install, JServer is included. If you choose to perform a custom Oracle install, ensure that JServer is selected as an option for installation.

For Oracle 9i, you must enable JVM (JServer) when you create the database instance, or any transactions from Tivoli Identity Manager will fail.

Preparing to Install Oracle on AIX

Complete the following procedures prior to installing Oracle on an AIX system:

1. Log in to the AIX system as root.
2. Ensure that the AIX system has the following filesets installed:
   - bos.adt.base
   - bos.adt.1ibm

   The Oracle product installation links with local libraries to create Oracle executables. Without the filesets, the links will fail and Oracle will not install or run correctly. You can install these filesets from the AIX developer's toolkit CD.

3. Verify that your system meets or exceeds the free disk space requirements for the following directories:
   - /usr: 3 GB
   - /var: 300 MB
   - /tmp: 2 GB

   For AIX, the default Oracle installation directory is /usr.

Notes:

a. To determine disk space availability, enter the following command:
   `df - Ivk`

   Output values are in units of 1024 bytes.

4. Create a CD-ROM filesystem, if not already present, using the SMITTY utility:
   a. Type $ mkdir /cdrom from the console or command line.
   b. Type $ smitty cdrfrfs from the console or command line.
      The following menu appears:

      Add a CDROM File System
      Type or select values in entry fields.
      Press Enter AFTER making all desired changes.
      [Entry Fields]
      * DEVICE name
      * MOUNT POINT
      Mount AUTOMATICALLY at system restart?
      no +

   c. Select a CD-ROM drive by pressing F4, selecting a drive, and pressing Enter.
   d. Hit Enter again to create the filesystem. Exit SMITTY with F10 when the creation command completes.
   e. Mount the cdrom directory with the following command:
      
mount /cdrom

5. Create mount points to use with Oracle databases:
   $ mkdir /u01
   $ mkdir /u02

6. Set permissions for the mount points to allow the Oracle user account to write to them during the installation:
   $ chmod 777 /u01
   $ chmod 777 /u02

7. Use SMIT to create two groups; a user group named dba and a user group named oper.

8. Use SMIT to create a new user called oracle. Complete the following steps for the new user account.
   a. Set the Primary GROUP of the account to the dba group you created.
   b. Set the HOME directory of the account to /home/oracle.
   c. Set the login shell (Initial PROGRAM) to /bin/sh.

   The Oracle account will run the installer. This account must be used only for installing and maintaining Oracle.

9. Check that a file path of /usr/1bin exists and is included in the PATH for the Oracle user account. This path can be set by editing /home/oracle/.profile.

10. Create the oratab file by executing the oratab.sh script located in the orainst directory of the CD.
    $ ./oratab.sh

11. Sign on to the system as the oracle user:
    $ su - oracle

12. View the umask settings for the oracle account.
    $ umask

    The umask should be set to 022. If the account’s umask is not set to 022, set it with the following command:
$ umask 022

13. Edit .profile and add the following environment variable settings:
   - Oracle 8i:
     ```
     ORACLE_BASE=/u01/app/oracle; export ORACLE_BASE
     ORACLE_HOME=$ORACLE_BASE/product/8.1.7; export ORACLE_HOME
     LIBPATH=$ORACLE_HOME/lib; export LIBPATH
     LD_LIBRARY_PATH=$ORACLE_HOME/lib:$ORACLE_HOME/network/lib; export LD_LIBRARY_PATH
     ORACLE_SID=or1; export ORACLE_SID
     ORACLE_TERM=vt100; export ORACLE_TERM
     ```
   - Oracle 9i:
     ```
     ORACLE_BASE=/u01/app/oracle; export ORACLE_BASE
     ORACLE_HOME=$ORACLE_BASE/product/9.2.0.0.0; export ORACLE_HOME
     LIBPATH=$ORACLE_HOME/lib; export LIBPATH
     LD_LIBRARY_PATH=$ORACLE_HOME/lib:$ORACLE_HOME/network/lib; export LD_LIBRARY_PATH
     ORACLE_SID=or1; export ORACLE_SID
     ORACLE_TERM=vt100; export ORACLE_TERM
     ```

   Make sure that the oracle user’s PATH includes $ORACLE_HOME/bin, /bin and /usr/bin. If it does not, add them to .profile.

14. Source the profile using the following command:
   ```
   $ ./.profile
   ```
   The UNIX shell reads the profile and initializes or updates the current environment based on values in the profile.

15. Run rootpre.sh to ready the machine for install from /cdrom:
   ```
   $ ./rootpre.sh
   ```

You are now ready to begin the Oracle installation.

**Preparing to Install Oracle on Solaris**

Complete the following procedures prior to installing Oracle on a Solaris system:

1. Log in to the Solaris system as root.
2. Ensure that the kernel parameters set for the system meet or exceed values required for the installation. Refer to the Oracle 8i Installation Guide for more information.
3. Create mount points to use with Oracle databases:
   ```
   $ mkdir /u01
   $ mkdir /u02
   ```
4. Start the admintool utility from a console, using the following command:
   ```
   # admintool
   ```
5. In the Admintool window, click Browse -> Groups. The Admintool:Groups window opens.
7. Create two groups; a user group named dba and a user group named oinstall.
8. In the Admintool:Groups window, click Browse -> Users. The Admintool:Users window opens.
9. Use admintool to create a new user called oracle. Complete the following steps for the new user account.
   a. Set the Primary Group of the account to the oinstall group you created.
   b. Set the Secondary Group of the account to the dba group you created.
   c. Ensure that the radio button beside the Create Home Directory field is selected. In the Path field, enter /export/home/oracle as the home directory for the user oracle.
   d. Set the Login Shell to /bin/sh.
The Oracle installer must be run under this account. This account will be used only for installing and maintaining Oracle.

10. Sign on to the system as the oracle user:
    
    `# su - oracle`

    View the umask settings for the oracle account.
    
    `$ umask`

    The umask should be set to **022**. If the account’s umask is not set to 022, set it with the following command:
    
    `$ umask 022`

    Also modify `.profile` to reflect the change.

11. Add the following to `/export/home/oracle/.profile` for the oracle account:
    
    - **Oracle 8i**:
      
      ```bash
      ORACLE_BASE=/u01/app/oracle; export ORACLE_BASE
      ORACLE_HOME=$ORACLE_BASE/product/8.1.7; export ORACLE_HOME
      ORACLE_SID=orcl; export ORACLE_SID
      ORACLE_DOC=$ORACLE_HOME/doc; export ORACLE_DOC
      ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data; export ORA_NLS33
      PATH=$ORACLE_HOME/bin:/usr/bin:/usr/local/bin:/usr/ccs/bin:/usr/ucb:/usr/openwin/bin:
      ```
    
    - **Oracle 9i**:
      
      ```bash
      ORACLE_BASE=/u01/app/oracle; export ORACLE_BASE
      ORACLE_HOME=$ORACLE_BASE/product/9.2.0.0; export ORACLE_HOME
      ORACLE_SID=orcl; export ORACLE_SID
      ORACLE_DOC=$ORACLE_HOME/doc; export ORACLE_DOC
      ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data; export ORA_NLS33
      PATH=$ORACLE_HOME/bin:/usr/bin:/usr/local/bin:/usr/ccs/bin:/usr/ucb:/usr/openwin/bin:
      ```

    If you require `/usr/ucb` in your search path make sure it is listed after `/usr/ccs/bin` in the PATH setting.

12. Source the profile using the following command:
    
    `$ . ~/.profile`

You are now ready to begin the Oracle installation. Refer to the appropriate Oracle documentation and install the software. After a successful installation, return to the configuration instructions contained in this section.

### Preparing to Install Oracle on HP-UX

Complete the following procedures prior to installing Oracle on an HP-UX system:

1. Log in to the HP-UX system as root.
2. Ensure that the kernel parameters set for the system meet or exceed values required for the installation. Refer to the installation guide for Oracle for more information.
3. Create mount points to use with Oracle databases:
   
   ```bash
   $ mkdir /u01
   $ mkdir /u02
   ```
4. Start the SAM (Sequential data Access via Metadata) utility from a console, using the following command:
   
   `# sam`

5. In the SAM window, click **Accounts for Users and Groups**. The SAM:Accounts for Users and Groups window opens.
6. In the SAM:Accounts for Users and Groups window, click **Groups**. The SAM:Groups window opens.
7. Create two groups; a user group named **dba** and a user group named **oinstall**.

9. Create a new user called oracle. Complete the following steps for the new user account.
   
a. Set the Primary Group of the account to the oinstall group you created.
   
b. Set the Secondary Group of the account to the dba group you created.
   
c. Ensure that the radio button beside the Create Home Directory field is selected. In the Path field, enter /home/oracle as the home directory for the user oracle.
   
d. Set the Login Shell to /bin/sh.

   The Oracle installer must be run under this account. This account will be used only for installing and maintaining Oracle.

10. Sign on to the system as the oracle user:

        # su - oracle

   View the umask settings for the oracle account.

        $ umask

   The umask should be set to 022. If the account’s umask is not set to 022, set it with the following command:

        $ umask 022

   Also modify .profile to reflect the change.

11. Add the following to /home/oracle/.profile for the oracle account:

        • Oracle 8i:

                ORACLE_BASE=/u01/app/oracle; export ORACLE_BASE
                ORACLE_HOME=$ORACLE_BASE/product/8.1.7; export ORACLE_HOME
                ORACLE_SID=or1; export ORACLE_SID
                ORACLE_HOME=/u01/app/oracle/product/8.1.7; export ORACLE_HOME
                ORACLE_BASE=/u01/app/oracle;
                ORACLE_HOME=$ORACLE_BASE/product/8.1.7; export ORACLE_HOME
                ORACLE_SID=or1; export ORACLE_SID
                ORACLE_HOME=/u01/app/oracle/product/8.1.7; export ORACLE_HOME

        • Oracle 9i:

                ORACLE_BASE=/u01/app/oracle; export ORACLE_BASE
                ORACLE_HOME=$ORACLE_BASE/product/9.2.0.0; export ORACLE_HOME
                ORACLE_SID=or1; export ORACLE_SID
                ORACLE_HOME=/u01/app/oracle/product/9.2.0.0; export ORACLE_HOME
                ORACLE_BASE=/u01/app/oracle;
                ORACLE_HOME=$ORACLE_BASE/product/9.2.0.0; export ORACLE_HOME

   If you require /usr/ucb in your search path make sure it is listed after /usr/ccs/bin in the PATH setting.

12. Source the profile using the following command:

        $ . ~/.profile

   You are now ready to begin the Oracle installation. Refer to the appropriate Oracle documentation and install the software. After a successful installation, return to the configuration instructions contained in this section.

**Preparing to Install Oracle on Windows**

Complete the following procedures prior to installing Oracle on a Windows system:

1. Verify that your system meets or exceeds the system requirements listed in the installation guide for Oracle for the type of installation you intend to perform.

2. Log in to the Windows system with the Administrator account that you will use for the installation.
You are now ready to begin the Oracle installation.

**Configuring Oracle after Installation**

There are several post-installation tasks that must be completed to configure Oracle for use in a Tivoli Identity Manager framework.

1. Verify that the following line exists in the $ORACLE_HOME/dbs/init.ora file:
   - Oracle 8i:
     ```
     compatible=8.1.0
     ```
   - Oracle 9i:
     ```
     compatible=9.2.0.0
     ```

2. Create a database for use with Tivoli Identity Manager.
   The following is a sample SQL script that can be used to create your database. The values in the script should be changed to match your site’s requirements.
   ```
   CREATE DATABASE sample
   CONTROLFILE REUSE
   LOGFILE '/u01/oracle/sample/redo01.log' SIZE 1M REUSE,
   '/u01/oracle/sample/redo02.log' SIZE 1M REUSE,
   '/u01/oracle/sample/redo03.log' SIZE 1M REUSE,
   '/u01/oracle/sample/redo04.log' SIZE 1M REUSE
   DATAFILE '/u01/oracle/sample/system01.dbf' SIZE 10M REUSE
   AUTOEXTEND ON
   NEXT 10M MAXSIZE 200M
   CHARACTER SET UTF8;
   ```
   ```
   CREATE ROLLBACK SEGMENT rb_temp STORAGE (INITIAL 100 k NEXT 250 k);
   ALTER temporary system tablespace online before proceeding
   ALTER ROLLBACK SEGMENT rb_temp ONLINE;
   ```
   ```
   CREATE TABLESPACE rbs
   DATAFILE '/u01/oracle/sample/sample.dbf' SIZE 5M REUSE AUTOEXTEND ON
   NEXT 5M MAXSIZE 150M;
   CREATE TABLESPACE users
   DATAFILE '/u01/oracle/sample/users01.dbf' SIZE 3M REUSE AUTOEXTEND ON
   NEXT 3M MAXSIZE 150M;
   CREATE TABLESPACE temp
   DATAFILE '/u01/oracle/sample/temp01.dbf' SIZE 2M REUSE AUTOEXTEND ON
   NEXT 2M MAXSIZE 150M;
   ```
   ```
   CREATE ROLLBACK SEGMENT rb1 STORAGE (INITIAL 50K NEXT 250K)
   tablespace rbs;
   CREATE ROLLBACK SEGMENT rb2 STORAGE (INITIAL 50K NEXT 250K)
   tablespace rbs;
   CREATE ROLLBACK SEGMENT rb3 STORAGE (INITIAL 50K NEXT 250K)
   tablespace rbs;
   CREATE ROLLBACK SEGMENT rb4 STORAGE (INITIAL 50K NEXT 250K)
   tablespace rbs;
   ```
   ```
   ALTER ROLLBACK SEGMENT rb1 ONLINE;
   ALTER ROLLBACK SEGMENT rb2 ONLINE;
   ALTER ROLLBACK SEGMENT rb3 ONLINE;
   ALTER ROLLBACK SEGMENT rb4 ONLINE;
   ```
   ```
   DROP ROLLBACK SEGMENT rb_temp;
   ```
   ```
   ALTER ROLLBACK SEGMENT rb_temp OFFLINE;
   ```
   ```
   3. Increase the value for Oracle connections from the default of 50 to a value of 150 by editing the PROCESSES parameter of the $ORACLE_HOME/dbs/init.ora file.
**Note:** Oracle connection requirements will vary greatly between enterprises. Set your connection value to a value appropriate for your environment.

4. Increase the Oracle tablespace from the default to the maximum amount available using the `alter` sql command.

```
SQL> alter database datafile 'location of DBF file\ENROLE1_DATA_001.DBF' resize 500m
SQL> alter database datafile 'Oracle db location of DBF file\ENROLE1_IDX_001.DBF' resize 500m
```

5. Start Oracle:

```
# su - oracle
# svrmgrl
> connect internal
> startup
> quit
```

6. Start the Oracle listener service:

```
# su - oracle
# lnsrctl start
```
Chapter 4. Directory Server Configuration

This chapter describes how to configure the directory server for use with Tivoli Identity Manager.

Sun ONE Directory Server Configuration

**Note:** In the following statements, my_suffix is any value for the suffix that you define for Tivoli Identity Manager, such as com.

To configure the Sun ONE Directory Server, do the following:

1. Start the iPlanet Console.
   The iPlanet Console login dialog window appears.
2. Verify the port number in the Administration URL, type in your password, and click OK.
3. Go to your Directory Server in the console tree and click Open.
4. Select the Configuration tab.
5. Right-click Data in the directory server tree on the Configuration tab, and click New Root Suffix.
   The Create new root suffix dialog window appears.
6. Type dc=my_suffix in the New suffix text field on the Create new root suffix dialog window.
7. Type the desired database name in the Database name text field.
   For example, type the following:
   itimdb
8. Select the Create associated database automatically check box if it is not selected and click OK.
   The Confirmation Needed dialog window appears.
9. On the Confirmation Needed dialog window, click Yes.
   The Directory Server console reappears.
10. Select the Directory tab.
11. Right-click the name of the directory server in the directory server tree.
    A pop-up menu appears.
12. Select dc=my_suffix under New Root Object in the pop-up menu.
    The New Object dialog window appears.
13. Select domain and click OK.
    The Property Editor dialog window for dc=my_suffix appears.
14. Click OK in the Property Editor dialog window.
    The Directory Server console reappears.
15. Select the Tasks tab and click Restart the Directory Server.
    The Sun ONE Directory Server is now set up.
16. Increase the memory cache available for the Tivoli Identity Manager Server by completing the following procedures:
    a. Open the directory server console and click the Configuration tab.
b. Expand the Data node in the directory tree and click the **Database Settings** tab.

c. Click the **LDBM Plug-in Settings** tab.

d. Set the Maximum Cache Size setting to an appropriate value based on your hardware’s physical memory.
   
   If Sun ONE Directory Server is installed on its own machine, it is recommended that this value be set to 75% of the system’s available memory.

e. Click **Save**.

f. Expand the Tivoli Identity Manager application node.
   
   For example, this could be dc=com.

g. Select the database object in the Tivoli Identity Manager application node and click the **Database Settings** tab.

h. Set the “Memory available for cache” setting to an appropriate value based on your hardware’s physical memory.
   
   If Tivoli Identity Manager is the only application using this directory, it is recommended that this value be set to 60% of the "Maximum Cache Size" set on the LDBM Plug-in Settings tab.

i. Click **Save**.

j. Click the **Tasks** tab and restart the directory server.
Chapter 5. Single Server Installation: Tivoli Identity Manager Server

This chapter describes tasks that install and configure the Tivoli Identity Manager Server in a single-server configuration.

Installation tasks include the following:

- “Before You Begin”
- “Installing the Tivoli Identity Manager Server” on page 23
- “Optionally Installing a Language Pack” on page 37
- “Starting and Stopping the Tivoli Identity Manager Server” on page 37
- “Testing Tivoli Identity Manager Server Communication” on page 38
- “Certificate Authority for Server-Agent Communication” on page 38
- “Increasing the System Memory Usage” on page 39

Before You Begin

Before you begin, do the following:

- Ensure that the following Tivoli Identity Manager prerequisites are met for a single-server configuration:

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Running</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>✔️</td>
<td>Chapter 3, “Database Configuration,” on page 9</td>
</tr>
<tr>
<td>Directory server</td>
<td>✔️</td>
<td>Chapter 4, “Directory Server Configuration,” on page 17</td>
</tr>
<tr>
<td>WebLogic Server</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Ensure free disk space and virtual memory requirements are met. For more information, refer to the IBM Tivoli Identity Manager Release Notes.

**Note:** On UNIX, the installation process may incorrectly calculate the amount of free space on a shared NFS drive, indicating that there is not enough free space. To work around this problem, install on a local drive or disable the installation process from checking for the amount of free space available. To do so, set the environmental variable CHECK_DISK_SPACE to OFF. For example:

```bash
CHECK_DISK_SPACE=OFF; export CHECK_DISK_SPACE
```

- Ensure you have the correct administrative authority. If not, obtain the authority and re-login to the system to activate the proper authorization.

  On UNIX, you must have root authority.

- On the computer on which Tivoli Identity Manager will be installed, set the appropriate value for your locale to ensure the language format is recognized.

  **Note:** In Japanese, ensure that the encoding method Shift-JIS is supported. License information may not be viewable if these values are not set. Set the following value for the locale environment variable:

  - Solaris: LC_ALL=ja_JP.PKC

© Copyright IBM Corp. 2004
If you are using Oracle for your database, you need to copy the Oracle JDBC driver (in the file name classes12.zip) from the supplementary CD into a temporary local directory.

Complete the information worksheet for your configuration.

**Information Worksheet for Single-Server Installation**
Collect the following information before you begin installation:

**WebLogic Information**
Collect the following information about the WebLogic Server.

- **BEA Home Directory**
  BEA installation directory. Default value is /usr/local/bea

- **WebLogic Server Directory**
  WebLogic Server home directory. Default value is /usr/local/bea/weblogic700

**Tivoli Identity Manager Information**
Determine the values for the following properties for the Tivoli Identity Manager Server:

- **Tivoli Identity Manager**
  Directory where Tivoli Identity Manager will be installed.

- **Domain Base Directory**
  Base directory location of the WebLogic domain dedicated to Tivoli Identity Manager.

- **Domain Name**
  Name of the WebLogic domain dedicated to Tivoli Identity Manager.

- **Server Name**
  Name of the server where this instance of Tivoli Identity Manager is being installed.

- **Encryption Key**
  Key used to encrypt Tivoli Identity Manager passwords and other sensitive text. The default value is sunshine. The key can be any word or phrase. This word or phrase should be used as the encryption key for each member of the cluster. This value is stored in the enRole.properties file as enrole.encryption.password.

**Database Information**
Collect the following information for the relational database management system:

- **Database Type**
  Type of database used for your system.

  **Note:** Only supports the Oracle database.

- **Admin ID**
  The Administrator User ID that you created when you configured the database.

- **Admin Password**
  The password for the Administrator user ID.


<table>
<thead>
<tr>
<th><strong>Database Name</strong></th>
<th>Name of the database to be used with the Tivoli Identity Manager Server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Credentials for the database:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Database User</strong></td>
<td>The account that Tivoli Identity Manager Server uses to connect to the database. The user ID is enrole.</td>
</tr>
<tr>
<td><strong>Note:</strong> This user ID cannot be changed.</td>
<td></td>
</tr>
<tr>
<td><strong>User Password</strong></td>
<td>Password for the account that Tivoli Identity Manager Server uses to connect to the database. This password can be changed using the System Configuration Tool. See the IBM Tivoli Identity Manager Configuration Guide for more information about the System Configuration Tool.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>IP address or hostname of the database server. Required for Oracle and SQL Server 2000 (SP3) databases.</td>
</tr>
<tr>
<td><strong>Port Number</strong></td>
<td>Port number of the database server. Required for Oracle and SQL Server 2000 (SP3) databases.</td>
</tr>
</tbody>
</table>

Additionally, the installation windows report the following Database Pool information during installation. The database pool information determines the number of JDBC connections that Tivoli Identity Manager Server can open to the database. For more information, refer to the *IBM Tivoli Identity Manager Configuration Guide*.

Evaluate the following in relation to your site needs:

| **Initial Capacity** | Initial number of JDBC connections that Tivoli Identity Manager Server can open to the database |
| **Maximum Capacity** | Maximum number of JDBC connections that Tivoli Identity Manager Server can open to the database at any one time |
| **Login Delay Seconds** | Time, in seconds, between connection creation. |

**Directory Server Information**
Collect the following information:

| **Principal DN** | The directory server Administrator user ID. For example, cn=root. |
| **Password** | The password of the Principal Distinguished Name user ID that you created when installing the directory server. |
| **Host name** | Fully-qualified host name of the directory server. For example, identity1.mylab.mydomain.com. |
Port __________________________________________

Port on which the directory server is listening, such as 389.

Number of hash buckets ____________________________

A hash bucket is a notional receptacle, a set of which might be used to
apportion data items for sorting or lookup purposes. Evaluate the default
(1) in relation to your site needs.

Name of your organization __________________________

The value that you enter in the Name of Your Organization field will be
displayed in the organization chart that is displayed on many of the Tivoli
Identity Manager graphical user interface screens. This value is typically
the more formal name of your company. For example, an organization
name is IBM Corporation.

Note: You may enter either single-byte (ASCII) characters or double-byte
character set characters in this field.

Default Org Short Name ____________________________

The value that you enter in the Default Org Short Name field will be used
internally in Sun ONE Directory Server to represent your organization.
This value is typically an abbreviation of your company name. For
example, a short name is ibmcorp.

Note: Enter only single-byte (ASCII) characters in the Default Org Short
Name field, such as an identifier in English.

Identity Manager DN Location _______________________

The value such as dc=com that you enter in the Location field must match
the suffix (for example, dc=com) that you created when you configured
LDAP.

Additionally, the installation windows report the following LDAP Connection Pool
Information fields for a pool of LDAP connections accessible by Tivoli Identity
Manager Server. For more information, refer to the IBM Tivoli Identity Manager
Configuration Guide.

Evaluate the following in relation to your site needs:

Max. pool size
Maximum number of connections the LDAP Connection Pool can have at
any time

Initial pool size
Initial number of connections created for the LDAP Connection Pool

Increment count
Number of connections added to the LDAP Connection Pool every time a
connection is requested once all connections are in use

Tivoli Identity Manager Logon Information

Note the following information for Tivoli Identity Manager:

User ID _________________________________________

The Tivoli Identity Manager user ID. The default after installation is itim
manager. Use this user ID when you log on to Tivoli Identity Manager.

Password _________________________________________
Password for the Tivoli Identity Manager user ID specified as it.im
manager. The default password after installation is secret.

Note: It is important that you change this password and make a record of
the new password immediately after you first log on.

Installing the Tivoli Identity Manager Server

Installing Tivoli Identity Manager requires installing the Tivoli Identity Manager
Server and configuring various server properties to enable it to connect to the
database and directory server. In a single-server configuration, there is only one
instance of the Tivoli Identity Manager Server installed for use.

The following flowchart describes the basic sequence of windows that install Tivoli
Identity Manager in a single-server configuration.
Figure 5. Single Tivoli Identity Manager Server Installation Overview
Navigate Initial Welcome and Licensing Windows

A series of welcome and licensing windows start the installation process. To navigate the initial windows, do the following:

1. Log on to the computer where the Tivoli Identity Manager Server will be installed.

   **Note:** You must log on using an account with system administration privileges.

2. Obtain the Tivoli Identity Manager product installation image.

3. Open a command prompt window and change to your CD-ROM drive.

4. Run the following installation program:
   
   ```
   instOS-WL.bin
   ```
   
   where OS is the abbreviation for your system’s operating system.

   The abbreviations are: AIX for the AIX operating system; SOL for the Solaris operating system; HPUX for the HP-UX operating system.

   The Language Selection window opens.

5. Select the desired language in the language drop-down menu and click **OK**.

   The License Agreement window opens.
6. Read the license agreement and decide whether to accept its terms.
7. Select the I accept the terms of the License Agreement radio button if you agree to the terms and click Next.
   The Choose Installation Type window opens. Proceed with choosing an installation type.

Figure 7. License Agreement Window

Figure 8. Choose Installation Type Window
Select the Installation Type and Directories

The next steps determine the type of Tivoli Identity Manager to install and the location of the WebLogic Server used by Tivoli Identity Manager.

1. Select the radio button for the type of installation you desire in the Choose Installation Type window and click Next.

   If you want to install a single-server version of Tivoli Identity Manager, select the Single Server radio button. If you want to install a clustered version of Tivoli Identity Manager, select the Cluster radio button.

   The Have you installed BEA WebLogic Server 7.0? window opens.

2. Click Yes if you have already installed the WebLogic Server.

   If you click No, you can continue with the installation but you will have to install WebLogic 7.0 before Tivoli Identity Manager will run. It is recommended that you exit the installation and install the WebLogic Server before installing Tivoli Identity Manager.

   The Where have you installed WebLogic Server 7.0? window opens.

![Figure 9. Where have you installed WebLogic Server 7.0? Window](image)

3. Enter the BEA home directory and the WebLogic Server home directories in their respective fields and click Next.

   **Note:** In a clustered installation, the WebLogic Server home directory should be the same for each member of the cluster.

   See the following section to proceed with the installation process.

Define the Tivoli Identity Manager Installation Location

This section describes how to define where the Tivoli Identity Manager Server is installed and how the Tivoli Identity Manager Server is recognized by the WebLogic Server.

The previous section ended with the Choose Install Folder window open.
1. Accept the default Tivoli Identity Manager installation directory (/itim45) or enter a different installation directory and click Next. The Specify the Tivoli Identity Manager Domain Information window opens.

2. Accept the default domain base directory (/bea/user_projects) or enter a different directory location.

3. Enter the name of the domain to which the Tivoli Identity Manager Server will be added in the Domain Name field.
4. Enter the name of the Tivoli Identity Manager Server in the Server Name field and click **Next**.
Proceed to the next section to continue with the installation process.

**Specify the Encryption Key and Install the Tivoli Identity Manager Server**

The previous section ended with the Specify the Encryption Key window open.

![Figure 12: Specify the Encryption Key Window](image)

1. Enter the encryption key and click **Next**.

   The encryption key is used to encrypt Tivoli Identity Manager passwords and other sensitive text. The default encryption key is *sunshine*. It is recommended that you change the encryption key.

   **Note:** The encryption key you input here must be the same as the one specified during the admin server installation.

   The Pre-Installation Summary window opens.
2. Review the information listed.
   If any of the information is incorrect, click Previous and correct the values. If there is not enough disk space, cancel the installation and ensure that the required disk space is available before installing Tivoli Identity Manager.

3. Click Install.
   A series of installation progress windows open during the interval that the installation requires. After the installation completes, you must configure the Tivoli Identity Manager Server.

4. Proceed to the following section to continue with the installation process.

**Initial Configuration of Tivoli Identity Manager Database**

After the Tivoli Identity Manager Server is installed, the Tivoli Identity Manager database must be configured. The installation program uses the database configuration tool to configure the database.

The previous section ended with the IBM Tivoli Identity Manager Database Configuration window open.
Note: If you are using Oracle for your database, you will need to copy the Oracle JDBC driver (in the file name classes12.zip) from the temporary local directory (where you saved the JDBC driver from the supplementary CD earlier) to the ITIM_HOME/lib directory.

1. Enter the database connection information in the appropriate fields of the IBM Tivoli Identity Manager Database Configuration window and click Test.
   If the test is successful, a message window opens confirming that the connection is successful.

2. Click OK.
   The IBM Tivoli Identity Manager Database Configuration window reappears with the Identity Manager User Information fields active.

3. Enter the Tivoli Identity Manager user ID and password in their respective fields and click Continue.
   The default values for these fields are listed in the information worksheet. A message window opens confirming that the database configuration is complete.

4. Click OK.
   The IBM Tivoli Identity Manager Directory Configuration window opens.

5. Proceed to configure the directory to continue with the installation process.

**Initial Configuration of the Directory for Tivoli Identity Manager**

The Tivoli Identity Manager directory server connection must be configured after installing the Tivoli Identity Manager Server. The following procedures describe how to configure the Tivoli Identity Manager Server to recognize the directory server.

The previous section ended with the IBM Tivoli Identity Manager Directory Configuration window open.
1. Enter the LDAP server information in the appropriate fields of the IBM Tivoli Identity Manager Directory Configuration window and click Test.
   If the test is successful, a message window opens confirming that the connection was successful.

2. Click OK.
   The IBM Tivoli Identity Manager Directory Configuration window reappears with the Identity Manager Directory Information fields active.

---

Figure 15. IBM Tivoli Identity Manager Directory Configuration Window
3. Select the database used with Tivoli Identity Manager.
4. Accept the default number of hash buckets or enter a new value.
   Hash buckets can hold up to 1,000,000 entries.
5. Complete the remaining Identity Manager Directory Information fields and click **Continue**.
   See the information worksheet for more information about each field. A message window opens confirming that the directory server configuration was successful.
6. Click **OK**.
   The directory server configuration tool closes and the system configuration tool window opens.

**Initial Configuration of Tivoli Identity Manager**

The remaining windows provide an initial configuration of Tivoli Identity Manager. During this activity, you can change values you initially set for the database server and the directory server and modify some system default configuration values. Default values that must be modified are detailed in the procedures.

1. Verify that the information listed on the General tab is correct.
2. Click the **Directory** tab and verify that the information listed is correct.

   If any of the information is not correct, modify the information and click **Test** to verify that the connection information is correct.

3. Click the **Database** tab and verify that the information listed is correct.

   If the information is not correct, modify the information and click **Test** to verify that the connection information is correct.
4. Click the **Logging** tab and modify the level of logging as desired.

5. Click the **Mail** tab and verify that the Identity Manager Server URL is correct.

   **Note:** In a clustered configuration, the Identity Manager Server URL should be the URL of the proxy server, if one is used.
6. Change the Mail From address to the Tivoli Identity Manager system administrator e-mail address for your site.

   **Note:** You must change this address. The default address is a valid IBM e-mail address. If you do not change this address you will send spam to the e-mail address listed.

7. Enter the mail server name in the respective field.

8. Click the UI tab and modify the values as desired.

   Refer to the *IBM Tivoli Identity Manager Configuration Guide* for additional information about customizing the user interface.
9. Click the **Security** tab and modify the values as desired.

![Figure 23. Security Tab of the System Configuration Window](image)

10. Click **OK** to finish configuring the Tivoli Identity Manager Server.
11. Proceed to the following section to continue with the installation process.

### Optionally Installing a Language Pack

After installing Tivoli Identity Manager, if the default language is not English, optionally obtain and mount the language pack CD for the Tivoli Identity Manager Server. Use command line mode to install the language pack. For example, enter the following:

```bash
java -jar itimlp_setup.jar
```

The Tivoli Identity Manager language pack setup program will start. To complete the language pack installation, follow the instructions that appear in the setup program panels.

**Note:** To run the Tivoli Identity Manager language pack setup program, Java runtime environment 1.3.1 should be accessible from the command line.

### Starting and Stopping the Tivoli Identity Manager Server

After the Tivoli Identity Manager Server is installed you must start the server. This section describes how to start and stop the Tivoli Identity Manager Server.

On UNIX servers, Tivoli Identity Manager installed a script to start and stop the Tivoli Identity Manager Server in the \*ITIM\*_HOME directory

To start the Tivoli Identity Manager Server, use the following command:

```bash
sh im.sh start
```
Note: Starting the Tivoli Identity Manager Server takes several minutes. Watch the BEA_HOME/user_projects/itim/logs/server_name.log file for a running message. The server_name is the name of the server defined earlier during installation.

To stop the Tivoli Identity Manager Server, use the following command:

sh itim.sh stop

---

Testing Tivoli Identity Manager Server Communication

To test whether the database, the directory server, and the Tivoli Identity Manager Server are correctly configured and communicating with each other, do the following:

1. Start Tivoli Identity Manager Server and any prerequisite applications.
2. Log on to Tivoli Identity Manager.
   For example, at a browser window, type the following:
   http://hostname/enrole

   where hostname is the fully-qualified name or IP address of the computer on which Tivoli Identity Manager Server is running.
3. Enter the Tivoli Identity Manager administrator user ID (itim manager) and password.
4. Take the necessary steps to create a user (an ITIM user).
   For more information, refer to online help or to the IBM Tivoli Identity Manager Policy and Organization Administration Guide.

---

Certificate Authority for Server-Agent Communication

Using the Tivoli Identity Manager system with a Tivoli Identity Manager Agent will require production certificates to ensure secure communication between the Tivoli Identity Manager Server and the Agent. The Certificate Authority that corresponds to the Tivoli Identity Manager Agent’s certificate must be located in the ITIM_HOME/cert directory. Refer to the IBM Tivoli Identity Manager Configuration Guide and to a specific agent’s installation guide for more information.

Notes:

1. In a cluster configuration, the certificate must be installed in the same directory on each member in order for the agent to locate the certificate.
2. If the default language is not English, before installing the first Tivoli Identity Manager agent, optionally obtain and mount the language pack CD for the Tivoli Identity Manager agents. Use command line mode to install the language pack for the agents on the Tivoli Identity Manager Server:
   java -jar itimlp_agents_setup.jar
   The Tivoli Identity Manager language pack setup program will start. To complete the language pack installation, follow the instructions that appear in the setup program panels.

   Note: To run the Tivoli Identity Manager language pack setup program, Java runtime environment 1.3.1 should be accessible from the command line.
3. For recommendations on where to install the agent profile in a cluster configuration, refer to the agent installation guide for your specific agent.
Increasing the System Memory Usage

The Tivoli Identity Manager Server is configured to use the least amount of memory required for basic operation in a standard installation. By default, the Tivoli Identity Manager Server is configured to use a minimum and maximum of 256 megabytes (MB) of memory. These values can be modified to enable the system to perform at optimum speed.

In order to optimize the performance of the Tivoli Identity Manager Server, 75% of the total memory available (up to a maximum of 1024 MB) should be reserved for the Tivoli Identity Manager Server, assuming no other software is running on the system. For example, if there is 1 gigabyte (GB) of memory available on the system where the Tivoli Identity Manager Server is installed, the Tivoli Identity Manager Server should be configured to use 768 MB.

The following are detailed procedures on how to increase the memory usage for the Tivoli Identity Manager Server.

1. Log into the system where the Tivoli Identity Manager Server is installed.
2. Open the Tivoli Identity Manager Server startup script in a text editor.
   - The script is located in the ITIM_HOME/bin directory. In a single-server installation, the script is named itim.sh. In a clustered installation, the script is named serverName.sh where serverName is the name of the managed server.
3. Find the following line in the script:
   MEM_ARGS=-XX:MaxPermSize=128m -Xms256m -Xmx256m
4. Change the -Xms and -Xmx settings to an appropriate value based on your hardware.
   - The -Xms value is the minimum memory usage.
   - The -Xmx value is the maximum memory usage.
   If Tivoli Identity Manager Server is the only application running on the machine, it is recommended that both the minimum and maximum memory usage parameters be set to 75% of the available system memory as long as they do not exceed 1024 MB, individually. BEA also recommends that these parameters be set to the same value.
5. Save the script.
6. Stop and restart the Tivoli Identity Manager service.
Chapter 6. Cluster Installation: Tivoli Identity Manager Server

This chapter describes installing and configuring the Tivoli Identity Manager Server in a regular cluster configuration.

Installation tasks include the following:
- “Before You Begin”
- “Installing the Tivoli Identity Manager Server” on page 45
- “Optionally Installing a Language Pack” on page 75
- “Starting and Stopping the Tivoli Identity Manager Server” on page 75
- “Testing Tivoli Identity Manager Server Communication” on page 75
- “Certificate Authority for Server-Agent Communication” on page 76
- “Configuring the Proxy Server” on page 76
- “Increasing the System Memory Usage” on page 78

Before You Begin

Before you begin, do the following:
- Ensure that the following Tivoli Identity Manager Server prerequisites are met for a clustered configuration:

Table 2. Prerequisite applications for clustered Tivoli Identity Manager Servers

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Running</th>
<th>For more information, see</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>✔️</td>
<td>Chapter 3, “Database Configuration,” on page 9</td>
</tr>
<tr>
<td>Directory Server</td>
<td>✔️</td>
<td>Chapter 4, “Directory Server Configuration,” on page 17</td>
</tr>
<tr>
<td>WebLogic Server</td>
<td>✔️</td>
<td>—</td>
</tr>
</tbody>
</table>

- Ensure free disk space and virtual memory requirements are met. For more information, refer to the IBM Tivoli Identity Manager Release Notes.

Note: On UNIX, the installation process may incorrectly calculate the amount of free space on a shared NFS drive, indicating that there is not enough free space. To work around this problem, install on a local drive or disable the installation process from checking for the amount of free space available. To do so, set the environmental variable CHECK_DISK_SPACE to OFF. For example: CHECK_DISK_SPACE=OFF;export CHECK_DISK_SPACE

- Ensure that you have correct administrative authority. If not, obtain the authority and re-login to the system to activate the proper authorization.
- You must have root authority.
- On the computer on which Tivoli Identity Manager will be installed, set the appropriate value for your locale to ensure the language format is recognized.

Note: In Japanese, ensure that the encoding method Shift-JIS is supported. License information may not be viewable if these values are not set. Set the following value for the locale environment variable:

- Solaris: LC_ALL=ja_JP.PKC
- AIX: LC_ALL=Ja_JP
  - The Weblogic Server must be installed in the same location on each each member machine of the cluster.
  - If you are using Oracle for your database, you need to copy the Oracle JDBC driver (in the file name classes12.zip) from the supplementary local CD into a temporary local directory.
  - Complete the information worksheet.

**Information Worksheet for Clustered Installation**

Collect the following information before you begin installation:

**WebLogic Information**

Collect the following information about the WebLogic Server.

**BEA Home Directory**

BEA installation directory. Default value is /usr/local/bea

**WebLogic Server Directory**

WebLogic Server home directory. Default value is /usr/local/bea/weblogic700

**Tivoli Identity Manager Information**

Determine the values for the following properties for the Tivoli Identity Manager Server:

**Tivoli Identity Manager**

Directory where Tivoli Identity Manager will be installed.

**Domain Base Directory**

Base directory location of the WebLogic domain dedicated to Tivoli Identity Manager.

**Domain Name**

Name of the WebLogic domain dedicated to Tivoli Identity Manager.

**Server Name**

Name of the server where this instance of Tivoli Identity Manager is being installed.

**Cluster Name**

Name assigned to the Tivoli Identity Manager cluster.

**Cluster Multicast Address**

Broadcast address used for WebLogic cluster communication.

**Cluster Multicast Port**

Port number used to access the other WebLogic Servers in the cluster.

**Encryption Key**

Key used to encrypt Tivoli Identity Manager passwords and other sensitive text. The default value is sunshine. The key can be any word or phrase. This word or phrase should be used as the encryption key for each member of the cluster. This value is stored in the enRole.properties file as enrole.encryption.password.

**Database Information**

Collect the following information for the relational database management system:

**Database Type**

Type of database used for your system.
Note: Only supports the Oracle database.

Admin ID ________________________________________________

The Administrator User ID that you created when you configured the database.

Admin Password ________________________________

The password for the Administrator user ID.

Database Name ________________________________

Name of the database to be used with the Tivoli Identity Manager Server.

Credentials for the database:

Database User

The account that Tivoli Identity Manager Server uses to connect to the database. The user ID is enrol.

Note: This user ID cannot be changed.

User Password

Password for the account that Tivoli Identity Manager Server uses to connect to the database. This password can be changed using the System Configuration Tool. See the IBM Tivoli Identity Manager Configuration Guide for more information about the System Configuration Tool.

IP Address ________________________________

IP address or hostname of the database server. Required for Oracle and SQL Server 2000 (SP3) databases.

Port Number ________________________________

Port number of the database server. Required for Oracle and SQL Server 2000 (SP3) databases.

Additionally, the installation windows report the following Database Pool information during installation. The database pool information determines the number of JDBC connections that Tivoli Identity Manager Server can open to the database. For more information, refer to the IBM Tivoli Identity Manager Configuration Guide.

Evaluate the following in relation to your site needs:

Initial Capacity

Initial number of JDBC connections that Tivoli Identity Manager Server can open to the database

Maximum Capacity

Maximum number of JDBC connections that Tivoli Identity Manager Server can open to the database at any one time

Login Delay Seconds

Time, in seconds, between connection creation.

Directory Server Information

Collect the following information:

Principal DN ________________________________
The directory server Administrator user ID. For example, cn=root.

**Password**

The password of the Principal Distinguished Name user ID that you created when installing the directory server.

**Host name**

Fully-qualified host name of the directory server. For example, identity1.mylab.mydomain.com.

**Port**

Port on which the directory server is listening, such as 389.

**Number of hash buckets**

A hash bucket is a notional receptacle, a set of which might be used to apportion data items for sorting or lookup purposes. Evaluate the default (1) in relation to your site needs.

**Name of your organization**

The value that you enter in the Name of Your Organization field will be displayed in the organization chart that is displayed on many of the Tivoli Identity Manager graphical user interface screens. This value is typically the more formal name of your company. For example, an organization name is IBM Corporation.

**Note:** You may enter either single-byte (ASCII) characters or double-byte character set characters in this field.

**Default Org Short Name**

The value that you enter in the Default Org Short Name field will be used internally in Sun ONE Directory Server to represent your organization. This value is typically an abbreviation of your company name. For example, a short name is ibmcorp.

**Note:** Enter only single-byte (ASCII) characters in the Default Org Short Name field, such as an identifier in English.

**Identity Manager DN Location**

The value such as dc=com that you enter in the Location field must match the suffix (for example, dc=com) that you created when you configured LDAP.

Additionally, the installation windows report the following LDAP Connection Pool Information fields for a pool of LDAP connections accessible by Tivoli Identity Manager Server. For more information, refer to the IBM Tivoli Identity Manager Configuration Guide.

Evaluate the following in relation to your site needs:

**Max. pool size**

Maximum number of connections the LDAP Connection Pool can have at any time

**Initial pool size**

Initial number of connections created for the LDAP Connection Pool
Increment count
Number of connections added to the LDAP Connection Pool every time a connection is requested once all connections are in use

**Tivoli Identity Manager Logon Information**
Note the following information for Tivoli Identity Manager:

**User ID**

The Tivoli Identity Manager user ID. The default after installation is itim manager. Use this user ID when you log on to Tivoli Identity Manager.

**Password**

Password for the Tivoli Identity Manager user ID specified as itim manager. The default password after installation is secret.

*Note:* It is important that you change this password and make a record of the new password immediately after you first log on.

---

**Installing the Tivoli Identity Manager Server**

Installing Tivoli Identity Manager requires installing the Tivoli Identity Manager Server and configuring various server properties to enable it to connect to the database and directory server. In a cluster configuration, an admin server and the managed servers must be installed individually.

Installing a Tivoli Identity Manager admin server loads Tivoli Identity Manager resources onto the WebLogic Administration Server of a WebLogic cluster. Tivoli Identity Manager resources include information such as directory server connection information, database information, and managed resources location information.

Installing a Tivoli Identity Manager managed server loads the Tivoli Identity Manager Application Server onto a managed server in the WebLogic cluster. The Tivoli Identity Manager Application Server uses the information on the admin server to connect to the various resources, however, the actual processing of requests is completed by the managed server.

The following flowchart describes the basic sequence of windows that install Tivoli Identity Manager in a clustered configuration.

*Note:* The admin server must be installed before any of the managed servers are installed in the cluster.
Figure 24. Clustered Tivoli Identity Manager Server Installation Overview
Installing the Admin Server

The following sections describe, in detail, the procedures to install the admin server for a clustered Tivoli Identity Manager Server.

Note: The admin server must be installed before any managed servers are installed.

Navigate Initial Welcome and Licensing Windows

A series of welcome and licensing windows start the installation process. To navigate the initial windows, do the following:

1. Log on to the computer where the Tivoli Identity Manager Server will be installed.

   Note: You must log on using an account with system administration privileges.

2. Obtain the Tivoli Identity Manager product installation image.

3. Open a command prompt window and change to your CD-ROM drive.

4. Run the following installation program:

   `instOS-WL.bin`

   where OS is the abbreviation for your system’s operating system.

   The abbreviations are: AIX for the AIX operating system; SOL for the Solaris operating system; HPUX for the HP-UX operating system.

   The Language Selection window opens.

![Language Selection window](image)

Figure 25. Language Selection window

5. Select the desired language in the language drop-down menu and click OK.

   The License Agreement window opens.
6. Read the license agreement and decide whether to accept its terms.
7. Select the I accept the terms of the License Agreement radio button if you agree to the terms and click Next.
   The Choose Installation Type window opens. Proceed with choosing an installation type.
Select the Installation Type and Directories
The next steps determine the type of Tivoli Identity Manager to install and the location of the WebLogic Server used by Tivoli Identity Manager.

1. Select the radio button for the type of installation you desire in the Choose Installation Type window and click Next.

   If you want to install a single-server version of Tivoli Identity Manager, select the Single Server radio button. If you want to install a clustered version of Tivoli Identity Manager, select the Cluster radio button.

   The Have you installed BEA WebLogic Server 7.0? window opens.

2. Click Yes if you have already installed the WebLogic Server.

   If you click No, you can continue with the installation but you will have to install WebLogic 7.0 before Tivoli Identity Manager will run. It is recommended that you exit the installation and install the WebLogic Server before installing Tivoli Identity Manager.

   The Where have you installed WebLogic Server 7.0? window opens.

3. Enter the BEA home directory and the WebLogic Server home directories in their respective fields and click Next.

   **Note:** In a clustered installation, the WebLogic Server home directory should be the same for each member of the cluster.

   See the following section to proceed with the installation process.

**Determine the Cluster’s Configuration**
This section describes the procedures to specify the type of server to install for the cluster and the cluster information.

The previous section ended with the Specify the Server Type window open.
1. Select the Admin Server radio button in the Specify the Server Type window and click Next.
   The Choose Install Folder window opens.

2. Accept the default installation directory (/itim45) or enter a different installation directory and click Next.
   The Specify the Tivoli Identity Manager Domain Information window opens.
3. Accept the default domain base directory (/usr/local/bea/weblogic700/user_projects) or enter a different directory location.
4. Enter the name of the domain to which the Tivoli Identity Manager Server will be added in the Domain Name field.
5. Enter the name of the Tivoli Identity Manager Server in the Server Name field and click Next.
   The Specify the Cluster Information window opens.
6. Enter the cluster’s name, multicast address, and multicast port number in the respective fields and click **Next**.

   See “Tivoli Identity Manager Information” on page 42 for more information about these values.

   Proceed to the following section to continue with the installation process.

**Specify the Encryption Key and Install the Tivoli Identity Manager Server**

The previous section ended with the Specify the Encryption Key window open.
1. Enter the encryption key and click Next.

   The encryption key is used to encrypt Tivoli Identity Manager passwords and other sensitive text. The default encryption key is sunshine. It is recommended that you change the encryption key.

   **Note:** The encryption key you input here must be the same as the one specified during the admin server installation.

   The Pre-Installation Summary window opens.
2. Review the information listed.
   If any of the information is incorrect, click Previous and correct the values. If there is not enough disk space, cancel the installation and ensure that the required disk space is available before installing Tivoli Identity Manager.

3. Click Install.
   A series of installation progress windows open during the interval that the installation requires. After the installation completes, you must configure the Tivoli Identity Manager Server.

4. Proceed to the following section to continue with the installation process.

**Initial Configuration of Tivoli Identity Manager Database**

After the Tivoli Identity Manager Server is installed, the Tivoli Identity Manager database must be configured. The installation program uses the database configuration tool to configure the database.

The previous section ended with the IBM Tivoli Identity Manager Database Configuration window open.
Note: If you are using Oracle for your database, you will need to copy the Oracle JDBC driver (in the file name classes12.zip) from the temporary local directory (where you saved the JDBC driver from the supplementary CD earlier) to the ITIM_HOME/lib directory.

1. Enter the database connection information in the appropriate fields of the IBM Tivoli Identity Manager Database Configuration window and click Test.
   If the test is successful, a message window opens confirming that the connection is successful.

2. Click OK.
   The IBM Tivoli Identity Manager Database Configuration window reappears with the Identity Manager User Information fields active.

3. Enter the Tivoli Identity Manager user ID and password in their respective fields and click Continue.
   The default values for these fields are listed in the information worksheet. A message window opens confirming that the database configuration is complete.

4. Click OK.
   The IBM Tivoli Identity Manager Directory Configuration window opens.

5. Proceed to configure the directory to continue with the installation process.

**Initial Configuration of the Directory for Tivoli Identity Manager**

The Tivoli Identity Manager directory server connection must be configured after installing the Tivoli Identity Manager Server. The following procedures describe how to configure the Tivoli Identity Manager Server to recognize the directory server.

The previous section ended with the IBM Tivoli Identity Manager Directory Configuration window open.
1. Enter the LDAP server information in the appropriate fields of the IBM Tivoli Identity Manager Directory Configuration window and click Test. If the test is successful, a message window opens confirming that the connection was successful.

2. Click OK.

The IBM Tivoli Identity Manager Directory Configuration window reappears with the Identity Manager Directory Information fields active.
3. Select the database used with Tivoli Identity Manager.

4. Accept the default number of hash buckets or enter a new value.
   Hash buckets can hold up to 1,000,000 entries.

5. Complete the remaining Identity Manager Directory Information fields and click **Continue**.
   See the information worksheet for more information about each field. A message window opens confirming that the directory server configuration was successful.

6. Click **OK**.
   The directory server configuration tool closes and the system configuration tool window opens.

**Initial Configuration of Tivoli Identity Manager**

The remaining windows provide an initial configuration of Tivoli Identity Manager. During this activity, you can change values you initially set for the database server and the directory server and modify some system default configuration values. Default values that must be modified are detailed in the procedures.

1. Verify that the information listed on the General tab is correct.
2. Click the **Directory** tab and verify that the information listed is correct.
   If any of the information is not correct, modify the information and click **Test** to verify that the connection information is correct.

3. Click the **Database** tab and verify that the information listed is correct.
   If the information is not correct, modify the information and click **Test** to verify that the connection information is correct.
4. Click the **Logging** tab and modify the level of logging as desired.

5. Click the **Mail** tab and verify that the Identity Manager Server URL is correct.

   **Note:** In a clustered configuration, the Identity Manager Server URL should be the URL of the proxy server, if one is used.
6. Change the Mail From address to the Tivoli Identity Manager system administrator e-mail address for your site.

   **Note:** You must change this address. The default address is a valid IBM e-mail address. If you do not change this address you will send spam to the e-mail address listed.

7. Enter the mail server name in the respective field.

8. Click the UI tab and modify the values as desired.

   Refer to the *IBM Tivoli Identity Manager Configuration Guide* for additional information about customizing the user interface.
9. Click the **Security** tab and modify the values as desired.

![Security Tab of the System Configuration Window](image)

**Figure 44. Security Tab of the System Configuration Window**

10. Click **OK** to finish configuring the Tivoli Identity Manager Server.
11. Proceed to the following section to continue with the installation process.

**Registering a Managed Server**

This section describes how to register a managed server with the Admin Server. Managed servers can be registered before Tivoli Identity Manager is installed on the system.

The previous section ended with the Register Managed Server window open.

![Register Managed Server Window](image)

**Figure 45. Register Managed Server Window**
1. Click Add in the Register Managed Server window. The Edit Server Info window opens.

![Edit Server Info Window](image)

*Figure 46. Edit Server Info Window*

2. Enter the managed server connection information into the appropriate fields and click Add.

   **Note:** The Listening Address can be an IP address or a hostname.

   The Edit Server Info window closes and the Register Managed Server window reappears with the managed server listed.

3. Repeat the previous procedures to add additional managed servers.

4. Click Save after all managed servers have been registered.

   The Install Complete window opens.

5. Click Done to finish the installation process.

---

**Installing a Managed Server**

The following sections describe, in detail, the steps to install a managed server for a clustered Tivoli Identity Manager Server. The managed server must be registered with the admin server before being installed. If the managed server has not been registered with the admin server, the managed server will not be recognized as a member of the cluster.

If the admin server has not been installed, see "Installing the Admin Server" on page 47. If the admin server has been installed but the managed server has not been registered with it, execute the registeredManagedServers.bin program in the ITIM_HOME/bin directory on the admin server and register the managed server before installing it.

The installation directory must be identical for all the managed servers in the cluster. Otherwise, later runtime difficulties will occur in certificate recognition or in HR feed activities on different cluster member computers.

The following procedures must be repeated for each managed server in the cluster.

**Note:** If you are running a managed server on the same computer as the admin server, it is unnecessary to run the installation for a managed server. The commands to start the managed server will automatically be created when you register the managed server with the admin server.

---

**Navigate Initial Welcome and Licensing Windows**

A series of welcome and licensing windows start the installation process. To navigate the initial windows, do the following:
1. Log on to the computer where the Tivoli Identity Manager Server will be installed.

   **Note:** You must log on using an account with system administration privileges.

2. Obtain the Tivoli Identity Manager product installation image.

3. Open a command prompt window and change to your CD-ROM drive.

4. Run the following installation program:
   ```
   inst0S-WL.bin
   ```
   where OS is the abbreviation for your system’s operating system.
   The abbreviations are: AIX for the AIX operating system; SOL for the Solaris operating system; HPUX for the HP-UX operating system.
   The Language Selection window opens.

![Language Selection window](image1)

   **Figure 47. Language Selection window**

5. Select the desired language in the language drop-down menu and click **OK**.
   The License Agreement window opens.

![License Agreement window](image2)

   **Figure 48. License Agreement Window**
6. Read the license agreement and decide whether to accept its terms.

7. Select the I accept the terms of the License Agreement radio button if you agree to the terms and click **Next**.

   The Choose Installation Type window opens. Proceed with choosing an installation type.

![Choose Installation Type Window](image)

**Figure 49. Choose Installation Type Window**

**Select the Installation Type and Directories**

The next steps determine the type of Tivoli Identity Manager to install and the location of the WebLogic Server used by Tivoli Identity Manager.

1. Select the radio button for the type of installation you desire in the Choose Installation Type window and click **Next**.

   If you want to install a single-server version of Tivoli Identity Manager, select the **Single Server** radio button. If you want to install a clustered version of Tivoli Identity Manager, select the **Cluster** radio button.

   The Have you installed BEA WebLogic Server 7.0? window opens.

2. Click **Yes** if you have already installed the WebLogic Server.

   If you click **No**, you can continue with the installation but you will have to install WebLogic 7.0 before Tivoli Identity Manager will run. It is recommended that you exit the installation and install the WebLogic Server before installing Tivoli Identity Manager.

   The Where have you installed WebLogic Server 7.0? window opens.
3. Enter the BEA home directory and the WebLogic Server home directories in their respective fields and click Next.

   **Note:** In a clustered installation, the WebLogic Server home directory should be the same for each member of the cluster.
   
   See the following section to proceed with the installation process.

**Determine the Cluster’s Configuration**

This section describes the procedures to specify the type of server to install for the cluster and the cluster information. The previous section ended with the Specify the Server Type window open.
1. Select the Managed Server(s) radio button in the Specify Server Type window and click Next.

The Choose Install Folder window opens.

**Note:** The installation directory must be identical for all the managed servers in a cluster. Otherwise, later runtime difficulties will occur in certificate recognition or in HR feed activities on different cluster member computers.
2. Accept the default Tivoli Identity Manager installation directory (/itim45) or enter a different installation directory and click Next. The Specify the Tivoli Identity Manager Domain Information window opens.

3. Accept the default domain base directory (/usr/local/bea/weblogic700/user_projects) or enter a different directory location and click Next.
The Specify the Admin Server Information window opens.

![Specify the Admin Server Information Window](image)

*Figure 54. Specify the Admin Server Information Window*

4. Verify that the admin server is running.
5. Modify the default admin server URL to match your admin server’s URL.
6. Accept the default WebLogic user password if you did not change the user password during the admin server install and click **Next**

If you changed the WebLogic user password when you installed the admin server, you must enter that same password during each managed server installation.

The Specify the LDAP Directory Server Information window opens. Proceed to the following section to continue with the installation process.
Specify Directory Server Connection Information

1. Enter the directory server information in the appropriate fields in the Specify the LDAP Directory Server Information window. These values must match the values entered during the admin server installation.

2. Click Next.
   The Specify the Encryption Key window opens.

Specify the Encryption Key and Install the Tivoli Identity Manager Server

The previous section ended with the Specify the Encryption Key window open.
1. Enter the encryption key and click Next.

The encryption key is used to encrypt Tivoli Identity Manager passwords and other sensitive text. The default encryption key is sunshine. It is recommended that you change the encryption key.

Note: The encryption key you input here must be the same as the one specified during the admin server installation.

The Pre-Installation Summary window opens.
2. Review the information listed. If any of the information is incorrect, click Previous and correct the values. If there is not enough disk space, cancel the installation and ensure that the required disk space is available before installing Tivoli Identity Manager.

3. Click Install. A series of installation progress windows open during the interval that the installation requires. After the installation completes, you must configure the Tivoli Identity Manager Server.

4. Proceed to the following section to continue with the installation process.

**Initial Configuration of a Managed Tivoli Identity Manager Server**

Configuring a managed server is very similar to configuring an admin server. The following procedures describe how to configure a managed server. Many of the values used to configure the admin server will need to be used for the managed server.

1. Verify that the information listed on the General tab is correct. If any of the information is not correct, modify the information and click Apply.
2. Click the Directory tab and verify that the information listed is correct.
   If the information is not correct, modify the information and click Test. If the test is successful, click Apply.

3. Click the Logging tab and modify the level of logging as desired.
   If the managed server is on a separate computer from the admin server, the logging level defined will only apply to the managed server.
   If you modify any value, click Apply.
4. Click the **Mail** tab and verify that the Identity Manager Server URL is correct.

   **Note:** In a clustered configuration, the Identity Manager Server URL should be the URL of the proxy server, if one is used.

5. Change the Mail From address to the Tivoli Identity Manager system administrator e-mail address for your site.
   This value should be the same address entered during configuration of the admin server.

   **Note:** You must change this address. The default address is a valid IBM e-mail address. If you do not change this address you will send spam to the e-mail address listed.
6. Enter the mail server name in the respective field and click **Apply**.
7. Click the **UI** tab and modify the values as desired.
   Refer to the *IBM Tivoli Identity Manager Configuration Guide* for additional information about customizing the user interface.

![UI Tab of the System Configuration Tool for Managed Servers](image)

> **Figure 62. UI Tab of the System Configuration Tool for Managed Servers**

   If you modified any value, click **Apply**.

8. Click the **Security** tab and modify the values as desired.
   If you modified any value, click **Apply**.

![Security Tab of the System Configuration Tool for Managed Servers](image)

> **Figure 63. Security Tab of the System Configuration Tool for Managed Servers**

9. Click **OK** to finish configuring the Tivoli Identity Manager Server.
   The Install Complete window opens.
10. Click **Done** to finish the installation process.

---

**Optionally Installing a Language Pack**

After installing Tivoli Identity Manager, if the default language is not English, optionally obtain and mount the language pack CD for the Tivoli Identity Manager Server. Use command line mode to install the language pack. For example, enter the following:

```java -jar itimlp_setup.jar```

The Tivoli Identity Manager language pack setup program will start. To complete the language pack installation, follow the instructions that appear in the setup program panels.

**Note:** To run the Tivoli Identity Manager language pack setup program, Java runtime environment 1.3.1 should be accessible from the command line.

---

**Starting and Stopping the Tivoli Identity Manager Server**

The Tivoli Identity Manager admin server is configured to start automatically after installation. However, the managed servers must be started after installation. This section describes how to start and stop an Tivoli Identity Manager Server.

On UNIX servers, Tivoli Identity Manager installed a script to start and stop the Tivoli Identity Manager Server in the `ITIM_HOME` directory. For the admin server, the script is named `itim.sh`. For managed servers, the script is named `server_name.sh` where `server_name` is the name of the managed server.

To start the Tivoli Identity Manager Server, use the following command:

```sh
itim.sh start
```

or

```sh
server_name.sh start
```

**Note:** Starting the Tivoli Identity Manager Server takes several minutes. Watch the `server_name.log` file for a running message. The `server_name` is the name of the server defined earlier during installation. The log file is located in `BEA_HOME/user_projects/itim/logs/` on the admin server and in `BEA_HOME/user_projects/itim/server_name/` on the managed servers.

To stop the Tivoli Identity Manager Server, use the following command:

```sh
itim.sh stop
```

or

```sh
server_name.sh stop
```

---

**Testing Tivoli Identity Manager Server Communication**

To test whether the database, the directory server, and the Tivoli Identity Manager Server are correctly configured and communicating with each other, do the following:

1. Start Tivoli Identity Manager Server and any prerequisite applications.
2. Log on to Tivoli Identity Manager.

   For example, at a browser window, type the following:
http://hostname/enrole

where hostname is the fully-qualified name or IP address of the computer on which Tivoli Identity Manager Server is running.

3. Enter the Tivoli Identity Manager administrator user ID (itim manager) and password.

4. Take the necessary steps to create a user (an ITIM user).

For more information, refer to online help or to the IBM Tivoli Identity Manager Policy and Organization Administration Guide.

Certificate Authority for Server-Agent Communication

Using the Tivoli Identity Manager system with a Tivoli Identity Manager Agent will require production certificates to ensure secure communication between the Tivoli Identity Manager Server and the Agent. The Certificate Authority that corresponds to the Tivoli Identity Manager Agent’s certificate must be located in the ITIM_HOME/ cert directory. Refer to the IBM Tivoli Identity Manager Configuration Guide and to a specific agent’s installation guide for more information.

Notes:

1. In a cluster configuration, the certificate must be installed in the same directory on each member in order for the agent to locate the certificate.

2. If the default language is not English, before installing the first Tivoli Identity Manager agent, optionally obtain and mount the language pack CD for the Tivoli Identity Manager agents. Use command line mode to install the language pack for the agents on the Tivoli Identity Manager Server:

   java -jar itimlp_agents_setup.jar

   The Tivoli Identity Manager language pack setup program will start. To complete the language pack installation, follow the instructions that appear in the setup program panels.

   Note: To run the Tivoli Identity Manager language pack setup program, Java runtime environment 1.3.1 should be accessible from the command line.

3. For recommendations on where to install the agent profile in a cluster configuration, refer to the agent installation guide for your specific agent.

Configuring the Proxy Server

After installing the Tivoli Identity Manager Server, you must configure your Web proxy server to recognize the clustered Tivoli Identity Manager Server, if you are using a Web proxy server. The Web proxy server acts as a load balancer for the cluster.

The following sections describe how to configure your Web proxy server for use with Tivoli Identity Manager Server. WebLogic can use the Microsoft Internet Information Services (IIS) HTTP Server or the Apache HTTP Server as a Web proxy server. Refer to the WebLogic user manual for the latest supported version of the IIS and Apache HTTP Servers.

IIS HTTP Server Configuration

The following procedures describe how to configure the IIS HTTP Server for use with the Tivoli Identity Manager Server. For detailed information on configuring the IIS HTTP Server, refer to the IIS HTTP Server documentation.

1. Log into the system where the Tivoli Identity Manager Server is installed.
2. Copy the iisproxy.dll from the WebLogic_Home/server/bin directory of your WebLogic Server into a directory that is accessible by the IIS HTTP Server.

3. Create a file called iisproxy.ini in the WebLogic_Home/server/bin directory that contains the following lines:

   # This file contains initialization name/value pairs
   # for the IIS/WebLogic plug-in.

   WebLogicCluster=IPAddress1:port, IPAddress2:port
   IPAddress1 and IPAddress2 should be the IP addresses and port numbers for the managed servers in the cluster. If you have more than two managed servers in the cluster, you must append the list with the additional server information.

4. Copy the iisproxy.ini file to the directory where the copy of the iisproxy.dll file is located.

5. Add the application extension mapping to the IIS HTTP Server using the IIS service manager.
   Refer to the Microsoft Internet Information Services documentation for detailed procedures.

6. Restart the IIS HTTP Server.

**Apache HTTP Server Configuration**

The following procedures describe how to configure the Apache HTTP Server for use with Tivoli Identity Manager. For detailed information on configuring the Apache HTTP Server, refer to the Apache HTTP Server documentation.

1. Log into the system where the Tivoli Identity Manager Server is installed.

2. Copy the mod_wl_20.so file from the
   WebLogic_Home/server/lib/operatingsystem directory of your WebLogic Server to the APACHE_HOME/modules directory.
   Replace operatingsystem with the name of your operating system.

3. Add the following lines to the APACHE_HOME/conf/httpd.conf file:

   LoadModule weblogic_module modules/mod_wl_20.so

   <Location /enrole>
   SetHandler weblogic-handler
   </Location>

   <IfModule mod_weblogic.c>
   WebLogicCluster IPAddress1:port, IPAddress2:port
   </IfModule>

   IPAddress1 and IPAddress2 should be the IP addresses and port numbers for the managed servers in the cluster. If you have more than two managed servers in the cluster, you must append the list with the additional server information.

4. Verify that the syntax of the APACHE_HOME/conf/httpd.conf file is correct using the following command:

   APACHE_HOME/bin/httpd configtest

5. Restart the WebLogic Server.

6. Restart the Apache HTTP Server.
Increasing the System Memory Usage

The Tivoli Identity Manager Server is configured to use the least amount of memory required for basic operation in a standard installation. By default, the Tivoli Identity Manager Server is configured to use a minimum and maximum of 256 megabytes (MB) of memory. These values can be modified to enable the system to perform at optimum speed.

In order to optimize the performance of the Tivoli Identity Manager Server, 75% of the total memory available (up to a maximum of 1024 MB) should be reserved for the Tivoli Identity Manager Server, assuming no other software is running on the system. For example, if there is 1 gigabyte (GB) of memory available on the system where the Tivoli Identity Manager Server is installed, the Tivoli Identity Manager Server should be configured to use 768 MB.

The following are detailed procedures on how to increase the memory usage for the Tivoli Identity Manager Server.

1. Log into the system where the Tivoli Identity Manager Server is installed.
2. Open the Tivoli Identity Manager Server startup script in a text editor.
   The script is located in the ITIM_HOME/bin directory. In a single-server installation, the script is named itim.sh. In a clustered installation, the script is named serverName.sh where serverName is the name of the managed server.
3. Find the following line in the script:
   MEM_ARGS=-XX:MaxPermSize=128m -Xms256m -Xmx256m
4. Change the -Xms and -Xmx settings to an appropriate value based on your hardware.
   The -Xms value is the minimum memory usage.
   The -Xmx value is the maximum memory usage.
   If Tivoli Identity Manager Server is the only application running on the machine, it is recommended that both the minimum and maximum memory usage parameters be set to 75% of the available system memory as long as they do not exceed 1024 MB, individually. BEA also recommends that these parameters be set to the same value.
5. Save the script.
6. Stop and restart the Tivoli Identity Manager service.
Appendix A. Installation Images as Compact Discs and Fix Packs

Tivoli Identity Manager is provided by the following:

- Fix packs for the platforms and prerequisite applications supported by Tivoli Identity Manager version 4.5.0. For more information on obtaining these fix packs, see "Obtaining 4.5.1 Fix Packs."
- CDs containing the previous Tivoli Identity Manager version 4.5.0 and prerequisite applications.

For more information on all supported platforms and their prerequisite applications, refer to the IBM Tivoli Identity Manager Release Notes.

Obtaining 4.5.1 Fix Packs

Obtain the Tivoli Identity Manager version 4.5.1 fix packs for the platforms supported by Tivoli Identity Manager version 4.5.0 at the following Web site:

http://www-1.ibm.com/support/dlsearch.wss?rs=644

For example, a fix pack file has a name similar to the following:

4.5.1-TIM-platform-WAS-0001.zip

where platform is a value such as AIX.

Do the following:

1. Access the IBM Online Software support site.
   a. Register and establish your personal IBM online ID at the following Web site:
      http://www.ibm.com/software/support/
   b. Click help for information on completing the users section of the Update Maintenance Agreements dialog.
   c. Provide your Customer number (assigned by an IBM Passport Advantage Software Maintenance Agreement) in the maintenance agreements area of the IBM Online registration.

Version 4.0 Compact Discs

Tivoli Identity Manager Server version 4.5.0 provides the following compact discs (CDs). If you do not have all listed CDs, contact IBM Support.

Language Packs CD

The following table itemizes the contents of the language pack CD.

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>language packs</td>
<td>itimlp_setup.jar, itimlp_agents_setup.jar</td>
</tr>
</tbody>
</table>
Base Code Solaris CD for Tivoli Identity Manager using WebSphere Application Server

The following table itemizes the contents of the base code Solaris CD for Tivoli Identity Manager using WebSphere Application Server:

Table 4. Contents of base code Solaris CD for Tivoli Identity Manager using WebSphere Application Server

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Identity Manager Version 4.5 for WebSphere Application Server</td>
<td>instSOL-WAS.bin</td>
</tr>
<tr>
<td>Documentation ReadMeFirst</td>
<td>Docs-ReadMeFirst.pdf</td>
</tr>
</tbody>
</table>

Base Code Solaris CD for Tivoli Identity Manager for non-IBM Application Servers

The following table itemizes the contents of the base code Solaris CD for Tivoli Identity Manager using non-IBM Application Servers (WebLogic):

Table 5. Contents of base code Solaris CD for Tivoli Identity Manager using WebLogic

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Identity Manager Version 4.5 for WebLogic</td>
<td>instSOL-WL.bin</td>
</tr>
<tr>
<td>Documentation ReadMeFirst</td>
<td>Docs-ReadMeFirst.pdf</td>
</tr>
</tbody>
</table>

Supplemental Solaris CD 1

The following table itemizes the contents of supplemental Solaris CD 1:

Table 6. Contents of Supplemental Solaris CD 1

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebSphere Application Server base Version 5.0 Fix Pack 2</td>
<td>was50_fp2_solaris.zip</td>
</tr>
<tr>
<td>WebSphere Application Server Network Deployment Version 5.0 Fix Pack 2</td>
<td>was50_nd_fp2_solaris.zip</td>
</tr>
<tr>
<td>WebSphere Application Server base Version 5.0.2 interim fix (APAR PQ75794)</td>
<td>PQ75794.zip</td>
</tr>
<tr>
<td>WebSphere Application Server base and WebSphere Application Server Network Deployment Version 5.0.2 interim fix (APAR SOV62778)</td>
<td>ibmorb.jar</td>
</tr>
<tr>
<td>WebSphere Application Server JSP Compile interim fix (APAR PQ77263)</td>
<td>PQ77263.zip</td>
</tr>
</tbody>
</table>

Supplemental Solaris CD 2

The following table itemizes the contents of supplemental Solaris CD 2:

Table 7. Contents of Supplemental Solaris CD 2

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Directory Server Version 5.1</td>
<td>ids510-solaris-ismp-us.tar</td>
</tr>
<tr>
<td>IBM Directory Server Version 5.1 Fix Pack 1</td>
<td>FP5105-01.tar.Z</td>
</tr>
</tbody>
</table>
Table 7. Contents of Supplemental Solaris CD 2 (continued)

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
</table>
| IBM Directory Server referential integrity plug-in | DelRef/aix/libdelref.a  
DelRef/hpux/libdelref.sl  
DelRef/nt/libdelref.dll  
DelRef/sun/libdelref.so                |
| Tivoli Identity Manager Version 4.5 configuration file | DelRef/timdelref.conf |

Supplemental Solaris CD 3

The following table itemizes the contents of supplemental Solaris CD 3:

Table 8. Contents of Supplemental Solaris CD 3

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM DB2 Version 8.1 Fix Pack 2 (32 and 64 Bit)</td>
<td>Sol-FP2_U486567.tar.Z</td>
</tr>
</tbody>
</table>

Supplemental Solaris CD 4

The following table itemizes the contents of supplemental Solaris CD 4:

Table 9. Contents of Supplemental Solaris CD 4

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Type 4 JDBC driver</td>
<td>classes12.zip</td>
</tr>
<tr>
<td>Oracle Type 4 JDBC driver license file</td>
<td>LI_en</td>
</tr>
</tbody>
</table>

Base Code AIX CD for Tivoli Identity Manager using WebSphere Application Server

The following table itemizes the contents of the base code AIX CD for Tivoli Identity Manager using WebSphere Application Server:

Table 10. Contents of base code AIX CD for Tivoli Identity Manager using WebSphere Application Server

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Identity Manager Version 4.5 using WebSphere Application Server</td>
<td>instAIX-WAS.bin</td>
</tr>
<tr>
<td>Documentation ReadMeFirst</td>
<td>Docs-ReadMeFirst.pdf</td>
</tr>
</tbody>
</table>

Base Code AIX CD for Tivoli Identity Manager for non-IBM Application Servers

The following table itemizes the contents of the base code AIX CD for Tivoli Identity Manager using non-IBM application servers (WebLogic):

Table 11. Contents of base code AIX CD for Tivoli Identity Manager using WebLogic

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Identity Manager Version 4.5 for WebLogic</td>
<td>instAIX-WL.bin</td>
</tr>
<tr>
<td>Documentation ReadMeFirst</td>
<td>Docs-ReadMeFirst.pdf</td>
</tr>
</tbody>
</table>
Supplemental AIX CD 1

Note: Because of size constraints, the Fix Pack 2 for IBM DB2 on AIX is not provided on a supplemental CD. To obtain Fix Pack 2 for IBM DB2 on AIX, access the following FTP site:


or access the following Web site:

http://www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/v8fphist.d2w/report#AIX5

The following table itemizes the contents of supplemental AIX CD 1:

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebSphere Application Server base Version 5.0 Fix Pack 2</td>
<td>was50_fp2_aix.zip</td>
</tr>
<tr>
<td>WebSphere Application Server Network Deployment Version 5.0 Fix Pack 2</td>
<td>was50_nd_fp2_aix.zip</td>
</tr>
<tr>
<td>WebSphere Application Server base Version 5.0.2 interim fix (APAR PQ75794)</td>
<td>PQ75794.zip</td>
</tr>
<tr>
<td>WebSphere Application Server base and WebSphere Application Server Network Deployment Version 5.0.2 interim fix (APAR SOV62778)</td>
<td>ibmorb.jar</td>
</tr>
<tr>
<td>WebSphere Application Server JSP Compile interim fix (APAR PQ77263)</td>
<td>PQ77263.zip</td>
</tr>
</tbody>
</table>

Supplemental AIX CD 2

The following table itemizes the contents of supplemental AIX CD 2:

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Directory Server Version 5.1</td>
<td>ids510-aix-ismp-us.tar</td>
</tr>
<tr>
<td>IBM Directory Server Version 5.1 Fix Pack 1</td>
<td>FP510A-01.tar</td>
</tr>
<tr>
<td>IBM Directory Server referential integrity plug-in</td>
<td>DelRef/aix/libdelref.a</td>
</tr>
<tr>
<td></td>
<td>DelRef/hpux/libdelref.sl</td>
</tr>
<tr>
<td></td>
<td>DelRef/nt/libdelref.dll</td>
</tr>
<tr>
<td></td>
<td>DelRef/sun/libdelref.so</td>
</tr>
<tr>
<td>Tivoli Identity Manager Version 4.5 configuration file</td>
<td>DelRef/timdelref.conf</td>
</tr>
</tbody>
</table>

Supplemental AIX CD 3

The following table itemizes the contents of supplemental AIX CD 3:

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Type 4 JDBC driver</td>
<td>classes12.zip</td>
</tr>
<tr>
<td>Oracle Type 4 JDBC driver license file</td>
<td>LI_en</td>
</tr>
</tbody>
</table>
Base Code HP-UX CD for Tivoli Identity Manager for non-IBM Application Servers

The following table itemizes the contents of the base code HP-UX CD for Tivoli Identity Manager for non-IBM application servers (WebLogic):

Table 15. Contents of base code HP-UX CD for Tivoli Identity Manager using WebLogic

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Identity Manager Version 4.5 using WebLogic</td>
<td>instHPUX-WL.bin</td>
</tr>
<tr>
<td>Documentation ReadMeFirst</td>
<td>Docs-ReadMeFirst.pdf</td>
</tr>
</tbody>
</table>

Base Code Windows 2000 CD for Tivoli Identity Manager using WebSphere Application Server

The following table itemizes the contents of the base code Windows 2000 CD for Tivoli Identity Manager using WebSphere Application Server:

Table 16. Contents of base code Windows 2000 CD for Tivoli Identity Manager using WebSphere Application Server

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Identity Manager Version 4.5 using WebSphere Application Server</td>
<td>instW2K-WAS.exe</td>
</tr>
<tr>
<td>Documentation ReadMeFirst</td>
<td>Docs-ReadMeFirst.pdf</td>
</tr>
</tbody>
</table>

Base Code Windows 2000 CD for Tivoli Identity Manager for non-IBM Application Servers

The following table itemizes the contents of the base code Windows 2000 CD for Tivoli Identity Manager for non-IBM application servers (WebLogic):

Table 17. Contents of base code Windows 2000 CD for Tivoli Identity Manager using WebLogic

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Identity Manager Version 4.5 for WebLogic</td>
<td>instW2K-WL.exe</td>
</tr>
<tr>
<td>Documentation ReadMeFirst</td>
<td>Docs-ReadMeFirst.pdf</td>
</tr>
</tbody>
</table>

Supplemental Windows 2000 CD 1

The following table itemizes the contents of supplemental Windows 2000 CD 1:

Table 18. Contents of supplemental Windows 2000 CD 1

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebSphere Application Server base Version 5.0 Fix Pack 2</td>
<td>was50_fp2_win.zip</td>
</tr>
<tr>
<td>WebSphere Application Server Network Deployment Version 5.0 Fix Pack 2</td>
<td>was50_nd_fp2_win.zip</td>
</tr>
<tr>
<td>WebSphere Application Server base Version 5.0.2 interim fix (APAR PQ75794)</td>
<td>PQ75794.zip</td>
</tr>
</tbody>
</table>
Table 18. Contents of supplemental Windows 2000 CD 1 (continued)

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebSphere Application Server base and</td>
<td>ibmorb.jar</td>
</tr>
<tr>
<td>WebSphere Application Server Network Deployment Version 5.0.2 interim fix (APAR SOV62778)</td>
<td></td>
</tr>
<tr>
<td>WebSphere Application Server JSP Compile</td>
<td>PQ77263.zip</td>
</tr>
<tr>
<td>interim fix (APAR PQ77263)</td>
<td></td>
</tr>
</tbody>
</table>

Supplemental Windows 2000 CD 2

The following table itemizes the contents of supplemental Windows 2000 CD 2:

Table 19. Contents of supplemental Windows 2000 CD 2

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Directory Server Version 5.1</td>
<td>ids510-windows-us.zip</td>
</tr>
<tr>
<td>IBM Directory Server Version 5.1 Fix Pack 1</td>
<td>FP510W-01.zip</td>
</tr>
<tr>
<td>IBM Directory Server referential integrity plug-in</td>
<td></td>
</tr>
<tr>
<td>DelRef\aix\libdelref.a</td>
<td></td>
</tr>
<tr>
<td>DelRef\hpux\libdelref.sl</td>
<td></td>
</tr>
<tr>
<td>DelRef\nt\libdelref.dll</td>
<td></td>
</tr>
<tr>
<td>DelRef\sun\libdelref.so</td>
<td></td>
</tr>
<tr>
<td>Tivoli Identity Manager Version 4.5 configuration file</td>
<td>DelRef\timdelref.conf</td>
</tr>
</tbody>
</table>

Supplemental Windows 2000 CD 3

The following table itemizes the contents of supplemental Windows 2000 CD 3:

Table 20. Contents of supplemental Windows 2000 CD 3

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM DB2 Version 8.1 Fix Pack 2</td>
<td>W2K-FP2.zip</td>
</tr>
</tbody>
</table>

Supplemental Windows 2000 CD 4

The following table itemizes the contents of supplemental Windows 2000 CD 4:

Table 21. Contents of supplemental Windows 2000 CD 4

<table>
<thead>
<tr>
<th>Product</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Type 4 JDBC driver</td>
<td>classes12.zip</td>
</tr>
<tr>
<td>Oracle Type 4 JDBC driver license file</td>
<td>LI_en</td>
</tr>
</tbody>
</table>
Appendix B. Upgrading from Tivoli Identity Manager 4.3 to Version 4.5 using WebLogic, and then to Version 4.5.1

This section describes upgrading previous data and schema from Tivoli Identity Manager version 4.3 using WebLogic to Tivoli Identity Manager version 4.5 using WebLogic. After completing the upgrade from version 4.3 to version 4.5, use the Tivoli Identity Manager version 4.5.1 installation image to upgrade version 4.5 to version 4.5.1.

**Note:** After upgrading, the Tivoli Identity Manager Server will continue to use the existing directory server and database.

The directory structures of the previous and current release of Tivoli Identity Manager are different. At version 4.3, the WebLogic server binaries are installed as part of `ENROLE_HOME`, and the application domain `enrole` is created within the WebLogic server configuration.

At version 4.5 (and 4.5.1), the application domain is created in `BEA_HOME` under `user_projects`, in the domain directory that includes the server and cluster configuration files and application log files. The following figure illustrates the differences:

```
4.3 Directory Structure

```

```
ENROLE_HOME
  └── bin
  └── cert
  └── config
  └── data
  └── doc
  └── enRoleUninstallerData
  └── extensions
  └── lib
  └── weblogic
    └── bin
    └── config
        └── enrol
            └── applications
                └── logs
        └── ext
        └── Lib
        └── Sample
        └── uninstaller
```

```
4.5 Directory Structure

```

```
ITIM_HOME
  └── bin
  └── cert
  └── config
  └── data
  └── doc
  └── extensions
      └──itimUninstallerData
  └── lib
  └── BEA_HOME
      └── user_projects
          └──itim
              └── applications
                  └── logs
              └── userConfigs
```

*Figure 64. Differences in version 4.3 and version 4.5/4.5.1 directory structures*
Before Upgrading

Before upgrading from version 4.3 to version 4.5, do the following:

1. Back up the directory server.
   
   On the iPlanet Directory Server, use the iPlanet console to perform the backup. During upgrade of the directory server, entries within the Tivoli Identity Manager sub-tree are scanned for the string "enrole" (case-insensitive). If an attribute’s value contains the string "enrole", that string is changed to "itim". This string replacement is done for all attributes except those listed in the ITIM_HOME/data/enRoleUnchangedAttributes.properties file. Before beginning the upgrade process, export the contents of the Tivoli Identity Manager 4.3 LDAP sub-tree to an LDIF file. Search the LDIF file for the string "enrole". If you find attributes that should not be changed during upgrade, do the following:
   
   a. Select No for LDAP Directory Upgrade during the Tivoli Identity Manager 4.5 installation.
   
   b. Edit the ITIM_HOME/data/enRoleUnchangedAttributes.properties file to add the attribute names.
   
   c. Invoke the LDAP Directory Upgrade manually.

2. Back up the database.
   
   On the database server, use the administrative console to perform a database backup.

3. Back up the existing Tivoli Identity Manager directory for each server in the cluster.
   
   This allows you to save any customizations so that you can re-implement them after the upgrade. You can use a tar or a zip utility to back up the information.

4. Before upgrading, ensure that the Tivoli Identity Manager GUI pending queue is clear and that all recurring scheduled events such as reconciliations are deleted. Workflow preservation is not supported when upgrading from Tivoli Identity Manager version 4.3 to Tivoli Identity Manager version 4.5. Prior to an upgrade, not ensuring the workflow engine is idle may result in exceptions being thrown when Tivoli Identity Manager attempts to read recurring or pending events that were created in a previous installation.
   
   One quick way to check whether the workflow engine is idle is to check the number of messages in the workflow queues (including workflow and workflow pending). Using the Weblogic Admin Console, do the following:
   
   a. Start the Admin Console.
   
   b. Open your domain in the tree.
   
   c. Click Services -> JMS -> Servers -> JMServer in the domain tree.
   
   d. Click the Monitoring tab on the right window.
   
   e. Click the link Monitor all Active JMS Destinations.
   
   f. Check Attribute Messages. The value of Messages must be 0 for all the listed queues.

5. Stop the Tivoli Identity Manager Server, or in the cluster, stop all the servers. See “Starting and Stopping the Tivoli Identity Manager Server” on page 75 for detailed information about stopping the cluster members.

6. Verify that the directory server and database are running.

7. Ensure the database server is up and running.
If you are using Oracle as the Tivoli Identity Manager database, login to SQLPlus using an account which can grant privileges to the user ‘enrole’.

Typically, the Oracle user ‘system’ can grant these privileges.

For example, log on with the following:

```
sqlplus system/password@itim_db_instance
```

Grant permission to user ‘enrole’ to ‘Create any procedure’. Enter the following command:

```
SQL> GRANT CREATE ANY PROCEDURE to enrole;
```

Quit the session. Enter the following command:

```
SQL> quit;
```

8. Install WebLogic Server version 7.0.

Notes:

1. After the upgrade, previous audit and log data may not be relevant to the new data.

2. Upgrading the Tivoli Identity Manager Server removes any customization previously implemented.

---

**Upgrading from Single Server Version 4.3 to Single Server Version 4.5**

The following procedures describe how to upgrade a single server installation of Tivoli Identity Manager version 4.3 to a single server installation of Tivoli Identity Manager version 4.5. If you have a clustered installation of Tivoli Identity Manager version 4.3 and want to upgrade it to Tivoli Identity Manager version 4.5, see “Upgrading from Cluster Version 4.3 to Cluster Version 4.5” on page 93.

Be sure to complete the procedures in “Before Upgrading” on page 86 before upgrading Tivoli Identity Manager. Backing up the information is the only way to save any customizations.

---

**Prepare to Upgrade the Server**

This section describes the initial process to upgrade the Tivoli Identity Manager Server.

1. Log on to the Tivoli Identity Manager Server to be upgraded.

   You must log on using an account with system administrator privileges.

2. Install BEA WebLogic 7.0 using the typical installation option.

3. Obtain the Tivoli Identity Manager product installation image.

4. Open a command prompt window.

5. Type the following command:

   ```
   inst0S-WL.bin
   ```

   where OS is the abbreviation for your system’s operating system. The abbreviations are: AIX for the AIX operating system; Solaris for the Solaris operating system; HP-UX for the HP-UX operating system.

   The Language Selection window opens.

6. Select the language to use during installation and click OK.

   The License Agreement window opens.

7. Read the license agreement and decide whether to accept its terms.

8. Select the I accept the terms of the License Agreement radio button if you agree to the terms and click Next.
The Choose the Installation Type window opens. Proceed with the following section to continue with the upgrade.

**Select the Installation Type and Directories**

The next steps determine the type of Tivoli Identity Manager to install and the location of the WebLogic Server used by Tivoli Identity Manager.

1. Select the radio button for the type of installation you desire in the Choose Installation Type window and click **Next**.
   
   If you want to install a single-server version of Tivoli Identity Manager, select the **Single Server** radio button. If you want to install a clustered version of Tivoli Identity Manager, select the **Cluster** radio button.
   
   The Have you installed BEA WebLogic Server 7.0? window opens.

2. Click **Yes** if you have already installed the WebLogic Server.
   
   If you click **No**, you can continue with the installation but you will have to install WebLogic 7.0 before Tivoli Identity Manager will run. It is recommended that you exit the installation and install the WebLogic Server before installing Tivoli Identity Manager.
   
   The Where have you installed WebLogic Server 7.0? window opens.

   ![Figure 65. Where have you installed WebLogic Server 7.0? Window](image)

3. Enter the BEA home directory and the WebLogic Server home directories in their respective fields and click **Next**.

   **Note:** In a clustered installation, the WebLogic Server home directory should be the same for each member of the cluster.

   See the following section to proceed with the installation process.

**Define the Installation Location**

The procedures in this section identify the location of the existing Tivoli Identity Manager installation and upgrades it.
The previous section ended with the Choose Install Folder window open.

![Choose Install Folder Window](image)

**Figure 66. Choose the Install Folder Window**

1. Enter the location where the existing Tivoli Identity Manager Server is installed and click **Next**.

   **Note:** If you choose a different location, the installation program will not detect the existing installation and will install a new Tivoli Identity Manager Server.

   The Do you want to upgrade? window opens.

2. Click **Yes** to upgrade the Tivoli Identity Manager Server.

   The Do you want to upgrade the LDAP Directory during installation? window opens.

3. Click **Yes**. This will initiate an LDAP directory upgrade during installation.

   **Note:** You can choose to upgrade the LDAP directory after the installation by selecting **No**. After the installation, invoke the `ldapUpgrade` utility located in the `bin` directory.

   The Specify the Tivoli Identity Manager Domain Information window opens.
4. Accept the default domain base directory
   (/usr/local/bea/weblogic700/user_projects) or enter a new value.
5. Enter the name of the domain on which the Tivoli Identity Manager will run
   and the name of the server and click Next.
   In the previous release, the default domain name was enrol. In the current
   release, the default domain name isitim.
   Proceed to the following section to continue with the upgrade process.

**Upgrade the Tivoli Identity Manager Server Schemas**

The following procedures describe how to upgrade the schemas associated with
Tivoli Identity Manager.

The previous section ended with the Pre-Installation Summary window open.
1. Click **Install** in the Pre-Installation Summary window.

   The Installing Tivoli Identity Manager window opens and a message line appears in the window describing the current installation process. After the database schema is upgrade, a message window opens confirming that the database schema upgrade is complete.

2. Click **OK**.

   The directory server schema is upgraded and a message window opens confirming that the directory schema upgrade is complete.

3. Click **OK**.

   The upgrade process completes and the System Configuration window opens. The fields on the tabs are populated with values from the previous installation of Tivoli Identity Manager.

4. Confirm that the values on the tabs are correct and click **OK**.

   Proceed to the following section to continue with the upgrade process.

**Complete the Upgrade Process**

The previous section ended with the Install Complete window open. Complete the upgrade process by clicking **Done**.

**Updating Certificate Information**

Upgrading from Tivoli Identity Manager version 4.3 to Tivoli Identity Manager version 4.5 does not preserve the SSL certificate setting in the config.xml file. You will need to manual update the SSL certificate settings through the WebLogic admin console.

1. Start the WebLogic server if not started yet.
2. Open the WebLogic admin console. At a browser window, type the following URL:

   http://hostname/console

---

Appendix B. Upgrading from Tivoli Identity Manager 4.3 to Version 4.5 using WebLogic, and then to Version 4.5.1 91
where the hostname is the host name or IP address of the admin server.

3. Click your domain name in the tree.
4. Click Servers under your domain name.
5. Click the name of the server for which to update the SSL certificate settings.
6. Click the Connections tab in the right pane.
7. Click the SSL tab under the Connections tab.
8. Modify the values to match your system’s configuration.
9. Click Apply.
10. Repeat the previous procedures for all members in your cluster, if you have a clustered configuration.

Re-Implement Customizations
Upgrading the Tivoli Identity Manager Server removes any customizations made to the server. Retrieve the customized files from the backup copy of the Tivoli Identity Manager directories and implement the customizations in the new, upgraded versions of the files.

Common items that are customized are the logo, LDAP schema, the authentication mechanism, and Java security.

Updating Custom Logos
If you had previously customized the logo in the Tivoli Identity Manager graphical user interface (GUI), you will need to move the graphic file to the new location.

The previous location was:
../enrole/weblogic/config/enrole/applications/enrole/images

where ../enrole was the Tivoli Identity Manager home directory.

The graphic must be placed in the
BEA_HOME/user_projects/itim/applications/enrole/images directory after Tivoli Identity Manager is upgraded.

Verifying Logging Settings
After upgrading the Tivoli Identity Manager Server, previous logging settings are overwritten. If you did not configure the logging settings during installation and accepted the defaults, you will need to update your logging settings after the upgrade is complete.

To update your logging settings, use the System Configuration Tool. Refer to the IBM Tivoli Identity Manager Configuration Guide for detailed information on using the System Configuration Tool and configuring the logging settings.

Starting and Stopping the Tivoli Identity Manager Server
After the Tivoli Identity Manager Server is installed you must start the server. This section describes how to start and stop the Tivoli Identity Manager Server.

On UNIX servers, Tivoli Identity Manager installed a script to start and stop the Tivoli Identity Manager Server in the ITIM_HOME directory.

To start the Tivoli Identity Manager Server, use the following command:

sh itim.sh start
Note: Starting the Tivoli Identity Manager Server takes several minutes. Watch the BEA_HOME/user_projects/itim/logs/server_name.log file for a running message. The server_name is the name of the server defined earlier during installation.

To stop the Tivoli Identity Manager Server, use the following command:

    sh itim.sh stop

Testing Tivoli Identity Manager Server Communication

To test whether the database, the directory server, and the Tivoli Identity Manager Server are correctly configured and communicating with each other, do the following:

1. Start Tivoli Identity Manager Server and any prerequisite applications.
2. Log on to Tivoli Identity Manager.
   For example, at a browser window, type the following:
   
   http://hostname/enrole

   where hostname is the fully-qualified name or IP address of the computer on which Tivoli Identity Manager Server is running.
3. Enter the Tivoli Identity Manager administrator user ID (itim manager) and password.
4. Take the necessary steps to create a user (an ITIM user).
   For more information, refer to online help or to the IBM Tivoli Identity Manager Policy and Organization Administration Guide.

Upgrading from Cluster Version 4.3 to Cluster Version 4.5

The following procedures describe how to upgrade a clustered installation of Tivoli Identity Manager version 4.3 to a clustered installation of Tivoli Identity Manager version 4.5. If you have a single server installation of Tivoli Identity Manager version 4.3 and want to upgrade to Tivoli Identity Manager version 4.5, see “Upgrading from Single Server Version 4.3 to Single Server Version 4.5” on page 87.

Be sure to complete the procedures in “Before Upgrading” on page 86 before upgrading Tivoli Identity Manager. Backing up the information is the only way to save any customizations.

To upgrade version 4.3 to version 4.5, do the following:

1. “Upgrade the Admin Server”
2. “Upgrade the Managed Servers” on page 99
3. “Re-implement Customizations” on page 104

Upgrade the Admin Server

On the computer on which the administration server is installed, do the following:

Prepare to Upgrade the Server

This section describes the initial process to upgrade the Tivoli Identity Manager Server.

1. Log on to the Tivoli Identity Manager Server to be upgraded.
   You must log on using an account with system administrator privileges.
2. Install BEA WebLogic 7.0 using the typical installation option.
3. Obtain the Tivoli Identity Manager product installation image.

4. Open a command prompt window.

5. Type the following command:
   
   inst05-WL.bin

   where OS is the abbreviation for your system’s operating system. The abbreviations are: AIX for the AIX operating system; SOL for the Solaris operating system; HPUX for the HP-UX operating system.

   The Language Selection window opens.

6. Select the language to use during installation and click OK.
   
   The License Agreement window opens.

7. Read the license agreement and decide whether to accept its terms.

8. Select the I accept the terms of the License Agreement radio button if you agree to the terms and click Next.
   
   The Choose the Installation Type window opens. Proceed with the following section to continue with the upgrade.

**Select the Installation Type and Directories**

The next steps determine the type of Tivoli Identity Manager to install and the location of the WebLogic Server used by Tivoli Identity Manager.

1. Select the radio button for the type of installation you desire in the Choose Installation Type window and click Next.
   
   If you want to install a single-server version of Tivoli Identity Manager, select the Single Server radio button. If you want to install a clustered version of Tivoli Identity Manager, select the Cluster radio button.
   
   The Have you installed BEA WebLogic Server 7.0? window opens.

2. Click Yes if you have already installed the WebLogic Server.
   
   If you click No, you can continue with the installation but you will have to install WebLogic 7.0 before Tivoli Identity Manager will run. It is recommended that you exit the installation and install the WebLogic Server before installing Tivoli Identity Manager.
   
   The Where have you installed WebLogic Server 7.0? window opens.
3. Enter the BEA home directory and the WebLogic Server home directories in their respective fields and click Next.

   **Note:** In a clustered installation, the WebLogic Server home directory should be the same for each member of the cluster. See the following section to proceed with the installation process.

**Define the Installation Location**

The procedures in this section identify the location of the existing Tivoli Identity Manager installation and upgrades it.

The previous section ended with the Specify the Server Type window open.
1. Select the Admin Server radio button in the Specify the Server Type window and click Next.
   The Choose Install Folder window opens.

2. Enter the location where the existing Tivoli Identity Manager Server is installed and click Next.
Note: If you choose a different location, the installation program will not detect the existing installation and will install a new Tivoli Identity Manager Server.

The Do you want to upgrade? window opens.

3. Click Yes to upgrade the Tivoli Identity Manager Server.

The Do you want to upgrade the LDAP Directory during installation? window opens.

4. Click Yes. This will initiate an LDAP directory upgrade during installation.

Note: You can choose to upgrade the LDAP directory after the installation by selecting No. After the installation, invoke the ldapUpgrade utility located in the bin directory.

The Specify the Tivoli Identity Manager Domain Information window opens.

![Specify the Tivoli Identity Manager Domain Information Window](image)

5. Accept the default domain base directory (/usr/local/bea/weblogic700/user_projects) or enter a new value.

6. Enter the name of the domain on which the Tivoli Identity Manager will run and the name of the server and click Next.

   In the previous release, the default domain name was enrole. In the current release, the default domain name isitim.

   Proceed to the following section to continue with the upgrade process.

**Upgrade the Tivoli Identity Manager Server Schemas**

The following procedures describe how to upgrade the schemas associated with Tivoli Identity Manager.

The previous section ended with the Pre-Installation Summary window open.
1. Click **Install** in the Pre-Installation Summary window.
   The Installing Tivoli Identity Manager window opens and a message line appears in the window describing the current installation process. After the database schema is upgraded, a message window opens confirming that the database schema upgrade is complete.

2. Click **OK**.
   The directory server schema is upgraded and a message window opens confirming that the directory schema upgrade is complete.

3. Click **OK**.
   The upgrade process completes and the System Configuration window opens. The fields on the tabs are populated with values from the previous installation of Tivoli Identity Manager.

4. Confirm that the values on the tabs are correct and click **OK**.
   Proceed to the following section to continue with the upgrade process.

**Update the Managed Server Information**

After the Tivoli Identity Manager Server and the schemas are upgraded, you must verify that the managed servers are correctly identified and registered with the admin server. The following procedures describe how to verify that the managed server information is correct.

The previous section ended with the Register Managed Server window open.
1. Verify that the connection information for each of the managed servers is correct.
   
   If any of the information is not correct, modify the information by clicking **Edit** and change the information as needed.

2. Delete any server that will no longer be in the cluster by selecting the server name and clicking **Delete**.

3. Click **Save** to save the information for all managed servers.
   
   The Install Complete window opens.

4. Click **Done** to exit the installation program.

---

**Register Managed Servers window**

1. Verify that the connection information for each of the managed servers is correct.
   
   If any of the information is not correct, modify the information by clicking **Edit** and change the information as needed.

2. Delete any server that will no longer be in the cluster by selecting the server name and clicking **Delete**.

3. Click **Save** to save the information for all managed servers.
   
   The Install Complete window opens.

4. Click **Done** to exit the installation program.

---

**Upgrade the Managed Servers**

The following sections describe how to upgrade a managed server.

**Prepare to Upgrade the Server**

This section describes the initial process to upgrade the Tivoli Identity Manager Server.

1. Log on to the Tivoli Identity Manager Server to be upgraded.
   
   You must log on using an account with system administrator privileges.

2. Install BEA WebLogic 7.0 using the typical installation option.

3. Obtain the Tivoli Identity Manager product installation image.

4. Open a command prompt window.

5. Type the following command:

    ```
    inst0S-WL.bin
    ```

   where OS is the abbreviation for your system’s operating system. The abbreviations are: AIX for the AIX operating system; SOL for the Solaris operating system; HPUX for the HP-UX operating system.

   The Language Selection window opens.

6. Select the language to use during installation and click **OK**.

   The License Agreement window opens.
7. Read the license agreement and decide whether to accept its terms.

8. Select the I accept the terms of the License Agreement radio button if you agree to the terms and click Next.

   The Choose the Installation Type window opens. Proceed with the following section to continue with the upgrade.

Select the Installation Type and Directories

The next steps determine the type of Tivoli Identity Manager to install and the location of the WebLogic Server used by Tivoli Identity Manager.

1. Select the radio button for the type of installation you desire in the Choose Installation Type window and click Next.
   If you want to install a single-server version of Tivoli Identity Manager, select the Single Server radio button. If you want to install a clustered version of Tivoli Identity Manager, select the Cluster radio button.
   The Have you installed BEA WebLogic Server 7.0? window opens.

2. Click Yes if you have already installed the WebLogic Server.
   If you click No, you can continue with the installation but you will have to install WebLogic 7.0 before Tivoli Identity Manager will run. It is recommended that you exit the installation and install the WebLogic Server before installing Tivoli Identity Manager.

   The Where have you installed WebLogic Server 7.0? window opens.

![Figure 75. Where have you installed WebLogic Server 7.0? Window](image)

3. Enter the BEA home directory and the WebLogic Server home directories in their respective fields and click Next.

   **Note:** In a clustered installation, the WebLogic Server home directory should be the same for each member of the cluster.

   See the following section to proceed with the installation process.
Define the Installation Location and Complete the Upgrade Process

The procedures in this section identify the location of the existing Tivoli Identity Manager installation and upgrades it.

The previous section ended with the Specify the Server Type window open.

![Specify the Server Type Window](image)

Figure 76. Specify the Server Type Window

1. Select the Managed Server(s) radio button in the Specify the Server Type window and click Next.
   The Choose Install Folder window opens.
2. Enter the location where the existing Tivoli Identity Manager Server is installed and click Next.

   **Note:** If you choose a different location, the installation program will not detect the existing installation and will install a new Tivoli Identity Manager Server.

   The Do you want to upgrade? window opens.

3. Click Yes to upgrade the Tivoli Identity Manager Server.
   The Specify the Tivoli Identity Manager Domain Information window opens.
4. Accept the default domain base directory (/usr/local/bea/weblogic700/user_projects) or enter a new value and click Next.
   The Pre-Installation Summary window opens.

5. Click Install.
   The Installing Tivoli Identity Manager window opens and a message line appears in the window describing the current installation process. The upgrade
process completes and the System Configuration window opens. The fields on the tabs are populated with values from the previous installation of Tivoli Identity Manager.

6. Confirm that the values on the tabs are correct and click OK. The Install Complete window opens.

7. Click Done to complete the upgrade process.

**Updating Certificate Information**

Upgrading from Tivoli Identity Manager version 4.3 to Tivoli Identity Manager version 4.5 does not preserve the SSL certificate setting in the config.xml file. You will need to manual update the SSL certificate settings through the WebLogic admin console.

1. Start the WebLogic server if not started yet.
2. Open the WebLogic admin console. At a browser window, type the following URL:
   
   http://hostname/console

   where the *hostname* is the host name or IP address of the admin server.
3. Click your domain name in the tree.
4. Click Servers under your domain name.
5. Click the name of the server for which to update the SSL certificate settings.
6. Click the Connections tab in the right pane.
7. Click the SSL tab under the Connections tab.
8. Modify the values to match your system’s configuration.
9. Click Apply.
10. Repeat the previous procedures for all members in your cluster, if you have a clustered configuration.

**Re-Implement Customizations**

Upgrading the Tivoli Identity Manager Server removes any customizations made to the server. Retrieve the customized files from the backup copy of the Tivoli Identity Manager directories and implement the customizations in the new, upgraded versions of the files.

Common items that are customized are the logo, LDAP schema, the authentication mechanism, and Java security.

**Updating Custom Logos**

If you had previously customized the logo in the Tivoli Identity Manager graphical user interface (GUI), you will need to move the graphic file to the new location.

The previous location was:

```
../enrole/weblogic/config/enrole/applications/enrole/images
```

where `../enrole` was the Tivoli Identity Manager home directory.

The graphic must be placed in the

```
BEA_HOME/user_projects/itim/applications/enrole/images directory after Tivoli Identity Manager is upgraded.
```
Verifying Logging Settings
After upgrading the Tivoli Identity Manager Server, previous logging settings are overwritten. If you did not configure the logging settings during installation and accepted the defaults, you will need to update your logging settings after the upgrade is complete.

To update your logging settings, use the System Configuration Tool. Refer to the IBM Tivoli Identity Manager Configuration Guide for detailed information on using the System Configuration Tool and configuring the logging settings.

Starting and Stopping the Tivoli Identity Manager Server
The Tivoli Identity Manager admin server is configured to start automatically after installation. However, the managed servers must be started after installation. This section describes how to start and stop an Tivoli Identity Manager Server.

On UNIX servers, Tivoli Identity Manager installed a script to start and stop the Tivoli Identity Manager Server in the ITIM_HOME directory. For the admin server, the script is named itim.sh. For managed servers, the script is named server_name.sh where server_name is the name of the managed server.

To start the Tivoli Identity Manager Server, use the following command:

```
sh itim.sh start
```

or

```
sh server_name.sh start
```

**Note:** Starting the Tivoli Identity Manager Server takes several minutes. Watch the server_name.log file for a running message. The server_name is the name of the server defined earlier during installation. The log file is located in BEA_HOME/user_projects/itim/logs/ on the admin server and in BEA_HOME/user_projects/itim/server_name/ on the managed servers.

To stop the Tivoli Identity Manager Server, use the following command:

```
sh itim.sh stop
```

or

```
sh server_name.sh stop
```

Testing Tivoli Identity Manager Server Communication
To test whether the database, the directory server, and the Tivoli Identity Manager Server are correctly configured and communicating with each other, do the following:

1. Start Tivoli Identity Manager Server and any prerequisite applications.
2. Log on to Tivoli Identity Manager.
   - For example, at a browser window, type the following:
     ```
     http://hostname/enrole
     ```
   - where hostname is the fully-qualified name or IP address of the computer on which Tivoli Identity Manager Server is running.
3. Enter the Tivoli Identity Manager administrator user ID (itim manager) and password.
4. Take the necessary steps to create a user (an ITIM user).
For more information, refer to online help or to the *IBM Tivoli Identity Manager Policy and Organization Administration Guide*.

**Upgrading Version 4.5 using WebLogic to 4.5.1**

After completing the previous steps that upgrade and configure Tivoli Identity Manager version 4.3 using WebLogic to Tivoli Identity Manager version 4.5 using WebLogic, use the Tivoli Identity Manager version 4.5.1 installation image to upgrade Tivoli Identity Manager version 4.5 using WebLogic to version 4.5.1.
Appendix C. Upgrading from Tivoli Identity Manager 4.5 to Version 4.5.1 using WebLogic

This section describes upgrading previous Tivoli Identity Manager version 4.5 using WebLogic to Tivoli Identity Manager version 4.5.1 using WebLogic.

**Note:** After upgrading, the Tivoli Identity Manager Server will continue to use the existing directory server and database.

**Before Upgrading**

Before upgrading from version 4.5 to version 4.5.1, do the following:

1. Back up the directory server.
   On the directory server side, use the administrative console to perform the backup.

2. Back up the database.
   On the database server, use the administrative console to perform a database backup.

3. Back up the existing Tivoli Identity Manager directory for each server in the cluster.
   This allows you to save any customizations so that you can re-implement them after the upgrade. You can use a tar or a zip utility to back up the information.

4. Back up the existing Tivoli Identity Manager domain folder.
   The default domain folder is in the `BEA_HOME/user_projects/itim` directory.

5. Before upgrading, ensure that the Tivoli Identity Manager workflow engine has no tasks running for reconciliation, identity feed, policy enforcement, or any other provisioning tasks. Prior to an upgrade, not ensuring the workflow engine is idle may result in exceptions being thrown when Tivoli Identity Manager attempts to read recurring or pending events that were created in a previous installation.

   One quick way to check whether the workflow engine is idle is to check the number of messages in the workflow queues (including workflow and workflow pending). Using the Weblogic Admin Console, do the following:
   a. Start the Admin Console.
   b. Open your domain in the tree.
   c. Click **Services -> JMS -> Servers -> JMSServer** in the domain tree.
   d. Click the Monitoring tab on the right window.
   e. Click the link **Monitor all Active JMS Destinations**.
   f. Check **Attribute Messages**. The value of Messages must be 0 for all the listed queues.

6. Stop the Tivoli Identity Manager Server, or in the cluster, stop all the servers. See [“Starting and Stopping the Tivoli Identity Manager Server” on page 75](#) for more information about stopping the cluster members.

7. Verify that the directory server and database are running.

**Note:** Upgrading the Tivoli Identity Manager Server removes any customization that was previously implemented.
Upgrading from Single Server Version 4.5 to Single Server Version 4.5.1

The following procedures describe how to upgrade a single server installation of Tivoli Identity Manager version 4.5 to a single server installation of Tivoli Identity Manager version 4.5.1. If you have a clustered installation of Tivoli Identity Manager version 4.5 and want to upgrade it to Tivoli Identity Manager version 4.5.1, see "Upgrading from Cluster Version 4.5 to Cluster Version 4.5.1" on page 113.

Be sure to complete the procedures in "Before Upgrading" on page 107 before upgrading Tivoli Identity Manager. Backing up the information is the only way to save any customizations.

Prepare to Upgrade the Server

This section describes the initial process to upgrade the Tivoli Identity Manager Server.

1. Log on to the Tivoli Identity Manager Server to be upgraded.
   You must log on using an account with system administrator privileges.
2. Obtain the Tivoli Identity Manager installation image.
3. Open a command prompt window.
4. Type the following command:
   ```
   inst0S-WL.bin
   ```
   where OS is the abbreviation for your system’s operating system. The abbreviations are: AIX for the AIX operating system; 50L for the Solaris operating system; HP-UX for the HP-UX operating system.
   The Language Selection window opens.
5. Select the language to use during installation and click OK.
   The License Agreement window opens.
6. Read the license agreement and decide whether to accept its terms.
7. Select the I accept the terms of the License Agreement radio button if you agree to the terms and click Next.
   The Choose the Installation Type window opens. Proceed with the following section to continue with the upgrade.

Select the Installation Type and Directories

The next steps determine the type of Tivoli Identity Manager to install and the location of the WebLogic Server used by Tivoli Identity Manager.

1. Select the radio button for the type of installation you desire in the Choose Installation Type window and click Next.
   If you want to install a single-server version of Tivoli Identity Manager, select the Single Server radio button. If you want to install a clustered version of Tivoli Identity Manager, select the Cluster radio button.
   The Have you installed BEA WebLogic Server 7.0? window opens.
2. Click Yes if you have already installed the WebLogic Server.
   The Where have you installed WebLogic Server 7.0? window opens.
3. Enter the BEA home directory and the WebLogic Server home directories in their respective fields and click **Next**.

   **Note:** In a clustered installation, the WebLogic Server home directory should be the same for each member of the cluster. See the following section to proceed with the installation process.

**Define the Installation Location**

The procedures in this section identify the location of the existing Tivoli Identity Manager installation and upgrade it.

The previous section ended with the Choose Install Folder window open.
1. Enter the location where the existing Tivoli Identity Manager Server is installed and click Next.

   **Note:** If you choose a different location, the installation program will not detect the existing installation and will install a new Tivoli Identity Manager Server.

   The Do you want to upgrade? window opens.

2. Click **Yes** to upgrade the Tivoli Identity Manager Server.

**Upgrade the Tivoli Identity Manager Server Schemas**

The following procedures describe how to upgrade the schemas associated with Tivoli Identity Manager.

The previous section ended with the Pre-Installation Summary window open.
1. Click Install in the Pre-Installation Summary window.
   The Installing Tivoli Identity Manager window opens and a message line
   appears in the window describing the current installation process. After the
   database schema is upgrade, a message window opens confirming that the
   database schema upgrade is complete.

2. Click OK.
   The directory server schema is upgraded and a message window opens
   confirming that the directory schema upgrade is complete.

3. Click OK.
   The upgrade process completes and the System Configuration window opens.
   The fields on the tabs are populated with values from the previous installation
   of Tivoli Identity Manager.

4. Confirm that the values on the tabs are correct and click OK.
   Proceed to the following section to continue with the upgrade process.

Complete the Upgrade Process

The previous section ended with the Install Complete window open. Complete the
upgrade process by clicking Done.

Re-implement Customizations

Upgrading the Tivoli Identity Manager Server removes any customizations made
   to the server. Retrieve the customized files from the backup copy of the Tivoli
   Identity Manager directories and implement the customizations in the new,
   upgraded versions of the files.

   Common items that are customized are the logo, LDAP schema, the authentication
   mechanism, and Java security.

Figure 82. Pre-Installation Window
Updating Custom Logos
If you had previously customized the logo in the Tivoli Identity Manager graphical
user interface (GUI), you will need to move the graphic file to the new location.

The graphic must be placed in the
BEA_HOME/user_projects/itim/applications/enrole/images directory after Tivoli
Identity Manager is upgraded.

Verifying Logging Settings
After upgrading the Tivoli Identity Manager Server, previous logging settings are
overwritten. If you did not configure the logging settings during installation and
accepted the defaults, you will need to update your logging settings after the
upgrade is complete.

To update your logging settings, use the System Configuration Tool. Refer to the
IBM Tivoli Identity Manager Configuration Guide for detailed information on using
the System Configuration Tool and configuring the logging settings.

Starting and Stopping the Tivoli Identity Manager Server
After the Tivoli Identity Manager Server is installed you must start the server. This
section describes how to start and stop the Tivoli Identity Manager Server.

On UNIX servers, Tivoli Identity Manager installed a script to start and stop the
Tivoli Identity Manager Server in the ITIM_HOME directory

To start the Tivoli Identity Manager Server, use the following command:
sh itim.sh start

**Note:** Starting the Tivoli Identity Manager Server takes several minutes. Watch the
BEA_HOME/user_projects/itim/logs/server_name.log file for a running
message. The server_name is the name of the server defined earlier during
installation.

To stop the Tivoli Identity Manager Server, use the following command:
sh itim.sh stop

Testing Tivoli Identity Manager Server Communication
To test whether the database, the directory server, and the Tivoli Identity Manager
Server are correctly configured and communicating with each other, do the
following:
1. Start Tivoli Identity Manager Server and any prerequisite applications.
2. Log on to Tivoli Identity Manager.
   For example, at a browser window, type the following:
   http://hostname/enrole

   where hostname is the fully-qualified name or IP address of the computer on
   which Tivoli Identity Manager Server is running.
3. Enter the Tivoli Identity Manager administrator user ID (itim manager) and
   password.
4. Take the necessary steps to create a user (an ITIM user).
   For more information, refer to online help or to the IBM Tivoli Identity Manager
   Policy and Organization Administration Guide.
Upgrading from Cluster Version 4.5 to Cluster Version 4.5.1

The following procedures describe how to upgrade a clustered installation of Tivoli Identity Manager version 4.5 to a clustered installation of Tivoli Identity Manager version 4.5.1. If you have a single server installation of Tivoli Identity Manager version 4.5 and want to upgrade to Tivoli Identity Manager version 4.5.1, see “Upgrading from Single Server Version 4.5 to Single Server Version 4.5.1” on page 108.

Be sure to complete the procedures in “Before Upgrading” on page 107 before upgrading Tivoli Identity Manager. Backing up the information is the only way to save any customizations.

To upgrade version 4.5 to version 4.5.1, do the following:

1. “Upgrade the Admin Server”
2. “Upgrade the Managed Servers” on page 117
3. “Re-implement Customizations” on page 120

Upgrade the Admin Server

On the computer on which the administration server is installed, do the following:

Prepare to Upgrade the Server

This section describes the initial process to upgrade the Tivoli Identity Manager Server.

1. Log on to the Tivoli Identity Manager Server to be upgraded.
   You must log on using an account with system administrator privileges.
2. Obtain the Tivoli Identity Manager installation image.
3. Open a command prompt window.
4. Type the following command:

   \texttt{instOS-WL.bin}

   where OS is the abbreviation for your system’s operating system. The abbreviations are: AIX for the AIX operating system; 50L for the Solaris operating system; HPUX for the HP-UX operating system.
   The Language Selection window opens.
5. Select the language to use during installation and click \texttt{OK}.
   The License Agreement window opens.
6. Read the license agreement and decide whether to accept its terms.
7. Select the I accept the terms of the License Agreement radio button if you agree to the terms and click \texttt{Next}.
   The Choose the Installation Type window opens. Proceed with the following section to continue with the upgrade.

Select the Installation Type and Directories

The next steps determine the type of Tivoli Identity Manager to install and the location of the WebLogic Server used by Tivoli Identity Manager.

1. Select the radio button for the type of installation you desire in the Choose Installation Type window and click \texttt{Next}.
   If you want to install a single-server version of Tivoli Identity Manager, select the Single Server radio button. If you want to install a clustered version of Tivoli Identity Manager, select the Cluster radio button.
Have you installed BEA WebLogic Server 7.0? window opens.

2. Click Yes if you have already installed the WebLogic Server.
   If you click No, you can continue with the installation but you will have to install WebLogic 7.0 before Tivoli Identity Manager will run. It is recommended that you exit the installation and install the WebLogic Server before installing Tivoli Identity Manager.

The Where have you installed WebLogic Server 7.0? window opens.

3. Enter the BEA home directory and the WebLogic Server home directories in their respective fields and click Next.

   Note: In a clustered installation, the WebLogic Server home directory should be the same for each member of the cluster.
   See the following section to proceed with the installation process.

**Define the Installation Location**

The procedures in this section identify the location of the existing Tivoli Identity Manager installation and upgrade it.

The previous section ended with the Specify the Server Type window open.
1. Select the Admin Server radio button in the Specify the Server Type window and click Next.
   The Choose Install Folder window opens.

2. Enter the location where the existing Tivoli Identity Manager Server is installed and click Next.
Note: If you choose a different location, the installation program will not detect the existing installation and will install a new Tivoli Identity Manager Server.

The Do you want to upgrade? window opens.

3. Click Yes to upgrade the Tivoli Identity Manager Server.

Proceed to the following section to continue with the upgrade process.

Upgrade the Tivoli Identity Manager Server Schemas

The following procedures describe how to upgrade the schemas associated with Tivoli Identity Manager.

The previous section ended with the Pre-Installation Summary window open.

Figure 86. Pre-Installation Window

1. Click Install in the Pre-Installation Summary window.

The Installing Tivoli Identity Manager window opens and a message line appears in the window describing the current installation process. After the database schema is upgraded, a message window opens confirming that the database schema upgrade is complete.

2. Click OK.

The directory server schema is upgraded and a message window opens confirming that the directory schema upgrade is complete.

3. Click OK.

The upgrade process completes and the System Configuration window opens. The fields on the tabs are populated with values from the previous installation of Tivoli Identity Manager.

4. Confirm that the values on the tabs are correct and click OK.

The Install Complete window opens.

5. Click Done to exit the installation program.
Upgrade the Managed Servers

The following sections describe how to upgrade a managed server.

**Prepare to Upgrade the Server**

This section describes the initial process to upgrade the Tivoli Identity Manager Server.

1. Log on to the Tivoli Identity Manager Server to be upgraded.
   You must log on using an account with system administrator privileges.
2. Obtain the Tivoli Identity Manager installation image.
3. Open a command prompt window.
4. Type the following command:
   ```
   instOS-wL.bin
   ```
   where OS is the abbreviation for your system’s operating system. The abbreviations are: AIX for the AIX operating system; SOL for the Solaris operating system; HPUX for the HP-UX operating system.
   The Language Selection window opens.
5. Select the language to use during installation and click **OK**.
   The License Agreement window opens.
6. Read the license agreement and decide whether to accept its terms.
7. Select the I accept the terms of the License Agreement radio button if you agree to the terms and click **Next**.
   The Choose the Installation Type window opens. Proceed with the following section to continue with the upgrade.

**Select the Installation Type and Directories**

The next steps determine the type of Tivoli Identity Manager to install and the location of the WebLogic Server used by Tivoli Identity Manager.

1. Select the radio button for the type of installation you desire in the Choose Installation Type window and click **Next**.
   If you want to install a single-server version of Tivoli Identity Manager, select the Single Server radio button. If you want to install a clustered version of Tivoli Identity Manager, select the Cluster radio button.
   The Have you installed BEA WebLogic Server 7.0? window opens.
2. Click **Yes** if you have already installed the WebLogic Server.
   If you click **No**, you can continue with the installation but you will have to install WebLogic 7.0 before Tivoli Identity Manager will run. It is recommended that you exit the installation and install the WebLogic Server before installing Tivoli Identity Manager.
   The Where have you installed WebLogic Server 7.0? window opens.
3. Enter the BEA home directory and the WebLogic Server home directories in their respective fields and click **Next**.

   **Note:** In a clustered installation, the WebLogic Server home directory should be the same for each member of the cluster.

   See the following section to proceed with the installation process.

**Define the Installation Location and Complete the Upgrade Process**

The procedures in this section identify the location of the existing Tivoli Identity Manager installation and upgrade it.

The previous section ended with the Specify the Server Type window open.
1. Select the Managed Server(s) radio button in the Specify the Server Type window and click Next.
   The Choose Install Folder window opens.

2. Enter the location where the existing Tivoli Identity Manager Server is installed and click Next.
**Note:** If you choose a different location, the installation program will not detect the existing installation and will install a new Tivoli Identity Manager Server.

The Do you want to upgrade? window opens.

3. Click **Yes** to upgrade the Tivoli Identity Manager Server.

   The Pre-Installation Summary window opens.

   ![Pre-Installation Summary Window](image)

   *Figure 90. Pre-Installation Window*

4. Click **Install**.

   The Installing Tivoli Identity Manager window opens and a message line appears in the window describing the current installation process. The upgrade process completes and the System Configuration window opens. The fields on the tabs are populated with values from the previous installation of Tivoli Identity Manager.

5. Confirm that the values on the tabs are correct and click **OK**.

   The Install Complete window opens.

6. Click **Done** to complete the upgrade process.

**Re-Implement Customizations**

Upgrading the Tivoli Identity Manager Server removes any customizations made to the server. Retrieve the customized files from the backup copy of the Tivoli Identity Manager directories and implement the customizations in the new, upgraded versions of the files.

Common items that are customized are the logo, LDAP schema, the authentication mechanism, and Java security.

**Updating Custom Logos**

If you had previously customized the logo in the Tivoli Identity Manager graphical user interface (GUI), you will need to move the graphic file to the new location.
The graphic must be placed in the 
`BEA_HOME/user_projects/itim/applications/enrole/images` directory after Tivoli Identity Manager is upgraded.

**Verifying Logging Settings**

After upgrading the Tivoli Identity Manager Server, previous logging settings are overwritten. If you did not configure the logging settings during installation and accepted the defaults, you will need to update your logging settings after the upgrade is complete.

To update your logging settings, use the System Configuration Tool. Refer to the *IBM Tivoli Identity Manager Configuration Guide* for detailed information on using the System Configuration Tool and configuring the logging settings.

**Starting and Stopping the Tivoli Identity Manager Server**

The Tivoli Identity Manager admin server is configured to start automatically after installation. However, the managed servers must be started after installation. This section describes how to start and stop an Tivoli Identity Manager Server.

On UNIX servers, Tivoli Identity Manager installed a script to start and stop the Tivoli Identity Manager Server in the `ITIM_HOME` directory. For the admin server, the script is named `itim.sh`. For managed servers, the script is named `server_name.sh` where `server_name` is the name of the managed server.

To start the Tivoli Identity Manager Server, use the following command:

```
sh itim.sh start
```

or

```
sh server_name.sh start
```

**Note:** Starting the Tivoli Identity Manager Server takes several minutes. Watch the `server_name.log` file for a running message. The `server_name` is the name of the server defined earlier during installation. The log file is located in `BEA_HOME/user_projects/itim/logs/` on the admin server and in `BEA_HOME/user_projects/itim/server_name/` on the managed servers.

To stop the Tivoli Identity Manager Server, use the following command:

```
sh itim.sh stop
```

or

```
sh server_name.sh stop
```

**Testing Tivoli Identity Manager Server Communication**

To test whether the database, the directory server, and the Tivoli Identity Manager Server are correctly configured and communicating with each other, do the following:

1. Start Tivoli Identity Manager Server and any prerequisite applications.
2. Log on to Tivoli Identity Manager.

   For example, at a browser window, type the following:
   
   ```
   http://hostname/enrole
   ```

   where `hostname` is the fully-qualified name or IP address of the computer on which Tivoli Identity Manager Server is running.
3. Enter the Tivoli Identity Manager administrator user ID (itim manager) and password.

4. Take the necessary steps to create a user (an ITIM user).

For more information, refer to online help or to the IBM Tivoli Identity Manager Policy and Organization Administration Guide.
Appendix D. Uninstalling

The Tivoli Identity Manager process uninstalls the following:

- Tivoli Identity Manager
- Tivoli Identity Manager application and configuration settings created for Tivoli Identity Manager on WebLogic Server
- All ITIM_HOME files copied to a target system during the Tivoli Identity Manager installation

**Note:** Uninstalling Tivoli Identity Manager does not modify existing database tables or the Directory server schema. The Tivoli Identity Manager uninstaller only removes the Tivoli Identity Manager application from within WebLogic Server.

To uninstall additional products that may have been installed during the Tivoli Identity Manager installation, such as WebLogic Server for example, please refer to the appropriate documentation for the product.

---

**Steps to Uninstall Tivoli Identity Manager**

To uninstall Tivoli Identity Manager, do the following:

1. Uninstall the Tivoli Identity Manager application by running the following command on the computer on which Tivoli Identity Manager is installed:
   
   ```
   ITIM_HOME/itimUninstallerData/Uninstall_ITIM
   ```

2. Proceed through the uninstall wizard panels to confirm you wish to uninstall Tivoli Identity Manager.

3. After the uninstall completes successfully, remove any residual directories, configuration files, and log files for Tivoli Identity Manager from your filesystem.

To verify that Tivoli Identity Manager has been uninstalled and removed as an application from WebLogic Server, do the following:

1. Verify that the Tivoli Identity Manager directories are deleted.

   **Note:** Some directories may still remain since the uninstall program does not remove dynamic files. These file can include various log files. However, all application files should no longer be available on the system.

2. Verify that the Tivoli Identity Manager registry items are removed.

   The location of the registry items is dependent on your operating system.

   For Solaris systems, the registry items were located in the `/var/sadm/pkg/ITIM/pkginfo` directory.

   For HP-UX systems, the registry items were located in the `/var/adm/sw/products/ITIM/pfiles/INDEX` directory.

   For AIX systems, use the `ls1pp -La` command to display the existing registry items.
Appendix E. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.
Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged should contact:

IBM Corporation
2ZAA/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

**Trademarks**

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DB2
IBM
IBM logo
SecureWay
Tivoli
Tivoli logo
Universal Database
WebSphere

Lotus is a registered trademark of Lotus Development Corporation and/or IBM Corporation.

Domino is a trademark of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.
Glossary

A

access. The privilege to use information or data stored on computer systems.

account. The set of parameters that define the login information and access control information for a user.

account report. A report that lists people and their associated accounts and whether or not the account is in compliance with current policies.

access control information (ACI). Data that identifies the access rights of a group or principal. See also access control.

ACI origin. The branch in the organization tree where the ACI is created.

ACI target. The set of entities that are controlled by the ACI.

active account. An account that exists and that is in use by the owner to access a resource.

admin domain. A business unit that is used to logically separate organizational responsibilities and manage access rights.

alias. An identity for a user, usually referred to as the user ID. A person can have several aliases, for example: GSmith and GWSmith.

attribute enforcement. The process in which system administrators define the attributes that are required for an account and the values that are valid for those attributes.

audit trail. The record of transactions for a computer system during a given time period.

authentication. The process of identifying an individual, usually based on a user name and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

authorization. In computer security, the right granted to a user to communicate with or make use of a computer system. The process of granting a user either complete or restricted access to an object, resource, or function.

Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity.

authorization owner. A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

B

branch. Each level within the organization tree is called a branch. Each type of branch in the tree is indicated by a different icon. The contents of a branch with sub-units can be viewed by clicking the plus (+) sign next to it.

business partner organization. A class of person that is not a direct employee of the company or organization, but that might need access to the company’s resources.

business partner person. A person in a business partner organization.

business unit. A subsidiary entity of an organization.

C

central data repository. The database used to record and store user and access privilege data for all registered users, including transaction and maintenance records.

Certificate Authority (CA). An organization that issues certificates. The certificate authority authenticates the certificate owner’s identity and the services that the owner is authorized to use, issues new certificates, renews existing certificates, and revokes certificates belonging to users who are no longer authorized to use them.

challenge response. An authentication method that requires users to respond to a prompt by providing private information to verify their identity when logging in to the network.

completed requests. Requests that were submitted to the system and that are completed.

constraint. A limitation on a parameter or policy.

control type. An instance of the Java Type class that represents the type of field on a user interface.
credential. The User ID and password information for a user, which allows access to an account.

delegate. An individual who is designated as the responsible party to approve requests or provide information for requests for another user.

de-provision. To remove a service or component. For example, to de-provision an account means to delete an account from a resource.

digital certificate. An attachment to an electronic message used for security purposes.

Directory Services Markup Language (DSML). An XML implementation that provides a common format for describing and sharing directory services information among different directory systems.

disallowed action. A parameter set for reconciliations that defines action to take if the Tivoli Identity Manager Server finds accounts for persons who are not allowed to have an account for the selected service. This parameter is only valid if the Check Policy check box is selected.

domain administrator. An administrator that can define and manage provisioning entities, policies, services, workflow definitions, roles, and users within their admin domain, but only in his or her own admin domain.

DSML identity feed. One of Tivoli Identity Manager’s three default service types.

A DSML identity feed service imports user data from a human resources database or file and feeds the information into the Tivoli Identity Manager directory. The service can receive the information in one of two ways: a reconciliation or an unsolicited notification.

electronic forms. An electronic form serves as a template to define the parameters of the access being requested.

entitlement. In security management, a data structure, service, or list of attributes that represents policy information.

entity. 1) A person or object for which information is stored.

2) One of the following classes, as referred to by the Tivoli Identity Manager system:
   • Person
   • BPPerson
   • Organization
   • BPOrganization

escalation participant. In identity management, a person that has the authority to respond to requests that participants do not respond to within a specified escalation time. An escalation participant can be identified as an individual, as a roles, or by using a custom JavaScript script.

escalation limit. The amount of time, in days, hours, minutes or seconds, that a participant has to respond to a request, before an escalation occurs.

HR feed. An automated process in which the Tivoli Identity Manager system imports user data from a human resources database or file. Refer to DSML identity feed.

identity policy. The rules by which the Tivoli Identity Manager system defines how a user’s ID is created.

inactive account. An account that exists in the system, but that is not in use by the account owner.

ITIM group. A user group within the Tivoli Identity Manager Server.

System access and administration can be structured around ITIM groups. However, before a person can be assigned to an ITIM group, the user must be provisioned with an ITIM account. Once the person is provisioned with an ITIM account, the person is an ITIM user and can be added to an ITIM group.

join directive. The set of rules that define how to handle attributes when two or more provisioning policies conflict.

keyword. An index entry that identifies the policy in a search.

location. One of the types of subsidiary entities that can be added to an organization. Typically, locations are used to logically separate geographic locations for organizational management purposes.
O

operation report. A report that lists Tivoli Identity Manager operation requests by type of operation, date, who requested the operation, and who the operation is requested for.

organization. In identity management, a body of users and resources which is fairly independent. Although the sharing of resources between organizations is possible, the level of integration between the organizations is relatively low. Generally, an organization represents a company.

organization tree. A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organizational role. In identity management, an attribute that is used to determine membership to policies that grant access to various managed resources.

organizational unit. A body of users and resources within an organization defined to sub-divide an organization into more manageable groups. Users are assigned to only one organizational unit. Resources are also assigned to only one organizational unit unless they are defined as global to an organization.

orphan (orphan accounts). Accounts on a remote resource whose owner in the Tivoli Identity Manager system cannot be determined.

owner. A person in the Tivoli Identity Manager system that owns an account or a service.

P

participant. In identity management, a person that has the authority to respond to a request that is submitted through the workflow engine. A participant can be identified as an individual, as a roles, or by using a custom JavaScript script.

password. In computer and network security, a specific string of characters entered by a user and authenticated by the system, which allows the user to gain access to the system and to the information stored within it.

password expiration period. The amount of time a password can be used before the user is forced to change it.

password policy. The rules that define the set parameters that all passwords must meet, such as length, and the type of characters allowed and disallowed.

pending requests. Requests that have been submitted to the system but that have not yet been completed.

personal information. A user’s personal information. This information can include last name, first name, home address, phone number, e-mail address, office number, supervisor, etc.

policy. In Tivoli, a set of rules that are applied to managed resources. For example, a policy can apply to passwords or to resources that a user attempts to access.

policy enforcement. The manner in which the Tivoli Identity Manager system allows or disallows accounts that violate provisioning policies.

provision. To set up and maintain a user’s access to a system in the organization.

provisioning policy. A policy that defines the access to various types of managed services, such as Tivoli Identity Manager or operating systems. Access is granted to all persons or based on a person’s organizational role. Access can also be granted specifically to persons who are not members of any organizational role.

Q

query. A way in which to limit a reconciliation to return smaller packets.

R

reconciliation. In identity management, the process of synchronizing the accounts and supporting data on the central data repository with the accounts and supporting data on the managed resource.

reconciliation report. A report that lists the orphan accounts found since the last reconciliation was performed.

rejected report. A report that lists requests denied by date, who requested the operation, and who the operation is requested for.

request. An action item in the Tivoli Identity Manager system asking for approval or information.

requestee. The person for whom a request is submitted.

requestor. A person who submits a request.

resource. A hardware, software, or data entity that is managed by Tivoli software. See also managed resource.

resource provisioning management (rpm). The management principle that combines three key elements - business logic, workflow management, and
distribution agents - which together centrally manage the provisioning of users with access to information and business resources.

restore. To reactivate an account that was suspended.

request for information (RFI). In identity management, an action item that requests additional information from the specified participant and that is a required step in the workflow.

S

scope. The range that a policy can affect.
Typically, the scope is defined as single or subtree. When the scope is defined as single, the policy only affects entities in the same branch in which the policy is defined. When the scope is defined as sub-tree, the policy affects the branch in which it is defined and all other branches that are subordinate to the policy’s branch of origin.

service. A program that performs a primary function within a server or related software.

service selection policy. A JavaScript filter that determines which service to use in a provisioning policy.

shared secret. An encrypted value used to retrieve a user’s initial password to access the Tivoli Identity Manager system. This value is defined when the user’s personal information is initially loaded into the system.

signature authority. The right to approve or deny a request that is submitted to the workflow engine. A user or group of users is granted signature authority when they are designated as the participant or escalation participant in a workflow design.

secure socket layer (SSL). A protocol for transmitting private documents through the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection.

static organizational role. An organizational role that can only be assigned manually.

subprocess. A workflow design that is started as part of another workflow design.

supervisor. A person in the Tivoli Identity Manager system that is designated as the owner of a business unit.

suspend. The act of deactivating an account so the account owner cannot log into the resource.

system administrator. Individuals with access to all areas in the system.
A pre-configured ITIM Group is provided in the Tivoli Identity Manager system. This ITIM Group is designed to grant members maximum access to the system.
Users who are members of the administrator ITIM Group have access to all system functions and data.

T

Tivoli Identity Manager Agent. An intelligent interface between the targeted managed system and the Tivoli Identity Manager Server. It acts as a trusted virtual administrator and is a critical component that translates user requests and provides secure configurations access to various targeted systems.

Tivoli Identity Manager Server. A software and services package designed to deploy policy-based provisioning solutions.

to do list. The list of actions items assigned to a user for completion.

U

user. Any person who interacts with the system.

user class. An LDAP class such as inetorgperson or BPPerson.

user interface (UI). The display used by the user to interact with the system.

user name. The ID used by the user to access the system. This ID also identifies the user to the system and allows the system to determine the user’s access rights based on the user’s membership in various organizational roles and ITIM groups.

user report. A report that lists all Tivoli Identity Manager operations by date, who requested the operation, and who the operation is requested for.

W

workflow. The sequence of activities performed in accordance with the business processes of an enterprise.
Index

A
accessibility statement for documentation ix
accessing documents online ix
Admin ID, database field 20, 43
Admin Password, database field 20, 43
administrative authority, ensure before installation 19, 41
audience, who should read this book vii

B
BEA Home Directory, WebLogic Server field 20, 42

C
CA certificate
requirements 38, 76
CDs 79
Choose installation type
installation input 26, 27, 48, 49, 64, 88, 94, 100, 108, 113, 117
cluster
installation
admin server 47
Apache HTTP server configuration 77
configuring the proxy server 76
determining cluster configuration 49, 65
IIS HTTP server configuration 76
initial configuration of a managed server 71
installing a managed server 62
registering a managed server 61
specifying directory server connection information 69
Tivoli Identity Manager Server 41
installation flowchart 45
prerequisites
database 41
directory server 41
WebLogic 41
worksheet 42
Cluster Multicast Address, Tivoli Identity Manager field 42
Cluster Multicast Port, Tivoli Identity Manager field 42
Cluster Name, Tivoli Identity Manager field 42
configuration
database 30, 54
directory 31, 32, 55, 56
Tivoli Identity Manager
database tab 34, 58
directory tab 34, 58
general tab 33, 57
logging tab 35, 59
mail tab 35, 59
security tab 37, 61
UI tab 36, 60
configuring
Oracle 14
Sun ONE Directory Server 17
contacting software support ix
conventions used in this document x

D
database
configuration
initial 30, 54
field
Admin ID 20, 43
Admin Password 20, 43
Database Name 21, 43
Database Type 20, 43
Database User 21, 43
Initial Capacity 21, 43
IP Address 21, 43
Login Delay Seconds 21, 43
Maximum Capacity 21, 43
Port Number 21, 43
User Password 21, 43
database configuration
installation input 30, 54
Database Name, database field 21, 43
Database Name, database pool field 21, 43
database tab 34, 58
Database Type, database field 20, 43
Database User, database field 21, 43
Default Org Short Name, directory server field 22, 44
directory
configuration
initial 31, 55
reappearance with active fields 32, 56
directory configuration
installation input 31, 32, 55, 56
directory server
field
Default Org Short Name 22, 44
Host name 21, 44
Identity Manager DN Location 22, 44
Increment count 22, 45
Initial pool size 22, 44
Max. pool size 22, 44
Name of your organization 22, 44
Number of hash buckets 22, 44
Password 21, 44
Port 22, 44
Principal DN 21, 44
directory structure differences
upgrading
Tivoli Identity Manager Server 85
directory tab 34, 58
documents, Tivoli Identity Manager library vii
accessing documents online ix
related documents ix
Domain Base Directory, Tivoli Identity Manager field 42
Domain Name, Tivoli Identity Manager field 42

E
encryption
key 29, 52, 69
Encryption key
installation input 29, 52, 69
Encryption Key, Tivoli Identity Manager field 42

© Copyright IBM Corp. 2004
installing (continued)
Tivoli Identity Manager Server (continued)
single-server 19
IP Address, database field 21, 43

Language selection
installation input 25, 47, 63
License Agreement
installation input 25, 47, 63
Log on
installation input 25, 47, 63
logging tab 35, 59
Login Delay Seconds, database pool field 21, 43

Name of your organization, directory server field 22, 44
Number of hash buckets, directory server field 22, 44

Oracle
configuring 14
installing
AIX 9
HP-UX 12
Solaris 11
Windows 13

Password
directory server field 21, 44
Password, Tivoli Identity Manager field 23, 45
Port
directory server field 22, 44
Port Number, database field 21, 43
Pre-Installation summary
installation input 29, 53, 70, 90, 97, 110, 116
prerequisite
worksheet
cluster 42
prerequisites
authority as root 19, 41
class 19, 41
database 41
directory server 41
WebLogic 41
root user 19, 41
single-server
administrative authority 19, 41
database 19
directory server 19
WebLogic Server 19
worksheet
single-server 20
Principal DN, directory server field 21, 44
Product CD installation input 25, 47, 63 properties value single-server
  Domain Base Directory 20
  Domain Name 20
  Encryption Key 20
  Server Name 20
  Tivoli Identity Manager 20 publications, Tivoli Identity Manager library vii accessing documents online ix related documents ix

R requirements
  CA certificate 38, 76 root
  authority 19, 41
  user 19, 41

S security tab 37, 61
Server Configuration and Implementation
  cluster 6
  Overview 3
  single–server 4
Server Name, Tivoli Identity Manager field 42 single-server configuration installing 19 installation
  Tivoli Identity Manager Server 19 installation flowchart 23 installation sequence
  choose install folder 27
  specify domain information 28 prerequisites
  administrative authority 19, 41
  database 19
  directory server 19
  WebLogic Server 19 properties value
  Domain Base Directory 20
  Domain Name 20
  Encryption Key 20
  Server Name 20
  Tivoli Identity Manager 20 worksheet 20 software support, contacting ix Start installation wizard
  installation input 25, 47, 63 starting and stopping
  Tivoli Identity Manager Server 37, 75, 92, 105, 112, 121 Sun ONE Directory Server
  configuring 17 support, contacting software ix system configuration
  installation input 91, 98, 111, 116
  system configuration, database tab
  installation input 34, 58
  system configuration, directory tab
  installation input 34, 58
  system configuration, general tab
  installation input 33, 57 system configuration, logging tab
  installation input 35, 59 system configuration, mail tab
  installation input 35, 59 system configuration, security tab
  installation input 37, 61 system configuration, UI tab
  installation input 36, 60

T
  database 34, 58
directory 34, 58
  general 33, 57
  logging 35, 59
  mail 35, 59
  security 37, 61
  UI 36, 60
Terminology WebLogic 3 test communication
  Tivoli Identity Manager Server 38, 75, 93, 105, 112, 121 Tivoli Identity Manager configuration
  database tab 34, 58
directory tab 34, 58
gen
  general tab 33, 57
  logging tab 35, 59
  mail tab 35, 59
  security tab 37, 61
  UI tab 36, 60
field
  Cluster Multicast Address 42
  Cluster Multicast Port 42
  Cluster Name 42
  Domain Base Directory 42
  Domain Name 42
  Encryption Key 42
  Password 23, 45
  Server Name 42
  Tivoli Identity Manager directory 42
  User ID 22, 45
uninstalling 123
  additional products 123
  database tables 123
directory server schema 123
  steps 123
upgrading 87, 93, 99, 108, 113, 117
customizations, removal 92, 104, 111, 120
  schemas 90, 97, 110, 116
  updating custom logos 92, 104, 112, 120
Tivoli Identity Manager directory, Tivoli Identity Manager field 42
Tivoli Identity Manager Server CA certificate 38, 76 installing
  cluster 41
  flowchart, cluster 45
  flowchart, single-server 23
  single-server 19
starting and stopping 37, 75, 92, 105, 112, 121
  test communication 38, 75, 93, 105, 112, 121
upgrading before upgrading 86, 107
  completing the upgrade process 91, 101, 118
defining installation location 101, 118
Tivoli Identity Manager Server *(continued)*
upgrading *(continued)*
defining the installation location 95, 114
directory structure differences 85
from cluster version 4.3 to cluster version 4.5 93
from cluster version 4.5 to cluster version 4.5.1 113
from single server version 4.3 to single server version 4.5 87
from single server version 4.5 to single server version 4.5.1 108
from Tivoli Identity Manager 4.3 85
from Tivoli Identity Manager 4.5 107
the admin server 93, 113
updating the managed server 98

**U**

UI tab 36, 60
uninstalling
Tivoli Identity Manager 123
additional products 123
database tables 123
directory server schema 123
steps 123
upgrading
Tivoli Identity Manager 87, 93, 99, 108, 113, 117
customizations, re-implementing 92, 104, 111, 120
schemas 90, 97, 110, 116
updating custom logos 92, 104, 112, 120
Tivoli Identity Manager Server
before upgrading 86, 107
completing the upgrade process 91, 101, 118
defining installation location 101, 118
defining the installation location 95, 114
directory structure differences 85
from cluster version 4.3 to cluster version 4.5 93
from cluster version 4.5 to cluster version 4.5.1 113
from single server version 4.3 to single server version 4.5 87
from single server version 4.5 to single server version 4.5.1 108
from Tivoli Identity Manager 4.3 85
from Tivoli Identity Manager 4.5 107
the admin server 93, 113
updating the managed server 98

User ID, Tivoli Identity Manager field 22, 45
User Password, database field 21, 43

**W**

WebLogic
server configurations 3
cluster 6
single-server 4
terminology 3
admin server 3
cluster 3
managed server 3
single-server 3
Web proxy server 3
WebLogic Server
field
BEA Home Directory 20, 42
WebLogic Server Directory 20, 42
WebLogic Server Directory, WebLogic Server field 20, 42

136 IBM Tivoli Identity Manager: Server Installation Guide on UNIX using WebLogic
Program Number: 5724–C34

Printed in USA