Oracle® Fusion Middleware

Installation Guide for Oracle Identity Management

11*g* Release 1 (11.1.1)

E12002-02

October 2009

ORACLE®

Oracle Fusion Middleware Installation Guide for Oracle Identity Management, 11*g* Release 1 (11.1.1)

E12002-02

Primary Author: Don Biasotti

Contributors: Niranjan Ananthapadmanabha, Biju Albert, Fermin Castro, Kurt Heiss, Kevin Hwang, Peter LaQuerre, Stephen Lee, Solomon Nelson, Arivoli Tirouvingadame, Srinivasa Vedam, Shari Yamaguchi

Contents

3 Before Installing Oracle Identity Management

4 Performing Common Installation Tasks

5 Installing and Configuring Oracle Internet Directory

6 Installing and Configuring Oracle Virtual Directory

7 Installing and Configuring Oracle Directory Integration Platform

8 Installing and Configuring Oracle Directory Services Manager

9 Installing and Configuring Oracle Identity Federation

Preface

This Preface provides supporting information for the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* and includes the following topics:

Audience

The *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* is intended for administrators that are responsible for installing Oracle Identity Management components.

This document assumes you have experience installing enterprise components. Basic knowledge about the Oracle Identity Management components and Oracle Application Server is recommended.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

This section identifies additional documents related to Oracle Identity Management. You can access Oracle documentation online from the Oracle Technology Network (OTN) Web site at the following URL:

http://www.oracle.com/technology/documentation/

Note: Printed documentation is available for sale from the Oracle Store Web site at the following URL:

http://oraclestore.oracle.com/

Refer to the following documents for additional information on each subject:

Oracle Fusion Middleware

- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Security Guide*

Oracle Identity Management

- *Oracle Fusion Middleware Getting Started with Oracle Identity Management*
- *Oracle Fusion Middleware User Reference for Oracle Identity Management*

Installing and Upgrading

- *Oracle Fusion Middleware Installation Planning Guide*
- *Oracle Fusion Middleware Quick Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Upgrade Planning Guide*
- *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Getting Started With Installation for Oracle WebLogic Server*
- *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*

High Availability

- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

Oracle Internet Directory

- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management*

Oracle Directory Integration Platform

- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*

Oracle Virtual Directory

- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

Oracle Directory Services Manager

- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*

Oracle Identity Federation

- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

Oracle Single Sign-On

- *Oracle Application Server Single Sign-On Administrator's Guide 10g Release 10.1.4.0.1* available at:

  `http://www.oracle.com/technology/documentation/oim1014.html`

Oracle Delegated Administration Services

- *Oracle Identity Management Guide to Delegated Administration 10g Release 10.1.4.0.1* available at:

  `http://www.oracle.com/technology/documentation/oim1014.html`

Repository Creation Utility

- *Oracle Fusion Middleware Repository Creation Utility User's Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Understanding Oracle Identity Management 11*g* Release 1 (11.1.1)

This chapter provides a brief overview of Oracle Identity Management 11*g* Release 1 (11.1.1) and this guide. This chapter includes the following topics:

- What is Oracle Fusion Middleware?
- What is Oracle Identity Management?
- Which Components are in Oracle Identity Management 11g Release 1 (11.1.1)?

> **See:** The "Related Documents" section in this guide's Preface for a list of documents that provide additional information about the topics described in this chapter.

1.1 What is Oracle Fusion Middleware?

Oracle Identity Management is part of Oracle Fusion Middleware. Oracle Fusion Middleware is a collection of standards-based software products that spans a range of tools and services: From Java EE and developer tools, to integration services, business intelligence, and collaboration. Oracle Fusion Middleware offers complete support for development, deployment, and management.

1.1.1 What is Oracle Enterprise Manager Fusion Middleware Control?

Oracle Enterprise Manager Fusion Middleware Control is a Web browser-based graphical user interface that you can use to monitor and administer Oracle Fusion Middleware components, including Oracle Identity Management components, that are installed in Oracle WebLogic Server domains.

> **Note:** When you install Oracle Identity Management components in a new domain, the Fusion Middleware Control management component is included.

1.2 What is Oracle Identity Management?

Oracle Identity Management enables enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources—both within and beyond the firewall. With Oracle Identity Management, you can deploy applications faster, apply the most granular protection to enterprise resources, automatically eliminate latent access privileges, and much more.

Oracle Corporation leads the industry with award-winning Identity Management offerings that constitute the most comprehensive solution offered by any vendor, including:

- Web Access Control
- Adaptive Access Control
- Identity Federation
- Identity Administration
- User Access Provisioning
- Role Management
- Directory Services

For more information about Oracle Identity Management, refer to the Identity Management home page on Oracle Corporation's Web site at:

http://www.oracle.com/identity

1.3 Which Components are in Oracle Identity Management 11*g* Release 1 (11.1.1)?

Oracle Identity Management 11*g* Release 1 (11.1.1) includes the following components:

- Oracle Internet Directory
- Oracle Directory Integration Platform
- Oracle Virtual Directory
- Oracle Directory Services Manager
- Oracle Identity Federation

1.3.1 Oracle Single Sign-On and Oracle Delegated Administration Services Certification for 11*g* Release 1 (11.1.1)

Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* are required components for Oracle Portal, Forms, Reports and Discoverer Release 10*g* and Release 11*g*.

There are no 11*g* Release 1 (11.1.1) versions of Oracle Single Sign-On and Oracle Delegated Administration Services. However, both Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) are certified for use with Oracle Internet Directory 11*g* Release 1 (11.1.1).

If you are running Oracle Single Sign-On or Oracle Delegated Administration Services Release 10*g*, you can either:

- Continue using Oracle Single Sign-On and Oracle Delegated Administration Services Release 10g with Oracle Internet Directory Release 10g.

  or

- Upgrade to Oracle Internet Directory 11g Release 1 (11.1.1) to use its new features.

See: The following for more information:

- Chapter 10, "Installing Oracle Single Sign-On and Oracle Delegated Administration Services Against Oracle Internet Directory."
- Chapter 10, "Configuring Single Sign-On in Oracle Fusion Middleware," in the *Oracle Fusion Middleware Security Guide*, for recommended single sign-on solutions for Oracle Fusion Middleware.

2

Understanding the Oracle Identity Management 11*g* Release 1 (11.1.1) Installation

This chapter provides an overview of the Oracle Identity Management 11*g* Release 1 (11.1.1) installation. This chapter includes the following topics:

2.1 Using This Guide

Each document in the Oracle Fusion Middleware Documentation Library has a specific purpose. The specific purpose of this guide is to explain how to:

1. Install single instances of Oracle Identity Management 11*g* Release 1 (11.1.1) components.
2. Verify the installation was successful.
3. Get started with the component after installation.

This guide covers the most common, certified Oracle Identity Management deployments. The following information is provided for each of these deployments:

- **Appropriate Deployment Environment**: Helps you determine which deployment is appropriate for your environment.
- **Components Deployed**: Identifies the components that are installed in each deployment.
- **Dependencies**: Identifies the components each deployment depends on.
- **Procedure**: Explains the steps for the deployment.

As described in "Installation Types: "Install and Configure" vs. "Install Software - Do Not Configure"" on page 2-3, the procedures in this guide explain how to deploy Oracle Identity Management components explicitly using the **Install and Configure** installation option.

However, if you install Oracle Identity Management components using the **Install Software - Do Not Configure** installation option and then later decide you want to configure them using the Oracle Identity Management 11*g* Release 1 (11.1.1) Configuration Wizard, you can still use the procedures in this guide, as the screens and tasks will be the same as if you used the **Install and Configure** option.

2.2 Overview of Installation Process

The following is an overview of the steps to install Oracle Identity Management 11*g* Release 1 (11.1.1):

1. Review Chapter 2, "Understanding the Oracle Identity Management 11g Release 1 (11.1.1) Installation," for context.
2. Review Chapter 3, "Before Installing Oracle Identity Management," for information about what you should consider before you deploy Oracle Identity Management.
3. Review Chapter 4, "Performing Common Installation Tasks," to understand the tasks that you must perform for most deployments. Understanding this information before you start will expedite and simplify the deployment process.
4. Install, verify, and get started with your Oracle Identity Management component by referring to its specific chapter in this guide.
5. Use the appendixes in this guide as needed.

2.3 Additional 11*g* Release 1 (11.1.1) Deployment Information

This topic describes additional sources for 11*g* Release 1 (11.1.1) deployment information, including documentation on the following subjects:

- Upgrading to 11g Release 1 (11.1.1)
- Installing 11g Release 1 (11.1.1) for High Availability

> **See Also:** The "Related Documents" section in this guide's Preface for a list of documents that provide additional information about Oracle Identity Management components.

2.3.1 Upgrading to 11*g* Release 1 (11.1.1)

This guide does not explain how to upgrade previous versions of Oracle Identity Management components to 11*g* Release 1 (11.1.1). To upgrade an Oracle Identity Management component:

From Release 10*g* to 11*g* Release 1 (11.1.1), refer to:

- *Oracle Fusion Middleware Upgrade Planning Guide*
- *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*

From 11*g* Release 1 (11.1.1.1.0) to 11*g* Release 1 (11.1.1.2.0), refer to:

- "Special Instructions for Oracle Fusion Middleware 11g Release 1 (11.1.1.1.0) Users" in the *Oracle Fusion Middleware Installation Planning Guide*

2.3.2 Installing 11*g* Release 1 (11.1.1) for High Availability

This guide does not explain how to install Oracle Identity Management components in High Availability (HA) configurations. To install an Oracle Identity Management component in a High Availability configuration, refer to the following documents:

- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

2.4 Installation Types: "Install and Configure" vs. "Install Software - Do Not Configure"

The Select Installation Type screen in the Installer presents two options: **Install and Configure** and **Install Software - Do Not Configure**. This section describes both options:

- Understanding the "Install and Configure" Option
- Understanding the "Install Software - Do Not Configure" Option

2.4.1 Understanding the "Install and Configure" Option

Choose the **Install and Configure** option to install Oracle Identity Management components and simultaneously configure some of their fundamental elements, such as passwords, user names, and so on. Oracle Identity Management components start running and are immediately ready for use after deploying them using the **Install and Configure** option.

If you choose the **Install and Configure** option, you will see additional Installer screens that will not appear using the **Install Software - Do Not Configure** option. These additional screens prompt you for information the Installer uses to configure Oracle Identity Management components.

Important: The procedures in this guide explain how to deploy Oracle Identity Management components explicitly using the **Install and Configure** option.

2.4.2 Understanding the "Install Software - Do Not Configure" Option

Choose the **Install Software - Do Not Configure** option to install Oracle Identity Management components without configuring them during installation. If you choose the **Install Software - Do Not Configure** option, the Installer installs the component software and then closes. Oracle Identity Management components will *not* start running after deploying them using the **Install Software - Do Not Configure** option, as additional configuration is needed.

After you install components using the **Install Software - Do Not Configure** option, you can configure them at a later time using the Oracle Identity Management 11*g* Release 1 (11.1.1) Configuration Wizard. To start the Oracle Identity Management 11*g* Release 1 (11.1.1) Configuration Wizard, execute the *ORACLE_HOME*/bin/config.sh script (config.bat on Windows).

Important: The procedures in this guide explain how to deploy Oracle Identity Management components explicitly using the **Install and Configure** option.

However, if you install Oracle Identity Management components using the **Install Software - Do Not Configure** option and then later decide you want to configure them using the Oracle Identity Management 11*g* Release 1 (11.1.1) Configuration Wizard, you can still use the procedures in this guide, as the screens and tasks will be the same as if you used the **Install and Configure** option.

The only difference between the screens for configuring components is how you access them—Through the Installer if you choose the you the **Install and Configure** option, or through the Configuration Wizard after executing the *ORACLE_HOME*/bin/config.sh script (config.bat on Windows).

2.5 Understanding Oracle WebLogic Server Administration Domain Options

During installation, you have several options for choosing how the Oracle Identity Management components are installed in relation to an Oracle WebLogic Server administration domain. A domain includes a special WebLogic Server instance called the Administration Server, which is the central point from which you configure and manage all resources in the domain.

This section describes each domain option for installing Oracle Identity Management components:

- Create New Domain
- Extend Existing Domain
- Expand Cluster
- Configure Without a Domain

See: The "Understanding Oracle WebLogic Server Domains" chapter in the *Oracle Fusion Middleware Understanding Domain Configuration for Oracle WebLogic Server* guide for more information about Oracle WebLogic Server administration domains.

2.5.1 Create New Domain

Select the **Create New Domain** option to create a new Oracle WebLogic Server administration domain and install Oracle Identity Management components in it. When you install Oracle Identity Management components in a new domain, the Fusion Middleware Control management component and the Oracle WebLogic Administration Server are automatically deployed with them.

2.5.2 Extend Existing Domain

Select the **Extend Existing Domain** option to install Oracle Identity Management components in an existing Oracle WebLogic Server administration domain. When you install Oracle Identity Management components using this option, they are essentially "joining" an existing domain.

> **Note:** To install Oracle Identity Management components in an existing Oracle WebLogic Server administration domain, each Oracle WebLogic Server Home, Oracle Middleware Home, and Oracle Home directory in the domain must have identical directory paths and names.

If you want to install and configure Oracle Identity Management components in an existing Oracle WebLogic Server administration domain, by using either the Installer or the Oracle Identity Management 11*g* Release 1 (11.1.1) Configuration Wizard, the existing domain must have been created using the Oracle Identity Management 11*g* Release 1 (11.1.1) Installer. You cannot extend an existing domain for Oracle Identity Management components if the domain was created by another program, such as the Oracle SOA Installer or the Oracle WebLogic Server Configuration Wizard.

> **Note:** When you install components using the **Extend Existing Domain** option, you must provide some credentials for the existing domain, including the user name for the domain. You must enter the user name in ASCII characters only.

2.5.3 Expand Cluster

Select the **Expand Cluster** option to install Oracle Identity Management components in an Oracle WebLogic Server cluster for High Availability (HA). This document does not explain how to install Oracle Identity Management components in HA configurations. Refer to the following documents for more information:

- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

2.5.4 Configure Without a Domain

Select the **Configure without a Domain** option to install Oracle Identity Management components and configure them to be without domain membership.

> **Note:** Only the Oracle Internet Directory and Oracle Virtual Directory components are certified for installation without a domain.

For Oracle Internet Directory, the **Configure without a Domain** option is appropriate for environments that have *both* of the following conditions:

- You do not want to include Oracle Internet Directory in a WebLogic Server administration domain for management purposes.
- You do not want to manage Oracle Internet Directory using Fusion Middleware Control.

For Oracle Virtual Directory, the **Configure without a Domain** option is appropriate if you want to register Oracle Virtual Directory with a remote WebLogic Administration Server for management purposes, but you do not want to install Oracle WebLogic Server locally.

2.6 Installing Components on Separate Systems

You can install Oracle Fusion Middleware instances on separate systems. You can also distribute Oracle Fusion Middleware components over multiple systems, which is especially useful for Oracle Identity Management components. You might want distribute components to improve performance, security, scalability, and availability of Oracle Identity Management services.

The following are two (of many) examples of Oracle Identity Management deployments that benefit from distributing components over multiple systems:

- Oracle Internet Directory on one system, and Oracle Directory Services Manager and Oracle Directory Integration Platform on a separate system.
- Oracle Identity Management components use an Oracle Database to contain the Oracle Metadata Repository. The Oracle Identity Management components and the Oracle Database are installed on separate systems.

Note: If you install Oracle Identity Management components on a separate system from the database containing the Oracle Metadata Repository, the Oracle Identity Management components will need network access to the repository.

See: The following documents if you want to configure more than one Oracle Internet Directory against the same Oracle Metadata Repository:

- *Oracle Fusion Middleware Installation Planning Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

2.7 Executing the oracleRoot.sh Script on UNIX Platforms

During installation on UNIX platforms, the Installer prompts you to log in as the root user and run the oracleRoot.sh script. You must log in as the root user because the script creates files, edits files, and changes the permissions of certain Oracle executable files in the /usr/local/bin/ directory.

If the oracleRoot.sh script finds files of the same name, it prompts you to indicate whether or not to override the existing files. Back up the existing files (you can do this from another window), then overwrite them.

2.8 Understanding the State of Oracle Identity Management Components After Installation

This topic provides information about the state of Oracle Identity Management components after installation, including:

- Default SSL Configurations
- Default Passwords
- Ports Assigned Using Auto Port Configuration

2.8.1 Default SSL Configurations

By default, Oracle Internet Directory and Oracle Virtual Directory are installed with SSL configured. You must configure SSL for the Oracle WebLogic Administration Server and Oracle WebLogic Managed Server after installation.

> **See:** The *Oracle Fusion Middleware Administrator's Guide* for more information.

2.8.2 Default Passwords

By default, the passwords for all Oracle Identity Management components are set to the password for the Oracle Identity Management Instance. For security reasons, after installation, you should change the passwords of the various components so they have different values.

> **See:** The following documents for information about changing passwords for Oracle Identity Management components:
>
> - *Oracle Fusion Middleware Administrator's Guide*
> - Component-specific guides listed in the "Related Documents" section in this guide's Preface.

2.8.3 Ports Assigned Using Auto Port Configuration

When you use the Auto Port Configuration option during installation, the Installer follows specific steps to assign ports. The following information describes the default ports and port assignment logic the Installer uses to assign ports for various Oracle Identity Management components when you use the Auto Port Configuration option during installation.

- **Oracle Virtual Directory:**
  - Non-SSL port: 6501
  - SSL port: 7501
  - Admin port: 8899
  - HTTP port: 8080

  First, the Installer attempts to assign the default port. If the default port is unavailable, the Installer tries ports within a range of 50 from the default port. For example, when the Installer assigns the non-SSL port for Oracle Virtual Directory, it first attempts to assign 6501. If 6501 is unavailable, it tries ports from 6501 to 6551. The Installer uses this approach to assign all Oracle Virtual Directory ports.
- **Oracle Internet Directory:**
  - Non-SSL port: 3060
  - SSL port: 3131

  First, the Installer attempts to assign default ports. If the non-SSL port is unavailable, the Installer tries ports from 3061 to 3070, then from 13060 to 13070. Similarly, the Installer first attempts to assign 3131 as the SSL port, then ports from 3132 to 3141, and then from 13131 to 13141.
- **Oracle Identity Federation**: 7499

  First, the Installer attempts to assign the default port. If the default port is unavailable, the Installer tries ports in increments of one, that is: 7500, then 7501,

then 7502, and so on. The Installer tries ports up until 9000 to find an available port.

- **Oracle Directory Services Manager**: 7005

  First, the Installer attempts to assign the default port. If the default port is unavailable, the Installer tries ports in increments of one, that is: 7006, then 7007, then 7007, and so on. The Installer tries ports up until 9000 to find an available port.

- **Oracle WebLogic Administration Server**: 7001

3

Before Installing Oracle Identity Management

This chapter provides information you should review before installing Oracle Identity Management components. It includes the following topics:

3.1 System Requirements and Certification

Before performing any installation, read the system requirements and certification documentation to ensure that your environment meets the minimum installation requirements for the components you are installing. Both of these documents are available on Oracle Technology Network (OTN).

Oracle Fusion Middleware System Requirements, Prerequisites, and Specifications

The system requirements document covers information such as hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches:

http://www.oracle.com/technology/software/products/ias/files/fusion_requirements.htm

> **Note:** The system requirements document also covers Oracle Universal Installer Startup Requirements.

Oracle Fusion Middleware Supported System Configurations

The certification document covers supported installation types, platforms, operating systems, databases, JDKs, and third-party products:

http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html

3.2 Installing and Configuring Java Access Bridge (Windows Only)

If you are installing Oracle Identity Management on a Windows system, you have the option of installing and configuring Java Access Bridge for Section 508 Accessibility. This is only necessary if you require Section 508 Accessibility features:

1. Download Java Access Bridge from the following Web site:

   http://java.sun.com/javase/technologies/accessibility/accessbridge/

2. Install Java Access Bridge.
3. Copy `access-bridge.jar` and `jaccess-1_4.jar` from your installation location to the `jre\lib\ext` directory.
4. Copy the `WindowsAccessBridge.dll`, `JavaAccessBridge.dll`, and `JAWTAccessBridge.dll` files from your installation location to the `jre\bin` directory.
5. Copy the accessibility.properties file to the `jre\lib` directory.

3.3 Installing Oracle WebLogic Server and Creating the Oracle Middleware Home

Before you can install Oracle Identity Management 11*g* Release 1 (11.1.1) components, you must install Oracle WebLogic Server and create the Oracle Middleware Home directory.

Note: If you are installing Oracle Internet Directory 11*g* Release 1 (11.1.1) without an Oracle WebLogic administration domain, you do not need to install Oracle WebLogic.

Perform the following steps to install Oracle WebLogic Server and create the Oracle Middleware Home directory. You can refer to the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for complete information about installing Oracle WebLogic Server.

1. Insert the Oracle WebLogic Server CD-ROM or download the Oracle WebLogic Server Installer from the following Web site:

   http://www.oracle.com/technology/software/products/ias/htdocs/wls_main.html

2. Locate the appropriate executable file for your system, such as:

   - wls1032_linux32.bin for 32-bit Linux systems
   - wls1032_win32.exe for 32-bit Windows systems
   - wls1032_generic.jar for all 64-bit platforms

   The 32-bit executable files are bundled with the appropriate JDK version. If you use the 64-bit installer, you will need to invoke the installer with a supported JDK for your platform. This JDK must be installed on your system before you install Oracle WebLogic Server. Refer to the Oracle Fusion Middleware certification document for a list of supported JDKs for your platform:

   http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html

3. Run the Oracle WebLogic Server Installer directly from the CD-ROM, or copy the file to your local system and run it locally. For 64-bit installations:

   - Before running the installer, set the `DISPLAY` environment variable on your system.
   - Replace *`JAVA_HOME`* with the installation location of the supported JDK you installed for your platform.
   - Use the `-d64` flag when using 32/64-bit hybrid JDK's (such as the HP JDK for HP-UX and SUN JDK for Solaris SPARC).
   - Execute *`JAVA_HOME`*`/bin/java -version` (or *`JAVA_HOME`*`/bin/java -d64 -version` on 32/64-bit hybrid JDKs) to ensure that your *JAVA_HOME* refers to a 64-bit JDK.

   Examples for 32-bit systems:

   Linux:

   ```
   ./wls1032_linux32.bin
   ```

   Windows:

   ```
   wls1032_win32.exe
   ```

   Examples for 64-bit systems:

   UNIX:

   ```
   JAVA_HOME/bin/java -jar wls1032_generic.jar
   ```

   or

   ```
   JAVA_HOME/bin/java -d64 -jar wls1032_generic.jar
   ```

   Windows:

   ```
   JAVA_HOME\bin\java -jar wls1032_generic.jar
   ```

   Note: After you start the Oracle WebLogic Server Installer, the Welcome screen appears.

4. Click **Next**. The Choose Middleware Home Directory screen appears.
5. Select **Create a new Middleware Home** and identify the desired location for your new Middleware Home directory, which is the top-level directory for all Oracle Fusion Middleware products. The WebLogic Home directory will be created inside the Middleware Home directory.

   Note: If the Middleware Home directory already exists on your system, it must be an empty directory.

   Click **Next**. The Register for Security Updates screen appears.
6. Select whether or not you want to receive the latest product and security updates. If you choose not to receive anything, you will be asked to verify your selection before continuing.

   Click **Next**. The Choose Install Type screen appears.

7. Select **Typical** and click **Next**. The Choose Product Installation Directories screen appears.
8. Specify the desired location for your WebLogic Server Home directory and click **Next**.

   If you are installing Oracle WebLogic Server on a UNIX system, the Installation Summary screen appears. Go to step 9 now.

   If you are installing Oracle WebLogic Server on a Windows system, the Choose Shortcut Location screen appears. Specify a location where you want Windows to create a shortcut to Oracle products and click **Next**. The Installation Summary screen appears.
9. Click **Next** on the Installation Summary screen.

   The Installation Progress screen appears.
10. Click **Next**. The Installation Complete screen appears.
11. De-select **Run Quickstart** and click **Done** to exit the Installer.

Notes:

- The same user that installed Oracle WebLogic Server must install Oracle Identity Management.
- Do not log in to the Oracle WebLogic Server Administration Console during Oracle Identity Management installation.

3.4 Managing the Oracle WebLogic Server Node Manager Utility for Oracle Identity Management Installations

For Oracle Identity Management Installations that require Oracle WebLogic Server, you must perform the following steps after installing Oracle WebLogic Server and before installing Oracle Identity Management:

1. Verify the Oracle WebLogic Server Node Manager utility is stopped. If it is running, kill the process.
2. Determine if the nodemanager.properties file is present in the *WL_HOME*/common/nodemanager/ directory.
   - If the nodemanager.properties file is *not* present, continue installing Oracle Identity Management.
   - If the nodemanager.properties file *does* exist, open it and verify that the `ListenPort` parameter is included and that it is set. If the `ListenPort` parameter is not included or set, edit the nodemanager.properties file so that it is similar to the following, where *NODE_MANAGER_LISTEN_PORT* represents the port the Node Manager listens on, such as 5556:

     `ListenPort=`*`NODE_MANAGER_LISTEN_PORT`*

3.5 Installing Oracle Database

You must install an Oracle Database before you can install some Oracle Identity Management components, such as:

- Oracle Internet Directory

- Oracle Identity Federation, if you want to use an RDBMS data store

For the latest information about supported databases, visit the following Web site:

http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html

The database must be up and running to install the relevant Oracle Identity Management component. The database does not have to be on the same system where you are installing the Oracle Identity Management component.

The database must also be compatible with Oracle Repository Creation Utility (RCU), which is used to create the schemas that Oracle Identity Management components require. For information about RCU requirements, refer to the system requirements document at the following Web site:

http://www.oracle.com/technology/software/products/ias/files/fusion_requirements.htm

3.6 Creating Database Schema Using the Repository Creation Utility (RCU)

You must create and load the appropriate Oracle Fusion Middleware schema in your database before installing the following Oracle Identity Management components and configurations:

- Oracle Internet Directory, if you want to use an existing schema rather than create a new one using the Installer during installation.

> **Note:** When you install Oracle Internet Directory, you have the choice of using an existing schema or creating a new one using the Installer. If you want to use an existing schema, you must create it using the Repository Creation Utility (RCU) before you can install Oracle Internet Directory. If you choose to create a new schema during installation, the Installer creates the appropriate schema for you and you do not need to use the RCU.

- Oracle Identity Federation Advanced configurations that use RDBMS for the Federation Store, Session Store, Message Store, or Configuration Store.

You create and load Oracle Fusion Middleware schema in your database using the RCU, which is available in the Oracle Fusion Middleware 11g Release 1 (11.1.1) release media and on the Oracle Technology Network (OTN) Web site. You can access the OTN Web site at:

http://www.oracle.com/technology/index.html

> **Note:** RCU is available only on Linux and Windows platforms. Use the Linux RCU to create schemas on supported UNIX databases. Use Windows RCU to create schemas on supported Windows databases.

When you run RCU, create and load only the following schema for the Oracle Identity Management component you are installing—do not select any other schema available in RCU:

- For Oracle Internet Directory, select only the **Identity Management - Oracle Internet Directory** schema

- For Oracle Identity Federation, select only the **Identity Management - Oracle Identity Federation** schema

---

Note: When you create schema, be sure to remember the schema owner and password that is shown in RCU. For Oracle Identity Federation, it is of the form *PREFIX*_OIF. You will need to provide this information when configuring Oracle Identity Federation with RDBMS stores.

See: The *Oracle Fusion Middleware Repository Creation Utility User's Guide* for complete information.

3.7 Optional Environment-Specific Preparation

This topic describes optional environment-specific tasks you may want to perform before installing Oracle Identity Management 11*g* Release 1 (11.1.1). This topic includes the following sections:

- Using Symbolic Links
- Installing Oracle Identity Management on DHCP Hosts
- Installing Oracle Identity Management on a Multihomed System

3.7.1 Using Symbolic Links

If you want to install Oracle Identity Management using symbolic links, you must create them before installation. For example, you could create symbolic links for the installation by executing the following commands:

```
prompt> mkdir /home/basedir
prompt> ln -s /home/basedir /home/linkdir
```

Then, when you run the Installer to install Oracle Identity Management, you can specify `/home/linkdir` as the Oracle Home.

After installation, you cannot create symbolic links to the Oracle Home. Also, you cannot move the Oracle Home to a different location and create a symbolic link to the original Oracle Home.

3.7.2 Installing Oracle Identity Management on DHCP Hosts

If you plan to install Oracle Identity Management components on a DHCP server, you must ensure the Installer can resolve host names. This may require editing the /etc/hosts file on UNIX systems, and installing a loopback adapter on Windows systems. The following information provides general examples, you should alter these examples to make them specific to your environment.

On UNIX systems:

Configure the host to resolve host names to the loopback IP address by modifying the /etc/hosts file to contain the following entries. Replace the *variables* with the appropriate host and domain names:

```
127.0.0.1 hostname.domainname hostname
127.0.0.1 localhost.localdomain localhost
```

Confirm the host name resolves to the loopback IP address by executing the following command:

```
ping hostname.domainname
```

On Windows systems:

Install a loopback adapter on the DHCP server, which assigns a local IP address to your system.

After installing the adapter, add a line to the %SYSTEMROOT%\system32\drivers\etc\hosts file immediately after the localhost line and using the following format, where *IP_address* represents the local IP address of the loopback adapter:

```
IP_address   hostname.domainname   hostname
```

3.7.3 Installing Oracle Identity Management on a Multihomed System

You can install Oracle Identity Management components on a multihomed system. A multihomed system is associated with multiple IP addresses, typically achieved by having multiple network cards on the system. Each IP address is associated with a host name and you can create aliases for each host name.

The Installer retrieves the fully qualified domain name from the first entry in /etc/hosts file on UNIX, or the %SYSTEMROOT%\system32\drivers\etc\hosts file on Windows. For example, if your file looks like the following, the Installer retrieves myhost1.mycompany.com for configuration:

```
127.0.0.1 localhost.localdomain localhost
10.222.333.444 myhost1.mycompany.com myhost1
20.222.333.444 devhost2.mycompany.com devhost2
```

For specific network configuration of a system component, refer to the individual component's documentation listed in "Related Documents"for more information.

4

Performing Common Installation Tasks

This chapter describes tasks that are common to most Oracle Identity Management installations and configurations. It includes the following topics:

4.1 Starting an Installation

This topic explains the steps that are common to starting most Oracle Identity Management installations and configurations. It begins with starting the Installer and ends after you complete the steps on the Prerequisites Check screen.

> **Note:** Starting the Installer as the `root` user is not supported.

Perform the following steps to start an Oracle Identity Management installation:

1. Start the Installer by executing one of the following commands:

   UNIX: ./runInstaller

   Windows: *DRIVE*:\setup.exe

   After the Installer starts, the Welcome screen appears.
2. Click **Next** on the Welcome screen. The Select Installation Type screen appears.
3. Select **Install and Configure** and click **Next**. The Prerequisites Check screen appears.
4. Monitor the prerequisites checking.
   - If there is an issue, an error or warning message will appear. Investigate the issue and resolve it. After resolving the issue, click **Retry** to restart the prerequisite checks.

Note: You can proceed with the installation without resolving the issue by clicking **Continue**. However, failing to resolve the issue during the prerequisites checking may cause additional issues later in the installation.

- If all prerequisite checks pass inspection, click **Next**.

The Select Domain screen appears. Continue by referring to the appropriate procedure in this document for the installation you want to perform.

4.2 Creating the Inventory Directory (UNIX Only)

If you are installing on a UNIX system, and if this is the first time any Oracle product is being installed on your system with the Oracle Universal Installer, you will be asked to provide the location of an inventory directory. This is where the installer will set up subdirectories and maintain inventory data for each Oracle product that is installed on this system.

Follow the instructions in Table 4–1 to configure the inventory directory information:

Table 4–1 Inventory Directory and Group Screens

Screen	Description
Specify Inventory Directory	Specify the Oracle inventory directory and group permissions for that directory. The group must have write permissions to the Oracle inventory directory. Click **OK** to continue.
Inventory Location Confirmation	Run the createCentralInventory.sh script as root. Click **OK** to continue.

4.3 Identifying Installation Directories

This topic describes directories you must identify in most Oracle Identity Management installations and configurations—it does not describe one particular Installer screen. During installation, you will have to identify other component-specific directories not described in this topic.

The common directories described in this section include the following:

- Oracle Middleware Home Location
- Oracle Home Directory
- WebLogic Server Directory
- Oracle Instance Location
- Oracle Instance Name

4.3.1 Oracle Middleware Home Location

Identify the location of your Oracle Middleware Home directory. The Installer creates an Oracle Home directory for the component you are installing under the Oracle Middleware Home that you identify in this field. The Installer also creates an Oracle Common Home directory under the Oracle Middleware Home. The Oracle Common Home contains the binary and library files required for Oracle Enterprise Manager

Fusion Middleware Control and Java Required Files (JRF). There can be only one Oracle Common Home within each Oracle Middleware Home.

The Oracle Middleware Home directory is commonly referred to as *MW_HOME*.

> **Note:** To install Oracle Identity Management components in an existing Oracle WebLogic Server administration domain, each Oracle Middleware Home directory in the domain must have identical directory paths and names.

4.3.2 Oracle Home Directory

Enter a name for the component's Oracle Home directory. The Installer uses the name you enter in this field to create the Oracle Home directory under the location you enter in the Oracle Middleware Home Location field. The Installer installs the files (such as binaries and libraries) required to host the component in the Oracle Home directory.

The Oracle Home directory is commonly referred to as *ORACLE_HOME*.

> **Note:** To install Oracle Identity Management components in an existing Oracle WebLogic Server administration domain, each Oracle Home directory in the domain must have identical directory paths and names.

4.3.3 WebLogic Server Directory

Enter the path to your Oracle WebLogic Server Home directory. This directory contains the files required to host the Oracle WebLogic Server. It is commonly referred to as *WL_HOME*.

> **Note:** To install Oracle Identity Management components in an existing Oracle WebLogic Server administration domain, each Oracle WebLogic Server Home directory in the domain must have identical directory paths and names.

4.3.4 Oracle Instance Location

Enter the path to the location where you want to create the Oracle Instance directory. The Installer creates the Oracle Instance directory using the location you enter in this field and using the name you enter in the Oracle Instance Name field. Do not enter a path to an existing directory that contains files—if you enter a path to an existing directory, that directory must be empty.

The Installer installs the component's configuration files and runtime processes in the Oracle Instance directory. Runtime components will write only to this directory. You can identify any location on your system for the Oracle Instance directory—it does not have to reside inside the Oracle Middleware Home directory.

4.3.5 Oracle Instance Name

Enter a name for the Oracle Instance directory. The Installer uses the name you enter in this field to create the Oracle Instance directory at the location you specify in the Oracle Instance Location field. This directory is commonly referred to as *ORACLE_INSTANCE*.

Instance names are important because Oracle Fusion Middleware uses them to uniquely identify instances. If you install multiple Oracle Fusion Middleware instances on the same computer, for example, an Oracle Identity Management instance and an Oracle WebLogic Server instance, you must give them different names.

The name you enter for the Oracle Instance directory must:

- Contain only alphanumeric and underscore (_) characters
- Begin with an alphabetic character (a-z or A-Z)
- Consist of 4-30 characters
- Not contain the hostname or IP address of the computer

Note: You cannot change the Oracle Instance name after installation.

4.4 Determining Port Numbers

If you want to install an Oracle Identity Management 11*g* Release 1 (11.1.1) component against an existing Oracle Identity Management 11*g* Release 1 (11.1.1) component, you may need to identify the ports for the existing component. For example, if you want to install Oracle Directory Integration Platform 11*g* Release 1 (11.1.1) against an existing Oracle Internet Directory 11*g* Release 1 (11.1.1) component, you must identify its port when you install Oracle Directory Integration Platform.

You can get information about ports using the following:

- Fusion Middleware Control.

  Click **Ports** on the Fusion Middleware Control home page. This takes you to a page that lists all ports in use and the suggested port ranges for different components.

- $*ORACLE_INSTANCE*/config/OPMN/opmn/ports.prop

  Note: If you change a component's port number after installation, the ports.prop file is *not* updated.

- The $*ORACLE_INSTANCE*/bin/opmnctl status -l command to see port numbers of components managed by OPMN.

4.5 Completing an Installation

This topic explains the steps that are common to completing most Oracle Identity Management installations and configurations. It begins with the steps on the Installation Summary screen and ends after the Installation Complete screen.

When the Installation Summary screen appears, perform the following steps to complete the installation:

1. Verify the installation and configuration information on the Installation Summary screen.
   - Click **Save** to save the installation response file, which contains your responses to the Installer prompts and fields. You can use this response file to perform silent installations. Refer to Appendix B, "Performing Silent Installations" for more information.

Note: The installation response file is not saved by default—you must click **Save** to retain it.

- Click **Install**. The Installation Progress screen appears.

2. Monitor the progress of your installation. The location of the installation log file is listed for reference. After the installation progress reaches 100%, the Configuration Progress screen appears.

Note: On Unix systems, after the installation progress reaches 100%, a confirmation dialog box appears with information about the oracleRoot.sh script. Execute the script in different terminal as described in "Executing the oracleRoot.sh Script on UNIX Platforms" on page 2-6 and continue to the Configuration Progress screen.

3. Monitor the progress of the configuration. The location of the configuration log file is listed for reference. After the configuration progress reaches 100%, the Installation Complete screen appears.

4. By default the installation summary file, which can help you get started with administration, is saved to the *OUI_INVENTORY*/logs/ directory. The filename is of the form: installSummary*DATE*.txt. This file contains information about the configuration, such as locations of install directories and URLs for management components.

   If desired, you can click the **Save** button on the Installation Complete screen and choose a different name and location for the file.

   Click **Finish** to close and exit the Installer.

4.6 Optional: Configuring the Minimum Amount for Oracle WebLogic Server's Maximum Heap Size

After installing Oracle Identity Management 11*g* Release 1 (11.1.1), if you want to configure the minimum (lowest) level of maximum heap size (-Xmx) required for Oracle WebLogic Server to host Oracle Identity Management components, perform the steps in this section.

Note: This is an *optional* step, typically performed only for test, development, or demonstration environments.

The minimum (lowest) levels for maximum heap size are:

- Oracle WebLogic Administration Server: 512 MB
- Oracle WebLogic Managed Server: 256 MB

Perform the following steps to configure the heap size for Oracle WebLogic Administration Servers and Oracle WebLogic Managed Servers:

1. Open the setDomainEnv script (.sh or .bat) in the *MW_HOME*/user_projects/domains/*DOMAIN_NAME*/bin/ directory.

2. Locate the *last* occurrence of the `EXTRA_JAVA_PROPERTIES` entry.

3. In the last occurrence of the `EXTRA_JAVA_PROPERTIES` entry, locate the *last* occurrence of heap size parameters: `-Xmx`, `-Xms`, and so on.

   Note: These are the heap size parameters for the Oracle WebLogic Administration Server.

4. Set the heap size parameters (`-Xms` and `-Xmx`) for the Oracle WebLogic Administration Server as desired, for example: `-Xms256m` and `-Xmx512m`

5. To set the heap size parameters for the Oracle WebLogic Managed Server, enter the text in Example 4–1 immediately below the *last* occurrence of the `EXTRA_JAVA_PROPERTIES` entry and:

   - Set the heap size parameters (`-Xms` and `-Xmx`) as desired, for example: `-Xms256m -Xmx256m`
   - Replace `wls_ods1` with the name of the Oracle WebLogic Managed Server hosting Oracle Directory Services Manager.
   - Replace `wls_oif1` with the name the Oracle WebLogic Managed Server hosting Oracle Identity Federation.

Example 4–1 Heap Size Parameters for Oracle WebLogic Managed Server

```
if [ "${SERVER_NAME}" = "wls_ods1" -o  "${SERVER_NAME}" = "wls_oif1" ] ; then
        EXTRA_JAVA_PROPERTIES=" ${EXTRA_JAVA_PROPERTIES} -Xms256m -Xmx256m "
        export EXTRA_JAVA_PROPERTIES
fi
```

6. Save and close the setDomainEnv script.

7. Restart the Oracle WebLogic Administration Server and the Oracle WebLogic Managed Server by referring to Appendix A, "Starting and Stopping the Oracle Stack."

   Note: On UNIX systems, if you execute the `ps -ef` command and `grep` for `AdminServer` or the name of the Oracle WebLogic Managed Server (for example, `ps -ef | grep AdminServer` or `ps -ef | grep wls_oif1`), the output contains multiple occurrences of heap size parameters (-Xmx and -Xms).

   Be aware that the last occurrence of the heap size parameters in the output are effective and have precedence over the preceding occurrences.

4.7 Locating Installation Log Files

The Installer writes log files to the *ORACLE_INVENTORY_LOCATION*/logs directory on UNIX systems and to the *ORACLE_INVENTORY_LOCATION*\logs directory on Windows systems.

On UNIX systems, if you do not know the location of your Oracle Inventory directory, you can find it in the *ORACLE_HOME*/oraInst.loc file.

On Microsoft Windows systems, the default location for the inventory directory is C:\Program Files\Oracle\Inventory\logs.

The following install log files are written to the log directory:

- install*DATE-TIME_STAMP*.log
- install*DATE-TIME_STAMP*.out
- installActions*DATE-TIME_STAMP*.log
- installProfile*DATE-TIME_STAMP*.log
- oraInstall*DATE-TIME_STAMP*.err
- oraInstall*DATE-TIME_STAMP*.log

5

Installing and Configuring Oracle Internet Directory

This chapter explains how to install and configure Oracle Internet Directory. It includes the following topics:

- Installing and Configuring Oracle Internet Directory with Oracle Directory Services Manager and Fusion Middleware Control in a New WebLogic Administration Domain
- Installing and Configuring Oracle Internet Directory with Oracle Directory Integration Platform, Oracle Directory Services Manager, and Fusion Middleware Control in a New WebLogic Administration Domain
- Installing and Configuring Only Oracle Internet Directory in an Existing WebLogic Administration Domain
- Installing and Configuring Only Oracle Internet Directory Without a WebLogic Administration Domain
- Verifying Oracle Internet Directory
- Getting Started with Oracle Internet Directory After Installation

5.1 Installing and Configuring Oracle Internet Directory with Oracle Directory Services Manager and Fusion Middleware Control in a New WebLogic Administration Domain

This topic describes how to install and configure Oracle Internet Directory with Oracle Directory Services Manager and Fusion Middleware Control in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

5.1.1 Appropriate Deployment Environment

The installation and configuration described in this topic is appropriate for environments that have *all* of the following conditions:

- You want to manage Oracle Internet Directory using Fusion Middleware Control.
- You want Oracle Internet Directory to be in a WebLogic administration domain.

- There is no WebLogic Administration Server managing other 11*g* Release 1 (11.1.1) Oracle Directory Services components.
- You want to install Oracle Internet Directory and a WebLogic Administration Server colocated on the same host.

5.1.2 Components Deployed

Performing the installation and configuration in this section deploys the following components:

- WebLogic Administration Server
- Oracle Internet Directory
- Oracle Directory Services Manager
- Fusion Middleware Control

5.1.3 Dependencies

The installation and configuration in this section depends on the following:

- Oracle WebLogic Server
- Oracle Database
- If you want to use an existing schema, *Identity Management - Oracle Internet Directory* schema existing in the Oracle Database.

5.1.4 Procedure

Perform the following steps to install and configure Oracle Internet Directory with Oracle Directory Services Manager and Fusion Middleware Control in a new domain:

1. Install the Oracle Database for Oracle Internet Directory. Refer to "Installing Oracle Database" on page 3-4 for more information.
2. Decide if you want to create a new schema for Oracle Internet Directory using the Installer during installation or if you want to use an existing schema:
   - If you want to create a new schema using the Installer, continue this procedure by going to step 3 now.
   - If you want to use an existing schema, it must be present in the Oracle Internet Directory database before you can install Oracle Internet Directory. Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.
3. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
4. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
5. On the Select Domain screen, select **Create New Domain** and enter the following information:
   - Enter the user name for the new domain in the User Name field.
   - Enter the user password for the new domain in the User Password field.
   - Enter the user password again in the Confirm Password field.
   - Enter a name for the new domain in the Domain Name field.

Click **Next**. The Specify Installation Location screen appears.

6. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
7. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.
8. Select **Oracle Internet Directory**. The Oracle Directory Services Manager and Fusion Middleware Control management components are automatically selected for this installation.

   Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
9. Choose how you want the Installer to configure ports:
   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Specify Schema Database screen appears.
10. Choose whether to use an existing schema or to create a new one using the Installer.

Note: If you want to use an existing schema, it must currently reside in the database to continue with the installation. If it does not currently reside in the database, you must create it using the Repository Creation Utility now.

Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.

To use an existing schema:

a. Select **Use Existing Schema**.

b. Enter the database connection information in the Connect String field. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.

c. Enter the password for the existing ODS schema in the Password field.

d. Click **Next**.

Note: If your existing ODS and ODSSM schemas have different passwords, the Specify ODSSM Password screen will appear after you click **Next**. Enter the password for your existing ODSSM schema and click **Next**.

The Create Oracle Internet Directory screen appears.

e. Continue the installation by going to step 11 now.

To create a new schema:

a. Select **Create Schema**.

b. Enter the database connection information in the Connect String field. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.

c. Enter the name of the database user in the User Name field. The user you identify must have DBA privileges.

d. Enter the password for the database user in the Password field.

e. Click **Next**. The Enter OID Passwords screen appears.

f. Create a password for the new ODS schema by entering it in the ODS Schema Password field.

Enter it again in the Confirm ODS Schema Password field.

g. Create a password for the new ODSSM schema by entering it in the ODSSM Schema Password field.

Enter it again in the Confirm ODSSM Schema Password field.

h. Click **Next**. The Create Oracle Internet Directory screen appears.

11. Enter the following information for Oracle Internet Directory:

- Realm: Enter the location for your realm.
- Administrator Password: Enter the password for the Oracle Internet Directory administrator.
- Confirm Password: Enter the administrator password again.

Click **Next**. The Installation Summary screen appears.

12. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

5.2 Installing and Configuring Oracle Internet Directory with Oracle Directory Integration Platform, Oracle Directory Services Manager, and Fusion Middleware Control in a New WebLogic Administration Domain

This topic describes how to install and configure Oracle Internet Directory with Oracle Directory Integration Platform, Oracle Directory Services Manager, and Fusion Middleware Control in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment

5.2.1 Appropriate Deployment Environment

The installation and configuration described in this topic is appropriate for environments that have *both* of the following conditions:

- You want to install Oracle Internet Directory and Oracle Directory Integration Platform colocated on the same host.
- There is no WebLogic Administration Server managing other 11*g* Release 1 (11.1.1) Oracle Directory Services components.

5.2.2 Components Deployed

Performing the installation and configuration in this section deploys the following components:

- WebLogic Administration Server
- Oracle Internet Directory
- WebLogic Managed Server
- Oracle Directory Integration Platform
- Oracle Directory Services Manager
- Fusion Middleware Control

5.2.3 Dependencies

The installation and configuration in this section depends on the following:

- Oracle WebLogic Server
- Oracle Database
- If you want to use an existing schema, *Identity Management - Oracle Internet Directory* schema existing in the Oracle Database.

5.2.4 Procedure

Perform the following steps to install and configure Oracle Internet Directory with Oracle Directory Integration Platform, Oracle Directory Services Manager, and Fusion Middleware Control in a new domain:

1. Install the Oracle Database for Oracle Internet Directory. Refer to "Installing Oracle Database" on page 3-4 for more information.
2. Decide if you want to create a new schema for Oracle Internet Directory using the Installer during installation or if you want to use an existing schema:
   - If you want to create a new schema using the Installer, continue this procedure by going to step 3 now.
   - If you want to use an existing schema, it must be present in the Oracle Internet Directory database before you can install Oracle Internet Directory. Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.

3. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
4. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
5. On the Select Domain screen, select **Create New Domain** and enter the following information:
   - Enter the user name for the new domain in the User Name field.
   - Enter the user password for the new domain in the User Password field.
   - Enter the user password again in the Confirm Password field.
   - Enter a name for the new domain in the Domain Name field.

   Click **Next**. The Specify Installation Location screen appears.
6. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
7. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.
8. Select **Oracle Internet Directory** and **Oracle Directory Integration Platform**. The Oracle Directory Services Manager and Fusion Middleware Control management components are automatically selected for this installation.

   Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
9. Choose how you want the Installer to configure ports:
   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Specify Schema Database screen appears.
10. Choose whether to use an existing schema or to create a new one using the Installer.

    Note: If you want to use an existing schema, it must currently reside in the database to continue with the installation. If it does not currently reside in the database, you must create it using the Repository Creation Utility now.

    Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.

To use an existing schema:

a. Select **Use Existing Schema**.

b. Enter the database connection information in the Connect String field. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.

c. Enter the password for the existing ODS schema in the Password field.

d. Click **Next**.

Note: If your existing ODS and ODSSM schemas have different passwords, the Specify ODSSM Password screen will appear after you click **Next**. Enter the password for your existing ODSSM schema and click **Next**.

The Create Oracle Internet Directory screen appears.

e. Continue the installation by going to step 11 now.

To create a new schema:

a. Select **Create Schema**.

b. Enter the database connection information in the Connect String field. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.

c. Enter the name of the database user in the User Name field. The user you identify must have DBA privileges.

d. Enter the password for the database user in the Password field.

e. Click **Next**. The Enter OID Passwords screen appears.

f. Create a password for the new ODS schema by entering it in the ODS Schema Password field.

Enter it again in the Confirm ODS Schema Password field.

g. Create a password for the new ODSSM schema by entering it in the ODSSM Schema Password field.

Enter it again in the Confirm ODSSM Schema Password field.

h. Click **Next**. The Create Oracle Internet Directory screen appears.

11. Enter the following information for Oracle Internet Directory:

- Realm: Enter the location for your realm.
- Administrator Password: Enter the password for the Oracle Internet Directory administrator.
- Confirm Password: Enter the administrator password again.

Click **Next**. The Installation Summary screen appears.

12. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

5.3 Installing and Configuring Only Oracle Internet Directory in an Existing WebLogic Administration Domain

This topic describes how to install and configure only Oracle Internet Directory in an existing WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

5.3.1 Appropriate Deployment Environment

The installation and configuration described in this topic is appropriate for environments that have *both* of the following conditions:

- A WebLogic Administration Server is available to manage 11*g* Release 1 (11.1.1) Oracle Directory Services components and you want Oracle Internet Directory to join that domain.
- You want to install Oracle Internet Directory separately from the WebLogic Administration Server.

5.3.2 Components Deployed

Performing the installation and configuration in this section deploys only Oracle Internet Directory.

5.3.3 Dependencies

The installation and configuration in this section depends on the following:

- Oracle WebLogic Server
- Oracle Database
- If you want to use an existing schema, *Identity Management - Oracle Internet Directory* schema existing in the Oracle Database.

5.3.4 Procedure

Perform the following steps to install and configure only Oracle Internet Directory in an existing domain:

1. Install the Oracle Database for Oracle Internet Directory. Refer to "Installing Oracle Database" on page 3-4 for more information.
2. Decide if you want to create a new schema for Oracle Internet Directory using the Installer during installation or if you want to use an existing schema:
   - If you want to create a new schema using the Installer, continue this procedure by going to step 3 now.
   - If you want to use an existing schema, it must be present in the Oracle Internet Directory database before you can install Oracle Internet Directory. Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.

3. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
4. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
5. On the Select Domain screen, select **Extend Existing Domain** and enter the following information:
   - Enter the name of the host that contains the domain in the Host Name field.
   - Enter the Oracle WebLogic Server listen port in the Port field.
   - Enter the user name for the domain in the User Name field.
   - Enter the password for the domain user in the User Password field.

   Click **Next**. The Specify Installation Location screen appears.
6. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
7. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.
8. Select only **Oracle Internet Directory**. Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
9. Choose how you want the Installer to configure ports:
   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Specify Schema Database screen appears.
10. Choose whether to use an existing schema or to create a new one using the Installer.

Note: If you want to use an existing schema, it must currently reside in the database to continue with the installation. If it does not currently reside in the database, you must create it using the Repository Creation Utility now.

Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.

To use an existing schema:

a. Select **Use Existing Schema**.

b. Enter the database connection information in the Connect String field. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.

c. Enter the password for the existing ODS schema in the Password field.

d. Click **Next**.

Note: If your existing ODS and ODSSM schemas have different passwords, the Specify ODSSM Password screen will appear after you click **Next**. Enter the password for your existing ODSSM schema and click **Next**.

The Create Oracle Internet Directory screen appears.

e. Continue the installation by going to step 11 now.

To create a new schema:

a. Select **Create Schema**.

b. Enter the database connection information in the Connect String field. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.

c. Enter the name of the database user in the User Name field. The user you identify must have DBA privileges.

d. Enter the password for the database user in the Password field.

e. Click **Next**. The Enter OID Passwords screen appears.

f. Create a password for the new ODS schema by entering it in the ODS Schema Password field.

Enter it again in the Confirm ODS Schema Password field.

g. Create a password for the new ODSSM schema by entering it in the ODSSM Schema Password field.

Enter it again in the Confirm ODSSM Schema Password field.

h. Click **Next**. The Create Oracle Internet Directory screen appears.

11. Enter the following information for Oracle Internet Directory:

- Realm: Enter the location for your realm.
- Administrator Password: Enter the password for the Oracle Internet Directory administrator.
- Confirm Password: Enter the administrator password again.

Click **Next**. The Installation Summary screen appears.

12. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

5.4 Installing and Configuring Only Oracle Internet Directory Without a WebLogic Administration Domain

This topic describes how to install and configure only Oracle Internet Directory without a WebLogic administration domain. It includes the following sections:

5.4.1 Appropriate Deployment Environment

The installation and configuration described in this topic is appropriate for environments that have *both* of the following conditions:

- You do not want to include Oracle Internet Directory in a WebLogic administration domain for management purposes.
- You do not want to manage Oracle Internet Directory using Fusion Middleware Control.

5.4.2 Components Deployed

Performing the installation and configuration in this section deploys only Oracle Internet Directory.

5.4.3 Dependencies

The installation and configuration in this section depends on the following:

- Oracle Database
- If you want to use an existing schema, *Identity Management - Oracle Internet Directory* schema existing in the Oracle Database.

5.4.4 Procedure

Perform the following steps to install and configure only Oracle Internet Directory without a domain:

1. Install the Oracle Database for Oracle Internet Directory. Refer to "Installing Oracle Database" on page 3-4 for more information.
2. Decide if you want to create a new schema for Oracle Internet Directory using the Installer during installation or if you want to use an existing schema:
   - If you want to create a new schema using the Installer, continue this procedure by going to step 3 now.
   - If you want to use an existing schema, it must be present in the Oracle Internet Directory database before you can install Oracle Internet Directory. Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.
3. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.

4. Select **Configure without a Domain** on the Select Domain screen and click **Next**. The Specify Installation Location screen appears.
5. Enter the following information in each field:
   - **Oracle Middleware Home Location**: If an Oracle Middleware Home directory already exists, enter the path to it in this field. If an Oracle Middleware Home directory *does not* exist, enter a path to the location where you want the Installer to create the directory that will contain the Oracle Common Home and Oracle Home directories. The Installer creates an Oracle Common Home directory and an Oracle Home directory inside the directory you identify in this field.

     The Oracle Middleware Home directory is commonly referred to as *MW_HOME*.

     Note: The Oracle Middleware Home directory is *not* required to contain an Oracle WebLogic Server installation.

   - **Oracle Home Directory**: Enter a name for the Oracle Home directory. The Installer uses the name you enter in this field to create the Oracle Home directory under the location you enter in the Oracle Middleware Home Location field. The Oracle Home directory is commonly referred to as *ORACLE_HOME*.
   - **Oracle Instance Location**: Enter the directory path to the location where you want to create the Oracle Instance directory. The Installer creates the Oracle Instance directory using the location you enter in this field and using the name you enter in the Oracle Instance Name field. You can identify any location on your system for the Oracle Instance directory—it does not have to reside inside the Oracle Middleware Home directory.
   - **Oracle Instance Name**: Enter a name for the Oracle Instance directory. The Installer uses the name you enter in this field to create the Oracle Instance directory at the location you specify in the Oracle Instance Location field. This directory is commonly referred to as *ORACLE_INSTANCE*.

   After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
6. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.
7. On the Configure Components screen, select only **Oracle Internet Directory**. Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
8. Choose how you want the Installer to configure ports:
   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.

- Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

Click **Next**. The Specify Schema Database screen appears.

9. Choose whether to use an existing schema or to create a new one using the Installer.

Note: If you want to use an existing schema, it must currently reside in the database to continue with the installation. If it does not currently reside in the database, you must create it using the Repository Creation Utility now.

Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.

To use an existing schema:

a. Select **Use Existing Schema**.

b. Enter the database connection information in the Connect String field. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.

c. Enter the password for the existing ODS schema in the Password field.

d. Click **Next**.

Note: If your existing ODS and ODSSM schemas have different passwords, the Specify ODSSM Password screen will appear after you click **Next**. Enter the password for your existing ODSSM schema and click **Next**.

The Create Oracle Internet Directory screen appears.

e. Continue the installation by going to step 10 now.

To create a new schema:

a. Select **Create Schema**.

b. Enter the database connection information in the Connect String field. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.

c. Enter the name of the database user in the User Name field. The user you identify must have DBA privileges.

d. Enter the password for the database user in the Password field.

e. Click **Next**. The Enter OID Passwords screen appears.

f. Create a password for the new ODS schema by entering it in the ODS Schema Password field.

Enter it again in the Confirm ODS Schema Password field.

g. Create a password for the new ODSSM schema by entering it in the ODSSM Schema Password field.

   Enter it again in the Confirm ODSSM Schema Password field.

h. Click **Next**. The Create Oracle Internet Directory screen appears.

10. Enter the following information for Oracle Internet Directory:

    - Realm: Enter the location for your realm.
    - Administrator Password: Enter the password for the Oracle Internet Directory administrator.
    - Confirm Password: Enter the administrator password again.

    Click **Next**. The Installation Summary screen appears.

11. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

Note: If you perform this installation and configuration, but later decide you want to manage Oracle Internet Directory using Fusion Middleware Control, you must register Oracle Internet Directory with a WebLogic Administration Server.

Refer to the "Registering an Oracle Instance or Component with the WebLogic Server" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for more information.

5.5 Verifying Oracle Internet Directory

Verify the Oracle Internet Directory installation by:

- Executing the `$ORACLE_INSTANCE/bin/opmnctl status -l` command.
- Executing the `$ORACLE_HOME/bin/ldapbind` command on the Oracle Internet Directory non-SSL and SSL ports.

5.6 Getting Started with Oracle Internet Directory After Installation

After installing Oracle Internet Directory, refer to the "Getting Started with Oracle Internet Directory" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

6

Installing and Configuring Oracle Virtual Directory

This chapter explains how to install and configure Oracle Virtual Directory. It includes the following topics:

- Installing and Configuring Oracle Virtual Directory with Oracle Directory Services Manager and Fusion Middleware Control in a New WebLogic Administration Domain
- Installing and Configuring Only Oracle Virtual Directory in an Existing WebLogic Administration Domain
- Installing and Configuring Only Oracle Virtual Directory Without a WebLogic Administration Domain
- Verifying Oracle Virtual Directory
- Getting Started with Oracle Virtual Directory After Installation

6.1 Installing and Configuring Oracle Virtual Directory with Oracle Directory Services Manager and Fusion Middleware Control in a New WebLogic Administration Domain

This topic describes how to install and configure Oracle Virtual Directory with Oracle Directory Services Manager and Fusion Middleware Control in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

6.1.1 Appropriate Deployment Environment

The installation and configuration described in this topic is appropriate for environments that have *all* of the following conditions:

- You want to manage Oracle Virtual Directory using Fusion Middleware Control.
- You want Oracle Virtual Directory to be in a WebLogic administration domain.
- There is no WebLogic Administration Server managing other 11*g* Release 1 (11.1.1) Oracle Directory Services components.

- You want to install Oracle Virtual Directory and a WebLogic Administration Server colocated on the same host.

6.1.2 Components Deployed

Performing the installation and configuration in this section deploys the following components.

- WebLogic Administration Server
- Oracle Virtual Directory
- Oracle Directory Services Manager
- Fusion Middleware Control

6.1.3 Dependencies

The installation and configuration in this section depends on Oracle WebLogic Server.

6.1.4 Procedure

Perform the following steps to install and configure Oracle Virtual Directory with Oracle Directory Services Manager and Fusion Middleware Control in a new domain:

1. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
2. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
3. On the Select Domain screen, select **Create New Domain** and enter the following information:
   - Enter the user name for the new domain in the User Name field.
   - Enter the user password for the new domain in the User Password field.
   - Enter the user password again in the Confirm Password field.
   - Enter a name for the new domain in the Domain Name field.

   Click **Next**. The Specify Installation Location screen appears.
4. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
5. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.
6. Select only **Oracle Virtual Directory**. The Oracle Directory Services Manager and Fusion Middleware Control management components are automatically selected for this installation.

Ensure no other components are selected and click **Next**. The Configure Ports screen appears.

7. Choose how you want the Installer to configure ports:
   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Specify Oracle Virtual Directory Information screen appears.
8. Enter the following information:
   - LDAP v3 Name Space: Enter the name space for Oracle Virtual Directory. The default value is dc=us,dc=oracle,dc=com.
   - HTTP Web Gateway: Select this option to enable the Oracle Virtual Directory HTTP Web Gateway.
   - Secure: Select this option if you enabled the HTTP Web Gateway and you want to secure it using SSL.
   - Administrator User Name: Enter the user name for the Oracle Virtual Directory administrator. The default value is cn=orcladmin.
   - Password: Enter the password for the Oracle Virtual Directory administrator.
   - Confirm Password: Enter the password for the Oracle Virtual Directory administrator again.
   - Configure Administrative Server in secure mode: Select this option to secure the Oracle Virtual Directory Administrative Listener using SSL. This option is selected by default. Oracle recommends selecting this option.

   Click **Next**. The Installation Summary screen appears.
9. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

6.2 Installing and Configuring Only Oracle Virtual Directory in an Existing WebLogic Administration Domain

This topic describes how to install and configure only Oracle Virtual Directory in an existing WebLogic administration domain. It includes the following sections:

6.2.1 Appropriate Deployment Environment

The installation and configuration described in this topic is appropriate for environments that have *both* of the following conditions:

- A WebLogic Administration Server is available to manage 11*g* Release 1 (11.1.1) Oracle Directory Services components and you want Oracle Virtual Directory to join that domain.

- You want to install Oracle Virtual Directory separately from the WebLogic Administration Server.

6.2.2 Components Deployed

Performing the installation and configuration in this section deploys only Oracle Virtual Directory.

6.2.3 Dependencies

The installation and configuration in this section depends on Oracle WebLogic Server.

6.2.4 Procedure

Perform the following steps to install and configure only Oracle Virtual Directory in an existing domain:

1. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
2. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
3. On the Select Domain screen, select **Extend Existing Domain** and enter the following information:
   a. Enter the name of the host that contains the domain in the Host Name field.
   b. Enter the Oracle WebLogic Server listen port in the Port field.
   c. Enter the user name for the domain in the User Name field.
   d. Enter the password for the domain user in the User Password field.

   Click **Next**. The Specify Installation Location screen appears.
4. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
5. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.
6. Select only **Oracle Virtual Directory**. Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
7. Choose how you want the Installer to configure ports:
   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

Click **Next**. The Specify Oracle Virtual Directory Information screen appears.

8. Enter the following information:
   - LDAP v3 Name Space: Enter the name space for Oracle Virtual Directory. The default value is dc=us,dc=oracle,dc=com.
   - HTTP Web Gateway: Select this option to enable the Oracle Virtual Directory HTTP Web Gateway.
   - Secure: Select this option if you enabled the HTTP Web Gateway and you want to secure it using SSL.
   - Administrator User Name: Enter the user name for the Oracle Virtual Directory administrator. The default value is cn=orcladmin.
   - Password: Enter the password for the Oracle Virtual Directory administrator.
   - Confirm Password: Enter the password for the Oracle Virtual Directory administrator again.
   - Configure Administrative Server in secure mode: Select this option to secure the Oracle Virtual Directory Administrative Listener using SSL. This option is selected by default. Oracle recommends selecting this option.

   Click **Next**. The Installation Summary screen appears.
9. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

6.3 Installing and Configuring Only Oracle Virtual Directory Without a WebLogic Administration Domain

This topic describes how to install and configure only Oracle Virtual Directory without a WebLogic administration domain. It includes the following sections:

6.3.1 Appropriate Deployment Environment

Perform the installation and configuration in this topic if you want to register Oracle Virtual Directory with a remote WebLogic Administration Server for management purposes, but you do not want to install Oracle WebLogic Server locally.

> **Note:** To manage Oracle Virtual Directory using Fusion Middleware Control in this environment, you must register Oracle Virtual Directory with the remote WebLogic Administration Server after installation.

6.3.2 Components Deployed

Performing the installation and configuration in this section deploys only Oracle Virtual Directory.

6.3.3 Dependencies

The installation and configuration in this section depends on Oracle WebLogic Server.

6.3.4 Procedure

Perform the following steps to install and configure only Oracle Virtual Directory without a domain:

1. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
2. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
3. Select **Configure without a Domain** on the Select Domain screen and click **Next**. The Specify Installation Location screen appears.
4. Enter the following information in each field:
   - **Oracle Middleware Home Location**: If an Oracle Middleware Home directory already exists, enter the path to it in this field. If an Oracle Middleware Home directory *does not* exist, enter a path to the location where you want the Installer to create the directory that will contain the Oracle Common Home and Oracle Home directories. The Installer creates an Oracle Common Home directory and an Oracle Home directory inside the directory you identify in this field.

     The Oracle Middleware Home directory is commonly referred to as *MW_HOME*.

     Note: The Oracle Middleware Home directory is *not* required to contain an Oracle WebLogic Server installation.

   - **Oracle Home Directory**: Enter a name for the Oracle Home directory. The Installer uses the name you enter in this field to create the Oracle Home directory under the location you enter in the Oracle Middleware Home Location field. The Oracle Home directory is commonly referred to as *ORACLE_HOME*.
   - **Oracle Instance Location**: Enter the directory path to the location where you want to create the Oracle Instance directory. The Installer creates the Oracle Instance directory using the location you enter in this field and using the name you enter in the Oracle Instance Name field. You can identify any location on your system for the Oracle Instance directory—it does not have to reside inside the Oracle Middleware Home directory.
   - **Oracle Instance Name**: Enter a name for the Oracle Instance directory. The Installer uses the name you enter in this field to create the Oracle Instance directory at the location you specify in the Oracle Instance Location field. This directory is commonly referred to as *ORACLE_INSTANCE*.

   After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
5. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.

- If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
- If you do not want to be notified about security issues, leave all fields empty.

Click **Next**. The Configure Components screen appears.

6. Select only **Oracle Virtual Directory**. Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
7. Choose how you want the Installer to configure ports:
   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Specify Oracle Virtual Directory Information screen appears.
8. Enter the following information:
   - LDAP v3 Name Space: Enter the name space for Oracle Virtual Directory. The default value is dc=us,dc=oracle,dc=com.
   - HTTP Web Gateway: Select this option to enable the Oracle Virtual Directory HTTP Web Gateway.
   - Secure: Select this option if you enabled the HTTP Web Gateway and you want to secure it using SSL.
   - Administrator User Name: Enter the user name for the Oracle Virtual Directory administrator. The default value is cn=orcladmin.
   - Password: Enter the password for the Oracle Virtual Directory administrator.
   - Confirm Password: Enter the password for the Oracle Virtual Directory administrator again.
   - Configure Administrative Server in secure mode: Select this option to secure the Oracle Virtual Directory Administrative Listener using SSL. This option is selected by default. Oracle recommends selecting this option.

   Click **Next**. The Installation Summary screen appears.
9. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.
10. Execute the following command to register Oracle Virtual Directory with the WebLogic Administration Server. Registering with the WebLogic Administration Server allows you to manage Oracle Virtual Directory using Fusion Middleware Control.

```
$ORACLE_INSTANCE/bin/opmnctl registerinstance
 -adminHost HOSTNAME
 -adminPort WEBLOGIC_PORT
 -adminUsername WEBLOGIC_ADMIN_USERNAME
```

> **Note:** You will be prompted for the WebLogic administrator's user name and password.

For example:

```
$ORACLE_INSTANCE/bin/opmnctl registerinstance \
 -adminHost myhost \
 -adminPort 7001 \
 -adminUsername weblogic \
```

Note: The default administrative port on the WebLogic Administration Server is 7001.

6.4 Verifying Oracle Virtual Directory

Verify the Oracle Virtual Directory installation by:

- Executing the `$ORACLE_INSTANCE/bin/opmnctl status -l` command.
- Executing the `$ORACLE_HOME/bin/ldapbind` command on the Oracle Virtual Directory non-SSL and SSL ports.

6.5 Getting Started with Oracle Virtual Directory After Installation

After installing Oracle Virtual Directory, refer to the "Getting Started with Administering Oracle Virtual Directory" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

7

Installing and Configuring Oracle Directory Integration Platform

This chapter explains how to install and configure Oracle Directory Integration Platform. It includes the following topics:

- Installing and Configuring Oracle Directory Integration Platform with Fusion Middleware Control in a New WebLogic Administration Domain
- Installing and Configuring Only Oracle Directory Integration Platform in an Existing WebLogic Administration Domain
- Installing Oracle Directory Integration Platform when Oracle Internet Directory is Running in SSL Mode 2 - Server Only Authentication
- Verifying Oracle Directory Integration Platform
- Getting Started with Oracle Directory Integration Platform After Installation

7.1 Installing and Configuring Oracle Directory Integration Platform with Fusion Middleware Control in a New WebLogic Administration Domain

This topic describes how to install and configure Oracle Directory Integration Platform with Fusion Middleware Control in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

7.1.1 Appropriate Deployment Environment

The installation and configuration described in this topic is appropriate if there is no WebLogic Administration Server managing other 11*g* Release 1 (11.1.1) Oracle Directory Services components and Oracle Internet Directory is installed without a domain.

7.1.2 Components Deployed

Performing the installation and configuration in this section deploys the following components:

- WebLogic Managed Server

- Oracle Directory Integration Platform
- WebLogic Administration Server
- Fusion Middleware Control

7.1.3 Dependencies

The installation and configuration in this section depends on the following:

- Oracle WebLogic Server
- Oracle Internet Directory
- Oracle Database for Oracle Internet Directory
- *Identity Management - Oracle Internet Directory* schema existing in the Oracle Internet Directory database.

7.1.4 Procedure

Perform the following steps to install and configure Oracle Directory Integration Platform with Fusion Middleware Control in a new domain:

1. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
2. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
3. On the Select Domain screen, select **Create New Domain** and enter the following information:
   - Enter the user name for the new domain in the User Name field.
   - Enter the user password for the new domain in the User Password field.
   - Enter the user password again in the Confirm Password field.
   - Enter a name for the new domain in the Domain Name field.

   Click **Next**. The Specify Installation Location screen appears.
4. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
5. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.
6. Select only **Oracle Directory Integration Platform**. The Fusion Middleware Control management component is automatically selected for this installation.

   Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
7. Choose how you want the Installer to configure ports:

- Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
- Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

Click **Next**. The Specify OID Details screen appears.

8. Identify the Oracle Internet Directory for Oracle Directory Integration Platform by entering the following information:
   - Hostname: Enter the hostname or IP address of the Oracle Internet Directory host.
   - Port: Enter the Oracle Internet Directory LDAP SSL port.
   - User Name: Enter the user name of the Oracle Internet Directory Administrator.
   - Password: Enter the password for the user name Oracle Directory Integration Platform will use to connect to Oracle Internet Directory.

   Click **Next**. The Specify Schema Database screen appears.
9. Enter the following information about the Oracle Internet Directory schema:
   - Connect String: Enter the database connection information. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
   - Password: Enter the password for the ODSSM schema in the Password field.

   Click **Next**. The Installation Summary screen appears.
10. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

7.2 Installing and Configuring Only Oracle Directory Integration Platform in an Existing WebLogic Administration Domain

This topic describes how to install and configure only Oracle Directory Integration Platform in an existing WebLogic administration domain. It includes the following sections:

7.2.1 Appropriate Deployment Environment

The installation and configuration described in this topic is appropriate for the following environments:

An environment that has the following condition:

- A WebLogic Administration Server is managing an 11*g* Release 1 (11.1.1) Oracle Internet Directory component and you want Oracle Directory Integration Platform to join that domain.

An environment that has the following condition:

- A WebLogic Administration Server is managing other 11*g* Release 1 (11.1.1) Oracle Directory Services—but not Oracle Internet Directory, which is installed without a domain.

7.2.2 Components Deployed

Performing the installation and configuration in this section deploys the following components:

- WebLogic Managed Server
- Oracle Directory Integration Platform

7.2.3 Dependencies

The installation and configuration in this section depends on the following:

- Oracle WebLogic Server
- Oracle Internet Directory
- Oracle Database for Oracle Internet Directory
- *Identity Management - Oracle Internet Directory* schema existing in the Oracle Internet Directory database.

7.2.4 Procedure

Perform the following steps to install and configure only Oracle Directory Integration Platform in an existing domain:

1. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
2. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
3. On the Select Domain screen, select **Extend Existing Domain** and enter the following information:
   - Enter the name of the host that contains the domain in the Host Name field.
   - Enter the Oracle WebLogic Server listen port in the Port field.
   - Enter the user name for the domain in the User Name field.
   - Enter the password for the domain user in the User Password field.

   Click **Next**. The Specify Installation Location screen appears.
4. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
5. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.

- If you do not want to be notified about security issues, leave all fields empty.

Click **Next**. The Configure Components screen appears.

6. Select only **Oracle Directory Integration Platform**. Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
7. Choose how you want the Installer to configure ports:
   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Specify OID Details screen appears.
8. Identify the Oracle Internet Directory for Oracle Directory Integration Platform by entering the following information:
   - Hostname: Enter the hostname or IP address of the Oracle Internet Directory host.
   - Port: Enter the Oracle Internet Directory LDAP SSL port.
   - User Name: Enter the user name of the Oracle Internet Directory Administrator.
   - Password: Enter the password for the user name Oracle Directory Integration Platform will use to connect to Oracle Internet Directory.

   Click **Next**. The Specify Schema Database screen appears.
9. Enter the following information about the Oracle Internet Directory schema:
   - Connect String: Enter the database connection information. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
   - Password: Enter the password for the ODSSM schema in the Password field.

   Click **Next**. The Installation Summary screen appears.
10. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

7.3 Installing Oracle Directory Integration Platform when Oracle Internet Directory is Running in SSL Mode 2 - Server Only Authentication

You cannot install Oracle Directory Integration Platform 11*g* Release 1 (11.1.1) when Oracle Internet Directory is already installed and running in SSL Mode 2 - Server Only Authentication.

If Oracle Internet Directory is already installed and running in SSL Mode 2 - Server Only Authentication, you must perform the following steps to install Oracle Directory Integration Platform 11*g* Release 1 (11.1.1):

1. Configure Oracle Internet Directory to temporarily run in SSL Mode 0 - No Authentication.

Refer to the "Configuring Secure Sockets Layer (SSL)" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for complete information.

2. Install Oracle Directory Integration Platform using the appropriate procedure in this chapter.
3. Configure Oracle Internet Directory to run in SSL Mode 2 - Server Only Authentication again. Refer to the "Configuring Secure Sockets Layer (SSL)" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.
4. Configure Oracle Directory Integration Platform to run in SSL Mode 2 by referring to the following sections in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*:
   - Configuring Oracle Directory Integration Platform for SSL Mode 2 - Server Only Authentication
   - Managing the SSL Certificates of Oracle Internet Directory and Connected Directories

7.4 Verifying Oracle Directory Integration Platform

Verify the Oracle Directory Integration Platform installation using the `dipStatus` command, which is located in the $*ORACLE_HOME*/bin/ directory.

> **Note:** You must set the *WL_HOME* and *ORACLE_HOME* environment variables before executing the `dipStatus` command.

The following is the syntax for the `dipStatus` command:

```
$ORACLE_HOME/bin/dipStatus -h HOST -p PORT -D wlsuser [-help]
```

- `-h | -host` identifies the Oracle WebLogic Server where Oracle Directory Integration Platform is deployed.
- `-p | -port` identifies the listening port of the Oracle WebLogic Managed Server where Oracle Directory Integration Platform is deployed.
- `-D | -wlsuser` identifies the Oracle WebLogic Server login ID.

> **Note:** You will be prompted for the Oracle WebLogic Server login password. You cannot provide the password as a command-line argument.
>
> Best security practice is to provide a password only in response to a prompt from the command. If you must execute `dipStatus` from a script, you can redirect input from a file containing the Oracle WebLogic Server password. Use file permissions to protect the file and delete it when it is no longer necessary.

7.5 Getting Started with Oracle Directory Integration Platform After Installation

After you install Oracle Directory Integration Platform, no additional configuration is needed. The next step is to create synchronization profiles.

The *Oracle Fusion Middleware Integration Guide for Oracle Identity Management* explains how to manage Oracle Directory Integration Platform. For information about creating synchronization profiles using Oracle Enterprise Manager Fusion Middleware Control Console, refer to the "Managing Synchronization Profiles Using Fusion Middleware Control" section in that guide.

8

Installing and Configuring Oracle Directory Services Manager

This chapter explains how to install and configure Oracle Directory Services Manager. It includes the following topics:

- Installing and Configuring Only Oracle Directory Services Manager in a New WebLogic Administration Domain
- Installing and Configuring Only Oracle Directory Services Manager in an Existing WebLogic Administration Domain
- Verifying Oracle Directory Services Manager
- Getting Started with Oracle Directory Services Manager After Installation

8.1 Installing and Configuring Only Oracle Directory Services Manager in a New WebLogic Administration Domain

This topic describes how to install and configure only Oracle Directory Services Manager in a new WebLogic administration domain. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

8.1.1 Appropriate Deployment Environment

The installation and configuration described in this topic is appropriate if Oracle Internet Directory was installed without a domain and you want to manage it using Oracle Directory Services Manager.

8.1.2 Components Deployed

Performing the installation and configuration in this section deploys the following components:

- WebLogic Managed Server
- Oracle Directory Services Manager
- WebLogic Administration Server
- Fusion Middleware Control

8.1.3 Dependencies

The installation and configuration in this section depends on Oracle WebLogic Server.

8.1.4 Procedure

Perform the following steps to install only Oracle Directory Services Manager in a new domain:

1. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
2. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
3. On the Select Domain screen, select **Create New Domain** and enter the following information:
   - Enter the user name for the new domain in the User Name field.
   - Enter the user password for the new domain in the User Password field.
   - Enter the user password again in the Confirm Password field.
   - Enter a name for the new domain in the Domain Name field.

   Click **Next**. The Specify Installation Location screen appears.
4. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
5. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.
6. Select only **Oracle Directory Services Manager**. The Fusion Middleware Control management component is automatically selected for this installation.

   Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
7. Choose how you want the Installer to configure ports:
   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Installation Summary screen appears.
8. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

8.2 Installing and Configuring Only Oracle Directory Services Manager in an Existing WebLogic Administration Domain

This topic describes how to install and configure only Oracle Directory Services Manager in an existing WebLogic administration domain. It includes the following sections:

8.2.1 Appropriate Deployment Environment

The installation and configuration described in this topic is appropriate if you want to deploy an additional Oracle Directory Services Manager component in an existing domain.

8.2.2 Components Deployed

Performing the installation and configuration in this section deploys the following components:

- WebLogic Managed Server
- Oracle Directory Services Manager

8.2.3 Dependencies

The installation and configuration in this section depends on Oracle WebLogic Server.

8.2.4 Procedure

Perform the following steps to install and configure only Oracle Directory Services Manager in an existing domain:

1. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
2. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
3. On the Select Domain screen, select **Extend Existing Domain** and enter the following information:
   a. Enter the name of the host that contains the domain in the Host Name field.
   b. Enter the Oracle WebLogic Server listen port in the Port field.
   c. Enter the user name for the domain in the User Name field.
   d. Enter the password for the domain user in the User Password field.

   Click **Next**. The Specify Installation Location screen appears.
4. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
5. Choose how you want to be notified about security issues:

- If you want to be notified about security issues through email, enter your email address in the Email field.
- If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
- If you do not want to be notified about security issues, leave all fields empty.

Click **Next**. The Configure Components screen appears.

6. Select only **Oracle Directory Services Manager**. Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
7. Choose how you want the Installer to configure ports:
   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Installation Summary screen appears.
8. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

8.3 Verifying Oracle Directory Services Manager

To verify the Oracle Directory Services Manager installation, enter the following URL into your browser's address field:

http://*host*:*port*/odsm

- *host* represents the name of the WebLogic Managed Server hosting Oracle Directory Services Manager.
- *port* represents the WebLogic Managed Server listen port. You can determine the exact port number by examining the following file:

  `$MW_HOME/ORACLE_IDENTITY_MANAGEMENT_DOMAIN/servers/MANAGED_SERVER/data/nodemanager/MANAGED_SERVER.url`

Oracle Directory Services Manager is installed and running if the Welcome to Oracle Directory Services Manage screen appears.

Note: While the appearance of the Welcome screen verifies Oracle Directory Services Manager is installed and running, you cannot connect to Oracle Internet Directory or Oracle Virtual Directory from Oracle Directory Services Manager without the appropriate credentials.

8.4 Getting Started with Oracle Directory Services Manager After Installation

After you install Oracle Directory Services Manager, no additional configuration is needed. The next step is to log in to Oracle Internet Directory or Oracle Virtual Directory. The process for logging in to both directory servers is the same. Information about logging in to both Oracle Internet Directory and Oracle Virtual Directory

provided below so you can learn more about Oracle Directory Services Manager in the context of each directory server.

- For information about logging in to Oracle Internet Directory from Oracle Directory Services Manager, refer to the "Logging in to the Directory Server from Oracle Directory Services Manager" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.
- For information about logging in to Oracle Virtual Directory from Oracle Directory Services Manager, refer to the "Logging in to the Directory Server from Oracle Directory Services Manager" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

9

Installing and Configuring Oracle Identity Federation

This chapter explains how to install and configure Oracle Identity Federation. It includes the following topics:

9.1 Using the Information in This Chapter

Oracle Identity Federation deployments vary greatly. As described in the following topics, there are several components, and several options for those components, that comprise an Oracle Identity Federation deployment.

Use this chapter as a starting point for your Oracle Identity Federation deployment, as it does not describe every possible installation and configuration. You should also use the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*, which provides additional and detailed deployment information, to supplement the information in this chapter.

9.2 Understanding Oracle Identity Federation Deployments

When you install Oracle Identity Federation 11*g* Release 1 (11.1.1), a WebLogic Managed Server is created and the Oracle Identity Federation J2EE application is installed on it. If you install Oracle Identity Federation in a new Oracle WebLogic Server administration domain by selecting the Create Domain option, the Fusion Middleware Control management component is also deployed.

Oracle Identity Federation functionality depends on several components and modules. You can integrate and configure these components and modules during or after the Oracle Identity Federation installation.

The following is a list and brief description of some of the components and modules that determine Oracle Identity Federation functionality. Refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation* for complete information.

- **Authentication Engine**: The module that challenges users when they log in.
- **User Data Store**: The repository containing the identity information of the users the Oracle Identity Federation system authenticates.
- **Federation Data Store**: The repository containing federated user account linking data.
- **Service Provider (SP) Integration Engine**: The module that creates a local authenticated session for the user based on a received federated Single Sign-On (SSO) token.
- **User Session Store and Message Store**: The repository containing transient runtime session state data and protocol messages.
- **Configuration Data Store**: The repository containing Oracle Identity Federation configuration data.

9.3 Understanding Oracle Identity Federation Basic and Advanced Installations

There are two types of Oracle Identity Federation 11*g* Release 1 (11.1.1) installations: Basic and Advanced. This topic describes both types of installations and includes the following sections:

- Basic Installation
- Advanced Installation

9.3.1 Basic Installation

The Basic installation deploys Oracle Identity Federation with minimum functionality enabled and the following configuration:

- No User Data Store
- No Federation Store
- JAAS Authentication Engine
- Test Service Provider (SP) Engine
- Memory Session Data Store
- Memory Message Data Store
- XML file system Configuration Store

9.3.2 Advanced Installation

The Advanced installation allows you to choose between different types of data stores and authentication engines. The following is a list and description of the types of data stores and authentication engines you can choose during an Advanced installation:

Authentication Engine

- JAAS: Delegates authentication to the application server.
- LDAP: Uses form login and LDAP bind with credentials supplied by user to authenticate against LDAP repository.

User Data Store

- None: No User Data Store. Typically used with Custom or JAAS Authentication Engines, environments without user attributes, or Windows CardSpace.
- LDAP: Typical configuration that stores user data in an LDAP repository.
- RDBMS: Uses database tables with user names (and optionally user attributes) in columns.

Federation Data Store

- None: No Federation Data Store. Typically used when there are no persistent account linking records. No Federation Data Store is also an alternative to using name identifiers, such as e-mail address, X.509 DN, Kerberos, or Windows Name Identifier.
- LDAP: Stores federation in an LDAP repository. Commonly deployed when the User Data Store is also LDAP.
- RDBMS: Stores federation in a relational database repository. Commonly deployed when the User Data Store is also RDBMS.
- XML: Stores federation data in an XML file system. Commonly used for testing purposes.

User Session Store and Message Store

- Memory: Stores transient runtime session state data and protocol messages in in-memory tables. Commonly used for single instance deployments. Memory provides better performance than the RDBMS User Session Store, but increases runtime memory requirements.
- RDBMS: Stores transient runtime session state data and protocol messages in a relational database. Recommended for High Availability cluster environments.

> **Note:** User Session Store and Message Store appear in the Installer as separate configuration items, however, most deployments use the same type of repository for both stores.

Configuration Data Store

- File System: Stores Oracle Identity Federation configuration data on the local file system. Commonly used in single-instance and testing environments.
- RDBMS: Stores Oracle Identity Federation configuration data in a relational database. Commonly used in High Availability environments or single-instances with failover redundancy.

9.4 Configuring Oracle HTTP Server for Oracle Identity Federation

When you install Oracle Identity Federation, Oracle HTTP Server also gets installed. Oracle HTTP Server is required when using Oracle Identity Federation for enterprise level single sign-on with Oracle Single Sign-On and Oracle Access Manager. Although Oracle Identity Federation can function without Oracle HTTP Server, there are advantages to configuring it as a proxy for Oracle Identity Federation.

To configure the Oracle HTTP Server so that the Oracle Identity Federation application can be accessed through Oracle HTTP Server ports, you can:

- Use the **Install and Configure** option as described in this chapter and select Oracle HTTP Server and Oracle Identity Federation on the Configure Components screen.
- Use the Configuration Wizard (config.sh or config.bat) and select Oracle HTTP Server and Oracle Identity Federation.

> **See:** The "Deploying Oracle Identity Federation with Oracle HTTP Server" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation* for more information about integrating Oracle Identity Federation and Oracle HTTP Server.

9.5 Performing Basic Oracle Identity Federation Installations

This topic describes how to perform a Basic Oracle Identity Federation installation and configuration. It includes the following sections:

9.5.1 Appropriate Deployment Environment

The Basic Oracle Identity Federation installation and configuration is appropriate for:

- Creating a base to gradually build complex implementations upon after installation
- Deploying test environments
- Deploying small, self-contained configurations

9.5.2 Components Deployed

Performing the Basic Oracle Identity Federation installation and configuration deploys the following components:

If you install Oracle Identity Federation in a new domain:

- WebLogic Managed Server
- Oracle Identity Federation
- WebLogic Administration Server
- Fusion Middleware Control
- *Optionally*, Oracle HTTP Server

If you install Oracle Identity Federation in an existing domain:

- WebLogic Managed Server
- Oracle Identity Federation
- *Optionally*, Oracle HTTP Server

9.5.3 Dependencies

The Basic Oracle Identity Federation installation and configuration depends on Oracle WebLogic Server.

9.5.4 Procedure

Perform the following steps to deploy a Basic Oracle Identity Federation installation and configuration:

1. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
2. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
3. On the Select Domain screen, choose whether to install Oracle Identity Federation in a new or existing domain:

To install Oracle Identity Federation in a new domain:

   a. Select **Create New Domain**.
   b. Enter the user name for the new domain in the User Name field.
   c. Enter the user password for the new domain in the User Password field.

      Enter the user password again in the Confirm Password field.
   d. Enter a name for the new domain in the Domain Name field.
   e. Click **Next**. The Specify Installation Location screen appears.

   Continue the installation by going to step 4 now.

To install Oracle Identity Federation in an existing domain:

   a. Select **Extend Existing Domain**.
   b. Enter the name of the host that contains the domain in the Host Name field.
   c. Enter the listen port for the WebLogic Administration Server in the Port field.
   d. Enter the user name for the domain in the User Name field.
   e. Enter the password for the domain user in the User Password field.

   Click **Next**. The Specify Installation Location screen appears.

4. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
5. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.

6. Select **Oracle Identity Federation**—and *optionally*, **Oracle HTTP Server**. Refer to "Configuring Oracle HTTP Server for Oracle Identity Federation" on page 9-3 for information about configuring these two components simultaneously.

   If you are installing Oracle Identity Federation in a new domain, the Fusion Middleware Control management component is automatically selected for installation.

   Ensure no other components are selected and click **Next**. The Configure Ports screen appears.

7. Choose how you want the Installer to configure ports:

   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Select Oracle Identity Federation Configuration Type screen appears.

8. Select **Basic** and click **Next**. The Specify OIF Details screen appears.

9. Enter the following information:

   - PKCS12 Password: Enter the password Oracle Identity Federation will use for encryption and for signing wallets. The Installer automatically generates these wallets with self-signed certificates. Oracle recommends using the wallets only for testing.
   - Confirm Password: Enter the PKCS12 password again.
   - Server ID: Enter a string that will be used to identify this Oracle Identity Federation instance. A prefix of `oif` will be added to the beginning of the string you enter. Each logical Oracle Identity Federation instance within an Oracle WebLogic Server administration domain must have a unique Server ID. Clustered Oracle Identity Federation instances acting as a single logical instance will have the same Server ID.

   Click **Next**. The Installation Summary screen appears.

10. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

9.6 Performing Advanced Oracle Identity Federation Installations

This topic generally describes how to perform an Advanced Oracle Identity Federation installation and configuration. Refer to the next two topics in this chapter for information on performing specific Advanced Oracle Identity Federation installations.

This topic includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

9.6.1 Appropriate Deployment Environment

The Advanced Oracle Identity Federation installation provides a fast and simplified method for deploying Oracle Identity Federation with its vital components integrated and configured.

9.6.2 Components Deployed

Performing the Advanced Oracle Identity Federation installation and configuration deploys the following components:

If you install Oracle Identity Federation in a new domain:

- WebLogic Managed Server
- Oracle Identity Federation
- WebLogic Administration Server
- Fusion Middleware Control
- *Optionally*, Oracle HTTP Server

If you install Oracle Identity Federation in an existing domain:

- WebLogic Managed Server
- Oracle Identity Federation
- *Optionally*, Oracle HTTP Server

9.6.3 Dependencies

The Advanced Oracle Identity Federation installation and configuration depends on the following components:

- Oracle WebLogic Server
- Oracle Database, if using RDBMS for User Store, Federation Store, Session Store, Message Store, or Configuration Store.
- New *Identity Management - Oracle Identity Federation* schema existing in the database, if using RDBMS for Federation Store, Session Store, Message Store, or Configuration Store.
- Database table for storing user dative using RDBMS for User Store
- LDAP repository, if using LDAP for Authentication, User Store, or Federation Store.

9.6.4 Procedure

Perform the following steps to deploy an Advanced Oracle Identity Federation installation and configuration:

1. Decide if you want to use RDBMS for User Store, Federation Store, Session Store, Message Store, or Configuration Store. If you do, perform the following steps a and b.
   a. Install the database for Oracle Identity Federation. Refer to "Installing Oracle Database" on page 3-4 for more information.
   b. Create the *Identity Management - Oracle Identity Federation* schema in the database. Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.

Note: The schema is not required for RDBMS User Stores.

2. Decide if you want to use an LDAP repository for Authentication, User Store, or Federation Store. If you do, you must install the LDAP repository before you can install Oracle Identity Federation.
3. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
4. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
5. On the Select Domain screen, choose whether to install Oracle Identity Federation in a new or existing domain:

To install Oracle Identity Federation in a new domain:

a. Select **Create New Domain**.
b. Enter the user name for the new domain in the User Name field.
c. Enter the user password for the new domain in the User Password field.
d. Enter the user password again in the Confirm Password field.
e. Enter a name for the new domain in the Domain Name field.
f. Click **Next**. The Specify Installation Location screen appears.

Continue the installation by going to step 6 now.

To install Oracle Identity Federation in an existing domain:

a. Select **Extend Existing Domain**.
b. Enter the name of the host that contains the domain in the Host Name field.
c. Enter the listen port for the WebLogic Administration Server in the Port field.
d. Enter the user name for the domain in the User Name field.
e. Enter the password for the domain user in the User Password field.
f. Click **Next**. The Specify Installation Location screen appears.

6. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
7. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.
8. Select **Oracle Identity Federation**—and *optionally*, **Oracle HTTP Server**. Refer to "Configuring Oracle HTTP Server for Oracle Identity Federation" on page 9-3 for information about configuring these two components simultaneously.

If you are installing Oracle Identity Federation in a new domain, the Fusion Middleware Control management component is automatically selected for installation.

Ensure no other components are selected and click **Next**. The Configure Ports screen appears.

9. Choose how you want the Installer to configure ports:

   - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
   - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

   Click **Next**. The Select Oracle Identity Federation Configuration Type screen appears.

10. Select **Advanced** and click **Next**. The Specify OIF Details screen appears.

11. Enter the following information:

    - PKCS12 Password: Enter the password Oracle Identity Federation will use for encryption and for signing wallets. The Installer automatically generates these wallets with self-signed certificates. Oracle recommends using the wallets only for testing.
    - Confirm Password: Enter the PKCS12 password again.
    - Server ID: Enter a string that will be used to identify this Oracle Identity Federation instance. A prefix of `oif` will be added to the beginning of the string you enter. Each logical Oracle Identity Federation instance within an Oracle WebLogic Server administration domain must have a unique Server ID. Clustered Oracle Identity Federation instances acting as a single logical instance will have the same Server ID.

    Click **Next**. The Select OIF Advanced Flow Attributes screen appears.

12. Select the appropriate option for each configuration item and click **Next**.

    Note: User Session Store and Message Store appear in the Installer as separate configuration items, however, most deployments use the same type of repository for both stores.

    The screens that appear next depend on the options you selected for the configuration items on the Select OIF Advanced Flow Attributes screen. The following information describes all possible screens that may appear. This information about all possible screens that may appear is not presented in a linear sequence and your installation may not encounter all of the screens. Enter information for the appropriate screens and proceed to step 13.

If you selected LDAP for Authentication Type, the Specify Authentication LDAP Details screen will appear. Enter the following information:

- LDAP Type: Select the appropriate LDAP repository.
- LDAP URL: Enter the URL connection string for the LDAP repository in the form: *protocol://hostname:port*

Note: If you selected Microsoft Active Directory for the LDAP Type, you must specify an SSL LDAP URL, that is, ldaps://*hostname*:*port*.

- LDAP Bind DN: Enter the bind DN for the LDAP repository.
- LDAP Password: Enter the password for the bind DN.
- User Credential ID Attribute: Enter the LDAP attribute Oracle Identity Federation will use to authenticate users. For example, if you enter **mail** and the value of the mail attribute for a user is jane.doe@domain.com, then Jane Doe must enter **jane.doe.@domain.com** when challenged. Values for the LDAP attribute you identify for User Credential ID Attribute must be unique for all users.
- User Unique ID Attribute: Enter the LDAP attribute that will uniquely identify users to Oracle Identity Federation. The value you enter must be identical to the value you enter for the User Data Store's User ID Attribute parameter. For example, if you enter mail for User Unique ID Attribute and you configure the User Data Store's User ID Attribute parameter with a value of EmailAddress, then the value of mail in the authentication engine repository must equal the value of EmailAddress in the User Data Store. Values for the LDAP attribute you identify for User Unique ID Attribute must be unique for all users.
- Person Object Class: Enter the LDAP object class that represents a user in the LDAP repository. For example: inetOrgPerson for Oracle Internet Directory and Sun Java System Directory Server, and user for Microsoft Active Directory.
- Base DN: Enter the root DN that searches will start from.

If you selected LDAP for User Store, the Specify LDAP Attributes for User Data Store screen will appear. Enter the following information:

- LDAP Type: Select the appropriate LDAP repository.
- LDAP URL: Enter the URL connection string for the LDAP repository in the form: *protocol://hostname:port*

Note: If you selected Microsoft Active Directory for the LDAP Type, you must specify an SSL LDAP URL, that is, ldaps://*hostname*:*port*.

- LDAP Bind DN: Enter the bind DN for the LDAP repository.
- LDAP Password: Enter the password for the bind DN.
- User Description Attribute: Enter the readable LDAP attribute that will identify the owner of a federation record. For example: uid for Oracle Internet Directory and Sun Java System Directory Server, and sAMAccountName for Microsoft Active Directory.
- User ID Attribute: Enter the LDAP attribute that will uniquely identify the user during authentication. For example: uid for Oracle Internet Directory and Sun Java System Directory Server, and sAMAccountName for Microsoft Active Directory.
- Person Object Class: Enter the LDAP object class that represents a user in the LDAP repository. For example: inetOrgPerson for Oracle Internet Directory and Sun Java System Directory Server, and user for Microsoft Active Directory.
- Base DN: Enter the root DN that searches will start from.

If you selected RDBMS for User Store, the Specify User Store Database Details screen will appear. Enter the following information:

- HostName: Enter the connection string to the database host in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
- Username: Enter the database username.
- Password: Enter the password for the database user.
- Login Table: Enter the name of the table that will store user data. The value you enter must be a valid table name, and the values you enter for User ID Attribute and User Description Attribute must be valid column names in the table you identify.
- User ID Attribute: Enter the name of the table column to use for the Oracle Identity Federation user ID. The value you enter must be a valid column name in the table you identified for the Login Table parameter.
- User Description Attribute: Enter the name of the table column to use for the user description. The value you enter must be a valid column name in the table you identified for the Login Table parameter.

If you selected LDAP for Federation Store, the Specify LDAP Attributes for Federation Data Store screen will appear. Enter the following information:

- LDAP Type: Select the appropriate LDAP repository.
- LDAP URL: Enter the URL connection string for the LDAP repository in the form: *protocol://hostname:port*

Note: If you selected Microsoft Active Directory for the LDAP Type, you must specify an SSL LDAP URL, that is, ldaps://*hostname*:*port*.

- LDAP Bind DN: Enter the bind DN for the LDAP repository.
- LDAP Password: Enter the password for the bind DN.
- User Federation Record Context: Enter the location of the container where you want Oracle Identity Federation to store federation records. If the container you identify does not exist, it will be created at runtime. However, if you identify cn=example,dc=test,dc=com as the User Federation Record Context, dc=test,dc=com must exist in the LDAP repository.
- LDAP Container Object Class: *Optional*. Enter the object class for the container that stores federation records. If this field is empty, the default value of applicationProcess is used.
- Active Directory Domain: Appears only if you select Microsoft Active Directory for the LDAP Type. Enter the name of the Microsoft Active Directory domain.

If you selected RDBMS for Federation Store, the Specify Federation Store Database Details screen will appear. Enter the following information:

- HostName: Enter the connection string to the database host in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.

- Username: Enter the name of the schema owner created by RCU, which is of the form *PREFIX*_OIF.
- Password: Enter the password for the database user.

If you selected RDBMS for User Session Store, Message Store, or Configuration Store, the Specify Transient Store Database Details screen will appear. Enter the following information:

- HostName: Enter the connection string to the database host in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
- Username: Enter the name of the schema owner created by RCU, which is of the form *PREFIX*_OIF.
- Password: Enter the password for the database user.

13. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

9.7 Advanced Example: Installing and Configuring Oracle Identity Federation with Oracle Internet Directory in a New WebLogic Administration Domain for LDAP Authentication, User Store, and Federation Store

This section describes how to install and configure Oracle Identity Federation with Oracle Internet Directory in a new WebLogic administration domain for LDAP Authentication, User Store, and Federation Store.

Note: When you install Oracle Identity Federation with Oracle Internet Directory, the Installer automatically configures connection, credential, attribute, and container settings using the Oracle Internet Directory configuration.

This section includes the following information about this installation and configuration:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

9.7.1 Appropriate Deployment Environment

Perform the installation and configuration in this topic to quickly deploy Oracle Identity Federation with Oracle Internet Directory as the LDAP repository for Authentication, User Store, and Federation Store.

9.7.2 Components Deployed

Performing the installation and configuration in this section deploys the following components:

- WebLogic Managed Server
- Oracle Identity Federation
- Oracle Internet Directory
- Oracle Directory Services Manager
- WebLogic Administration Server
- Fusion Middleware Control
- *Optionally*, Oracle HTTP Server

9.7.3 Dependencies

The installation and configuration in this section depends on the following components:

- Oracle WebLogic Server
- Oracle Database for Oracle Internet Directory
- *Identity Management - Oracle Internet Directory* schema existing in the database for Oracle Internet Directory
- Oracle Database for Oracle Identity Federation, if using RDBMS for Session Store, Message Store, or Configuration Store.
- New *Identity Management - Oracle Identity Federation* schema existing in the database for Oracle Identity Federation, if using RDBMS for Session Store, Message Store, or Configuration Store.

9.7.4 Procedure

Perform the following steps to install and configure Oracle Identity Federation with Oracle Internet Directory in a new domain for LDAP Authentication, User Store, and Federation Store:

1. Decide if you want to use RDBMS for Session Store, Message Store, or Configuration Store. If you do, perform the following steps a and b.
   a. Install the database for Oracle Identity Federation. Refer to "Installing Oracle Database" on page 3-4 for more information.
   b. Create the *Identity Management - Oracle Identity Federation* schema in the database. Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.
2. Install the Oracle Database for Oracle Internet Directory. Refer to "Installing Oracle Database" on page 3-4 for more information.
3. Create the *Identity Management - Oracle Internet Directory* schema in the database for Oracle Internet Directory. Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.
4. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
5. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.
6. On the Select Domain screen, select **Create New Domain** and enter the following information:

- User Name: Enter the user name for the new domain.
- User Password: Enter the user password for the new domain.

  Enter the user password again in the Confirm Password field.
- Domain Name: Enter a name for the new domain.

Click **Next**. The Specify Installation Location screen appears.

7. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.
8. Choose how you want to be notified about security issues:
   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.
9. Select **Oracle Internet Directory**, **Oracle Identity Federation**, and *optionally*, **Oracle HTTP Server**. Refer to "Configuring Oracle HTTP Server for Oracle Identity Federation" on page 9-3 for information about configuring Oracle HTTP Server with Oracle Identity Federation.

   The Oracle Directory Services Manager and Fusion Middleware Control management components are automatically selected for this installation.

   Ensure no other components are selected and click **Next**. The Configure Ports screen appears.
10. Choose how you want the Installer to configure ports:
    - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
    - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

    Click **Next**. The Specify Schema Database screen appears.
11. Identify the ODS schema for Oracle Internet Directory that you created in step 3 by selecting **Use Existing Schema** and entering the following information:
    - Enter the database connection information in the Connect String field. The connection string must be in the form of *hostname*:*port*:*servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form of *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
    - Enter the password for the ODS schema in the Password field and click **Next**.

    Note: If your existing ODS and ODSSM schemas have different passwords, the Specify ODSSM Password screen will appear after you click **Next**. Enter the password for your existing ODSSM schema and click **Next**.

The Create Oracle Internet Directory screen appears.

12. Enter the following information for Oracle Internet Directory:
    - Realm: Enter the location for your realm.
    - Administrator Password: Enter the password for the Oracle Internet Directory Administrator.
    - Confirm Password: Enter the administrator password again.

    Click **Next**. The Specify OIF Details screen appears.

13. Enter the following information:
    - PKCS12 Password: Enter the password Oracle Identity Federation will use for encryption and for signing wallets. The Installer automatically generates these wallets with self-signed certificates. Oracle recommends using the wallets only for testing.
    - Confirm Password: Enter the PKCS12 password again.
    - Server ID: Enter a string that will be used to identify this Oracle Identity Federation instance. A prefix of `oif` will be added to the beginning of the string you enter. Each logical Oracle Identity Federation instance within an Oracle WebLogic Server administration domain must have a unique Server ID. Clustered Oracle Identity Federation instances acting as a single logical instance will have the same Server ID.

    Click **Next**. The Select OIF Advanced Flow Attributes screen appears.

    Notes:
    - Notice that the options for Authentication Type, User Store and Federation Store are automatically set to LDAP because you are installing Oracle Internet Directory with Oracle Identity Federation.
    - The Installer sets the User Federation Record Context to cn=fed,*BASE_REALM*, where *BASE_REALM* is typically dc=us,dc=oracle,dc=com.

14. Select the appropriate option for each configuration item and click **Next**:

    Note: User Session Store and Message Store appear in the Installer as separate configuration items, however, most deployments use the same type of repository for both stores.

    - User Session Store: **Memory** or **RDBMS**
      - Select Memory to store transient runtime session state data in in-memory tables.
      - Select RDBMS to store transient runtime session state data in a relational database.
    - Message Store: **Memory** or **RDBMS**
      - Select Memory to store transient protocol messages in in-memory tables

  - Select RDBMS to store transient protocol messages in a relational database.
- Configuration Store: **File** or **RDBMS**
  - Select File to store Oracle Identity Federation configuration data on the local file system.
  - Select RDBMS to store Oracle Identity Federation configuration data in a relational database.

Note: The screens that appear next depend on the options you selected for the configuration items.

- If you selected RDBMS for User Session Store, Message Store, or Configuration Store, go to step 15 now.
- If you did *not* select RDBMS for User Session Store, Message Store, or Configuration Store, go to step 16 now.

---

15. Enter the following information on the Specify Transient Store Database Details screen:
    - HostName: Enter the connection string to the database host in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
    - Username: Enter the name of the schema owner created by RCU, which is of the form *PREFIX*_OIF.
    - Password: Enter the password for the database user.
16. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

9.8 Advanced Example: Installing and Configuring Oracle Identity Federation in a New or Existing WebLogic Administration Domain with RDBMS Data Stores

This topic describes how to install and configure Oracle Identity Federation in a new or existing WebLogic administration domain with RDBMS data stores. It includes the following sections:

- Appropriate Deployment Environment
- Components Deployed
- Dependencies
- Procedure

9.8.1 Appropriate Deployment Environment

Perform the installation and configuration in this topic to quickly deploy Oracle Identity Federation with RDBMS User Store, Federation Store, Session Store, Message Store, and Configuration Store.

9.8.2 Components Deployed

Performing the installation and configuration in this section deploys the following components:

If you install Oracle Identity Federation in a new domain:

- WebLogic Administration Server
- Fusion Middleware Control
- WebLogic Managed Server
- Oracle Identity Federation
- *Optionally*, Oracle HTTP Server

If you install Oracle Identity Federation in an existing domain:

- WebLogic Managed Server
- Oracle Identity Federation
- *Optionally*, Oracle HTTP Server

9.8.3 Dependencies

The installation and configuration in this section depends on the following:

- Oracle WebLogic Server
- Oracle Database for User Store, Federation Store, Session Store, Message Store, and Configuration Store.
- New *Identity Management - Oracle Identity Federation* schema existing in the database for Federation Store, Session Store, Message Store, and Configuration Store.
- Table for storing user data in the User Store database.
- LDAP repository, if using LDAP for Authentication.

9.8.4 Procedure

Perform the following steps to install and configure Oracle Identity Federation in a new or existing domain with RDBMS User Store, Federation Store, User Session Store, Message Store, and Configuration Store:

1. Install the database(s) for the RDBMS User Store, Federation Store, User Session Store, Message Store, and Configuration Store. Refer to "Installing Oracle Database" on page 3-4 for more information.
2. Create the *Identity Management - Oracle Identity Federation* schema in the database(s). Refer to "Creating Database Schema Using the Repository Creation Utility (RCU)" on page 3-5 for more information.
3. Decide if you want to use an LDAP repository for Authentication. If you do, you must install the LDAP repository before you can install Oracle Identity Federation.
4. Install Oracle WebLogic Server. Refer to "Installing Oracle WebLogic Server and Creating the Oracle Middleware Home" on page 3-2 for more information.
5. Start your installation by performing all the steps in "Starting an Installation" on page 4-1. After you complete those steps, the Select Domain screen appears.

6. On the Select Domain screen, choose whether to install Oracle Identity Federation in a new or existing domain:

To install Oracle Identity Federation in a new domain:

a. Select **Create New Domain**.

b. Enter the user name for the new domain in the User Name field.

c. Enter the user password for the new domain in the User Password field.

d. Enter the user password again in the Confirm Password field.

e. Enter a name for the new domain in the Domain Name field.

f. Click **Next**. The Specify Installation Location screen appears.

g. Continue the installation by going to step 7 now.

To install Oracle Identity Federation in an existing domain:

a. Select **Extend Existing Domain**.

b. Enter the name of the host that contains the domain in the Host Name field.

c. Enter the listen port for the WebLogic Administration Server in the Port field.

d. Enter the user name for the domain in the User Name field.

e. Enter the password for the domain user in the User Password field.

f. Click **Next**. The Specify Installation Location screen appears.

7. Identify the Homes, Instances, and the WebLogic Server directory by referring to "Identifying Installation Directories" on page 4-2. After you enter information for each field, click **Next.** The Specify Security Updates screen appears.

8. Choose how you want to be notified about security issues:

   - If you want to be notified about security issues through email, enter your email address in the Email field.
   - If you want to be notified about security issues through My Oracle Support (formerly MetaLink), select the My Oracle Support option and enter your My Oracle Support Password.
   - If you do not want to be notified about security issues, leave all fields empty.

   Click **Next**. The Configure Components screen appears.

9. Select **Oracle Identity Federation**—and *optionally*, **Oracle HTTP Server**. Refer to "Configuring Oracle HTTP Server for Oracle Identity Federation" on page 9-3 for information about configuring these two components simultaneously.

   If you are installing Oracle Identity Federation in a new domain, the Fusion Middleware Control management component is automatically selected for installation.

   Ensure no other components are selected and click **Next**. The Configure Ports screen appears.

10. Choose how you want the Installer to configure ports:

    - Select **Auto Port Configuration** if you want the Installer to configure ports from a predetermined range.
    - Select **Specify Ports using Configuration File** if you want the Installer to configure ports using the staticports.ini file. You can click **View/Edit File** to update the settings in the staticports.ini file.

Click **Next**. The Select Oracle Identity Federation Configuration Type screen appears.

11. Select **Advanced** and click **Next**. The Specify OIF Details screen appears.
12. Enter the following information:
    - PKCS12 Password: Enter the password Oracle Identity Federation will use for encryption and for signing wallets. The Installer automatically generates these wallets with self-signed certificates. Oracle recommends using the wallets only for testing.
    - Confirm Password: Enter the PKCS12 password again.
    - Server ID: Enter a string that will be used to identify this Oracle Identity Federation instance. A prefix of `oif` will be added to the beginning of the string you enter. Each logical Oracle Identity Federation instance within an Oracle WebLogic Server administration domain must have a unique Server ID. Clustered Oracle Identity Federation instances acting as a single logical instance will have the same Server ID.

    Click **Next**. The Select OIF Advanced Flow Attributes screen appears.
13. Select the following and click **Next**:
    - Authentication Type: **JAAS** or **LDAP**
      - Select JAAS to delegate authentication to the application server.
      - Select LDAP to authenticate against an LDAP repository.
    - User Store: **RDBMS**
    - Federation Store: **RDBMS**
    - User Session Store: **RDBMS**
    - Message Store: **RDBMS**
    - Configuration Store: **RDBMS**

    Note: The screen that appears next depends on what you selected for Authentication:
    - If you selected LDAP for Authentication Type, the Specify Authentication LDAP Details screen appears. Continue you installation by going to step 14 now.
    - If you selected JAAS for Authentication Type, the Specify User Store Database Details screen appears. Continue you installation by going to step 15 now.

    ---

14. Enter the following information on the Specify Authentication LDAP Details screen to identify the LDAP repository that will perform authentication:
    - LDAP Type: Select the appropriate LDAP repository.
    - LDAP URL: Enter the URL connection string for the LDAP repository in the form: *protocol://hostname:port*

    Note: If you selected Microsoft Active Directory for the LDAP Type, you must specify an SSL LDAP URL, that is, ldaps://*hostname*:*port*.

- LDAP Bind DN: Enter the bind DN for the LDAP repository.
- LDAP Password: Enter the password for the bind DN.
- User Credential ID Attribute: Enter the LDAP attribute Oracle Identity Federation will use to authenticate users. For example, if you enter **mail** and the value of the mail attribute for a user is jane.doe@domain.com, then Jane Doe must enter **jane.doe.@domain.com** when challenged. Values for the LDAP attribute you identify for User Credential ID Attribute must be unique for all users.
- User Unique ID Attribute: Enter the LDAP attribute that will uniquely identify users to Oracle Identity Federation. The value you enter must be identical to the value you enter for the User Data Store's User ID Attribute parameter. For example, if you enter mail for User Unique ID Attribute and you configure the User Data Store's User ID Attribute parameter with a value of EmailAddress, then the value of mail in the authentication engine repository must equal the value of EmailAddress in the User Data Store. Values for the LDAP attribute you identify for User Unique ID Attribute must be unique for all users.
- Person Object Class: Enter the LDAP object class that represents a user in the LDAP repository. For example: inetOrgPerson for Oracle Internet Directory and Sun Java System Directory Server, and user for Microsoft Active Directory.
- Base DN: Enter the root DN that searches will start from.

Click **Next**. The Specify User Store Database Details screen appears.

15. Enter the following information to identify the database that will store user data:
    - HostName: Enter the connection string to the database host in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
    - Username: Enter the database username.
    - Password: Enter the password for the database user.
    - Login Table: Enter the name of the table that will store user data. The value you enter must be a valid table name, and the values you enter for User ID Attribute and User Description Attribute must be valid column names in the table you identify.
    - User ID Attribute: Enter the name of the table column to use for the Oracle Identity Federation user ID. The value you enter must be a valid column name in the table you identified for the Login Table parameter.
    - User Description Attribute: Enter the name of the table column to use for the user description. The value you enter must be a valid column name in the table you identified for the Login Table parameter.

    Click **Next**. The Specify Federation Store Database Details screen appears.
16. Enter the following information to identify the database that will store federated user account linking data:
    - HostName: Enter the connection string to the database host in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
    - Username: Enter the name of the schema owner created by RCU, which is of the form *PREFIX*_OIF.

- Password: Enter the password for the database user.

Click **Next**. The Specify Transient Store Database screen appears.

17. Enter the following information to identify the database that will store transient runtime session state data, protocol messages, and Oracle Identity Federation configuration data:
    - HostName: Enter the connection string to the database host in the form: *hostname:port:servicename*. For Oracle Real Application Clusters (RAC), the connection string must be in the form: *hostname1*:*port1*:*instance1*^*hostname2*:*port2*:*instance2*@*servicename*.
    - Username: Enter the name of the schema owner created by RCU, which is of the form *PREFIX*_OIF.
    - Password: Enter the password for the database user.

    Click **Next**. The Installation Summary screen appears.
18. Complete the installation by performing all the steps in "Completing an Installation" on page 4-4.

9.9 Verifying Oracle Identity Federation

Verify the Oracle Identity Federation installation by:

- Accessing the Oracle Identity Federation metadata at the following URL. Oracle Identity Federation was installed and the Oracle Identity Federation server is running if you can access the metadata.

  http://*host*:*port*/fed/sp/metadata

  Note: *host* represents the name of the WebLogic Managed Server where Oracle Identity Federation was installed. *port* represents the listen port on that WebLogic Managed Server.

- Accessing Fusion Middleware Control to verify that Oracle Identity Federation is available and running. For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the Oracle Fusion Middleware Administrator's Guide.

9.10 Getting Started with Oracle Identity Federation After Installation

After installing Oracle Identity Federation, refer to the "Common Tasks" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

10

Installing Oracle Single Sign-On and Oracle Delegated Administration Services Against Oracle Internet Directory

This chapter explains how to install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1).

> **Note:** If you already have Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) installed against Oracle Internet Directory Release 10g, refer to the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management* for information on upgrading to Oracle Internet Directory 11*g* Release 1 (11.1.1).

This chapter includes the following topics:

10.1 Understanding the inspre11.pl Script

You must use the inspre11.pl Perl script when installing Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1). This topic describes how to use the inspre11.pl script.

The inspre11.pl script is located in the $*ORACLE_HOME*/ldap/bin/ directory on the host where Oracle Internet Directory 11*g* Release 1 (11.1.1) is installed. Perl is located in the $*ORACLE_HOME*/perl/bin/ directory.

Before you execute the inspre11.pl script, you must set the following environment variables:

- *ORACLE_INSTANCE* to the Oracle Internet Directory 11*g* Release 1 (11.1.1) Oracle Instance location.
- *ORACLE_HOME* to the Oracle Internet Directory 11*g* Release 1 (11.1.1) Oracle Home location.

The following is the syntax for the inspre11.pl script:

```
$OID11gR1_ORACLE_HOME/perl/bin/perl \
$OID11gR1_ORACLE_HOME/ldap/bin/inspre11.pl OID_HOST OID_PORT {-ssl | -nonssl} \
OID_COMPONENT TNS_CONNECT_STRING ODS_PASSWORD ORCLADMIN_PASSWORD \
{-op1 | -op2 | -op3}
```

The following list defines each of the options for the inspre11.pl script:

OID_HOST
Identifies the host where Oracle Internet Directory 11*g* Release 1 (11.1.1) is installed.

OID_PORT
The SSL or non-SSL Oracle Internet Directory port.

-ssl
Indicates the port identified by *OID_PORT* is the Oracle Internet Directory SSL port.

-nonssl
Indicates the port identified by *OID_PORT* is the Oracle Internet Directory non-SSL port.

OID_COMPONENT
The name of the Oracle Internet Directory component, such as oid1. You can identify the name of the Oracle Internet Directory component using the $*ORACLE_INSTANCE*/bin/opmnctl status command.

TNS_CONNECT_STRING
Represents the Oracle Internet Directory database connect string defined in the *ORACLE_INSTANCE*/config/tnsnames.ora file. The default value is oiddb.

> **Note:** Only use the Oracle Internet Directory database connect string defined in the *ORACLE_INSTANCE*/config/tnsnames.ora file—do not use any other tnsnames.ora file to identify the connect string.

ODS_PASSWORD
The password for the ODS schema.

ORCLADMIN_PASSWORD
The password for the Oracle Internet Directory administrator, which is typically cn=orcladmin.

-op1
Enables anonymous bind and disables entry caching. While the -op1 option does not use the *TNS_CONNECT_STRING* value, you must include it when executing inspre11.pl with the -op1 option.

-op2
Resets the Oracle Internet Directory version to allow you to install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0). This option also sets the seealso attribute to point to the database identified by the *TNS_CONNECT_STRING* option.

-op3
Sets the Oracle Internet Directory version back to 11*g* Release 1 (11.1.1) and enables entry caching.

10.2 Procedure

Perform the following steps to install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1):

1. Install Oracle Internet Directory 11*g* Release 1 (11.1.1). Refer to Chapter 5, "Installing and Configuring Oracle Internet Directory" for more information.
2. Execute the inspre11.pl script with -op1. This will enable anonymous bind in Oracle Internet Directory and allow the Oracle Application Server Metadata Repository Creation Assistant (OracleAS RepCA) to load schema into the database for Oracle Single Sign-On and Oracle Delegated Administration Services. Execute the script as follows:

   ```
   $OID11gR1_ORACLE_HOME/perl/bin/perl \
   $OID11gR1_ORACLE_HOME/ldap/bin/inspre11.pl OID_HOST OID_PORT {-ssl | -nonssl} \
   OID_COMPONENT TNS_CONNECT_STRING ODS_PASSWORD ORCLADMIN_PASSWORD -op1
   ```

   Note: If desired, you can disable anonymous bind in Oracle Internet Directory in the last step of this procedure.

3. Use the OracleAS RepCA Release 10.1.4.3.0 to create and load Oracle Single Sign-On 10.1.4.0.1 schema in the database. You can get OracleAS RepCA 10.1.4.3.0 from the Oracle Technology Network (OTN) Web site:

   `http://www.oracle.com/technology/`

   Note: While there is no documentation specifically for OracleAS RepCA Release 10.1.4.3.0, you can use the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for Release 10*g* (10.1.4.0.1) for general information on how to use OracleAS RepCA. Be aware that the database requirements listed in this document do not apply to the OracleAS RepCA Release 10.1.4.3.0.

   You can get the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for Release 10*g* (10.1.4.0.1) from the Oracle Identity Management 10*g* (10.1.4) Documentation Library located on the OTN Web site.

   When you run OracleAS RepCA 10.1.4.3.0:

   - You must register the Oracle Single Sign-On schema with Oracle Internet Directory using its SSL port. This is required for various Oracle Single Sign-On and Oracle Internet Directory interdependencies.
   - You might receive error messages that some database session parameters do not have appropriate values. If you receive these errors, you should reset the parameters identified by OracleAS RepCA, adhering to the minimum values that are given. After you reset the parameters, exit OracleAS RepCA and start it again. If you used SPFILE as the scope in any of the `alter` commands, you may also have to restart the database.
   - Only the schema required for Oracle Single Sign-On will be loaded, not all schema.

4. Reset the ODS password to the value that was set when Oracle Internet Directory was installed and restart Oracle Internet Directory. You must reset the password because it was randomized when you loaded the Oracle Single Sign-On 10.1.4.0.1 schema in the database.

   Perform the following steps:

   a. Use SQL*PLUS to connect the database as the SYS user.

   b. Change the ODS password using `alter user ods` identified by *PASSWORD*, where *PASSWORD* represents the ODS schema password before running the OracleAS RepCA.

   c. Set the TNS_ADMIN environment variable to point to the $*ORACLE_INSTANCE*/config directory.

   d. Execute the following command, where *TNS_CONNECT_STRING* represents the Oracle Internet Directory database connect string defined in the *ORACLE_INSTANCE*/config/tnsnames.ora file. You can set the TNS_ADMIN environment variable if you want to use a different location.

   ```
   $OID11gR1_ORACLE_HOME/ldap/bin/oidpasswd \
   connect=TNS_CONNECT_STRING create_wallet=true
   ```

   e. Restart Oracle Internet Directory.

5. Execute the inspre11.pl script with -op2, which resets the Oracle Internet Directory version and allows you to install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.0.1). The -op2 option will also verify the orcldirectoryversion attribute has a value of OID 10.1.4.0.1.

   Execute the script as follows:

   ```
   $OID11gR1_ORACLE_HOME/perl/bin/perl \
   $OID11gR1_ORACLE_HOME/ldap/bin/inspre11.pl OID_HOST OID_PORT {-ssl | -nonssl} \
   OID_COMPONENT TNS_CONNECT_STRING ODS_PASSWORD ORCLADMIN_PASSWORD -op2
   ```

6. Install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.0.1) in an *ORACLE_HOME* directory that is different from the *ORACLE_HOME* where you installed Oracle Internet Directory. Do not install Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.0.1) in the same *ORACLE_HOME* where you installed Oracle Internet Directory 11*g* Release 1 (11.1.1).

   You can get Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.0.1) from the Oracle Technology Network (OTN) Web site. To access the OTN Web site, go to the following URL:

   `http://www.oracle.com/technology/`

Note: If you are installing Oracle Single Sign-On and Oracle Delegated Administration Services against a Release 11.x database, you must apply **Patch 5649850 for release 10.1.0.5** to the Oracle Single Sign-On *ORACLE_HOME* directory. Patch 5649850 updates the 10.1.0.5 JDBC driver, allowing connectivity to a Release 11.x database.

When you install Oracle Single Sign-On and Oracle Delegated Administration Services, apply patch 5649850 before running the Configuration Assistant on Windows systems, or when you are prompted to run the root.sh script on UNIX systems.

You can get **Patch 5649850 for release 10.1.0.5** from My Oracle Support (formerly MetaLink), located at:

http://metalink.oracle.com/

7. Upgrade Oracle Single Sign-On and Oracle Delegated Administration Services to Release 10*g* (10.1.4.3.0) by applying the Oracle Identity Management 10g (10.1.4.3.0) Patch Set. You can get the Oracle Identity Management 10g (10.1.4.3.0) Patch Set from My Oracle Support (formerly MetaLink) by searching for Bug or Patch Number 7215628.

   You can access My Oracle Support (formerly MetaLink) at:

   http://metalink.oracle.com/

8. Execute the inspre11.pl script with -op3, which sets the Oracle Internet Directory version back to 11*g* Release 1 (11.1.1). For example:

```
$OID11gR1_ORACLE_HOME/perl/bin/perl \
$OID11gR1_ORACLE_HOME/ldap/bin/inspre11.pl OID_HOST OID_PORT {-ssl | -nonssl} \
OID_COMPONENT TNS_CONNECT_STRING ODS_PASSWORD ORCLADMIN_PASSWORD -op3
```

9. Executing the inspre11.pl script with -op1 in step 2 enables anonymous bind in Oracle Internet Directory. If desired, you can disable anonymous bind in Oracle Internet Directory by referring to "Managing Anonymous Binds" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

10.3 Verifying Oracle Single Sign-On and Oracle Delegated Administration Services

Verify the Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) installation against Oracle Internet Directory 11*g* Release 1 (11.1.1) by logging in to Oracle Delegated Administration Services. You will be redirected to Oracle Single Sign-On and prompted to log in. If you have access to the Oracle Delegated Administration Services content after logging in to Oracle Single Sign-On, the installation against Oracle Internet Directory 11*g* Release 1 (11.1.1) was successful.

10.4 Getting Started After Installation

The following information describes how to get started after installing Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1).

10.4.1 Getting Started with Oracle Single Sign-On Release 10g (10.1.4.3.0)

After installing Oracle Single Sign-On Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1) as described in this chapter, refer to the "Basic Administration" chapter in the *Oracle Application Server Single Sign-On Administrator's Guide 10g Release 10.1.4.0.1* available at:

http://www.oracle.com/technology/documentation/oim1014.html

10.4.2 Getting Started with Oracle Delegated Administration Services Release 10g (10.1.4.3.0)

After installing Oracle Delegated Administration Services Release 10*g* (10.1.4.3.0) against Oracle Internet Directory 11*g* Release 1 (11.1.1) as described in this chapter, refer to the "Getting Started with Oracle Delegated Administration Services" chapter in the *Oracle Identity Management Guide to Delegated Administration 10g Release 10.1.4.0.1* available at:

http://www.oracle.com/technology/documentation/oim1014.html

A

Starting and Stopping the Oracle Stack

You must start and stop the components of the Oracle stack in a specific order. This appendix describes that order and contains the following topics:

- Starting the Stack
- Stopping the Stack

> **Note:** When executing the startManagedWebLogic and stopManagedWebLogic scripts described in the following topics:
>
> - The default value for *DOMAIN_NAME* is IDMDomain
> - *SERVER_NAME* represents the name of the Oracle WebLogic Managed Server. The default value for the Oracle Directory Integration Platform and Oracle Directory Services Manager WebLogic Managed Server is wls_ods1. The default value for the Oracle Identity Federation WebLogic Managed Server is wls_oif1.
> - You will be prompted for values for *USER_NAME* and *PASSWORD* if you do not provide them as options when you execute the script.
> - The value for *ADMIN_URL* will be inherited if you do not provide it as an option when you execute the script.

A.1 Starting the Stack

Start the stack components in the following order:

1. Start the Oracle WebLogic Administration Server by executing the following command:

   MW_HOME/user_projects/domains/*DOMAIN_NAME*/bin/startWebLogic.sh

   > **Note:** When you start the Oracle WebLogic Administration Server from the command line, it runs in the foreground and prints output to the screen.

2. Ensure the Node Manager is running. Normally, the Oracle WebLogic Administration Server starts the Node Manager. If the Node Manager is not running, start it by executing the following command:

   MW_HOME/user_projects/domains/*DOMAIN_NAME*/bin/startNodeManager.sh

3. Start system components, such as Oracle Internet Directory and Oracle Virtual Directory, by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the system components have started by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

4. Start WebLogic managed components, such as Oracle Directory Integration Platform, Oracle Identity Federation, and Oracle Directory Services Manager, by executing the following command:

```
MW_HOME/user_projects/domains/DOMAIN_NAME/bin/startManagedWebLogic.sh \
SERVER_NAME {ADMIN_URL}
```

Note: You can use the Oracle WebLogic Administration Console to start managed components in the background. See *Oracle Fusion Middleware Introduction to Oracle WebLogic Server* for more information.

A.2 Stopping the Stack

You can stop the Oracle WebLogic Administration Server and all the managed servers by using Oracle WebLogic Administration Console. See *Oracle Fusion Middleware Introduction to Oracle WebLogic Server* for more information.

To stop the stack components from the command line, perform the following steps:

1. Stop WebLogic managed components, such as Oracle Directory Integration Platform, Oracle Identity Federation, and Oracle Directory Services Manager, by executing the following command:

```
MW_HOME/user_projects/domains/DOMAIN_NAME/bin/stopManagedWebLogic.sh \
{SERVER_NAME} {ADMIN_URL} {USER_NAME} {PASSWORD}
```

2. Stop system components, such as Oracle Internet Directory and Oracle Virtual Directory, by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

3. Stop the Oracle WebLogic Administration Server by executing the following command:

```
MW_HOME/user_projects/domains/DOMAIN_NAME/bin/stopWebLogic.sh
```

4. If you want to stop the Node Manager, you can use the `kill` command:

```
kill -9 PID
```

B

Performing Silent Installations

This appendix describes how to install Oracle Identity Management in silent mode. This appendix contains the following topics:

B.1 What is a Silent Installation?

A silent installation eliminates the need to monitor the Oracle Identity Management installation because no graphical output is displayed and no input by the user is required.

To perform a silent Oracle Identity Management installation, you invoke the Installer with the -silent flag and provide a response file from the command line. The response file is a text file containing variables and parameter values which provide answers to the Installer prompts.

B.2 Before Performing a Silent Installation

This topic describes tasks that may be required before you perform a silent installation. This topic includes the following sections:

B.2.1 UNIX Systems: Creating the oraInst.loc File

The Installer uses the Oracle inventory directory to keep track of all Oracle products installed on the systems. The inventory directory is stored in a file named oraInst.loc. If this file does not already exist on your system, you must create it before starting a silent installation.

Perform the following steps to create the oraInst.loc file if it does not exist:

1. Log in as the root user.
2. Using a text editor such as vi or emacs, create the oraInst.loc file in any directory. The contents of the file consist of the following two lines:

```
inventory_loc=oui_inventory_directory
inst_group=oui_install_group
```

Replace *oui_inventory_directory* with the full path to the directory where you want the Installer to create the inventory directory. Replace *oui_install_group* with the name of the group whose members have write permissions to this directory.

3. Exit from the root user.

> **Note:** After you performing the silent installation on UNIX platforms, you must run the *ORACLE_HOME*/root.sh script as the root user. The root.sh script detects settings of environment variables and enables you to enter the full path of the local bin directory.

B.2.2 Windows Systems: Creating the Registry Key

If you have not installed Oracle Identity Management on your system, you must create the following Registry key and value:

```
HKEY_LOCAL_MACHINE / SOFTWARE / Oracle / inst_loc = [inventory_directory]
```

Replace *inventory_directory* with the full path to your Installer files. For example: C:Program Files\Oracle\Inventory

B.3 Creating Response Files

Before performing a silent installation, you must provide information specific to your installation in a response file. Response files are text files that you can create or edit in a text editor. The Installer will fail if you attempt a silent installation using a response file that is not configured correctly.

Several default response files, which you can use as templates and customize for your environment, are included in the installation media. These default response files are located in the Disk1/stage/Response directory on UNIX, or in the Disk1\stage\Response directory on Windows.

The following is a list of the default response files included in the installation media:

- im_install_only.rsp: Use this response file to install Oracle Identity Management components without configuring them.
- im_install_config.rsp: Use this response file to install and configure Oracle Identity Management components.
- im_config_only.rsp: Use this response file with the Oracle Identity Management 11g Release 1 (11.1.1) Configuration Wizard (config.sh script or config.bat) in *ORACLE_HOME*/bin/ to configure installed components.

B.3.1 Securing Your Silent Installation

Your response files contain certain passwords required by the Installer. To minimize security issues regarding these passwords in the response file, follow these guidelines:

- Set the permissions on the response files so that they are readable only by the operating system user who will be performing the silent installation.
- If possible, remove the response files from the system after the silent installation is completed.

B.4 Performing a Silent Installation

To perform a silent Oracle Identity Management installation, you invoke the Installer with the -silent flag and provide a response file from the command line.

On UNIX

The following is the syntax for running the Installer from the command line on UNIX systems:

```
runInstaller [-mode] [-options] [(COMMAND_LINE_VARIABLE=VARIABLE_VALUE)*]
```

For example:

```
./runInstaller -silent -response FILE
```

On Windows

The following is the syntax for running the Installer from the command line on Windows systems:

```
setup.exe [-mode] [-options] [(COMMAND_LINE_VARIABLE=VARIABLE_VALUE)*]
```

For example:

```
setup.exe -silent -response FILE
```

B.5 Installer Command Line Parameters

Table B–1 lists and describes supported Installer command line parameters:

Table B–1 Installer Command Line Parameters

Parameter	Description
Installation Modes - Only One Mode Can be Specified	
-i | -install	Launches the Installer in GUI mode. This is the default mode and is used if no mode is specified on the command line.
-silent	Install in silent mode. The Installer must be passed either a response file or command line variable value pairs.
-d | -deinstall	Launches the Installer in GUI mode for deinstallation.
-p | -prerequisite	Launches the Installer in GUI mode but only checks the prerequisites. No software is installed.
-v | -validate	Launches the Installer in GUI mode and performs all prerequisite and validation checking, but does not install any software.
-sv | -silentvalidate	Performs all prerequisite and validation checking in silent mode. You must pass the Installer either a response file or a series of command line variable value pairs.
Installation Options	
-help | --help | --usage	Displays the usage parameters for the runInstaller command.
-invPtrLoc *file*	Pointer to the inventory location file. Replace file with the full path and name of the oraInst.loc file.
-response *file* | -responseFile *file*	Pointer to the response file. Replace file with the full path and name of the response file.

Table B–1 (Cont.) Installer Command Line Parameters

Parameter	Description
-jreLoc *location*	Pointer to the location where Java Runtime Environment (JRE) is installed. Replace *location* with the full path to the jre directory where your JRE is installed.
-logLevel *level*	Specify the level of logging performed by the Installer; all messages with a lower priority than the specified level will be recorded. Valid levels are: ■ severe ■ warning ■ info ■ config ■ fine ■ finer ■ finest
-debug	Obtain debug information from the Installer.
-force	Allow the silent installation to proceed in a non-empty directory.
-printdiskusage	Log debugging information pertaining to disk usage.
-printmemory	Log debugging information pertaining to memory usage.
-printtime	Log debugging information pertaining to time usage. This command causes the timeTakentimestamp.log file to be created.
-waitforcompletion	Windows only - the Installer will wait for completion instead of spawning the Java engine and exiting.
-noconsole	Messages will not be displayed to the console window.
-ignoreSysPrereqs	Ignore the results of the system prerequisite checks and continue with the installation.
-executeSysPrereqs	Execute the system prerequisite checks only, then exit.
-paramFile *file*	Specify the full path to the oraparam.ini file. This file is the initialization file for the Installer. The default location of this file is Disk1/install/platform.
-novalidation	Disables all validation checking performed by the Installer.
-nodefaultinput	For the GUI install, several screens have information or default values pre-populated. Specifying this option disables this behavior so that no information or values are pre-populated.
Command Line Variables	
Installer Variables	Installer variables are specified using *varName=value*. For example: `ORACLE_HOME=/scratch/install/Oracle_IDM1`
Session Variables	Session variables are specified using session:*varName=value*

C

Deinstalling and Reinstalling Oracle Identity Management

This appendix provides information about deinstalling and reinstalling Oracle Identity Management 11*g* Release 1 (11.1.1). It contains the following topics:

- Deinstalling Oracle Identity Management 11g Release 1 (11.1.1)
- Reinstalling Oracle Identity Management 11g Release 1 (11.1.1)

> **Note:** Always use the instructions provided in this appendix for removing the software. If you try to remove the software manually, you may experience problems when you try to reinstall the software. Following the procedures in this appendix ensures that the software is properly removed.

C.1 Deinstalling Oracle Identity Management 11*g* Release 1 (11.1.1)

This topic contains procedures for deinstalling Oracle Identity Management 11*g* Release 1 (11.1.1) and contains the following sections:

- Deinstalling the Oracle Identity Management Oracle Home
- Deinstalling the Oracle Common Home
- Deinstalling Applications Registered with Oracle Single Sign-On 10g Release 10.1.4.3.0

C.1.1 Deinstalling the Oracle Identity Management Oracle Home

The deinstaller attempts to remove the Oracle Home directory from which it was started. Before you choose to remove your Oracle Identity Management Oracle Home directory, make sure that it is not in use by an existing domain and that you stop all running processes that use this Oracle Home.

Deinstalling Oracle Identity Management will not remove any WebLogic domains that you have created—it only removes the software in the Oracle Identity Management Oracle Home directory.

This section describes how to deinstall your Oracle Identity Management Oracle Home using the graphical, screen-based deinstaller. However, you can also perform a silent deinstallation using a response file. A deinstall response file template that you can customize for your deinstallation is included in the Disk1/stage/Response directory on UNIX, or in the Disk1\stage\Response directory on Windows.

Perform the following steps to deinstall your Oracle Identity Management Oracle Home using the graphical, screen-based deinstaller:

1. Verify your Oracle Identity Management Oracle Home is not in use by an existing domain.
2. Stop all processes that use the Oracle Identity Management Oracle Home.
3. Open a command prompt and move (cd) into the *IDENTITY_MANAGEMENT_ORACLE_HOME*/oui/bin directory (UNIX) or the *IDENTITY_MANAGEMENT_ORACLE_HOME*\oui\bin directory (Windows).
4. Invoke the Deinstaller from command line using the -deinstall option. For example:

   On UNIX:

   ```
   ./runInstaller -deinstall
   ```

   On Windows:

   ```
   setup.exe -deinstall
   ```

   The Welcome screen appears.
5. Click **Next**. The Select Deinstallation Type screen appears.
6. Select the deinstallation type you want to perform. Table C–1 lists and describes each of the deinstallation types:

Table C–1 Deinstallation Types

Type	Description
Deinstall Oracle Home	Select this option to deinstall the binaries contained in the listed Oracle Identity Management Oracle Home. If you select this option, the Deinstall Oracle Home screen appears next, where you can save a response file that contains the deinstallation settings before deinstalling.
Deinstall ASInstances managed by WebLogic Domain	Select this option to deinstall the Oracle Identity Management system component instances, such as Oracle Internet Directory and Oracle Virtual Directory, that are registered in a WebLogic domain. If you select this option, the Specify WebLogic Domain Detail screen appears next where you identify the administration domain containing the system components you want to deinstall. The Select Managed Instance screen appears next, where you identify the instances you want to deinstall.
DeInstall Unmanaged ASInstances	Select this option to deinstall the Oracle Identity Management system component instances, such as Oracle Internet Directory and Oracle Virtual Directory, that are not registered in a WebLogic domain. If you select this option, the Specify Instance Location screen appears next where you identify the instances you want to deinstall.

7. Regardless of the option you choose and the subsequent screens that appear, you will arrive at the Deinstall Progress screen, which shows the progress and status of the deinstallation. If you want to quit before the deinstallation is completed, click **Cancel**.

Click **Finish** after the deinstallation progresses to 100%. The Deinstallation Complete screen appears.

8. Click **Finish** on the Deinstallation Complete screen to exit the deinstaller.

C.1.2 Deinstalling the Oracle Common Home

The *ORACLE_COMMON_HOME* directory located in the *MW_HOME* directory contains the binary and library files required for Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF). Before you deinstall the *ORACLE_COMMON_HOME* directory, ensure that no other Oracle Fusion Middleware software, such as Oracle SOA Suite, depends on *ORACLE_COMMON_HOME*. You cannot deinstall the *ORACLE_COMMON_HOME* directory until all software that depends on it has been deinstalled.

Perform the following steps to deinstall the *ORACLE_COMMON_HOME* directory:

1. Stop all processes that use the *ORACLE_COMMON_HOME* directory.
2. Deinstall your Oracle Identity Management Oracle Home by performing the steps in Deinstalling the Oracle Identity Management Oracle Home.
3. Open a command prompt and move (cd) into the *ORACLE_COMMON*/oui/bin/ directory (on UNIX) or the *ORACLE_COMMON_HOME*\oui\bin\ directory (on Windows).
4. Invoke the Deinstaller from command line using the -deinstall option and the -jreLoc option, which identifies the location where Java Runtime Environment (JRE) is installed. For example:

   On UNIX:

   ```
   ./runInstaller -deinstall -jreLoc FULL_PATH_TO_JRE_DIRECTORY
   ```

   On Windows:

   ```
   setup.exe -deinstall -jreLoc FULL_PATH_TO_JRE_DIRECTORY
   ```

   The Welcome screen appears.
5. Click **Next**. The Select Deinstallation Type screen appears.
6. Select the **Deinstall Oracle Home** option at the top of the Select Deinstallation Type screen.

   Note: The path to the *ORACLE_COMMON_HOME* directory appears in the text describing the **Deinstall Oracle Home** option.

   Click **Next**. The Deinstall Oracle Home screen appears.
7. Confirm the correct *ORACLE_COMMON_HOME* directory is listed and click **Deinstall**.

   The Deinstallation Progress screen appears, along with a Warning dialog box prompting you to confirm that you want to deinstall the *ORACLE_COMMON_HOME* directory.
8. Click **Yes** on the Warning dialog box to confirm you want to remove the *ORACLE_COMMON_HOME* directory. The deinstallation begins.
9. Click **Finish** after the deinstallation progresses to 100%. The Deinstallation Complete screen appears.

10. Click **Finish** on the Deinstallation Complete screen to exit the deinstaller.

C.1.3 Deinstalling Applications Registered with Oracle Single Sign-On 10*g* Release 10.1.4.3.0

To deinstall a partner application registered with Oracle Single Sign-On 10*g* Release 10.1.4.3.0, you must manually deregister the partner application from Oracle Single Sign-On. Refer to the "Reregister mod_osso on the single sign-on middle tiers" section in Chapter 9 of the *Oracle Application Server Single Sign-On Administrator's Guide 10g Release 10.1.4.0.1* available at:

`http://www.oracle.com/technology/documentation/oim1014.html`

C.2 Reinstalling Oracle Identity Management 11*g* Release 1 (11.1.1)

Perform the following steps to reinstall Oracle Identity Management 11*g* Release 1 (11.1.1):

1. Verify the directory you want to reinstall Oracle Identity Management into does not contain an existing Oracle Identity Management instance. If it does, you must deinstall it before reinstalling. You cannot reinstall Oracle Identity Management 11*g* Release 1 (11.1.1) in a directory that contains an existing Oracle Identity Management instance.
2. Reinstall Oracle Identity Management as if it was the first installation by performing the steps in the appropriate procedure in this guide.

D

Troubleshooting the Installation

This appendix describes solutions to common problems that you might encounter when installing Oracle Identity Management. It contains the following topics:

- General Troubleshooting Tips
- Installation Log Files
- Need More Help?

D.1 General Troubleshooting Tips

If you encounter an error during installation:

- Consult the Oracle Fusion Middleware 11*g* Release 1 (11.1.1). You can access the Release Notes on the Oracle Technology Network (OTN) Documentation Web site. To access this Web site, go to the following URL:

  `http://www.oracle.com/technology/documentation`

- Verify your system and configuration is certified. See "System Requirements and Certification" on page 3-1 for more information.
- Verify your system meets the minimum system requirements. See "System Requirements and Certification" on page 3-1 for more information.
- Verify you have satisfied the dependencies for the deployment you are attempting. Each deployment documented in this guide contains a "Dependencies" section.
- If you entered incorrect information on one of the installation screens, return to that screen by clicking **Back** until you see the screen.
- If an error occurred while the Installer is copying or linking files:
  1. Note the error and review the installation log files.
  2. Remove the failed installation. See "Deinstalling Oracle Identity Management 11g Release 1 (11.1.1)" on page C-1 for more information.
  3. Correct the issue that caused the error.
  4. Restart the installation.

D.2 Installation Log Files

The Installer writes log files to the *ORACLE_INVENTORY_LOCATION*/logs directory on UNIX systems and to the *ORACLE_INVENTORY_LOCATION*\logs directory on Windows systems.

On UNIX systems, if you do not know the location of your Oracle Inventory directory, you can find it in the *ORACLE_HOME*/oraInst.loc file.

On Microsoft Windows systems, the default location for the inventory directory is C:\Program Files\Oracle\Inventory\logs.

The following install log files are written to the log directory:

- install*DATE-TIME_STAMP*.log
- install*DATE-TIME_STAMP*.out
- installActions*DATE-TIME_STAMP*.log
- installProfile*DATE-TIME_STAMP*.log
- oraInstall*DATE-TIME_STAMP*.err
- oraInstall*DATE-TIME_STAMP*.log

D.3 Need More Help?

If you cannot solve a problem using the information in this appendix, look for additional information in My Oracle Support (formerly MetaLink) at http://metalink.oracle.com.

If you cannot find a solution to your problem, open a service request.